L-053

大学のユーザ認証システムの統合
－大阪教育大学の場合－
Integration of Authentication System in University
－Case Study of Osaka Kyoiku University－

宇土 喬浩†　　松井 聰治†　　佐藤 隆士‡
Takahiro UTO　Kikuji MATSUI　Takashi SATO

1．はじめに

学生や教職員が教育, 研究, 業務などの分野でコンピュータを使用する際, 必ずユーザ ID とパスワードの入力を要求される. これは対象の正当性を求める検証であり, 個人が所有するコンピュータ上の情報を不特定多数の第三者から保護するために必要不可欠なものである. この検証を認証と呼び, 認証の際には個人を特定するための ID やパスワード等が予めコンピュータ上やシステム上に管理されていなければならない.

大阪教育大学の認証システムは, 各運用システムごとに認証 ID とパスワードが全く別々に管理されているため, 利用者はそれぞれ異なる ID と異なるパスワードを自己管理する事になる. そのため, 新システムの導入, 拡張の度に新しい ID と新しいパスワードを保持する事になり, ユーザの負担増, 作業効率, 利便性の低下が問題視されている. システム側も新システム導入の度にユーザ管理をしなければならないため, 運用上の負担も大きく, また, 個人情報を複数のシステムで管理するため, 常にセキュリティホールや不正アクセスなどの危険要素を抱える事になる. 今回これらの問題の解決策として大学が管理する ID やパスワード, それに付随する個人情報を一箇所に統合して管理する統合認証システム[1, 2, 3]を提案し, 設計, 構築テストを行った. 本稿では初めに統合認証システムの導入から構築まで, 続いて統合認証システムへのユーザデータの移行について説明する.

2．統合認証システム導入の目的

前述の問題を解決するため, 本研究の目的を以下に挙げる.

(1) 利用者 ID, パスワードの統一, 共通化によるユーザの管理負担軽減, 及び個人情報管理業務の効率化.
(2) 新システム導入の際の連携の容易化.
(3) シングル・サインオンによる利便性の向上.
(4) 認証機構の統合に伴うセキュリティの強化.

3．統合認証システム

統合認証システムを実装するため, システム上にディレクトリサービスを提供する LDAP[4]サーバ, Windows 互換のサービスを提供する Samba[6]サーバを構築する. ここで, LDAP とはネットワークを利用するユーザ名やマシン名などの様々な情報を管理するディレクトリサービスにアクセスするためのプロトコルである. Samba には LDAP サーバとしての機能は備わっていないため, Samba, LDAP 間のデータベース連携を支援する smbldap-tools[7]を導入する.

† 大阪教育大学 大学院教育学研究科 総合基礎科学専攻 数理情報コース

‡ 大阪教育大学 情報処理センター

3.1 設計

システムの OS は Fedora Core 5[8]を使用し, LDAP サーバと Samba サーバを同一システム上に構築する. クライアントの OS は Windows XP Professional, Fedora Core 5, FreeBSD を使用し, 統合認証システムにドメイン参加させた後, 認証(ドメイン認証)を行う. システム構成を図 1 に示す.

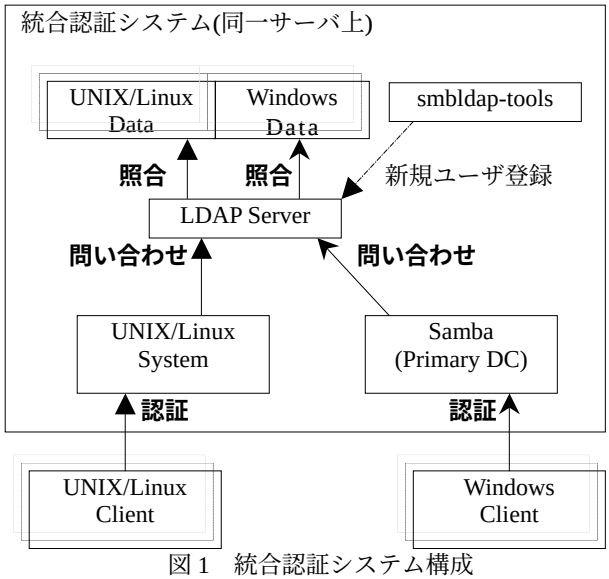

図 1　統合認証システム構成

3.2 システム構築

システムの構築を以下の手順で行った.

(1) LDAP サーバの構築, 起動, システム内部認証方式の変更.
(2) Samba サーバの構築, 起動.
(3) Samba-LDAP 間の連携.

(1)では, LDAP サーバ構築後, 認証時に LDAP サーバの情報を参照するようにシステム内部の認証方式を変更した(表 1). 変更方法は, 自動で認証方式の変更が可能な authconfig を使用した. これにより passwd, shadow ファイルに登録されているデータと LDAP データベースに登録されているデータを認証時に参照するようになる.

表 1　システム内部認証方式

	変更前	変更後
passwd	files	files ldap
shadow	files	files ldap
group	files	files ldap

(2)では, Windows のログオン認証を実現するために Samba サーバに PDC(プライマリドメインコントローラ)の

機能を付加させて構築する. また, ユーザが使用するコンピュータは必ずしも同一のコンピュータであるとは限らない事, ユーザが設定の異なる複数のコンピュータを利用する事を考慮し, プロファイルは移動プロファイルではなく固定プロファイルに変更し, Windows ログオン時にシステム上のホームディレクトリをネットワークドライブとして接続するようにした(図 2).

```
logon home =
logon path = C:\*****\profile
logon drive = z:
```

図 2　固定プロファイル設定(一部)

(3)では, LDAP 側, Samba 側で Samba-LDAP 間の連携作業を行うために smbldap-tools を導入した. これにより, UNIX/Linux, 及び Samba/Windows ユーザデータの追加, 変更, 削除をコマンド操作で行うことが可能になり, 自動的に LDIF 形式に従って LDAP データベースに登録される. 但し, smbldap-tools は管理者, マシンの追加, ユーザデータを LDAP データベースに移行した後のユーザデータ修正で使用する事とした

4．ユーザデータ移行

ユーザデータ(ここでは認証に必要な ID, パスワード等のデータを指す)移行に関しては, 既存のユーザデータをそのまま統合認証システムに移行する案と, 統合認証システムに新たにユーザを新規作成する案が提案されたが, 後者の場合, 新規登録, 新規パスワードの設定と, 利用者へのパスワード変更通知等に多くの時間と手間を要するため, 既存するユーザデータをそのまま統合認証システムに移行させ, 利用者がこれまで使用していた ID とパスワードで統合認証システムを利用できるよう試みた.

ユーザデータの移行は, 既存のシステム(Solaris)上のユーザデータ(pasawd, shadow)を LDIF 形式に書き換え, ldapadd コマンドを使用して LDAP データベースに登録した. SID 等の Samba 固有のオブジェクトクラスは LDAP データベース追加後に smbldap-usermod コマンドを使用してオブジェクトを付加した(図 3). なお, パスワードの暗号フォーマットは既存のユーザデータのパスワード暗号フォーマットに従い, CRYPT で定義した.

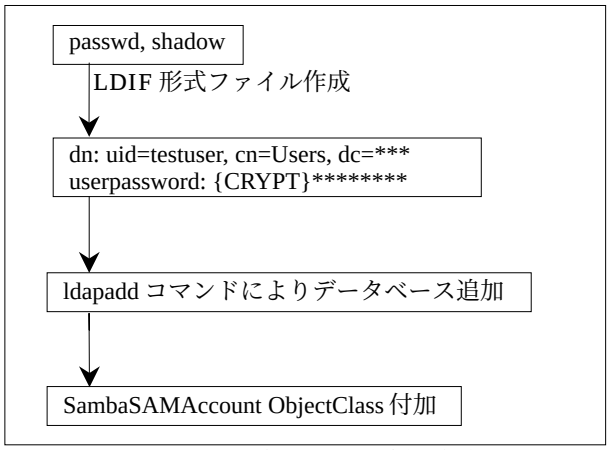

図 3　既存ユーザの移行手順

この移行手順に従い, サンプルユーザデータを用いて統合認証システムに移行させた結果, UNIX/Linux 間の認証(サービスも含む)に成功したが, Samba/Windows 間の認証に失敗した. これは, UNIX/Linux で扱う暗号パスワードと Samba/Windows で扱う暗号パスワードが異なるためであり, 統合認証を実現するためには LDAP データベース上に 1 つの ID に対し 2 種類の暗号パスワード(UNIX/Linux パスワード, Samba/Windows パスワード)を登録しなければならない(表 2).

表 2　LDAP データベース上のパスワード管理

	既存ユーザ	新規ユーザ
CRYPT(Password)	○	○
sambaNTPassword	×	○
sambaLMPassword	×	○
UNIX/Linux 認証	○	○
Samba/Windows 認証	×	○

5．まとめと今後の課題

本稿では, 学内の利用者 ID とパスワードの統一を図るための統合認証システムの構築方法とユーザデータの移行について述べた. 結果として, 統合認証システムによる UNIX/Linux 間認証が実現できた. しかし, Samba/Windows 間認証に関しては, **4**.でも取り上げた通り認証ができない状態である. この問題を解決するために, 既存の Windows Server 上で管理されているユーザデータを統合認証システムに移行させる手法による UNIX/Linux+Samba/Windows データベースの構築に取り組んでいる. この手法により, UNIX/Linux 認証は **4**.で扱ったデータを, Samba/Windows 認証は Windows Server 上で管理されているデータを照合できるのではないかと考えている. また, ユーザデータの複製を行うための複製サーバの構築, サーバ間ネットワークの整備など, セキュリティを強化するための対策も行わなければならない.

参考文献

[1] 奥村 勝, 本山 聡, 三河 邦夫, 福岡大学における統合認証システムの構築と運用について, 情報処理学会研究報告 2006-DSM-40, Vol. 2006, No.38, pp.7-12 (2006).
[2] 葛生 和人, UNIX-Windows 統合認証, 名古屋大学情報連携基盤センターニュース Vol. 6, No.2, pp.168-189 (2007.05).
[3] 江藤 博文, 只木 進一, 総合情報基盤センター新システム概要, 学術情報処理研究 No.10, pp.75-80 (2006).
[4] 稲地 稔 他, LDAP Super Expert, 技術評論社, pp.15-56 (2006).
[5] OpenLDAP, http://www.openldap.org/
[6] Samba, http://us3.samba.org/samba/
[7] SMBLDAP-TOOLS Addons, http://smbldap-addons.sourceforge.net/
[8] Fedora Project, http://fedoraproject.org/