

# 統合認証システムの導入と IC カード番号登録システムの開発

高橋 佳大<sup>1)</sup>, 名取 勝敏<sup>1)</sup>, 小野垣 仁<sup>1)</sup>, 唐崎 幸弘<sup>1)</sup>, 馬場 健一<sup>2)</sup>

1) 工学院大学 情報システム部

2) 工学院大学 情報科学研究教育センター

yoshihiro@cc.kogakuin.ac.jp

## Introduction of the Integrated Authentication System and Development of the IDm Registration System.

Yoshihiro Takahashi<sup>1)</sup>, Katsutoshi Natori<sup>1)</sup>, Hitoshi Onogaki<sup>1)</sup>,

Yukihiro Karasaki<sup>1)</sup>, Ken-ichi Baba<sup>2)</sup>

1) Information System Department, Kogakuin University

2) The Center for Information Science, Kogakuin University

### 概要

今まで大学の共同利用コンピュータシステムとして導入していた認証システムは、大学のシステムでを使用することを前提として設計されていたが、システムの更新に合わせて、法人の事務システムや附属中学・高校でも利用可能な学園全体の統合認証システムとして導入をすることにした。

また、貸出用 PC ロッカーや一般教室の AV 装置は、IC カードを使用した認証を採用することとしたため、IC カード番号を認証システムへ登録するシステムの開発を行った。

## 1 はじめに

工学院大学 (以下、本学) の共同利用コンピュータシステムは 3~4 年毎に更新を行っている。大学の教育・研究用システムの一部という導入経緯から、認証システムもその一部として導入してきたため、今までのシステム (旧システム) では、大学の共同利用コンピュータシステム等の認証に限定されていた。そのため、法人が所有する事務システム、各種システムにおいては、大学の教育・研究用の認証システムとは異なり、ID、パスワードを独自に管理しなければならず、管理コストが問題となっていた。そこで 2017 年のシステム更新に合わせて、導入する認証システムの設計をこれまでとは大幅に変更し、法人や附属中高のシステムでも利用可能な学園全体の統合認証システム (新システム) として導入することとした。

また、認証システムの統合化により、各種システムの認証情報を一括管理することができる。本学では、貸出用 PC ロッカーの導入と、新宿キャンパスの一般教室 AV 装置の更新も行い、これらのシステムにおいて学生証・教職員証を用いた IC カード認証を採用することとした。そこで、統合認証システムの連携システムのひとつとして、こ

れら個人の IC カード番号を認証システムへ登録するためのシステムを新たに開発した。

## 2 旧システムの問題点

旧システムは大学の共同利用コンピュータシステムでの運用を前提としていたため、次のような問題があった。

- 管理するユーザは、共同利用コンピュータシステムへのアカウント作成が必須である。
- eduroam 等の特定のシステムのみを利用可能なユーザを作成することができない。
- ポータルシステム等の法人が運用するシステムに対応できない。
- 附属中高で管理するシステムに対応できない。
- 認証システムの連携には運用ネットワークをそのまま使用しており、セキュリティ上の懸念がある。

## 3 新システムの方針・概要

### 3.1 システムの方針

旧システムでの問題点を整理し、新システムを設計する上での方針は次の通りとした。

- 特定のシステムには依存しない設計とする。

- 法人や中高も含めた学園全体のシステムに対応可能とする。
- ユーザ情報をどのシステムに連携するかを自由に選択可能とする。
- 将来的に、管理対象とするシステムの追加を容易とする。
- シングルサインオンを実現するため、SAML に対応した認証システムの基盤を整備する。
- 国立情報学研究所が主導する学認との連携を可能とする。
- 認証システムの連携は、運用ネットワークとは異なる、管理用のネットワークを使用する。

表 1 に新システムの導入時点で管理対象とするシステムを示す。旧システムでも管理対象としていた大学の共同利用コンピュータシステム、eduroam システムに加えて、今回新規で導入をした IC カード認証を行うためのシステムを追加している。また、2017 年 8 月に中高の教育システムの更新も行うことから、中高の教育システムと校務システムを管理対象として追加することとした。

なおシングルサインオンのための SAML 認証システムについては、バックエンドとなる LDAP サーバを今回のシステム更新の導入対象とし、実際に認証連携を行う SP は将来計画にて対応することとした。

表 1 統合認証の対象システム

システム	主な利用者
共同利用コンピュータシステム (大学)	大学 学生 大学 教職員
図書館システム	大学 学生 大学 教職員
研究者情報システム	大学 教員
eduroam システム	大学 学生 大学 教職員
SSO 用 SAML 認証システム	(将来計画用)
IC カード認証システム	大学 学生 大学 教職員
教育システム (中学・高校)	中高 生徒 中高 教職員
校務システム (中学・高校)	中高 教員

### 3.2 システムで保持する情報

表 2 に新システムの内部で保持する情報を示す。

統合認証システムでは、認証・認可に必要なとなる情報のみを保持することとした。個人情報管理している、教職員の人事システムや学生・生徒の学籍システムからは、必要最小限のデータのみを連携することで、認証には必要のない個人情報は保持しない設計となっている。

表 2 システムで保持する情報

個人 ID
パスワード
氏名 (漢字・カナ)
個人番号
教職員番号・学籍番号
IC カード番号
大学共同利用コンピュータシステム 登録情報
・メールアドレス
・ホームディレクトリ容量
・印刷可能枚数
・LMS 役割 (学生・教員)
・AD アカウント情報
・Linux アカウント情報
中高教育システム 登録情報
・個人 ID
・メールアドレス
・AD アカウント情報
中高校務システム 登録情報
・個人 ID
・AD アカウント情報

### 3.3 システムの概要

図 1 に新システム全体の概要を示す。個人情報を管理している人事・学籍システムから、氏名、個人番号、教職員番号・学籍番号の情報を取得している。また、各システムへの認証情報の配信は、利用者が使用する運用ネットワークとは独立した、認証システム連携用の専用ネットワークを使用することで、安全性を高めている。図書館システムや研究者情報システムは、共同利用システムの LDAP サーバを参照する設計となっている。

利用者がパスワードを変更する場合は、情報を保持している管理用サーバとは異なる、利用者用サーバを使用する。

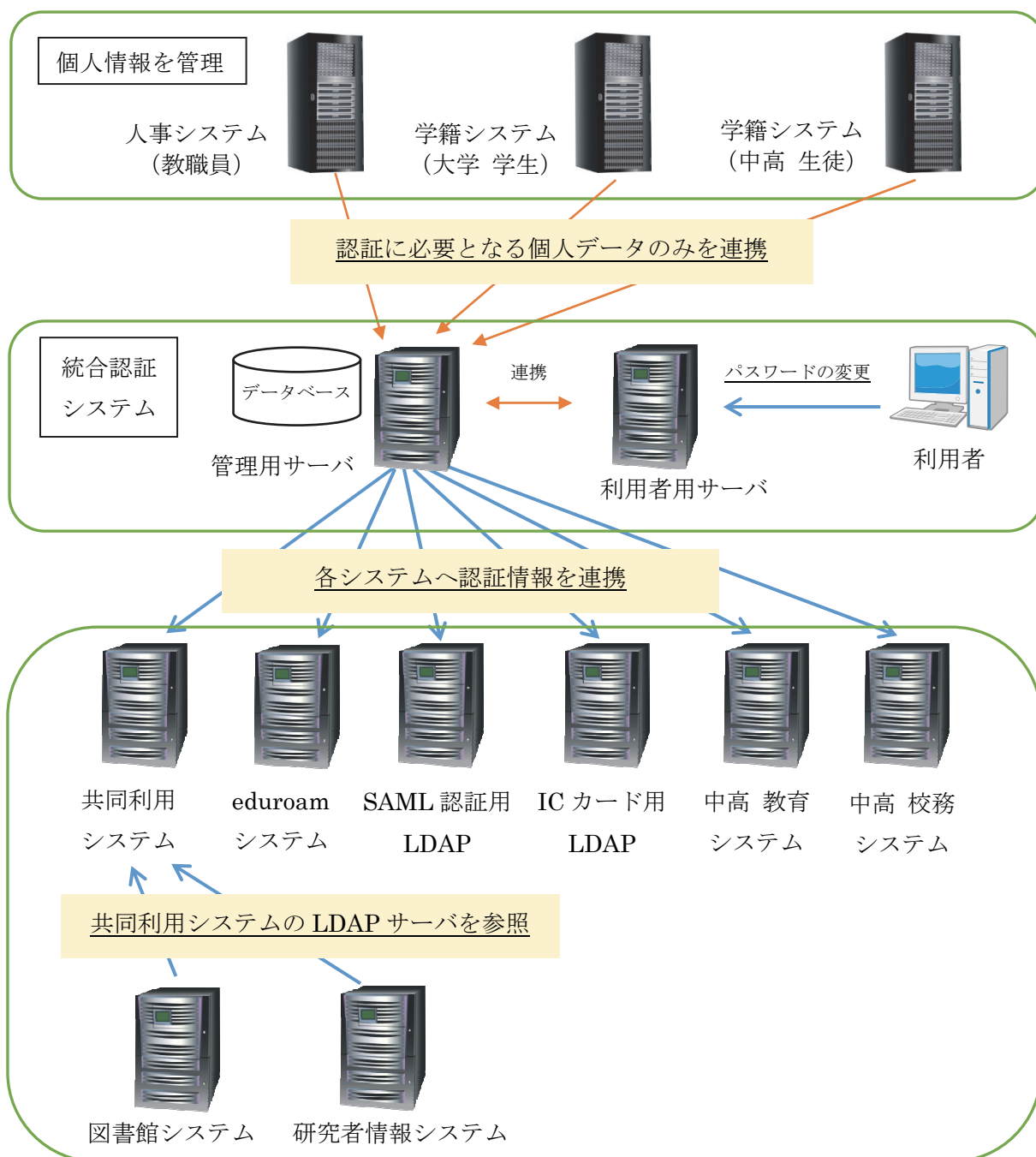


図 1 統合認証システムの概要

## 4 IC カード番号の管理

### 4.1 システム開発の背景

本学の学生の学生証は、2008 年から FCF キャンパス仕様の IC カードを採用し、出席管理等に使われてきた。また教職員証は、2015 年から学生証と同様に FCF キャンパス仕様の IC カードに変更し、八王子キャンパスの一般教室 AV 装置での認証や、新宿キャンパスにおける研究室エリアの入室管理に使われてきた。

しかし今まで IC カード認証を採用してきたシ

ステムでは、それぞれのシステムで独自の方法によって IC カード情報を管理しており、システム導入時の負担となっていた。

今回、新宿キャンパスにて新たに導入する貸出用 PC ロッカーや一般教室 AV 装置における IC カード認証を検討する上で、今までのような個々のシステムでの独自の対応ではなく、新たに構築する統合認証システムにおいて管理できるようにした。そこで、統合認証システムにおいて、学生証・教職員証に記録されている IC カード番号 (IDm) を一元管理できるように設計し、さらに IDm

を統合認証システムへ自動で登録するシステムを新たに開発した。

## 4.2 IDm の登録方法

IDm を統合認証システムへ登録するにあたり、考慮すべき点として、IC カード発行時に必ずしも統合認証システムへのユーザ登録が完了しているとは限らない、外部貸出等の用途にも IC カードを発行しており個人に紐付かないカードがある、という点があげられた。

これらの課題を解決するため、学生証・教職員証の発行から、統合認証システムに IDm を登録するまでの流れを次のように設計した。図 2 に本システムの概要を示す。

1. IC カード発行機にてカードの発行ログを出力し、そのログをネットワークフォルダに保存する。
2. IDm 登録システムにおいて、上記のネットワークフォルダを参照し、新規で発行された IC カードの情報をローカルのデータベースに格納する。
3. 統合認証システムに登録されているユーザの一覧を取得し、上記のデータベースに格納する。
4. IDm 登録システムのローカルデータベースに格納されている、IC カード情報と統合認証システムのユーザ情報から、登録すべき IDm の一覧を抽出する。

5. 抽出した IDm を統合認証システムへ登録する。

これらの処理を行うシステムを新規開発し、プログラムを定期的に自動実行することで、統合認証システムへの IDm の自動登録を実現することができた。

## 4.2 発生した問題

本システム稼働後に、一部の学生より、IC カード認証にて正常に認証ができないという報告が寄せられた。

調査をしてみると、認証でエラーとなる学生は、以前に学生証の再発行をしているが、古い学生証をそのまま継続して使用していることが判明した。

本来であれば再発行後の新しい学生証を使用すべきであるため、この問題は学生証の取り扱いに関する運用の問題と考えられる。

## 5 まとめ

統合認証システムの新システムを導入したことにより、学園全体の認証システムとシングルサインオンのための基盤を整備することができた。

また、学生証・教職員証の IDm を合わせて管理することが可能となり、IC カード管理の厳密化と利用者の利便性向上につなげることができた。

今後はこのシステムを活用し、法人が運用するポータルシステム等の認証統合を進めていきたい。

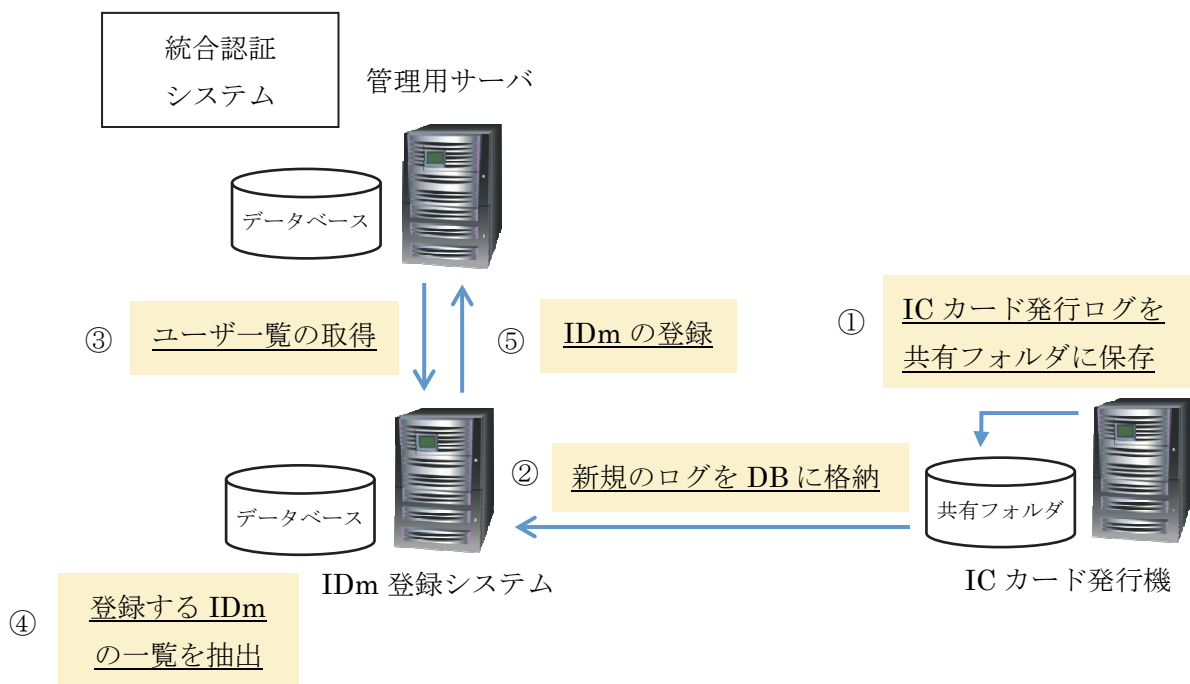


図 2 IDm 登録システムの概要