3G-3

統合認証基盤システム構築に関する一考察

稗田　隆　　河野 圭太　　岡田　俊明　　大隅 淑弘†

国立大学法人 岡山大学　情報統括センター‡

1. はじめに

近年，ICT 利用者の利便性の向上，運用管理コスト等の削減を実現すべく，統合認証基盤システムの構築が進んでいる[1)，2)]。

国立大学法人岡山大学（以下，当大学）においても，生涯に亘って利用可能な岡大 ID を導入し，多数のシステムでのシングルサインオン（Single Sign-On：SSO）の導入や，学術認証フェデレーション（学認：GakuNin）との連携を実現している[3)]。

本稿では，統合認証基盤システムを拡張し，当大学に関係する同窓生，サポータまで含めたすべての関係者を管理可能とする機能拡充を行い，生涯に亘って一元的に認証可能とするシステムを構築したのでその概要について報告する。

２．統合認証基盤システムの概要

当大学の統合認証基盤システムは，統合認証マスタ DB と統合認証管理システムを中心として構築している。

この統合認証基盤システムは，①全構成員に対して統一的に ID を付与（岡大 ID）すること，②岡大 ID の生涯利用を実現すること，③一度の ID・パスワード入力で各種システムを利用できる SSO を実現すること，④学認との連携すること，を実現している。

また，各個人に対して管理すべき属性情報の増加に対応するために拡張性を優先した統合認証マスタＤＢ構成を採用し，マスタＤＢの情報は統合認証管理システムにより管理され，各種システムに提供される。統合認証管理システムでは，ロールに基づく権限管理やワークフローの機能が実装されており，管理者だけでなく利用者自身による属性情報の変更や，各自が直接希望する多様な利用システムの申請ができる。

岡山大学統合認証基盤システムは，全構成員に対して 2010 年 6 月に運用を開始した[4)]。

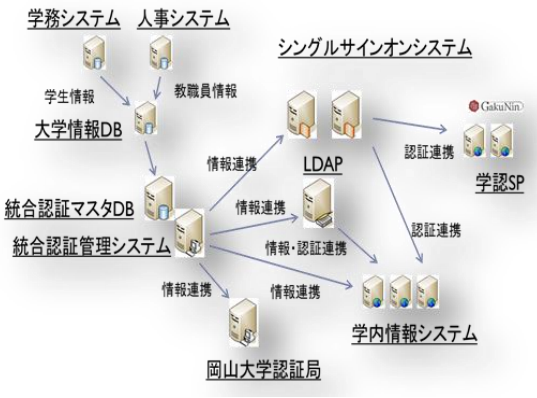

図１　統合認証システムの構成

３．新たな統合認証基盤システムの構築

新たな統合認証基盤システムでは，対象とする関係者の増加への対応を目的に開発する。これまでは，卒業生に対しては，卒業時に生涯に亘って利用可能な生涯メールアドレスを付与していたが，在学時とは異なったアドレスを付与していた。

本年度から入学時，及び採用時で付与するメールアドレスの生涯利用を可能とし，卒業時のメール移行などを不要とし，在学時と同じ岡大 ID による認証サービスを受けることが可能となる。実現のためには，現在すでに１万人を超える現行の卒業生管理システムの巻き取りや岡大 ID を持たない同窓生への対応などが必要になる。

（１）個人情報管理データベースの構築

現在の卒業生，退職教職員情報データベースを，新たに大学情報データベースの一部として構成員情報データベースを構築する。情報を，ID,メールアドレス，システム操作権限属性等の制御系情報と，個人情報に分離して管理し，情報の公開，検索を可能とした。

なお，在校生，卒業生の区別情報は統合認証マスタ DB が管理する。

Consideration about the Integrated Authentication Base System Construction

† Takashi HIEDA, Keita KAWANO, Tosiaki OKADA, and Yoshihiro OOSUMI

‡ Center for Information Technology and Management, Okayama University

（2）構成員情報システムへのログイン・ログアウト機能

岡大 ID を有する場合，Shibboleth 認証を行い，認証後のポータル画面経由でサービスを受ける現行と同一のインタフェースを実現した。しかし，岡大 ID を持たない場合は統合認証管理システムの利用ができないため，今回独自に開発した個別認証画面により ID（独自 ID）,パスワードを用いて構成員情報データベースを利用する。

これに関しては，順次岡大ＩＤへ移行することで二重運用を解消する予定である。

（3）新規対象者の登録

新入学生，新規採用教職員等，新規に岡大 ID を付与された構成員は，大学情報データベースを介在して必要な情報が自動的に連携する。また，個別に岡大 ID を付与した場合も，本連携機能により自動的に情報の整合性が実現される。

（4）個人情報の管理，表示機能

各自が登録した情報は岡大 ID を基本とした URL により表示可能である。既に岡大 ID，パスワードでログインが完了している場合，全ての情報が表示，及び編集可能である。ログインを行っていない場合，セキュリティレベルにより公開設定された情報のみが WEB ページに表示される。これにより，岡大 ID を知る当大学の関係者であれば一定レベルの情報が検索可能である。

なお，情報の公開レベルは，情報登録した各自の公開設定と大学で付与する利用者のアクセス権限レベルにより決定される。

（5）個人情報の検索機能

ログイン後のユーザはアクセス権限に従った情報検索が可能である。特に同窓生間のコミュニケーションを推進するため個人の興味等の設定情報，卒業年度などの任意の項目による検索，簡易な方法でメールの送信や，掲示板による大学とのコミュニケーションを可能としている。

（6）パスワードを忘れた場合の対応

従来は在学生が主な対象でありパスワード忘れに対しては，対面による本人確認により新たなパスワードを発行している。しかし新たな統合認証基盤システムでは利用者が全国に分布し対面でのパスワード再発行は困難である。このため，ストレスのないパスワード再発行サービスを提供する必要がある。今回は，リマインダ機能が有効に利用できない経験を踏まえ，個人の個別メールアドレスの登録と，生年月日，氏名などの個人情報により本人認証を行い，Pin コードをメールで送ることで本人確認する方式を採用した。

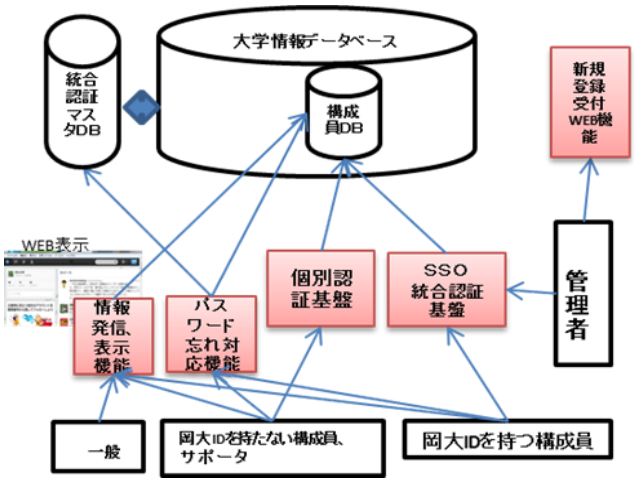

図２　新たな統合認証基盤システムの機能

４．おわりに

新たな統合認証基盤システムは 2013 年 4 月から正式にサービスを開始する予定であり，今後運用面での課題を順次解決していく必要がある。現在想定している課題は，

① 想定するユーザ数は現状の当大学の学生数をベースにした 2 万人前後から，新たなサービスでは 50 万人程度に増加する。これに対するシステム性能面での対応，セキュリティの脅威に対するより強固な対応が求められる。

② パスワード再発行に関しては，スマートフォンを生体情報的に扱い，保持による本人認証や，Google の 2 段階認証等を参考により強固で，便利な手段の採用が求められる。

③ 当大学の同窓生，サポータ間の緊密なコミュニケーション基盤となるためにはより一層の SNS 機能の強化，Facebook 等の既存のサービスとの連携などを含めた拡充が必要になる。

本稿で報告した新たな統合認証基盤システムの運用を通して順次より効率的で，利用者に易しいサービスへと拡張していく予定である。

参考文献

1） 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. 2010;14:31-9.
2） 松平拓也. Shibboleth による金沢大学統合認証基盤の構築と今後の展開. 第 4 回統合認証シンポジウム:2010 年 12 月 22 日;佐賀:佐賀大学;2010.p.33-48.
3） 河野圭太. 岡山大学における統合認証化の取り組みと電子ジャーナルとの連携,医学図書館　2012； 59(3):192-4
4） 河野圭太, 藤原崇起, 大隅淑弘, 岡山聖彦, 山井成良,稗田隆. 岡山大学における生涯 ID を実現する統合テムの構築. 学術情報処理研究. 2011;15:171-5.