◇◇◇◇◇◇
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

2009 年に全学統合 ID 管理システム [1](以下，統合 ID システム) が導入されて以来，情報科学センターや事務，学科等の情報システムの利用者アカウント管理も順次統合 ID システムと連係する形へと移行してきました．また情報システム面の整備と並行して，アカウント登録や削除の処理に係る事務的なワークフローも確立され，全学規模での利用者アカウントの取り扱いルールやポリシーも年を追うごとに充実してきています．統合 ID システムが目標とする大学全体での統一的な利用者アカウント管理は，着実に整備が進みつつあると言えるでしょう．

その一方で，言わば手探り状態から機能を立ち上げた初代の統合 ID システムは，実際に運用を重ねるにつれ，学内のアカウント管理の実態にそぐわず利用しにくい面もあることが見えてきました．そこで第二世代にあたる 2014 年のシステムの更新にあたっては，システムの構成や ID 管理の体系などの必要要件を大幅に見直して単純化することで，より本学の実情に即した新たなシステムを再構築することをめざしました．

本稿では，前システムからの主要な変更点を中心に，2014 年度より稼働開始した新しい全学統合 ID 管理システムの概要を説明します．

2　システムの特徴

2.1　システム間連係インターフェース

前システムの導入段階では，将来的にどのようなシステムが統合 ID システムと連係するかについて十分見通せていなかったこともあり，できるだけ多様な連係インターフェースに対応できる ID 管理ソフトウェア製品 (Sun Identity Manager) を採用しました．しかし，高機能である分連係インターフェースの構築，設定が複雑であったため，システム連係を新たに構築しようとするごとにそのための高いコストを負担しなければならず，これが新たなシステム連係を展開する上での障害となっていました．

一方，これまでに学内で構築した連係事例においては，連係先のシステムのアカウント管理はすべて LDAP または Active Directory (AD) を用いていました．他のシステム事例などを見ても，現在新たに構築，導入される情報システムにおけるアカウント管理は，後方互換性など特別な事情がない限り，これら 2 つが事実上の標準となっています．そこで今回の統合 ID システムの設計にあたっては，連係対象を LDAP と AD のみに限定することによって連係インターフェース設定の簡素化を図りました．

その結果，システム間連係の立ち上げや修正，更新などの作業はかなり単純化され，簡単なものであれば Web パネルによる操作で対応できるようにもなっています．これにより，前システムでは連係構築のコストが負担できずに統合 ID システムとの (直接) 接続が難しかった比較的小規模なシステムについても，今後は比較的容易に統合 ID システムを利用できるようになるのではないかと考えています．

[1]情報科学センター，jin@isc.kyutech.ac.jp

2.2 ID 管理体系

前統合 ID システムのスタート時には，全学の教職員，学生を対象とする基本アカウント (現在の九工大 ID) を設定し，その情報はパスワードも含めて学科等の連係先システムに配信されていました．しかし，事務系のシステムとの連係を検討する中で，教職員のみが対象でよりセキュリティ的な配慮が必要な事務系のシステムのアカウントを，学生を含み学内のさまざまな学科等でも使用されるアカウントと共用するのは (パスワードの漏洩などの) リスクが大きいのではないかという問題提起がありました．議論の結果，利用者が管理するアカウントが増える問題はあるものの，事務系システムの利用に特化した教職員向けのアカウント (オフィス ID) を新たに導入することになりました．オフィス ID アカウントは連係先を事務系のディレクトリサーバに限定し，アカウント情報が漏洩するリスクを最小限に抑えています．オフィス ID は前の統合 ID システムのもとで導入されましたが，新システムでも引き続き運用されています．

また前統合 ID システムにおいては，全ての利用者に KID という固有の ID を割り当て，その人が持つ全てのアカウント情報をその KID のもとに集約する設計になっていました．例えば，学部から大学院に進学してアカウントの ID が変わった場合にも，それらを同一人の別のアカウントとして管理することが可能になっていました．しかし実際には，進学や再雇用などで新しい学生番号，職員番号が割り振られると，その人の同一性を保証する根拠が失われるため，結局 KID についても新たに発行して「別人」として取り扱うしかありませんでした．

KID による利用者の同定と複数アカウントの集約管理が事実上有名無実化している状況を受けて，新システムではこれを廃止し，アカウント (九工大 ID およびオフィス ID) 単位で利用者を管理する方法に改めました．複数のアカウントを持つ利用者は，統合 ID システムを利用する際に自分がどのアカウントを使おうとしているかを意識する必要がありますが，利用者の多くが九工大 ID を一つだけ持つ学生であるためか，これまでのところ実質的な影響はそれほど大きくないようです．システム面では ID データベースの構造がシンプルになったため，それを参照，更新する管理者 I/F，利用者 I/F の画面設計や関連処理の論理設計などもかなり単純化されました．

2.3 多要素認証

現在多くの情報システムで使用されている，文字による ID とパスワードを使った利用者認証方式 (パスワード認証) は，広く普及し容易に利用できる反面，セキュリティ的な強度はそれほど高くありません．これに対し，異なるアプローチの認証方式を複数組み合わせて使うことでより強力な認証を行うのが多要素認証と呼ばれる方式です．実際にはパスワード認証と使い捨てパスワード (ワンタイムパスワード: OTP) 認証の組み合わせなどが比較的よく使われます．

現在統合 ID システムが管理する認証情報もパスワード認証を想定した ID とパスワードのセットですが，将来的により強いセキュリティを求められるシステムと連係することを想定し，今回新たに Web ベースのサービスに対して多要素認証の機能を提供するサブシステム (ファルコンシステムコンサルティング社 WisePoint Shibboleth) を導入しました．なお，こうした強力な認証機能は業務系システムでより必要性が高いという判断により，今回のサブシステムはオフィス ID アカウントを使用するシステム (主に事務系) のみが対象となっています．

利用者から見た WisePoint のシステムは，本来利用しようとする Web サイト (サービス) に対する認証機能を提供する一種のフロントエンドとして動作します．利用者はまず WisePoint サーバにアクセスして二段階の認証を行います．認証が成功したアクセスについてはその後本来の Web サイトに中継され，利用者があらためて認証することなしにサイトにログインすることができます．

WisePoint サーバにおける第一段階の認証は一般的なパスワード認証で，続いて OTP による認証を行います．OTP 認証についてはいくつかの方式が実用化されていますが，本システムでは Web ブラウザ

図 1: 多要素認証における認証画面の例

の画面に図 1 のような小さな画像の配列 (マトリクス) を表示し，その中からあらかじめ自身で決めておいたいくつかの画像の並び (たとえば，すいか–カメラ–ライオン) を順番にクリックすることで認証を行います．マトリクスの画像の並びは認証のたびに変化し，発生する OTP も毎回異なるものになります．

2016 年 2 月現在，多要素認証サブシステムはテスト用の Web サイトと接続して，技術的な問題点や運用面での課題などの評価を行っています．実際のサイトと接続しての本番運用については具体的な開始時期は未定ですが，接続にあたっては対象サイト側の改修，調整作業が必要であり，また想定される対象サイトの重要性からも慎重な取り扱いが求められることから，もう少し準備期間が必要になることが予想されます．

2.4　その他

一般の利用者が統合 ID システムに直接触れるのはパスワード変更を行う場合がほとんどではないでしょうか．一方，九工大 ID やオフィス ID のパスワードを忘れてログインできなくなった場合，これまでは平日日中に情報科学センターの窓口などに出向いてパスワードの再発行の手続きを行う必要がありました．

こうしたパスワード忘れへの対応をもっと簡単にするため，今回のシステムの利用者向け機能には，自分でパスワードを確認できるパスワードリマインダ機能が加わりました．秘密の質問とその回答，さらにリマインダメッセージを受信するためのメールアドレスをあらかじめ自分で登録しておくことで，メールと Web が使用できる環境であればセルフサービスでパスワードを確認することができるようになりました．遠隔地や休日にパスワードがわからなくなった場合には，特に有用な機能となるでしょう．

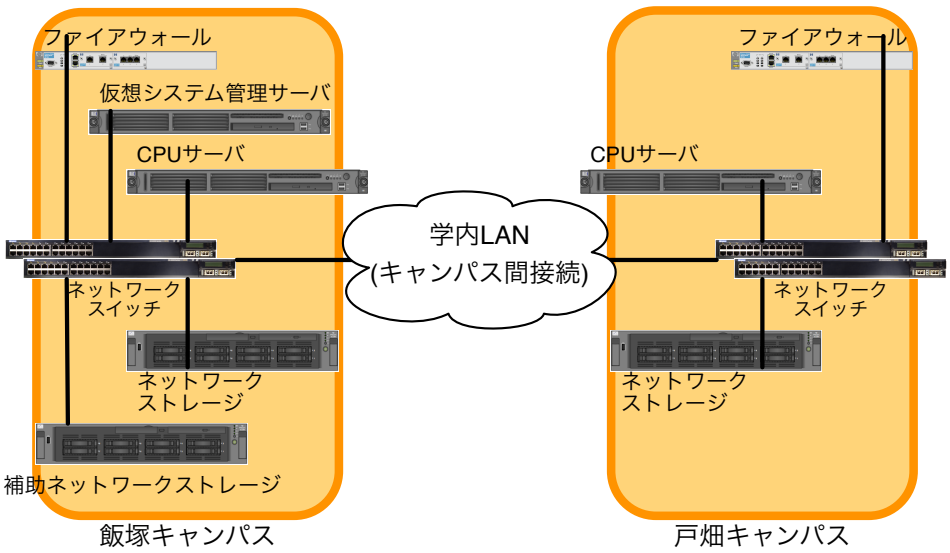

図 2: 主要機器の構成

3　システム構成の概要

今回の統合 ID システムは，構築設計上の柔軟性や将来的な拡張性の確保，また運用における柔軟性や障害時の復旧対応の観点などから，仮想マシン (VM) 方式による仮想サーバシステムを全面的に採用しました．図 2 に主要な機器の構成と接続関係を示します．

仮想サーバシステムは，飯塚キャンパスに設置した CPU サーバとネットワークストレージを中心に構成されます．中核である CPU サーバとストレージについては戸畑キャンパス側に同一構成の予備機をそれぞれ設置し，さらに飯塚側ストレージのデータを随時戸畑 (予備機) 側に複製 (レプリケーション) することで，ハードウエア障害などが発生した場合に運用を予備機側で引き継ぎ，比較的短時間でサービスを再開できるように配慮しました．仮想サーバシステムとしては小規模ですが，能力的にはまだ余裕を残しており，将来的なサービスの拡大 (運用する仮想サーバの増加) にも対応できるものとなっています．

一方，統合 ID システムの論理的なシステム構成の方は，前システムと比較的近い形となりました．図 3 にその概要を示します．

統合 ID システムのシステム要素のうち，利用者，管理者に対する操作インターフェース (Web インターフェース) や ID データベースの管理，連係システムとのインターフェースなど，システムの主要部は，2 つの仮想サーバ上に富士通の統合アカウント管理パッケージ UnifIDone を用いて構築されています．また多要素認証サブシステム (WisePoint Shibboleth) は 3 つの仮想サーバを使って動作します．

4　おわりに

これまでに，学内の主要な (共用) 情報システムの大部分が直接または間接的に統合 ID システムとの連係を完了し，共通のアカウント (九工大 ID，オフィス ID) を用いて利用できるようになりました．また，学術認証フェデレーション (学認) との連係により，電子ジャーナルを始めとする多くの学術系のサービスについても，普段学内で使っている九工大 ID アカウントで利用できるようになっています．

近年はクラウドコンピューティングに代表される高機能低コストな情報基盤サービスが大量に提供されるようになり，大学でも情報システムを外部委託 (アウトソーシング) して運用する事例が急速に増え

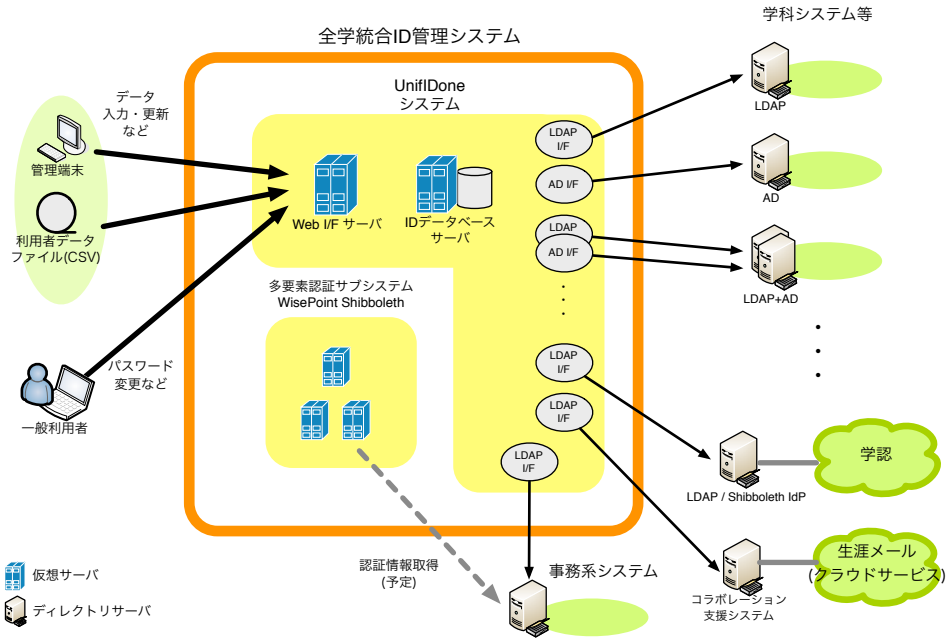

図 3: システム構成の概要

てきました．本学でも学認に加えてクラウド型サービスを利用した生涯メールの提供が始まり，個人から部局レベルでのクラウドコンピューティングサービス類の利用が増えつつあることから，共用サービスについてもこうした外部サービスへのシフトが進むことが予想されます．今後は統合 ID システムの連係対象も多くが外部サービス化していくことを視野に入れながら，システムの改善や運用面での模索を続けていきたいと考えています．

参考文献

[1] 中山仁: 全学統合 ID 管理システムの概要，九州工業大学情報科学センター広報第 23 号，pp.19–22，2011 年