Vol.2016-IOT-35 No.3
Vol.2016-SPT-20 No.3
2016/9/23

管理運用システム「Salut」の概要

櫻田武嗣[†1]　三島和宏[†1]　石橋みゆき[†1]　萩原洋一[†1]

概要：本学では，2016 年 2 月に教育用電子計算機システムの全面的な更新を行った．電子メールをはじめとする様々なシステムの更新を行ったが，その一部として今回管理運用システムを構築し，運用を開始した．この管理運用システム「Salut」はユーザからの各システムの申請を受け付ける処理だけでなく，アカウントの棚卸し等の機能，他システムとの自動連携による権限付与など様々な機能を有し，さらにクラウドサービスへの自動展開も行うことが可能である．本稿では，本学でこれまで運用してきた申請管理システムについて触れ，さらにこのシステムの特徴について述べる．

キーワード：管理運用システム，システム間連携，申請システム

About the System called “Salut” for Management and Operation

TAKESHI　SAKURADA[†1]　KAZUNORI　MISHIMA[†1]
MIYUKI　ISHIBASHI[†1]　YOICHI　HAGIWARA[†1]

Abstract: In our university, it was to update the computer system for education in February 2016. It has been updated many of the system, including the e-mail system as well as a computer room. In this update, we make the management and operation system "Salut", began the operation. "Salut" accepts the use application of each system from the user. In addition, "Salut" has the features, such as intersystem coordination and account inventory. "Salut" is also cooperation with the cloud service. In this paper, we describe our previous application management system. And it describes the features of the "Salut" system.

Keywords: User management system, Intersystem coordination, Application management system.

1. はじめに

学校や企業で情報ネットワーク等を含む情報システムを利用するには多くの場合，情報システム用のアカウントが必要である．システムが単独で動作している場合には，各システム内にアカウントを作成するだけで管理できるが，いくつもの情報システムを利用させる場合にはアカウントを何らかの形で管理しておく必要がでてくる．企業や初等中等教育現場の多くの場合には情報システムを利用する人をあらかじめ把握できる．企業の場合には授業員，初等中等教育の場合には教職員,児童,生徒といった具合である．またそれぞれの職種に応じてシステムの利用権限を付ければ良いことが多く比較的管理しやすい．

しかしながら高等教育機関，特に大学等においては事情が異なる．東京農工大学（以下，本学と記す）でも正規教職員，正規学生の他に非常勤職員や講師，名誉教授，短期留学生，単位互換学生，連携大学院の学生，派遣職員，共同研究員，業務委託先など様々な人が大学に出入りしており，全員を把握できているわけではない．これに加えて学会や公開講座なども行われており，情報システムを利用する可能性のある人を把握することはさらに困難である．

本学でも古くから情報システムの利用者の管理[1]を行ってきており，これまでにいくつかのシステムを構築し，運用[2]してきた．他大学においてもネットワーク利用情報の管理などは行われてきている[3][4]．しかしながらこれまでの利用者管理用のシステムは，バックエンドはデータベースで保持しているものの,利用者側にはシステムの利用・廃止申請が行える程度の Web インタフェースを提供する程度であった．このため自分が多くの情報システムの中のどれを利用できるのかを確認することが難しかった．また情報システムの利用権限も職種で決めていたため，複数の職種を掛け持つ兼務の場合には個別に権限を割り当てできないため，その扱いが難しかった．また多くのシステムへアカウント情報を反映するのが手動であったり，情報システム管理の業務委託などに対応できていなかったりと課題が多かった．

2016 年 2 月の本学の教育用電子計算機システムの入れかえに合わせ，利用者からの申請などを受け付けることができる管理運用システムを新たに整備し直した．本稿ではこのシステムの概要について述べる．

2. これまでの管理運用システムの課題

情報システムを運用する場合には，大きく分けてアカウントなどを含む利用者関連の管理と，システム自体の管理の２つがある．後者はシステム構成管理，状態監視，ログ監視などがあり，すでに様々なシステムがある．本稿では

†1 東京農工大学総合情報メディアセンター
Information Media Center, Tokyo University of Agriculture and Technology.

前者のユーザ関連の管理を行うシステムについて述べる．

一般的に利用者やアカウント管理としてLDAP(Lightweight Directory Access Protocol)やAD(Microsoft Active Directory)が利用されることが多い．小規模なシステムであればこれらだけを利用すればシステムの利用管理ができるが，組織が複雑になったり，システム数が多くなってきたりと大規模になるとLDAPやADだけで管理する事は難しい．

実際の運用ではLDAPやADの前段階に利用者，アカウントを管理するシステムが用意される．我々も前述のようにシステムをいくつか構築し利用してきた．

しかしながら我々が使用してきたこれまでのシステムではいくつかの課題が残っていた．管理することを目的としていたため，利用者自身が現在の状態の把握や新たなシステムの利用開始,停止をするのが分かりにくかった.また，アカウント名，パスワードでログインするシステムの管理ではできてもIPアドレスの管理やファイアウォール設定，DNS設定の管理などはできなかった．

運用する側でも課題があり，利用者などから申請された内容を実システムに反映する作業は，どこかに手作業が入る形となってしまっていた．さらに最近では外部のシステムの利用や，システムの運用を一部外部委託するようになってきており，それらに対応するのが課題となっていた．具体的には利用者からの申請などがあった際に，外部委託の業者がその内容を確認し，システムの設定を行い，設定完了を大学側へ伝える必要がある．これまでは電子メールなどでやりとりしており，どこまで設定されたのかの管理が煩雑になっていた．また管理運用システムで外部委託業者などについて考えられていなかったため，管理者側の権限付けが細かく設定できず，見せる情報を細かくコントロールできなかった．このため何を設定しなくてはいけないかについても大学側で抜き出して電子メールなどで依頼を行っていた．

他方で2016年にシステムの運用を変更するのにあたって新たに考慮すべき点がある．

第一にアカウント名と個人管理番号の紐付けの変更がある．これまでアカウント名は個人管理番号（学籍番号や職員番号）に基づき生成したものを利用していたが，ランダムに生成したアカウント名を配布する．学籍番号などは連番であるため，これに基づいて生成されたこれまでのアカウント名は推測される可能性が非常に高かった．また学生が転学科などした場合には学籍番号が変わるため，同一学生であるにもかかわらずアカウント名も変わってしまっていた.職員番号もある番号と紐付いて生成されているため，外部に漏れてしまうのは問題であった．したがって外部のシステムをこのアカウントを使って利用することは難しかった．

第二にアカウントの共用を無くす事を考えていたため，これに対応させる必要があった．本学ではWebページやメーリングリストなどは複数の人によって共同で管理することが多かった．そのため，Webサーバやメーリングリストのアカウントを発行すると，そのアカウント（同一）で複数人がログインして使用する状態となっていた．同一のアカウントとパスワードを複数人で共用しており，本来ならば誰か管理から抜けた場合にはパスワードを変更しなくてはならないが，全員に対して新しいパスワードを周知することが容易ではないため，パスワードの管理が甘くなることが多かった．またこの場合，何か起こった際に誰がその操作をしたのかを追跡できないという問題もあった．個人ごとにアカウントとパスワードを分けつつ，同じWebページやメーリングリストなどを管理できる仕組みをつくり，それに対応した管理運用システムを用意する必要がある．

第三に管理側の権限分けである．前述のように業務の一部を外部委託することも含め，業務に必要な情報以外は見せたくない．これまでは管理側はほぼすべて同一の権限であったが，システム管理側においても権限を複数設定したい．そのための管理運用システム側の対応が必要である．

3. 新しい管理運用システム「Salut」の機能

前述のような課題を解決するため，2016年2月の教育用電子計算機システム更新の際に新たな管理運用システム「Salut」を構築し，運用を開始した．大学などの通常の企業とは違う構造を柔軟に受け止めるための工夫をしている．

Salutの主な機能を次に述べる．

(1) 利用者向けアカウント管理機能

利用者はSalutにログインし，自分が現在利用可能な状態にあるシステム一覧や申請状況一覧の表示，新規申請を行うことができる（図1）．

Salutのログインは，新しく発行するランダムな各自のアカウント名(2016年のシステムからはTUAT-IDと命名)を配布するために，これまでの学籍番号や職員番号に基づいて生成されたアカウント名

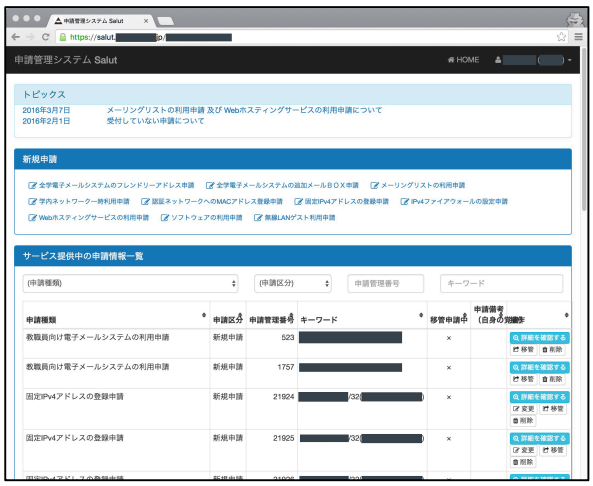

図1 利用者側のログイン後の画面

(SPICA-ID と呼び区別)でもログインが可能である．ログインをするとログイン画面内で TUAT-ID の確認が可能となっている．

利用者の情報を流してもらう上流のシステムはシステムごとに各利用者の名前の入力規則が異なったり，外字を使っていて他のシステムでは利用出来なかったりするため，Salut に初回ログイン時に，各利用者に対して氏名（日本語，英語）それぞれを入力させるようにし，パスワードも初期配布のものから変更させるようにした（入力しないと先へ進めない）．

(2) パスワード再発行機能

Salut にログインし，利用者自身のパスワード変更が可能である．また追加のメール BOX(新規メールアドレス)を申請していた場合には，その追加のメール BOX 用のパスワードを忘れた場合には，Salut から利用者自身がパスワードの再設定が可能である．

TUAT-ID に対するパスワードを利用者が忘れてしまった場合には，管理室でのパスワード再発行となる．パスワード再発行の権限を持つ管理室の担当者が Salut にログインし，学生証または職員証をカードリーダ(初期構築はバーコードリーダを利用)で読み取ると，担当者が指定したレシートプリンタから自動的に新規パスワードが印字されて出力される．この新規パスワードは自動的に他システムにも設定される．特に今回利用した一部のクラウドサービスでは，他のシステム自動連携動作が実行されている場合には時間がかかるため，利用者には 15〜30 分程度で全システムに反映が完了すると伝えている．非常勤講師などで，職員証が発行されていない場合には，本人である事を証明できる ID カードなどを提示してもらった上で，管理室担当者が Salut システムにアカウント名を入力し，新規パスワードを発行する．

管理室担当者が Salut システムにログインしなければ操作ができないため，誰が誰のパスワードの再発行をしたのかを追跡できる．

(3) システム利用申請機能

利用者は Salut にログインし，各種システムの利用申請が可能である．ライセンスの制限などにより申請できない場合には，申請項目自体が利用者からは見えないようになっている．

主な申請や設定項目は下記の通りである

(a) フレンドリ(エイリアス)アドレス申請
(b) 追加メール BOX(メールアドレス)申請
(c) メーリングリストの利用申請
(d) Web ホスティングサービス利用申請
(e) 認証ネットワークへの MAC アドレス登録申請
(f) 固定 IPv4 アドレス借用申請
(g) IPv4 ファイアウォール設定申請
(h) ソフトウェア利用申請
(i) 学内ネットワーク等一時利用申請
(j) 個人設定

TUAT-ID が発行されると，それに基づき Office365 と Google のそれぞれ Education 向けサービスが利用出来るようにアカウント(それぞれのメールアドレス)を自動的に付与している．しかし，ランダムに発行されたアカウント名をベースにしているため，名前やニックネームなどで電子メールを使いたい場合にはこのままでは利用できない．そこで(a)の申請により，フレンドリアドレスをその自動的に付与されたメールアドレスに紐付けて，同じメール BOX で受信できるようにしている．また (b)は追加で別途メール BOX(アドレス)を申請したい場合に利用する．

メーリングリストや Web ホスティングサービスで申請する内容は，システム上の ID の発行と管理する利用者の TUAT-ID の登録などである．実際にサービスが利用出来るようになると，利用者は各自の TUAT-ID でログインし，操作するシステム上の ID を選択し，それぞれのサービスの設定やコンテンツ入力を行う．これにより共同で管理するものであっても共通のパスワードを利用することなく，各自のパスワードで操作できるため，どの利用者が操作したのかを追跡できる．

キャンパスネットワークは認証システムを導入しており，ログインしなければ利用はできない．しかしながらサーバや分析機器などの専用機で，利用者がネットワークへのログイン操作ができない場合には，(e)，(f)などの申請を行い，検疫，認証を回避する．なお，(f)の申請には(e)で機器の MAC が登録されている必要があり，そのエラー判定処理などもしている．また TUAT-ID が発行されていない人がキャンパスネットワークや仮想端末室[5][6]を利用する際には，申請資格のある利用者が(i)の申請をして一時利用のためのアカウントを取得する．

サイトライセンスなどで保有しているソフトウェアの一部の配布管理をこのシステムから行っており，(h)の申請でソフトウェアも種類と利用する機器情報を登録する．登録が終わるとソフトウェア本体の取得，設定方法が書かれたページへのリンクなどがあらわれるようになっている．現時点では，ウィルス対策ソフトウェア，Microsoft Office の配布が行われている．

VPN，PPP，eduroam，学認サービスについては TUAT-ID 発行時に既に利用可能としているが，これまでの運用でも長期間使用する予定はないので止めておいて欲しいとの要望が何件かあったため，(j)の個人設定の項目からサービスの利用と一時休止がで

Vol.2016-IOT-35 No.3
Vol.2016-SPT-20 No.3
2016/9/23

図 2 個人設定項目ページ

きるようにした（図 2）．名前の変更などもここからできる．

(4) 利用者情報連携によるアカウント自動生成機能

一般企業などでは人事システムと連携し，全従業員へアカウントを配布可能であろうが，本学をはじめとする多くの大学では，前述のように 1 箇所で全員を把握できているわけではない．したがって複数の人物を管理しているシステムと連携し，名寄せをしてアカウントを生成する必要がある．本学の場合は，教職員は人事給与システム，学生は学務システムで把握されてはいるが全員ではない．実際にはこれに加えて派遣職員，業務委託をはじめとする大学とは直接雇用ではない非常勤職員，研究員，連携の大学院の学生（正式には他大学所属），名誉教授など様々な人が大学の何らかの情報システムを使うためにアカウントを欲している．しかしながらこれらは個々のデータベースや Excel などで管理されているだけで，連携されてはいなかった．事務の業務フローのヒアリングを行い，できるかぎり学籍番号または職員番号に準じた番号を付番してもらうようにした．しかしながら，人事給与システムや学務システムには入力してはもらえないため，これらを Salut に CSV で一括入力するためのインタフェースを作成した．付番されない人に対しては，前述の「学内ネットワーク等一時利用申請」により申請されたものを利用してもらう．

また人事給与システムと学務システムからは直接連携をしたかったが，それらのシステム管理担当者から難色を示されたため，一つシステムをはさむ形で人物のデータを 1 日 1 回 Salut へ自動的に流している．ひとつはさまれたシステムにより，データの有効期限などが抜けてしまっており，人物データの有効期限（卒業や退職予定日など）を何日か前に検出し，図書館システムなどへ連携することが，機能としては持っているが，現時点では実現できない．このため図書館システムなどで図書返却をうながす業務ができないでいる．

本学では学生証や職員証は IC カードである．しかしながら，この IC カード内のデータは，IC カード発行機内に蓄積されていただけであった．これを CSV 形式で出力し，Salut の CSV 入力インタフェースから手動で投入する．投入されたデータと他で入力されたデータを学籍番号や職員番号をもとに名寄せを自動的に行い Salut 内に格納する．この IC カードのデータはオンデマンド複合機のログインや入退館，教室の空調・AV 機器操作パネルなどに使用される．

Salut へ入力された人のデータに基づき TUAT-ID が自動で生成される．TUAT-ID は教職員系と学生系で異なった生成方法でランダムに生成されるが，どちらも内部にチェックデジットが入っており，TUAT-ID の間違いを検出できるようにしている．

(5) 実システムへの反映を自動化する機能

前述の「利用者情報連携によるアカウント自動生成機能」によって TUAT-ID が生成されると，その利用者にデフォルトで許可されたシステムに対してアカウントを作成すると共に，認証に使用する LDAP や AD への登録を行う．デフォルトでの設定の他，TUAT-ID 個別に各システムの利用可否を設定することができるようになっている．

また利用者によってシステムの利用や変更，廃止申請が行われると，特にセキュリティやリソースの消費に問題が無いものは，定期的に実システムへ自動的に反映する．IPv4 固定アドレスの払い出しや Web ホスティングなどに関しては管理室側で申請内容を Salut 上で一度確認し，承認処理をすると（図 3）自動的に実システムへ反映される．

しかしながらファイアウォールの設定に関しては，ルール設定の順番によって挙動がかわるため，ファイアウォールの機器側の設定を自動化することが難しく，機器への反映は手動となっている．この場合は，Salut 上で作業すべき内容が提示されるので，それにしたがって作業し，実システムへの変更作業が終了したら作業完了を Salut 上で行う形となる．

また Salut 内の利用者情報にて無効となった（卒業や退職などで在籍しなくなった）場合には，当該利用者が利用，申請していたシステム上のアカウントを廃止する処理を自動的に行う．

図 3 管理者側申請確認・承認画面

(6) システム管理作業者向け機能

Salut 内の申請情報の検索や，アカウント情報の検索，設定変更ができる．利用者が申請できない時に，代理で申請を行うことも可能となっている．

前述各機能内で既に触れたが，CSV ファイルによる利用者情報の一括アップロードなどや，申請内容の承認処理，パスワード忘れに対する新規パスワード発行処理などが管理者にて行える．それぞれの機能は，各管理者に対して 1 つずつ操作権限を付与する形であるため，パスワード変更しか行えない担当者をつくることなどが可能である．

またこれまでのシステムでは管理者が各システムへの反映を行っていたが，これからは多くで業者等への作業委託などが増えてくることが予想される．このため管理者と利用者の間に作業者という位置づけを設けた．この作業者は，自分が作業するために必要なシステムに対し，その申請内容だけを検索でき，作業内容の追加や作業の完了報告が可能である．この機能を Salut に新たに構築した．

(7) 利用申請の棚卸機能

利用者は多くのシステムの利用を行うが，課金などがされていなければ，実際に利用しなくなっても廃止処理を行わない傾向にある．これはこれまでの運用で経験してきたことである．したがってこれまでも年に 1 度システムの利用調査を行ってきた．継続利用の意思表示が無いアカウントに関しては廃止処理を行っていた．最初は各利用者に，それぞれの利用しているシステムをアカウント名が印字された紙を送付し，回答を求めていたが，2006 年からは電子的に回答してもらうようにした．しかしながら内容は電子メールで各利用者に送られるだけであり，さらに 1 度に全部を回答しなくてはならない状態で，利用者にとっては不便であった．

また管理側でも一度に全システムの利用調査を行っても，管理側で回答に基づいてシステム側を操作するのは労力を要した．そこでこの Salut では，システムごとに利用申請を行える仕組みを設け，利用者に Salut にログインしてもらいシステムの利用継続調査に回答してもらう形とした．利用調査期間内であれば，何度でも回答が可能であるため，継続するか判断に迷った場合には熟考してから回答してもらうことが可能である．また同じページから後述する移管手続き等も行えるようになっている．

4. Salut のシステムアカウント管理の工夫

Salut では申請情報やシステムアカウント名などを 2 段階（申請情報と台帳）で保持している（図 4）．利用者から申請が行われると，台帳と申請情報を検索し，重複が無いかなどを確認し，申請情報に申請内容を登録する．実システムへ反映が済むと台帳へ反映が行われる．システム管理側で運用などの面で保持しておきたいものは，一般利用者の申請とは別で管理したいこともあり台帳だけで管理する．

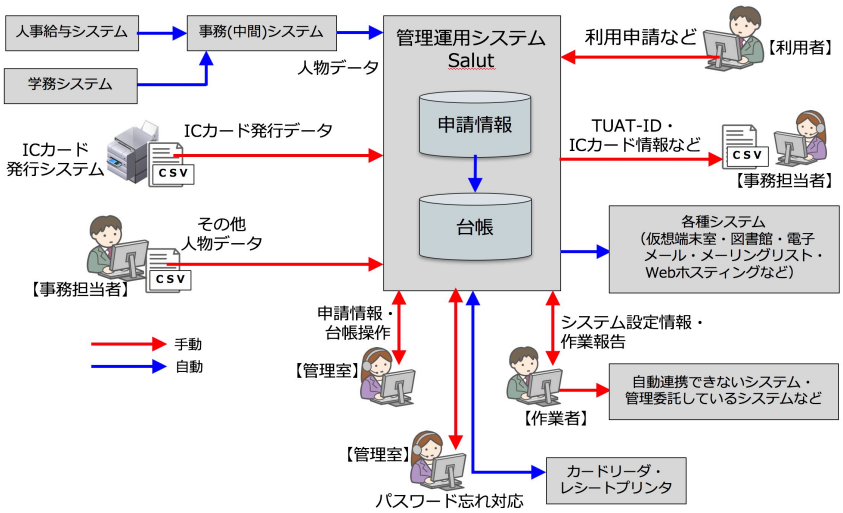

図 4 システム構成・連携図

またあらかじめ予約しておきたい（ユーザに使わせたくないアカウント名，例えば admin や root）なども台帳へ利用不可として登録しておき，申請できないようにする．

退職する人もいることから，申請したシステムアカウントの一部は，Salut 上で他のユーザへ移管できるようにしている．しかし移管される側も勝手に渡されても困るわけなので，利用者が移管手続きをして，移管先の相手が承認しないと実際には移管されないようにしている．

この他に後見人に似た仕組みもこの Salut では取り入れた．この仕組みの多くは名誉教授などの普段学内に来ていない利用者を対象としている．これらの方は学内の連絡が届きにくく，特に申請してから時間が経つと，申請したシステムアカウントの管理をしてもらえないことがある．そこで，その利用者の受け入れ担当者または事務担当者がその利用者に代わって申請内容を管理できるようにした．利用者をその担当者などにして実際には別に利用者がいる方法も考えられるが，この後見人に似た仕組みは，利用者本人があくまでコントロールできるが，その利用者が何もしないときやできない時は代わりにシステムアカウントの申請内容を管理できるものである．これにより少しでも管理されなくなるシステムアカウントを減らしていこうというものである．

5. Salut の構築と運用

教育用電子計算機システムの更新が 2016 年 2 月からとなっていたため，新しいアカウント体系の TUAT-ID を利用者自身に確認してもらうため Salut は 2015 年 12 月から運用を開始した．IPv4 アドレスや個別のシステムのアカウントなどこれまでデータベースにて一応は登録をして管理はしていたが，Salut にデータを移行するにあたり，データの整合性チェックをする必要があった．このため利用者には TUAT-ID の確認をしてもらう作業と並行してこれらの整合性チェックを行い，チェックが終了し Salut にデータの移行が終了したものから申請等ができるようにしていった．この整合性チェックの作業は思いの外時間がかかり，すべてのシステムの申請が Salut からできたのは 2015 年 5 月中旬となってしまった．

また職種などが 4 月から増えたが，事務側から連絡が無くシステム的には不明な職種コードが送付されてきたため，多くのシステムに対してデフォルトで利用出来るように設定できなかったことがあった．コードを連絡してもらい，そのコードが付いた利用者がデフォルトで利用可能なシステムを設定することで解決した．

またバックグランドでシステムに自動的に反映する部分では，多くのシステムでは問題なく動作したが，クラウドサービスである Office365 の設定では反映に時間がかかってしまう事例が発生した．Microsoft 側の問題となるため，本学側では対処できない．そのため，処理の順番を変えてできるだけ影響を受けなくすることしか行えていない．

その他は学内ほぼ全員が利用はしている状態ではあるが，特に大きな問題が起きることもなく，システム全体を含め動作している．

6. おわりに

本稿では利用者情報と各システムのアカウント，IP アドレスなどを一元管理する管理運用システム「Salut」について述べた．このシステムでは利用者が Web の画面を通して自身の利用している状況を確認でき，新たなシステムなどの利用申請も一元的に行うことが可能となった．またシステム連携をし，自動化を進めたことで，管理者による承認が必要ないものなどは利用者へのサービス提供時間も早めることができた．また利用者に代わって受け入れ担当者などが申請内容を管理できる仕組みなどをつくり，大学のような雑多な環境においてもアカウント管理ができるようにした．

今回構築し，運用している Salut は人事給与システムや学務システムなどと直接連携ができていないため，情報が欠落した状態で連携が行われている．今後はこれを直接連携できるようにすることで，卒業や退職予定の利用者に対して事前にアカウント終了予定のアナウンスを行ったり，図書館システム側と連携して図書返却の連絡をしたりすることができるよう，事務部門との連携やシステムの改修を行っていきたい．

謝辞 本システムの構築，運用開始にあたり大森浩氏をはじめとする株式会社 SRA 東北の方々，2016 年の電子計算機システムの構築業者であるユニアデックス株式会社の方々に協力いただいた．ここに謹んで感謝の意を表する．

参考文献

[1] 萩原洋一, 佐藤克巳, 飯田卓郎: 大規模分散システムの設計と実現(1) -- システムと利用者管理データベース, 学術情報処理研究集会, ISSN 1343-2915, No.1, pp.76-84 (1997).
[2] 櫻田武嗣, 石橋みゆき, 萩原洋一: 休眠アカウント調査のための Web を利用した情報サービス利用者確認システムの構築と運用, インターネットと運用技術シンポジウム 2008 論文集 (第 1 回), IOTS2008, vol.2008, No.13, 一般社団法人情報処理学会, issn 1344-0640, pp.31-38 (2008.12).
[3] 徐浩源, 大山清, 志村俊也: IP アドレス管理システムの開発と運用, 学術情報処理研究集会, No.8, pp.79-82 (2004).
[4] 井町智彦, 車古正樹, 松平拓也, 西川直樹: ネットワーク管理業務におけるデータベース活用, 学術情報処理研究,No.8, pp.93-98 (2004).
[5] 三島和宏, 櫻田武嗣, 萩原洋一: 東京農工大学の BYOD 化とこれに対応した新入学生教育の実施 , 研究報告インターネットと運用技術 (IOT), vol.2016-IOT-34, No.7, 一般社団法人情報処理学会, issn 0913-5685, pp.1-6(2016.6).
[6] 三島和宏, 櫻田武嗣, 鈴木創士, 門脇多人, 萩原洋一: 多様な BYOD 機器を考慮した次世代型仮想デスクトップ (DaaS) サービスの共創, 情報処理学会デジタルプラクティス, vol.7, No.2, 情報処理学会, issn 2188-4390, pp.136-147 (2016.4).