

# 福岡大学における統合認証システムの構築と運用について

奥村 勝<sup>†</sup>, 本山 聡<sup>††</sup>, 三河 邦夫<sup>††</sup>,

<sup>†</sup> 福岡大学総合情報処理センター <sup>††</sup> (株) 日本総合研究所

福岡大学では、これまで学内の情報システム毎に認証システムを構築し、運用を行ってきた。しかしながら、情報システムの増加に伴い、個別認証システムでは、利用者や運用部門の負担の増加が問題となっていた。この問題を解決すべく、認証システムを一元化する統合認証システムを新たに構築した。本論文では、統合認証システムの導入目的、設計方針ならびにシステム構成等について報告する。

## Construction and Operation Method of the Common Authentication System in the Fukuoka University

Masaru OKUMURA<sup>†</sup> Satoshi MOTOYAMA<sup>††</sup> Kunio MIKAWA<sup>††</sup>

<sup>†</sup> Information Technology Center, Fukuoka University

<sup>††</sup> The Japan Research Institute, Limited

In Fukuoka University, the authentication system of each information system is constructed, and has been operated. However, an increase in the load of the user and the operation section became a problem in an individual authentication system as the number of information systems increased. To solve these problems, a common authentication system that unified the authentication system was constructed. In this paper, we report on the purpose, the design policy of the common authentication system, and the system configuration, etc.

### 1 はじめに

近年、大学における情報化は加速しており、従来の教育研究分野以外にも学生生活支援や教職員の業務において、各種情報システムを利用することが日常的になりつつある。しかしながら、各システムでユーザ認証機能が独立して運用されている場合、学生や教職員などのサービス利用者は、個々のシステムを利用するために、多数の ID とパスワードを自己管理する必要が生じている。また、運用部門についても、提供サービス毎にユーザ管理業務が発生するなど、運用上の負担も大きい。このような情報システムの増加に伴う利用者の利便性の向上と、システム運用部門の負担軽減を目的として、福岡大学では全学的な情報システムの認証機能を統合化した統合認証システムを構築し、平成 17 年 4 月より運用を開始した。

本稿では、統合認証システムの導入の経緯や目的、システムの構成、また運用後の経過などから、その効果や問題点などについて報告を行う。以降、2 章

では導入の背景について、3 章で導入の目的、4 章でシステム構成、5 章でサブシステムの連携事例、6 章で運用について述べる。

### 2 統合認証システム導入の背景

統合認証システム導入以前の福岡大学において全学的に利用される情報システムとしては、総合情報処理センター（以下、センター）と図書館が提供する教育研究支援向けの 4 つの情報システムと、2 つの事務系情報システムならびに 2 つの学生生活支援システムの計 8 つの情報システムが運用されていた。しかしながら、それぞれのシステム運用部門が異なるため、利用者の立場からすると表 1 に示すように、利用者は 7~8 種類<sup>1</sup>の ID とパスワードを利用システム毎に認識し、使い分ける必要があった。

また、システム運用部門においても、ユーザ情報の追加・削除などのユーザ管理を部門ごとに行う必

<sup>1</sup> 実際には ID の文字列を共通化していたため、表面上利用者にはアカウント名の種類は少なく見えていたが、登録先が異なるということを厳密に数えた場合

要があったことや、ユーザ情報の入手先や更新の頻度が異なるため、全学的に見ると登録情報に不一致があるなどの問題もあった。そのような状況において、福岡大学では平成16年度より、全学的な情報化推進プロジェクトが推進されることとなり、平成19年度には表1のシステムも含めて約10数種類の情報システムが稼動することが計画されていた。しかし、従来と同様のシステム毎による個別認証による運用では、利用者の利便性や運用部門の負担の問題、さらには全学的にもシステム利用や運用時の統一性を欠くことがあらたな問題となることが予想された。そこで今後の情報システムの増加に対応するため、システム利用時の認証データを統合的に取り扱う統合認証システムの構築を行うことにした。

情報システム名	運用部門	学生	教職員
教育研究システム	センター	(1)	(1)
ダイアルアップPPP	センター	(2)	(2)
学内情報コンセント	センター	(3)	(3)
図書システム	図書館	(4)	(4)
グループウェア	センター	-	(5)
電子メールサービス	センター	-	(6)
事務情報システム	センター	(7)	(7)
自動証明書発行機	教務部	(8)	-

Table 1 統合認証導入前のシステムとアカウント数

### 3 統合認証システムの導入目的

統合認証システムの導入に際し、利用者ならびに運用部門が潜在的に抱える諸問題を解決すべく、次の事項を目的として検討、構築を行った。

#### 学内情報システムのIDとパスワード情報の統一

全学的に提供するシステムの利用者IDとパスワードを一組に共通化することで、利用者の情報システム利用時の利便性の向上を図る。

**ユーザ情報の管理業務の低減化** 従来運用部門毎に行っていたユーザ情報の登録・削除などを統合認証システムの運用部門が一元的に行うことで、全体的な管理業務の負担を減らす。また登録されている情報の鮮度を全学的にも維持する。

**問い合わせなど運用窓口の一本化** 認証システムが統一されることで、利用者対応の内容も一本化でき、利用者に対するサービスの向上と運用部門の負担を軽減する。

**今後の情報システムの追加連携の容易化** 将来的な情報システムの増加を見越した連携インタフェースを準備することで、新システム導入時のコストを減らすと同時に、利用者サービスの質も維持する。

## 4 統合認証システムの構成

本章では、統合認証システム全体のシステム構成とデータ処理を実現するソフトウェアの機能について述べる。

### 4.1 基本構成

#### 4.1.1 システム構成

統合認証システムは図1に示すように、認証対象となるユーザ情報の管理を行うユーザ情報管理サブシステム、認証システムの管理を行う認証システム管理サブシステムならびに実際に各システムからの認証を行うサブシステム用認証サーバ群から構成される。ユーザ情報管理サブシステムは、学生・教職員の基本情報に基づきアカウントの登録や削除処理を行う。認証システム管理サブシステムは、更新された内容をサブシステム用の認証サーバ群に対して反映する処理を行う。

#### 4.1.2 ユーザ情報の登録

統合認証システムに必要な情報の発生から、各種情報システムでの認証利用までの流れを図2に示す。統合認証システムに登録されるユーザの基本情報は、教職員に関しては人事システムを、また学生に関しては教務システムを起源として、氏名、学籍番号(職員番号)、所属、資格などの情報を抽出し、統合認証システムのユーザ基本情報としてユーザ情報管理サブシステムに登録している。また、学外者などの例外的なユーザ情報は直接、ユーザ情報管理サブシステムに登録することで対応している。

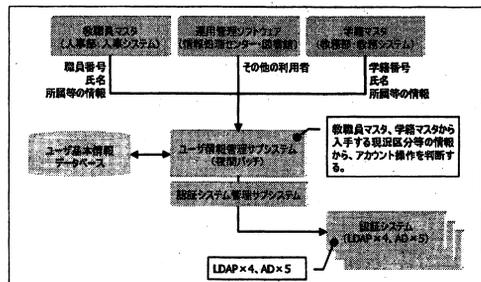


Fig. 2 ユーザデータの連携図

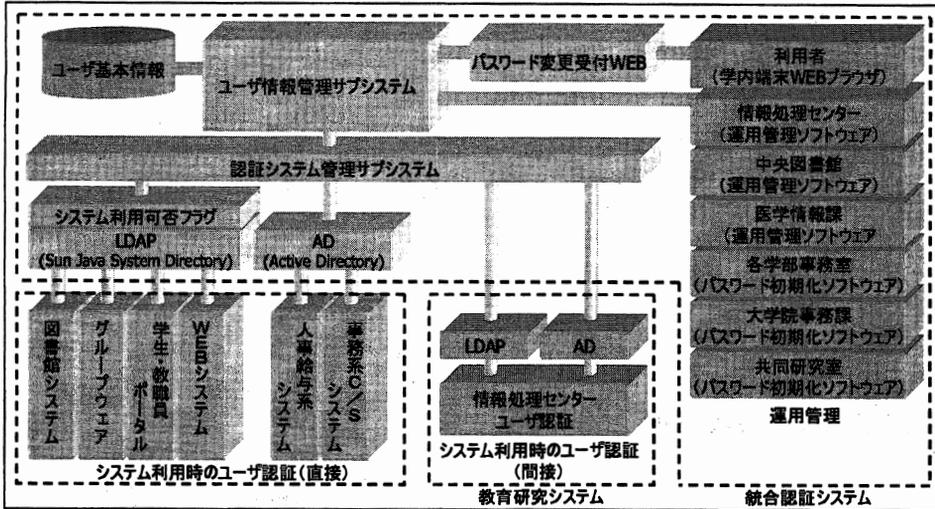


Fig. 1 統合認証システムの構成図

#### 4.1.3 各情報システムとの連携

ユーザー認証を必要とする各種情報システムは、統合認証システムに対してサブシステムとして認証処理連携を行い、システム利用者に認証機能を提供する。統合認証システムと情報システム間の認証連携の方法は、大きく次の2種類の形態で実現している(図1参照)。

- 直接認証 統合認証システムで準備した認証サーバに情報システム側から認証処理を依頼する方法。
- 間接認証 統合認証システムから、情報システム側で準備した認証サーバへユーザー情報を複製し、情報システム側の認証サーバで認証処理を行う方法。

統合認証システムが各情報システムに対して提供している機能は、基本的には認証処理のみであり、各情報システムに固有のサービスレベルに関する権限情報は統合認証システム側では保持していない。よって、利用者権限に応じたサービスを提供する場合は、各情報システム側でそれらの利用者権限情報を設定、保持する必要がある。なお、主たる認証手法としては、ActiveDirectory, LDAP を提供している。

#### 4.2 管理機能

##### 4.2.1 ユーザ基本情報

ユーザー情報管理サブシステムで保持するユーザー基本情報は表2の通りである。統合認証システムでは、

ID とパスワードの一致の成否を確認する手段を提供することを主目的としているため、連携する各サブシステム利用時のサービスレベルに関する権限情報について統合認証システムでは保持していない。しかしながら、各サブシステムの利用許可権の有無(後述のシステム利用可否フラグ)を利用者の所属情報などから自動生成するために、表2のような付随情報を保持している。

項目	学生	教職員
氏名	○	○
アカウント名/パスワード	○	○
職員番号(学籍番号)	○	○
職種	-	○
給与区分	-	○
発令資格	-	○
職務役職	-	○
所属部・所属学部	○	○
所属課・所属学科	○	○
現状区分	○	○
採用年月日・入学年月日	○	○
退職年月日・卒業年月日	○	○

Table 2 統合認証システムが持つユーザー基本情報

##### 4.2.2 システム利用可否フラグ

統合認証システムではユーザーのアカウント名とパスワードの認証処理を行う機能に加え、連携する各

サブシステムの利用許可権を設定するシステム利用可否フラグと呼ぶ機能を持たせている。この利用可否フラグの ON/OFF により利用者毎に利用できるシステムを集中的に管理・設定可能である。また、前述のユーザ基本情報の職種情報や所属情報に基づき、各システムの利用許可条件を設定することにより、自動的に利用許可権を付与する機能を持たせた。これにより人事異動などの利用者情報の変更に応じて、利用可能なシステムを自動的に変更することが可能となり、運用部門におけるオペレーションの軽減を図っている。図3に管理者が操作する利用可否フラグの設定画面を示す。

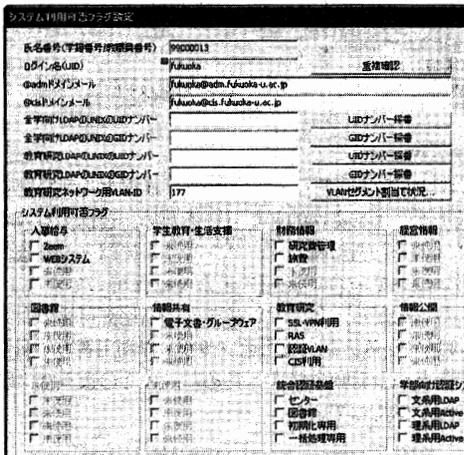


Fig. 3 利用者可否フラグの設定画面

## 5 統合認証システムの運用

平成 18 年 1 月現在、統合認証システムに連携しているシステムならびに今後連携予定のシステムを表3に示す。統合認証システムは表3に示すとおり平成 17 年 4 月より一部の学内情報システムの連携を開始してきたが、統合認証システム用のアカウント名とパスワードによる全面的なサービスの開始時期は、平成 17 年 9 月の教育研究用システムと図書システムのシステム更改時期に合わせて全学的な運用を開始した。

統合認証システムで管理するユーザ情報などは、複数の情報システムで共有して利用されるデータであるため、基本的な事項について共通事項としてフォーマットなどを定めた。また、認証システムの運用についても複数部門で連携して対応することが求められるため運用ルールを定め、全学的なシステム運用が行えるように準備した。本章では運用上、主要と

なる項目について述べる。

### 5.1 運用体制

運用体制を図4に示す。ユーザ基本情報は、教務部、人事部より提供を受け、センターにてユーザー情報管理サブシステムに登録を行っている。また、利用者の問い合わせ窓口としては、センターや各学部の窓口で専用ソフトを備えた端末を設置し、パスワード忘れなどの対応を実施している。

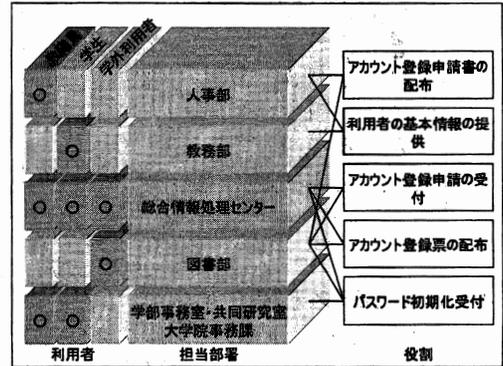


Fig. 4 運用体制図

### 5.2 登録対象者とアカウント情報

今後、学内で全学的に提供される情報システムは、統合認証システムと連携することを前提としているため、登録対象者としては大学の全構成員（学生、教員、職員）を範囲としている。平成 18 年 1 月現在で、約 24,000 人の登録が完了している。

利用者が付与するアカウント名については、既存の情報システムのアカウント情報を考慮し、学生については全学的に配布していた教育研究用システムのアカウント名を、教職員については業務連絡用に運用されていたグループウェアのアカウント名をそれぞれ統合認証におけるアカウント名として継続利用することとした。また、パスワードについては学生について入学時に配布した初期パスワードを、教職員については新たなパスワードを統合認証用のパスワードとして新たに設定した。

### 5.3 パスワードの有効期限と変更方法

統合認証システムの導入により、利用者は複数のシステムを一組の ID とパスワードで利用できるようになり利便性は向上したが、パスワードなどが漏洩した場合に多数のシステムを不正利用されるなどセキュリティ上の危険性が増大した。そのため統合認証システムでは、パスワードに対し有効期限を設

システム名	認証方法	利用可否フラグ	利用対象者	連携開始時期
SSL-VPN	直接 (LDAP)	利用	教職員	連携済み (平成 17 年 4 月)
教育研究システム	間接 (AD,LDAP)	利用	学生・教職員	連携済み (平成 17 年 9 月)
ダイヤルアップ PPP	直接 (LDAP)	利用	学生・教職員	連携済み (平成 17 年 9 月)
学内情報コンセント	直接 (LDAP)	利用	学生・教職員	連携済み (平成 17 年 9 月)
図書システム	直接 (LDAP)	未利用	学生・教職員	連携済み (平成 17 年 9 月)
電子文書ライブラリ	直接 (LDAP)	利用	教職員	連携済み (平成 17 年 10 月)
学生・職員ポータル	直接 (LDAP)	未利用	学生・教職員	連携済み (平成 17 年 12 月)
自動証明書発行機	直接 (LDAP)	未利用	学生	連携予定 (平成 18 年 4 月)
グループウェア	直接 (LDAP)	利用	教職員	連携予定 (平成 18 年 4 月)
旅費申請システム	直接 (LDAP)	利用	教職員	連携予定 (平成 18 年 11 月)
研究者情報システム	直接 (LDAP)	利用	教職員	連携予定 (平成 18 年 11 月)

Table 3 統合認証システムとの連携状況

け、期限が切れた場合は認証が成立しないようシステムの制限を行い、利用者には定期的にパスワードを変更させることを運用上のルールとした。

現在、パスワードの有効期限は、パスワード変更後、1年間として運用を行っている<sup>2</sup>。なお、有効期限が年度冒頭の3月末から4月にかかる場合は有効期限を自動的に5月末まで延長することで、講義開始直前直後の混乱を防止している。また、有効期限切れを防止するために、システムの90日前、60日前、30日前、7日前にそれぞれ電子メールで利用者へ変更を促す警告メッセージを送付する機能を準備している。

また、パスワードの変更は専用のWeb画面からのみ可能としており、各サブシステム側で変更が行えないように制限している。変更したパスワードは夜間バッチにて処理され、翌日より適用される。

#### 5.4 パスワード初期化処置

利用者が自分のパスワードを失念するなどした場合等に対応するため、運用窓口において図5のようなソフトを用いて利用者のパスワードを初期化する対応を行っている。窓口にて本人確認を行った後、専用ソフトにて当該利用者のパスワードを一時的に初期パスワードへと変更する。ただし、初期化されたパスワードは有効期限が当日のみとなっており、継続利用するために利用者は直ちに前述のパスワード変更手続きを実施して新たなパスワードを設定する必要がある。

<sup>2</sup> 平成17年の運用開始時のパスワードの有効期限は、平成18年2月末までとした

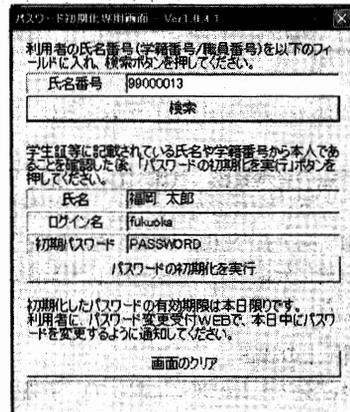


Fig. 5 パスワード初期化画面

## 6 導入の効果と今後の課題

### 6.1 統合認証システムの効果

統合認証システムの運用開始からまだ1年を経過しておらず、多忙となる年度末処理におけるユーザ情報の更新業務を完了していないため定量的な情報に基づくものではなく、定性的また予測的な範囲を超えるものではないが、次のような点が効果として期待できる。

**利用者から見た認証系の一元化** これまでは、システム毎にパスワードや管理部門が異なっていたが、統合認証システム導入後は全学的なサービスについては原則的に一元化されたため、利用者の立場からもシステムを利用する上で必要となるIDとパスワードの関係を把握しやすくなった。

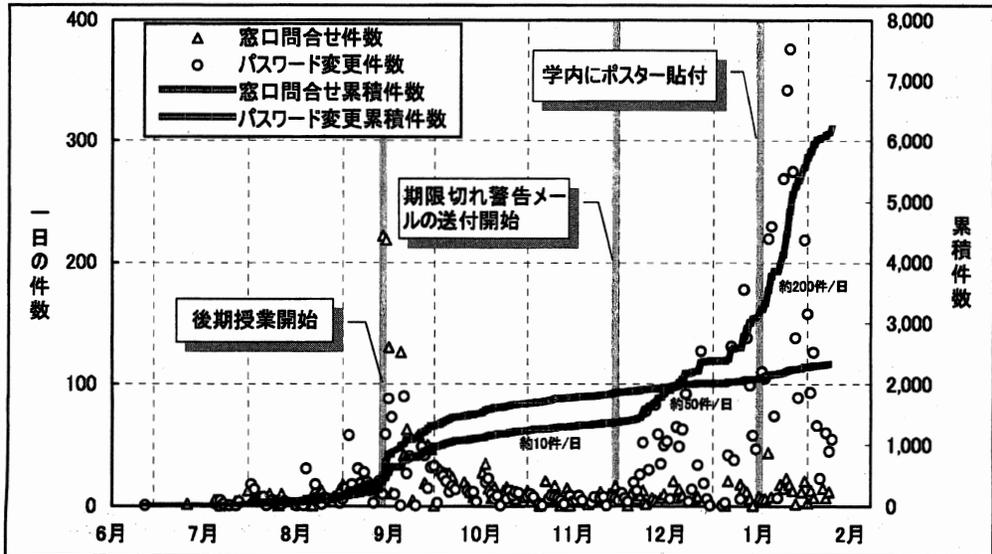


Fig. 6 窓口問い合わせ数ならびにパスワード変更数の推移 (平成17年6月～平成18年1月)

**ユーザ情報の管理業務の削減** 従来運用部門毎に行っていたユーザ基本情報の登録・削除などを統合認証システムの運用部門が一元的に行うことで、全学的に分担していたユーザ管理業務が削減可能となった。

## 6.2 運用上の課題

統合認証システムの運用に際して、予想される問題点としては大きく2点あった。一つは特に学生に多く見られる問題として、自己のパスワードを失念しての窓口への問い合わせ問題である。もう一点は、利用者がパスワードの有効期限を意識して主体的に変更を行うかという点であった。

パスワードを忘れた利用者による問い合わせの状況の推移については図6に見られるように、平成17年9月から増加が開始している。これは9月より運動を開始した教育研究システムを利用する際に、学生のパスワードが入学時の初期パスワードに初期化されていたため、初期パスワードを失念して問い合わせに来た学生が学生によるものである。このため窓口問い合わせの一日あたりの件数は、9月がピークになっている。

一方、パスワードの変更状況については、有効期限の90日前となる11月末よりメールによる警告文を送付したため、図6に見られるように12月より、変更累積者数が増加しつつある。しかしながら、平

成18年2月現在での、パスワード変更者数は学生で23%、教職員で66%程度であり、残る約17,000人はこのままでは2月末にて利用停止の状態となってしまう、4月の講義開始時に多くの学生がパソコンを利用できないなどの事態が発生し、授業に影響が出る恐れもある。このため、現在暫定的に有効期限を延長すること等を検討している。

## 7 おわりに

大学内の様々なシーンにおいてITを活用したサービスが増加する一方で、情報システムを利用する上で必要な認証機構の増加やユーザ情報の管理業務も増えつつある。このような問題に対応するために、福岡大学では学内的な認証処理を一元的に提供するために統合認証システムを構築し、運用を開始した。一元的にユーザ情報を管理できる仕組みと複数のシステムに認証サービスを提供できるサービスにより、利用者の利便性の向上と管理業務の低減を実現した。

今後、運用上の課題を解決しながら実績を積み、全学の情報システムの基盤となるサービスを目指したい。