Sun Identity Managerを用いた「小さな」統合ID管理システムの構築

2009年12月8日
CAUA第8回合同研究分科会@大阪

九州工業大学情報科学センター
中山 仁　　甲斐 郷子

はじめに

- H18年～現在までの九州工業大学における情報基盤整備について

- 特に、Sun Identity Manager (IdM) を中心とした統合ID管理システムの構築事例を紹介

1. まずは九工大の紹介

- **組織**
  - 2学部３研究科 (工学/情報工学/生命体工学)
  - 附属図書館
  - 情報科学センター　他15センター (時限組織含む)
- **構成員** (H21.5)
  - 学生数：5,963人
    （学部生4,364人、大学院生1,599人）
  - 教職員数：583名
- **３キャンパス (戸畑・飯塚・若松)**
  - キャンパス間がそれぞれ40km(ファイバー長64km)，20km(同24km)
  - サテライトキャンパスが他に2か所 (福岡市天神，東京)

2. 九工大を取巻く環境 (H18当時)

- 国立大学法人化 (H16.4)
- 文部科学省研究振興局「学術情報基盤の今後の在り方について(報告)」(H18.3.23)
- 文部科学大臣官房長「文部科学省行政効率化推進計画」(H16.6.15, H18.8.29改定)

……

- **情報化戦略に基づいた情報基盤整備**
- **情報セキュリティの確保**
- **学内情報の組織的管理・運用による情報ガバナンスの達成**
- **ボランティア管理から組織的管理・運営体制へ**
- **システム統合によるコストの削減**

3. 九工大の現状と課題 (H18当時)
(1)既存の情報システム

時代を先取り様々な情報化を推進
(キャンパスオートメーション)

S50(1975)年	全学部学生に対する情報処理教育の開始
S63(1988)年	全学部学生に対する入学時ID配布の開始，磁気カードによる身分証明書の導入
H 2(1990)年	磁気カードを用いた入退室管理システムの導入
H 4(1992)年	UNIXワークステーションを用いた集合教育の開始
H 7(1995)年	情報工学部にて教務情報システムの実験運用の開始
H15(2003)年	ICカードによる身分証明書および入退室管理システム導入　など

3. 九工大の現状と課題 (H18当時)
(1)既存の情報システム

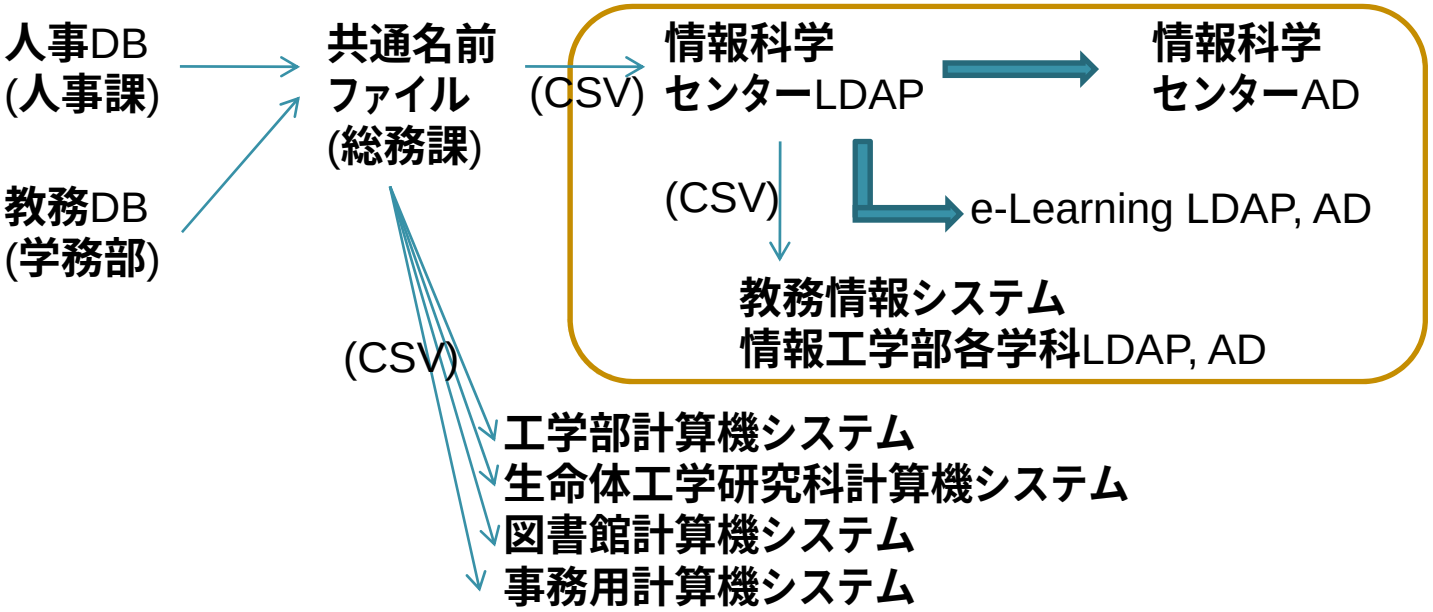
- **講義演習用システム：端末数約1700台**
  情報科学センターシステム，学科計算機システム(6学科+2専攻)，e-ラーニングシステム，高度マルチメディア教育システム，サテライトキャンパス計算機システム
- **学内ネットワーク**
  SINETとの接続，キャンパス間接続，キャンパス内LAN(有線，無線)，VPN，情報コンセント等
- **図書館計算機システム**
- **教務用システム**
  教務情報×2/証明書自動発行/ICカードによる入退出管理･出席管理の各システム
- **その他事務用計算機システム**
  事務用計算機システム，
  人事事務/給与計算/共済組合/授業料債権管理/授業料免除/統合文書管理/化学物質安全管理/会計/財務(資産管理)/スペース管理/特許管理/入試管理/グループウェアなど

3. 九工大の現状と課題 (H18当時)
(1)既存の情報システム

- **学内の各組織・委員会が独自に対応**
  → 全学の統一的な情報化戦略の不在
  - 学内構成員に均一に提供する情報サービス実現が困難
  - 情報基盤システムに関する情報収集が困難，学内周知の不徹底
  - 集約可能なシステムが複数存在するため，開発・運用コスト増加，統合利用への障壁
  - ライフサイクル管理の不在

3. 九工大の現状と課題 (H18当時)
(1)既存の情報システム

ユーザ管理について



- 情報科学センターLDAPは4月には数日に1度，それ以降は1カ月に1度差分を更新
- 情報科学センターでは毎年6月期にID削除処理
- 独自にユーザ管理しているシステムも多数 (給与計算，スペース管理，特許管理，会計，化学物質安全管理等)

3. 九工大の現状と課題 (H18当時)
(2)新たな情報サービス

- **大学法人化や高度ネットワーク社会に際し，情報化への取組みの必要性は年々増加**
- **法人化後のシステム構築**

  中期目標･中期計画DB/教員情報DB/教育職員評価システム/機関リポジトリ/ソフトウェアライセンス管理/エネルギー使用状況/自己評価･ポートフォリオシステムなど
- **学生・教職員だけでなく，卒業生・入学前学生・ゲストなども対象に**
- **新たなサービスにどのように取り組んでいくか**?

3. 九工大の現状と課題 (H18当時)
(3)その他の課題

- キャンパスLANの未整備部分の存在
- 情報セキュリティ対策の実施とボランティアベースのネットワーク/システム管理
  → 能力差，負荷増大，人員不足
- 計算機・ネットワークシステムの経費に対する明確な基準がない
- 情報化に着目した業務体系・業務改善が不徹底

3. 目標

(1)**安全で便利な情報基盤の構築**
(2)**教育・研究環境の充実・革新**
(3)**経営の効率化**

- **具体的な目標 (当初)**
  - 卒業生，入学前学生，非常勤等を含む九工大学生・職員・ゲストすべてを対象
  - 統一認証システムの構築による高度で統一的な情報管理，サービスの提供
  - 安全な情報セキュリティシステムの提供
  - 高度・迅速・便利・安全な学内情報サービスのワンストップ化を可能とする全学統一ポータルの構築

4. 情報基盤充実に向けての対応

- **文部科学省へ新規予算の要望** (H18-19**年度**)
  - キャリアパス教育，就職支援等とからめる
    → 予算獲得できず
- **学長裁量経費を用いて認証システムの調査研究** (H18-19**年度**)
  - **学内情報システムにおけるユーザ**ID**情報の調査**
    - 構成員と所属･番号(学生･職員番号)の関係
    - 学生･職員番号なしユーザの種別および人数．学内情報システムに対する影響
  - **他大学等の導入運用事例調査**
  - **製品調査**
  - **プロトタイプ構築用機材の購入**

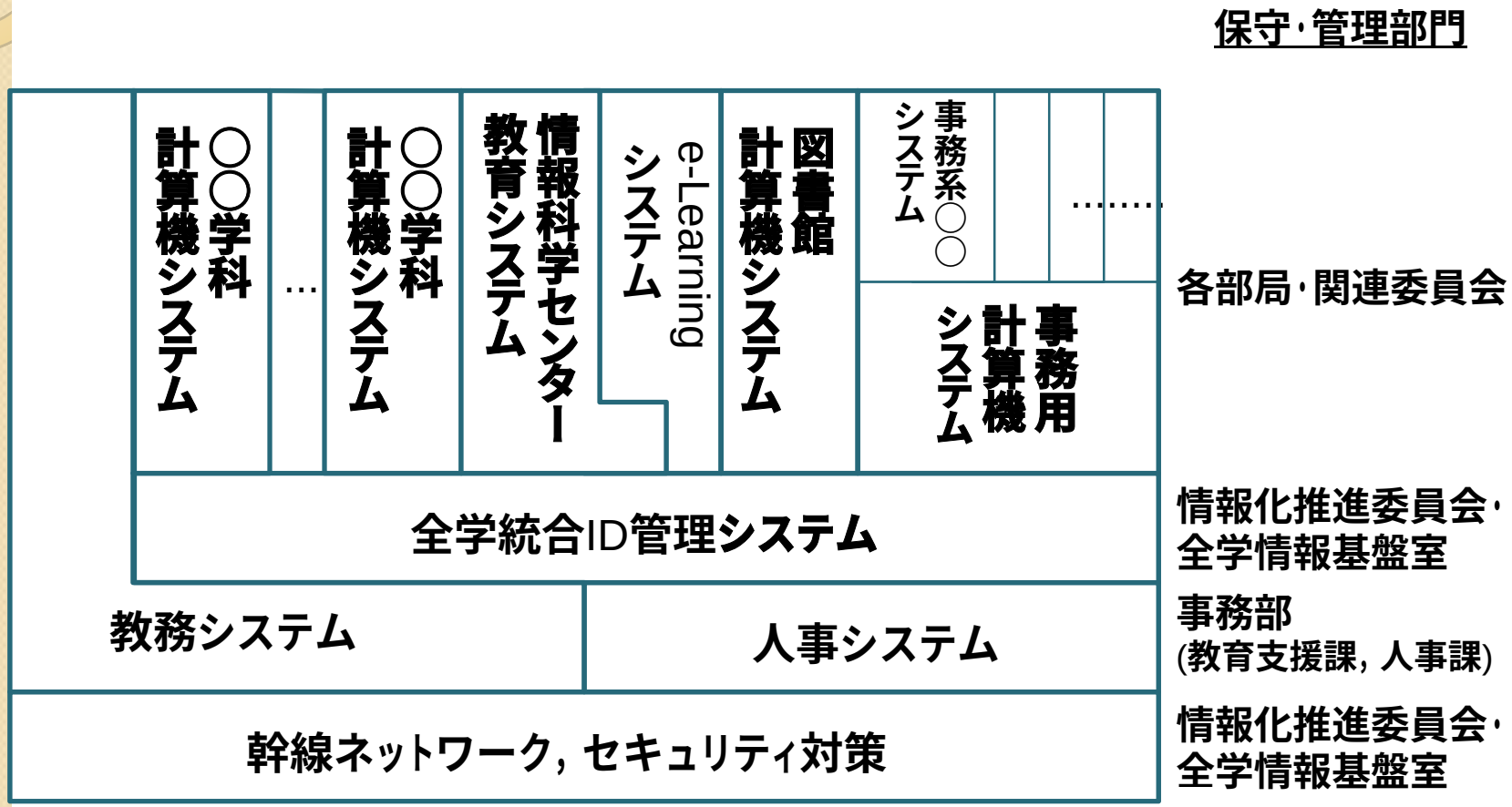
4. 情報基盤充実に向けての対応

- **具体的な目標 (改訂)**
  - 初年度に全学統合ID管理システムを導入
    学内情報システムは更新時に接続
    → 4～5年かけて全学情報システムを統合
    　統一的な情報管理，サービスもある程度の期間をかけて対応
  - 卒業生，入学前学生，非常勤等を含む九工大学生・職員・ゲストすべてを対象
    → 職員番号，学生番号がない人にも対応
    　ただし，厳密な名寄せはしない
  - 全学統一ポータルは後回し

4. 情報基盤充実に向けての対応

- **学内レンタル予算の再構成** (H19-20**年度**)
  - 情報システムに対する学内予算の利用状況調査
  - 学科計算機等レンタル予算の一律化
  - 情報基盤システムの定義と情報基盤システムのための学内予算の確保
- **学内各種情報システム更新時の指針の制定** (H20.9)
  - レンタル経費による情報システムおよび全学利用されている買取システムは
    - 全学統合ID管理システムと円滑に結合できること。
    - 情報セキュリティポリシーに関する基本規程（九工大規程第16号）と整合すること。
    - 仕様策定委員会の委員に情報化推進委員会より推薦された者を含むこと。

4. 情報基盤充実に向けての対応



5. 導入に向けた調査検討

- **他大学等の導入運用事例**
- **統合認証 (アカウント管理) 製品**
  - HP IceWall
  - IBM Tivoli
  - …

従来の「統合認証」は，私たちが欲しい物と少し違う？

5. 導入に向けた調査検討

- いわゆる「統合認証」システム
  - 明確なシステム構成
  - きちんとしたポリシーとガバナンス
  - トップダウン
- 九工大の現状
  - 多様(雑多)なシステム群
  - 運用ポリシー，運用体制(事務)が不透明
  - ボトムアップ (を束ねる必要)

5. 導入に向けた調査検討

- Sun Identity Manager (Sun IdM)
  - 既存のシステム間でID情報を「連係」
    - ポリシー設定次第で緩やかな統合が可能
    - 既存システム側の変更を最小限に
    - 必要に応じてより厳格なポリシー適用も
  - 標準でオープンな技術の採用
    - 標準プロトコルによるシステム間接続
    - (将来にわたり)多様なシステムへの対応

多様性と柔軟性を許す統合管理の可能性

6. システムの設計

- **基本方針**
  - Sun Identity Manager**を中心としたシステム**
  - **直近に必要な機能の確保**
    - 端末ログインアカウント(IDとパスワード)の管理と提供
    - 情報科学センターアカウントをベースとした運用
    - 最小限の管理機能
  - **各種システムとの連係**
    - 緩やかな連係運用
    - システム接続のためのコストは各システム側が負担
  - **拡張性**
    - 具体的な拡張計画は設定しない
    - 複数の異なるアカウント体系を受け入れる余地を入れる
  - **構成**
    - IDデータベース部分
    - システム連係部分

6. システムの設計

- IDデータベース
  - KID - 個人識別子
    - システム独自の一意ID
    - 学生番号，職員番号等に依存しない
    - 名寄せは当面考慮せず
  - RID - アカウント識別子
    - role (役割) ごとに割り当てられるID
      - 例)学生のA君，TAのA君
    - アカウント体系ごとに割り当てられるID
      - 例) 端末ログイン用，IDカード用
    - 1つのKIDに対し複数のRID

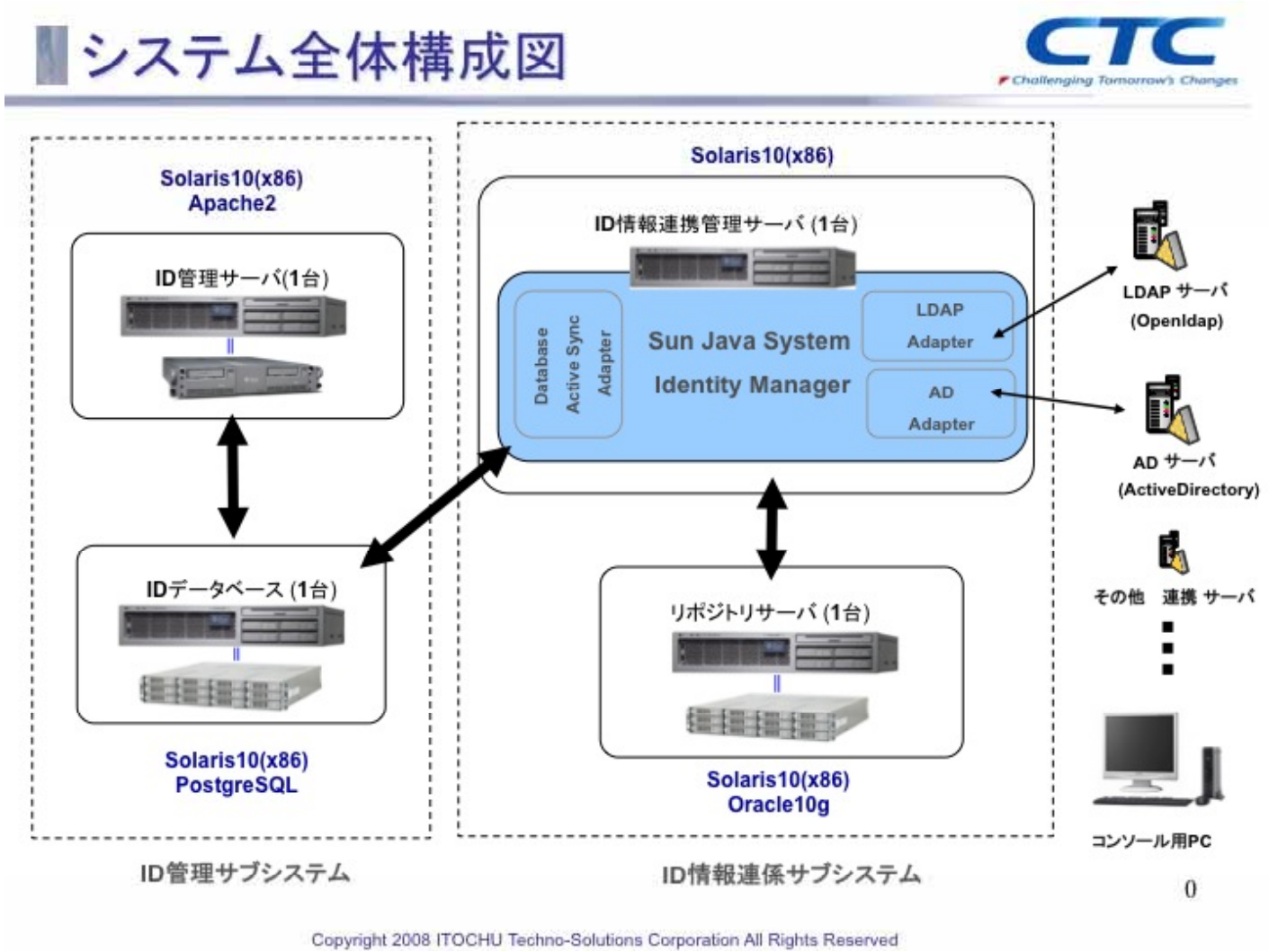
6. システムの設計

- システム連係
  - 情報科学センターシステムおよび同系統のアカウントを利用するシステムを対象(当面)
    - 学科等の共同利用端末，e-Learning用Appサーバなど
    - 同等あるいはサブセットのアカウントベース
    - ログインID + パスワード
    - LDAPおよびActiveDirectory対象
  - 連係先の独自運用を許容(ローカルIDなど)
    - 緩やかな連係関係
  - ディレクトリサーバへのデータ提供
    - 連係先システムがディレクトリサービスを運用
    - 認証も連係先システムが実施

7. システムの構築

- システム構築作業
  - IDデータベースの設計と構築
  - 連係システム(Sun IdM)の設計と構築
  - 調整およびテスト
  - アカウントシステム，データの移行
    - 旧情報科学センターシステムLDAPから
  - システム連係設定のテンプレート化
- 構築期間 = 実質6ヶ月
  - 必要最小限の機能の実現を優先

7. システムの構築



8. システムの現状と評価

- **現状**
  - 情報科学センターとの連係（LDAP，AD）
  - アカウントデータ管理
    - センター職員が担当
    - 従来のセンターアカウント管理業務の枠組み
  - 他システム(4システム)との連係準備中
    - 今年度末稼働開始予定

8. システムの現状と評価

- **性能など**
  - **多人数(100名程度)利用時の問題**
    - パスワード変更の反映時間が長い(～数十分)
    - 事前テストで発覚 → 修正後供用開始
  - その他不具合
    - 旧アカウントデータの移行の一部にミス
    - 利用者GUIの修正
    - 軽微なものばかりであり，すでに改修済み

8. システムの現状と評価

- **評価**
  - **アカウント管理システムとして**
    - **基本的には安定動作**
    - **機能面での軽微な問題はまだ見つかる**
    - **DB管理機能の機能不足**
  - 今後の連係先システムの増加
    - 伝搬時間
    - 障害時などの挙動(データー貫性)
    - 現時点では未確認部分多い

8. システムの問題点，課題

- DB管理者GUIの機能不足
  - 定型的な操作中心．できないことはSQL直打ちするしかない？
  - CUI操作スクリプトなどを整備して補完
- IDデータベースの拡張
  - 一般学生，職員以外の利用者への対応
    - 社会人セミナー受講者，共同研究者，etc
    - 想定はしていたが，具体的な対応は不十分
  - 今後のDB改良，拡張を誰がどのように行うべきか

8. システムの問題点，課題

- 統合IDシステムとの接続に係る課題
  - 接続設定のためのコスト
    - ディレクトリサービスを自主運用する必要
    - 初期設定費用，運用の手間や費用
    - 小規模システムやその運用者にとって負担大
    - LDAPなどIdM以外での連係方法の提供必要？
  - 接続先システム導入に対する影響
    - CTCによるIdMとの接続作業が必須
      → システム選定や構成上の自由度を下げる？
    - 接続設定テンプレートの利用
      → 可能な範囲の接続作業は自分たちで行う

10.おわりに

- 「小さな」統合IDシステム
  - できるところから手を付ける
  - 最小限必要な機能に集中
  - 拡張性への配慮
- Sun Identity Managerの活用
  - 柔軟性，多様性
    - 短期間でのシステム立ち上げ
  - 拡張性
    - 将来の展開への期待

10.おわりに

- 「小さな」統合IDシステム
  - 何はともあれ離陸はした
  - 真価を問われるのはこれから
- 学内システム群の統合，協調にとってのランドマーク
  - 実際に動いているシステム
  - 具体的な接続目標
  - システム連係に配慮する意識の醸成

小さく生んで大きく育てる