# 名大 ID 認証基盤システム上 Active Directory 連携の現状と課題

○堤守政

共通基盤技術支援室　情報通信技術系

## 概要

名古屋大学でサービスされている、名古屋大学 ID（名大 ID）による認証基盤システムについては、Active Directory（AD）連携の実現方法が一つの課題である。情報連携統括本部では、情報教育基盤システムのレンタル更新を機会に、この AD 連携を、Idsync から IMS(Identity Management System)による方式に切り替えた。

本報告では、Idsync の特徴と問題点、IMS を使った方式概要、今後の認証基盤システムの再構築について論ずる。

## 1　はじめに

名古屋大学では、2013 年秋に情報教育基盤システムがレンタル更新され、同年 10 月 1 日から新システムに移行した。この際、名古屋大学 ID（名大 ID）による認証基盤システムは、Active Directory（AD）連携部分の方式変更を行った。これまでのシステムでは、名大 ID の LDAP サーバ（Sun Java System Directory Server）と AD との間では、Sun の Idsync を用いて連携が行われてきた。今回のシステム更新では、これを廃止し、新たに IMS(Identity Management System)を導入し、かつ名大 ID パスワード変更プログラムの対応を行うことで、同様の機能を実現している。

本報告では、Idsync を用いて AD 連携していた時の特徴と問題点を整理し、今回の IMS を使った方式について概要を説明する。更に、名大 ID 認証基盤システムを今後どのように再構築するかについて、検討材料の提出を試みる。

## 2　旧システム

2013 年 9 月までの名古屋大学 ID 認証基盤システム概要を図-1 に示す。

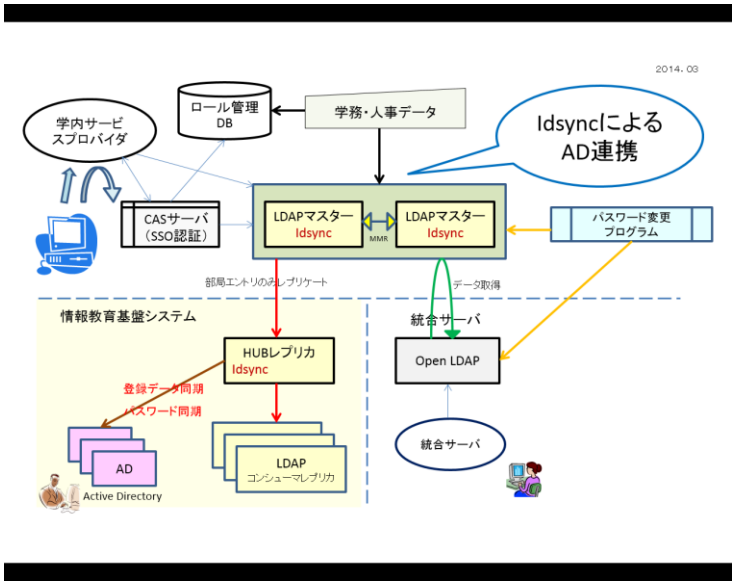


図-1　2013 年 9 月までの名古屋大学 ID 認証基盤システム概要

図-1 の上部では、まず学務・人事データから名大 ID と属性が構成され、LDAP マスターに格納する形態である。これらの認証情報は学内サービスプロバイダから利用される。その際、Web サービスの SSO（シングルサインオン）は、CAS(Central Authentication Service)を利用している。また情報連携統括本部では、CAS でロール認証が行えるシステムを提供している。

図-1 の下部では、LDAP マスターサーバに対する情報教育基盤システム又は統合サーバとの関連を示す。

情報教育基盤システムは情報メディア教育システム、情報文化学部、工学部情報工学コースの各システムで構成される。属性情報は、HUB レプリカを介して、LDAP サーバと AD に対し、名大 ID/パスワード情報が連携される。AD 連携は Idsync を用いて自動的に行われる。しかし LDAP マスターサーバは、Idsync の導入によって AD 側と密結合になってしまった。そのため、情報教育基盤システムのレンタル期間中は、LDAP マスターサーバの更新が困難になるという状況が生じた。

統合サーバは、主に文系学部の Web やメール環境を集約したシステム及び全学メールサービスから構成されている。認証サーバには OpenLDAP が採用された。

その他、図では省略しているが、情報科学研究科で設置している LDAP コンシューマレプリカサーバ（Sun Java System Directory Server）に対しても、部局向けのレプリケーションを実施している。

一方、名大 ID の利用者には、Web インタフェースのパスワード変更サービスを提供している。このプログラムは、LDAP マスター及び OpenLDAP サーバ上のユーザパスワードを一括更新する。【6】

## 3　現システム

2013 年 10 月からの名古屋大学 ID 認証基盤システム概要を図-2 に示す。

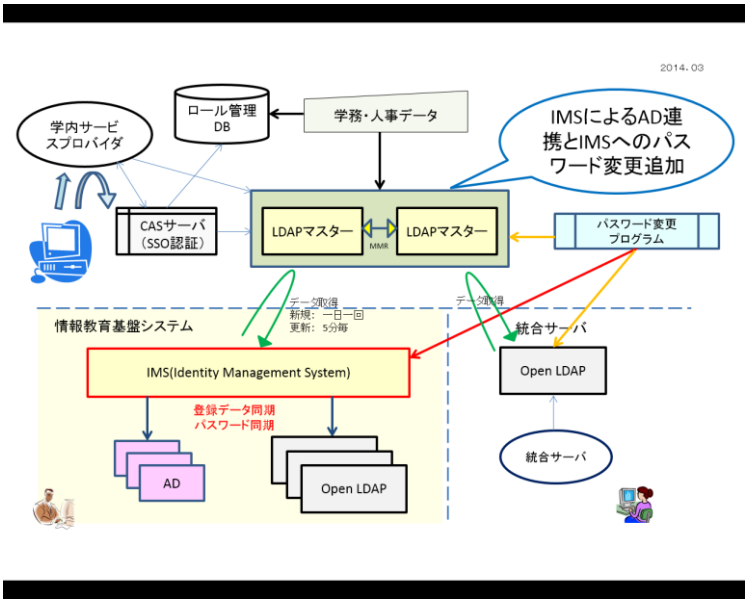


**図-2　2013 年 10 月からの名古屋大学 ID 認証基盤システム概要**

レンタル更新後の情報教育基盤システム認証系は、OpenLDAP と AD で構成されている。大きな変更点は、① Idsync を廃止し IMS を導入したこと、② 名大 ID パスワード変更プログラムを IMS 上のパスワードも変更するように機能追加したこと、の 2 点である。

本来 IMS は、ID の発行から更新・削除までを、その配下の認証システムを含め一貫して同期させる ID プロビジョニング機能を持っている。しかし、今回、情報教育基盤システムで導入した IMS は、LDAP マスターサーバから ID 情報を定期的に取得し、情報教育基盤システム内の ID プロビジョニングを受け持つことに

限定したものである。

一方、名大 ID パスワードについては、① LDAP マスターサーバ、② 統合サーバ上 OpenLDAP サーバ、③ IMS、について独自プログラムで更新処理を行っている。今回、IMS 上名大 ID パスワードの更新処理にあたっては、メーカ側からプログラムインタフェースの提供を受け、それを呼び出す形でパスワード更新を実現した。プログラムは Java 言語を使用し、IMS に対して SSL 接続を行い、XML 形式レスポンスのパース処理を行い、エラー対応等を実現している。【6】

## 4　将来構想

今後の構成案として、2 つの可能性が考えられる。一つは現在の構成を継承する方法、もう一つは名大 ID マスターとして IMS を採用する方法である。

### 4.1 現在の構成を継承

これは、図-2 の方法であって、LDAP マスターサーバと IMS の共存形態である。パスワード更新プログラムは現在のプログラムを利用する。この形態でも AD 連携は継続可能である。懸案は LDAP マスターサーバの継続である。メーカ提供の最新 LDAP Server は、ライセンス及びサポート契約が必須となっており、これを採用するかどうかは予算も含めて検討・決定する必要がある。一方、自前で LDAP サービスを行う方法としては、フリーかつオープンソースの実装である”Open LDAP”あるいは”Red Hat Directory Server”などの利用が考えられる。前者の”Open LDAP”は、小規模での実績は多いが、設定や管理手法が原始的にならざるを得ない。後者の”Red Hat Directory Server”については、GUI インタフェースによる管理が可能である。ライセンス契約すれば、メーカからのサポートも期待できるので有力な候補である。これは、オープンソースの Directory Server である”389 Directory（旧 Fedra Directory Server）”の系列である。

### 4.2 名大 ID マスターとして IMS を採用

この方法による形態例を、図-3 に示す。

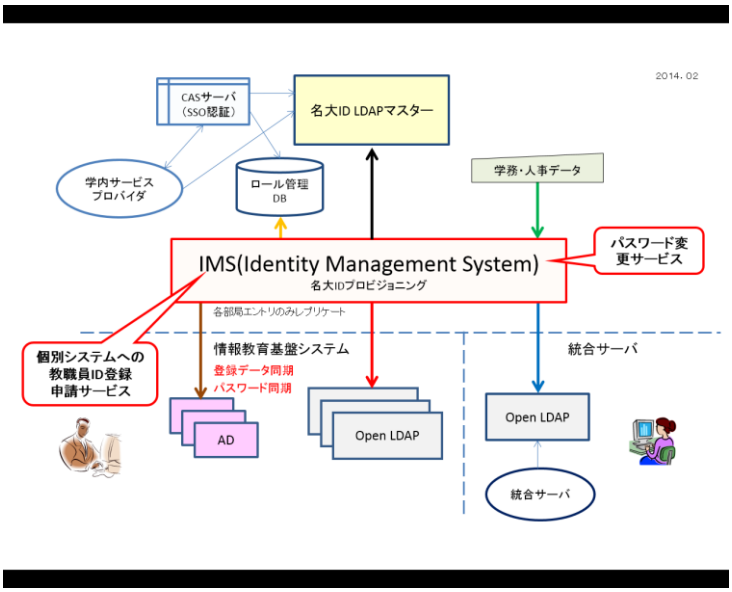


**図-3　IMS をメインにした名古屋大学 ID 認証基盤システムのイメージ**

特徴としては、IMS へのデータ登録を、学務・人事データに一本化する点である。一度 IMS に登録した名大 ID データは各種 LDAP サーバや AD、又はデータベースに対して、ID のプロビジョニングを行うことが可能になる。またパスワード更新は IMS 提供のものを利用すれば良い。管理者から見ると理想的な方法と言える。課題としては、属性情報のテーブル設計とインタフェース部分の既存プログラム改修、及びデータ移行

計画が必要である。また相当なサポート・ライセンス料も考慮しておかないといけない。これだけの処理をIMS で行おうとすると、オプション料金が掛かるため、費用も高額になると予想される。

## 5　おわりに

以上、名大 ID の認証基盤システムについて、AD 連携の実現方法を軸に、現状と将来について検討した。今後の課題としては、① IMS の位置づけ、② LDAP サーバの選択、がある。①は、IMS を名大 ID 情報データのマスターにするかどうかという選択である。マスターとするためには、既存システムとの整合性の確保、移行方法の検討及び、予算の確保が必要である。②は、今のところ、”Red Hat Directory Server”又は”OpenLDAP”を候補として考えている。これについては、事前にテストやライセンスの調査を行い、適切な判断を行う。

個人技術としては、AD へのユーザ ID の登録・更新、及びパスワードの直接更新ができることが課題である。特にパスワードの直接更新は、マイクロソフトが情報公開していないこともあって保証されていない。しかしこの技術を確立すれば、独自でプログラム開発を行いシステム構築することも可能である。【5,6,7,8,9】

一方で、少しイレギュラーな方法として、AD サーバを名大 ID マスターとする方法も考えることは可能である。しかしこの方式については、今のところ対応予定がない。

新システムを構築するに当たっては、以下の点を考慮する必要がある。

① 各マシン間の結合度を小さくし、独立して更新可能にしておく
② 移行期間中は、新旧システムの混在状態での運用サービスとなる
③ ライセンス及びサポート費用を見込む
④ システムバックアップと復旧計画は、予め盛り込んでおく
⑤ セキュリティの確保に注意を払う

最後に、日頃、何かとお世話になっている情報連携統括本部、情報基盤センター及び情報通信技術系の同僚諸氏に感謝する。

## 参考文献

[1] 田島嘉則,山田一成,柘植朗,堤守政,”名古屋大学 ID サーバ正式運用に伴うツールプログラムの開発”,全国共同利用情報基盤センター研究開発論文集 No.29, 2007 年 10 月

[2] 堤守政,柘植朗,”中規模ディレクトリサーバの再構築”, 核融合科学研究所技術研究会報告書,2008 年 3 月 11 日

[3] 山田一成, 堤守政,田島嘉則,柘植朗, ”名古屋大学 ID 運用に伴うツールプログラムの開発” , 核融合科学研究所技術研究会報告書,2008 年 3 月 11 日

[4] 堤守政,田島嘉則,山田一成,柘植朗,”名古屋大学 ID 管理・運用ツールのチームプログラム開発”, 名古屋大学技術研修会報告, 2008 年 3 月 13 日

[5] 堤守政, ”Samba・LDAP(Solaris)を使ったユーザ端末の UNIX-Windows 統合認証”, 全国共同利用情報基ンター研究開発論文集 No.31, 2009 年 11 月

[6] 堤守政, ”SpringWebFlow による名大 ID ユーザ用プログラム作成”, 名古屋大学技術研修会報告, 2012 年 2 月 29 日

[7] 堤守政,”名古屋大学 ID 認証基盤システム構成案の検討”, 全国共同利用情報基盤センター研究開発論文集 No.34, 2012 年 11 月

[8] http://www.dirmgr.com/blog/2010/8/26/ldap-password-changes-in-active-directory.html

[9] http://codezine.jp/article/detail/6109