名古屋工業大学における認証基盤システム構築と学認

名古屋工業大学
情報基盤センター
准教授
齋藤彰一

名古屋工業大学

■工学部の単科大学

- 学生数：約6000人
  - → 第一部，第二部，博士課程（前期・後期）
- 教職員数：約700人（非常勤，派遣職員など含む）

■情報基盤センター

- 学内の計算機・ネットワークの管理
- e-education，情報リテラシ教育支援
- 事務業務システムの支援
- 教授（兼務）2，准教授　4，助教　2
- 技術職員　専任3，他の部署との兼務7

名古屋工業大学の情報基盤システム

■2007年4月に情報基盤システムを導入

- 全教職員・学生の**IDを統一**
- **ICカード**を全教職員，学生に発行
  - → 接触・非接触のハイブリッド
- **シングルサインオン（SSO）**で導入
  - → Sun Java Identity Manager Suite
- 教職員ポータル，学生ポータルの導入
- 学生関係
  - → 全教室にICカード（非接触）による出欠システムを導入
  - → CMSにMoodleを全面導入（全講義を登録）
- 事務関係
  - → 事務局全計算機をシンクライアント化＆ICカード認証
  - → 電子ワークフロー（物品購入・旅費申請等）を導入

現在来年４月稼働に向けて次期システムの準備中

ID統合と人に関する情報管理

統一データベース

ID統合とICカード

■ ICカードによる高度なセキュリティ

- 偽造改ざん不可能
- 身分証明書との統合により確実な本人認証

■ シングルサインオン・SSO

- 利用者負担の軽減
- 今後導入する**すべてのシステムはSSO**とすること！

■ ID統合を実施

- IDを一人1つに
- 人事・学務システムに基づくユーザ登録
  - → 学内の「すべての人」の洗い出し
  - → 派遣職員・研究生（システム未登録ユーザ）なども登録
- ID統合の核として統一データベースを開発

統一データベース

- **目的：大学内に存在する「人」に関する情報の統一的管理の実現と情報共有を促進する**
- **学内すべての「人」に関する情報の管理**
  - 人事DB・学務DB＆DBに載らない人たちも登録（全員！）
    - → 登録されないとICカードが発行されない
  - DB記載事項以外の情報は自分でメンテナンスを行う
- **学内の情報システムに対して情報を供給**
  - 統一データベース内の情報を一次データとし、他の学内システムは、統一ＤＢからデータを獲得
  - すべてのデータは統一ＤＢを参照することを学内に徹底することにより、同じことを何度も収集することを無くす

「人」に関する情報の管理

■登録体制の確立

- 所属によってアクセス制御するために，発令日の朝には更新（登録）が完了している必要がある
- 「正確な情報」を「必要な期日までに」登録できる事務体制の確立が必須

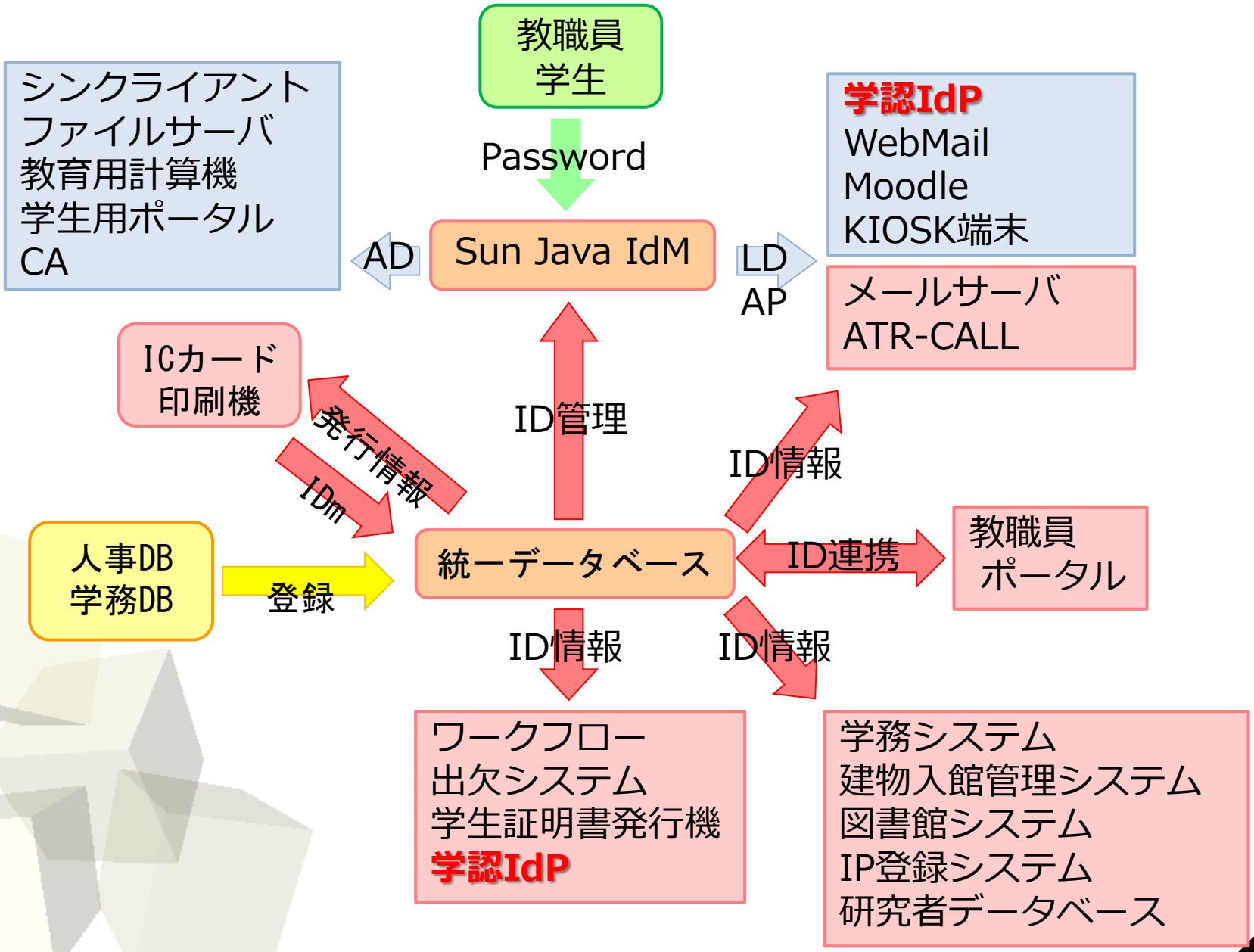
■人事イベント（教職員関係）

- 採用，再雇用，退職，配置換え，役職等就任
  → 人事DBに載らない人の退職把握が難しい

■異動イベント（学生関係）

- 入学・退学・休学・卒業・修了
- 転学科・転学部・転専攻
  → 学務チームによる一括登録

ＩＤ情報連携図


教職員
学生
Password
シンクライアント
ファイルサーバ
教育用計算機
学生用ポータル
CA
AD
Sun Java IdM
LD
AP
学認IdP
WebMail
Moodle
KIOSK端末
メールサーバ
ATR-CALL
ICカード
印刷機
発行情報
IDm
ID管理
ID情報
人事DB
学務DB
登録
統一データベース
ID連携
教職員
ポータル
ID情報
ID情報
ワークフロー
出欠システム
学生証明書発行機
学認IdP
学務システム
建物入館管理システム
図書館システム
IP登録システム
研究者データベース

名工大におけるSSOと学認

学内SSO

大学間SSO

名工大のサービス運用方針

- **全事務システムをCIO・情報基盤センターが把握**
- **SSOでないサービスは認めない**
  - 学外からの利用は除く
  - SSO導入前から稼働しているシステムは除く
- **VM化して基盤サーバで運用する**
  - 導入時からセンタースタッフが関与する
- **物理的制約によって基盤サーバに配置できない場合は？**
  - VPNを活用（VPNの先の部屋は施錠してもらう）

SSO・リバースプロキシ方式

■ Sun Java Identity Manager Suite

- Shibbolethではありません
- リバースプロキシ方式を採用

■ SSOサービスはリバースプロキシを経由して利用

- すべてのサービスはSSO化して、基盤サーバサブネットに配置
- 前提：方針に基づきサービスを集中配置

■ 学内開発のSSOアプリはHTTPヘッダ認証

- HTTPヘッダ内に認証済みユーザIDを埋め込む方式
- SSOアプリはヘッダ内のユーザIDを信用

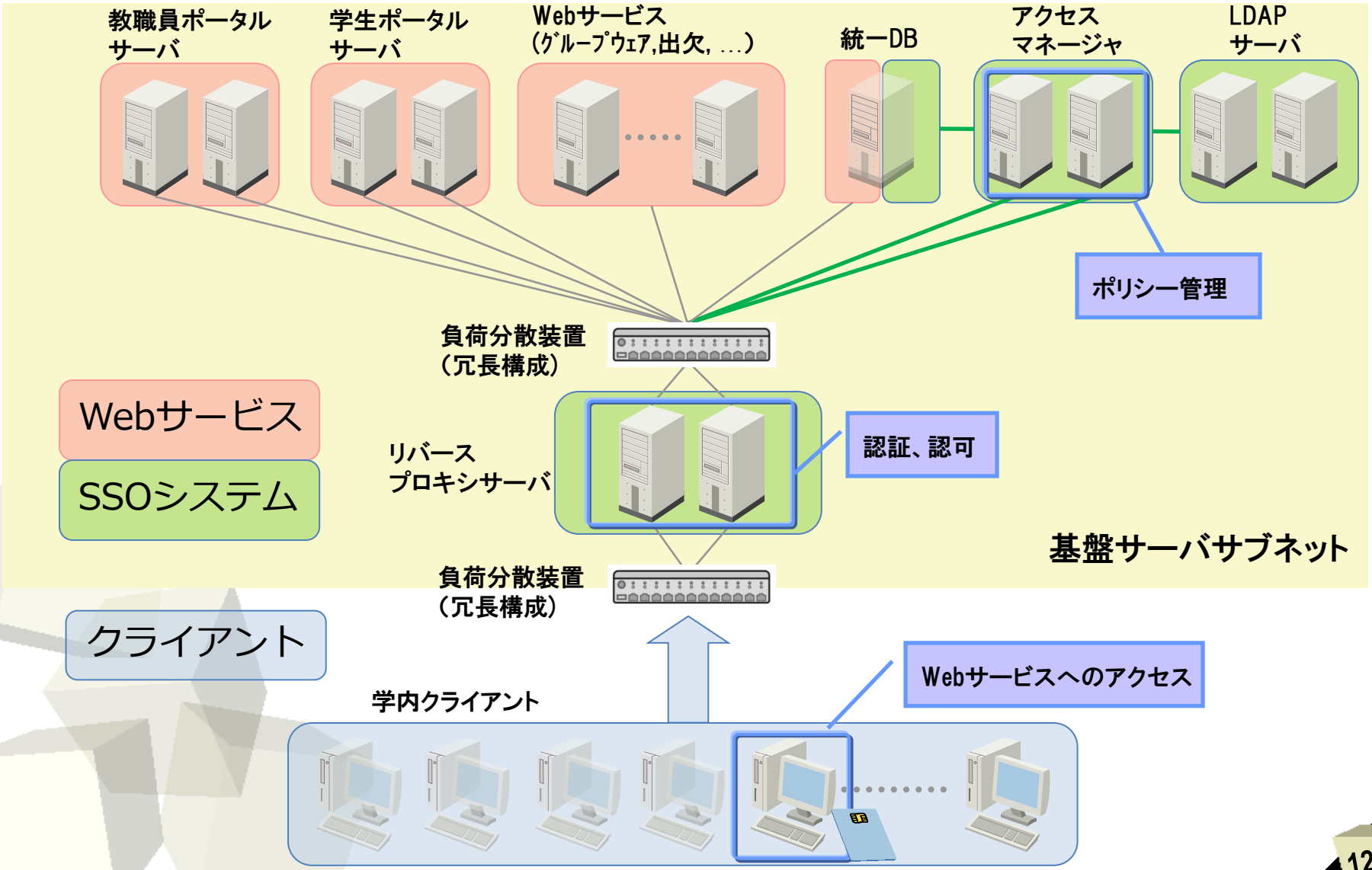
■ 既存アプリについてはフォーム認証

- 既存Webフォームに認証システムがユーザIDとパスワードをセットする方式
- Webフォームに合わせた設定が必要（アプリ側の改変は不要）

シングルサインオンシステム構成

概要図

[システム規模]学生数:約6000名、教職員数:約700名



リバースプロキシ・Shibboleth

- **IIS対応・ICカード認証対応への不安（6年前）**
- **サーバ集中配置・VM化が基本方針**
  - 安全なサーバサブネットへのサーバ配置変更が前提
  - 物理的移動ができないサーバはVPNで接続
- **SP化が可能か分からないアプリもあった**
  - リバースプロキシならフォーム認証が可能
- **属性情報は統一DBがSQL・CSVで配る！**
- **安全なサーバサブネットの確保**
- **属性情報の利用**
- **アプリ対応**
  - 名工大の場合：順次切り替えはできず、導入時にすべてが動作していなければならなかった＆ICカード認証必須

名工大の場合

導入の判断

名工大の学認IdP

2011年6月稼働

ユーザ情報の取得

- パスワードのみLDAPを利用
- 属性情報は統一DB(MySQL)を直接利用

構築目的

- 学内
  - → 基盤サーバに収容できないサービスのSSO化
- 学外
  - → 学認利用
  - → 東海アカデミッククラウドの構築

東海アカデミッククラウド

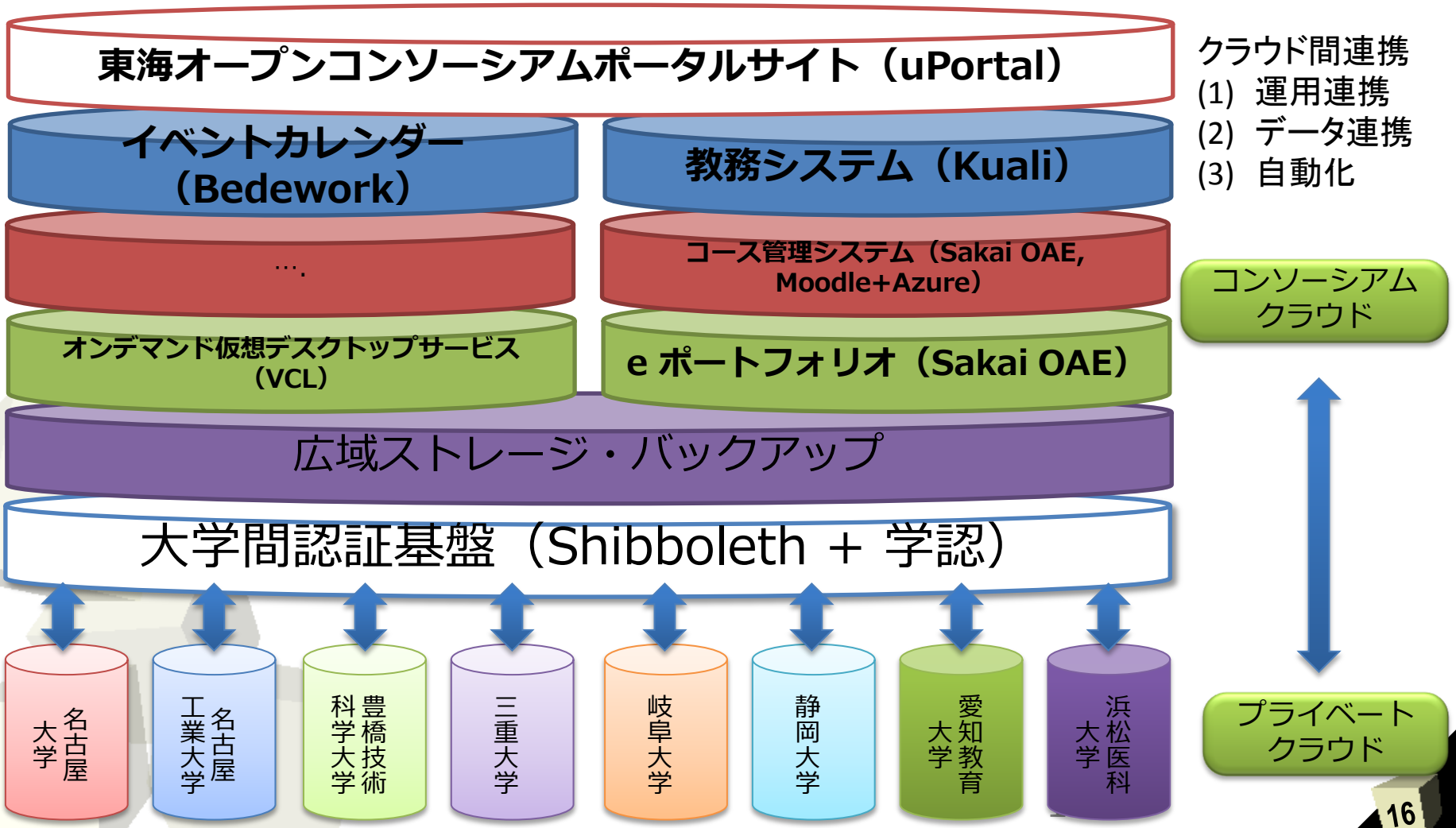
- **我々がほしいのはサービスである！OSや計算機ではない！**

クラウド

- **東海地区の国立大学で研究開発中**
- **各大学が学内開発したWEBサービスをオープンソース化し、大学毎にカスタマイズ**
  - ソフトウエアは常にアップデート可能状態に
  - 開発・保守コストの低減
- **認証基盤**
  - Shibboleth・学認による大学間認証連携

各大学のプライベートクラウド間をつなぐインタークラウド

東海アカデミッククラウド　中期目標（３－５年？）



まとめ

■名工大

- 統一データベースを核とした「人」の情報管理と情報共有を行っている
- ICカード・リバースプロキシSSOによる認証

■東海アカデミッククラウド

- 東海地区国立大学による共通サービス基盤構築実験
- Shibboleth・学認による大学間認証
- 参考：IEICE IA研究会・ITRC meet30の発表
  - → 「Shibboleth・CAS連携による東海アカデミッククラウド認証基盤の構築」梶田将司他