2005-11-18
第5回CAUA合同分科会
センター運用分科会

一橋大学における認証システム

奈古屋広昭
一橋大学総合情報処理センター

はじめに

- 2003.04 から運用している一橋大学総合情報処理センターの認証システムについて、です。
- というわけで2年半前の古いネタですいません。
  - しかも泥縄な仕様と実装
- 内容
  - 一橋大学の概要
  - 導入にいたる経緯
  - 実装の概略
  - 現状・課題・今後の展開
  - まとめ

一橋大学の概要

- 社会科学系の「総合」大学
  - 4学部・6研究科・1研究所・9センター
- 都内に3つのキャンパス
  - 国立・小平・神田
- ユーザ数 (2005-05-01現在)
  - 教職員: 614 (公式値だが、実際には若干怪しい数字)
  - 学部生: 4619
  - 大学院生: 1915
  - その他: 数百人？
  - 諸々合計で8000人程度？

導入以前(1)

- 国立大学の情報系センターには電算機借料という予算項目がある(あった)。
  - メインフレーム時代からの遺産？
  - 4-5年毎にシステム更新(いままでは。今後は？)
  - 一橋大学の場合は〇百万円/月
  - (ここでは)レンタルシステムと呼ぶ
- 主に教育系システムの構築・運用に費やされる。
  - PC端末・プリンタ・教材提示装置 etc
  - 各種サーバ・ネットワーク機器
  - …

導入以前(2)

- 1999.4 – 2003.3 のレンタルシステム
  - お役所なので入札 → 富士通(株)が落札
  - PC (Windows NT 4.0) が220台
    - NTサーバによるNTドメイン認証
  - プリンタ (s)
  - UNIXワークステーション(s)
    - DAS なディスクアレイ装置(250GB)
  - ネットワーク機器(s)
  - 経済統計データベース
  - …

導入以前(3)

- 一応「統合認証」となっていた。
  - (ここでは)統合認証 == 1アカウント+1パスワード
  - Single Sign On ではない
- 「スルーPASS」という商用製品を利用。
  - Solaris マシンと NTサーバが各々マスターとなっている。
  - アカウント登録やパスワード変更などの処理時に両マスターの同期をとるという仕組み(だったはず)。
  - 重大な問題は発生しなかったがマスターが2箇所というのはなにかと不便であった。

導入以前(4)

- 運用中のイベント
  - キャンパスネットワークの全面更新(2001.7)
    - 簡易認証VLANの導入
  - ファイルサーバの商用製品(TAS)が動かなくなったのでsamba に入れ替え
  - 学内からのセンターシステムとの連携要請
    - ストレージ、認証、…

レンタルシステム更新計画(1)

- 2003.4 に更新予定のレンタルシステムについての計画を検討し始めたのが 2002 後半頃。
- 主要な要求項目
  - PC は「素の」Windows マシン x 200台強
    - ディスクレスにしたい
  - ストレージは一極集中、なるべく容量大
  - アカウント管理の一元化
  - その他もろもろ
    - プリンタ、各種ソフトウェア、経済統計データベース、Web Based Training System、…

レンタルシステム更新計画(2)

- いくつかの業者さん(含むCTC)に仕様の詰めや見積をお願いして、比較検討してみた。
- どうも予算が足らないぞ…
  - ボスレベルでの政治力行使
    - 学内予算分捕り → 成果上がらず
    - 「総合情報処理センター化」による予算増を期待（後述）
  - 現場レベルでの準備
    - 機能的に分離できそうなところを切り分ける
    - 手持ち資源でできるとこまでやってみる
      - 将来予算がつくまで凌げればよし

レンタルシステム更新計画(3)

- 入札仕様確定 (2002.7)
  - サーバ系の一部(DNS/メール/Web etc) とアカウント管理系のコアは仕様から外した。
  - ディスクレス Windows XP PC x 214
    - Samba 2.x (相当)でNTドメインを構築し参加できるように指定
  - 2TBのNAS
    - Samba 2.x (相当)のNTドメインに参加できるよう指定
  - その他もろもろはとくに削らず
    - 削れなかった、というべき
- 入札～開札 (2002.8 – 9)
  - けっきょく富士通(株)のみが入札・落札、数十万円/月の予算超過

レンタルシステム更新計画(4)

- 仕様から外した部分については別予算での導入を期待していた。
- 「総合情報処理センター化」による予算増がある！
  - 国立大学特有のハイアラーキー
    - 大計センター > 総合情報処理センター > 情報処理センター
    - 基盤センターとかいろいろできているので現在では崩壊？
- 2002年度までは総合情報処理センターに「格上げ」されると予算増、そのかわり年2校程度。
- 2003年度は一橋大学を含めて5校が「総合」化。ただし予算は据え置き:-(
  - そして2004年度からは「国立大学法人」体制がスタート

レンタルシステム更新計画(5)

- 仕様から外した部分については自力でなんとかするしかないなあ。
  - ハードウェアはPCを掻き集めて都合をつける
  - Debian GNU/Linux を導入
  - 定番の apache, qmail, courier, samba, openldap, djbdns, mysql などを導入・設定
  - 業者担当のレンタルシステムとの連携
- 2003.4 から運用開始、なんとか大事に至らず今日までこれました。

認証システム(1)

- 仕様(最低限)
  - NTドメイン
  - LDAP / NIS / RADIUS
  - での認証が同一ID/パスワードで可能
  - アカウント情報が機械的に取り出せる
  - アカウント情報の登録・更新・削除ができる
  - ユーザ向けのアカウント情報変更インターフェース
- 基本的には Linux の上にでも samba / openldap あたりを導入すればOK

認証システム(2)

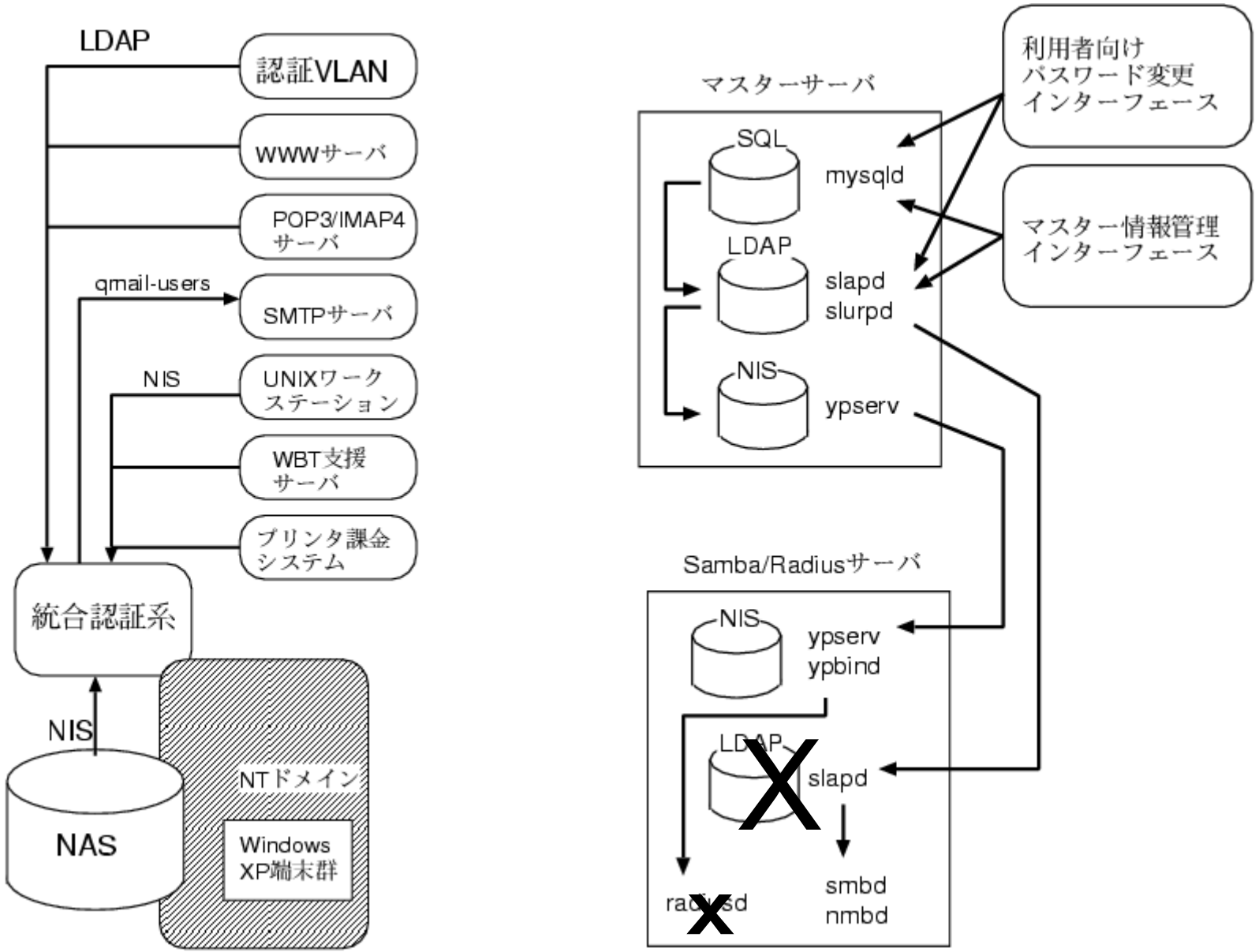
- 最初の実装
  - LDAP
    - Openldap on Debian GNU/Linux (マスター)
    - Openldap on Solaris 8 (replica, レンタルシステムに含む)
  - NTドメインPDC
    - Samba 2.x on Solaris 8 (レンタルシステムに含む）
    - “ldap server” として LDAP サーバを指定
  - NIS / RADIUS
    - Debian パッケージをそのまま利用
    - LDAP からデータをとってくるように若干修正
  - ユーザインターフェース
    - PHP4 + apache-ssl + mod_ldap で簡易なものを自作

認証システム(3)

- 実運用してみての不具合
  - Openldap on Solaris 8 がどうも安定しない
    - 高負荷がかかると yield() 暴走 → kill -9 → データベース再構築
  - マスター情報が LDAP 上というのはいろいろと具合が悪い(ような気がした)
    - アカウントの状態遷移のエミュレートが困難(な気がした)
    - 大量のデータ取得には意外と時間がかかる(ような気がした)
      - 現行システムでは約1万件のエントリ全取得に数十秒かかる
    - UidNumber を一意に割り当てるのが面倒

認証システム(4)

- 現在の実装
  - SQL
    - Mysql on Debian GNU/Linux (マスター情報保持)
  - LDAP
    - Openldap on Debian GNU/Linux (マスター)
  - NTドメインPDC
    - Samba 2.x on Solaris 8 (レンタルシステムに含む）
    - “ldap server” として LDAP サーバを指定
  - NIS / RADIUS
    - Debian パッケージをそのまま利用
    - LDAP からデータをとってくるように若干修正
  - ユーザインターフェース
    - PHP4 + apache-ssl + mod_ldap で簡易なものを自作


LDAP
認証VLAN
WWWサーバ
POP3/IMAP4
サーバ
qmail-users
SMTPサーバ
NIS
UNIXワーク
ステーション
WBT支援
サーバ
プリンタ課金
システム
統合認証系
NIS
NAS
NTドメイン
Windows
XP端末群
マスターサーバ
SQL
mysqld
LDAP
slapd
slurpd
NIS
ypserv
利用者向け
パスワード変更
インターフェース
マスター情報管理
インターフェース
Samba/Radiusサーバ
NIS
ypserv
ypbind
LDAP
slapd
smbd
nmbd

ちょっとテクニカルな話

- MySQL テーブル構造
- OpenLDAP: スキーマ
- NIS
  - 5分毎に LDAP上の全データを検索して変換
    - 一時しのぎのつもりだったので…
- qmail-users
  - SQLデータからメール配送設定を生成
    - つまり静的なデータベースを使っている
- NFS
  - ユーザのホームディレクトリは NAS 上に配置、それを認証マスターサーバも NFS マウントしている
    - ユーザホームディレクトリの作成・変更・削除を直接実行可能

ハードウェア

- PC サーバ (Debian GNU/Linux sarge)
  - Pentium-III/800MHz x 2
  - RAM: 512MB → 1024MB
  - Disk: RAID1 SCSI (36GB)
  - NIC: 100BASE-TX
- Sparc サーバ (日本語Solaris 8)
  - Fujitsu PRIMEPOWER 200
  - SPARC64/600MHz x 2
  - RAM: 1024MB → 2048MB
  - Disk: RAID1 SCSI (72GB)
  - NIC: 1000BASE-T

現状

- 2005-11-13 現在
  - 13873アカウント、内有効なものは8156アカウント
  - この認証システムを利用しているサービス
    - NAS (NTドメイン / NIS)
    - Window PC 群 (NTドメイン)
    - プリンタ利用枚数制限 (NIS)
    - Solaris 8 ワークステーション群 (NIS)
    - メール系のシステム (SQL / LDAP)
    - 認証VLAN (LDAP)
    - Web系のシステム(LDAP / NIS)
    - センター外からの利用
      - 附属図書館、ロースクール

課題

- 信頼性・冗長性の欠如
  - ハードウェア・ソフトウェア共に single failure point だらけ
- 管理インターフェースが貧弱
  - 直接 LDAP や SQL を操作する部分が多く、自動化不足
  - ロギングをほとんどおこなっていない
- セキュリティ対策が弱い
  - サーバや通信路の安全性確保
  - パスワード一元化のデメリット
- 細かいところ
  - SQLマスター化が不完全、Samba 3、NIS を捨てたい
- (技術的な話ではないが)運用体制が確立されていない
  - 総背番号制、1ユーザ1アカウント、…

今後の展開

- 大学の情報基盤整備には全学的なアカウント管理の一元化が必須(だと思う)
  - 統合認証から Single Sign On へ
  - ユーザ情報を必要とする学内各種データベースとの融合
  - 肌理細かなアクセス・サービスレベルのコントロール
- ということで来たる2006年にはドンと予算がついてまともな商用認証システムに全面更新の予定
  - 政治的事情により R, F 社さんあたりが先行していますがガチガチクローズな発注にはしないはずなので CTC さんもよかったら応札してください:-)
  - それまで、もうしばらくの間は現行システムを維持

まとめ

- いわゆるオープンソース製品の部品としての完成度の高さ
  - 開発コミュニティのみなさまに感謝！
- 連携部分だけをちょこちょこと自作すれば、この程度の実用システムをはなんとか構築・運用できる
  - オープンなプロトコルの有難さ
- スケーラビリティ
  - 一定規模以上のシステムでは重要な問題
    - ex. 東大ECCSとは端末数が1桁違う
  - その閾値は年々上昇？ → 適当に作ってもとりあえず動く範囲が拡大？
    - 本稿の内容は閾値以下の範囲だったと思う

Q & A