IC カード全学導入に向けた認証基盤システム整備と評価

Development and evaluation of authentication infrastructure system in the aim of introducing an entire smart card system

清水　さや子†，戸田　勝善†，吉田次郎‡
Sayako SHIMIZU†, Masayoshi TODA†, Jiro YOSHIDA‡

smz@kaiyodai.ac.jp, toda@ kaiyodai.ac.jp, jiroy@ kaiyodai.ac.jp

†東京海洋大学情報処理センター
‡東京海洋大学大学院海洋科学技術研究科

†Information Processing Center, Tokyo University of Marine Science and Technology
‡The Graduate School of Marine Science and Technology, Tokyo University of Marine Science and Technology

概要

近年，大学において認証システムが重要視されるようになり，認証基盤システムの充実化や利用者アカウントの厳格な管理が求められている．東京海洋大学では 2006 年のシステム更新時に統合認証システムを導入することによりアカウントの一元化を図った．アカウントの一元化はユーザにとっては一組のアカウントとパスワードを覚えるだけで複数のシステムが利用できるため，利便性の向上につながったが，アカウントの管理や統合認証システムと連携するシステムにおける運用については，問題が山積みになっていた．そこで，2011 年のシステム更新では，IC カードの全学導入も考慮したシステムを検討する必要があり，アカウントやシステムの管理方法も含め認証基盤システムの見直しを検討し，新たに統合ディレクトリシステムの構築を行った．統合ディレクトリシステムの構築により，アカウントやシステムの一元管理が実現することができ，運用の効率化につながった．本稿では，旧システムでの問題点および新しく構築した統合ディレクトリシステムで解決できた問題について述べる．

キーワード

認証基盤システム，アカウント，統合ディレクトリシステム，IC カード

1. はじめに

近年，統合認証システムが導入されアカウントとパスワードの一元化が進みつつある[１]．アカウントとパスワードの組み合わせは一度破られると，後々に重大な問題に発展する恐れがあるため，さらなる認証セキュリティの強化として IC カードによる認証システムが使われることも多くなっている．

東京海洋大学は，2003 年 10 月 1 日に東京商船大学と東京水産大学が統合されて発足した大学である．統合に伴い両大学に存在していた情報処理センターも組織としては統合されたが，システムについてはレンタル契約上の問題等により，地区ごとに異なるシステムが稼働していた. そして, 統合から約 3 年が経過した 2006 年 8 月に，情報処理センターシステムの更新を行い，キャンパスごとに独立して稼働していたそれぞれのシステムを統合し，アカウントにおいても一元管理できるよう統合認証システムを導入し，実質的な統合を行った.

IC カードは，旧東京水産大学にあたる品川キャンパスで, 不正アクセス防止のため 2000 年から教育システムの認証用に導入されていた経緯より，2006 年 8 月のシステム更新時に, 全学的に IC カード学生証が導入されることになった[２][３]．これによって，全学的に教育システム利用時には IC カード認証が取り入れられた. この時より，統合認証システム導入によるアカウントの一元化，IC カード学生証導入による各種 IC カードを使った認証システムが利用可能になったが[４]，アカウント管理の問題，各システムのユーザ登録方法の問題，各システムに対する認可の問題等，様々な問題も発生していた.

2011 年の情報処理センターシステム更新では，これらの問題解決に向けて，ユーザおよびシステムの一元管理ができるシステムの構築を検討した．また，IC カードについては現時点では学生に対してのみ IC カード学生証を導入しているが, 教職員向けに IC カード身分証の導入も検討中であるため，IC カード全学導入を前提に認証基盤システムの設計を行い，新しく統合ディレクトリシステムの構築を行った.

2 章では，認証基盤システムの整備に至った様々な問題について述べ，3 章では，問題解決するための統合ディレクトリシステムの設計について，4 章では，構築したシステムとその評価，5 章でまとめと今後の展望について述べる.

2. 認証基盤システムの整備に至った旧システムの問題

アカウントの一元管理を実現した統合認証システムでは，アカウントの管理が重要となる．大学の構成員は学生と教職員だけでなく，短期間採用の職員や派遣社員，企業在席の研究者等などのさまざまな期間，さまざまな身分の人（以下，一時利用者とする）が存在する.

2.1 アカウント管理の問題

旧システムでのアカウントは，統合認証システムを管理している情報処理センター発行のアカウントとして，登録，管理は，情報処理センターで行っていた．登録方法は学生の場合と教職員や派遣社員，研究員等の場合で大きく異なっていた.

i. 学生情報の登録

学生情報を登録する場合, 学生は IC カード学生証が導入されていることより，入学者が決定し次第，学生担当係が IC カード学生証の発行用データ作成し, 学生証の発行手続きを行う．その後，情報処理センターではこの発行用データを受領し加工することにより，システムに反映させていた．学生情報を削除する場合は，同じく学生担当係から年度末に卒業者・退学者リストを受け取り，その情報に基づいて削除作業を行っていた．学生情報については，学生担当係からの情報を基に登録・削除作業を行っていたため，大きな間違いは発生しなかった.

ii. 教職員や研究員等情報の登録

教職員や研究員等の情報を登録する場合，学生以外は IC カード身分証が導入されていないため, IC カード発行用のデータを作成している部署がなかった．それで，新規採用の教職員は，着任時にアカウント登録申請書を情報処理センターに提出し，情報処理センターにて申請書情報の確認後，登録用データを作成し，登録作業を行っていた．アカウント削除は，離任時に本人が削除申請書を情報処理センターに提出し，情報処理センターにて削除作業を行っていた. これらは, 情報処理センターでは，個人情報を管理しておらず，本人の申請に基づき登録・削除作業を行っていたため，着任しても申請せずにアカウントを保持していない人や，離任しても削除申請がないため，退職者が削除されていない人がいることも多くあった. 特に常勤教職員以外については, 把握が困難で，離職後でもメールや図書館のサービスが利用可能な状況が生じていたため，ライセンス違反となる可能性があった.

各システムに対するアカウント管理の重要性は認識していたが，情報処理センターではユーザの正確な在職状況の有無を確認する術がなかった．また，身分属性に応じて，利用できるサービスが異なるが，身分属性を判断することが困難な場合があり，間違った情報が登録されることもあった．最近では，学認に参加する大学も増えており，東京海洋大学においても学認の参加に向けて準備を進めている所である．学認に参加することは，所属する大学のアカウントで学認加盟機関の様々なサービスを受けることができるようになるため[５][６]，さらなるアカウントの厳格な管理が求められるため，認証基盤シ

ステムの整備が必要であった.

2.2 各システムのユーザ情報の登録方法に関する問題

旧システムでは，以下のシステムが統合認証システムと連携していた.

- Gateway サーバ，研究支援サーバ
- ファイルサーバ
- Mail サーバ
- 研究室用 www サーバ
- 教育用 UNIX サーバ
- 教育用 Windows ドメインサーバ
- E-Learning サーバ（2 種類）
- SSL-VPN システム
- 無線 LAN 認証システム※1
- SSO ポータルシステム※1

統合認証システムと連携しているメールサーバやファイルサーバ，Windows ドメインサーバや E-Learning サーバ等ほとんどのシステムが，統合認証システムの LDAP サーバとは別に，身分属性に応じて個別にユーザ情報の登録をしなければならなかった．これらのユーザ情報の登録は，情報処理センターで行っていた．申請書に記されている情報を基に LDAP サーバ登録用データを作成し，LDAP サーバに登録後，LDAP サーバ登録用データをシステムごとに必要な形に加工し，システムごとに登録作業を行っていた．そのため，1 回のユーザ情報の登録作業に 1～2 時間要していた. あらかじめ登録日を決めていたが，ユーザにとっては，申請書を提出しても即時にアカウントが発行されず，システムが利用できない状態であることが多々あり，不便が生じていた.

2.3 システムに対する認可の問題

情報処理センターでは，認証基盤システムとしてアクセスしてきた情報の照合をすることはできても，各部局で個別にシステムを立ち上げ，管理されているシステムに対して，利用者に利用権を与えるという「認可」を行うことは非常に難しい．情報処理センターが管理するシステムであれば，認可は行えるが，情報処理センターシステムの中には，過去の経緯により，他部局管理のシステムを導入しユーザ管理をおこなわなければならないことがあった．具体的には，事務用 Windows ドメインサーバの管理であった．ユーザの正しい情報が管理できない中，また，日々，管理・運用業務に追われている少人数の組織で※2これらの作業を行うことは非常に負担となっていた.

2.4 IC カードの管理に対する問題

東京海洋大学では，2006 年度の情報処理センターシステム更新時より，学生に対しては IC カード学生証が発行されることになり，情報処理センター教育システムのログイン時の認証，証明書発行システムや図書館の図書貸出システム等で利用している．2010 年度の情報処理センターシステム更新時には，全学的に IC カード身分証の導入を検討しており，IC カード発行・管理システムは，学生向けではなく，全学のシステムとして管理運用できるようにする必要があった.

IC カード発行・管理システムは全学のシステムということより，システムの設計や構築，管理運用は情報処理センターで行うが，システム内の情報は各担当係（IC カード学生証であれば学生担当係，教職員向け IC カードであれば教職員担当係等）が必要に応じて作成し，登録することになっていた．これは，情報処理センターでは正しい在籍者情報を保持していないことと，組織の規模より個々の IC カード発行，失効，再発行等の管理運用が行うことが非常に困難であるためである.

現在，IC カード身分証の導入については停滞中であるが，導入された場合，教職員に対しては教職員担当係，派遣職員に対しては契約担当係等，身分属性によって担当部局が異なるが，各担当係が IC カード発行用のデータを作成することになる．そうなれば，情報処理センターでは，学生情報と同様，登録ユーザ情報の漏れがなくなり，適正なアカウント管理が行えるものと考えた.

3. 統合ディレクトリシステムの設計と構築

前章で紹介した旧システムの問題の解決に向けて，ユーザ情報および各システムの利用権および IC カード発行・管理システムの一元管理ができる統合ディレクトリシステムの設計・構築を行った．本章では問題解決において検討した内容について述べる．統合ディレクトリシステムでは，身分属性ごとの各担当係が IC カード身分証（学生証含む）用のデータを登録すれば，アカウント発行，身分属性ごとに異なる利用システムへのユーザ情報登録，登録したアカウントに対する IC カードの管理が行うことが可能になる．さらに，統合ディレクトリシステムでは，情報処理センターの管理外のシステムに対して，

※1 これらは 2006 年度のシステム更新時ではなく，2010 年度に新たに構築したシステムである.

※2 東京海洋大学情報処理センターは，専任職員（技術系職員）2 名，兼任のセンター長 1 名および兼任の副センター長 2 名，非常勤職員（事務系）数名で構成されている.

そのシステムの管理者がユーザごとに利用権の可否を設定することができる.

3.1 他大学の導入事例

一般的にアカウントの発行は，採用時・入学時に，担当部署からユーザ情報のデータを受け取り，センターが発行する場合や[５], 採用後・入学後にユーザが申請し，申請があったユーザのみ発行する場合がある．前者については，先進的に，全学レベルで事務方が全学 ID 管理をしている大学もあるが，全学 ID が発行されるだけでは，センター管理のシステムのシステムが利用できるわけではない[８]．大規模大学のように，学内にサーバが分散しており，部局ごとにメールサーバがあり，部局ごとにメールアカウントを発行しているため，採用時・入学時に全学アカウントがなくても問題ないような大学もあるが[９]，本学のような小規模大学では，メールサーバは情報処理センターで一元管理しており，利用には全学アカウントを利用するため，採用時・入学時にアカウント発行できるシステムであるのが望ましい．さらに，認証基盤システムやアカウントの管理が重要視され，専用の組織（センターやチーム）を立ち上げた大学もみられる[９][１０]が，本学においては，全学的にそのような動きがないため，専用の組織を立ち上げるのは困難であると思われる.

3.2 アカウント管理の問題回避に向けて

現在，東京海洋大学には，約 3000 人の学生と約 700 人の教職員，その他として派遣職員や企業研究者等の一時利用者で構成されている.

情報処理センターでは，統合認証システムのアカウント発行に必要な情報として，アカウント，氏名，ローマ字氏名，学籍番号（教職員番号），契約期間（ある場合），身分属性（所属グループ）等の比較的簡易な情報を管理していた．これらとは別に，事務局では詳細な個人情報を格納した DB を管理している．しかし，身分属性ごとに担当部署が異なるため，それぞれの部署に DB が存在する．本来は，この事務局の管理する DB と連携して必要情報を自動抽出し，統合ディレクトリシステムに反映させられることが望ましいが，事務専用ネットワーク内で稼働しているシステムであるため，セキュリティや個人情報等のポリシー問題もあることより，連携することが非常に難しかった．そこで，DB を管理している事務局で，必要情報を抽出し，採用・入学の度に，統合認証システム用のアカウントを登録・発行することができれば, アカウント情報は比較的正しい情報となる. しかし，事務局に登録業務を依頼することは，事務職員にとって技術的に困難であること，また業務が負担増になることなどから旧システム時においては難しかった.

3.2.1 IC カード発行用データとアカウント発行用データ

東京海洋大学では, 全学的に IC カード身分証の導入が検討されている．そうなると，事務局では，身分属性ごとの各担当部署を明らかにし，担当部署ではそれぞれの IC カードを発行することになる.

先に導入されている IC カード学生証を例に挙げると，IC カード発行用のデータに必要な情報は，漢字氏名，ローマ字氏名，学籍番号（教職員番号），所属，有効期限等である．これらの情報のほとんどが統合認証システムのアカウント発行に必要な情報と重複する. IC カード発行用データに発行するアカウント情報さえ追加すれば，アカウント発行用のデータとなる．これらより，IC カード発行システムと統合認証システムのアカウント情報の登録が一度で行えるようなシステムの設計を行った.

ここで問題となるのは，アカウント名である．従来は申請時に希望アカウント名を受け付けていたが，個別対応および重複確認の手間もあった．かねてから運用効率化における問題になっていた．これらを踏まえて，今回を期に，アカウント登録時に自動でローマ字氏名から指定の文字を抜き出し重複防止文字を追加する仕組みを作成した．これによって，従来の希望アカウント名の申請は廃止し，IC カード発行用データを登録するだけでアカウントが自動で発行することができるようになり，登録時の個別対応の手間が削減できた.

ただし，海洋大メールシステムでは，メールアドレスが*アカウント名*@kaiyodai.ac.jp としているため，発行されたアカウント名に対応したメールアドレスになる．現状では，本人の希望するメールアドレスが作成できないため，エイリアスを作成するなどして対応中であるが，今後は, メールアドレスにアカウント名を出さないよう，個人の希望メールアドレスが使用できるよう，検討中である.

3.2.2 登録担当係

IC カードを発行する場合，大学という組織においては身分属性ごとに担当部署が異なるため，どういった身分属性の人をどういった部署が担当すべきかが問題になる. 大学という組織は教員・職員の他，派遣契約職員や受託研究員・共同研究者等も在籍する．これらの人は在籍期間も業務もさまざまであるため，把握が非常に困難である．さらに，事務局を通さずに出入りしている企業在席の研究者等もいるが，非常に多くのパターンが予想されるため，今回は検討しないこととした.

まず，事務局で把握できる学生以外の人員に対して，

表 1　登録担当ロール

項	ロール分け	操作対象ユーザ
1	学生担当係	学生
2	教職員担当係	教職員
3	派遣契約等担当係	派遣契約などの職員
4	研究員等担当係	受託研究員等・共同研究者・訪問研究者等
5	ゲスト・テスト用アカウント担当係	ゲストカード・テストアカウント・システム管理者用アカウント
6	全管理者	全ユーザ

身分属性により 25 のグループに分けグループ ID を設定する．学生に対しては，便宜上，学科ごと入学年度ごとにグループ分けグループ ID を設定する．これらのグループ ID に対して，今回の統合ディレクトリシステムにおいては，学生は 1 グループ，学生以外は人員担当部署ごとに 5 つのグループの合計 6 つのグループ分ける．6 つに分けたグループには，それぞれ担当ロールとして事務局の担当部署を割り当て（表 1），それぞれの担当ロールは，割り当てられたグループに属する人員の IC カード発行手続きを行うと同時にアカウントの発行ができるようにする．

これらによって，項 2.4 の問題も解決し，アカウント登録漏れや削除漏れ問題も解消されると考える．

表 2　IC カード管理ロール

項	ロール分け	操作対象 IC カード
1	IC カード学生証管理係	学生証
2	IC カード職員証管理係	教職員証
3	IC カード簡易利用証管理係	派遣契約などの施設利用カード
4	IC カード簡易利用証管理係	受託研究員等・共同研究者・訪問研究者等用の施設利用カード
5	ゲスト・テスト・管理用カード担当係	ゲストカード・テスト用カード・
6	全管理者	システム管理者用のカード

本システム導入時においては，それぞれの登録担当ロールが IC カードを発行する設計であるが，大学当局の要望により，将来的に同じ部署の中でも登録担当係と IC カード管理係と分かれる可能性があるとのことより，さらに，表 2 のとおり，IC カード管理ロールも作成し，それぞれ担当する対象のカード情報に分ける（表 2）．操作対象 IC カードは，それぞれ操作対象ユーザと同じとする．

3.3　各システムにおけるユーザ登録方法

旧システムでは項 2.2 のとおり，システムごとに個別にユーザ登録を行っていたが，アカウントが発行されると，統合認証システムや，連携しているシステムに対しても自動でユーザ情報が登録されることが望ましい．そこで，統合ディレクトリシステムでは，グループ ID ごとに，以下のシステムに対して利用可否情報の DB を作成しておき，アカウントが発行されると，グループ ID を閲覧し，該当グループ ID に対して利用可能なシステムのユーザ登録や利用領域の割当てが自動でされるようにする．また，アカウント削除時には，統合ディレクトリシステム上からアカウントが削除されることにより，利用可能であったシステムからユーザ情報や利用領域の削除を自動で行う．

- LDAP サーバ
- Gateway サーバ，計算サーバ
- ファイルサーバ
- Mail サーバ
  - 転送メールシステム含む
  - Web ファイルシステム含む
- 研究室用 web サーバ
- DNS ツールシステム（IP アドレス管理用）
- 教育用 Windows ドメインサーバ
- 教育用プリンタ管理システム
- E-Learning サーバ
- 無線 LAN 認証システム※1
- SSO ポータルシステム※1

これらの実現により，アカウントを発行するだけで，利用できるシステムにユーザ情報の一括登録ができるようになるため，各システムに対する登録・削除作業の手間が削減され，非常に運用効率化につながる．

3.4　他部署管理システムの利用権発行方法

旧システムでは項 2.3 の通り，過去の経緯により，他部署管理のシステムを情報処理センターシステムとして導入し，ユーザ登録も情報処理センターで行うことがあった．情報処理センターでは，他部署管理のシステムに対して，個々のユーザに対する利用権の可否を知ることが非常に困難であり，非常に手間が発生していた．

2010 年度のシステム更新時には，旧システムで導入していた事務局用 Windows ドメインサーバは事務局に移転したが，新しく図書館システム用に SSL-VPN が導入されることになった．SSL-VPN は図書館に申請があった

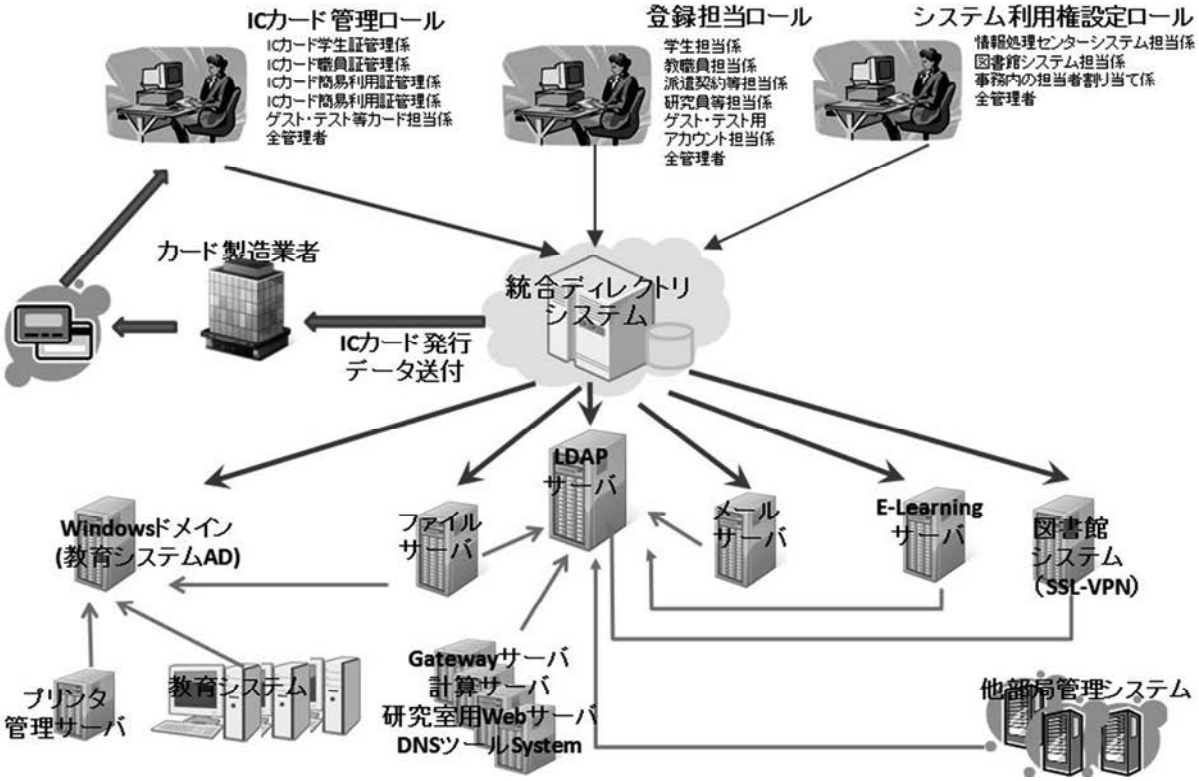

図 1　統合ディレクトリシステム

人だけ利用できるシステムであるため，情報処理センターでは，ユーザ登録を行うことはできない．そこで，事務職員でも比較的操作しやすいインターフェースを構築する必要があった．また，情報処理センターシステムにおいてもアカウント登録時にあらかじめ設定しているシステムに対して自動でユーザ登録されるが，個別に設定変更する場合もでてくる．さらに，登録担当ロールと IC カード管理ロールの各担当係の割り当てについては，事務局内で行われるため，事務局内で担当係の割り当てができたほうが効率がよい．

表 3　システム利用権設定ロール

ロール分け	操作するシステム
情報処理センターシステム担当係	情報処理センターシステムの各システムにおける認可
図書館システム担当係	図書館システムにおける認可
事務内の担当者割り当て係	登録担当ロール・IC カード管理ロールに関する認可
全管理者	システム利用権に関する属性の全て

これらより，表 3 のとおりロール分けし，統合ディレクトリシステムでロールごとに操作するシステム分けを行った．各ロールの担当係が担当範囲内について個別にユーザを設定できるようにする．ただし，操作対象者が事務局内の担当係となるため，Web 上から簡単に操作できるように簡素なインターフェースを構築した．

4. 構築した統合ディレクトリシステムの運用と評価

新しく構築した統合ディレクトリシステムでは，各登録担当者がユーザ情報を登録しアカウント発行を行うと，あらかじめ設定しているグループ ID ごとに，各システムの利用可否を確認し，利用可能なシステムに対して自動でユーザ登録が行える．また，将来的に身分属性ごとに IC カードの管理担当者も設定できるよう構築している．さらに，各システムの利用権を個別に登録や変更する際には，システム利用権担当者により，設定変更することができる（図 1）．本章では，本システムの運用方法について述べる．

4.1　ユーザ情報の登録

教職員であれば採用時，学生であれば入学時時に，それぞれ担当ロールの係が IC カード発行用のデータを作成し，統合ディレクトリシステムの管理画面よりユーザ情報の登録・アカウント発行業務を行う．

図 2　ユーザ登録用画面

ユーザ情報の登録作業は，1 部署で集中して行うのではなく，担当ロールごとに担当者が作業を行うため，Web インターフェース上で行う．さらに，作業は事務職員が行うため，図 2 のように比較的分かりやすくシンプルにする．登録作業における負担を軽減するため，登録情報は必要最低限の個人情報とする．登録時に Web インターフェース上のグループ ID を選択することで，あらかじめグループ ID ごとに設定されている利用可能なシステムに対して自動でユーザ登録される．グループ ID は登録時に選択するが，設定間違いを最低限にするため，担当ロールごとに複数のグループ ID が登録できるが，1 つのグループ ID に対して登録できるのは 1 つのロールとしている．また，IC カードの券面に表記される所属情報は，登録時に詳細に入力する必要はなく，あらかじめグループ ID 対して所属名の紐付けが行えるよう設定しているため，正しいグループ ID を選択するだけでよい．

IC カードの発行は，登録時に Web インターフェース上の「カード発行ステータス」箇所を「発行」とすることにより，ユーザ情報登録後，IC カード発行に必要なデータが抽出される．抽出されたデータをカード発行会社が指定する Web 入稿システムでアップロードすることにより，カードが発行される．

Web インターフェース上では必要な情報をテキストボックスに入力して登録するか，登録件数が多い場合は，あらかじめ csv ファイルを作成して一括登録も可能とする．Web インターフェース上から個別削除や一括削除もできる．

4.2　アカウントとカードの有効期限

登録時にアカウントとカードの有効期限の設定する．有効期限後は自動的に各システムのアカウントとグループ ID ごとに登録された利用可能なシステムの利用を停止する．通常は有効期限後，直ちにアカウント削除を行うのがよいが，例えば 3/31 に卒業した人が，4/1 にどうしても必要なデータを吸い上げるのを忘れていた事を思い出した時等に対応できるよう，有効期限後は一時的にアカウントをロック状態，カード使用不可状態にして，2 か月後に自動でアカウント削除を行う．登録時に有効期限を設定することにより，基本的には事務担当者が削除作業をする必要はない（表 4）．

IC カードの有効期限は，学生であればアカウント有効期限と同じであるが，教職員であれば，5 年間とする．非常勤職員の場合，アカウントの有効期限は長くても年度末までであるため，年度末までにアカウントの期限延長作業をする必要がある．ただし，カードには有効期限が記されるため，更新の可能性のある教職員に対しては，あらかじめ有効期限を 5 年とする．カードの有効期限前に退職した場合，先にアカウントの有効期限が切れるため，IC カードの停止処理を行わなくても，システムは利用できなくなる．ただし，認証基盤システムと連携して

表 4　アカウントの登録と有効期限に対するシステムとカードの利用可否

イベント	フロー	日付例	対応	アカウント利用可否	カード利用可否
新規登録	アカウント登録	2012/4/1	常勤教職員のアカウント有効期限は 2020 年と設定 非常勤はアカウントの有効期限を 1 年間に設定	○	×
	IC カード発行依頼	2012/4/2	IC カード発行依頼処理(業者に発行依頼) 学生証の IC カード有効期限はアカウントの有効期限と同じ (教職員の IC カード有効期限は 5 年間と設定)	○	×
	IC カード納品	2012/4/9	IC カード担当係宛に納品	○	×
	IC カード受け渡し	2012/4/10	IC カード個人に配布	○	○
期限延長	期限延長	2013/3/2	アカウントの有効期限が切れる前に再設定	○	○
期限切れ	IC カード返却	2013/3/21	IC カード返却	○	×
	期限切れ	2013/3/31	アカウントの自動的一時停止 IC カードの停止処理は行われないが、アカウントは停止 カードが返却されていなくても、ログイン不可	×	×
	アカウント削除	2013/5/31	2 ヶ月後にアカウント削除	×	×

おらず，カード内の読み取り可能な製造ID（IDm）等を認証情報とする簡易入退館システム等を個別に運用している場合にては，失効処理をしない限り，カードさえ持っていれば使えてしまうため，認証システムを管理する部局は運用ポリシー等を設定しておかなければならない.

4.3 IC カード運用上のイベント時の対応

IC カードを運用する際には，IC カード紛失，再発行，留年，休学，復学というイベントが発生する．これらのイベントについて，表 5 のように設定した.

I. IC カード紛失時

カードの使用停止処理を行い，数日間待ってカードが見当たらない場合は再発行手続きを行う．その間は，アカウントは停止処理しないため，カードを使ったシステムのみ利用できなくなる．再発行カードが納品された時点で，カード停止処理が解除され，新しいカード情報が上書きされ，カードを使ったシステムも利用できるようになる.

II. 留年の場合

アカウントは有効期限内に期限延長処理をしなければならない．カードについては券面に有効期限が記されているため，再発行することになる．カードがない間は，カードを使ったシステムのみ利用できない.

III. 休学の場合

アカウントも IC カードも停止処理を行うため，IC カードを使ったシステムも情報処理センターが管理する学内システムも利用できなくなる．復学した際にはアカウントと IC カードの復活処理を行い，両システムが利用できるようになる.

4.4 アカウントに対するパスワード変更および利用システム閲覧サービス

統合ディレクトリシステムではアカウントやシステムの登録等だけではなく，ユーザがパスワードを変更する際のインターフェースを提供している．ユーザがパスワード設定を行う際には，統合ディレクトリシステムの該当 URL にアクセスし，アカウントと現パスワードを入力してログインし，新パスワードの入力を行えば，LDAP サーバに反映される仕組みである.

また，ユーザごとに利用できるシステムが異なるため，ユーザごとに利用可能システムの一覧が表示できるインターフェースも備えている．ユーザが該当 URL にアクセスすることにより，各システムの一覧とそれぞれ利用の可否が表示される.

4.5 運用の評価

本システムの構築により，今まで情報処理センターで行っていた，個々のユーザに対する登録，変更，削除作業が事務局への移行を実現した．このため，今まで情報処理センターのアカウントとして，利用されてきたアカウントが，全学的なアカウントとなった．アカウントの管理が事務局に移行したことにより，ユーザ ID 通知書の発行・通知やパスワード再発行作業も事務の担当係が行うことになった．また，ユーザの情報を別の DB で保持している部署においてそれぞれ登録を行うため，ユーザ情報の登録漏れや誤入力がほとんどなくなった．ただし，非常勤職員用アカウントの有効期限については，一

表 5 イベント発生時のシステムとカードの利用可否

イベント	フロー	対応	アカウント利用可否	カード利用可否
IC カード紛失	紛失届	IC カードの一時停止処理	○	×
	紛失確定	一時停止している IC カードの執行処理(再発行)	○	×
IC カード再発行	IC カード発行依頼	IC カード発行依頼処理(業者に発行依頼)	○	×
	IC カード納品	IC カード担当係宛に納品	○	×
	IC カード受け渡し	IC カード個人に受け渡し	○	○
留年	留年決定	アカウントの有効期限延長	○	○
	IC カード返却	IC カード失効処理(再発行あり)	○	×
休学	休学・停学申請	アカウントの一時停止 IC カードの一時停止処理	×	×
復学	復学申請	アカウントの復活処理 IC カードの復活処理	○	○

部厳格な管理が行えていないケースもあるようである．本システム構築によって，情報処理センターとしては業務軽減の効率化が実現されたほか，かねてから問題であった正確なアカウント管理が行えるようになったといえる．

5. まとめ

本システムでは，IC カードの全学導入にむけて認証基盤システムを整備するため，旧システムでの問題を分析し，新しく統合ディレクトリシステムを構築した．

旧システムで問題となっていたアカウント管理，各システムのユーザ登録方法，各システムに対する認可についてさまざまな検討を行った結果，全てを一元管理できる統合ディレクトリシステムを構築した．アカウント発行・管理については，旧システムでは情報処理センターが行っていたが，本システム導入により，事務局の担当係が発行・管理を行うことになった．各システムに対するユーザ情報の登録は，旧システムでは個別に行っており，1 回の登録に約 1 ～2 時間かかっていた．しかし，統合ディレクトリシステムにアカウントを登録すると，グループ ID ごとにあらかじめ登録している利用可能なシステムに自動でユーザ登録されるため，1 回の登録にかかる時間は，数分程度となった．さらに各システムに対する認可については，旧システムでは，登録対象ユーザが不明であったり複雑であったが，簡易な Web インターフェースを用意することにより，各担当部局の担当者が容易に，認可を行えるようになった．

さらに，旧システムでは IC カード発行システムは単体のシステムとして稼働していたが，本システムでは統合ディレクトリシステムが包含し，IC カードの発行・失効等の管理も可能とした．

本システムが稼働して約 1 年になるが，Web インターフェースの一部改修は必要とするものの，大きな問題は発生していない．今後，IC カード身分証の全学導入が行われる予定であるが，本システムの構築により，比較的にスムーズに導入でき，システムも稼働できることを期待する．

参考文献

[1] 江原康生「大阪大学における新全学 IT 認証基盤システムの構築と運用」電子情報通信学会論文誌 D, Vol.J95-D, No.5, 1172-1182, 2012

[2] 清水さや子，横田賢史，戸田勝善，吉田次郎「東京海洋大学における IC カード学生証の運用・評価および今後の展開」学術情報処理研究 No.13, 64-73, 2009

[3] 清水さや子，横田賢史，戸田勝善，吉田次郎「東京海洋大学における全学 IC カード導入と多機能化に向けた取り組み」学術情報処理研究 No. 14, 149-152, 2010

[4] 清水さや子, 清水悦郎, 戸田勝善「IC カード認証・統合認証の連携システムの開発とその現状・評価」大学情報システム環境研究 VOL.11, 94-102, 2008

[5] 中村素典, 山地一禎, 片岡俊幸, 西村健, 庄司勇木, 古村隆明, 岡部寿男「学術認証フェデレーションを活用するサービスの展開」第 27 回インターネット技術第 163 委員会（ITRC）研究会 CIS 分科会,2010

[6] 松平 拓也, 笠原 禎也, 高田 良宏, 東 昭孝, 二木 恵, 森 祥寛「大学における Shibboleth を利用した統合認証基盤の構築」情報処理学会論文誌 52(2), 703-713, 2011

[7] 沖野浩二, 布村紀男「富山大学における認証基盤の整備による業務軽減評価」学術情報処理研究 No. 14, 31-39, 2010

[8] 岩沢和男, 宮原俊行, 中川敦, 岩田則和, 西村浩二, 吉富健一「センターサービス利用登録システムの再構築」学術情報処理研究 No. 15, 149-152, 2011

[9] 京都大学情報環境機構” IC カード導入の効果” http://www.iimc.kyoto-u.ac.jp/ja/services/cert/iccard/merit.html

[10] 飯田勝吉, 新里卓史, 伊東利哉, 渡辺治「キャンパス共通認証認可システムの構築と運用」電子情報通信学会論文誌 B,Vol.J92-B No.10 pp.1554-1565,2009