全学的な情報システムのための統合認証システム*

奥　村　　勝**, ***

Integrated Authentication System for Campus-wide Information Systems

Masaru Okumura

Computers and networks become an infrastructure for information and communication. And currently all members of an university have their own user IDs for the information systems in campus. If those information systems require their own authentication mechanisms, user have to manage varisous user IDs and administorators are required to collect and maintain user information for each information systems separately. In this paper, we arranged the associated problems to the traditional authentication mechanism, and describe the nessessity of an integrated authentication for campus-wide information systems. We also report the integrated authentication system in Fukuoka University.

Key Words: Integrated Authentication, ID, Password, Information System, LDAP, ActiveDirectory

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，構成員である利用者（教職員ならびに学生）が，全学的に展開される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．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，利用者の立場からすると８種類のアカウント（ログイン ID）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情報システム毎に行う必要があった．

一方，福岡大学では平成16年度より教務系システムや大学事務系の業務システムの全面更改などを含む，ICT キャンパスの構築を目指した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予定されていた．このような状況において，従来の運用形態を継続した場合，利用者や運用部門の負担といった問題は解決されず，さらには全学的にもシステム利用や運用の統一性を欠くことが新たな問題となることが容易に予想された．

そこで，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した．平成19年４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12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]．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，

* 平成19年５月31日受付
** 電気工学科
*** 総合情報処理センター研究開発室

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，著者が本学における統合認証システムの企画，設計，構築に携わった経緯から，従来の運用方式での問題を整理し，学内における認証情報（アカウントとパスワード）の一元化を行い学内のさまざまな情報システムへ提供する統合認証システムの必要性について述べる．また，福岡大学において新たに構築した統合認証システムのシステム構成や運用面での効果や課題について報告を行う．

表1 統合認証システム導入前のアカウント数

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

2. 統合認証システムの必要性

情報処理技術が一般化したことにより，大学においても従来の教育研究以外の分野，例えば学生の生活支援サービスや教職員の業務ツールとして様々な情報システムを利活用することはもはや日常的である．これらの情報システムでは，利用者を制限したり，特定したりするために，必要に応じて利用者認証が行われている．統合認証システム（統合認証基盤とも呼ばれる）とは，これら情報システムの利用のための認証情報（代表的なもので言えばアカウントとパスワード）や認証の仕組みを組織内で統合し，必要に応じて様々な情報システムに一元的に提供する枠組みのことである[3]．本章では，これらの認証情報や認証の仕組みを統合する必要性について，福岡大学の実情も加味して論じ，既存の運用形態での問題点を整理する．

先にも述べたが平成16年（2004年）当時の福岡大学において全学的に提供される情報システムとしては，表１に示すように複数の部門により提供される８種類の情報システムがあった．次節より，これらの情報システムを利用する利用者，情報システムを提供する運用部門，運用部門の母体となる大学組織，の３者の視点からこれまでの運用形態の問題点を整理する．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小・中規模の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．

2.1 利用者の立場から

2.1.1 複数アカウント管理の危険性

利用者（学生ならびに教職員）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，各システムの認証情報の管理がそれぞれ独立していたため，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自己管理する必要があった．このように多数のアカウントとパスワードの管理を利用者に求めることは，利用者がパスワードに平易なものを設定したり，他人の目に安易に触れる場所にメモする，といったセキュリティ上の問題を誘発し易く危険である．

2.1.2 システム間の関係の不明瞭さ

アカウントとパスワードは運用部門からシステム毎に利用者へ提供されていたため，利用者は表１に示されるようなシステムとシステムの関係を把握することが困難であった．そのため，あるシステム利用する際に誤って異なるシステムのアカウントとパスワードを入力して利用できない等のトラブルを招く一因となっていた．また，そのようなトラブル時に問合せを行うにも，システムと運用部署の関係も把握しにくいため問題解決までに複数の部署に問合せを行うことになるなど，利用者がサポートを適切に受けにくいという問題もあった．本来，利用者へのサービス向上を目的として提供されている情報システムが，その数が増えることにより認証というシステムの入り口でのトラブルを招き，本来の目的を阻害するという事態も生じていた．

2.2 運用部門の立場から

2.2.1 認証システムの増加

運用部門は新しい情報システムを導入する度にNISやActiveDirectory，RADIUS等の認証サーバを設置してきた．認証システムを情報システムに対する利用者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，ほぼ提供する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．

2.2.2 ユーザ情報の維持管理

認証サーバに登録するユーザ情報（学籍番号／職員番号，氏名等）については，運用部門毎に学生情報もしく

＊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を厳密に数えた場合

は教職員情報を入手して認証サーバへ登録していた．これらのユーザ情報は学籍原簿，人事原簿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2.2.1節で述べた認証サーバの数だけ，認証サーバ上のユーザ情報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．

2.2.3　利用者対応の増加

これは2.1.2節の逆の立場から捉えた問題といえるが，運用部門においては利用者からのシステム利用におけるアカウントとパスワードの問題についての問い合わせに頻繁に対応する必要があった．これら利用者への対応も運用部門毎にユーザ情報を管理することに起因する管理コストの増加である．

2.3　大学組織全体の立場から

2.3.1　情報化推進の障害

福岡大学が進めていた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のグループウェアや教務関係の処理等をオンライン化等を，学生向けには各種教育・生活支援サービスのオンライン化等，大規模な情報システムによるサービスの提供を予定していた．また，これらの情報システムを大学の構成員である教職員や学生が日常的に利活用することが情報化の達成目標でもあった．しかしながら，2.1節や2.2節で述べたような認証情報を情報システム毎に管理する運用方式では，利用者や運用部門の負担が大きく，新たな情報システムの利用や導入そのものが敬遠される恐れもあり，大学としての情報化推進の障害にもなりかねない問題でもあった．

2.3.2　アカウントの適切な管理

各システムの利用者に対する利用権限の付与については運用部門毎に管理・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仕組みはなかった．また，運用部門毎でのユーザ管理では，2.2.2節で述べたユーザ情報の維持管理の負担からシステムの利用権限が即座に反映されないことや，退職，卒業した利用者のアカウントが削除されずに放置されるなど，適切なアカウント管理がされておらず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．

2.3.3　情報倫理教育の観点から

教育機関としては，学生を含む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2.1.1節で述べたような危険性を教育すべき立場にあるが，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，一部の現場においては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．情報倫理教育上の観点からもパスワードの重要性を認識させ，パスワードの変更を促すことが現実にできるようなシステムにする必要があった．

2.4　既存の運用方式における問題のまとめ

2.1～2.3節で３者の視点から，平成16年当時の本学において全学的に展開されていた情報システムの認証についての問題点をまとめた．これらの諸問題に共通し，の根幹をなしている点は，それぞれの運用部門が提供するシステムが独自の認証システムを有し，個別に運用を行っていることに大きく起因している．それぞれのシステムの利用対象者は同じ集団（教職員や学生）を対象としているにも係わらず，システム毎にユーザ情報を管理し，アカウントとパスワードを発行していることが，先に述べた諸問題や弊害を招いてきたと言える．

このため対象となる利用者集団が複数の情報システム間で共通であるなら，これらの利用者情報を一元的に管理し，全学で共通に利用できる認証システムを構築することができれば，利用者及び管理者の双方にとって，またその母体組織となる大学組織全体からみても大きな利点となる．

なお，本章で述べたような問題は，福岡大学に固有の問題ではなく，組織内の利用者に対して複数の情報システムを提供している多くの組織において共通する問題でもある[3]，[4]，[5]．「IT の活用領域が拡大するとともにシステム全体の整合性が失われることが少なくない」という予測が具体的な問題となって現実化したといえる．このような“分断されたシステム”をもたらす要因には，複数システム間の認証連携に必要が技術が未成熟であった点も一因ではあるが，運用する組織が「縦割り」であることも大きな原因であることが，同様の問題を抱え，統合認証システムを導入した他大学の事例からも指摘されている．つまり，各部局毎に情報化，ネットワーク化を実施したことによって，結果として組織全体としてのシステム間の整合性が失われ，本章で述べたような諸問題を招いた．また，システム間の不整合を部門横断的に調整，解決する強力な組織体制が欠如していたことも原因の一つであるといえる．

そもそも利用者へのサービスの向上，業務の効率化などを目標としている情報システムが，つぎはぎ的に追加された結果，認証データの例に述べたようなシステム間の整合性を欠いた“分断されたシステム”をもたらすこととなった．これらは単に情報システムを構成するコンピュータの性能や認証方式等の技術的な手段では解決できない，システムを運用する組織（人的要素）に強く根ざした問題であることに，我々は注意を払う必要がある．これらの問題を解決することが，多額の費用を伴う IT 化を，大学に限らず組織内で有効に進める上でのキーポイントであるといえる．

3. 統合認証システムの実現目標と具体的施策

本章では本学の統合認証システムの実現目標と，その目標達成のために採った具体的施策について述べる．

3.1 統合認証システムの目標

第２章で整理した諸問題を解決すべく，福岡大学における統合認証システムの導入では本節で述べる事項を目標として設計，開発を行った．

3.1.1 学内における認証システムの統合

従来の運用方式の根本的な問題を踏まえ，情報システムの運用に必要な認証データや認証の仕組みを各情報システム毎や部門毎で運用しなくて済むようにすることを目標とした．この目標を実現するために大学全体として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新たに情報基盤として整備し，学内の情報システムの運用部門に対し提供することとした．また，統合認証システムの導入以後，全学的に利用される情報システムは統合認証システムと連携して運用することを，大学の情報化における基本方針として定め．以後，追加・更新される情報システムは原則として運用部門を問わず，統合認証システムへ認証連携するサブシステムとすることとした．

3.1.2 アカウントとパスワードの共通化

これまで情報システム毎で異なっていたアカウントとパスワードを統合認証システムの導入を契機に，一利用者に対し一組のアカウントとパスワードに共通化し，利用者の利便性の向上と情報システムの利用促進を図ることを目標とした．

一般的に統合認証システムを実現する方法として，利用者のアカウントとパスワードを利用するシステム間で一組に共通化する方法と，シングルサインオン（SSO: SingleSignOn）と呼ばれる技術により，個々のシステム上でのアカウントとパスワードは異なるが，いずれかのシステムにおいて認証を成立させることで他のシステムの認証をシステム間で自動的に行わせ，アカウントやパスワードの違いを利用者に意識させない方法がある．

今回の認証システムの統合では，学内に散在する情報システムを利用するためのアカウント情報とシステムの関係を利用者に分かりやすいものに再構築し，その結果，各種情報システムの利用を促進することを主たる目標とした．そのため，複数のシステムを一度の認証行為により横断的に利用できる SSO については，統合認証システムの機能目標とはしないこととし，前者の共通化の方法を採用することとした．

3.1.3 問い合わせなどの運用窓口の集約

認証システムが統一されることで，利用者対応の内容や対応部門も集約することを目標とした．これにより，利用者に対し明確な対応窓口を設けることができ，サービスの向上を図ると同時に，従来の情報システムの運用部門の負担の軽減を図ることとした．

3.1.4 ユーザ情報の管理業務の軽減

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い，大学組織全体としてのユーザ情報の管理業務を削減することを目標とした．また，登録されているユーザ情報の現状化（更新）についても一元的に実現することとした．これにより，従来各運用部門が行っていたシステム毎のユーザ情報の管理業務は基本的に不要となる．

3.1.5 情報システムの追加連携の容易化

平成19年度で連携対象となる情報システムは予め把握できていたが，今後も新たな情報システムの追加連携が予測されるため，将来的な情報システムの追加を見越した連携インタフェースを準備することを目標とした．追加連携を容易に行えるインタフェースを準備することで，システム追加連携時の導入コストを減らすと同時に，学内における情報システム全体の認証に関する整合性も維持することとした．

3.2 実現のための具体施策

3.1節で述べた統合認証システムの目標に対し，目標実現のために実施した具体的施策について述べる．

3.2.1 既存アカウントの統合

アカウントとパスワードを一組に共通化するために，既存の複数の情報システムのアカウントを利用者毎に唯一に再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（ログイン ID）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（@cis.fukuoka-u.ac.jp）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（@adm.fukuoka-u.ac.jp）のアカウント名を，それぞれ統合認証における新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設定した．

3.2.2 ユーザ情報の一元登録

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，一元的なユーザ情報とした上で統合認証システムに一括登録することにした．また，異動などにより人事情報が変更された際も，統合認証システムのユーザ情報に自動的に変更が反映されるような仕組みを取り入れることにした．この仕組みにより，従来各運用部門が行っていたユーザ情報の個別入手，変更などの処理は不要となり，

統合認証システムに各運用部門の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．

3.2.3　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軽減させるために，統合認証システムでは人事情報に連動して，各システムの利用権限を利用者毎に自動付与す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できるもので，各システムの利用権限（後述の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，統合認証システムのユーザ情報にその変更が反映された段階で自動的に権限付与の再設定が行われる．従来，異動等により人事情報が変更となった利用者を特定のシステムへ追加したり，削除したりといった手作業で行っていた一連のユーザ情報の変更作業が，人事情報に連動して自動的に行われるようになる．この結果，2.2.2節で述べた運用部門の作業負担を大幅に軽減すると同時に，常に最新の人事情報を反映した適切な利用権限が利用者のアカウントに付与されることとなり，人為的ミスや2.3.2節で述べた作業漏れによる利用権限の設定ミス等が防止可能となる．

3.2.4　詳細な権限設定情報の分離

連携する情報システムによっては，システム内で利用者毎に詳細な権限設定を行うことができるものもある．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，各システム毎に設定可能な詳細な利用権限については連携するサブシステム側で別途保持させることとした．

3.2.5　情報システムとの認証インタフェース

認証連携する情報システムとの認証インタフェースを標準化するために原則 LDAP もしくは Active Directory のいずれかによる認証接続とした．

4.　統合認証システムの構成

本章では本学において構築した統合認証システムのシステム構成と主要な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２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（LDAP，AcitiveDirectory）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，サブシステム内のユーザ基本情報に対し，アカウントの登録や削除処理を行う．また，同サブシステムには利用者からのパスワード変更を受け付ける専用Webや，統合認証システムの運用管理部門や利用者対応窓口が利用する運用管理ソフトウェアが連携する．また，認証システム管理サブシステムは更新されたユーザ基本情報の内容を認証サーバ群（LDAP，ActiveDirectory）に対して反映する処理を行う．

統合認証システムのソフトウェア構成については，ユーザ情報管理サブシステムについては新たに開発したソフトウェアにより構成している．認証システム管理サブシステムについては，市販の認証情報の連携ソフトウェアを活用した．また，システムのハードウェア構成については，認証サービスが停止すると連携する各種情報システムの利用に大きな影響を及ぼすため，サービスの安定稼動に備えた冗長化したサーバ構成としている．

4.1.2　ユーザ情報の登録

統合認証システムに必要なユーザ情報の発生から，各種情報システムでの認証利用までの流れを図１に示す．統合認証システムに登録される利用者の基本情報は，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する．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する．

4.1.3　情報システムとの認証連携

ユーザ認証を必要とする学内の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，次の２種類の形態で実現している（図２参照）．

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直接依頼する方法．

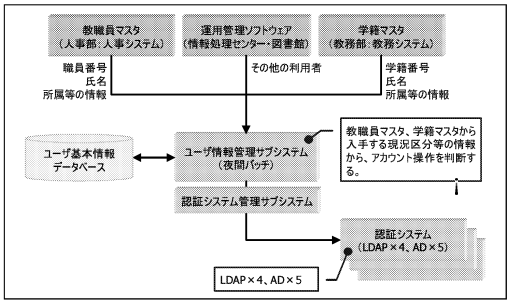

図1 ユーザ情報の連携図

間接認証　情報システム側で準備した認証サーバへ統合認証システムの持つ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.

また，主たる認証手法として，ActiveDirectory, LDAP の２手法を提供している.

4.2　管理機能

4.2.1　ユーザ基本情報

ユーザ情報管理サブシステムで保持するユーザ基本情報の内容は表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，3.2.4節で述べたように連携する各情報システム利用時の詳細権限に関する情報については保持していない．しかしながら，3.2.3節で述べた各情報システムの利用許権限の有無（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	○	○

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 設定により，利用者毎に利用できる情報システムを集中的に管理・設定可能である．また，3.2.3節で述べたように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ユーザ情報の変更に応じて，利用可能な情報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.

5.　統合認証システムの運用

平成19年４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学的なサービスの開始は，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，要となる項目について述べる.

5.1　運用体制

統合認証システムの運用体制を図４に示す．統合認証システムの主たる運用は情報センターが行うこととした．ユーザ基本情報の元となる情報は，教務部，人事部より提供を受け，情報センターにてユーザ情報管理サブシステムに登録を行う．また，利用者の問い合わせ窓口としては，情報センターや各学部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利用者への対応を実施している.

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19年４月現在で，約24,000人の登録が完了している.

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連携している多数のシステムを不正利用される恐れがあるなど，セキュリティ上の危険性は増した面がある．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っている．また，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ている.

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

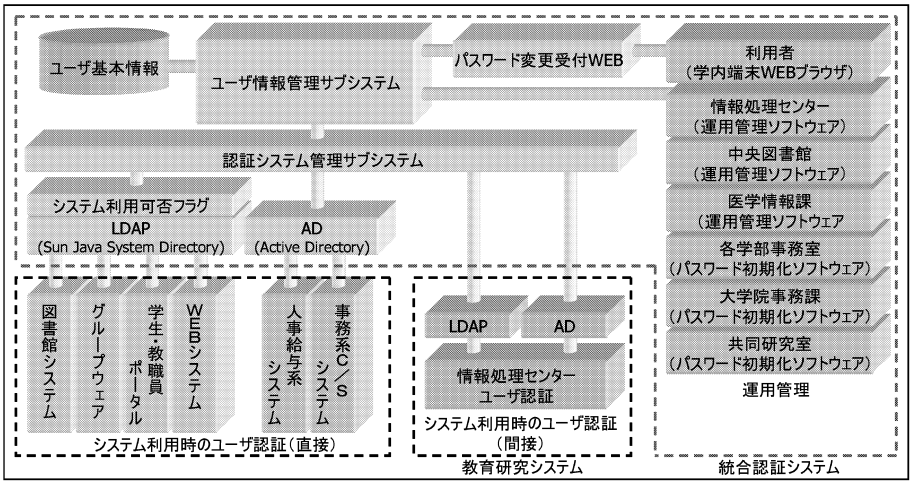

図2 統合認証システムの構成図

図3 利用者可否フラグの設定画面

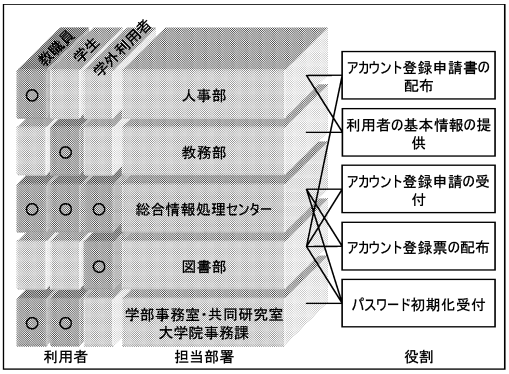

図4 運用体制図

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，年度（前期講義）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，連携する情報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．

6.　効果と今後の課題

6.1　導入の効果

統合認証システムの効果について客観的な評価を行うための調査を現時点では実施していないので数値による効果を示すことは難しいが，定性的に得られた効果について述べる．

表3 統合認証システムとの連携状況

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）
PC 用ウィルス対策システム	直接（AD）	未利用	教職員	連携済み（平成18年４月）
人事・給与システム	直接（LDAP）	利用	教職員	連携予定（平成19年10月）

6.1.1　利用者への効果

統合認証システムの導入後，全学的な情報システムについての認証の仕組みが統合されたため，利用者の立場からするとシステムを利用する上で必要となるアカウントとパスワードの関係を把握しやすくなり，多数のアカウントとパスワードを管理する必要がなくなった．この結果，利用者は多くのシステムをシンプルに利用することができるようになったと思われる．平成19年３月からは Web による履修登録なども開始し，多くの学生がパソコンや情報システムを利用する場面が増えたが，従来のようなシステムとアカウントの関係の不明瞭さがなくなり，大幅な履修手続きの変更にも係わらず，利用に際して大きな混乱が生じなかったことも導入効果の一面であると考えられる．

また，統合認証システムの運用開始と同時に対応窓口も，図４にあるように明確化された．このことも，従来と比べ利用者サービスとして効果を挙げていると思われる．

6.1.2　運用部門への効果

情報システムの運用部門の一例として，情報センターが運用する教育研究システムの認証連携の例を取り上げる．教育研究システムでも，これまでは独自に認証サーバを準備し，ユーザ情報を更新することで認証機能を実現していた．平成17年９月から稼動した新システム（FUTURE３）[6]では図５に示すように，PC（Windows/Linux），汎用 UNIX サーバなどの計算機へのログインや，PPP，SSL-VPN，認証 VLAN 等のネットワークサービス利用時の認証など８種類の提供サービスのすべての認証を統合認証システムに連携する構成へと移行した．連携する認証サーバとしては，学生，教員，事務職員を利用対象者とするサービスを全学向け LDAP サーバで対応し，学生，教員のみを対象とするサービスについては教育研究用 LDAP ならびに同 ActiveDirectory サーバで対応する構成となっている．

各認証サーバへはユーザ情報管理サブシステムから認証システム管理サブシステムを経由して配信されるアカウント情報に基づき，各種サービスに対し認証機能を提供している．統合認証システムとの認証連携により，従来，情報センターが独自に行ってきた各システムに対するユーザ情報の維持管理は，統合認証システム側で一元的に管理されているため，各システムに対するユーザ情報を管理業務は不要となり，管理運用面での負担が大幅に軽減された．また，アカウント情報以外にシステム利用のための補足情報（例えば，UID ナンバー，GID ナンバー，ホームディレクトリパス，LOGIN スクリプトなど）を別途 CSV 形式で連携させる機能も備えており，ユーザ追加・削除などの作業も自動化できる仕組みも準備した．これらの複合効果により，システムに対するユーザの追加・削除の自動化がほぼ達成された．

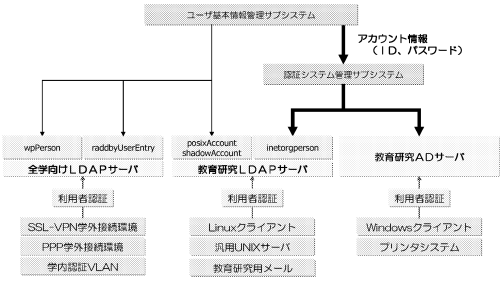

図5 教育研究システムの認証連携例

6.2　運用上の課題

統合認証システムを利用し，学内における情報システムの運用を開始した後，特に問題となった事項は，パスワード未変更者の問題であった．初期パスワードの有効期限切れ90日前となる平成17年11月末より†メールによる警告文を送付する等の情宣活動を利用者に対し行ったが，平成18年２月末でのパスワード未変更者数は約12,000名に及んだ．このままでは多数の学生がパスワードの有効期限切れのため利用停止状態となってしまい，平成18年４月の前期講義開始時にパソコンを利用できないなど授業に影響が出る恐れが生じた．このため，初年度に限り有効期限を２月末から５月末まで延長する措置をとった．この措置により平成18年５月末での最終的な未変更者は約3,400名となった．パスワードの変更措置が毎年必要であること，利用停止時に各種情報システムが利用できなくなるデメリットを利用者が実感を持つように至れば，これらの問題は次第に減少するものと思われる．

統合認証システムの運用は学内の複数部門が連携して情報システムを稼動させるという本学ではこれまであまり例がない事例であった．運用に先立ち，それぞれの部門毎の役割を明確にしたにも関わらず，連携が不十分な結果となった点もあった．これらの原因としては，運用部門の多くがこれまで「縦割り」的な部門単独での業務が中心であったこと，情報の消費者（利用者）としての経験はあっても情報の供給者としての意識や経験が浅く，情報を連携させて機能させるというスタイルに現場や組織が追従できていないこと，に起因したものと思われる．今後の部門間の連携による運用を通じて，役割や意識の改革が進むものと期待したい．

6.3　学内の状況を鑑みた今後の課題

平成16年度から進められてきた福岡大学の情報化推進プロジェクトは，平成18年度においてほぼ予定していた情報システムが稼動を開始し，統合認証システムと連携する状況になった．このことを受けて統合認証システムとしては，当初予定していた全学的に利用される各種情報システムのための認証基盤としての機能を十分に果たすこととなった．また，運用も定着化しつつあることから，その目的は十分に達せられたとみなすことができる．しかしながら，学内における情報化や社会環境の変化は継続的に進行しているため，本学の情報基盤の一つである統合認証システムも，今後状況に応じて機能の追加や運用の見直しなどを継続的に行う必要がある．本節では，福岡大学における統合認証システムにおける将来的な課題などについて述べる．

統合認証システムの全学向け情報システムへの役割については当初の目的を達したと言えるが，学内にはこれまで述べなかった，学部や学科等で一部の利用者を対象として運用されている小・中規模の情報システムも多数存在する．統合認証システムのシステム連携機能では，これらの小・中規模の情報システムへの連携拡大についても当初より予定しており，そのための機能も有している．これまでのところ，統合認証システムの運用部門である情報センターでは，小・中規模情報システム向けの連携インタフェースや運用手順などを取り纏め，学内のシステム管理者等へ認証連携を促す広報等を実施してきた．認証連携のために必要な要件等の条件や制約はあるものの，従来個別に行ってきた利用者の登録管理や独自パスワードの発行作業などが，統合認証システムと連携することで不要となるだけでなく，学生等へのアカウントの周知も他の情報システムと共通となるため容易になるため，これら小・中規模の情報システムの運用者には活用を求めたい．

統合認証システムの当初の目標として，学内に散在する情報システムのアカウントを使いやすく，分かりやすい形で利用者に示すことで，各システムの利用促進を図る狙いがあった．これについてはアカウントとパスワードを一組に共通化することにより利用者が複数の情報システムを利用する上での一つの課題が解決されたと言える．一方で，日常的に使う Web アプリケーションのような形態のものについては，一度認証を行えば連動するシステムについても認証画面をスキップする SSO のような機能を望む声が今後増えるものと予想される．今後も Web アプリケーションは増加することが予想されるため，部分的な SSO 連携については検討が必要な課題の一つと言える．

また，統合認証システムと関連する事項として，学内における学生証ならびに職員証が平成18年４月より IC カード化されたことがある．学生証ならびに職員証には近年普及しつつある非接触型の IC が搭載された IC カードとなっており，従来の磁気カードと異なり，カード内に数 KByte のデータを記憶することが可能である．また，必要に応じてリーダー・ライターを介してカード内のデータの読み書きを行うことも可能となっている．これらを活用した学内サービスとしては平成19年４月より，講義室に取り付けられた IC カードリーダーを活用した出席管理システムが全学的に稼動開始している．この読み書き可能な IC カードのデータ領域から，カードリーダー等を活用して学籍番号や職員番号などをチェックすることで建物の入館・入退室管理やパソコン利用時のユーザ認証の機器として活用することも可能である．しかし

† 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．

ながら，IC カードを認証機器として利用する場合，カードに関する基本情報（所有者や再発行回数，有効期限）などをチェックする仕組みを必要とするが，個々の IC カードの利用部門においてこれら IC カードに関する情報を管理することは大変負担が大きく，情報システムのアカウントとパスワードを部門単位で管理運用していた2.2節の状況と同様の諸問題をもたらすこととなる．このため，大学内において IC カード化された学生証・職員証を情報システムの認証機器として活用するためには，やはりカード内の情報を一元的に管理する共通基盤の整備が必要となる．統合認証システムには既に，表２のような項目情報を保持する仕組みが備わっており，このユーザ基本情報の延長として IC カードに関する必要な情報を保持することで，既存の統合認証システムの仕組みを活用して，IC カード向けの共通基盤の役割を持たせることも比較的容易であると推測される．全学的な認証基盤としての観点からも，今後，IC カード化された学生証・職員証に関する IC カード情報まで含めて大学組織内において統合管理することが望ましい．

6.4　統合認証に関連する学外の状況

福岡大学外に目を向けると現在，独立行政法人化した国立大学を中心として，今後盛んになると予測される大学間での学生や教職員の交流（単位互換や施設利用）などに対応するために，１大学内での認証基盤の整備に留まらず，大学間での情報システムの利用を想定した認証基盤であるUPKI（University PKI）の研究ならびに実用化が進められている[7]．

本学で実現した統合認証システムは，個人認証の仕組みとしてアカウント名（ログイン ID）とパスワードという文字列の組み合わせを，利用者が記憶に頼って保持し安全性を確保するという，認証の方式としては極めて古典的で単純な方式に基づくものである．仕組みが単純であるため特段の装置などを必要としない反面，通常解読防止のために定期的にパスワードを変更するなどの対処が必要となる．また，多数のシステムを利用する場合や複雑なパスワードであっても，人の記憶に頼って管理せざるを得ないという問題がある．これらの問題に対処する方法として，公開鍵認証（PKI: Public Key Infrastrucutre）を用いる方法がある．公開鍵認証を用いた認証を行うことで，パスワード（文字列）による認証において問題となるパスワード解読に対する脅威に対する耐性を高めることができる．また，IC カードなどの認証デバイスに PKI の鍵を保持させることで，利用者は各システムの利用場面においてパスワードを記憶することや入力するといった作業からも解放される．UPKI では，これらの PKI 技術を大学内の情報システムの認証方式として採用することに加えて，全国のUPKI 採用大学間において認証データの相互利用を図り，異なる大学の学生や教職員が他の大学のシステムやサービスを利用することを容易にすることを目指している．

私立大学である本学にとって，現時点では直接的な関係はないものの，近い将来，国立大学を中心とする大学等では，全国の大学間にまたがる各種情報システムの利用のための情報基盤が整備，実用化されるという動向があることに関しては，今後も注意を払う必要がある．また，これらの取り組みに関連して，2.4節で述べたような情報システムの活用領域の拡大のネックとなっていた学内組織の連携や調整を行い，大学組織内の情報化を総合的に整備する組織作りが国立大学に留まらず他大学でも積極的に進められている点にも留意する必要があると思われる．

7.　おわりに

本稿では，組織内における複数数の情報システムの認証情報が個別に管理されることにより生じる“分断されたシステム”の持つ諸問題について整理し，認証情報や認証処理を統合する統合認証システムの必要性について述べた．また，その解決の実例として平成17年度（2005年）より運用を開始した福岡大学の統合認証システムの具体例を述べ，諸問題を解決する仕組みや運用体制などを報告した．

従来の運用方式の抱えていた課題を整理し，改善策を盛り込む形で統合認証システムを構築することで従来の課題を解決し，福岡大学内における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という認証情報を，利用者にとって分かりやすい仕組みへ，また運用部門にとっては管理業務の負担の少ない仕組みへと移行することができた．学内における情報システムの利活用を促進するための情報基盤として統合認証システムの整備を行ったことは，情報化推進プロジェクトにより新たに構築された多数の情報システムが円滑に機能していることからも有意義な取り組みであったといえる．

謝　辞

統合認証システムの構築ならびに運用開始にあたり，プロジェクト携われた統合認証基盤ワーキンググループのメンバー，総合情報処理センターのスタッフならびに(株)日本総研ソリューションズの本山聡氏，三河邦夫氏の協力を得たことを，ここに記して謝意を表します．

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］江藤，渡辺，只木，渡辺，全学的な共通情報アクセス環境のための統合認証システム情報処理学会研究会報告，2002-DSM-27，pp.31-36，2002.
［4］金西，松浦，大家三好，佐野，大恵，矢野，徳島大学における大学ポータルの構築とその運用について情報処理学会研究会報告，2005-DSM-39，pp.1-6，2005.
［5］尾川，敷田，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情報処理学会研究会報告，2005-DSM-39，pp.31-36，2005.
［6］西原，藤村，奥村，新教育研究システム*FUTURE3*の概要，情報処理教育研究集会予稿集，pp.123-126，2005.
［7］*UPKI*イニシアテイブ，
https://upki-portal.nii.ac.jp/