

大学におけるアイデンティティマネジメント

Identity Management in University-Wide Computer Environments

あらまし

ここ数年でLDAP (Lightweight Directory Access Protocol) をベースとした「統合認証」が普及し、現在は利用者情報を含めて統合的に管理することを目的とした「アイデンティティマネジメント」システムを望む声が増えている。多くのマルチベンダサービスを導入している大学ネットワークにおいても、ユーザ情報を効率的に管理するための「統合的なユーザ管理」が必須要件として挙げられることが多い。しかし、その実現にはコストを含めいくつかの壁が存在する。

本稿では、アイデンティティマネジメントシステムを構築するに当たり解決しなければならない課題とその解決へのアプローチ方法、および富士通が提供する大学向け統合アカウント管理パッケージ“Campusmate/ICAssist”の特長について紹介する。

Abstract

In recent years, widespread use of integrated authentication based on Lightweight Directory Access Protocol (LDAP) has increased the demand for identity management systems that enable integrated management of user information. In addition, universities, which often have multi-vendor networks, require integrated management so they can better handle their user information and streamline their management. Identity management systems have several benefits, but they also have many problems, for example, they are expensive. In this paper, we describe some of the difficulties with identity management systems. Then, we describe the Campusmate/ICAssist Identity Management package we have developed for universities to overcome these difficulties.



役 誠雄 (えき しげお)
文教ソリューション統括部 所属
現在、私立大学向けITソリューションビジネス、および大学向けパッケージの企画に従事。



安納順一 (あんのう じゅんいち)
文教ソリューション統括部 所属
現在、大学向け統合ユーザ管理パッケージ、および授業支援システムの企画、開発に従事。

まえがき

まだ「アイデンティティマネジメント」という考え方が一般的でなかったころ、「統合アカウント管理」とは「個々のサービスで管理されているユーザIDとパスワードの統一」、すなわち「統合認証」を意味していた。しかし、大学側が提供する学生サービスが増えるに従い、個々の学生サービスが管理しているユーザ情報（氏名、メールアドレス、学籍番号、所属など）の統合的な管理が重要視されるようになってきた。アイデンティティマネジメントを実現するためのソフトウェアは高機能で高価な汎用パッケージが多く、それだけでは大学のユーザ管理業務に適用することが難しい。そのため、業務に合わせた個別開発が必須となり導入コストを圧迫する要因となっている。

この問題を解決するため、富士通は大学におけるユーザ管理業務に特化した大学向け統合アカウント管理パッケージ「Campusmate/ICAssist（キャンパスメイト/アイシーアシスト）」を開発した。

本稿では、従来のユーザ認証からアイデンティティマネジメントに至るニーズの変遷について述べるとともに、アイデンティティマネジメントを実現するに当たって壁となる課題とその解決に向けたアプローチの方法、最後にCampusmate/ICAssistの特長と今後の展開について紹介する。

ユーザIDとパスワードの管理

認証とは個人を特定することであり、その手段として最も多く用いられているのがユーザIDとパスワードの組合せで利用者本人を特定する方式である。

ユーザIDとパスワードによって個人を特定するには、それらが保管されている格納庫（リポジトリ）と、認証を行うための手順（プロトコル）が必要となる。ユーザIDやパスワードを格納することができ、かつ認証のためのプロトコルが規定されたサービスを一般的に「ディレクトリサービス」と呼ぶ。図-1に示すように、リポジトリ内のユーザIDとパスワードが分かっても、プロトコルが一致しない場合には認証を行うことができない。

代表的なディレクトリサービスとして、主にUNIX系コンピュータの認証に使用されるNIS（Network Information Service）やレガシーWindows系コ

ンピュータの認証に使用されるSAM（Security Account Manager）、LDAP（Lightweight Directory Access Protocol）をサポートしているMicrosoft Active Directory、Novell eDirectory、Sun Java Directory Service、OpenLDAPなどが挙げられる。

認証を必要とするアプリケーションサービスが、どのようなディレクトリサービスをサポートしているかについては製品個々の設計思想に依存するものであり、世界共通の指針は存在しない。例えば、富士通の授業支援システム「Campusmate/CourseNavig（キャンパスメイト/コースナビ）」の場合、ローカル認証とLDAP認証から選択することができる。

ローカル認証の場合、ユーザIDとパスワードはCampusmate/CourseNavigが持つ独自のデータベースがリポジトリとなり、認証手順も独自のプロトコルとなる。このようなシステムが複数存在する場合、リポジトリと認証手順も複数存在することになり、必然的にシステム管理者のユーザ管理コストは増大する。加えて、利用者も複数のユーザIDとパスワードを覚えておく必要があるが、多くの場合システム管理者側はパスワード忘却などへの対処方法を用意しておかなければならない。

LDAP認証の場合、認証に必要な情報はアプリケーションサービスではなく、LDAP認証をサポートしているディレクトリサービス側のリポジトリに格納される。LDAPとはRFC（Request For Comment）によりその構造や動作が定義された標準規格であり、特定の製品を示すものではない。そのため、LDAP認証をサポートしているアプリケーションサービスを導入する場合には、どのベンダのLDAP対応ディレクトリサービスを採用するのかが

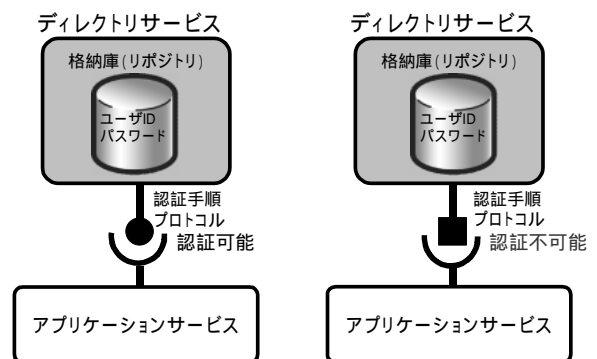


図-1 ディレクトリサービスの構造
Fig.1-Structure of directory service.

事前に検討する必要があるものの、独自形式のローカル認証とは異なり設計者の汎用的な知識を生かせるというメリットがある。また、LDAPを利用するアプリケーションサービスで共用することができるため、ローカル認証と異なり1種類のユーザIDとパスワードを覚えておけばよく、パスワード忘却が発生しづらいと言える。

大学では、学生サービスを目的としてマルチベンダによるITシステムが稼働している。それらのサービスを利用するには、多くの場合「認証」が必要であり、利用者は自身のユーザIDとパスワードをアプリケーションサービスごとに覚えておく必要があった。従来、これは個人情報や学内の秘密情報を管理する上で利用者に要求される最低限の義務であるという認識が主流であった。しかし、ここ10年の利用者層とアプリケーションサービスの拡大により状況は一変した。

分散から統合へ

ディレクトリサービスを構築する上で、最も重要な課題の一つとして「利用者のパスワード忘却への対応」が挙げられる。住所や電話番号など、頻繁に利用し、かつ一度覚えたらしばらくは変更する必要のない情報と異なり、ユーザ認証に使用されるパスワードはとかく忘れがちである。複数のアプリケーションサービスで使用しているパスワードが異なる場合は言うまでもない。

利用者のパスワード忘却への対応は、情報処理センターの窓口業務を多忙にし、ときにはパソコンへのログオンができないことで授業の進行を止めてしまうこともある。一方で、パスワードを忘れないようにと紙に書き留めておく利用者も多く、このことが秘密情報を危険にさらしてしまうことがある。これらの問題から、管理者側は複数のパスワードを利用者に覚えることを強要するのではなく、同じパスワードを確実に覚えてもらう方向に転換した。2003年度以降に大学から出された要求仕様のほぼ100%がユーザIDとパスワードの統一について触れている。

ユーザIDとパスワードを統一するには、二通りの方法が考えられる。一つ目は、すべてのディレクトリサービスに対して同じユーザIDとパスワードを登録する方法である。この方法の場合、利用者が

ある一つのディレクトリサービスのパスワードを変更した場合には、同時にほかのディレクトリサービスにもパスワードを同期することが必須要件となる。コンピュータサービスが情報処理センター内部のものであった時代には、本方式も現実的なソリューションであったと言えるが、ほぼすべての学生サービスがIT化されつつある現在、複雑な同期の仕組みを開発する必要があり、リスクを伴いやすい。

二つ目の方法は、統合認証サービスの構築である。統合認証とは、リポジトリとプロトコルを統一し、すべてのアプリケーションサービスが同じディレクトリサービスに対して認証要求を行うものである。こうしたニーズを実現に向けて後押ししたのがLDAPの普及である。これは2000年前後に発表されたノベル社のNDS (Novell Directory Services) やマイクロソフト社のWindows Active Directoryが深くかかわっていると言える。主要なOSが標準の認証プロトコルとしてLDAPを採用したことにより、それらをプラットフォームとするアプリケーションサービスの多くも追従することになった。現在では認証プロセスのデファクトスタンダードになっていると言える。

LDAPは、その認証プロトコルが世界共通であること、標準スキーマが明確であること、かつプラットフォーム依存がないという点に大きな利点がある。例えば、Active Directoryで構築されたLDAPサーバを使用して、Linuxのログオン認証を行うことができるため、従来のようにUNIX系とWindows系の認証プラットフォームを個別に検討する必要がない。

LDAPの普及と周辺のアプリケーションサーバの対応により、従来問題となっていた複数のユーザIDとパスワードの管理問題はほぼ解決したと言える。開発者にとっても、豊富に用意されたライブラリを使用するだけで、アプリケーションサービスにLDAP認証を組み込むことが可能であるため、LDAPは認証プロトコルとしては確固たる地位を確立したと言える。

統合認証に残された問題点

LDAPの普及は統合認証の実現に一役買うことになったが、一方で、アプリケーションサービスから物理的に切り離された独立システムであることから問題点も存在する。

一つは、学生サービスの入り口である認証サービスが、ディレクトリサービスによって集中管理されているため、ディレクトリサービスのダウンがサービス全体のダウンにつながる点である。また、利用者が増えるに従い負荷の問題も無視できない。ただし、これらはディレクトリサービス自身の性能向上とユーザ情報のカタログ化、複数サーバによるマルチマスタ構成などにより問題のないレベルにまで向上している。

深刻なのは、リポジトリの分割による登録作業の煩雑化であろう。統合認証が目指したのはユーザIDとパスワードの統一のみであり、一般的にアプリケーションサービス固有の情報を統合することまでは考慮されていない。現在、大多数のアプリケーションサービスは、LDAPをログオン認証のみに使用しており、氏名やメールアドレス、所属、学籍番号など、ユーザIDをキーとして付帯される情報については従来通り自身のデータベース上で管理している。そのため、ユーザIDとパスワードをディレクトリサービスに登録した上で、ほかの情報をアプリケーションサービスに登録しなければならない。また、従来はアプリケーションサービス内に閉じていた利用者管理は、中央に設置されたディレクトリサービスを共通で使用することにより、学内の壁を越えた運用管理が求められるようになった。多くの大学が抱える問題点の一つにシステム管理者の不足が挙げられるが、アプリケーションサービスの増加とユーザ管理の煩雑化はディレクトリサービス管理部門に対し、従来以上のパワーを強いるようになったのである。

統合認証からアイデンティティマネジメントへ

ディレクトリサービスの運用コストを低減し、かつ利用者の利便性を損なわないようにするにはアプリケーションサービス間でユーザ情報の管理方法について統一的な規格を定義する必要がある。しかしこれを実現することは容易ではない。アプリケーション開発部門の合意はもとより、真に利用者のメリットを追求するにはベンダ間のアライアンスにまで広げることになるからである。

そこで、現在のアプリケーションサービスに手を入れず、かつこうした現状を少しでも改善するために登場したのが、アイデンティティマネジメントという考え方である。管理対象をユーザIDとパスワードから、ユーザの個人情報全般にまで広げて統合的に管理するという意味が込められている。

統合認証とアイデンティティマネジメントの違いを図-2に示す。統合認証では、ディレクトリサービスに登録するのはユーザIDとパスワードだけであり、アプリケーションサービス固有の情報はサービスごとに個別に登録する。これに対し、アイデンティティマネジメントでは、ディレクトリサービスにはアプリケーションサービス固有の情報を含めて登録し、登録した情報は各アプリケーションサービスに自動的に同期される。そのため、アプリケーションサービス固有に登録する必要がなく、1回の登録で済むため管理コストを低減することができる。マイクロソフト社やノベル社、サンマイクロシステムズ社といった基本ソフトを提供するベンダは、アイデンティティマネジメントを実現するためのソフ

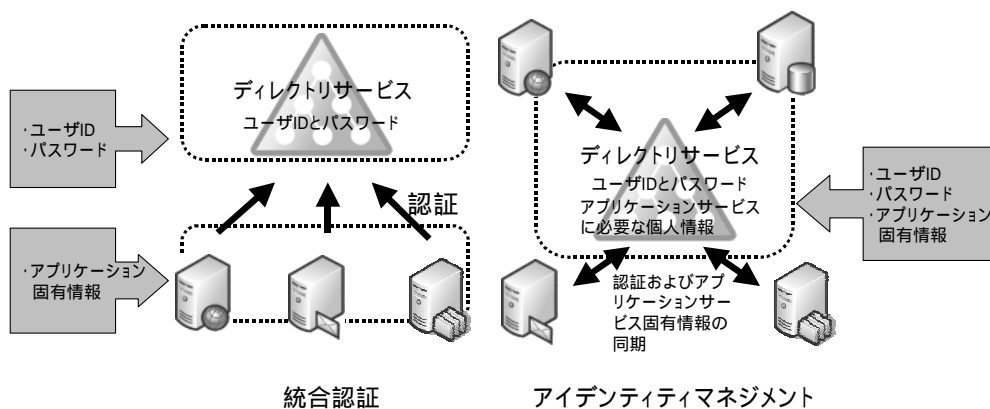


図-2 統合認証とアイデンティティマネジメントの違い

Fig.2-Difference between integrated authentication and identity management.

トウェア開発に積極的に取り組んでおり、現在ではユーザ情報の同期にとどまらず、統合的なセキュリティポリシー管理、ユーザIDのライフマネジメント管理などアカウント管理全般にわたる技術に発展しつつある。

アイデンティティマネジメントの実現に向けて

ここ3年余りで大学商談におけるアイデンティティマネジメントの重要性は急速に増大しているが、そうした要求に対して汎用的なアイデンティティマネジメント製品をそのまま適用することは、多くの場合難しいと言える。その理由は2点挙げられる。

一つ目の理由は導入コストである。汎用的なアイデンティティマネジメント製品は、高価である。とくに大学のような利用者数が数千~1万人以上の規模になると、ライセンス料だけでも莫大な出費となってしまう。

二つ目の理由は機能の問題である。汎用化されたアイデンティティマネジメント製品は、それを素材として開発することを前提に提供されている場合が多い。用意されているGUIは必要最小限であり、専任のユーザ管理者を設置することが難しい大学において、使いこなすことは容易でない。そのため、従来は大学の運用に合わせたオーダメイドシステムを開発する必要があった。このことは必然的に導入コストの増大へとつながり、一方で学生サービスへの投資を減らすという本末転倒な結果へとつながる。

大学におけるアイデンティティマネジメントに要求されるのは、テクノロジーとしての高機能さではなく、業務を定型化するための作りこまれたインタフェースと、新たに追加されるサービスを吸収するための柔軟性である。従来は柔軟性を含めて定型化を図ろうとしてきたため、結果として完全なオーダメイドシステムとなってしまう、コストの増大を招いていたと言える。

ユーザ管理業務のモデリング

富士通は、大学におけるアイデンティティマネジメントの実現に向け、2年にわたって大学ユーザ管理業務のモデリングを行ってきた。その中で特に注力したのは、定型化できる処理と柔軟性を残さなければならない処理を明確にすることである。

(1) 定型化が必要な処理

定型化が必要な処理とは、主に管理者の手作業が発生する業務であり、以下に示す四つのタスクである。

- ・ユーザの登録
- ・ユーザの削除
- ・パスワード初期化
- ・ユーザ情報の更新

それぞれのタスクは、図-3に示すように、「データの準備」「データの確認」「データの処理」「結果の確認」という四つのプロセスで構成されている。これらのプロセスには必ず大学固有のルールが存在しており、これが業務を複雑にし、定型化を困難にしている原因であることが分かった。しかし、それぞれのプロセスの入力情報と出力情報を明確にすると、実は大学固有のルールをパラメタとしてとらえられることが見えてくる。すなわち、各プロセスのパラメタを変更可能にすることで、大学ごとに特別な機能を作りこむことなく大学固有のニーズを吸収することができることが分かった。

(2) 柔軟性を残さなければならない処理

柔軟性を残さなければならない処理とは、主にディレクトリサービスや、アプリケーションサービスへの同期、そしてユーザ登録作業に伴う付帯作業（ホームディレクトリの作成やユーザ環境の基本設定など）である。同期の具体的な処理方法は大学ごとに構築されているサービスや運用方法によって異なることが多く、かつプラットフォームも多彩であるために単純なパラメタ化を行うことが難しい。とくに、GUIとして作りこんでしまうことは新たな

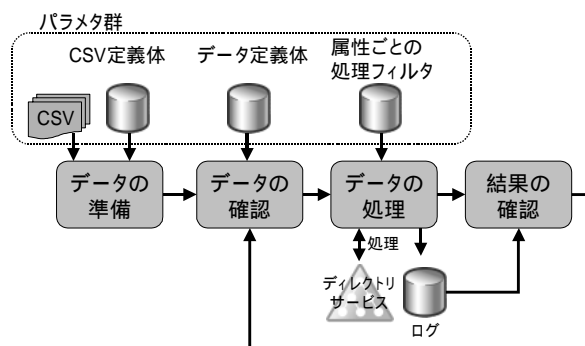


図-3 ユーザ管理業務を構成する四つのプロセス
Fig.3-Four processes that constitutes user management tasks.

サービスの追加や処理方法の変更に対応することが困難になるため絶対に避けるべきである。同期処理には、できる限り現場で対応可能な技術を用い、必要に応じて修正することが可能な余地を残しておく必要がある。

こうした検討を経て、「登録と同期を完全に分離する」という、2段階登録方式の機能を兼ね備えたユーザ管理パッケージを開発することが決まった。

Campusmate/ICAssist

Campusmate/ICAssistは、2年にわたる業務のモデリングの結果から開発された新しいタイプのアカウント管理パッケージである(図-4)。Campusmate/ICAssistは、過去20大学のユーザ管理事例をもとに分析を行った結晶であり、本パッケージの適用により導入コストを従来の半分以下に低減することが可能である。大学のユーザ管理業務をターゲットにしており、情報処理センタが行う定型的な業務を標準機能として実装している。ほかのディレクトリサービスへの同期は、必要に応じてスクリプトを作成すればよく、そのベースとなるサンプルスクリプトも提供している。

Campusmate/ICAssistの特長を以下に示す。

(1) Active Directoryを格納庫として使用

Windowsクライアントを認証するため大多数の大学ではActive Directoryが導入されている。ここにはパソコンを利用するすべての利用者が登録されているため、これを管理簿とすることは非常に効率が良い場合が多い。専用のLDAPサーバや管理用の

DBMS (Database Management System) を新規に導入する必要がないため投資を抑えることもできる。

(2) ユーザ管理の定型的な機能を標準装備

大学が必要としている代表的なユーザ管理機能を標準で実装することで、新たな開発を抑えることができるだけでなく、煩雑であった管理業務を定型化することができる。大学によって異なる初期登録用ファイルの形式や、パスワードの形式などはすべて設定変更画面からパラメータを修正することで吸収できる。

(3) 登録と同期の分離

図-4に示すように、中央の管理簿であるActive Directoryに対するユーザ管理業務と、ほかのディレクトリサービスやアプリケーションサービスへの同期処理を完全に分離した構造となっている。また同期処理には、利用者が作成したスクリプトやバッチファイルを指定することができるため、学内運用に合った柔軟な同期処理が構築可能である。

今後の展開

Campusmate/ICAssistでは、さらなる業務の効率化を進めるため、サービスのSOA (Service Oriented Architecture) 化を目指している。これは、情報の交換をXML形式のメッセージで送受信する機能で、ほかのアプリケーションサービスに対するユーザ情報の公開や認証の代行をすることを目的としている。例えば、図-5に示すように富士通の大学事務パッケージ“Campusmate-J”から授業

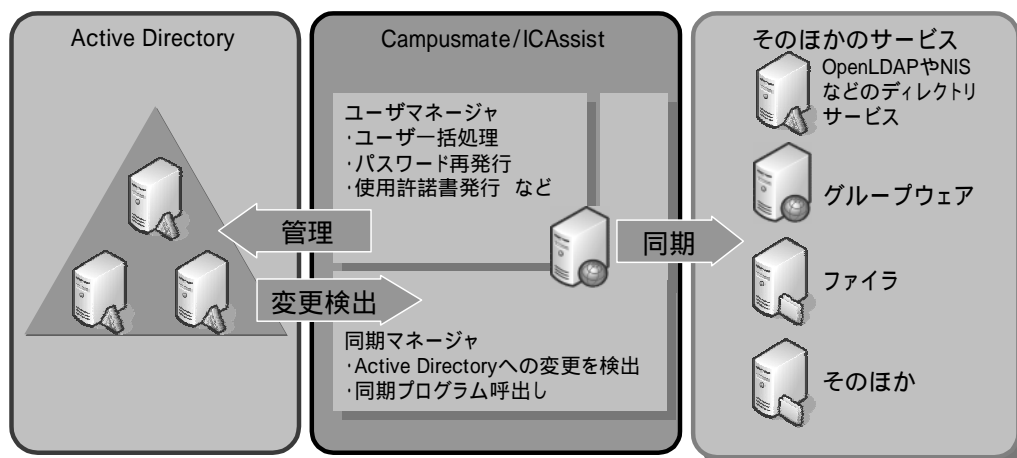


図-4 Campusmate/ICAssistによるアカウント管理
Fig.4-Management of user identities by Campusmate/ICAssist.

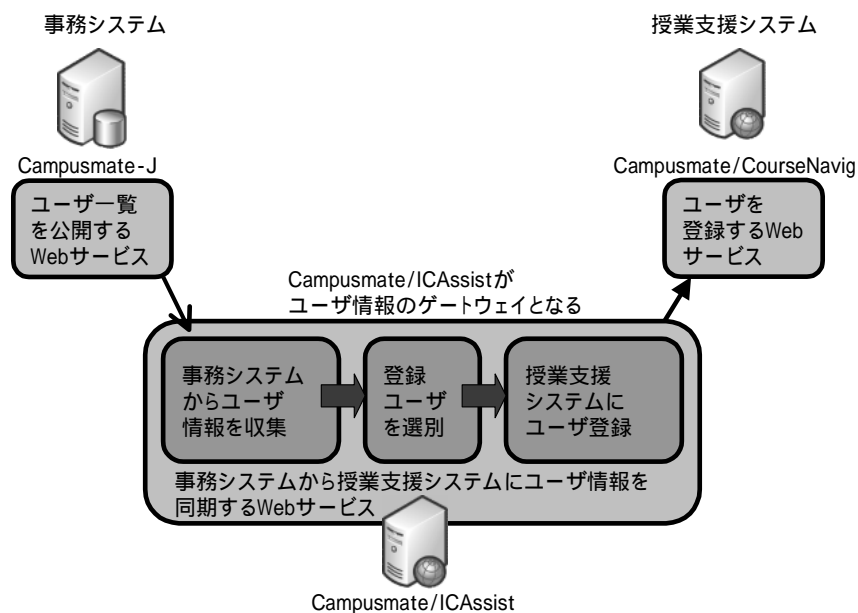


図-5 SOAによる外部システムとのシームレスな連携
Fig.5-Seamless cooperation with external system by SOA.

支援システムCampusmate/CourseNavigへの利用者情報登録をCampusmate/ICAssistを利用してシームレスに中継するといった機能を目指している。これに伴いアカウント管理業務が局所化されてしまうという危険性がある。これを避けるため、複数部門からの利用を想定した管理機能の実装も進めていく予定である。

む す び

より効率的なアカウント管理を実現するには、アイデンティティマネジメントは必須であると言える。しかし、とかく高機能なツールは管理コストの増大といったデメリットを生んでしまう可能性がある。Campusmate/ICAssistは、完全に大学向けに開発したパッケージであり、情報科学センターにおけるアカウント管理業務のコスト低減を第一の目的としている。今後、ますます複雑化する学生サービス管理の一助となることを確信している。