名古屋大学のユーザ認証基盤の現状紹介

名古屋大学情報連携基盤センター　平野 靖
名古屋大学大学院多元数理科学研究科　内藤 久資
名古屋大学情報連携基盤センター　梶田 将司
名古屋大学情報連携基盤センター　小尻 智子
名古屋大学情報連携基盤センター　間瀬 健二

サイエンティフィック・システム研究会システム技術分科会2005年度第2回会合資料　2006/1/18

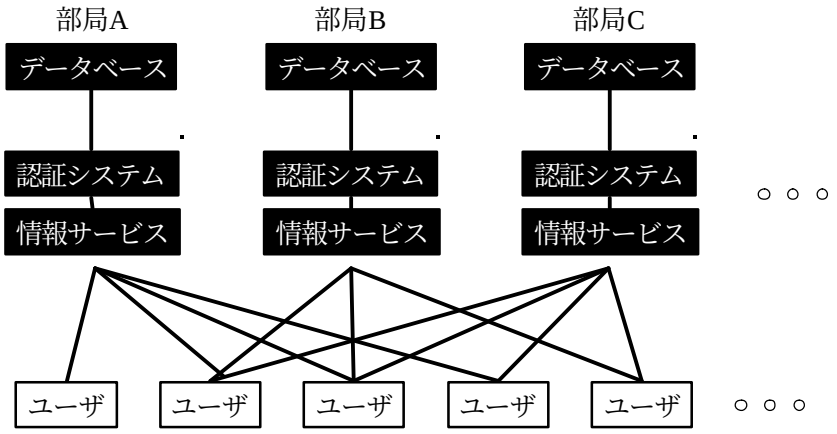
大学の事情

- 縦割り的
- 各部局が独自に行動
- トップダウン的な指示はなじまないことが多い

いくつものID

- 大学(部局)の情報化
- 個々の部局が運用する情報サービスのために個別にIDとパスワードを発行
- 1人にいくつものIDが付与

部局ごとのID体系



複数のIDがあることの問題点

- 複数のIDを覚える手間をユーザに強いる
- 手帳やディスプレイに貼られたポストイットにIDとパスワードの組を記述することなどにより，これらの漏洩の危険性を拡大

全学的に統一されたID体系が必要

全学ID

- 名古屋大学の全学的に統一されたID体系
- 学内情報サービスプロバイダ*に認証機能とユーザ情報の提供
- 情報連携基盤センターがサーバを管理・運用
- 事務局総務企画部人事労務課，財務部情報企画課，および学務部の協力

*全学向け・部局向け情報サービスを提供する名古屋大学の職員，あるいは学内団体

名古屋大学の規模(1)

- 学部学生　9,800名
- 大学院学生　6,000名
- 研究生　1,000名
- 教員　1,800名
- 事務職員・技術職員　1,500名
- 非常勤職員　3,000名

平成17年5月1日現在

名古屋大学の規模(2)

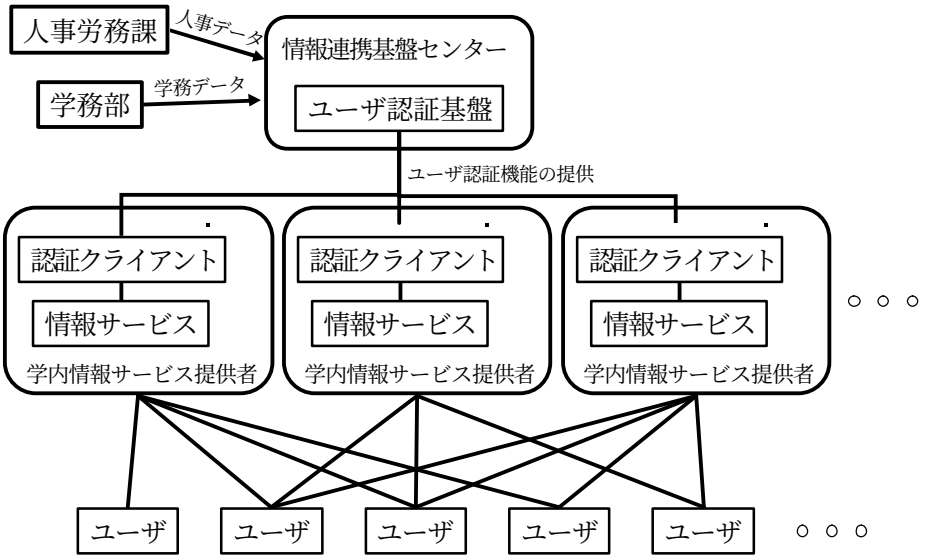
- 新規卒業生　2,200名
- 新規修了生　2,500名

- 既卒業生(新制)　76,500名
- 既卒業者(旧制)　4,100名
- 既修了生　41,000名

平成16年度現在

(注：現在は全学IDの付与を行っていない)

全学ID運用部局



全学IDのメリット (学内情報サービスのユーザ)

- 誰が提供するサービスであっても, 共通のIDとパスワードを用いて, サービスを受けることができる.
- 究極的には大学内で使用するIDとパスワードは1つのみでよい.

全学IDのメリット
(学内情報サービスプロバイダ)

- ユーザ情報の管理の手間を削減できる．とくに，IDとパスワードの生成や，異動による所属情報の変更，利用資格の付与・抹消などの手間から解放される．
- 氏名や所属部局などのユーザ情報をユーザに入力させたり，プロバイダが入力したりすることなく入手できる．

全学IDのメリット
(大学)

- 学内情報サービスに必要となる総所有コスト(TCO, Total Cost of Ownership)の低減化が実現できる

⇩

これまで必要以上に使われてきた情報化関係経費を別の目的や，さらなる情報化などに使用できる．

ユーザ認証システムを使うには

- 情報連携基盤センターにディレクトリサービス利用申請書を提出
- 学内情報サービスプロバイダは責任者, および実務担当者の氏名 ･所属などを明記を要求

ユーザ認証システム

- 学内情報サービスの種類に応じた2つのユーザ認証システム
  - LDAP (UNIXやWindowsのログインなど)
  - CAS (主にWebアプリケーション向け)

*CASサーバが用いるユーザ情報はLDAPサーバに格納されているため, 認証用データベースは同一

LDAPとは

- Lightweight Directory Access Protocolの略
- 電子的な「電話帳」と通信し，各種の情報を読み書きするためのプロトコル
- 運用目的にあわせて任意の情報を追加可能
- ユーザを識別する属性とパスワード属性を使用することで認証に使用可能
- 任意の属性をLDAPクライアントに送信可能

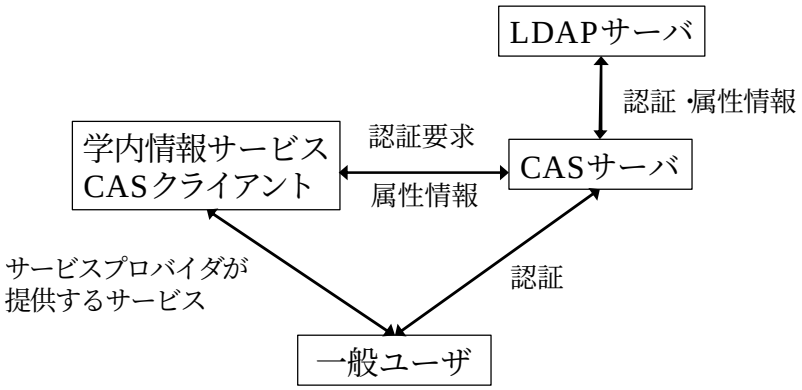
CASとは(1)

- Central Authentication Serviceの略
- 米国Yale大学が開発
- Single Sign-On (SSO)を実現可能
- 標準的なWeb技術だけを用いて実装可能
- ユーザインタフェースとしてWebブラウザを利用
- Java, PHP, Perl, PL/SQL, Pythonなどのための CASクライアント構築用のライブラリ
- 北米を中心に豊富な採用実績(2005年6月現在, 30を越える大学で採用)

CASとは(2)

- 認証情報はユーザ・CASサーバ間で通信
- 暗号化すべきは
  ユーザ・CASサーバ間と,
  学内情報サービス・CASサーバ間
  → CASサーバにのみサーバ証明書が必要
  →コスト削減可能

CASとは(3)



名大版CAS

- 強力な権限管理機構を付加

  CAS^2 (Central Authentication and Authorization Service)
- 権限管理情報は任意のデータベースに格納可能(名大ではLDAPサーバに格納)

LDAPを利用する学内情報サービスプロバイダ

利用実績(13)：

- 本部(2)
- 附属図書館(1)
- 理学部(1)
- 情報科学研究科(1)
- 情報メディア教育センター(2)
- 情報連携基盤センター(6)

利用例：

教育用計算機システム(情報メディア教育センター)

図書館システム(附属図書館)

CASを利用する
学内情報サービスプロバイダ

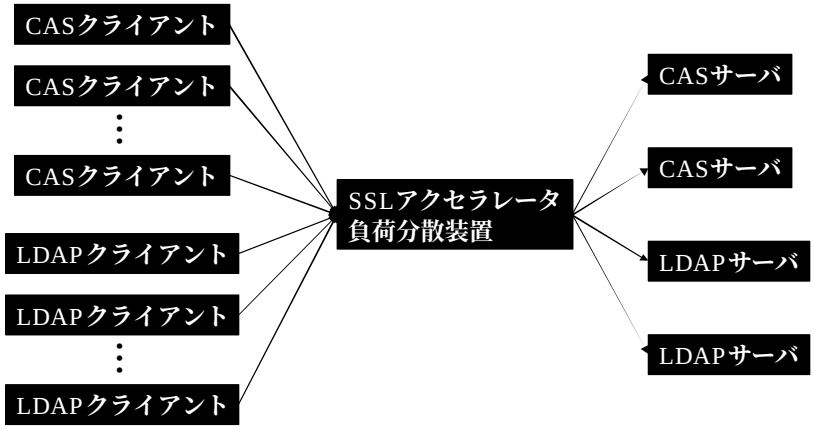
利用実績(9)：

- 本部(3)
- 法学部(2)
- 高等教育研究センター(1)
- 情報メディア教育センター(2)
- 情報連携基盤センター(1)

利用例：

WebCT(情報メディア教育センター)
教務システム(学務情報システム推進委員会)
大学ポータル(情報連携基盤センター)

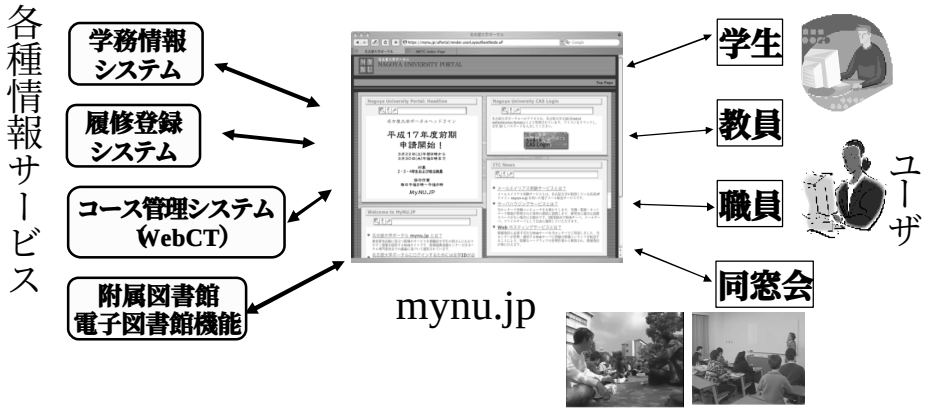
冗長化・暗号化



Single Sign-On

- ある学内情報サービスで一度認証を受けるだけで，他の学内情報サービスでは改めて認証を受ける必要がないシステム

Single Sign-Onによるワンストップサービス



全学IDにより，Single Sign-Onを実現

＊ 名大版CAS(CAS²)によるSSOの実現の仕組みについては，下記の文献を参照してください．
内藤ら：大学における統一認証基盤としてのCASとその拡張，情報処理学会論文誌(採録決定)

SSOの実績の例

- 教務システムにおける認証で利用
  - 平成16年度後期以降の成績入力
    平成16年度後期 :約1000人の教員(約4000科目)が19日間にわたって行った.
  - 平成17年度前期以降の履修登録
    平成17年度前期には約6500人(学部2～4年生)を対象に9日間にわたって行った.
- いずれの場合も別段の問題は発生せず.

まとめ

- 全学的に統一されたIDの必要性
- 名古屋大学での全学ID
- 名古屋大学のユーザ認証基盤の現状
  - LDAP,CAS

今後の課題(全学ID)

- 既存の学内情報サービスの認証機能の情報連携基盤センターが運用するユーザ認証基盤への移行
- 今後運用が開始される学内情報サービスにおいて全学IDを利用するように促す

今後の課題(CAS)

- CASの普及
- 他大学・機関などで動作しているCASサーバを経由して認証結果などの交換が必要となる.
- 大学間でのAuthentication, およびAuthorizationサービスの実現を目的としているShibbolethとの比較検討も必要
- 運用ツールの作成
- CAS^{2}のパッケージ化により, 他機関でも容易にCAS^{2}を利用できる状況にする計画

今後の課題(大学間連携)

- 国立情報学研究所, および全国7つの情報基盤センターが共同で各大学の認証システムを互換性を持たせる(CSI事業の一部(UPKI))
  - 共通の認証システムを作るのではなく, 各大学で独立の認証システムを持ち, それらが相互信頼
  - 各大学にCA
  - 国立情報学研究所にブリッジCA

謝辞

- 名古屋大学のユーザ認証基盤の一部はSun Microsystems社からの寄贈を受けた.
- CASの機能拡張に関しては下記の助成を受けた.
  - 文部科学省平成16年度委託事業「知的資産の電子的な保存・活用を支援するソフトウェア技術基盤の構築」研究開発課題「ユビキタス環境下での高等教育機関向けコース管理システム」(研究代表者:間瀬健二),
  - 文部科学省科学研究費基盤研究(A)「地域学術コンソーシアムにおけるe-Learning地域ハブに関する研究」(研究代表者:梶田将司, 課題番号:15200054)
- CASのパッケージ化は, 国立情報学研究所CSI(Cyber Science Infrastructure)経費の一部による.