解説

組織内認証基盤の構築

― 大阪府立大学における認証基盤の構築事例 ―

宮本貴朗[*1]・西本　隆[*2]・金森剛志[*2]・山本貴史[*2]・上田博文[*2]

[*1] 大阪府立大学総合教育研究機構／学術情報センター
[*2] NEC システムテクノロジー／第一公共システム事業部

大阪府立大学においては，平成17年4月に3つの大学の統合・再編と法人化が同時に行われ，その際に情報システムの再構築を迫られた．特に問題となったのは，これまで個別に運用されてきた情報システムの連携と認証基盤の構築である．本稿では，大阪府立大学で運用されている認証基盤である統合認証システムの設計理念や各種課題を克服するためのシステム設計等について紹介する．統合認証システムは，複数の情報システムの ID/ パスワードの統一，計算機ログインの統合，シングルサインオン，PKI システム，ディレクトリサービスなど一般的に認証基盤構築の際に用いられる技術を組み合わせることで構築されており，管理コストの低減，利便性とセキュリティの向上を考慮して設計されている．

はじめに

大阪府立大学においては，平成 17 年 4 月に 3 つの大学の統合・再編と法人化が同時に行われ，その際に大規模な情報システムの再構築が必要となった．まず最初に問題となったのは統合・再編によるカリキュラムの新設に対応した教務システムの構築と，これまでは自前で処理する必要のなかった財務会計や人事給与のためのシステムを独自で保有する必要が生じたことである．また，これまでは別の大学として個別に設計・運用されてきたキャンパスネットワークや情報教育システムなどの学内情報サービスについても再構築が必要となり，運用管理コストの低減，利便性とセキュリティの向上のため，個別の情報システムの連携と認証基盤の構築が課題となった．

本稿では，大阪府立大学で運用されている認証基盤である統合認証システムについて，その設計理念と設計時，開発・構築時，運用開始時に発生した各種課題を克服するためのシステム設計等について紹介する．統合認証システムは，複数の情報システムの ID/ パスワードの統一，計算機ログインの統合，シングルサインオン，PKI システム，ディレクトリサービスなど一般的に認証基盤構築の際に用いられる技術を組み合わせることで構築されており，管理コストの低減，利便性とセキュリティの向上を考慮して設計されている．また，認証基盤を構築する際には一般的にはディレクトリサーバを中心に置くよう設計することが多いが，ディレクトリサービスによる認証においては後述するように種々の制約があるため，本学の認証基盤の構築においては統合的に利用者情報を管理するシステム（利用者管理システム）を中心に据えた形態でシステム構築を行っている．

なお，ここで述べる主なシステムの設計・構築は平成 16 年度に行われたものであるため，現時点では技術的には少し古いものも含まれている．最近の認証基盤技術の動向については最後にまとめて紹介する．

情報システムの連携

まず，平成 17 年 4 月の大学の統合に向けてシステムの基本概念の設計が行われた．対象となるシステムは，情報交換の基盤となるキャンパスネットワーク，認証基盤の構築とポータルシステム，情報教育システム，財務会計システム，人事給与システム，教務学生システム，教員活動データベースシステムなどの事務系情報システムである．これらの個別の情報システム開発の共通点は，どのシステムも統合と法人化によって組織・体制の変更，基礎となる規則・規定の改変などがあり，それまでの既存システムでは対応できないため，新規開発が必要なことであった．

そこで，教員・職員・学生を利用者としてサービスする部分に関してはインタフェースを Web アプリケー

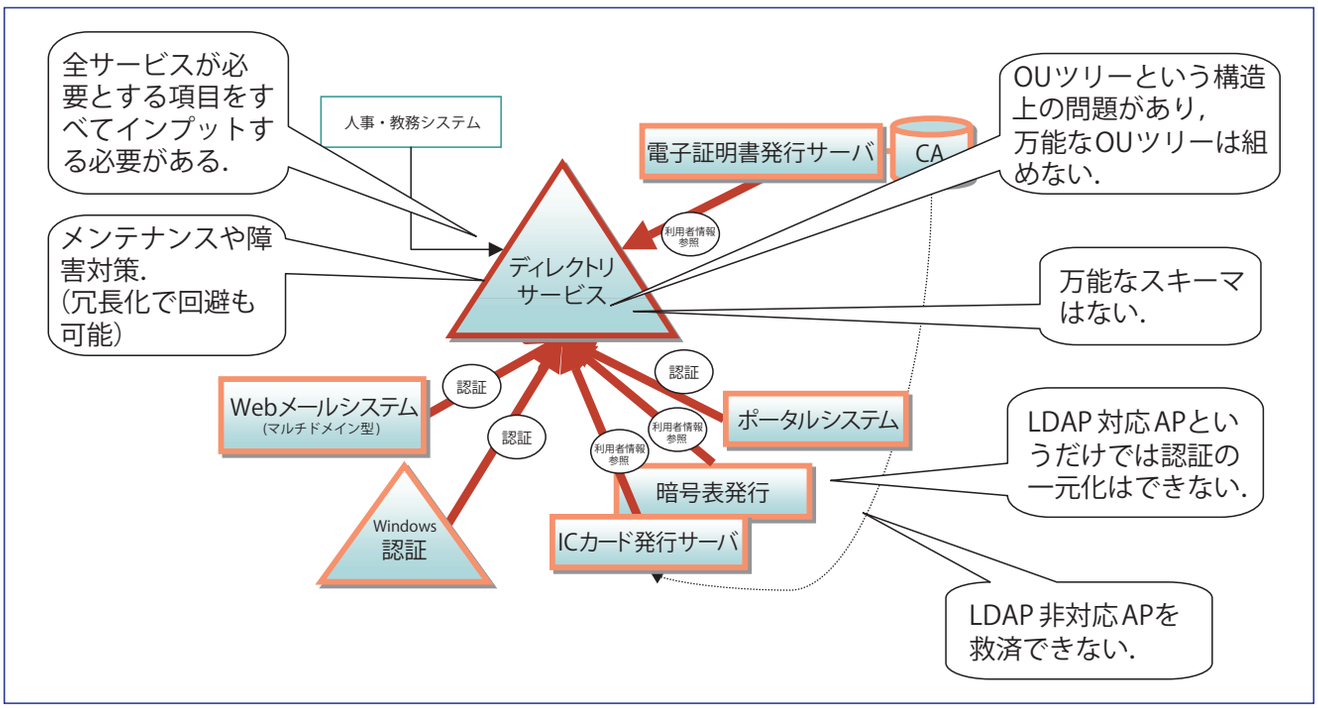

図-1　ディレクトリサービスによる認証の問題点

ションとして提供し，業務としてシステムを利用する場合においてもできるだけ Web アプリケーションの形態で利用できることを原則とした．大学内の情報サービスを一元的に提供するためのサービスサイトとして組織内ポータルシステムを構築し，認証連携する各情報システムに対してセキュリティ保護の重要度に応じて ID/ パスワード，PKI，暗号表の 3 つの認証方法を用いたシングルサインオン機能を提供することにした．また，同時に Web による発生源入力（情報の発生源になる人がシステムに直接入力すること，たとえば学生による Web 履修申請，教職員による物品購入依頼，出張旅費の登録など）の導入が計画された．

職員には各自に Windows 端末を配布し，計算機ログイン認証の一元化とともに搭載するアプリケーションを統一することにより管理コストの削減とサーバ側のアプリケーション開発の省力化を行った．端末が接続されるネットワークには持ち込み PC の接続を禁止し，情報漏洩防止やセキュリティ事故防止対策とした．また，職員・学生に対しては統一的に全学生・職員に Web メールシステムを提供し，職員・学生全員が使用できる環境を構築することとした．

これら情報システムの連携と管理コストの低減のため，利用者管理システムを中心とした統合認証基盤を構築し，利用者情報のシームレスな連携による利用者サービスの向上と，利用者情報を一元管理することによるセキュリティの向上を図ることを目標とした．

利用者管理システムとデータ連携サブシステム

これまで，大学においても情報化が進むに従い，多くの情報システムが部局ごとに開発・運用され，それぞれが ID/ パスワードを発行した結果，1 人がいくつもの ID/ パスワードを管理する必要があった．さらに今回は，3 つの大学の統合・再編と法人化が同時に行われ，事務系情報システムの再構築が必要になり，その結果，ID/ パスワードだけにとどまらず氏名や所属部署などの属性情報についても新旧の情報をさまざまな情報システムに格納する必要があった．

そこで，効率的かつ信頼性の高いサービスを提供するために，各サービスごとに分散している認証リソースを一元化し，ID/ パスワードのみならず，各種の属性情報についても情報の一元的な管理を行う統合利用者情報管理システムとして開発することとした．

《利用者管理システム》

一般的には，認証基盤の構築というと，LDAP（Lightweight Directory Access Protocol）サーバや ADS（Active Directory Server）などを中心としたディレクトリサービスをイメージすることが多い．しかし，**図-1** に示すように，認証システムを中心にして認証を一元化するモデルでは，クライアントとなる情報システムが，必要とする認証情報や各種利用者情報を網羅的かつ不整合なく保持する必要がある．そのため，最悪の場合にはクライアントの数だけの利用者管理構造を保持す

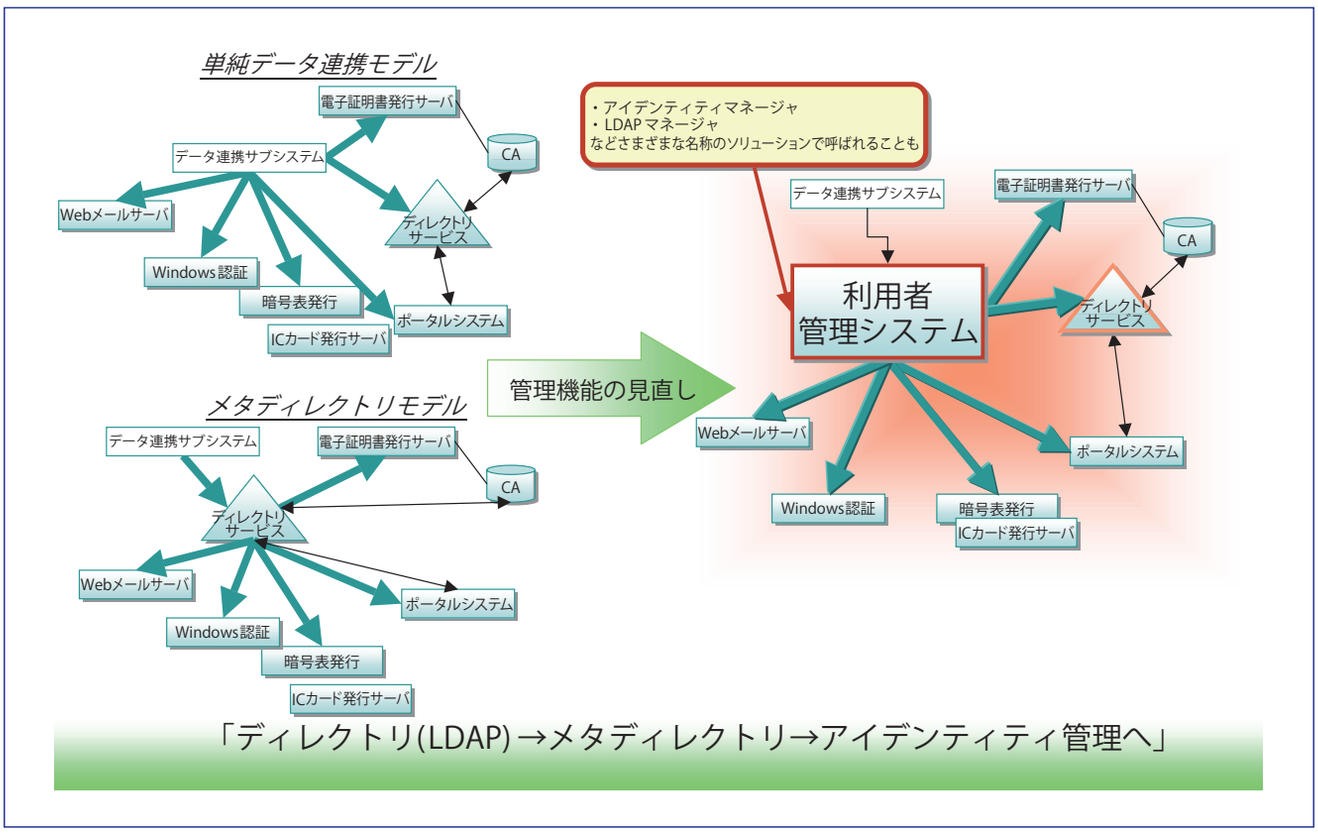

図 -2　利用者管理システムの位置付け

ることになり，それでは物理的に一元化されただけで管理コストは低減できない．特に，ディレクトリサービスを用いる場合にはデータベース構造に制約があり，データ項目間の関係が記述できないなどの問題がある．

そこで，個別の情報システムに必要となる情報と条件や要素などを分析し，認証情報や属性情報をパターンとしてまとめることができるかが問題となる．これまでは認証のための統一的な基準がなく，さらにその上でシステムがマルチベンダで構成されているため，個別の情報システムごとの独立した認証機能をそのまま利用せざるを得なかった．実際に，各情報システム固有に管理されている認証に関連する情報は，そのシステムの外部では管理できない情報も多く，しかも，人的に見てもそれらの情報の管理者が各部署に散在しており，運営上管理者を集約することが困難である情報も存在する．

そこで，**図 -2** に示すように，利用者情報の主たる管理機構は利用者管理システムに集約し，ディレクトリサービスなどの直接的に認証機能を提供するシステムはあくまでも最低限の検索情報管理システムと位置付けた．このことにより，利用者管理システムに対する管理・操作だけで全システムの利用者情報を一元的にコントロールできる．

利用者管理システムは，以下の設計思想および利点を持つ．

(1) 認証そのものを扱うのではなく，認証情報を管理するシステム
(2) ディレクトリサービスでは管理できない構造のデータの管理
(3) 付加的な属性情報（たとえば，システムアカウントに関連する情報）などの自動生成
(4) 運用管理のコスト削減

《認証要件の抽出とデータ連携サブシステムの設計》

認証機能を必要とする主なサービスは，財務会計システム，人事給与システム，教務学生システム，ポータルシステム，Web メールシステム，事務用 Windows 端末などがあり，それらのシステムはほとんどがパッケージベースのものであり，個別の情報システムごとに認証情報の入力インタフェース（入力データのフォーマットやデータ形式，必要データ数）が異なっており，利用者管理システムとの連携が問題となった．また，出力インタフェースも異なっており，個別の情報システム間でそれらを統一するには納期や費用の観点から現実的ではない．個別の情報システムごとにデータ形式が異なることは容易に想定できたが，実際には，同一ベンダ内のシステムにおいてもデータ形式が統一されておらず，ベンダ間だけでなくベンダ内においても連携の調整が必要であった．

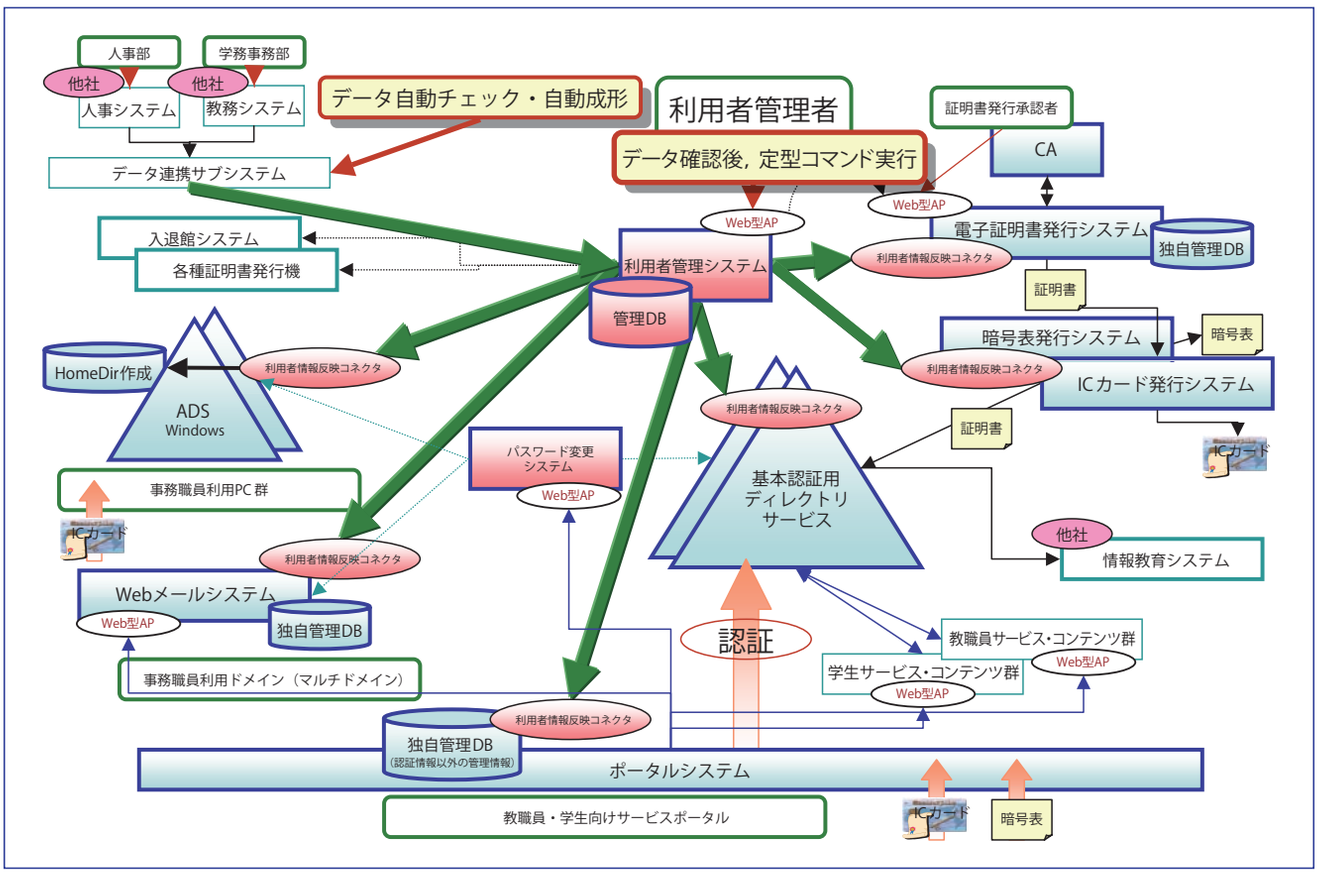

図 -3　大阪府立大学の認証基盤概念図

そこで，個別の情報システムで必要となる情報は，認証情報と属性情報のデータの発生源である人事給与システムおよび教務学生システム（教職員の情報に関しては人事給与システム，学生の情報に関しては教務学生システム）から取り込み，利用者管理データベースに登録するためのデータ連携サブシステムを開発した．

データ連携サブシステムの設計は，業務運用イメージを見据えた設計を行う必要があり，監視や承認，異常処理のリカバリなど認証情報や属性情報の完全性や安全性，一貫性を保証することが重要になる．そのため，ベンダ間の調整については，障害発生時の障害切り分けの観点からデータフローの設計，作業の分解点を決定することが必要であった．

ここで，本学における認証基盤である統合認証システムの概念図を**図 -3** に示す．

前述したように，認証情報および属性情報は情報の発生源である人事給与システムおよび教務学生システムからデータ連携サブシステムに取り込まれ，データを自動的にチェックするとともにデータ形式を変換して利用者管理システムのデータベースに格納される．利用者管理システムは，基本的な認証情報をディレクトリサービスや ADS に登録するとともに，必要に応じて個別の情報システムのデータベースに対して属性情報を登録する．

認証の際には，ディレクトリサービスに対しての LDAP による認証を基本とするが，利用者の Windows 端末のログイン認証に対しては ADS，LDAP に未対応の情報システムに対してはシステムカスタムメイドの独自システムにより認証連携する．

シングルサインオンの実現

認証基盤を構築するにあたり，認証を要するシステムをすべて洗い出し，統合認証基盤への適応可否と認証に必要な情報を整理することが重要である．この設計が，認証基盤の運用を左右する．本学では，高度なセキュリティを要求するアプリケーションも利用することから，通常の ID/ パスワードによる認証以外にも IC カードを用いた PKI（Public Key Infrastructure）認証，暗号表を用いた認証などの高度認証が可能な認証基盤を構築した．

認証基盤およびディレクトリサービスを使用する利用者サービスサイトとして本学ではポータルサイトを新たに構築した．高度認証（PKI，暗号表による認証）が必要なアプリケーションは，基本的には個別の情報システム側にあるが，個別の情報システムに高度認証を組み込むことは，費用的にも時間的にも非常に無駄が多い．そ

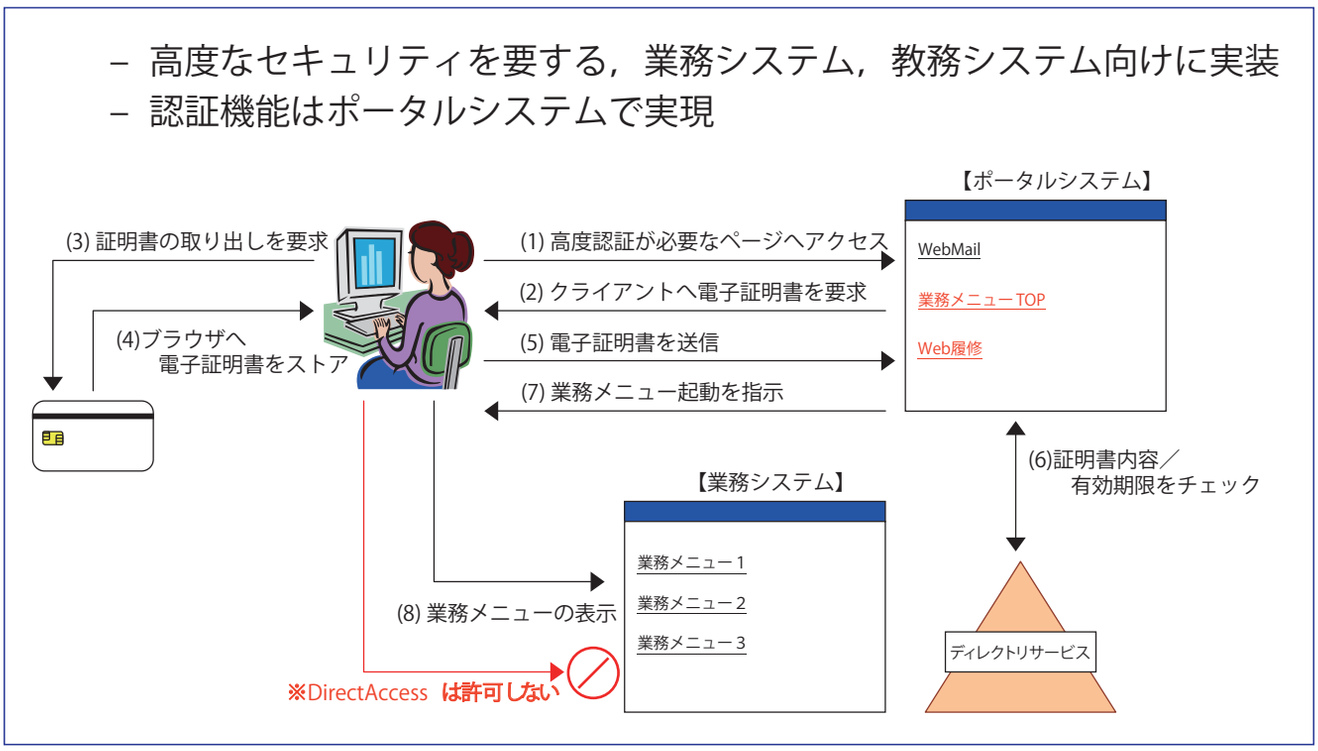

図 -4　高度認証のしくみ

こで，**図 -4** に示すように，ポータルシステム側に高度認証の仕組みを組み込み，高度認証が必要な場合はポータルシステムにて認証を行い，その認証結果を個別の情報システムに引き継ぐ形態で高度認証のシングルサインオンを実現することとした．

その結果，ポータルシステムにて認証された後には，通常は認証が必要な複数のアプリケーションを渡り歩く際にも個別の認証処理を必要としなくなった．また，個々の情報システムに認証情報を渡すことなく認証結果を得ることができるため，セキュリティの保護にも有効である．

《PKI（Public Key Infrastructure）》

PKI は，一般的には公開鍵基盤／公開鍵暗号基盤とも呼ばれ，公開鍵暗号を用いた認証や通信路の暗号化を用いることにより，インターネット／イントラネットを利用する際に脅威とされる，盗聴，改ざん，なりすましを防ぐことが可能である．

PKI を構成する要素として，電子証明書や認証局（CA：Certificate Authority），リポジトリを用意する必要がある．認証局の機能はさらに登録局（RA：Registration Authority），発行局（IA：Issuing Authority）に分けられる．発行局については，後述するように IC カードを用いて身分証明証としても利用することから，本人確認を学内で行う必要があり，大学内にて運用することとした．公開鍵へのディジタル署名方法として，信頼できる第三機関の利用や独自認証局の利用が可能であり，どちらの認証局を使用するかについては，運用のセキュリティポリシーに則り判断すべきである．認証局を独自で構築し運用するには，認証局自体のセキュリティを最高レベルで管理する必要があり，信用できない認証局では電子証明書が意味をなさない．本学では，認証局の運用については外部委託することも検討したが，コストおよび発行に必要な時間の問題から，最終的には学内で運用することとした．そのため，認証局の運用はプライベートな運用となっており，現状では他組織との連携はできていない．

《IC カード》

IC カードは，従来の磁気カードに比べ，セキュリティ面で優れており，現時点では，スキミングに対して最も有効なカードとされている．また，IC カード内部にメモリを搭載しており，磁気カードに比べ多くの情報を書き込むことが可能である．IC カードには，**図 -5** に示すように，読み書きの形態により「接触型」「非接触型」と両方の機能を併せ持つ「接触・非接触一体型」の 3 つのタイプが存在する．IC カードで実現したい運用を考慮して，どのようなカードを選択するのか検討する必要がある．具体的には，学内でサービスしている Web アプリケーションからの利用，入退出管理での利用，図書館システムでの利用，交通系など公共利用が可能なアプリケーションとの連動，電子マネー（ローカル

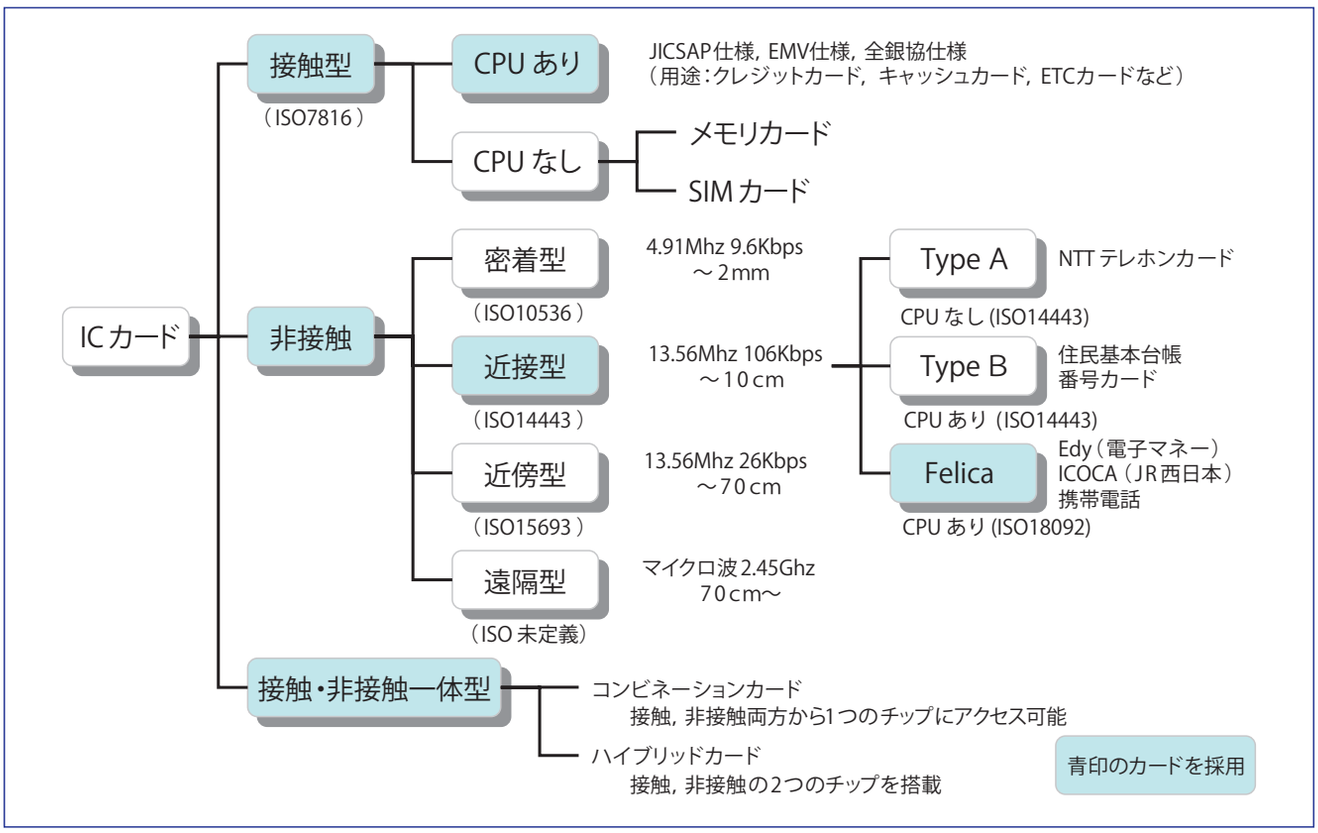

図 -5　IC カードの分類

マネー，プリペイド，ポストペイ）など多くのサービスを搭載することが可能になる．既存システムが IC に対応していない場合には，磁気カード情報を搭載させることも可能である．このように，「接触・非接触型一体型」と磁気ストライプ付きカードの機能を併せ持った IC カードも存在する．さらに非接触型は，通信方式の違いにより TypeA，TypeB，FeliCa 方式に分類される．

本学では，身分証明証（職員証／学生証）としても利用することから耐久性を考慮して非接触型のみの採用を検討したが，PKI に必要な情報を格納するためには IC チップの容量や演算機能を搭載する必要があったため，接触型＋非接触型（FeliCa）のハイブリッドカードを採用した．

ソフトウェア的には，パスワードや PKI の PIN コード（個人識別番号：Personal Identity Number）について，パスワード変更管理システムで生年月日をパスワードとして使用できないように実装するなどのセキュリティ的な対応を行っている．また，デザインの設計時にセキュリティだけでなく，顔写真や氏名は記載が必須であるが，学部名などの部署名や生年月日については記載の必要があるのかなどの個人情報保護の観点からも検討を行った．

利用者管理システムでは，技術的にはすべて自動連携を行うことが可能であったが，身分証明証発行 /IC カード発行については，自動的に発行せず，手動での確認・承認処理操作（ボタン押下等の必要最小限の介入で自動データ連携，および発行処理ができるようにシステム化）が必要な運用を行っている．これは，身分証明証を審査なく発行するのはセキュリティ上の問題があることと，IC カード発行については 1 枚あたり数千円の費用がかかるため，人的に印刷機を操作することでできるだけ印刷ミスをなくすためである．

《暗号表による認証》

PKI 認証は，IC カードリーダが必要になること，導入検討時点では利用可能な OS が Windows に限定されたことから，端末の環境が統一されていない教員の研究室からの利用においては，全員が利用できる条件を満たせなかった．また，自宅から利用する場合についても同様の問題があった．

そこで，高度認証においては PKI 認証だけではなく，暗号表によるワンタイムパスワード認証をポータルシステムに組み込むこととした．暗号表は，インターネットバンキングの暗証カードをヒントにしたマトリックス表（10 行 ×10 列）を用い，アプリケーション側よりマトリックス表の数カ所の座標の入力を求められる．

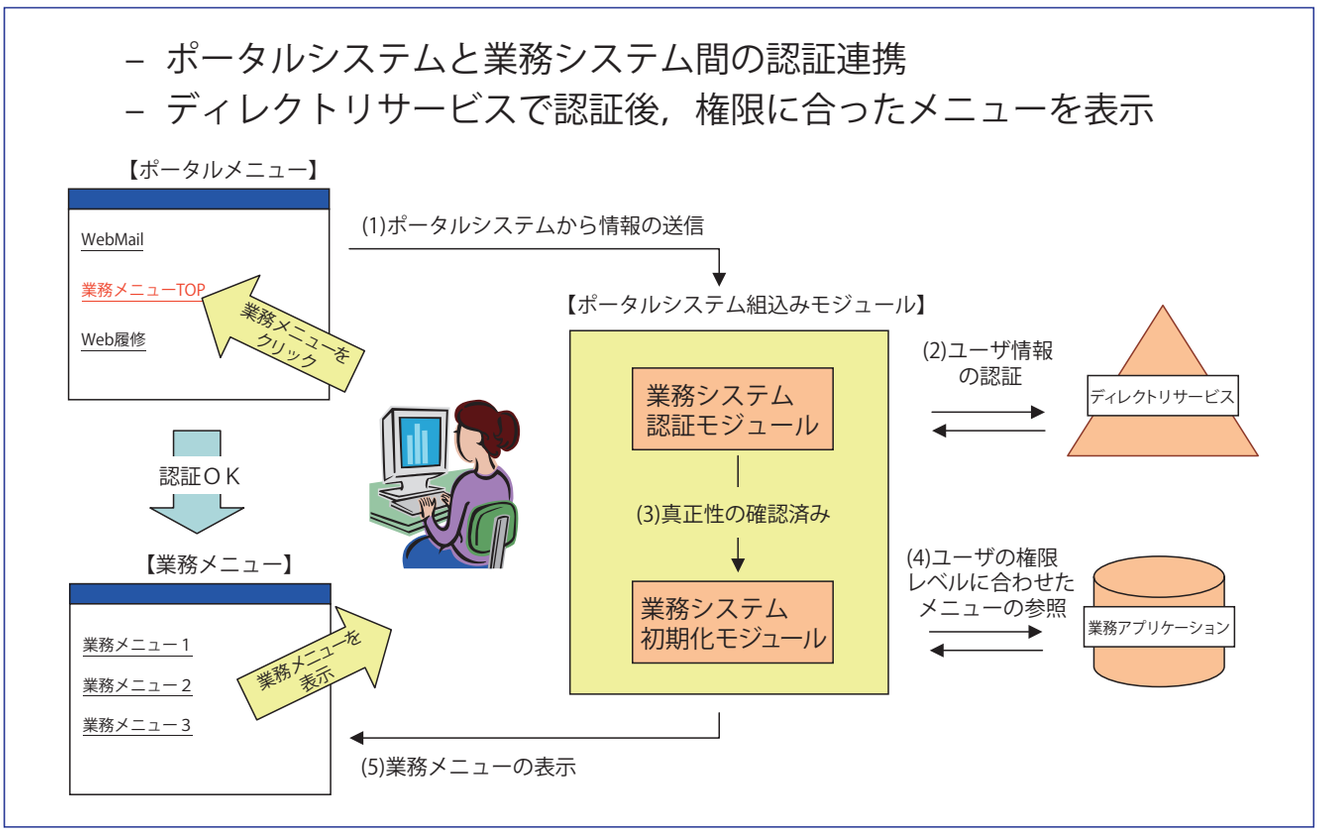

図 -6　認証連携のしくみ

《個別の情報システムとの認証連携》

ポータルシステムと個別の情報システムの連携には，シングルサインオンに必要な認証情報の連携と機能利用権限情報の判定と連携が必要となる．現実には，実際に採用された個別の情報システムは，いずれもシングルサインオンに対応できておらず，新たに組み込む必要があった．

ポータルシステムと個別の情報システムとの認証連携については，当時実現可能な手段としては，Form 認証，Agent 認証，Cookie 認証，リバースプロキシ認証があった．個別の情報システムは基本的にパッケージベースでの導入を前提としていたが，当時は他システムからのシングルサインオンが一般的ではなく，個別の情報システム側に特定の認証機構を要求することは困難と判断し，ポータルシステム側にすべての認証方式を実装する方針とした．

Form 認証は技術面とコスト面で実現が比較的容易であるが，業務アプリケーションの呼出し時の URL 漏洩の問題が懸念された．これについては，ポータル側で URL の隠蔽処理を組み込むことで回避した．Agent 認証は業務アプリケーション側の改造コストの問題，Cookie 認証はセキュリティ的な問題についての検討が必要であった．また，リバースプロキシ認証は隠蔽性には優れているが，当時はまだ製品が少なく，イニシャルコストおよび運用面においても相応のコストが必要となる．

個別の情報システム側のシングルサインオン認証モジュールは，既存の認証モジュールを置き換える形で実装を行った．大まかなロジックは，**図 -6** に示すように，(1) ポータルから送信されてくる情報（個別の情報システムにより要求する情報は異なる）を基に，(2) 認証モジュールがディレクトリサービスに認証情報の確認を行い，(3) 個別の情報システムで得られた認証結果の真正性を確認したら，(4) 初期化モジュールが業務アプリケーションに権限情報を参照し，(5) 権限情報に応じた業務メニューに移行するもので，(1) の部分はポータル側で個別のカスタマイズを可能にする，(2) の部分は業務アプリケーション間共通モジュールとすることにより開発コストの低減とセキュリティポリシー維持を両立させた．

3 大学の統合により，利用者管理項目の増加や利用者に提供する情報の多様化（ID/ パスワード，暗号表，IC カード）により管理データの増大が予想された．また，個別の情報システムのアクセス権限の管理も問題となる．理想的には，それぞれ個別の情報システムでのアクセス権限を示すフラグを統一的にディレクトリサービス上で管理し，各個人ごとにそのアクセスフラグを設定することにより，各サブシステムのアクセスコントロール

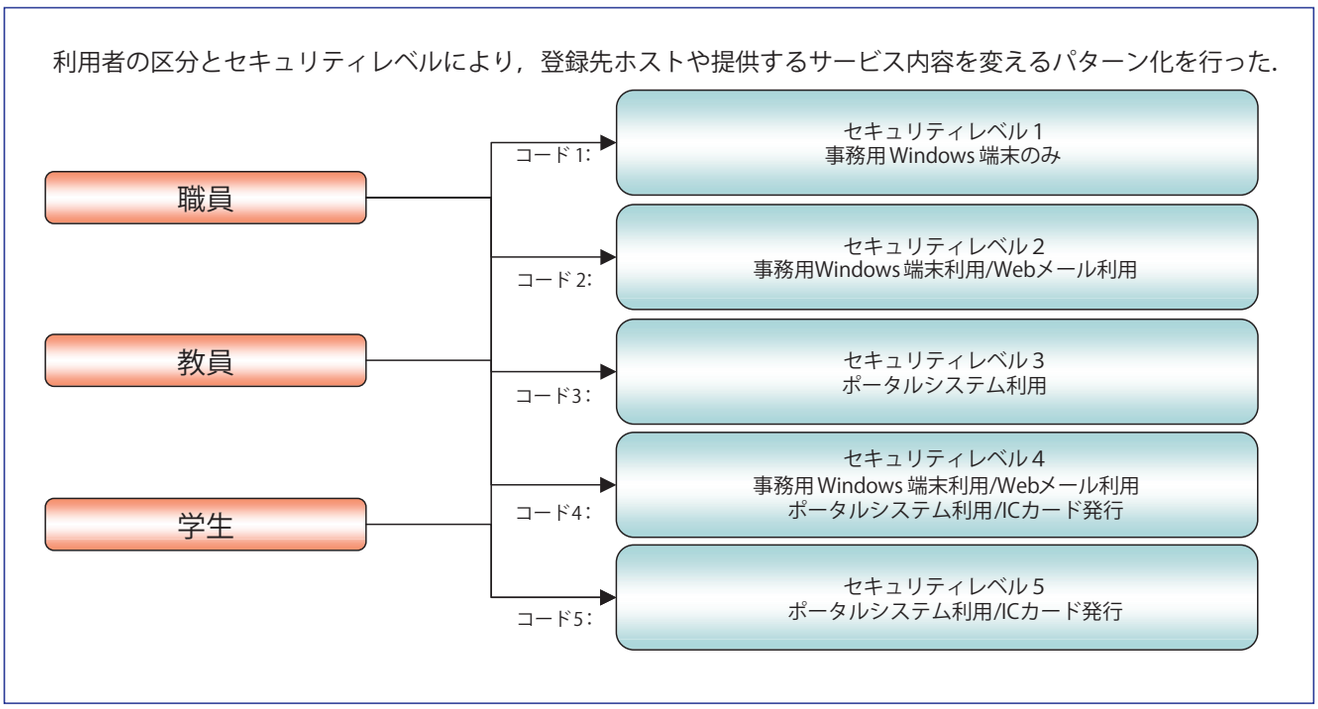

図-7　5つのセキュリティレベル

ができることが望ましい．しかし，実際の業務の現場においては業務上の権限が詳細に分かれており，個別の情報システムにおいてその権限設定を実現することは難しい．また一方，利用者の視点では利用者の区分（教員・職員・学生）により，アクセスできるサービスは大まかに分類できることから，セキュリティレベルという概念を用いたアクセス権限で運用することとした．

セキュリティレベルは，ディレクトリサービスで管理されている所属組織と職種，役員および個人指定などによる利用者の区分とデータ連携サブシステムで付加する個人ごとのセキュリティレベルを組み合わせて，**図-7**に示すように利用者を5段階に分けている．利用者管理システム配下の個別の情報システムの利用については，利用者管理システムからセキュリティレベルに従って自動的に個別の情報システムに対し，必要なアクセス権を設定している．

《ディレクトリサービスとログイン認証》

クライアント端末を認証するADSディレクトリサービスをレプリケーションすることは技術的には可能であったが，事務用Windows認証を行う利用者は全学の利用者ではなく，特定の利用者（事務職員）に限られること，レプリケーションで連携する場合は，ディレクトリサービスのツリー構造に合わせてレプリケーションする必要があることから，ADSとの連携については，利用者管理システムで実現した．

情報教育システムなど一部のシステムにおいては，非常勤の教員や特定の科目のみを履修する学生，イベントなどで本学の構成員以外の利用者登録が必要になるなどの例外的な処理が必要となるため，個別の情報システム独自の利用者管理システムが必要となる．そのため，ADSを直接参照せずに，ディレクトリサービスを参照する部分にサーバ／クライアント型のディレクトリ連携ツールを開発・導入することで利用者情報を取り出し，独自の利用者管理システムに認証情報を登録している．この場合，セキュリティ上の観点から，ディレクトリサービスへ接続できるクライアントの特定と，アクセスコントロールを各項目ごとに行い，どの場所から何を検索したのかすべてのログを収集している．

実際の開発・構築の際に発生した問題点と最近の技術動向

ここでは，問題点の発生時期を3つに分けて，システムの開発前から想定されていた問題，開発・構築の途中で見つかった新たな問題，運用を開始した後に発生した問題について，その問題点と対応について述べる．また，最近の認証基盤技術の動向について，本学の事例に照らして考察する．

《システムの開発前から想定されていた問題について》

- 各々の業務システムの認証および権限管理の実装方式

認証に関しては，前述したとおり，認証モジュールの差し替えと独立性が高い実装方式により比較的容易に実

現することができた．しかし，業務システムの権限管理の実装は困難を極めた．その理由は(1)権限管理は各業務システムと密接に絡んでおりアプリケーションの改修が困難であること，(2)業務システムの権限管理は所管の職員の業務であり，全学認証用のディレクトリサービスの直接的な情報操作を許可することでセキュリティ面で不安が生じることである．そのため，外部から権限を管理する機構は使用せずに運用することとした．

《開発・構築の途中で発生した問題について》

• 各業務システムの設計の遅延に伴うシステム間連携部分の設計の影響

本来，業務システムの詳細設計完了後に各サブシステム間の連携部分の設計が行われなければならない．しかし実際には，3つの大学統合・再編と法人化という大規模な事業のため，各業務システムは並行して詳細設計を行う必要が生じた．このため，システム間の連携部分の設計作業もスケジュール圧迫の中で並行して行わざるを得ない状況であり，マルチベンダ環境によるオーバヘッドも重なった．この問題に対しては，各ベンダごとの責任分解点の明確化とデータ連携サブシステムを導入することでモジュール化することにより開発期間の短縮で対応した．

• データ連携サブシステムのシステム肥大化

データ連携サブシステムの設計は，業務体制やセキュリティポリシーと密接に絡むため，十分な業務分析と設計作業が必要であったが，時間的制約により個別の情報システムごとの特性を十分に評価できなかった．そのため，運用開始後にいくつかの問題が発生することとなった．データ連携サブシステムの導入は，個別の情報システム間の連携を可能にし，個別の情報システムの改造経費を押さえることができたが，データ連携サブシステム自体は大規模なシステムとなったため，開発時間とコストが必要となった．

• ICカードの納入納期問題

ICカードの作成は，当初はカード業者へのアウトソーシングを検討した．しかし，8,000枚程度の発行枚数ではカード市場では小規模と判定され，ブランクカードの納期の制約が大きいこと，またカード印刷にいたっては，1～2カ月以上の時間を要することが判明した．

大学では，学籍情報入手からカード配布まで数日で行う必要があり，結果カード業者へのアウトソーシングは事実上断念せざるを得なかった．そのため，学内に用意したICカード印刷機3台で自営印刷を行う方針とした．結果的に，ICカード印刷ミスも少なく（1%未満）満足のいく成果を得られた．

《運用開始後に発覚した問題について》

• データの不整合の発生

データ発生源のシステムでの禁則処理が甘く，仕様外のレコードが生成された．具体的には必須データがブランクとなっていたり半角全角文字の混在，存在しない所属コード値の指定，外字コードなどである．当初は全件目視確認を行い対応，運用にチェック処理ルーチンを盛り込むことで解消を図った．

• 設計時には想定外の（検討漏れではない）例外事項の発生

設計当初，大学統合後の運用が定まっておらず設計時に考慮されていない内容もあった．たとえば，想定外の兼務の発生や学内ルール外のメールアドレスやドメインの要望等である．投資対効果を考慮し，手動設定による処置もしくはシステムの改造で対応を図った．

《最近の技術動向》

ここでは，最近の認証基盤に関する技術について，本学が構築した統合認証システムの事例に照らして考察する．

最近，少しずつ標準でLDAPに対応したアプリケーションが増えてきている．しかし実際には，認証のみLDAPを参照する製品が大半で，システム側にユーザ登録が必要になることに変わりはない．これは，業務システムには，権限情報が必須でありディレクトリサービスで管理している情報と異なることが原因と考えられる．また，シングルサインオンにおいては，構築当初に比べリバースプロキシ製品も増えており，機能も充実してきている．URLの隠蔽などセキュリティ効果も期待できる．ただし，同時接続時の性能面で十分な考慮が必要な上，コスト面での問題は残る．いずれにせよ，以前よりはSSO環境の構築はたやすくなってきているのは事実である．

データ連携という観点では，一般的なデータベースとディレクトリサービスを自動連携させる製品が登場し，画面からパラメータを設定するだけで連携できるものもある．ただ，どこまで自動連携させるのかの判断は難しく，必ずしも完全自動での運用は推奨できない．そのため，今回のシステムでは，あえて介入部分を設けている．いずれにせよ，以前と比べ格段にデータ連携環境の構築が容易になってきている．

ICカード発行に関しては，大学の特性を考慮すると身分証明証としての発行は，自営かそれに準ずる形とならざるを得ない．最新の印刷機は高性能化されており，

時間的にもコスト的にも十分に自営でICカード証明書の発行が可能な状況になった．

おわりに

当時は，認証基盤を使用したソリューションが少なく，各アプリケーションからどのように使用すればよいのかベンダごとに手法が異なっていた．これらの違いは，利用者管理システムを中心とした認証基盤を構築することとポータルシステムの導入により解消することができた．今回，認証基盤やICカードの導入を行ったが，効率的な利用をするためには多くの検討すべき項目がある．以下に，本システム導入後，拡張された機能と現在検討している機能を挙げる．

認証システム構築以降に導入されたシステムには，教育研究支援システム，図書館システムがあり，これらは認証基盤と連携して利用者管理が行われている．また，ICカードの利用として非接触のICチップを使用して，建物／部屋の入退出管理，出席管理，図書の貸出に利用されている．これらは，現時点ではセキュリティの問題から入退出管理のみ手作業での登録となっている．また，有線／無線のネットワークに接続する際に認証を必要とする認証ネットワークシステムやIPアドレスの申請などの各種のWebを用いたオンラインの申請手続きも連携されている．

最後に，本稿では大阪府立大学において設計・構築された認証基盤を例として組織内認証基盤について紹介した．今後，アクセス権限の設定などについての検討と，まだ連携ができていない学内の情報システムとの連携，他大学の訪問者を想定した他大学との認証連携の検討も必要であると考えている．この解説記事が少しでも読者の役に立つ情報となれば幸いである．

（平成20年2月26日受付）

宮本貴朗（正会員）
aki@center.osakafu-u.ac.jp

1987年大阪府立大学大学院総合科学研究科修士課程修了．1988年同大学大学院工学研究科博士後期課程退学．同年同大学計算センター助手．現在，大阪府立大学総合教育研究機構教授．学術情報センター教授および情報基盤システム研究所所長兼務．情報システム，情報ネットワーク，情報セキュリティに関する研究に従事．

西本　隆
nishimoto-txa@necst.nec.co.jp

1982年関西日本電気ソフトウェア（株）入社以来，NEC文教マーケットのシステム開発およびシステムSI構築に従事．現在，NECシステムテクノロジー（株）第一公共システム事業部第二システムグループ グループマネージャ．

金森剛志
kanamori-txb@necst.nec.co.jp

1991年関西日本電気ソフトウェア（株）入社以来，NEC文教マーケットのシステム開発およびシステムSI構築に従事．現在，NECシステムテクノロジー（株）第一公共システム事業部第二システムグループ主任．

山本貴史
yamamoto-txf@necst.nec.co.jp

1993年関西日本電気ソフトウェア（株）入社以来，NEC文教マーケットのシステム開発およびシステムSI構築に従事．現在，NECシステムテクノロジー（株）第一公共システム事業部第二システムグループ主任．

上田博文
ueda-hxc@necst.nec.co.jp

1994年関西日本電気ソフトウェア（株）入社以来，NEC文教マーケットのシステム開発およびシステムSI構築に従事．現在，NECシステムテクノロジー（株）第一公共システム事業部第二システムグループ主任．