

総合情報基盤センター新システム概要  
～ 学内組織との連携強化～  
Outline of New System of Computer and Network  
Center  
～ Cooperation with Administration Sections in  
University～

江藤博文、只木進一

Hirofumi ETO, Shin-ichi TADAKI

佐賀大学総合情報基盤センター

Computer and Network Center, Saga University

840-8502 佐賀市本庄町 1

1 Honjo, Saga 840-8502

*etoh@cc.saga-u.ac.jp, tadaki@cc.saga-u.ac.jp*

## 概要

総合情報基盤センターは2006年3月にシステム更新を行った。以前のシステムを継承しつつ、教務システムも同時に導入するなど事務組織との連携が強化された。新システムでは特に利用者情報・認証の統合を軸に作業を行った。この更新により、利用者情報の収集が容易となりまた、学内の各種情報システムへの認証の提供が可能となった。

## キーワード

利用者情報、認証、統合認証システム

## Abstract

Saga University replaced its main information system in March, 2006. Based on the same concept as in the previous system, the new system includes a student information system by introducing the new framework for cooperating with administration sections. The core of the system is a unified user management and authentication system, where data are collected online by the student-affairs sections and the human-resource section. The system provides user information and authentication to various information systems in our university.

## Keywords

User Information, Authentication, Integrated Authentication System

## 1 はじめに

総合情報基盤センター（以下、センターとする）では、2006年3月にシステムの更新を行った。今回のシステム更新では前回のシステムを踏襲しつつ、利用者情報・認証の統合を中心的な課題として事務組織との連携の強化を図っている。

新システムでは、センターの教育研究用システムだけではなく、利用者情報・認証の統合を考慮し、人事情報、学生情報、事務情報、図書館情報を包括的に設計した。事務との連携が強化されたことで、これら利用者に付随する情報の統合的な管理を行うことが可能となった。

新システムはセンターの教育研究システム、図書館システム、教務システム、事務端末、統合認証システムに分けることができる。

教育研究システムの演習用端末は、前回導入したディスクレス端末システムであるVID[1]の最新機器を導入し、更なる保守管理コストの削減を図った。また、センター内だけではなく図書館および就職相談室にも同じ端末を設置した。プリンタの管理にはPrintProcurer[2]を導入し、利用者あたり月300枚の印刷制限を行っている。

図書館システムは以前のシステムと同じNALIS[3]を導入し、センターとの更なる連携を図っている。

教務システムにはLiveCampus[4]を導入した。以前の教務システムは独立したシステムであったが、新システムではセンターの統合認証システムと連携が可能となるようにカスタマイズを行った。

事務端末はセンターの認証の配下に置き、利用時にユーザ名、パスワードで認証を行う仕様となった。

人事担当との連携のため、統合認証システムに人事入力インタフェースを開発した。既存の人事システムは現状のままとし、既存システムには無い詳細な検索機能などを付加することで両システムを共存させていくこととした。統合認証システム[5]は教務システム、図書館システム、人事担当とオンラインで結ばれ、連携が強化された。

システム構成を図1に示す。

## 2 利用者情報・認証の統合

### 2.1 必要性

利用者情報は情報システムにおける最も基本的な情報である。また、この情報に基づいて、認証と権限管理が行われる。この情報が不完全、不正確であることは、情報システムの管理運用の大きな障害となる。

近年、大学内に多数のオンライン情報システムが構築されている。従来は、個々の情報システムごとに利用者管理が行われてきた。このことが、利用者情報が不完全、不正確であることと、管理コストの増大の大きな原因となっている。また、利用者側からみると、複数のアカウントを持たされることになり、パスワード忘れやパスワード遺漏の原因となってきた。

組織内の情報システムに共通の利用者情報管理と認証機構を提供することは、システムの合理化の面だけでなく、利便性及び安全性の観点から非常に重要である。利用者情報と認証の統合により、複数の情報システムに対して、一貫した権限管理を導入し、効率性と安全性を高めることができる。利用者は、一つのアカウントだけを持つことになり、利便性が高まる。さらに、不正アクセスや情報遺漏の場合に、迅速に原因を特定できる。

特に、共通の利用者情報が、人事担当や教務担当などの原情報を有する部署から提供されることで、その情報の完全性と正確さが高められる。つまり、情報システムだけではなく、人事担当や教務担当との連携が不可欠である。

### 2.2 利用者情報収集

利用者情報を収集するにあたり、新システムでは対応する事務部署との連携を強化した。特に、統合認証システムでは図書館システム、教務システム、人事担当との連携の強化が行われ、学生情報及び教職員情報、図書館情報はすべてオンラインで統合認証システムに統合されることとなった。

各システム及び他の組織との関連図を図2に示す。

佐賀大学総合情報基盤システム構成図

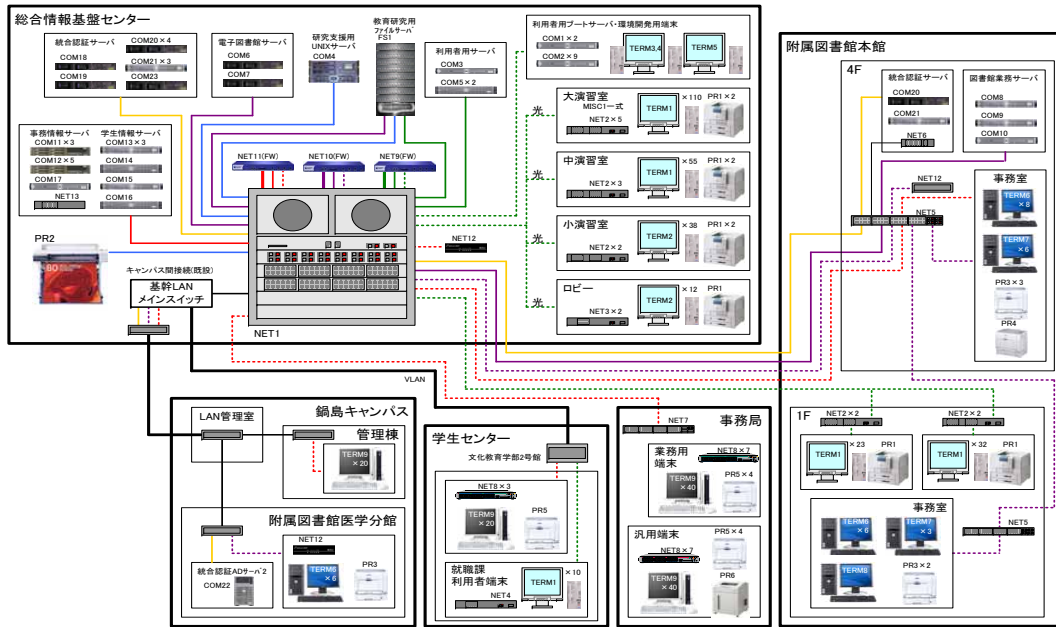


図 1: システム構成

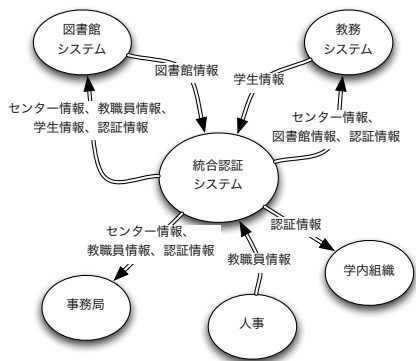


図 2: 統合認証関連図

利用者は大きく学生と教職員とその他に分けることができる。学生は教務システムから、教職員は人事担当から、その他については直接利用者情報がセンターへ届けられる。

教職員の情報を扱う人事担当には既存の人事システムが存在する。新システムでは統合認証システムに既存の人事システムを参考と同じ項目を入力可能なインターフェースを構築した。人事担当は統合認証の人事インターフェースから必要な情報を入力する。

その結果を既存の人事システムが取り込み可能な形式のファイルで保存し既存の人事システムに取り込む。

学生の利用者情報は教務システムで登録が行われる。教務システムは、登録された学生の利用者情報のうち必要な情報のみを統合認証システムにオンラインで送る。統合認証システムは送られてきた学生情報をもとにセンターのIDを作成するとともに必要な情報のみを図書館システムにオンラインで送る。

図書館システムは学生の利用者情報に図書館に必要な情報を付加し、統合認証システムにオンラインで送る。統合認証システムは学生の利用者情報に図書館情報とセンター情報を付加し、教務システムに送る。

教務システムは必要な情報を学生証に印字し学生に配布する。学生の登録にかかる作業では、すべてをオンラインで行うことが可能となった。

教職員の利用者情報は人事担当で登録が行われる。人事担当から入力された利用者情報は既存利用者と比較し、既存の利用者に同一利用者の存在の有無を確認する。同一利用者が存在しない利用者は登録候補の一覧として統合認証システムの管理画面に

表示される。センターの事務職員は登録候補一覧を確認し、登録が必要かどうかを判断し採用日を考慮して登録を行う。

## 3 利用者情報・認証の提供

### 3.1 認証の提供

センターでは統合認証システムに登録された利用者情報・認証を学内のサービスに提供している。

演習端末及び事務端末の認証のために統合認証システムでは認証を提供している。演習端末は Windows と Linux のデュアルブートである。そこで、統合認証システムでは Windows のために ActiveDirectory での認証を提供し、Linux のために LDAP での認証を提供している。事務端末は Windows だけのシングルブートなので、ActiveDirectory での認証を提供している。

Web 認証方式はサイトを運用する Web サーバの実装により様々な方式が存在する。これらの認証方式に対応するために統合認証システムでは LDAPS、POP3S、IMAPS、RADIUS などのいくつかの一般的な認証を提供している。

Opengate[6, 7, 8, 9, 10, 11] はセンターで開発した端末認証システムである。学生の個人所有の PC など、外部から持ち込まれた端末などでネットワークを利用際に認証を行う。この認証のためにセンターは認証を提供している。

### 3.2 利用者情報の提供

従来、人事以外の事務組織に必要な職員情報は人事担当から書類による提供を受けていた。新システムから、アクセス元及び利用者を制限しながらオンラインによる提供を行うこととなった。

現在、学内の一部で入退室管理のために電子錠の導入が行われている。電子錠を運用するためには利用者を一意に特定し、権限を管理する必要がある。しかし、既存の学内の組織で利用者を一意に特定が可能なのはセンターの統合認証システムだけである。そこで、センターから入退室管理のための利用者情報を提供することとした。

### 3.3 実装

利用者情報・認証の提供には、利用者情報を保持するデータベースとウェブサーバ、認証を提供する LDAP サーバにより構成される。

各組織から入力された利用者情報はデータベースと連携したウェブサーバにより利用者情報を必要とする組織に提供される。

認証を提供する LDAP サーバは複数の LDAP サーバにより構成され、各 LDAP サーバはメインの LDAP サーバと同期がとられている。但し、同期をとるのはユーザ名とパスワードのみである。各 LDAP サーバはセンターの演習端末の Linux 認証のための LDAP サーバと Windows 認証のための ActiveDirectory サーバ、事務端末認証のための ActiveDirectory サーバ、POP3S などの各種認証サービスのための LDAP サーバが置かれている。

事務端末は取り扱いに注意が必要な情報へのアクセスを行うため、ログインは厳密に規制しなければならない。このため、事務端末認証用 ActiveDirectory サーバへは初期登録状態では全てのアカウントが無効となっている。事務端末が利用可能な利用者を事務局の情報部門が統合認証システムを通して把握し、事務端末認証用 ActiveDirectory サーバのアカウントを有効化する。また、退職などで利用者がなくなった場合、センターのアカウントはしばらく残るが、事務端末認証用 ActiveDirectory サーバのアカウントは即座に無効化される。

複数の LDAP サーバが置かれているため、パスワードの変更の同期は非常に重要である。本システムではパスワード変更専用ウェブページを用意した。利用者がこのパスワード変更用ウェブページを介してパスワードを変更すると、メインの LDAP サーバからリアルタイムで各 LDAP サーバにパスワードの同期が行われる。

## 4 まとめと議論

センターでは 2006 年 3 月に新システムを導入した。新システムでは特に利用者情報・認証の統合を主に更新を行った。事務組織との連携が強化され、利用者情報の収集などの管理コストが削減され、厳

密な管理が可能となった。統合された利用者情報・認証により学内の各種サービに対して情報の提供が可能となった。

近年、業務の効率化のために様々な情報システムが導入されるようになった。一般に、情報システムの導入時のコストは考慮されるが、運用に要するコストは考慮されにくい。特に、情報システムの利用者情報を厳密に管理するための運用体制とコストは考慮されてこなかった。

組織内に複数の情報システムが導入され、組織の構成員が多数の情報システムを利用する場合には、利用者情報の管理は非常に重要になる。利用者情報の統合は運用コストの面だけではなく、セキュリティ面からも重要になる。システムへの組織内からの不正アクセスや、個人情報などの重要情報の漏洩を未然に防ぐためにも、利用者情報とアクセス権限の適切な管理が行われなければならない。その管理が継続して行われるためには、利用者情報の統合を可能とする技術的及び組織的対策が必要である。

新システムでは上記を考慮し、利用者情報及び認証の統合を行った。教育研究用情報システムを中心に据え、そこに人事担当部署と教務担当部署が情報を提供し、かつ事務情報システム及び教務情報システムに利用者情報を提供する形態とした。

大学業務のオンライン化が進むにつれ、様々な情報システムが構築される。こうした情報システムが適切に、かつ効率よく運用されるためには、全額統一的な利用者情報と認証の統合が必要である。新システムは、全額統一的な利用者情報と認証の統合を可能とする技術的方法を導入することに成功した。しかし、このシステムを運用するための組織的、規則的整備が残されている。

## 参考文献

- [1] 株式会社 ミントウェーブ  
「VID(Virtual Image Distributor)」  
<http://www.mintwave.co.jp/tc/vid.html>
- [2] 株式会社 Canon 「マルチ OS 対応 プリント出力上限管理システム:Print Producer」  
<http://cweb.canon.jp/Product/appli/printproducer/>
- [3] 株式会社 NTT データ九州「新世代図書館システム:NALIS(NTTDATA's Advanced Library Information System)」  
<http://www.nttdata-kyushu.co.jp/product/nalis.html>
- [4] 株式会社 NTT データ九州「次世代学内情報システム:LiveCampus」
- [5] 江藤博文、渡辺健次、只木進一、渡辺義明「大学における情報基盤整備の中核となる統合認証システム」分散システム/インターネット運用技術シンポジウム 2003, pp.43-48 (2003)
- [6] 渡辺健次、江藤博文、只木進一、渡辺義明「利用者認証と利用記録機能を実現するゲートウェイシステム Opengate の開発」信額技報告,IN99-95,TM99-61,OFS99-48,pp.43-48(2000).
- [7] 渡辺義明、渡辺健次、江藤博文、只木進一「利用と管理が容易で適用範囲が広い利用者認証ゲートウェイシステムの開発」情報処理学会論文誌,Vol.42,No.12,pp.2802-2809(2001).
- [8] 只木進一、江藤博文、渡辺健次、渡辺義明「公開端末及び利用者移動端末の認証システムとそのディスクレスマシンによる運用」学術情報処理研究,No.5,pp.15-20(2001).
- [9] 安田進一、羽石寛志、渡辺健次、渡辺義明、江藤博文、只木進一「Opengate を利用した公開端末の認証および利用記録」信額技報告,TM2004-12,pp.7-11(2004).
- [10] 江藤博文、只木進一、渡辺健次、渡辺義明「新しい教育用情報基盤の実現へ向けて-認証システムをベースとしたキャンパス規模のオープンネットワーク」学術情報処理研究,No.6,pp.13-20(2002).
- [11] 只木進一、江藤博文、渡辺健次、渡辺義明「利用者移動端末に対応したネットワークの運用-佐賀大学での Opengate の運用-」情報処理学会シンポジウムシリーズ,Vol.2004,No.3,pp.85-90(2004)