

増えるシステム、認証管理をどう軽減するのか？

－ 福岡大学における統合認証システム －

福岡大学 総合情報処理センター
奥村 勝
okkun@fukuoka-u.ac.jp

[Abstract]

福岡大学では、平成 17 年度より学生教育生活支援や事務業務システムなど多数のキャンパス情報システムを立ち上げた。これに際し、増加する情報サービスの利便性確保と認証情報の管理業務を軽減するために、学内利用者の ID とパスワードを共通化し、一元管理する統合認証システムを併せて構築し運用を開始した。稼働後 4 年を経過した統合認証システムの導入の経緯、システム構成、運用体制について報告する。また、平成 20 年に追加した IC カードサービス向け学内共通情報基盤についても紹介する。

[Keyword]

統合認証、アカウント統合、認証データ、IC カード

1 はじめに

近年、大学等の教育機関においても情報化は加速しており、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活用することが日常的になりつつある。そのため、基盤となる学内の認証システムの整備や強化が重要となってきた。しかしながら、各システム毎に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利用者 ID(以下、アカウント)とパスワードを自己管理する必要性が生じている。また、運用部門にお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。このような学内における情報システムの増加に対する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を利用する際のアカウントとパスワードを一元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。

平成 20 年 12 月現在、本学の教職員ならびに学生はシステムの違いを意識することなく、1 組の共通のアカウントとパスワードにより 13 種類の全学的な情報システムを利用できる状況となった **1), 2), 3)**。統合認証システムの構築により、利用者へ分かりやすい認証体系となったことに加え、運用部門の負担を軽減する仕組みも導入したことで、情報システムの増加に対しても運用の負担が増えないような構造となった。また、従来にはなかった複数部門間の連携による情報システムの運用も始まり、今後の大学内の情報化の基盤としての機能ならびに運用体制が確立された。

本稿では、著者が統合認証システムの企画、設計、構築に携わったことから、導入の目的、構築までの作業の経緯なども含め、福岡大学の統合認証システムについて紹介する。

2 統合認証システム導入の背景

統合認証システム導入前(平成 16 年)の福岡大学(学生数約 21,000 名、教職員約 3,000 名)において全学的に利用される情報システムとしては表 1 の 8 つのシステムがあった。しかしながら、システム運用部門が異なるため認証システムが個別に運用されており、利用者(学生や教職員)の立場からすると 8 種類のアカウントとパスワードを利用するシステム毎に管理し、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入学・卒業・異動等によるユーザ情報の登録・削除・変更などのユーザ管理を部門ごとに行う必要があった。

こ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実施される

こととなり、平成 19 年度には先の 8 種類のシステムも含めて約 12 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、従来の運用方式では、利用者の利便性や運用部門の負担の問題は解決されず、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新たな問題となることが予想された。そ

表 1 統合認証導入前(H16) のシステムとアカウント数

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)	-

こで、大学組織内における複数の情報システムのアカウントとパスワードを統合し、利用者の利便性を向上させるとともに、運用部門の負担を軽減させる機構である統合認証システムの実現を全学的な情報化を進める上での基本的な情報基盤として位置づけ、積極的に導入を行い平成 17 年 4 月より総合情報処理センター(以下、情報センター)を運用部門として運用を開始することとなった。

統合認証システムの検討から運用までの作業経過を図 1 に示す。以降、3 章で図 1 の①設計フェーズにおける問題の整理について、4 章で統合認証システムの目標について、5 章で②開発フェーズで設計した統合認証システムの構成について、6 章で運用体制について報告する。また、7 章で平成 20 年度に追加実装した学内 IC カードサービス向けの共通情報基盤について紹介する。

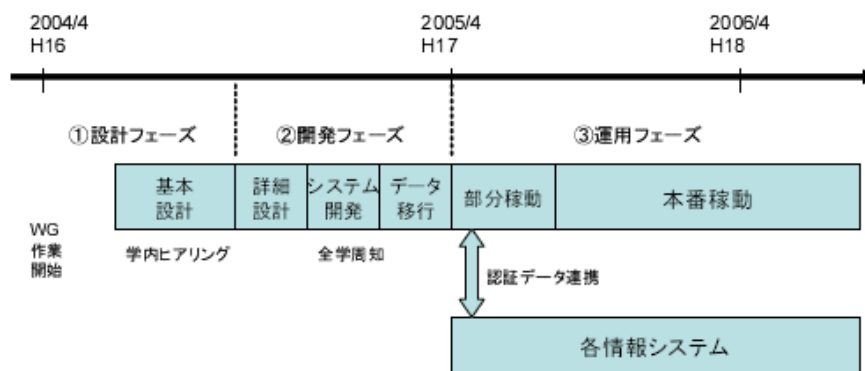


図 1 統合認証稼動までの作業経過

3 設計フェーズにおける問題点の整理

本章では図 1 の①設計フェーズにて整理した従来の個別運用方式の問題点について述べる。明らかになった問題点は、認証システムそのものに起因する問題と、認証データの一元化を実現する上での学内的な検討や実施を行う組織上の問題に大別される。

3.1 個別運用方式が抱える問題点

平成 16 年(2004 年)当時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、表 1 に示すようにそれぞれの運用部門が、8 種類の情報システム毎に個別に認証サーバ(データ)を管理し、運用していた(以降、この運用形態を個別運用方式と呼ぶこととする)。個別運用方式の問題点について利用者、運用部門、全学的観点の 3 者の視点から整理する。なお、この他にも学部や学科などの部門限定で運用されている情報システムも学内には多数存在するが、ここでは対象を全学的規模で利用される情報システムに限定する。

3.1.1 利用者の立場から

複数アカウントとパスワードの管理 利用者(学生、教職員)は表 1 に示される 8 種類のシステムを日常的に使う状況にあったが、各システムの認証データはそれぞれ異なるため、利用者の立場からすると 7~8

種類のアカウントとパスワードを管理する必要があった。

アカウントとシステムの関係が理解しにくい アカウントとパスワードは運用部門からシステム毎に提供されていたため、利用者は表1に示されるようなアカウントと他システムとの関係を把握することが困難であった。そのためシステム利用時の混乱を招く原因ともなっていた。

問合せ窓口が分かりにくい 利用時の認証トラブルについて問合せを行う際、システムと運用部署の関係も把握しにくいいため問題解決までに複数の部署に問合せを行うなど、利用者がサポートを適切に受けにくいという問題があった。

3.1.2 運用部門の立場から

システム毎に増える認証システム 新しい情報システムを導入する度に運用部門はNISやActiveDirectory、RADIUS等の認証サーバを設置してきた。各システムの利用権限の有無は認証サーバへのユーザ登録の有無で区別してきたため、ほぼ情報システムと同数の認証サーバが必要となっており、認証システムのスリム化が課題となっていた。

登録者情報の維持管理 ユーザ情報については、学生情報もしくは教職員情報を運用部門毎に独自に入手して認証サーバへ登録していた。これらユーザ情報は人事情報に連動していない単なる利用者リストであったため、入学や卒業、異動などが発生すると複数の認証サーバ上のデータを手作業で変更するなど、運用上の作業負担が生じていた。

3.1.3 大学全体の立場から

情報化推進の障害 情報化推進プロジェクトでは教職員向けには学内での情報共有のためにグループウェアを、学生向けには各種教育生活支援サービスを提供し、これらを日常的に活用することが大きな目標であった。しかしながら個別運用方式では利用者側の負担が大きく、新たな情報システムの利用そのものが敬遠される恐れがあり、大学としての情報化推進の障害にもなりかねなかった。

適切な利用権限の付与 各システムの利用権限の付与については運用部門毎で管理・設定しているため、大学全体としては特定の利用者についてのシステムの利用権限の有無を一元的に把握することはできない状況であった。また、運用部門毎でのユーザ管理では、ユーザ情報更新の負担からシステムの利用権限が即座に反映されないなどセキュリティ面からの問題も伴う運用となっている一面もあった。

パスワード管理についての教育 教育機関としては、学生などの利用者に対しパスワードについてはセキュリティ確保の点から定期的に変更することを教育すべき立場であるが、表1のように複数システムを利用する際の混乱を防ぐためにパスワードを同じ文字列にし、なるべく変更しないようにという矛盾する指導を行ってきた一面がある。教育上の観点からもパスワードの重要性を認識させ、頻繁に変更させても利用そのものに大きな支障を及ぼさないようなシステム作りが必要であった。

3.2 学内の組織体制の問題

学内の認証データを一元化するという全学的な観点から問題を解決するための部門横断的な検討組織や意思決定機関が不在であることが、もう一つの大きな問題であった。

大学における教育研究ならびに事務業務の情報化を担当する部門としてセンターが存在するものの、その企画と運用に関する権限は学内の一部の情報システムに限られおり、複数部所間で横断的に運用されるシステムの企画立案や方針決定を行う体制が学内的に整備されておらず、このような状況が認証データの分散や個別運用という問題を招き、放置してきたとも言える。

情報化推進プロジェクトのような学内の複数分野における情報システムの構築を部署を超えて連携しながら進めるために、実施体制として図2のような情報化推進委員会と各種専門部会からなる検討と意思決定のための体制を新たに立ち上げた。各システムについての具体的な検討は関係部署がシステム別WGに参画することで部署横断的なメンバーで検討を行うことにした。WGでの検討結果は上部の専門部会、情報化推進委員会での審議を経て決定され、大学の企画運営会議を経由して教員ならびに事務組織に指示がなされるような経路を新たに整えた。

また、このような大規模なシステム構築に学内の組織のみで対応することが困難であったため、全体のコンサルティングとプロジェクト管理を学外のコンサルティング会社に依頼し、大学の会議体に参加する

¹ 実際にはアカウント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厳密に数えた場合

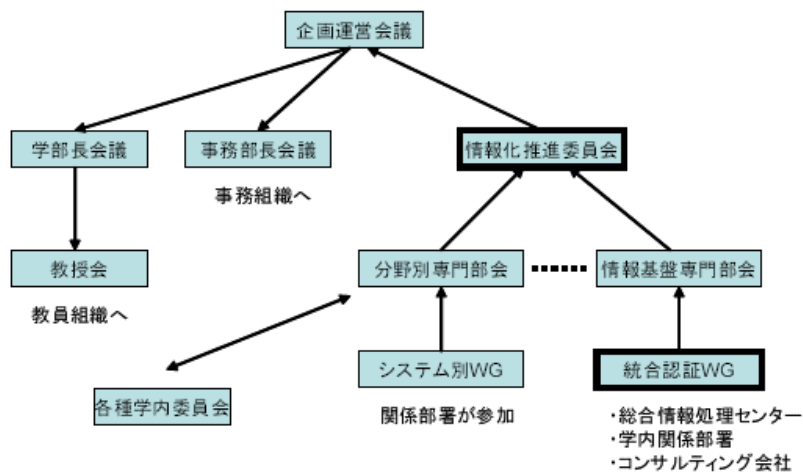


図2 新たに立ち上げた情報化推進体制

形でシステムの検討やシステム構築を行うことにした。本稿で取り上げる統合認証システムについての検討は、図2の情報基盤専門部会に設置された統合認証WGにて行われた。

4 統合認証システムの目標と具体的施策

4.1 統合認証システムの目標

設計フェーズ(図1①)での問題点を整理した上で、利用者ならびに運用部門等が潜在的に抱える諸問題を解決すべく、学内における認証データの一元化を目指し、次の事項を目標として統合認証システムの開発を行うこととした。

全学的見地からの認証系最適化作業 従来の個別運用方式から、全学的に利用するシステムに関しては大学全体としての利用者の認証データを一元管理する統合認証システムを基盤として提供、連携する方向への方針転換を行う。

アカウントとパスワードの共通化 全学的に提供するシステムのアカウント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と情報システムの利用促進を図る。

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。

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現状化を一元的に実現する。

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。

4.2 実現のための具体策

統合認証システムの目標に対し、実現のために実施した具体的施策について述べる。

4.2.1 既存アカウントの統合

アカウントとパスワードを共通化するために、既存の情報システムのアカウントを利用者毎にユニークに定義する必要が生じた。このため利用者に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。

4.2.2 利用者情報の一元登録

統合認証システムに登録するユーザ情報は、大学が管理する学籍情報ならびに人事情報を起源として入手し、統合認証システムに全学的処理として一括登録することにした。また、異動などにより人事データが変更された際も、統合認証システムのユーザ情報に反映されるような仕組みを取り入れることにした。これらの仕組みにより、従来各運用部門が行っていた情報の個別入手、変更などの処理は不要となり、統合認証システムに各種情報システムが連携することで常に最新のユーザ情報に基づく認証連携を行うことが可能となる。

4.2.3 システム利用権限の自動設定

運用部門でのユーザ管理の作業を更に低減させるために、統合認証システムに保持されている人事情報に連動して、各システムの利用権限の付与を自動的に行える仕組みを取り入れた。これは各情報システムの利用権限を、職種や所属部コードといった人事情報に基づくルールとして条件付けすることで、各システムの利用権限(システム利用可否フラグ)の付与を自動で行うものである。

この仕組みにより、起源となる学籍もしくは人事情報が変更され統合認証システムにその変更が連携された段階で自動的に権限付与の再設定が行われる。この結果、運用部門の作業負担を軽減すると同時に、常に人事情報を反映した適切な利用権限が付与されることとなり、人為的ミスや作業漏れによる利用権限の設定ミスが防止可能となった。

4.2.4 詳細な利用権限の分離

連携する情報システムによっては利用者毎に詳細な機能設定を行うことができるシステムもある。統合認証システムでは連携する情報システムに対し認証情報の提供と当該システムの利用権限の有無に関する情報のみを保持し、各システム毎に必要なとなる詳細な利用権限については連携するシステム側で別途保持させることとした。

4.2.5 情報システムとの認証インターフェース

統合認証システムでは連携する情報システムとの認証インターフェースを単純化するために原則 LDAP ならびに ActiveDirectory のいずれかとした。

4.2.6 シングルサインオン

シングルサインオンについては、システムの管理運用が全く異なり、アカウント管理もそれぞれで行う場合に、利便性の向上を目的として導入されるものであることから、今回の機能目標から削除した。

4.2.7 運用時の組織分担

統合認証システムの実現には、大きく運用に関して3つの役割を果たす組織が必要となった。それぞれ統合認証システムに必要なマスターデータを提供する部門、統合認証システム自体を運用する部門、そしてシステムを利用する利用者をサポートする部門である。WG などによる部門間での協議の結果、マスターデータの提供については教務部と人事部が、統合認証システムの運用についてはセンターが、利用者のサポート窓口としては各学部の事務室が分担して行うこととした。

5 統合認証システムの構成

本章では、図1の②開発フェーズにて構築を行った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。

5.1 基本構成

5.1.1 システム構成

統合認証システムは図3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。

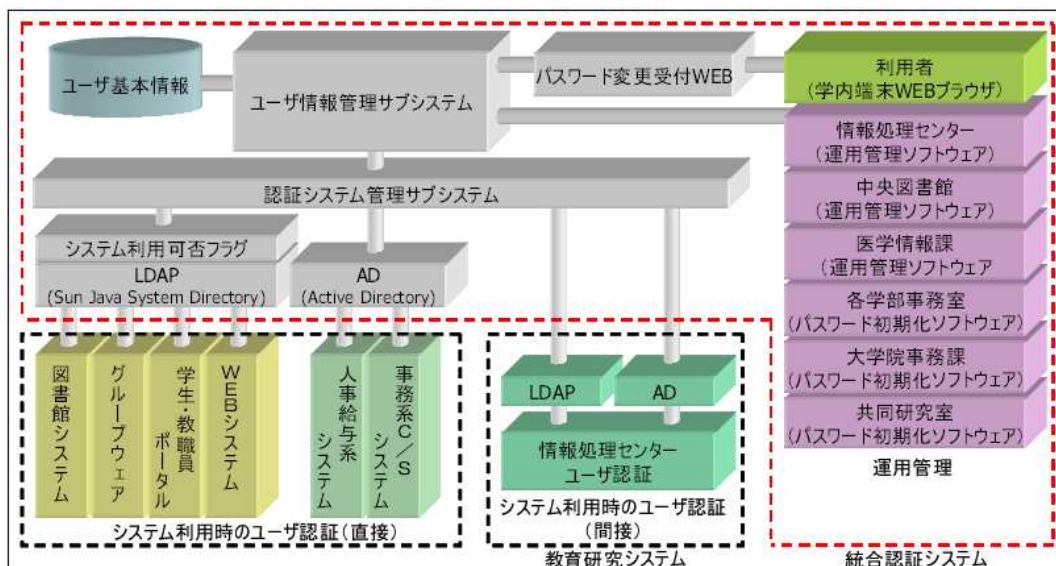


図3 統合認証システムの構成図

5.1.2 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4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。

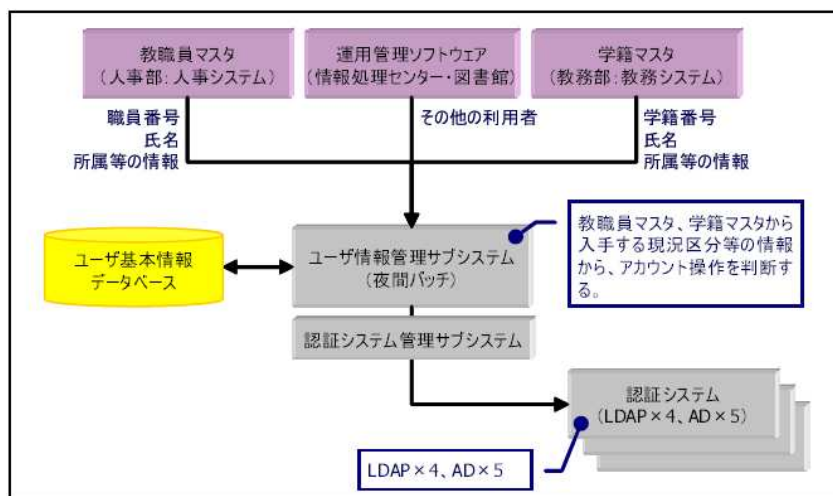


図4 ユーザデータの連携図

5.1.3 各情報システムとの連携

ユーザ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3参照)。

- 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。

なお、主たる認証手法としては、ActiveDirectory、LDAP を提供している。

5.2 管理機能

5.2.1 ユーザ基本情報

ユーザ情報管理サブシステムで保持するユーザ基本情報は表2の通りである。統合認証システムでは、アカウント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。

表2 統合認証システムが持つユーザ基本情報

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	-	○
雇用区分	-	○
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	○	○

5.2.2 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5に管理者が操作する利用可否フラグの設定画面を示す。

図5 利用者可否フラグの設定画面

6 統合認証システムの運用

平成 18 年 7 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。

表 3 統合認証システムとの連携状況

連携システム名	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)
ダイアルアップ 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)
グループウェア	直接 (LDAP)	利用	教職員	連携済み (平成 18 年 4 月)
自動証明書発行機	直接 (LDAP)	未利用	学生	連携済み (平成 18 年 4 月)
旅費申請システム	直接 (LDAP)	利用	教職員	連携済み (平成 18 年 11 月)
研究者情報システム	直接 (LDAP)	利用	教職員	連携済み (平成 18 年 11 月)
ウイルス対策配布システム	直接 (AD)	未利用	教職員	連携済み (平成 18 年 4 月)
E-learning システム	直接 (LDAP)	未利用	教職員・学生	連携済み (平成 19 年 4 月)
学部等の小規模システム (6)	直接 (LDAP)	未利用	教職員	連携済み

6.1 運用体制

運用体制を図 6 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に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。

6.2 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 20 年 12 月現在で、約 24,000 人の登録が完了している。

6.3 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アカウント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け、期限が切れた場合は認証が成立しないようシステム的な制限を行い、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。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、システム的に 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。

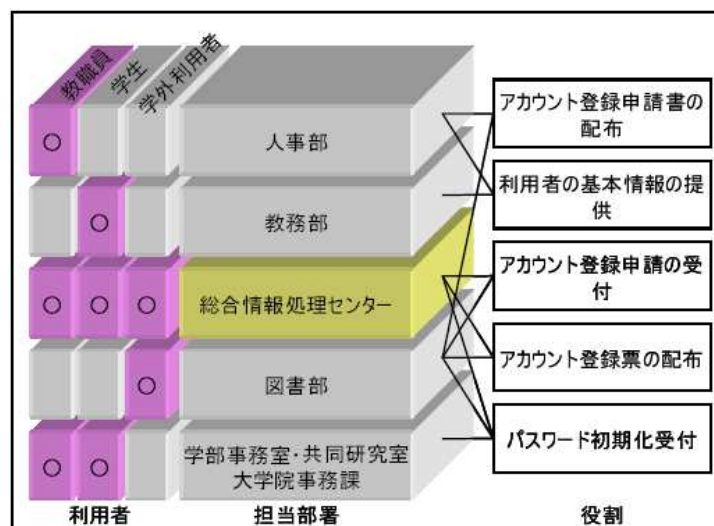


図6 運用体制図

6.4 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。

7 IC カードサービス向け共通情報基盤

7.1 大学における IC カードの利用

Felica に代表される非接触型 IC カードは、Suica おサイフケータイなどで広く普及しており、これらを IC カード学生証(職員証)として採用する教育機関も増えつつある。教育機関における IC カード学生証の利用シーンを整理すると大きく 2 分類されると思われる。1 つ目の利用シーンとしては、IC カードのもつ高いセキュリティ性を活かした個人認証デバイスとしての利活用、2 つ目は Edy 等の電子マネー機能を活用するものである。

福岡大学でも、平成 17 年度に学生証を従来の磁気カードから非接触型 IC カードタイプに切り替え、同時に職員証も同カードに合わせた。平成 19 年度に開始した出席調査等、下記一覧の★印のあるサービスにこの IC カード学生証/職員証(以下、IC カード)を使用している 4)。

- 個人認証デバイスとして
 - 職員証★
 - 学生証★
 - * 出席調査★
 - * 図書貸し出し★
 - * 証明書発行★
 - 入館・入室管理★
 - PC ログイン認証★
- 電子マネー
 - 食堂等での電子決済
 - PC 教室等でのプリンタ課金

7.2 カード発行情報の連携の必要性

次にキャンパスでの IC カードサービスを実現する上での問題点について整理する。前節で提示したようなサービスを展開する際に多くの大学等では、前提としては次のような状況であると想定される。

- A) ICカードの発行・配布対象は、原則大学の全構成員(学生、教職員)である
- B) 各ICカードサービスの運用はサービス部門単位であり、複数のサービス運用部門が存在する
- C) ICカードの発行部門とICカードサービスの運用部門は異なる

一般的なICカードの利用シーンでは、ICカード内に記録されている学籍(職員)番号、氏名などの基本データを参照して、サービス提供するのが一般的であろう。例えばICカード内の学籍番号のみをチェックするというサービスであればあまり問題は生じないが、ICカードを個人認証デバイスとしてより厳密に取り扱う場合には次のような事項を考慮する必要がある。

- D) 利用者のカードが現時点で有効なカードであるか否か(紛失や再発行、有効期限)
- E) 発行対象者の把握(発行対象者の増減)

例えば、あるICカードサービスの運用部門(以下、サービス運用部門)では、認証デバイスとしてICカードを利用する場合、学籍番号等の基本データ以外に上記のD)のチェックを厳密に行う必要性が生じる。利用者がICカードを紛失し、再発行した場合などにこのチェックを行わないと、紛失したカードを拾得した第三者がカードの再発行後もサービスを利用できることになる。また、仮に有効性のチェックを行っていたとしても、そもそもカードが再発行されたという最新の情報が、カード発行部門からサービス運用部門に遅滞なく伝達されている必要がある。また、サービス運用部門がE)について最新の情報を入手できていないと、発行済みの有効なカードに対して「当該カードのユーザは存在しない」と判断するケースもありえる。ICカード発行情報の連携が適切でない場合の運用イメージを図7(ア)に示す。

厳密にカードの有効性をチェックする必要がある場合、サービス運用部門では最新のカード発行情報を常に保持してする必要があるが、全構成員のICカード発行情報を最新の状態に維持することは運用部門の本来業務ではないし、同様の維持業務を複数の運用部門が実施することは非効率である。

このようにA),B),C)のような前提の場合、各運用部門のサービス対象者はA)のように全構成員であるのに対し、C)のようにICカードの発行部門とサービス運用部門が異なるためICカードの最新の発行情報を意識的に発行部門と運用部門間で連携する必要がある。また、サービス運用部門は複数部門に及ぶため、連携部門数の増加に対しても効率的に情報連携が行える仕組みが必要である。ICカード発行部門と運用部門間の理想的な情報連携のイメージを図7(イ)に示す。

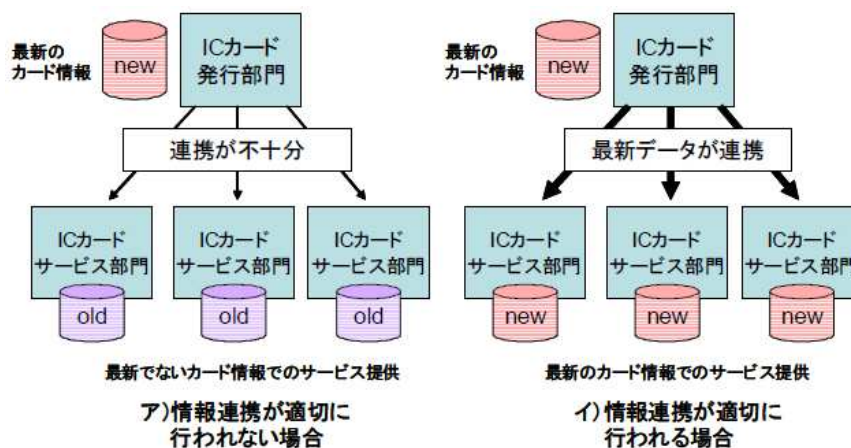


図7 ICカード発行情報の連携の必要性

ここまでの議論をから問題点を整理すると、次のようになる。

- カードの有効性を厳密にチェックする必要がある場合、サービス運用部門はICカード発行情報を常に現行化しておく必要がある。
- サービス運用部門が全構成員の情報を独自に現行化することは非現実的であり、カード発行部門から最新情報を入手できる必要がある
- サービス運用部門が複数部門に及んでも効率的に対応できる仕組みが必要である

- これらの情報連携が自動化して、継続的に行える必要がある。

7.3 IC カード向け共通情報基盤の整備

福岡大学においても先に提示した、IC カード学生証を利用した学内サービスを展開する上で、7.2 節で整理したような IC カード発行情報の問題に直面した。これらの問題を解決するために、IC カード発行部門と運用部門間で IC カードの発行に関する基本データを自動連携する共通基盤を整備することが、IC カードサービス本来の適正な効果を期待できること、また今後の IC カードサービスの展開が容易になると判断し、平成 20 年度に学内 IC カードサービス向け共通情報基盤(以降、IC カード共通情報基盤)を新たに整備することとなった。

IC カード共通情報基盤は、前節の統合認証システムへの機能追加として実装することとした。これは IC カードに関する情報そのものが、原則として大学の構成員(学生、教職員)である「人」に紐付いた情報であり、統合認証システムで管理している ID やパスワードと同様の観点で扱えること、また IC カード情報の発行部門も統合認証における個人情報の発行部門と同一であることに着目した。

ある個人に対する IC カード関連情報は、既存の統合認証システムの個人情報レコードを拡張して保持させることとした。また、各サービス運用部門へのデータ連携は統合認証システムが備える認証データの連携機能を利用し、サービス運用部門に必要な IC カード情報のみをファイル連携方式でデータ連携が行えるような機能を追加実装した。この実装方法により、新規に構築する場合と比べ、必要な機能を低コストに実現できた。統合認証システムとそれに追加した IC カード共通情報基盤のシステムイメージを図 8 に示す。

図 8 中の破線で囲んだ部分および破線矢印で示されるデータ経路が図 4 に対し、新たに IC カード共通情報基盤として追加機能する部分である。まず、IC カード発行部門である人事部および教務部から統合認証システムに取り込むデータ項目に、IC カードに関連する情報(再発行回数、有効期限、チェックデジット)を新たに追加した。これらの情報は学籍番号や氏名等の他の情報とともに統合認証システムのユーザ基本情報 DB に格納される。発行部門から提供される最新データはこのユーザ基本情報 DB に格納された後、ユーザ情報管理サブシステム、認証システム管理サブシステムを経て、IC カードサービスの運用部門のサーバへファイル連携方式で配信される。サービス運用部門は、配信された最新のユーザ情報から必要な項目を自部門の IC カードサービスに必要なデータとして取り込み利活用する。

IC カード共通情報基盤からサービス運用部門へ連携されるデータ項目を表 4 に示す。

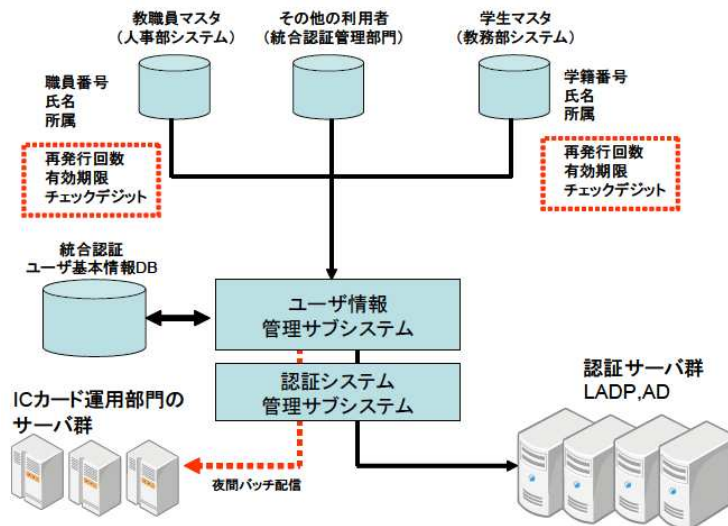


図 8 統合認証システム中の IC カード共通情報基盤 (点線部分)

表4 IC カードサービス部門へ連携されるユーザ基本情報

項目	学生	教職員
学校識別コード	○	○
学籍番号(職員番号)	○	○
氏名	○	○
所属部・所属学部	○	○
所属課・所属学科	○	○
再発行回数	○	○
有効期限	○	○
チェックデジット	○	○

7.4 連携事例

IC カード共通情報基盤に連携する IC カードサービスの一例として、情報センターが管理する PC 教室の入室管理システムの事例を紹介する。

平成 20 年 8 月に更新したセンター関連の入室管理システムは、17 箇所の PC 教室および関連設備のゲートに計 52 台の非接触型 IC カードリーダーを設置し、一元的に入室管理を行うシステムである。更新前のシステムでは、磁気カードを用いる方式であったため、磁気カードを持たない教職員²に対しては、センターが対象者に個別に磁気カードを発行していた。新たに導入した入室管理システムでは、全構成員が所持している IC カードの利用を前提としたため、運用部門によるカードの個別発行が不要になった。

入室管理システムにおけるカードチェックのイメージを図 9 に示す。サーバは IC カード共通情報基盤から最新の IC カード発行情報を入手し、サービス向け情報として保持している。ゲート横に設置された IC カードリーダーに、IC カードをかざすと、カードリーダーはカード内の FCF データ部分から学籍番号、再発行回数、有効期限、チェックデジット等を読み出し、IC カード共通基盤側から入手している最新のカード情報と比較、チェックを行う。このカードの有効性チェックにより、当該カードが有効であると判断できた場合のみ、本来のカード保持者に対するゲートの開錠判定処理などを行う。仮に、紛失したカードを悪用しようとした場合、適切にカード情報が反映されていれば、無効判定がなされることとなる。

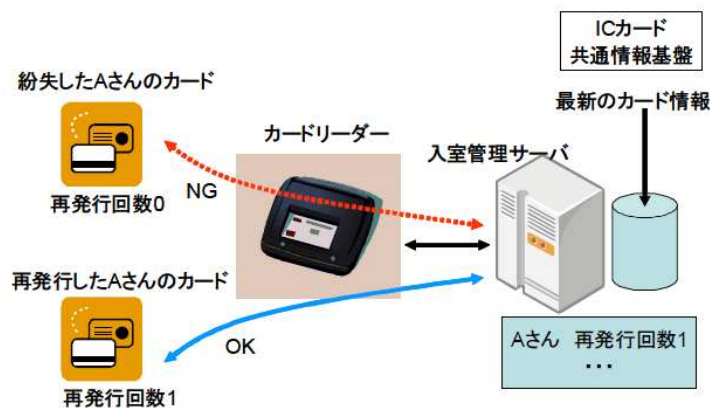


図9 IC カードの有効・無効チェック

8 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、福岡大学では統合認証システムを構築することで学内的な認証データの一元化を行った。認証データの一元化の実現にあたっては、既存の運用形態の問題点を明らかにし、利用者、管理者ならびに全学的な観点から問題の点の解決を図った。また、実現にあたっては技術的な問題のみならず、導入のための検討や運用を支える学内部署間の連携も重要な要因であることも経験的結論として得られた。

² 平成 18 年度の学生証および職員証の IC カード化以前は学生しか磁気カードを所持していなかったための措置

平成 17 年の運用開始から約 4 年が経過し、認証システムの運用としては安定期に入った。今では学生、教職員の多くが以前のような分断された情報システムであったことを忘れ去ったかのようにさまざまな情報サービスを統合認証のアカウントで利用している。利用者に裏側の複雑な認証システム存在を意識させることなくサービスが活用されているという点で、当初の目的は達成できたのではないかと感じている。

その一方で、この 4 年間で社会状況の変化や統合認証システムに求められる内容や機能の変容に対し、システムあるいは学内組織が解決しなければならない課題も多く、次期統合認証システムに向けて解決策を模索して行きたい。

参考文献

- 1) 奥村, 本山, 三河, 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, 情報処理学会研究会報告, 2006-DSM-40, pp.7-12, 2006.
- 2) 奥村, 本山, 三河, 学内における認証データの一元化の実現, 情報処理学会研究会報告, 2006-IS-97, pp.17-24, 2006.
- 3) 奥村, 統合認証システムと教育研究システムの連携, 平成 18 年度情報教育研究集会予稿集, 2006.
- 4) 奥村, 鶴田, 永星, 永田, 一瀬, 広瀬, 今野, 山口, IC カード学生証を活用した全学規模の出席管理システムの実現, 平成 19 年度情報教育研究集会予稿集, 2007.
- 5) 奥村, IC カードサービス向け学内共通情報基盤の構築, 平成 20 年度情報教育研究集会予稿集, 2008.
- 6) FCF(Felica Common-use Format), <http://www.fcf.jp/>