山口大学における統一認証の導入事例について

The Introduction of Unified Authentication in Yamaguchi University

久長　穣†，刈谷　丈治†，三池　秀敏‡

Yutaka HISANAGA †, Joji KARIYA †, Hidetoshi Miike ‡

hisa@yamaguchi-u.ac.jp, joji@yamaguchi-u.ac.jp, miike@yamaguchi-u.ac.jp

†山口大学大学情報機構メディア基盤センター

‡山口大学理工学研究科

† Media and Information Technology Center, Yamaguchi University

‡ Graduate school of Science and Engineering, Yamaguchi University

概要

大学において複数の情報システムが導入され，サービスが展開され，それぞれが独立に認証機能を提供するため，サービス毎に多くの ID とパスワードを記憶しなければならない問題点などから，全てのシステムで同様に用いられる統一認証が必要となってきている．山口大学では統一認証を全学で定常的に利用してもらうため，利用者にとって利用しやすいもの，提供側（管理者）にとって提供しやすいものであることを考え，利用者・提供者の立場にたって統一認証を提供し，自然に構築されるように配慮し，独自の取り組みを行い，統一認証を導入してきた．本学メディア基盤センター(以下，本センター)の主要サービスに利用者を誘導することで，ネットワーク接続におけるユーザ認証の統一，メールサービスにおけるユーザ認証及びメールアドレスの統一，Web サービスにおけるユーザ認証の統一を総合して，統一認証を実現した．

本センターの認証サービスのための個人情報は，当初図書館との連携だけだったが，学生部の学生情報，人事課の教職員情報をそれぞれ連携させることで，大学関係者の概ね全ての情報を保有することができ，現在では本センターの認証が大学の標準の認証として位置づけられている．本稿では，山口大学における統一認証導入の経緯等について述べるとともに、大学における認証導入のあり方、情報サービスのあり方について議論する．

キーワード

統一認証, ID，パスワード,電子メール,Web ページ

1. はじめに

国立大学が法人化される以前は，学部等で独自のサーバやWebサービスが存在し，サーバ毎に独立した認証が提供されていた．当初は，サービスが学部内にとどまり，また，サービスの量も少なかったため，利用者が複数のID(Identification，ユーザ名)とパスワードを使用する状況は少なかった．しかし，全学的なサービスが増えるにつれ，利用者は複数の ID とパスワードを記憶する必要が出てきた．このため，IDとパスワードを手帳にメモする，ディスプレーなどに貼り付けるなどパスワード管理が不十分な状況が発生してきた．一方，サービスを提供する側は，ID とパスワードの管理･運用が大変なため登録後のメンテナンスを行わない利用者やパスワードを忘れる利用者に対応するために，当初発行 ID とパスワードとを同一のものにする場合がある．折角 ID とパスワードで守られたシステムを構築しても，認証機能を導入していないのと変わらない状況となっている．この状況の解決には，大学内の特定部局が発行・管理し，全学で利用できる統一認証が必要である．そういった中，各大学においても統一認証の導入が進められてきている[1-4].

法人化した国立大学においては，トップダウンで統一認証を導入することも可能となってきているが，セキュリティ確保を目指すあまり，複雑な手続きやパスワードにすると利用されなくなり，逆に各部局で独自の認証が立ち上がってしまう．統一認証が全学で定常的に利用されるには，利用者にとって利用しやすいものであり，かつ提供側(管理者)にとって提供しやすいものである必要がある．利用時期に応じて，情報のセキュリティーレベル，利用者や提供者のセキュリティに関する認識，認証の技術レベル，及びクライアントやサーバソフトの対応状況などを総合して認証を導入する必要がある．本センターにおいてはこの点に着目し，それぞれの時期で利用者・提供者の立場にたった統一認証を提供し，自然に統一認証が構築されるように配慮した．

当初，先行している学部，学科や研究室において，独自のメールサーバが稼動していた．そういった状況下では利用者がサービス内容や ID とパスワード組み合わせが分からず，どこに問い合わせてよいかさえ不明になってきていた．利用者意識としては ID とパスワードについては，サーバの運用主体を考慮せず，とにかく本センターに問い合わせればよいと考えられていた．ただ、本センターでは，返答できないものやサーバの存在さえ知らないものも少なくなかった．

本学において，サービスにログインできない場合や，IDやパスワードを忘れた場合などには，まず本センターに問い合せが来ることが多かった．本センターではこの点に着目し ID とパスワードがネットワーク接続，電子メール(以下メールと略す)，Web ページなどの基本サービスの認証に用いられることを考慮し，図1に示すように、以下のような3つのフェーズに従い，本センターの主要サービスに利用者を誘導することで，統一認証の導入に先進的に取り組んできた．

第1フェーズ　ネットワーク接続におけるユーザ認証の統一
第2フェーズ　メールサービスにおけるユーザ認証及びメールアドレスの統一
第3フェーズ　Webサービスにおけるユーザ認証の統一

この間，本センターは，総合情報処理センター(平成7年4月改組：省令施設)から，平成14年4月より改組し，メディア基盤センター(省令施設)となっているが，本稿では両センターとも本センターと記述する．また，平成16年4月からは，本学附属図書館及び埋蔵文化財資料館とともに学術情報機構を構成し，機構長(副学長)の元に柔軟な組織運営を行っている．さらに，平成18年4月からは，総務部情報化推進室を併合し，大学情報機構として，全学の学術情報だけでなく，事務等を含む大学全体の情報環境の構築・支援を行うことを期待されている．

本稿では，山口大学における統一認証導入の経緯等について述べるとともに，大学等における統一認証導入のあり方・情報サービスのあり方について議論する．

2. ネットワーク接続におけるユーザ認証

2.1. 学部新入生に対するメディア基盤センターのアカウント発行

1997年度から全入学者を対象に本センターのIDとパスワードの発行を開始した．それまでは，希望者や演習利用者だけに発行していた．入学者確定後，学務部から入学者リストを取得し，それに対して機械的に ID と初期パスワードを割り当て，当初は A4 用紙サイズの登録証に ID と初期パスワード及びパスワードの運用・変更方法を記載して，各学部で行われる新入生オリエンテーションなどで配布・説明した．

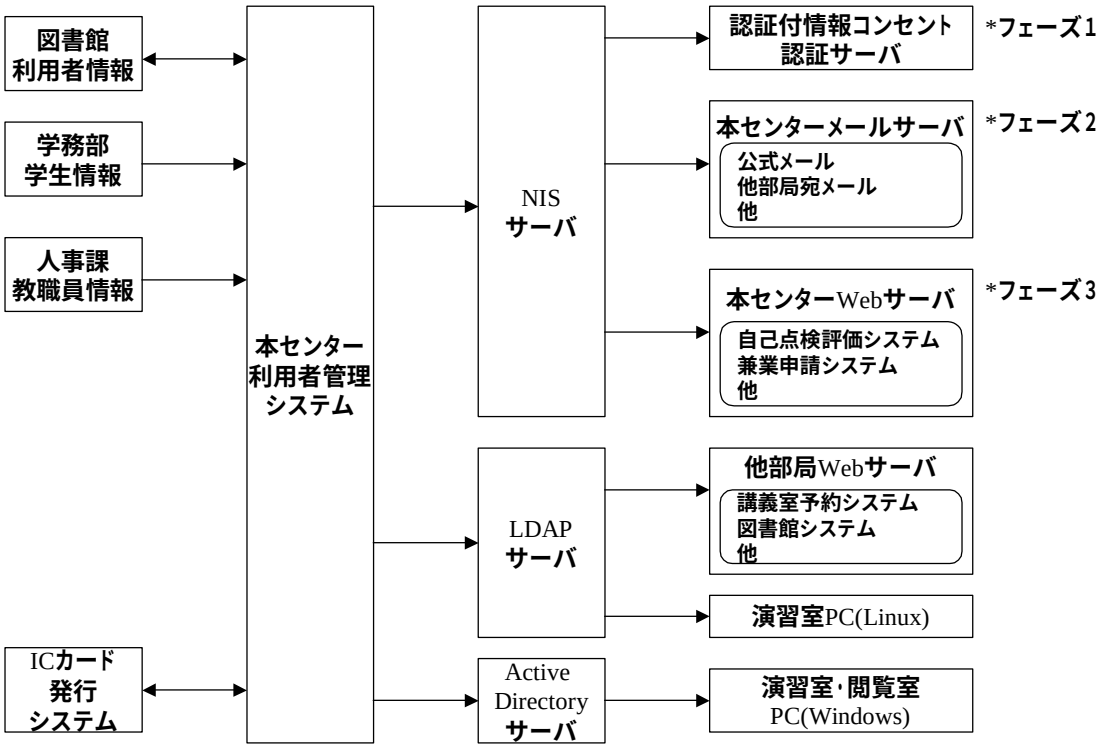

図1　山口大学における統一認証の概要

学生がパスワードを忘れた場合は，本センターにおいてパスワードを初期化（初期パスワードに変更）した．当初は，入学時に配布した登録証を紛失した学生が多かったため，学生証により本人確認を行った後にではあるが, 初期パスワードも教える必要もあった. そこで, 2000 年度からは，登録証を A4 用紙サイズではなく，携帯し易い学生証と同一サイズ（カードサイズ）で配布・説明することにした. 年次進行の結果, 学部学生においては, 2000 年には全学部学生が本センターの ID とパスワードを取得している状況になった.

2.2. 認証付情報コンセント

1998 年に図書館等に, 先駆けて認証付情報コンセントを整備した[5]．ノート PC が普及をはじめつつあり，DHCP(Dynamic Host configuration Protocol)[6]による PC のネットワーク設定の自動設定が可能になったことで，図書館等にノート PC をネットワークに接続できる環境を整備する要求が出てくるようになった．しかし，当時 DHCP にはユーザ認証機能が存在せず，接続すれば誰でも利用できるという問題があった．大学内でのサービスであることから，単に誰でも匿名で使える情報コンセントでは，サービス責任・教育責任が果たせないとともに利用者責任が明確とならない．接続にあたっては，利用者の認証と Web ページやメールへのアクセスログの保存が必要であると考えた.

そこで, ノート PC 接続後, Web ブラウザを起動し，認証ページにて ID とパスワードを入力してもらうことでユーザ認証を行い，ネットワークが利用できるユーザ認証システムを独自に構築した．その認証に本センターの ID とパスワードを用いた．図書館等限定された場所に整備されること，サービスの提供主体が本センターであること，また，対象が主に学生であったこと，学生は全員登録となっていることから，このシステムの導入を試行した．全学ネットワークの構築当初より本センターが全学ネットワークを管理し，サービスを提供してきたこと，認証付情報コンセントの整備がはじめてであったこと，などからシステムの導入が比較的容易に進められた.

認証方法は次のとおりである.

① ノート PC を認証付情報コンセントに接続すると DHCP による IP アドレス等が自動設定される.
② Web ブラウザを起動すると，認証サーバに接続され，認証ページが表示され，そこに本センターの ID とパスワードを入力する
③ 認証サーバは，メールサーバに接続し ID とパスワードの確認を行い，正しければ，ネットワーク利用を許可するフィルター設定を追加する.

教職員からは認証付情報コンセントが使えないなどの問合せがあったが，メディア基盤センターの ID とパスワードを取得してもらうことで対応した．この時点で，ネットワーク接続におけるユーザ認証は本センターの ID とパスワードに統一できたと考える（1998 年）.

現在では，認証付情報コンセントは，図書館，遠隔講

義室，各地区講義室，TV 会議室等に整備し，講義，会議等で活用できるようになっている．また，研究室学生へのネットワーク提供の一つとして，指導教員が研究室に認証付情報コンセントを導入するケースも増えてきた．特に，文系の指導教員に希望が多いのが特徴である．各研究室内に認証付情報コンセントを導入することは，利用者認証やログ管理はもちろん，ウイルス対応，ネットワークの不正利用，掲示板を利用した誹謗中傷等への対策の管理を，指導教員が教育的立場で行うのであるが，技術的な点に関しては本センターに依頼することができ，指導教官のネットワーク管理への負担が軽減される効果がある．

3. メールサービスにおけるユーザ認証

3.1. メールサーバの集約

本センターの主要サーバであり，学内構成員の多くが利用する可能性の最も高いものは，メールサーバである．1995 年以降，文部省からの連絡も，ファックスからメールに変わり，教員だけなく，事務系職員もメールの活用機会が増加し，メールの利用は当たり前となってきた．

メールサービスを利用したい教職員に対して，本センターのメールサービスを利用してもらえるようにすることで，学内構成員が本センターのメールアドレス及びその ID とパスワードを統一して持つことになると考えた．本センターのサーバを利用してもらえるように，学部学科などで運用されるメールサーバよりも，本センターのサーバの方が，安定であり，メールやフォルダのサイズ等の利用制限もなく，IMAP(Internet Message Access Protocol)[6]サービスの提供など，利用者にとって利便性，安定性が良く，管理者にとって管理コストがなくなるように努めた．このメールサービスの提供を安定運用するため，SMTP(Simple Mail Transfer Protocol)[6], POP3 (Post Office Protocol Version 3)[6], 及び IMAP のサービスのみを提供する専用サーバを構築した．

IMAP の特徴として，各利用者の受信箱やフォルダが全てサーバ側に保存される．利用者は，異なる場所から，異なる端末を使っても，同じ状態で，メールにアクセスできるといった点で POP3 に較べて優れている．学生や教員などは，学校で使用する PC と自宅や出張先で使用する PC が異なる場合が多い．また，異動の多い事務職員にとっても，メールがそのまま引き継げ，設定変更が容易であることから，利用者が増加している．Web メールサービスとの連携も行い易い．

3.2. 公式メールアドレスの運用開始

事務連絡や業務連絡等がメールで行われるようになり，学内構成員のメールアドレスを各部署で把握する必要が出てきた．当初は，事務系職員が学部や学科の教職員のメールアドレスを調査し，メールアドレスのリストを作成していたが，学部や学科サーバ，理系学部等においては，研究室サーバなどあり，メールアドレスの調査は困難であった．また，最新情報に保つことも困難であった．特定の学部や学科内で教職員のメールアドレスのリストは作成できたとしても，他学部や全学を対象としたメールアドレスのリストの作成にいたっては，ほとんど不可能であった．

そのため，2001 年 12 月 18 日付けで，当時の広中平祐学長の判断で，

1) 本センターのメールサーバに登録があるメールアドレスを公式メールアドレスとすること，
2) 全教職員がメールアドレスを取得すること，
3) メールアドレスの一覧を本学ホームページの学内限定版に掲載すること，

を文書にて通知頂いた．この背景としては，

1) 医療系や文系の多くの教職員，及びおおむね全学生が，本センターのメールサーバを利用していた，
2) ウイルスメール対策が実施されていた，
3) 全学へのメールサービスを提供しているのは本センターのみであった

こと等による．これにより，形式的には，大学の教職員及び学生全員が本センターの ID とパスワードを取得することとなった．登録方法は申請制をとったので登録しない教職員も若干いるため，登録のない教職員にはメールによる連絡が取れない等の問題があり，その後の課題となった．

また，通知文書の中に「E メールアドレスを本学ホームページの学内限定版に掲載する．」としたことで，学内の全教職員のメールアドレスの一覧表が作成できた．すなわち，学内の教職員の全リスト(個人情報)について人事課から本センターへの流れができた．しかし，人事課にとってのメリットが少なかったため，データの更新が迅速に行えなかったなどの問題点が課題となった．以後，この課題は，人事課を主体としたサービスとの連携を計ることで解決していった．この時点で，本センターのメールサービスにかかる経費は，大学が負担することとなり，利用者への負担としていた課金制度は廃止された．

3.3. センター外メールサーバ宛メールの転送

メールサービスの利用者が増加する一方，学部や学科で運用されているサーバは，メールサーバを立ち上げた教員が転勤，あるいは経年によるサーバに障害が生じる

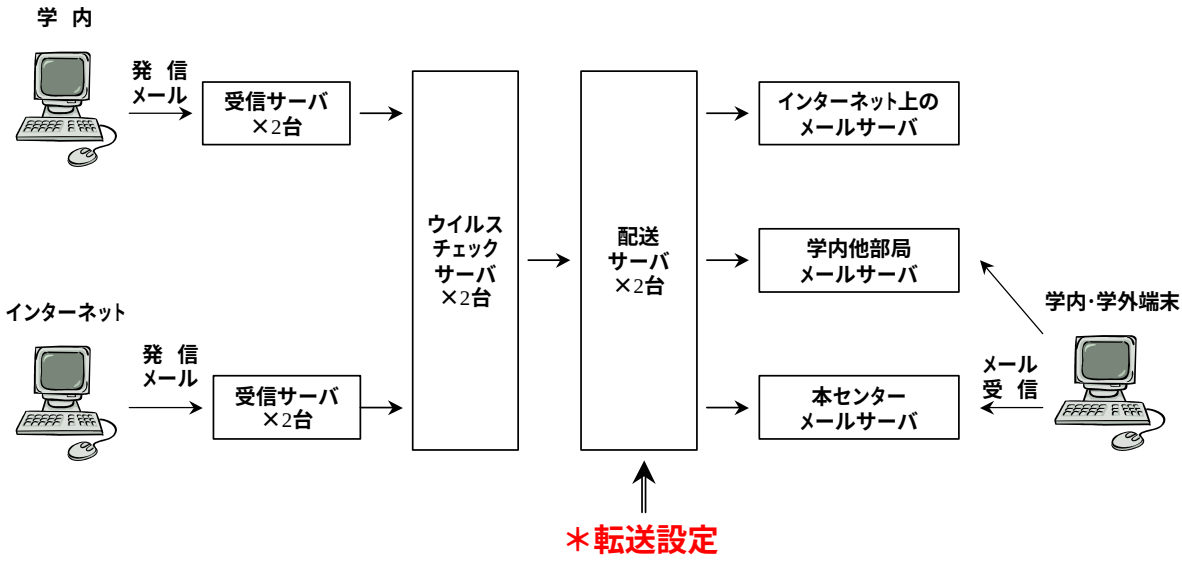

図2　メールの配信経路と転送設定

などで，安定運用が困難な状況になっていた．こうしたメールサーバが不調になると，まず本センターに問合せがくるが，本センターでは対応できないという事例が増えてきた．そこで，本センターに問合せがあった際，「本センターのメールサーバを利用していただければ，すぐ対応できるので，可能でしたら，本センターのメールサーバのご利用を検討ください．」と回答することとした．また，本センターのメールサーバへ移行する際の大きな障害の一つであるメールアドレスが変わる点については，メールの転送機能を提供することで解決した．

2003 年 4 月より，学部や学科のメールサーバの移転については，メールアドレスが変更することを嫌う利用者が多いことに配慮し，学部や学科のアドレスに送られたメールが，新しい本センター設置のメールサーバのメールアドレスに転送されるよう設定した．こうして，メールサービスの利用者がサーバ移行に伴う大きな障害を回避することができた．

図 2 に示すように，本学のメールは，学外から学内へ，及び学内から学外への，いずれであっても全てのメールは本センターが設置したメールのウイルスチェックサーバを通過後，配送サーバを経由して学内外に配送されるように構築している．すなわち，本学に関する全てのメールは配送サーバを通過する．この配送サーバに転送設定することで，オリジナルのメールアドレスを本センターのメールアドレスに変換して，メールを転送することができる．なお，メールのウイルスチェックサーバの導入は 2001 年，メールの配送経路を統一したのは 2002 年当初である．これらにより，本センターのメールサーバが全学メールサーバとして，名実ともに認知され，メールサービスにおけるユーザ認証が本センターのものに統一される流れが確立した(2003 年).

4. Web サービスにおけるユーザ認証

4.1. Web ページ提供者に認証機能の提供

2000 年 11 月より本センターの利用者であって Web サーバを用いて Web ページを作成しようとする Web ページ開設者に対して，本センターのユーザ認証を提供するサービスを開始した．本センターのメールサービスにおけるユーザ認証は本センターの NIS(Network Information Service)サーバと連携していた．このユーザ認証も NIS サーバと連携することで実現した．メールサービスと同じ認証を提供することから、po-login(Post Office login)認証と称している．本センターの Web サーバは本学構成員であれば誰でも Web ページの作成ができる．また po-login 認証を用いれば，Web ページ開設者は，本センターの ID とパスワードによる認証するページを容易に作成することができる．

po-login 認証は Web サーバの基本(Basic)認証を用いて実現している．Basic 認証はそのままでは，ユーザ名はパスワードを暗号化されずにそのまま送られるという欠点があるが，通信を暗号化する SSL(Secure Socket Layer)と組み合わせることで解決できる．

Web ページ開設者は，Web ページ閲覧者のユーザ認証後の ID を取得できる(ページ開設者が環境変数から ID を取得する CGI (Common Gateway Interface)プログラムを作成した場合)が，パスワードを取得できない．すなわち，Web ページ開設者は不正に Web ページ閲覧者の ID とパスワードのリストを作成することができない．こうすることで，本センターの Web サーバを用いてページ開設者が，ユーザ認証を必要とする Web ページを自由に作成す

ることができるようになった．Web ページを作成する側からも，本センターのユーザ認証を容易に利用できる独自の仕組みが提供された．

使い方は次のとおりである．

① Web ページ開設者は認証を必要とするページのファイルを po-login という名前のフォルダ内に置く．
② Web ページ閲覧者が po-login のフォルダ内のファイルを閲覧しようとすると web サーバの Basic 認証が実行され，認証のためのダイアログがブラウザに表示される．
③ Web ページ閲覧者が本センターの ID とパスワードを入力し，その認証が正しければ，Web サーバは該当ページをブラウザに送信する．

単にユーザ認証機能を利用するだけであれば，CGI プログラムを作成する必要もなく，フォルダを作成し，その中にファイルを置くだけである．特に、特定の利用者のみに閲覧を許可したい場合，po-login フォルダ内に .groupfile というファイルを作成し，閲覧を許可したい利用者のユーザ名を列挙することで実現できる．

さらに, 2004 年からは PHP(PHP: Hypertext Preprocessor) 言語及び Perl(Practical Extraction and Report Language)言語による CGI プログラムを作成し, 許可を得る必要はあるが，Web ページ閲覧者の職員情報を取得する機能を提供した. 2001 年から本学評価委員会において導入された自己点検評価(YUSE)システムは, 独自サーバで運用されていたが，2005 年から本センターの Web サーバ上に移行し，この認証機能を利用するようになった．

4.2. 兼業申請システム稼動による人事情報連携

本学保健管理センターは全学構成員に対して，定期健康診断サービスを提供しており，全学の構成員にサービスを提供している点で，本センターと同じ立場である．全学構成員のリストと各構成員のデータを有する必要がある．データの質や内容は異なるものの，1)全学構成員のリストとデータを保有する点，また 2)全学構成員のリストを作成するためには，学務部及び人事課の協力が必要である点, では本センターと同じである. 1999 年から，保健管理センターでの定期健康診断の自動計測システムの構築に当初からかかわり，健診から証明書発行までのシステム構築を支援した[7]．これにより，全学構成員の個人情報取扱いのノウハウを蓄積した．

2003 年 10 月から，人事課が担当している兼業申請のための Web 申請システムの構築についての相談があり，協力して新しくシステム構築をすることとした．これは

1) 多くの教職員が申請している，
2) 最新の職員情報が必要，
3) 人事課が協力してくれる点

などにより人事情報との連携が不可欠であり，今後の統一認証を進める上で大変有効であると判断したことによる．このシステムのユーザ認証に人事課の同意のもと，本センターの ID とパスワードを用いることとした. 2004 年 2 月からサービスの提供を開始した．システム構築以前は，申請書類の処理に 2 ヶ月以上必要であったが，現在では数日で対応できるようになった．このシステムが稼動後，年度が替わる頃にはほぼ全教員が公式メールアドレス及び本センターの ID とパスワードを取得することとなった．このことにより，ユーザ認証を提供するために必要な職員情報の提供が人事課より迅速に行えるようになった．

4.3. 教職員 IC カード導入

2005 年 4 月より，全教職員の名札としての IC カードを総務課，人事課と連携し導入した．IC カード導入は総務課が主幹し，本センターは技術的支援及びシステム構築を行った．IC カードは名札の他，入退室管理，複合機利用管理，図書館利用証等に用いている．

新規採用や異動の情報は，人事システムに入力された後，本センターの認証サーバ用のデータベースに連携される．このデータベースの情報と写真データを組み合わせて IC カードを発行し, データベースに必要な情報を書き込む．IC カードは全教職員に渡される．このデータベースは図書館システム，入退室システム，複合機利用管理システム等と連携している．

人事システムには登録されていないが，大学の業務を行っている構成員にも，IC カードを発行する必要があり，人事課の情報だけでは不十分であるが，他のシステムとも連携することで対応している．

4.4. LDAP 認証の提供

本センターは LDAP(Lightweight Directory Access Protocol)[6]による認証を，本センターが管理する演習用 PC の Linux OS の認証のため整備していた．2004 年に学務部及び施設部が導入した講義室予約システムに対して，LDAP 認証の提供を開始した．

各部局等でのサーバが、本センターが提供する LDAP サーバと連携しユーザ認証を行うことが一般的である．しかし、本センターの Web サーバ上でシステムを作成する場合，1)システム構築及び管理が容易である，2)標準でユーザ認証機能が利用できるため，現在，多くの Web システムが，個別サーバを構築するのではなく，本センターの Web サーバ上で稼動している．

5. 評価・議論

本センターのユーザ認証は計算機利用の認証から始まったが，この数年間，ネットワーク接続におけるユーザ認証，メールサービスにおけるユーザ認証，及び Web サービスにおけるユーザ認証と連携させることで，概ね大学としての統一認証が実現できた．ID 登録のための個人情報は当初図書館と連携するだけだったが，学生部の学生情報，人事課の教職員情報とをそれぞれ連携することで，大学関係者の概ね全ての情報を保有することができ，本センターのユーザ認証は大学の標準認証としての地位を確立してきた．このことは，今後，デジタル証明書等の新しいユーザ認証システムなどを導入する際にも抵抗なく実施できることを保証している．

本センターが運用する主要サーバ，特にメールサーバ，Web サーバに利用者を誘導することで，サービスの集約化ができ，統一認証に進んだ．また，サービスの質，セキュリティ向上のため本センターが主導する立場となっている．

現在は，人事情報の個人番号をもとにユーザ認証サービスを提供している．職種によっては，非常勤職員から常勤職員へ，また，逆に常勤職員から非常勤職員に変更する場合がある．変更の際には，個人番号が変更になり，人事システムのデータ上は別人と扱われている問題点がある．実際，人事システムのデータ上は旧個人番号の職員は退職として扱われている．個人番号が変更されると，これまでのサービスが受けられなくなる．IC カードも個人番号が変更された時点で無効となる．

上記のように個人番号が変更した場合は，2006 年 4 月より，次の方法で，対応付けを行うこととした．

① 個人番号が変更した職員は大学情報機構に IC カードを提示する．
② IC カード情報を旧個人番号から新個人番号に変更する処理を行う．旧個人番号と新個人番号の対応付けを行う．
③ 本センターの ID とパスワードは新個人番号に対応づける．

なお，この問題の根本的解決には，人事システム内での検討が必要である．

また，非常勤講師の場合，同一人物でありながら，講義を行う学部毎に異なる個人番号を有している場合がある．ユーザ登録されていない非常勤講師の ID の発行や，IC カードの発行を行うには，どれか特定の一つと関係付けることが必要である．現状では，非常勤講師の申請により発行しているので，申請時，個人番号を選んでもらうようにしている．

ユーザ認証で用いる本人を特定するための情報は，教務システム及び人事システムに頼らざるを得ない．認証を進める上で，これらのシステムに必要な改善を行う必要がある．現状のデータを移行しなければならないこれらのシステムでは，対応が難しいかもしれないが，新システムでは，個人と番号の対応関係が例外なく一対一になるように構成されることを期待したい．また，本センターとしても，支援しなければならない．

IC カードの発行は教職員に限られており，学生には発行していないが，今後学生への発行を視野に入れ，展開すべきサービス等の整理を行っていく必要がある．

本センターが提供するサービスに集約したことで，シングルサインオンの機能を実現できているが，今後，サービスが多様化し，サーバの複数化に対応するためサーバ間で連携するシングルサインオンの機能を提供する必要がある．

現状では，ID とパスワードの組み合わせによるユーザ認証であるが，よりセキュリティの高い認証方式が必要となってきている．たとえば，学外から非常勤講師が担当講義科目の成績を入力するなどといった場合，ID とパスワードの認証だけでは不十分である．入力者を特定するためにデジタル証明書等を用いたユーザ認証方式を導入していく必要がある．デジタル証明書の運用については，技術的には可能であっても，実際の運用を想定したときに，公開鍵や秘密鍵の運用管理，システムの運用等をスムーズに行う仕組みを考えていく必要がある．

6. まとめ

本センターでは，この数年間，統一認証の実現が自然に行えるよう取り組んできた結果，おおむね大学としての統一認証が実現できた．また，本センターが提供する基本サービスの一つであるユーザ認証サービスは，全学の標準のユーザ認証と位置づけられ，全学のユーザ認証の管理をする部署は本センターという認知を得ることができた．

事務システムについは，文部省(導入当時)が指導するシステムが稼動しているので，個別の認証であり，システム連携も行えない状況である．国立大学法人化後，大学独自のシステムへの移行が検討されている．本センターが所属する大学情報機構の情報化推進課と連携して，これらのシステム改変の際に，認証の統一や他システムとの連携などの機能を組み込む必要がある．

国立情報学研究所が構築を目指している全国大学共同電子認証基盤(UPKI)のような大学間での統一認証への参加にも，学内の統一認証は必要条件となっている．認証の統一だけでなく，学内の情報システムの整備には，本センターが支援・連携しながら進める必要があり，大学の中での本センターの位置づけが重要となっている．

参考文献

[1]酒井善則，研究教育を促進する先進的 ICT インフラストラクチャ整備，大学電子認証基盤シンポジウム，pp.67-72 (2006)

[2]曽根原登，岡田仁志，岡部寿男，島岡政基，谷本茂明，峯尾真一，渡辺克也，全国大学共同電子認証基盤（UPKI）の構築，平成１８年度国立情報学研究所オープンハウスシンポジウム－最先端学術情報基盤(CSI)の構築に向けて－，pp.41-46 (2006)

[3]平野靖，内藤久資源，梶田将司，小尻智子，間瀬健二，名古屋大学のユーザ認証基盤の現状，平成１８年度国立情報学研究所オープンハウスシンポジウム－最先端学術情報基盤(CSI)の構築に向けて－，pp.41-46 (2006)

[4]馬場健一，岡村真吾，寺西裕一，秋山豊和，中野博隆，大坂大学における学内認証基盤の構築，平成１８年度国立情報学研究所オープンハウスシンポジウム－最先端学術情報基盤(CSI)の構築に向けて－，pp.41-46 (2006)

[5]久長穣，岡田隆，刈谷丈治，情報コンセントのユーザ認証について, 学術情報処理研究 No.2, pp.77-81 (1998)

[6]笠野英松監修，インターネット RFC 辞典，アスキー出版局(1998)

[7]久長穣，平野均，平田牧三，自動入力とデータデース化による Web 連携検診システムの構築, 第 30 回中国･四国大学保健管理研究集会報告書, pp.100-103 (2000)