◇◇◇◇◇◇
解 説
◇◇◇◇◇◇

全学統合 ID 管理システムの概要

中山 仁[1]

1 はじめに

大学における情報サービスの拡大や業務の電子化の進展に伴って，情報システム利用者の識別，認証情報やその他の属性情報を適切に管理する，アイデンティティ管理 (ID 管理) の重要性が高まってきています.

ID 管理機能を活用することにより，ログインなどの認証の煩雑さを軽減したり，利用者プロファイルに応じてカスタマイズされたサービスを提供するなど，より高度で便利な利用環境を構築することが可能となりつつあります．一方，ID 管理が不十分だと，利用者に対してタイムリーに適切な情報サービスを提供することができません．また，セキュリティ上の脆弱性やリスクの大きな原因ともなります. 小さなシステムであればシステム管理者が ID 管理業務を行うこともできますが，教職員や学生などが多数利用するシステムにおいては，ID 管理も複雑化し作業量も増大するため，個々のシステムがきちんと対応することは容易ではありません.

本学においても，ID 管理を必要とする情報システムが増える中，ID 管理に係るコストを低減し，利用者にとってのユーザビリティを向上させるためには，より統一的で一貫性のある ID 管理を行うことが必要と考えられるようになってきました．そこで情報基盤の整備計画の一環として全学規模の ID 管理体制の整備が推進されることとなり，その第一歩かつ中核部分を担うものとして，全学統合 ID 管理システムが導入され 2009 年度より運用を始めました.

本稿では，この全学統合 ID 管理システム (以下，統合 ID システム) について，概要を説明します.

2 システム構成

統合 ID システムは，利用者情報を管理する ID データベース部と，各情報システムとの間で利用者情報の転送制御を行うシステム間連係部から構成されています (図 1).

ID データベース部には，利用者情報を管理する ID データベースサーバおよび，一般利用者や管理者からのアクセスインターフェースとなる ID 管理サーバ (Web サーバ) があります．利用者は，ID 管理サーバの一般利用者向け Web インターフェース[2]を用いて，パスワードの変更や，アカウント登録情報の確認などを行うことができます.

[1]情報科学センター，jin@isc.kyutech.ac.jp
[2]https://www.idm.isc.kyutech.ac.jp/users/

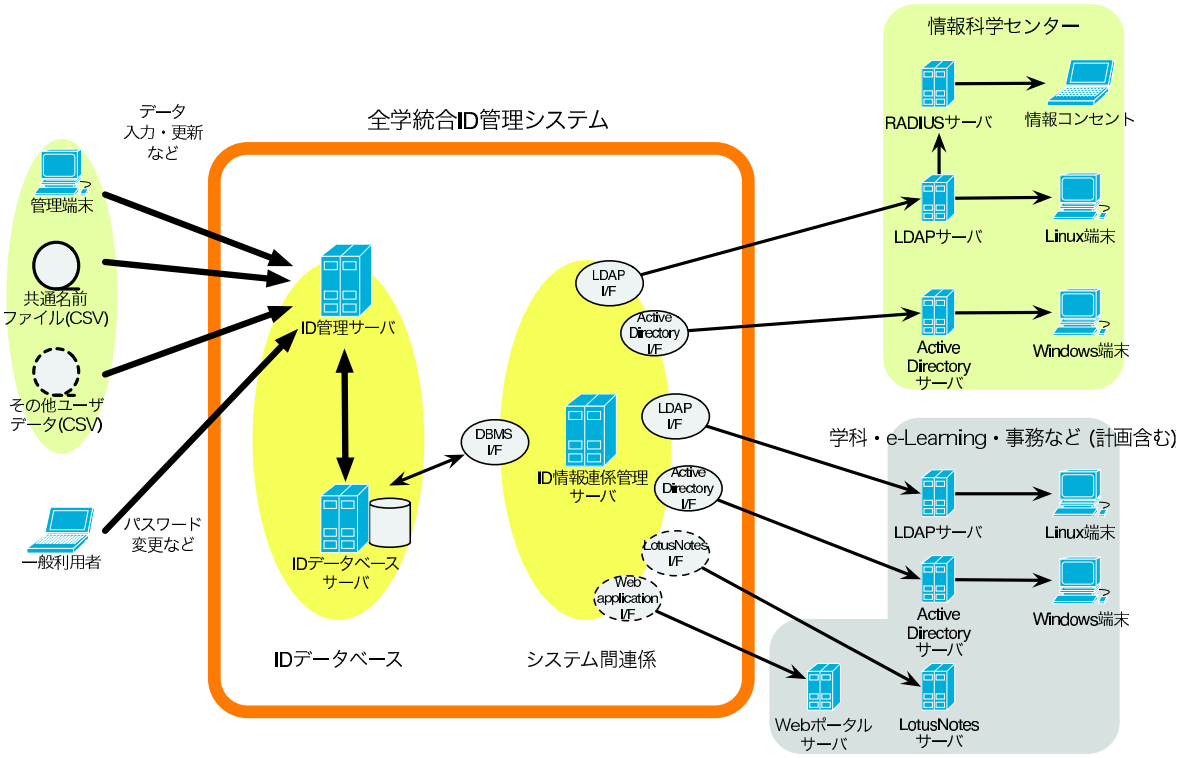

図 1: システム構成の概要

一方，システム間連係部は ID データベースのアカウント情報を各情報システムのアカウント管理システム (LDAP や Active Directory) へ伝播する部分です．ここでは，連係先システムごとにそれぞれ独立したシステム間連係インターフェースを構築する必要があります．

現在統合 ID システムで管理されている利用者のアカウントは，全ての学生，アカウントの登録 (任意) を行った教職員，その他の利用者で構成されています．またこの他に情報科学センターシステムで使用される，講義用および TA 用のアカウントも含まれます．

統合 ID システムに新たなアカウントが追加されると，その情報は日次処理によって連係先の各システムに伝播され，通常翌日には連係先システム側で有効になります．また，利用者が行ったパスワード変更の情報は，ほぼリアルタイム (数分程度) で各システムに反映されます．

3　ID データベース

ID データベースは主として，利用者個人の識別子である KID を主キーとする KID テーブルと，利用者のアカウントの識別子である RID を主キーとする RID テーブルとから構成されています．

KID テーブルは，氏名など基本的な個人属性情報のみを含みます．KID は統合 ID システムが独自に割り当てる個人識別子で，職員番号や学生番号などとは無関係に設定されています．KID は本来同一人に 1 つだけ割り当てられることを想定していますが，現状では事務処理上の制約などもあり，1 人に複数の KID が割り当てられる場合もあります[3]．

[3]学部学生が大学院に進学した場合など

今のところ，KID はほぼシステムの内部処理だけで使用されているため，一般の利用者が自身の KID を意識する機会はあまりありません．パスワード変更の際に使用する一般利用者向け Web ページの中で，KID を確認することができます[4].

一方，実際に利用者が使用するアカウント (ログインアカウントなど) に対応する情報を持つ部分が RID テーブルです．RID テーブルで管理される主な情報としては，アカウントの所有者 (KID)，認証情報 (ログイン ID とパスワード)，職員番号または学生番号，所属情報 (所属学科など) などがあります.

ID データベースでは，1 人の利用者が複数の立場 (例えば学生と TA のような) に対応する複数のアカウントを持つことを想定しているため，1 つの KID テーブルレコードに対し複数の RID テーブルレコードを対応づけることができます．今後別の新たなアカウント体系を導入する場合にも，対応する RID テーブルを設計して追加することにより現在の ID データベースの枠組みの中に収容することができます．将来的には，IC カード (職員証，学生証) や生体認証などの情報を利用することも可能となるかもしれません.

4　ID 情報の伝播

ある情報システムが統合 ID システムからの利用者の ID 情報の伝播を受けようとする場合，統合 ID システム側において，その情報システムに対応した新たな連係インターフェースを準備する必要があります[5]．連係インターフェースは，通信制御や，プロトコル変換，データ形式の変換などの基本的な機能に加えて，

- 伝播先システムのポリシーに対応した，利用者アカウントの制限 (特定の学科の学生の情報だけを伝播する，など) や，伝播する属性情報の選択
- 伝播先システムに依存するパラメタの設定 (UNIX システムであれば，アカウントごとの uid やホームディレクトリなど)

などの機能を設定することができます.

この連係インターフェースを含むシステム間連係部の開発には Sun Identity Manager という製品を使用しました．Sun Identity Manager はさまざまな伝播プロトコルをサポートし，また Java と XML による強力なカスタマイズ機能を有する製品ですが，統合 ID システムではこれまでのところ，使用されている伝播プロトコルは LDAP と Active Directory のみで，伝播設定も上にあげたような比較的シンプルな内容にとどまっています．これは，これまでに連係設定を行ったシステムがいずれも教育研究用で，基本的に同じような形態の ID 管理を行うシステムであることも要因の一つであろうと思われます.

5　おわりに

現在，学内の各種情報システムは，それぞれ更新または導入のタイミングに合わせて統合 ID システムへの接続をすすめています．これまでに情報科学センターシステムや各学部，学科の教育研究用シス

[4] ログイン直後の TOP ページで「個人情報変更」ボタンをクリックする
[5] 原則として，インターフェース構築に係るコストは連係先のシステム側が負担します

テム，e–ラーニング関連システムなどで連係作業が完了し，統合 ID システムの ID 情報に基づく利用者管理が行われています．今後，残る学科システム等においても順次連係設定が行われる予定です．

また 2011 年度以降，事務方を中心とする主要な業務系システムについても統合 ID システムへの接続が計画されています．これに伴い，業務系システムでの利用を想定した，新しい教職員用アカウント体系の導入準備がすすんでいます．

さらに現在，学術認証フェデレーション[6] との連係を準備しており，間もなく認証連係が開始される[7] 予定です．学術認証フェデレーションを利用することにより，国内外の様々な学術系のサービスや情報資源へのアクセスが，統合 ID システムのアカウントを用いてできるようになるため，利便性が大きく向上することが期待されます．

このように，大学全体に一貫性のある利用者 ID 情報を提供する統合 ID システムは，本学がより高度で安全な情報サービスを展開していく上で今や不可欠のものとなりつつあります．その一方で，現状のシステムは運用体制も含めてまだ未完成な部分も多く，今後も引き続きより良い解をめざして模索を続けていきたいと考えています．

[6] http://www.gakunin.jp/
[7] 当初は試行サービスとなります