オープンソースによる統合認証系の構築と運用

奈古屋広昭、松村芳樹、入来院ひさ子、鈴木令子、鷹野三千代
一橋大学総合情報処理センター†

概要

2003 年 4 月から運用を開始した、一橋大学総合情報処理センターの統合認証系は OpenLDAP や Samba のようないわゆるオープンソースなソフトウェアを活用して構築されている。本稿では、この統合認証系の構築と運用についての事例を報告する。

Making and operating of an integrated authentication system by open sources.

Hiroaki Nagoya, Yoshiki Matsumura, Hisako Irikeen, Reiko Suzuki, Michiyo Takano
Computer Center, Hitotsubashi University

Abstract

An integrated authentication system of the Computer Center, Hitotsubashi university, which started operation from April, 2003. The integrated authentication system are development by “Open Source” softwares such as OpenLDAP, Samba etc. This paper reports the example about making and operating of this integrated authentication system.

1 はじめに

一橋大学は約 7000 人の構成員 (学部生 5000 人・大学院生 1500 人・教職員その他 500 人) を抱える社会科学系の大学院大学である。全学共同利用施設である総合情報処理センターはこの 7000 人の利用者に対して

- ネットワークアクセス
- メールサーバ
- UNIX サーバ
- Windows 端末群
- WBT(Web Based Trainning) 支援サーバ

といった各種サービスを提供している。このようなサービスの運用には、利用者を識別するための統合認証系の存在が望ましい。しかし、従来、本学にはそのような用途向けの既存認証系は存在しなかった。

そのため 2003 年度に総合情報処理センターの研究教育支援システムが全面更新されるのを機に、センターサービス全般に対する統合認証系を導入するという方針が立てられた。

2 統合認証系に求められる要件

一般論および各種実装例については先行研究が多数ある [1, 2, 3, 4] が本稿では触れない。本学での統合認証系には以下の要件が必要とされた。

2.1 旧認証系からの認証情報の引き継ぎ

2002 年度末まで使われていた総合情報処理センターの旧研究教育支援システムは UNIX 環境と Windows 環境に大別されていたが、両環境での統合認証実現に「スルー PASS」[5] という商用製品を導入・利用していた。その結果、総合情報処理センターのアカウント保有者には

1. アカウント名 (個人識別 ID)
2. パスワードの UNIX-crypt ハッシュ (UNIX サーバの shadow ファイルに保存)

† 一橋大学総合情報処理センター / Computer Center, Hitotsubashi University
cc-adm@cc.hit-u.ac.jp

3. パスワードの NT パスワードハッシュ (Windows PDC 内に保存)

という 3 つの認証情報が存在することになった。数千人の利用者に対するパスワード再発行を避けるためには、これらの情報を引き継ぐ必要があった。

2.2 各種認証方式への対応

2.2.1 LDAP

統合認証の趨勢は LDAP にあると思われるので、将来性のためにも LDAP のサポートは必須であろう。また Samba を Windows Domain Controler として利用するためにも LDAP に対応しておく必要があった。

2.2.2 Windows Domain Controller

約 200 台のディスクレス Windows XP 端末の管理には Windows のドメイン認証を利用することになった (本学総合情報処理センターの運用能力からすると時期尚早と考えられたため Active Directory の導入は見送った)。そのため統合認証系はドメイン認証に対応できる必要があった。

2.2.3 NIS

導入予定の商用製品の認証システムが NIS のみに対応していたため、統合認証系は NIS に対応する必要があった。

2.2.4 RADIUS

既存のダイヤルアップ PPP サーバのために統合認証系は RADIUS にも対応する必要があった。

2.2.5 その他

既存のメールサーバや認証 VLAN については、統合認証系にあわせてソフトウェアや設定の変更をおこなうことで対応することとした。

3 オープンソースを採用した理由

このような要件を満たす統合認証系の具体的な実装として、本学ではいわゆるオープンソースなソフトウェア (MySQL, OpenLDAP, Samba etc) を核とする独自構築方式を選択した。これは以下のような理由による。

コスト削減 予算の都合上、商用製品による統合認証系の導入は厳しい状況にあった。そのためライセンス料金ゼロで導入可能なソフトウェア (必ずしもオープンソースである必要はない) を利用する実装しか選択肢が無かったという (非技術的ではあるが無視できない) 事情があった。

将来における自由の確保 本案件についての実装を検討していた時点では、本学における統合認証系の将来像を明確にすることができなかった。そのため特定の商用製品を導入することは将来における選択の自由を狭めてしまう危険が懸念された。その点、ライセンス料金ゼロなソフトウェアの組合せによる独自構築であれば、不要になった時点で「気軽に」廃棄できるため、そのような危険性は薄くなる。

高い安定性・情報の豊富さ 部品として採用したソフトウェア群はいずれも世界規模での広範囲な利用実績を誇っている。したがって実運用をおこなう上で、高いレベルの安定性を期待できると考えられた。また、そのソフトウェアについての様々な情報が非常に豊富であり容易に入手できる点も、選択決定のひとつの要因であった。

4 統合認証系の概要

4.1 マスターサーバ

IA32 アーキテクチャの PC に導入された Debian GNU/Linux[6] 上で動作している。統合認証系の全情報のマスターを保持している。

以下に述べる mysqld, slapd, slurpd, ypserv, ypbind が動作している。

4.1.1 MySQL サーバ (mysqld)

MySQL[7] を SQL サーバとして採用した。以下の情報をひとつのテーブルに保持している。

- アカウント名

- パスワード情報 (UNIX-crypt ハッシュ)
- パスワード情報 (NT パスワードハッシュ)
- GCOS フィールド
- アカウントの有効期限
- アカウントの状態 (有効・一時利用停止 etc)

利用者によるパスワードの変更　別マシン上で動作している WWW サーバ上に Apache-ssl[8], libauth-ldap[9], PHP[10] を用いた、利用者向けのパスワード変更インターフェースを用意している。現在のところ、変更したパスワードが統合認証系全体に反映されるのには最長で 5 分程度の時間がかかる。

マスター情報の管理　事務担当者向けに PHP ベースの管理インターフェースを用意し、そちらに以下のような日常的な管理を委託している。

- アカウントの新規登録・削除
- アカウントの一時停止状態のオンオフ
- パスワードの強制変更
- アカウントの有効期限の変更

4.1.2 LDAP サーバ (slapd, slurpd)

OpenLDAP[11] を LDAP サーバとして利用している。前出の MySQL サーバの情報を元に LDAP の情報を生成している。利用者のアカウントを保持するエントリのスキーマは以下のように設定した。

```
dn: uid=アカウント名,ou=USER,dc=...
objectClass: posixAccount
objectClass: shadowAccount
objectClass: sambaAccount
objectClass: inetOrgPerson
```

LDAP **データの生成**　MySQL データベースから現在有効なアカウントの情報のみを抽出し、LDIF に編集・入力することにより自動生成している。

LDAP **データの複製**　LDAP レプリカサーバへのデータ転送用に slurpd を動かしている。

利用者アカウント以外の情報　後述の Samba で利用するための Windows マシンアカウントや擬似ユーザアカウントのデータもこの LDAP サーバが保持している。これらについてはコマンドラインで LDIF を直接に編集する手動管理となっている。

4.1.3 NIS サーバ (ypserv, ypbind)

GNU/Linux NIS package[12] を利用している。現在のところ NIS のデータは LDAP データから 5 分毎に自動生成している。

4.2 Samba/Radius サーバ

sparc アーキテクチャの Solaris 8 マシン上で slapd, smbd, nmbd, ypserv, ypbind, radiusd が動作している。マスターサーバと本サーバが分離しているのはもっぱら性能上の理由であって、論理的には 1 台に集約可能である。

4.2.1 LDAP サーバ slapd

OpenLDAP を LDAP サーバとして利用している。マスターサーバのレプリカサーバとして動作している。

4.2.2 Samba サーバ (smbd, nmbd)

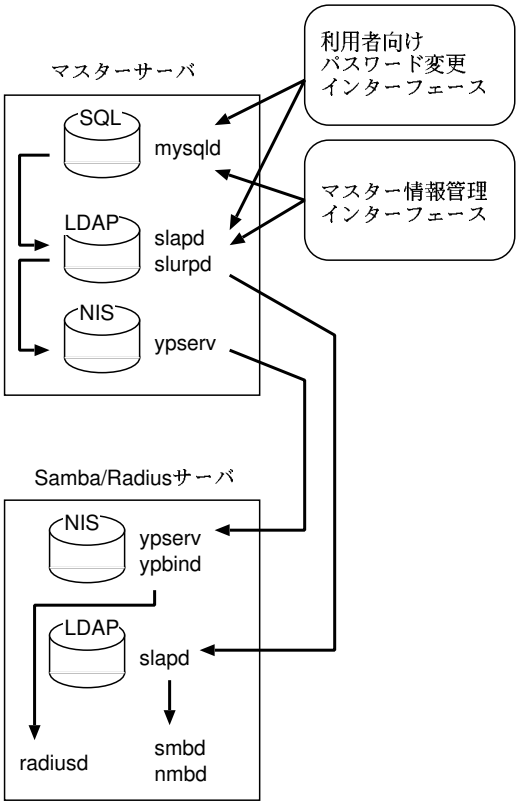
現在のところ samba-2.7.x-jp 系 [13, 14] を利用して Windows ドメインの PDC として運用されている。ドメイン認証に必要なデータはローカルで動作している slapd から引いている。なお、統合認証系とは直接には関係しないが、約 200 台の Windows XP 端末群に対するファイルサーバ (CIFS サーバ) としての機能も samba により提供している。

4.2.3 NIS サーバ (ypserv, ypbind)

Solaris8 附属の NIS パッケージを利用している。マスターサーバの NIS スレーブとして動作している。

4.2.4 RADIUS サーバ (radiusd)

DTC Radius[15] を利用している。認証情報は NIS (ローカルで動作している ypbind) から引いている。



5 統合認証系への移行

旧認証系から統合認証系への移行には次のような手順を踏んだ。なお、この移行作業の時点ではMySQL 関連部分が未完成だったため、一時的にLDAP 部分をマスター情報として運用を開始した。

1. 旧認証系のパスワード変更機能を停止。
2. Windows NT サーバ (PDC) からパスワード情報を抽出。
3. UNIX サーバからパスワード情報を抽出。
4. 2,3 の情報をマージしてアカウント情報のLDIF ファイルを作成。
5. 4 の LDIF ファイルをマスタサーバ上のLDAP データベースへ入力。
6. 各サービスを統合認証系へ接続。
7. 後日、マスタサーバ上の MySQL 部分が動作し始めた段階で、LDAP 側からアカウント情報を抽出・編集して MySQL 側へ入力。

本学のような中規模校ではアカウントの件数は 1 万に満たないため、1-5 の過程は数時間で終了した。

6 統合認証系を利用したサービスの現状

現在、本統合認証系を利用して提供されているサービスは次のようになっている。いずれも総合情報処理センター直轄のサービスであるが、今後は学内他組織への認証サービス提供も検討している。

6.1 NAS

利用者向けのデータストレージサービスとしてNAS (富士通 NR1000) を 1 台導入している。これについては NFS と CIFS 両方でのアクセスがあるため統合認証系の NIS および Windows ドメインを利用している。

6.2 Windows XP 端末群

約 200 台のディスクレス Windows XP 端末を導入したので、これらの端末認証に統合認証系のWindows ドメインを利用している。

6.3 プリンタ課金システム

プリンタ課金システムとして Ridoc IO Gate[16] という商用製品を導入した。このシステムは NIS にのみ対応しているので、統合認証系の NIS クライアントとして動作させている。

6.4 WBT 支援サーバ

学内でおこなわれる Web Based Trainning を支援するために webclass[17] という商用製品を導入した。このシステムは NIS / LDAP に対応しているが、現在は統合認証系の NIS クライアントとして動作させている。

6.5 UNIX ワークステーション

研究教育支援用の UNIX ワークステーションとして Solaris8 マシンが 1 台導入された。現在は統合認

証系の NIS クライアントとして動作しているが、将来的には LDAP クライアントへと移行したいと考えている。

6.6 WWW サーバ

OS としては Debian GNU/Linux を、HTTP サーバとしては apache-ssl を採用している。利用者認証をおこないたいエリアについては libauth-ldap モジュールにより統合認証系の LDAP クライアントとして認証をおこなっている。

6.7 メールサーバ

6.7.1 SMTP サーバ

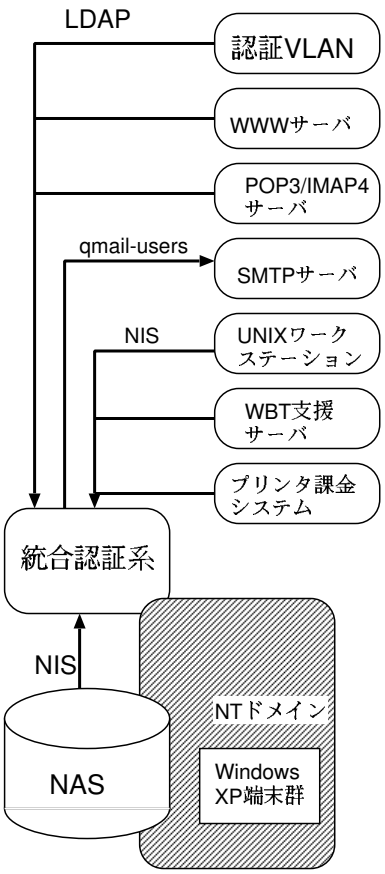
OS としては Debian GNU/Linux を、MTA としては qmail[18] を採用している。現時点では認証をおこなっていないが、利用者個々のメールボックスを特定する必要があるのでマスターサーバの MySQL データベースから `qmail-users` ファイルを自動生成して利用している。将来の SMTP AUTH などの導入時には LDAP クライアントとして動作することになるであろう。

6.7.2 POP3/IMAP4 サーバ

OS としては Debian GNU/Linux を、POP3/IMAP4 サーバとしては courier[19] を採用している。統合認証系の LDAP クライアントとして動作している。なお性能上の理由から本サーバについては LDAP のレプリカサーバをローカルに動かしている。

6.8 認証 VLAN

本学では 2002 年 6 月から OpenSSH[20] ベースの認証 VLAN を運用している [21, 22]。認証には PAM を利用しているので容易に LDAP 対応へ移行できた。現在は統合認証系の LDAP クライアントとして動作している。



7 まとめ

7.1 自己評価

高品質なオープンソースソフトウェア群を部品として活用することにより、いろいろな意味 (マンパワー・技術力・予算 etc) で資源不足である本学のような組織でも、実用に耐える統合認証系を構築・運用することができた。

7.2 今後の課題

いままで述べてきた本学の統合認証系については、以下のような課題が残されている。今後はこれらの課題解消に向けて努力したいと考えている。

7.2.1 安定稼働性の向上

本統合認証系は 2003 年 3 月末から運用を開始したが、次の一点を除いてはシステム障害など無く順

調に稼働している。

残念ながら Samba/Radius サーバ (Solaris8) についてはマスタサーバ側である程度の量 (だいたい 100 件以上) のデータ更新をおこなうと、ローカルな slapd が暴走状態に落ちいるという現象が数回観察されており、現在解決の目処が立っていない。本件については Linux サーバへの入れ替えも視野に入れた対応を検討中である。

7.2.2 冗長構成の導入

本統合認証系には現在のところ一切の冗長構成は導入されていない。Windows ドメインについては BDC の立ち上げ、LDAP/NIS についてはレプリカ/スレーブサーバの適切な配置、といった形で冗長度を上げることにより対障害性の向上が見込まれると思われる。

7.2.3 セキュリティ向上

本統合認証系そのものを守るという観点からは、現状のパケットフィルタリングや MySQL / OpenLDAP 独自のアクセス制限機構に加えて、サーバ間通信の SSL/SSH による暗号化・サーバ認証などの方策も導入した方がよいと思われる。

また利用者向けには、パスワード以外の認証情報 (各種の公開鍵方式など) も利用できるようにしていきたいと考えている。

7.2.4 全学構成員への個人 ID の付与 (総背番号制) と学内認証基盤の確立

本学では、学部生・大学院生の場合、総合情報処理センターアカウントのアカウント名 (= 本統合認証系のアカウント名/利用者識別 ID) は学籍番号と連動している。そのため転部や進学などで所属が移り、学籍番号が変更されるとアカウント名も変更されてしまうという弊害がある。

この難点を解消するためには、本学の構成員全員に対して所属の変更などに左右されない個人 ID を割り振る必要がある。この問題については技術面よりは事務的・政治的な非技術面が主となるので、本学事務局の主導による「全学構成員データベース」および「総背番号制」の整備計画が現在進行中である。将来的には本統合認証系におけるアカウント名としてこの背番号を用い、各種の個人情報は構成員データベースから採取する、という形での連携により両者があわさって学内認証基盤となる予定である。

8 おわりに

LDAP の構築と運用については主に [11, 23] を参考にした。本統合認証系の構築について協力いただいた富士通 (株) に感謝の意を表する。

参考文献

[1] 広島大学全学電子認証システム, 広大フォーラム 2003.8 月号 (No.377), http://home.hiroshima-u.ac.jp/forum/2003-8/
[2] 江藤博文, 渡辺健次, 只木進一, 渡辺義明. 大学における情報基盤整備の中核となる統合認証システム. DSM シンポジウム 2002, 2002.
[3] 岡部成玄, 山本裕一. 教育用基盤としての情報システム. DSM シンポジウム 2001, 2001.
[4] 倉前宏行, 島野顕継, 木村彰徳. ディレクトリサービスを用いた教育用 PC クラスタシステムの学生ユーザアカウント管理. DSM シンポジウム 2001, 2001.
[5] スルー PASS. 富士通北陸システムズ. http://www.fjh.fujitsu.com/tpass/
[6] Debian GNU/Linux, http://www.debian.org/
[7] MySQL, http://www.mysql.org/
[8] Apache-SSL, http://www.apache-ssl.org/
[9] libauth-ldap, http://www.rudedog.org/auth_ldap
[10] PHP, http://www.php.net/
[11] OpenLDAP, http://www.openldap.org/
[12] GNU/Linux NIS package, http://www.suse.de/~kukuk/
[13] Samba, http://www.samba.org/
[14] Samba-JP, http://www.samba.gr.jp/
[15] DTC Radius, http://www.dtc.co.jp/
[16] Ridoc IO Gate, http://www.ricoh.co.jp/
[17] Webclass, http://www.webclass.jp/
[18] qmail, http://cr.yp.to/qmail.html
[19] Courier Mail Server, http://www.courier-mta.org/
[20] OpenSSH, http://www.openssh.com/
[21] 奈古屋広昭. 社会科学系大学における認証付きアクセスポイントの構築と運用. 2002-DSM-25
[22] オープンアクセスフロア (仮称) 運用実験, http://www.cc.hit-u.ac.jp/monban/
[23] Internet2 Middleware Initiative, http://www.internet2.edu/