共通基盤サブシステム

江藤博文*
総合情報基盤センター†

1　はじめに

総合情報基盤センター (以下、センターとする) の新システムの中心ともなるサブシステムが共通基盤サブシステムです。本サブシステムでは、統合認証システムによる認証情報の提供だけではなく、各サブシステムへの情報の提供、各サブシステム間の情報の相互連携などを行っています。本サブシステムには佐賀大学の全構成員の情報を統合管理しており、センターシステムの核となっています。

以下、本サブシステムについて解説します。

2　機能

共通基盤サブシステムは基礎情報共有機能、統合認証機能、シングルサインオン機能、共通情報共有機能の 4 つの機能があります。各機能は他のサブシステムと密接に連携しており、情報の正確性・最新性に注意を払っています。

以下、各機能について紹介します。

2.1　基礎情報共有機能

人事および教務システムからの情報をとりまとめ、大学全構成員の利用者情報を保有し、各システムに必要な利用者の情報を取りまとめています。教職員の人事異動、学生の入学・卒業などの情報を随時更新し、常に最新の情報を共有します。

本サブシステムの中心となる機能です。

2.2　統合認証機能

他のシステムに認証情報を提供する、LDAP を中心とした認証機能です。UNIX、Windows 系システムに認証を提供します。また、利用者の認証パスワードを一元管理しており、いずれのシステムにも同一パスワードでログインが可能となっています。

2.3　シングルサインオン機能

本機能で用いられているシングルサインオンは、学術認証フェデレーション (学認:GakuNin)[1] で用いられている Shibboleth[2]を使用しています。学認は UPKI イニシアティブ[3]の事業の一つである大学間の認証連携です。センターでは昨年度よりこの学認に参加し、学内にサービするべく準備を行ってきました。

この機能により、いずれかのサービスに 1 度ログインすれば、連携しているサービスにはログイン無しでサービスの利用が可能です。

2.4　共通情報共有機能

学部・学科・講座などの組織の階層構造、職種・職名に関する情報を保有し、他のシステムと共有する機能です。利用者は必ずどこかの組織に属し、なんらかの職種・職名を持っており、システムを利用するにあたり権限の管理などに必要となります。今まではその情報を個々のシステムで保有していましたが、ここで保有する事で他のシステムでは保有する必要が無くなります。

*etoh@cc.saga-u.ac.jp
†http://www.cc.saga-u.ac.jp/

[1] https://upki-portal.nii.ac.jp/docs/fed
[2] http://shibboleth.internet2.edu/
[3] https://upki-portal.nii.ac.jp/

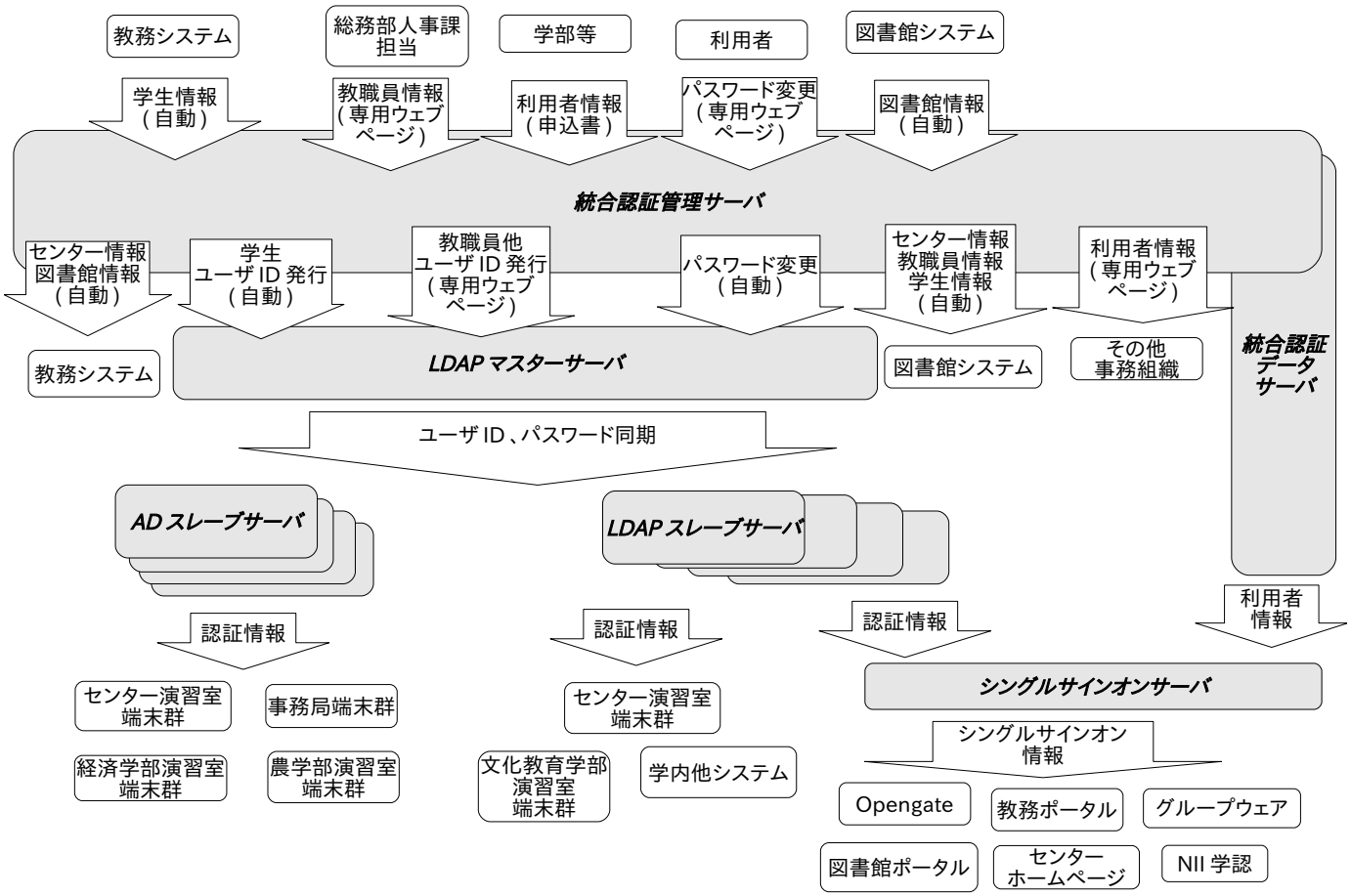

図 1: 共通基盤サブシステムデータフロー

3　サーバ

本サブシステムは、統合認証管理サーバ、統合認証データサーバ、LDAP マスターサーバ、AD スレーブサーバ、LDAP スレーブサーバ、シングルサインオンサーバの各サーバにより構成されています。サーバ間のデータのフローを図 1 に示します。

各サーバ間が密接に連携する事で、本サブシステムは運用されています。

以下、各サーバについて解説します。

3.1　統合認証管理サーバ

統合認証システムを管理しているサーバです。各システムからのデータの受け付け、各サブシステムへのデータの配布、センター ID の発行、パスワード変更など、本サブシステムの中核にあるサーバです。

3.2　統合認証データサーバ

3.1 統合認証管理サーバのバックでデータを管理しているデータベースサーバです。本サブシステムに関する全てのデータを保有しているため、セキュリティの観点から一般のネットワークからは直接アクセスはできません。

また、3.6 シングルサインオンサーバに利用者情報を提供しています。

3.3 LDAP マスターサーバ

利用者認証のマスターサーバです。認証の根本となるサーバのため、セキュリティの観点からこのサーバも一般のネットワークからは直接アクセスできないようになっています。

利用者の登録、変更はこのサーバにのみ行われます。変更情報が各スレーブサーバに伝搬し、常に同一パスワードでログインが可能となります。

3.4 AD スレーブサーバ

3.3 LDAP マスターサーバからの情報を受け、Windows クライアントの認証を行います。利用者の情報は常に LDAP マスターサーバからの一方通行で、本サーバから LDAP マスターサーバに情報が行く事はありません。この一方通行の情報の流れにより、全ての AD スレーブサーバの情報を同期しています。

センター演習室端末群 (Windows)、事務局端末群、経済学部演習室端末群、農学部演習室端末群に認証情報を提供しています。

3.5 LDAP スレーブサーバ

3.3 LDAP マスターサーバからの情報を受け、UNIX クライアントの認証を行います。3.4 AD スレーブサーバと同様に、LDAP マスターサーバに情報が行く事はありません。

センター演習室端末群 (Solaris)、文化教育学部端末群 (MacOSX)、3.6 シングルサインオンサーバ、学内の他のシステムに認証情報を提供しています。

3.6 シングルサインオンサーバ

2.3 シングルサインオン機能を提供するサーバです。Opengate、図書館ポータル、教務ポータル、グループウェアなどがこのシングルサインオンを利用しています。これにより、上記のいずれかのシステムにログインすれば、他のシステムを利用する場合には再度のログインの必要はありません。

4 終わりに

本サブシステムは、以前から構築・整備してきた統合認証システムを中心に、新たにシングルサインオン機能などを追加し、利用者の利便性を向上させました。学内の全ての情報システムがシングルサインオンに対応すれば、利用者の利便性は更に向上します。

学内で情報システムの運用されている方で、センターの認証の利用、シングルサインオンなどを検討されている方はセンターにご相談ください。