岡山大学における生涯 ID を実現する統合認証システムの構築

Construction of Integrated Authentication System to Realize Permanent ID in Okayama University

河野 圭太，藤原 崇起，大隅 淑弘，岡山 聖彦，山井 成良，稗田 隆
Keita KAWANO, Takaoki FUJIWARA, Yoshihiro OOSUMI, Kiyohiko OKAYAMA, Nariyoshi YAMAI, and Takashi HIEDA

keita@cc.okayama-u.ac.jp, fujiwara-t4@adm.okayama-u.ac.jp,
{oosumi, okayama, yamai, hieda-t}@cc.okayama-u.ac.jp

岡山大学情報統括センター
Center for Information Technology and Management, Okayama University

概要

近年, シングルサインオンの実現による利便性の向上と認証機能の一元化による ID 管理コストの削減および安全性の向上を目的として, 各大学において統合認証システムの導入が進んでいる. 岡山大学においても, 従来より，ID 一括管理システムや LDAP を利用して学内情報システムの ID とパスワードの統一を進めてきたが，全ての学生および教職員を包含する ID 体系が存在しないことや，進学の度に ID が変更されてしまうことが課題となっていた．本稿では，全構成員に対する統一的な ID 付与に加えて，付与した ID の生涯利用を実現するシステムとして平成 22 年 6 月より運用を開始した岡山大学統合認証システムの概要について報告する.

キーワード

統合認証，シングルサインオン，生涯 ID，認証一元化

1. はじめに

近年，シングルサインオンの実現による利便性の向上と認証機能の一元化による ID 管理コストの削減および安全性の向上を目的として，各大学において統合認証システムの導入が進んでいる[1]-[4].

統合認証システムの導入により，利用者は，利用するシステムごとに ID とパスワードを使い分けなければならない手間から解放され，一度の ID・パスワード入力で複数のシステムを利用することが可能になる．また，連携システムの管理者は，ID 管理を含む認証機能を統合認証システムに委託することにより，本来の業務である提供サービスの充実に専念できる.

岡山大学においても，従来より，ID 一括管理システムや LDAP を利用して各種情報システムの ID とパスワードの統一を進め，学内における利用者・連携システム管理者双方の ID 管理コスト削減に取り組んできた.

しかしながら，ID の利用に課金をしていた経緯も

あり，情報統括センターが発行する ID(センターID)を保持していない教職員もいたため，センターID のみで各種情報システムの統合認証化を進めることができなかった．その結果，センターID による統合認証を基本としつつも，学務システムの ID による統合認証，教員評価システムの ID による統合認証が同時に運用される状態となっていた．

また，学生に付与する ID は学生番号に基づいて発行されていたため，進学の度に新しい ID が作成され，それに伴いメールアドレスが変更されること，個人データが引き継げないことが課題となっていた．

本稿では，これらの課題を解決するため平成 22 年 6 月より運用を開始した岡山大学統合認証システムの概要について報告する．

2. 要求条件と構築方針

統合認証システムの構築にあたり，以下の要求条件を満足することが求められた．

(1) 全構成員に対する統一的な ID 付与を実現すること．
(2) ID の生涯利用を実現できること．
(3) 既存の運用に与える影響を最小限に抑えること．
(4) 効率的な ID 管理を実現すること．

まず，要求条件(1)および(4)を実現するため，認証情報は学務システムおよび人事システムとの自動連携によりマスタデータベースに集約して生成することを基本とした．また，集約された情報をセルフメンテナンス等により分散的に維持・管理できる管理システムを構築することにより，要求条件(4)の実現を目指した．

さらに，要求条件(1)および(2)を実現するため，ID 体系の見直しを行った．従来の ID 体系では，学生に対しては学生番号に基づく ID を，教職員に対しては希望に基づく任意文字列の ID を発行し，それをメールアドレスとしても利用していた．新しい ID 体系では，学生番号が変更された場合や学生が教職員として採用された場合にも継続して利用できる ID として，ランダムな英数字による ID（システム ID）を生成することとした．

ただし，要求条件(3)を考慮し，利用者がシステムへログインする際に入力する ID（岡大 ID）やメールアドレスとして利用する ID についてはそれぞれ独立に変更可能とし，統合認証システムの運用開始時には従来のセンターID を引き継ぐこととした．

図 1 にシステム ID と岡大 ID の関係をまとめた．

3. システム構成

図 2 にシステム構成を示す．

学務システムおよび人事システムを発生源とする構成員の情報は，大学情報データベースを経由して統合認証マスタデータベースに登録される．マスタデータベース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．

また，電子証明書による認証を実現する岡山大学認証局に加えて，各種情報システムへのシングルサインオンおよび認証機能の一元化を実現するためのシングルサインオンシステムが導入されている．

以下に統合認証管理システム・統合認証マスタデータベースおよびシングルサインオンシステムの詳細を述べる．

3.1. 統合認証管理システム・統合認証マスタデータベース

前述したように，全構成員に対する統一的な ID 付与を効率的に実現するため，学生の情報を保持する学務システムと，教職員の情報を保持する人事システムとの自動連携による ID 発行を実現した．学務システムおよび人事システムに登録された構成員情報は，夜間のデータベース連携により，大学情報データベースを経由して統合認証マスタデータベースに登録される．

名称	用途	割り当てルール	割り当て例
システムID	個人を識別するために付与するID	ランダムな英数字	p12qr345
岡大ID	システムにログインするために利用するID	個人が設定した文字列 (初期値は上記と同じランダムな英数字)	okadai-taro (初期値：p12qr345)

図 1　システム ID と岡大 ID

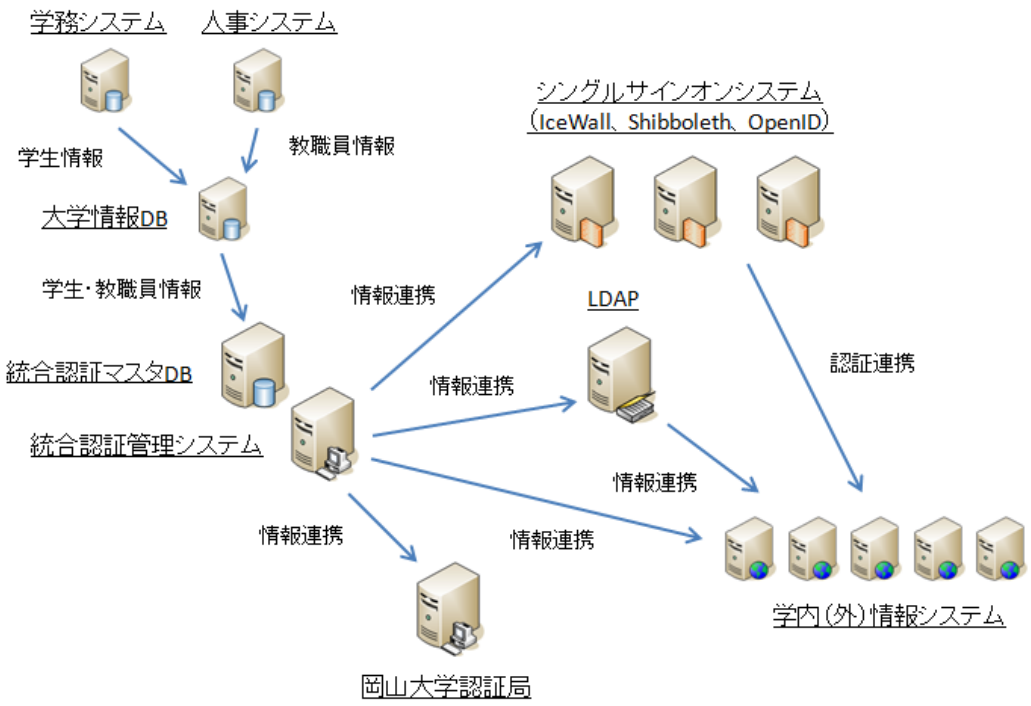

図 2　システム構成

また，統合認証マスタデータベースが保持する利用者の属性情報を管理するための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，利用システムの申請ができるようになっている．さらに，それらの属性情報は CSV 連携もしくは LDAP 連携により各種情報システムに提供することが可能であり，学内における ID 管理コストの削減を実現している．

図 3，図 4 に統合認証管理システムの個人属性変更画面，メール設定変更画面を示す．利用者は岡大 ID で統合認証管理システムにログイン後，権限の範囲内で岡大 ID や所属等の個人属性を変更し，連携システムに反映させることや，メールアドレスのエイリアスを設定すること等が可能である．

3.2.　シングルサインオンシステム

1 章で述べたように，過去に ID の利用に課金をしていた経緯もあり，センターID を保持していない教職員が存在した．正確には，教員については平成 21

図 3　個人属性変更画面

図 4　メール設定変更画面

年度より大学付与メールの運用を開始し，全教員がセンターID・パスワードを保持するようになっていたが，既存のメールアドレスへの転送も許可したため，センターID・パスワードが完全に浸透しているとは言い難い状況であった．

そこで，要求条件(3)を考慮し，シングルサインオンシステムについては既存の認証機能と並行して運用を開始することとし，当面は従来の方法でもシステムが使える状態を継続させることとした．

このため，リバースプロキシ型のシングルサインオン製品である日本 HP 社の IceWall を導入し，運用開始時には，教員評価システム，学務システム（教員向け），Web 購入システム，学内教職員専用ページとの連携を実現させた．

一方で，リバースプロキシ型のシングルサインオン製品には負荷集中の問題があるため，今後統合認証を実現するシステムについては，対応が困難なものを除き，Shibboleth または OpenID による認証連携を進めることとした．特に，現在，国立情報学研究所が主体となって進めている学認において，Shibboleth による組織間での認証連携が成功を収めつつあることもあり，本学においても Shibboleth を中心とした統合認証を進めている．

平成 23 年 7 月現在，30 を超えるシステムが岡大 ID で利用可能になっている．

4.　生涯 ID の実現

前述した ID 体系の見直しにより，学生番号が変更された場合や学生が教職員として採用された場合に ID の再割り当てを実施する必要が排除された．

しかしながら，ID の発行については要求条件(3)，(4)を考慮し，学生番号および個人番号に基づいて学務システムおよび人事システムとの自動連携で実施することとしたため，名寄せの実現が課題となった．

幸い，本学の学務システムでは，システム内部に個人を一意に特定する ID を保持していたため，この ID をキーとして名寄せを実施することにより，進学に伴う ID の引き継ぎ処理を自動化した．

一方で，教職員についても非常勤職員が常勤職員として採用された場合などに個人番号が変更されるが，人事システムには個人を一意に特定する内部 ID が存在しないため，自動での名寄せを断念した．

現在，学生から教職員への身分変更，非常勤職員から常勤職員への身分変更等については本人の申告に基づく手動での ID の引き継ぎを基本としており，システムとしての対応はカナ氏名と誕生日を用いた重複確認による気づきの提供にとどまっている．

このような生涯 ID の実現に伴い，Gmail を利用した学生向けのメールサービスについても，在学期間

中の継続利用が可能になった．ただし，要求条件(3)を考慮し，アドレス付与ルールの変更に伴うメール送信者側の混乱を避けるため，当面は従来の学生番号に基づくメールアドレスも，エイリアスとして持たせることにした．

5. 運用開始後の課題

平成 22 年 6 月の運用開始以降，以下のような課題が発生している．

まず，3.2 節で述べたように，本システムには 3 種類のシングルサインオンシステムが導入されており，相互の認証連携は実施されていない．そのため，シングルサインオンドメインが異なるシステムを利用しようとした場合，再度 ID とパスワードの入力が求められることになり，ネットワークを利用するための認証も含めると，1 日に複数回の ID・パスワード入力が必要になる．

費用の関係もあり，導入時には対応を見送った課題ではあったが，実際に運用を開始すると利用者からの問い合わせも多く，何らかの改善策が必要な状況となっている．

現在，文献[5]を参考に，ネットワーク認証，IceWall 認証，Shibboleth 認証の連携を実現するよう，検討を進めている．

また，前述したように，要求条件(3)，(4)を考慮した結果，岡大 ID は現時点の学生番号または個人番号と 1:1 に紐づくように定義されている．名寄せの実現により，ID の継続利用は可能な状態となっているが，正規生かつ非正規生であるため複数の学生番号を持つ場合や，学生と教職員を兼ねているため学生番号も個人番号も持つ場合には ID を引き継ぐことができず，個人に対して複数の岡大 ID が発行されてしまう．

この問題については，文献[6]のように，個人がログインに利用する ID をいずれかの岡大 ID に統一するような仕掛けの検討が必要であると考えている．

さらに，本システムの導入により，学生にとっては個人が任意に指定するアドレスによるメールサービスの継続利用が可能となったが，メールを受信する教職員にとっては From から学生番号が特定できないことが問題であるとの報告も寄せられている．

この問題については，必要に応じて 4 章で述べた従来のアドレス付与ルールに基づくエイリアスを From としても利用する運用の実現を検討している．

6. まとめ

本稿では，全構成員における統一的な ID 付与に加えて，付与した ID の生涯利用を実現するシステムとして平成 22 年 6 月より運用を開始した岡山大学統合認証システムの概要について報告した．

今後は 5 章で述べた課題の解決に加えて，残課題となっている学務システム（学生向け）や生涯メールとの認証連携を実施する予定である．

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，no.14，pp.31-39，Sept. 2010.

[2] 桝田 秀夫，“Shibboleth を含んだ統合認証システムの導入～京都工芸繊維大学の 2010 年導入事例～，”第 4 回統合認証シンポジウム，pp.15-18，Dec. 2010.

[3] 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，pp.33-48，Dec. 2010.

[4] 松浦 健二，“徳島大学における SSO の実現と課題，”第 4 回統合認証シンポジウム, pp.49-66, Dec. 2010.

[5] 藤村 喬寿，西村 浩二，相原 玲二，“大規模キャンパスネットワークにおける SSO 認証の設計と実装，”電子情報通信学会 IA 研究会技術研究報告，pp.13-18，Nov. 2009.

[6] 江原 康生，村尾 靖子，山口 文雄，“大阪大学における新全学 IT 認証基盤システムの構築と移行，”情報処理学会 IOT 研究会研究報告, pp.1-6, Feb. 2011.