

名古屋大学におけるアイデンティティ管理  
- 生涯IDとしての名古屋大学ID -

内藤久資

(Hisashi NAITO)

名古屋大学多元数理科学研究科  
名古屋大学情報連携統括本部情報戦略室

May 15, 2008

ITRC meet 23

# 共同研究者

---

- 全体

梶田 将司氏, 平野 靖氏, 間瀬 健二氏

- 名寄せ

太田 芳博氏, 田島 嘉則氏, 田島 尚徳氏

- 職員証・学生証

久保 仁氏

# Plan of Talk

---

- 名古屋大学 ID の目的
- これまでのとりくみ
  - 名古屋大学におけるアイデンティティマネージメント
- 認証基盤サービスとの関連
- 今後の改善と課題
- まとめ

# 名古屋大学 ID とは

- 名古屋大学構成員に対して一意的な ID を割り当てる
- 全学認証基盤の ID : 学内情報システムで利用可能
- ユーザの身分に関わらず一人 1 ID
- 「生涯 ID」として利用可能としたい
  - 卒業生・離職者に対するサービスにも適用可能
  - 一度名古屋大学 ID をもらったら, 身分が変わっても, 卒業・離職しても同じ ID を利用
- 将来は「図書館 Walk in User」なども対象としたい

# 以前の ID 体系

- 2007 年 12 月以前は「全学 ID」を利用
  - 学生： 学生番号をもとにした ID
  - 職員： 職員番号をもとにした ID
  - その他（研究生など）： 個別の ID
- 問題点
  - 身分が変わると ID が変更になる
    - サービスの継続が困難
  - 学生番号・職員番号が ID から推測可能
    - セキュリティ的な問題

# 全学 ID から名古屋大学 ID へ (1)

## ● 移行スケジュール

- 2008 年 1 月から名古屋大学 ID の利用を可能にする

## ● 移行内容

- 情報システムは名古屋大学 ID ・全学 ID のいずれでも認証可能とする
- 名古屋大学 ID ・全学 ID のいずれも同一のパスワードとする

# 全学 ID から名古屋大学 ID へ (1)

## ● 名古屋大学 ID の通知対象

- 在籍中の教職員学生（在籍中は全学 ID と名古屋大学 ID の両方を利用可能）
- 学生は 2008 年 4 月入学生から名古屋大学 ID のみ通知

## ● 全学 ID と名古屋大学 ID の例

- 教職員 (職員番号 12345678)
  - 全学 ID: t1234567
  - 名古屋大学 ID: ab0000112
- 学生 (学生番号 0601123456)
  - 全学 ID: s0112345
  - 名古屋大学 ID: ab0000114

## 全学 ID から名古屋大学 ID へ (2: 名寄せ)

- 同一人物が複数の全学 ID を所持している
  - 大学院生 & 非常勤職員 (TA, RA)
  - 正規教職員 & 非常勤職員 (所属部局以外で授業を担当)
  - 正規職員 & 大学院生 (職員が大学院に入学)
  - 複数の研究生 ID を持っている (年度更新をきちんとやっていない?)
  - 卒業・修了したはずの身分の ID が残っている
    - 研究生 ID & 正規学生 ID
    - 学部生の ID & 大学院生の ID

## 全学 ID から名古屋大学 ID へ (2: 名寄せ)

- 名寄せを行なうには各 ID の所有者情報が必要
  - 氏名（漢字・ヨミ・アルファベット表記）
  - 誕生日
  - 所属など
- これらの情報はホントに正しいの？
  - 氏名の表記はまちまち
  - 誕生日も入力ミスがありそう

# 全学 ID から名古屋大学 ID へ (2: 名寄せ)

## ● データソース

- 教職員：人事 DB（総務部人事労務課）
- （正規）学生：学生 DB（学務部学務企画課）
- その他：個別に申請

## ● データソースごとに表記ルールが異なる

- 氏名の表記方法が異なる
- 所属コードの体系が異なる

## 全学 ID から名古屋大学 ID へ (3: 関連した作業)

- 2007 年 秋： 職員録の電子化
  - 教職員の所属情報などを正しく格納する
- 2007 年 12 月： IC カード職員証の配布
  - 教職員の氏名表記
  - 職員証に名古屋大学 ID を記載する
- 2008 年 1 月： 全学メールの新システムへの移行
  - 主に学生の氏名（アルファベット）表記
  - メールアドレスを “familyname.firstname” 形式にする
  - 認証のベースに名古屋大学 ID を使う

# 全学 ID から名古屋大学 ID へ (4: 名寄せ TYPE I)

## ● 目的

- 既存の全学 ID から名古屋大学 ID への移行
- 複数の全学 ID を持つユーザを名寄せして一意的な名古屋大学 ID へ

## ● 手法

- 氏名表記 + 誕生日が一致すれば同一人物とみなす

## ● 問題点

- 氏名表記がまちまち
- 誕生日の入力ミスも発覚
- どの全学 ID の属性値を名古屋大学 ID へ移行するか？

# 全学 ID から名古屋大学 ID へ (4: 名寄せ TYPE I)

名寄せ状況		ユーザ数	割合
名寄せが不必要なユーザ		30,771 名	83.0%
名寄せが必要なユーザ	全学 ID を 2 つ付与	5,496 名	14.9%
	全学 ID を 3 つ付与	745 名	2%
	全学 ID を 4 つ付与	75 名	0.2%
	全学 ID を 5 つ付与	4 名	0.01%
	全学 ID を 6 つ付与	1 名	0.003%
	小計	6,321 名	17.0%

# 名古屋大学 ID はできたけど (名寄せ TYPE II)

- もうひとつのタイプの名寄せが必要
- 新入生・新規採用職員に対する名古屋大学 ID の発行
  - 学部から大学院へ進学, 大学院生が教職員として採用された
  - 既存の名古屋大学 ID を検索して, 新規発行対象者のみを選択する
  - 学生証・職員証, 全学メールアドレス, 教育用計算機システム ID の発行基礎データとなる
- 2008 年 4 月に大規模に実施
  - 氏名表記 + 誕生日をキーにした名寄せ
- とりあえず, 現時点では「問題なし」

# 名古屋大学 ID の新規発行方法

- 「正規」構成員

学生 DB, 人事 DB にデータが登録される

名寄せの実行

名古屋大学 ID 発行

- 研究生など

本人からの申請（将来は所属部局からの申請としたい）

名寄せの実行

名古屋大学 ID 発行

# 名古屋大学全学認証基盤

- 名古屋大学 ID を利用した認証基盤サービス
- 名古屋大学 ID ユーザ DB は LDAP に格納
- Authentication + Authorization + Single Sign On
  - LDAP および CAS<sup>2</sup> による Authentication
  - CAS<sup>2</sup> による Authorization, Single Sign On
- Directory Service
  - LDAP または CAS<sup>2</sup> による
- Web アプリケーションへの認証サービスは CAS<sup>2</sup> を推奨
- UNIX 認証に対しては “LDAP Hosting Service” を実施

# LDAP, CAS<sup>2</sup> を利用している学内アプリケーション数の推移

年度	LDAP	CAS <sup>2</sup>	合計	備考
2003	5		5	名古屋大学ポータル, WebCT, 全学メールシステム等
2004	4	4	8	CAS <sup>2</sup> 運用開始. 教務システム, 名古屋大学ポータル等で CAS <sup>2</sup> を利用
2005	3	4	7	教員プロフィール DB, 法科大学院学習支援システム等で CAS <sup>2</sup> を利用
2006	3	3	6	医学部会議室予約システム等で CAS <sup>2</sup> を利用
2007	2	2	4	利用予定を含む
合計	17	13	30	

# 全学認証基盤と名古屋大学 ID への移行

- 名古屋大学 ID への移行時には以下のポリシーを設定
  - 当面の間, 「全学 ID」でも「名古屋大学 ID」でも認証可能
  - 「全学 ID」でも「名古屋大学 ID」でもパスワードは共通

## LDAP へのデータの格納

```
dn: nagoyaunivid=名古屋大学 I D ,ou=user,o=nagoya-u  
nagIdNo: 「職員番号・学籍番号」  
NagoyaUnivID: 「名古屋大学 I D」  
ZengakuID: 「全学 I D」  
ZengakuIDs: 「名寄せされた全学 I D」(複数エントリ)
```

## LDAP Search

```
(|(NagoyaUnivID=%s)(ZengakuIDs=%s))
```

# 全学認証基盤とアイデンティティマネージメント

- 情報サービスが必要とするユーザ属性情報は認証基盤からのみ提供する
- 情報サービス側には余分なユーザ情報をもたせない
- 認証基盤は Authentication だけでなく, Authorization, Directory Service も行なっている.
- 認証基盤の各ユーザエントリに正しい属性値を格納する必要がある
  - 身分・所属情報などによるアクセス権限管理
  - 単なる所属情報だけではなく「兼務情報」も必要

## 問題点 (1: Provisioning の問題)

- ユーザ属性情報をいかにして正しく格納するか？
  - 適切な氏名表記を格納する必要がある
    - (明日の久保・Nの講演)
  - メタデータベースでの情報から修正する必要がある
    - 複数のメタデータベースを利用している
    - メタデータベースごとに format が違う
  - メタデータベースのレベルで整合性を取る必要がある
    - 氏名表記のルールが統一されていない
    - 所属を表わすコード体系が不整合である
- 研究生・短期滞在研究者などへの名古屋大学 ID 付与に関わる問題

## 問題点 (2)

- ユーザ属性情報をいかにして正しく格納するか？
  - 大学における「ユーザ属性」としては何が必要なのか？
  - LDAP のスキーマの言葉でまとめてみたい。
    - eduPerson Object class では不十分
- 整合性のある権限管理：ロールマネージメントの必要あり？
  - 誰がどのリソースにアクセス可能かを適切に管理したい

## 問題点 (3)

- 学務システムでの非常勤講師 ID
  - 職員番号・学生番号が内部 DB のキーとなっている
  - 非常勤講師には独自の ID を割り当てている
  - とりあえずは CAS<sup>2</sup> に機能を追加して逃げている
- 認証基盤とどうやって整合性をとるか？

# まとめ

- 名古屋大学 ID の導入・運用に関連する話題をもとに名古屋大学での IdM の枠組みを解説した
- 最も重要な問題は「人の属性値を正しく設定すること」(Provision) である.
- ソフトウェアを導入すれば解決できるわけではない
- IdM の問題点は名古屋大学固有の問題ではない
  - どのこの大学でも困っているはず
- 各大学の取り組みを共有したい

- N, 梶田, 平野, 間瀬, 名古屋大学における CAS<sup>2</sup> を核としたアイデンティティマネジメントの現状と課題, インターネットコンファレンス 2007 論文集
- 梶田, 太田, 田島, 田島, 平野, N, 間瀬, 生涯利用可能な名古屋大学 ID の導入に伴う名寄せ問題とその解決法, 情報処理学会研究報告, DSM-48, (2008)
- N, 山口, 梶田, 平野, 間瀬, 名古屋大学における統合サーバの構築と運用, 情報処理学会研究報告, IOT-1, (2008)
- 梶田, 太田, 田島, 田島, 平野, N, 間瀬, 生涯利用可能な名古屋大学 ID の新規発行における名寄せの方法に関する検討, 情報処理学会研究報告, IOT-1, (2008)
- N, 名古屋大学の全学認証基盤について国公立大学情報システム研究会報告 (富士通), (2008)
- その他, N の Web ページに資料あり