

教育用計算機ユーザ管理システムの改善と運用評価

安部 達巳, 田中 哲朗, 関谷 貴之, 丸山 一貴, 前田 光教, 有賀 浩

東京大学 情報基盤センター

{abe,tanaka,sekiya,kazutaka,maeda,aruga}@ecc.u-tokyo.ac.jp

概要：東京大学情報基盤センターの教育用計算機システムには 40,000 人規模のユーザが登録されており、ユーザ情報を教育用計算機システムおよび関連の各種サービスの認証に用いている。ユーザ情報の管理コストは看過できないものであり、2012 年 3 月の教育用計算機システムの更新に併せてユーザ管理システムの改善を行った。本稿では、ユーザ管理システム改善におけるシステム構築および導入後の運用について報告する。

1 背景

東京大学情報基盤センター（以下センター）は、本学学生と教職員の教育および研究における情報アクセスの基盤となる環境として、教育用計算機システム（ECCS, Educational Campuswide Computing System）を運用している。ECCS は約 1,300 台の端末システムやメールシステム等のサブシステムで構成され、ECCS のユーザ管理システムはこれらの ECCS 内のサブシステムおよび以下のサービスにユーザ認証情報を提供している。

- 携帯端末接続環境（有線、無線 LAN）
- 学習管理システム CFIVE†
- SSL-VPN（学外ネットワークアクセス）
- 学務システム

ECCS のユーザ登録数は年間最大‡で学生約 31,000、教職員約 4,000 であり、毎年約 5,000 ユーザを卒業等により削除し、ほぼ同数のユーザを入学等により新規登録している。また、継続する約 25,000 ユーザについては毎年度初頭に継続作業を行っている。ユーザ情報の管理はセンターが内製したデータベースとツール群で行っており、作業量の多さと共に相応のスキルが求められ、管理コストは看過できないものであった。

このような背景の下で、本センターでは 2012 年 3 月に ECCS の更新（ECCS2012[1]）を行い、同時にユーザ管理システムの改善を行った。本稿ではユーザ管理システム改善におけるシステム構築および導入後の運用について報告する。

† <http://cfive.itc.u-tokyo.ac.jp>

‡ 卒業等による削除対象ユーザの情報は管理上すぐには削除せず、約 1 年間保持している。

2 ユーザ管理システム構築

2.1 ECCS2012 以前のシステム構成

従来の ECCS のユーザ管理システムおよび関連するサブシステムの構成を図 1 に示す。

- a. 学務システム
- b. ユーザ管理サーバ（CentOS）
- c. ECCS 認証サーバ（LDAP / Active Directory）
- d. ECCS メールサーバ
- e. IC カード通知書発行システム[2]
- f. 認証を用いた各種サービス

ユーザ管理サーバは学務システムから学生の在籍情報を取得（a→b）し、教職員の情報は手入力によりユーザ情報を登録、保持している。ユーザ情報はユーザ管理サーバから認証サーバ、メールサーバ、IC カード通知書発行システムに提供され（b→c、b→d、b→e）、認証情報は認証サーバから各種サービスに提供されている（c→f）。

各種システムおよびサービスは基本的に商用の製品を用いて構築されているが、ユーザ管理システムは内製であり、Linux をベースとしてデータベース等のシステムやツール群が実装されている。新規利用者のユーザ登録作業も Linux の CUI から登録ツールを実行する必要があるため、作業手順については文書化されていたが、Linux の CUI の基本操作について熟知していることが前提であった。ゆえに、普段 Windows で作業している事務担当者には敷居が高く、利用者登録作業に関するトラブルが発生して、結果的に技術担当者が登録作業の多くを担当する傾向にあった。

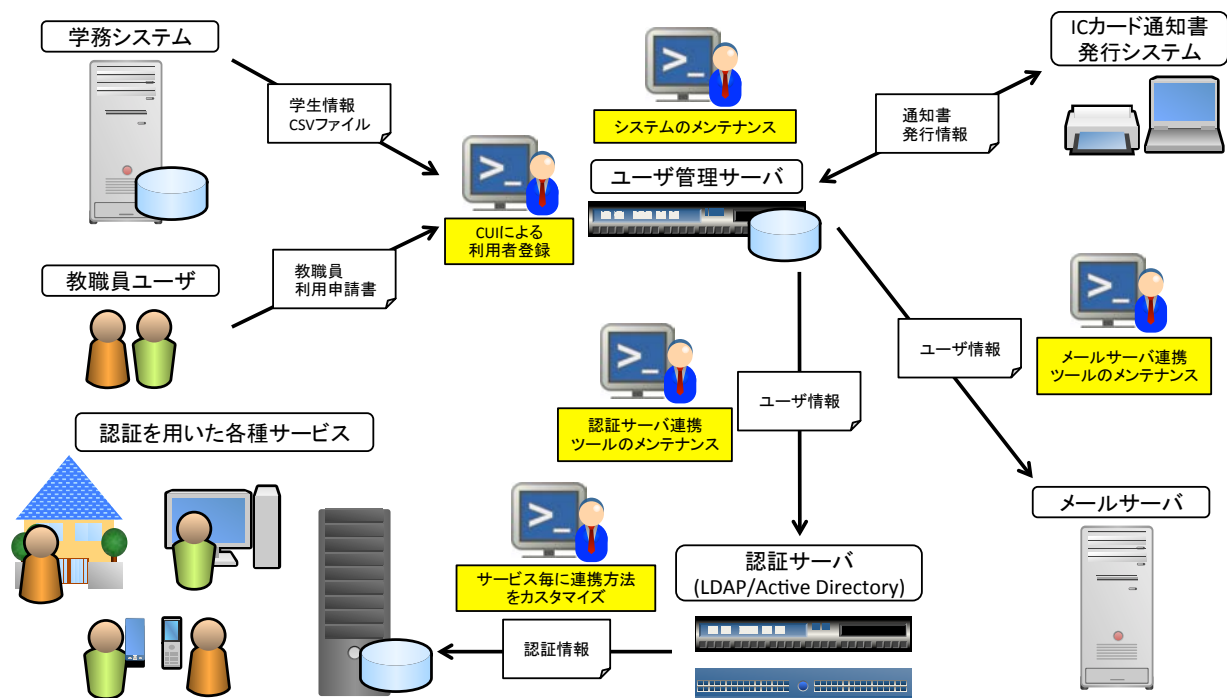


図 1 ECCS2012 以前のユーザ管理システム構成

また、ユーザ管理システムの構成や利用手順については、設計書や手順書として文書化していた。しかし、ユーザ情報を他のシステムに提供する連携ツールを技術担当者が改良した際に、変更されたシステムの構成や利用方法に関して、元の文書を更新し忘れることが稀にあった。その担当者が異動したことでメンテナンスのノウハウが失われて予想外のトラブルが発生し、業務が遅延することがあった。

2.2 ユーザ管理システムの要件の検討

前節より、ユーザ管理システムの課題は以下のものがあつた。

1. システム管理体制の強化
2. 利用者管理関連作業の効率化

1.についてはユーザ管理システムを今後もセンターの完全な内製で維持を続けていくことはコストおよびリスクが高いとの判断より、完全な内製を止めて調達対象の ECCS の一部としてユーザ管理システムを位置づけ、ECCS と同水準の管理体制とするべく、仕様書にユーザ管理システムの要件を加えた。

2.については事務担当者でも容易にユーザ登録作業が可能な GUI の管理ツールの機能を要件に

加えることとした。

また、ユーザ管理システムの要件の検討に際して、前節で述べた課題の他にも以下の課題が挙げられ、検討を行った。

3. 継続手続き作業の省力化
4. 各種システムとの連携機能強化

3.については利用資格を失効したアカウントの停止作業を、各サブシステムで連携して動作可能にするような機能を要件に加えることとした。

また、同一のパスワードが長期に亘って利用されたり、休眠アカウントが放置されたりすることを防ぐセキュリティ上の観点で、パスワードを毎年センターが付け替える処理をしていた。このために、学生約 22,000 人、教職員約 3,000 人の継続手続きを毎年行っており、特に学生の継続手続き作業は窓口で本人に直接手渡ししていたため、相当量の業務負荷があり、こちらも省力化が望まれていた。

4.については各種サービスとの連携について、部局（学部、研究科）の利用者に限定したユーザ情報、認証情報を提供してもらいたい、という要望が複数あり、要望毎に提供方法をカスタマイズして提供していた。これに対し、カスタマイズすることなく、個別に任意のユーザ情報、認証情報を提供する機能を要件に加えることとした。

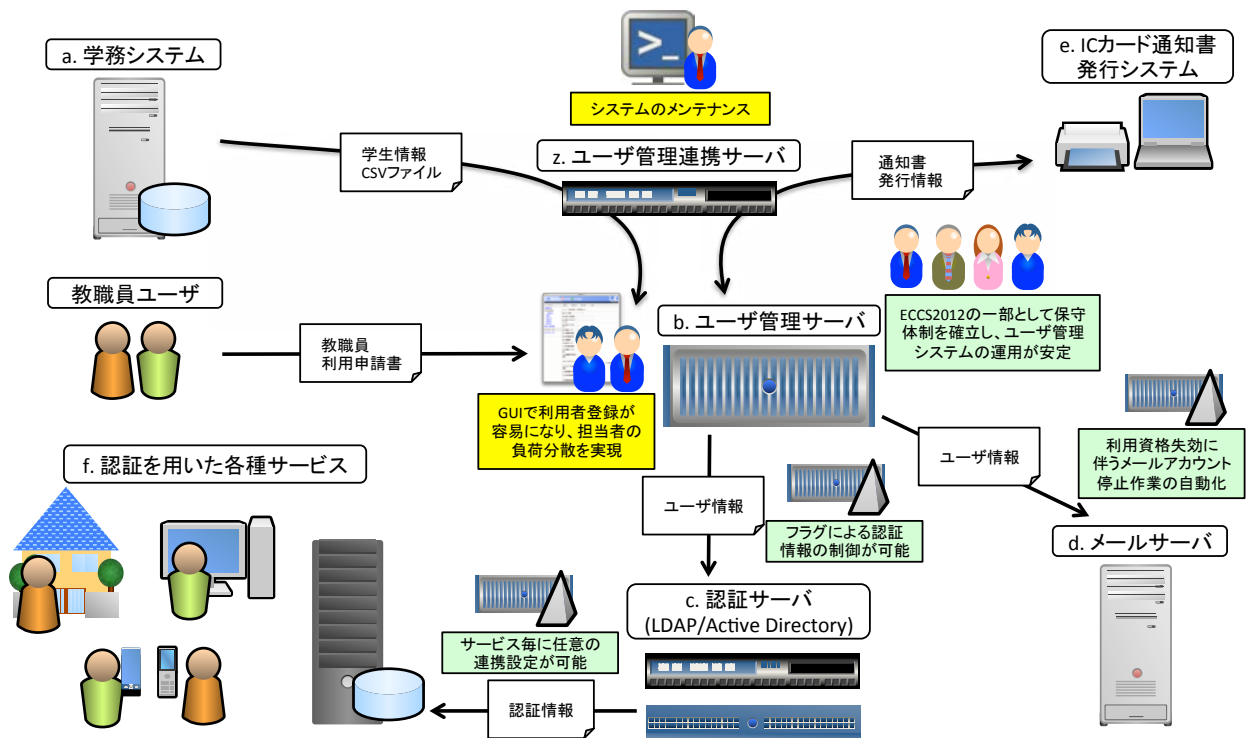


図 2 ECCS2012 のユーザ管理システム構成

4.についてはもう一点、各種システムおよびサービスのシングルサインオン機能（以下 SSO）を要件に加えることとした。

このように、ユーザ管理システムの構築に必要なと考えられる最小限の機能要件を ECCS2012 の仕様書に盛り込んだ。次節では ECCS2012 導入後のユーザ管理システム構成について報告する。

2.3 ECCS2012 のシステム構成

ECCS2012 のユーザ管理システム構成を図 2 に示す。図 2 の黄色のコメントはセンター担当者の業務として残った作業を、緑色のコメントはシステム更新により改善された作業を示している。

- a. 学務システム
- b. ユーザ管理サーバ（WebSAM SECUREMASTER[†]）
- c. ECCS 認証サーバ（LDAP / Active Directory）
- d. ECCS メールサーバ
- e. IC カード通知書発行システム
- f. 認証を用いた各種サービス
- z. ユーザ管理連携サーバ（CentOS）

最大の変更点はユーザ管理サーバを WebSAM

[†] <http://www.nec.co.jp/middle/WebSAM/products/secmaster/>

SECUREMASTER に入れ替えた (b) ことである。

前システムで稼働していた Linux サーバは学務システムおよび IC カード通知書発行システムとの連携を行うユーザ管理連携サーバとして残している (z) が、これは学務システムおよび IC カード通知書発行システムが ECCS2012 とは完全に独立したシステムであり、これらの修正は見送ったためである。

よって、前システムからの構成上の変更点は、学務システムから学生の在籍情報を取得する点 (a → z → b) とユーザ情報をユーザ管理サーバから IC カード通知書発行システムに提供する点 (b → z → e) である。また、ユーザ管理サーバから ECCS 認証サーバ、ECCS メールサーバにユーザ情報を提供する点 (b → c、b → d) は構成上の変更は無いが、連携するプログラム、ツール群は内製のものから WebSAM SECUREMASTER が提供するものに刷新した。

3 ユーザ管理システム更新後の運用

2.2 節では以下の課題が挙げられ、ユーザ管理システムの要件の検討を行った。

1. 利用者管理関連作業の効率化
2. システム管理体制の強化、安定化
3. 継続手続き作業の省力化

4. 各種システムとの連携機能強化

本章ではユーザ管理システムの更新によってこれらの課題がどのように改善されたかを報告する。

3.1 利用者管理関連作業の効率化

GUI 管理ツール（図 3）の導入により、CUI を意識することなく、利用者登録作業が容易になった。これより、技術担当者に集中していた年間約 5,000 件の利用者登録作業が事務担当者にも負荷分散され、作業の効率化とともに、技術担当者が不在の時にも利用者登録作業が滞りなく進められるようになった。



図 3 GUI 管理ツール

なお、ユーザ管理サーバは CUI の機能も有しており、CSV 形式のファイルを読み込ませることで一括登録、削除を実現しているため、GUI の不得手な部分も補っている。

3.2 システム管理体制の強化、安定化

WebSAM SECUREMASTER が各種システム、サービスと連携を行うようになり、仕様書に基づき保守体制が確立された。これよりユーザ管理サーバ自身および連携部分の障害時の対応が強化され、技術担当者に依存していたメンテナンスも無くなり安定した運用が可能となった。

また、有償ではあるが、機能拡張についてのサポートもあり、今後の機能改善についての案件が円滑に進められることが期待される。

3.3 継続手続き作業の省力化

今回のユーザ管理システムでは、アカウントおよびパスワードに有効期限を設けた。

従来は利用資格を失効したアカウントに対して、ECCS の各サブシステムやサービス毎にアカウントの利用停止措置を手動で実行していた。ECCS2012ではアカウント毎に設定した有効期限に基づくサブシステムの連携機能を実装し、利用資格を失効したアカウントの利用停止措置を自動化でき、アカウント停止作業の労力を大幅に削減できた。

パスワードに有効期限を設け、有効期限に達すると認証が通らなくなるようにした。これによって、従来と同レベルのセキュリティを保ちつつ、センターがパスワードを付け替えて新しいパスワードを利用者に通知するという多大な手間がかかる継続手続き作業を廃止できた。

3.4 各種システムとの連携機能強化

以前のユーザ管理システムでは、部局（学部、研究科）の利用者に限定したユーザ情報、認証情報を提供してもらいたい、という要望がある毎にシステムをカスタマイズして提供していたが、今回のユーザ管理システムでは独自の連携用フラグを設定し、フラグ毎に任意のユーザ情報、認証情報を提供できるようになり、柔軟性の高いサービス連携が容易に提供可能となった。

連携機能強化としてもう一点、SSO の実装を行った。SSOは現在、以下のシステムで連携しており、いずれかのシステムを利用（ログイン）することにより、他のシステムもユーザ名およびパスワードの入力無しに利用が可能[†]となっている。

- ECCS 端末 (Mac, Windows)
- ECCS 端末利用状況確認システム
- ECCS メールシステム
- 学習管理システム CFIVE

4 今後の課題

GUI 管理ツールの導入により利用者登録作業が容易になったことは 3.1 節で述べた通りである

[†] 2012年11月時点では学内ネットワークからのアクセスのみ利用可能となっている。

が、GUI管理ツールではユーザ名の変更（および連携システム、サービスへの変更反映）、属性値の変更といった機能も用意されており、今後はこれらの機能も有効活用し、利用者管理の一層の効率化を図りたい。

学生の継続手続き作業は大幅に改善、省力化されたが、教職員 3,000 ユーザに対する継続手続き作業は従来通り実施している。教職員については、学生の学務システムのような在籍情報を管理しているシステムと連携しておらず、個別に在籍を確認する必要があるためである。今後、教職員についても在籍情報を管理しているシステムとの連携を検討し、業務の省力化を進めていきたい。

SSO は現時点では ECCS 内の一部のシステムとの連携に留まっている。外部連携しているサービスを含め、今後も連携を広げ、同時に特定の利用者に限定したサービスとの連携も検討したい。

5 まとめ

従来のユーザ管理システムはセンターの内製で構築されており、システム管理体制に不安があった。ここで、完全な内製を止め、ECCS2012の一部としてユーザ管理システムの要件を検討し、更新を行った。ECCSの一部としてシステム管理体制が強化されたと共に、GUI管理ツールによる利用者管理作業の効率化、アカウント有効期限によるアカウント停止作業の自動化、パスワード有効期限による継続手続き作業の廃止、という業務の省力化を達成することができた。

また、新システムの機能を利用することにより、従来よりも柔軟性の高いサービス連携が提供可能となり、運用においても一層の省力化が期待される。新システムの機能の活用に関しては改善の余地があり、引き続き運用の省力化、システムおよびサービス連携の強化を進め、今後も報告していきたい。

参考文献

- [1] 丸山 一貴、関谷 貴之「教育用計算機システム ECCS2012 の構成」、大学 ICT 推進協議会 2012 年度年次大会、掲載決定
- [2] 宮寄 洋、小川 大典、「IC カードを使用したパスワード通知書発行システム」、平成 18 年度 情報教育研究集会 講演論文集、522-525 ページ、2006