中規模私立大学における統合認証基盤の構築と大学間共用eラーニングシステムとの連携

京都産業大学
コンピュータ理工学部　秋山　豊和
情 報 セ ン タ ー　　尾崎　孝治

内容

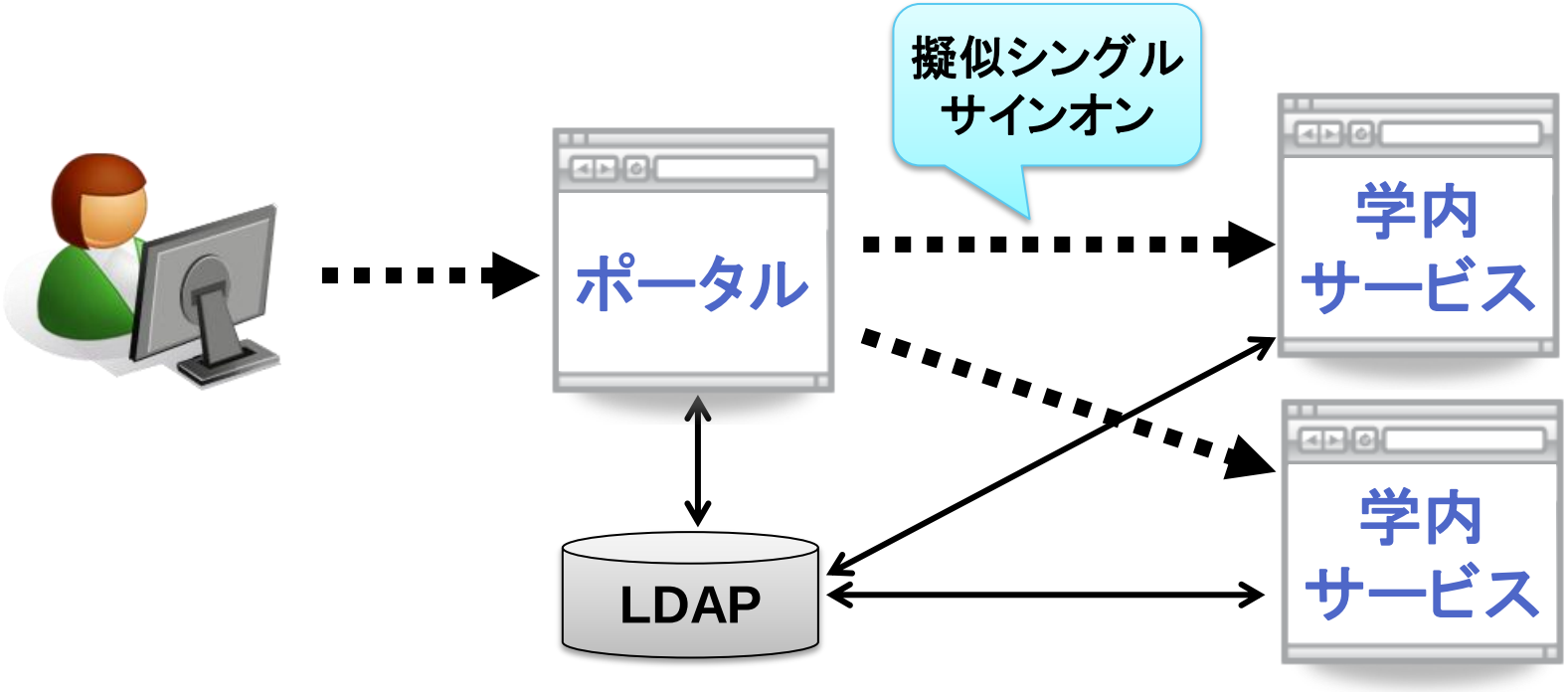
- ◆Shibboleth導入前の本学での統合認証基盤構築状況
- ◆大学間共用eラーニングシステムの紹介
- ◆Shibboleth導入の経緯とその利点・欠点
- ◆Shibbolethの学内認証への適用
- ◆学認の可能性

京都産業大学

- ◆開学1965年
- ◆１拠点８学部21学科
- ◆学生数　約13,000名
- ◆情報センター（事務組織）が基盤構築担当
- ◆オープンソースの積極的な利用
  - ➢情報処理教室のWindows/Linuxデュアルブート
    1999年603台，現在約2,000台
  - ➢moodleの全学利用 2005年～
  - ➢postfix, apache, openLDAP, postgreSQL, etc.

Shibboleth導入前の統合認証基盤の構築状況

- ◆OpenLDAPによる認証情報の集約
- ◆Webポータルを経由したアプリケーション利用



財団法人大学コンソーシアム京都

◆京都には大学がたくさん

◆地域・産業界を含めて協力体制の強化

➢50の大学と19の公共機関・企業が参加

◆単位互換制度

開始： 1994年

特徴： 京都は比較的大学間が近いので直接キャンパスまで行って受講できること

実績： 2008年度には46大学・短期大学が10テーマ506科目を提供。年間1万人が受講。

サービス： 単位互換制度申請システム

大学間共有eラーニングシステム

- ◆本学が代表校の戦略的大学連携支援事業
  - ➢eラーニングシステムの共有共用化に伴う教養教育の大学間連携と効率化の促進
  - ➢平成20年度採択
- ◆目的
  - ➢共用できるeラーニングサーバの設置
  - ➢遠隔講義環境の構築
  - ➢ビデオオンデマンド環境の構築

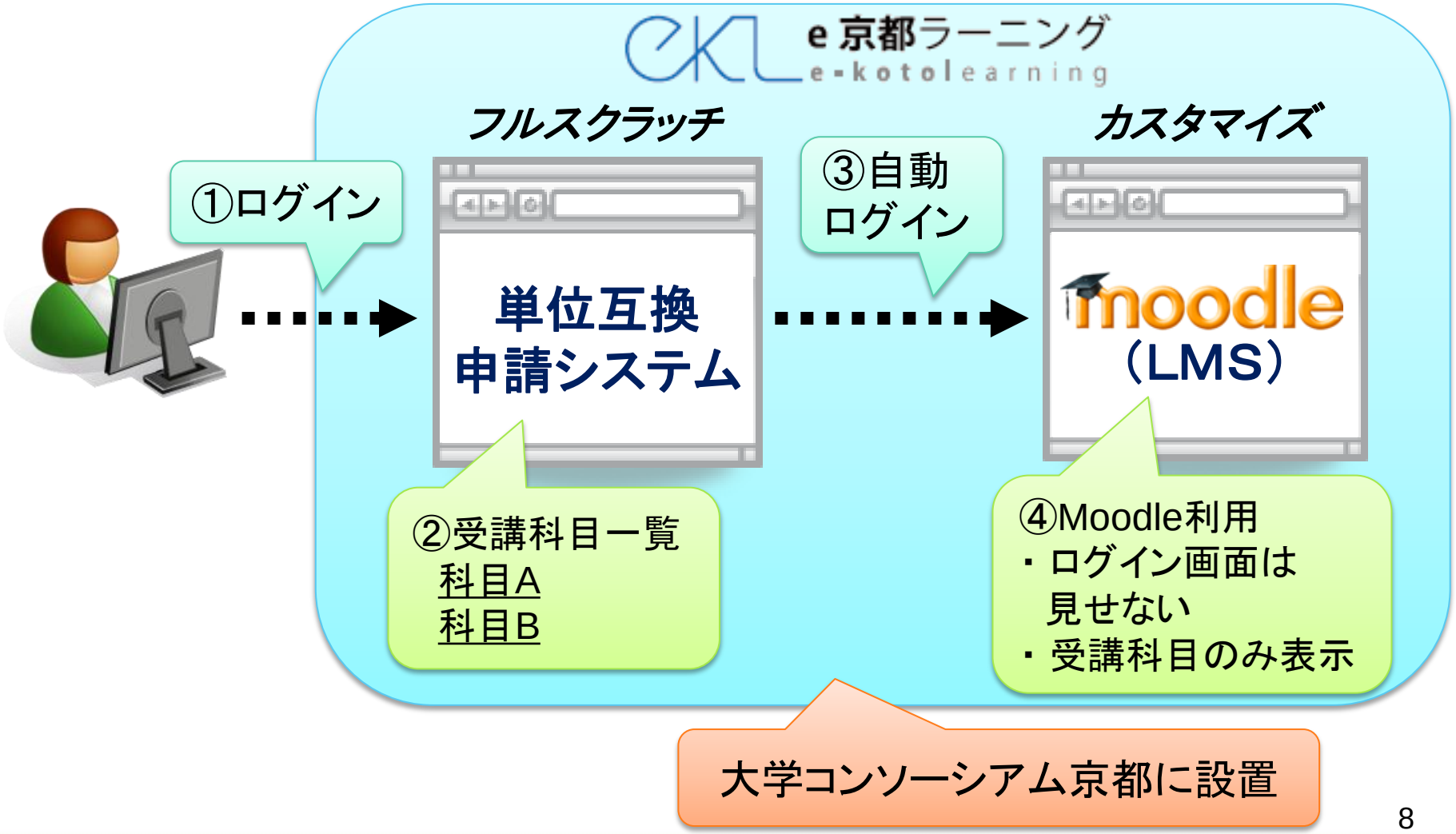
大学間共有eラーニングシステム

◆単位互換授業におけるeラーニングサーバ共用の必要性

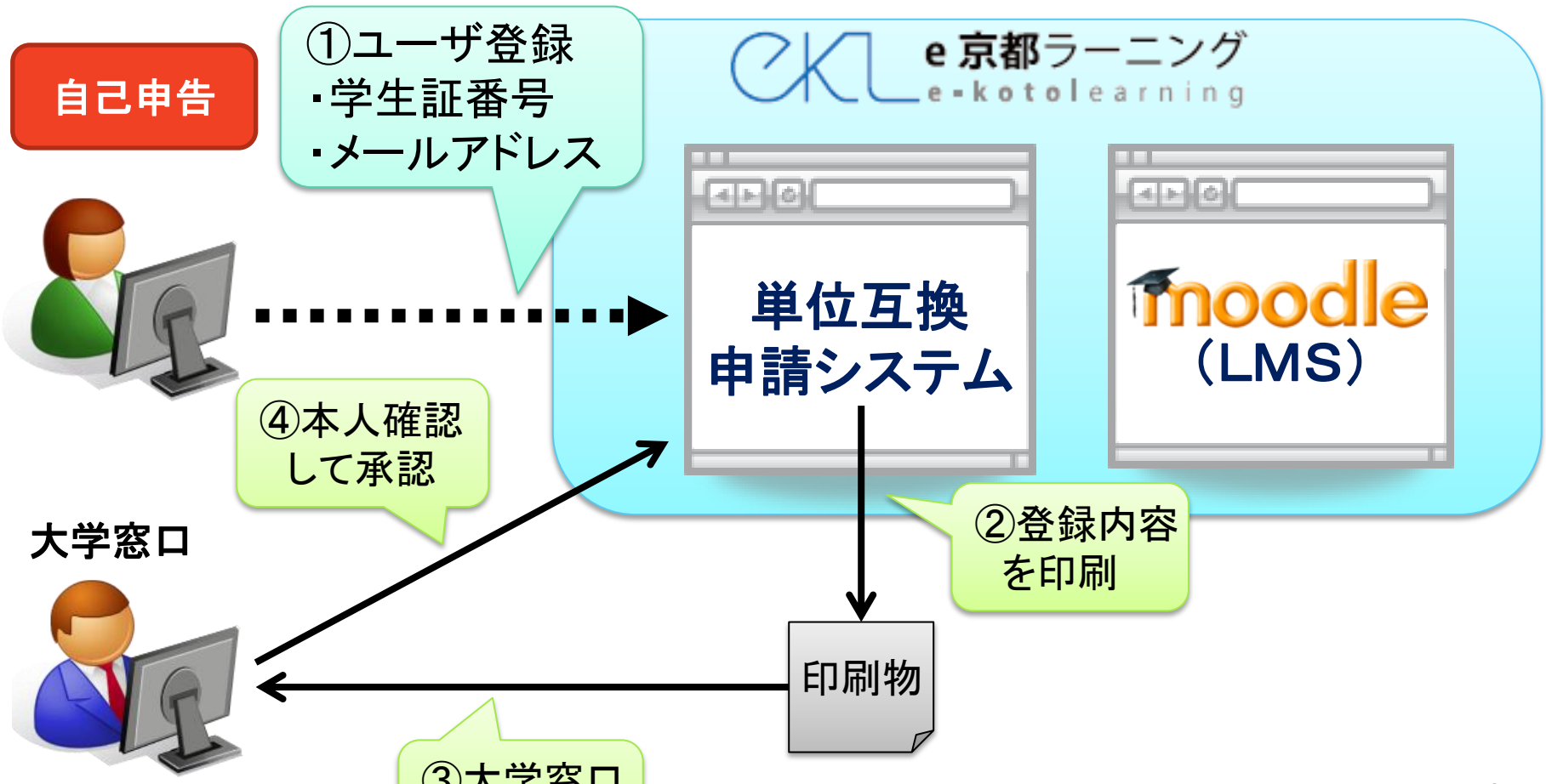
- ➢授業資料の配布
- ➢受講生への連絡、課題の提示

一般的な講義と同様であるが、他キャンパスから受講する学生がいるためその重要性が高い

eラーニングサーバの利用イメージ



eラーニングサーバの初期利用時の流れ



様々な要求・課題

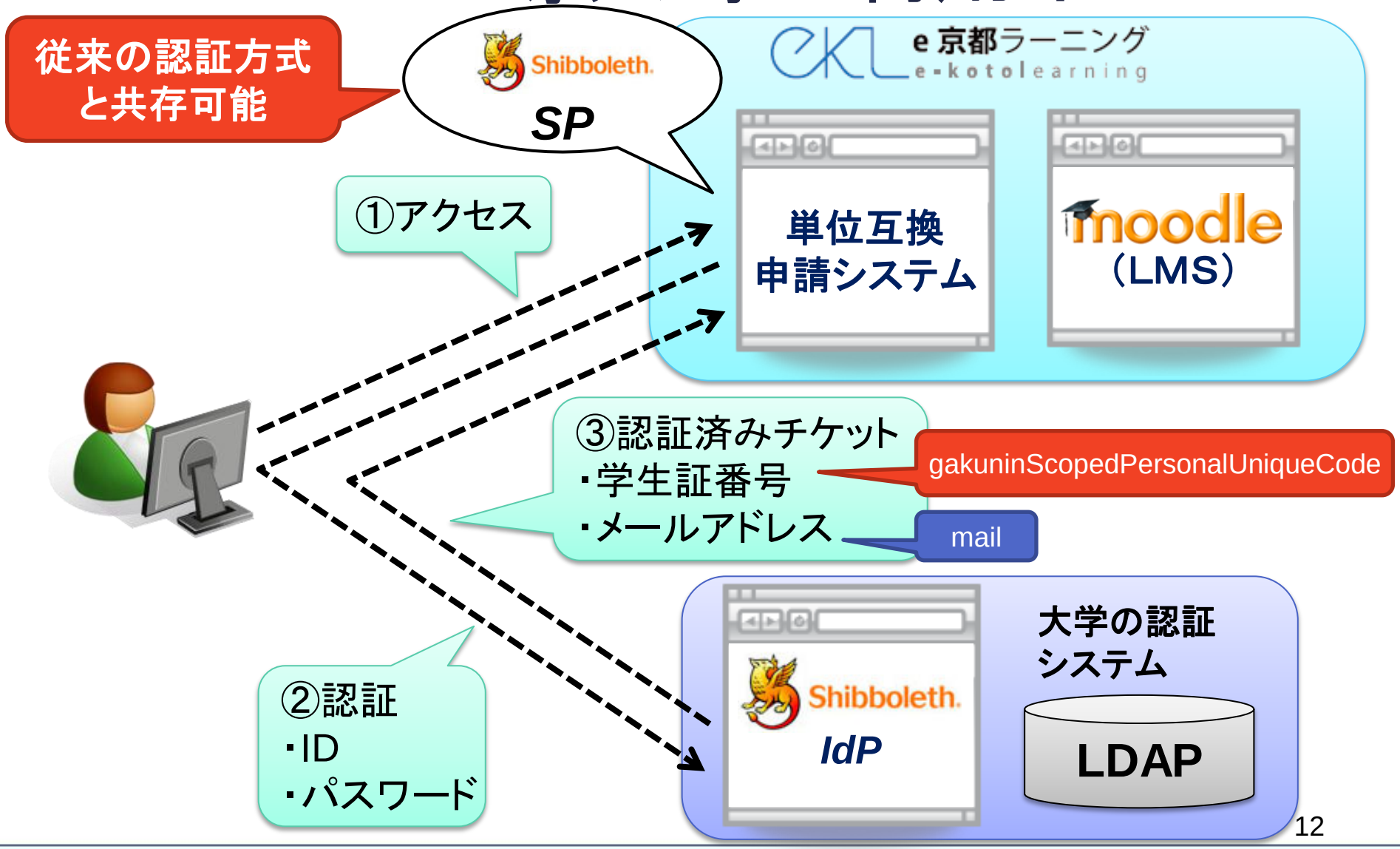
- ◆大学の認証システムと同じパスワードを使わせたい
  - ➢とはいえ，学外システムにパスワードは渡せない
- ◆申請者が入力した学生証番号に信頼性が必要
  - ➢繁忙期の窓口で本人確認をする余裕がない
  - ➢学生証番号が信頼できるなら紙を提出させる手順をなくせる
- ◆申請者を装った，第三者による虚偽申請の可能性をなくしたい
  - ➢騙られた学生は初期化されるまで自分の申請ができない

様々な要求・課題

Shibbolethを用いると

- ◆大学の認証システムと同じパスワードを使わせたい
  - ➢ ***大学の認証システムと連携可能***
- ◆申請者が入力した学生証番号に信頼性が必要
  - ➢ ***学生証番号は確実に本人のものを大学システムから渡せる***
- ◆申請者を装った，第三者による虚偽申請の可能性をなくしたい
  - ➢ ***本人による会員登録不要なので，第三者の偽登録の心配がない***

Shibboleth導入時の利用イメージ



Shibbolethの利点

◆IdP（接続する側）のセキュリティメリット

- SPにはユーザのパスワードが渡らない
- 利用しないユーザの個人情報は渡さなくて良い
- SP毎に渡す情報を制御可能
  - IdPの持つ情報が無条件にSPへ渡される訳ではない
- 学内システムのSSO化にも有効
  - 個々のシステムにはパスワードが渡らない
  - ベンダー製品でも導入時にShibboleth対応を明記すれば対応可

◆SP（接続される側）のセキュリティメリット

- 接続可能なIdPを制御可能
  - SPになると無制限に接続される訳ではない。
    例）特定のIdPからのみ接続を許可
- SPにユーザパスワードを持つ必要がない

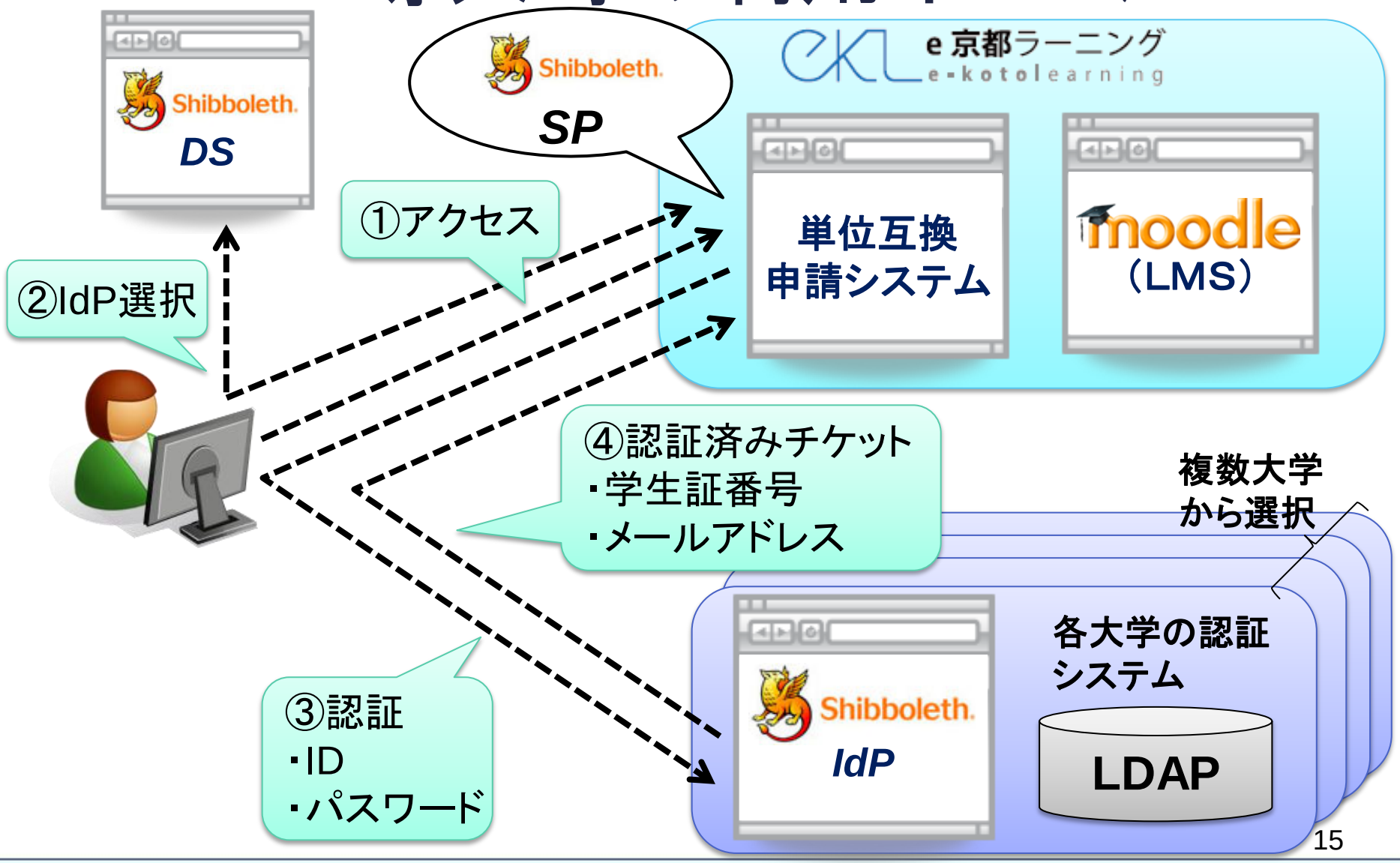
更に学認なら…

GakuNin

◆複数の大学での利用が容易に

- メタデータ（信頼するリスト、学認参加IdP、SP）をNII側で管理
  - IdP、SPでは自動的に参加IdP、SPのアップデートができる
- 学認参加IdPを選択するDS（Discovery Service）をNIIが提供
- NIIが主導する学術認証基盤
  - 学内に説明しやすい（SINET加入している本学の場合）

DS導入時の利用イメージ



DS導入時の課題と解決方法

- DS上にたくさんのIdPが表示される
  - 学認が提供するDSではすべての参加機関のIdPが表示される
  - IdPをフィルタリングする機能が必要
- SWITCH DS
  - SWITCHが開発
  - Embedded DSはSPに埋め込んで利用可能
- 拡張版SWITCH DS
  - 学認が開発
  - DSでのIdP検索機能を実装（サービス提供中）
  - Embedded DSでSPの設定(DiscoFeed)を参照し、連携していないIdPを自動でフィルタ可能

リスク

- ◆学認プロジェクトが終了する
  - 利用が多ければ継続されるはず
- ◆学認DSが(トラブルにより)停止する
  - 学内システムに影響が無いように設定可能
- ◆Shibbolethの開発が終了する
  - そこまで責任持てませんが…しばらくは大丈夫でしょう
- ◆信用できないIdPの参加
  - 公開SPが考えるべきリスク。当面は参加大学の数が少ないのでホワイトリスト方式でも運用可能
- ◆信用できないSPへのアクセスによる情報漏えい
  - IdPがデフォルトで属性を提供せず，SPごとに渡す属性をホワイトリストで設定していれば大丈夫
  - 京産大でクライアント・サーバ相互認証の機能を実装中

個人情報の取り扱いについて

◆本人が了承していれば問題ない

◆今回の事例では？

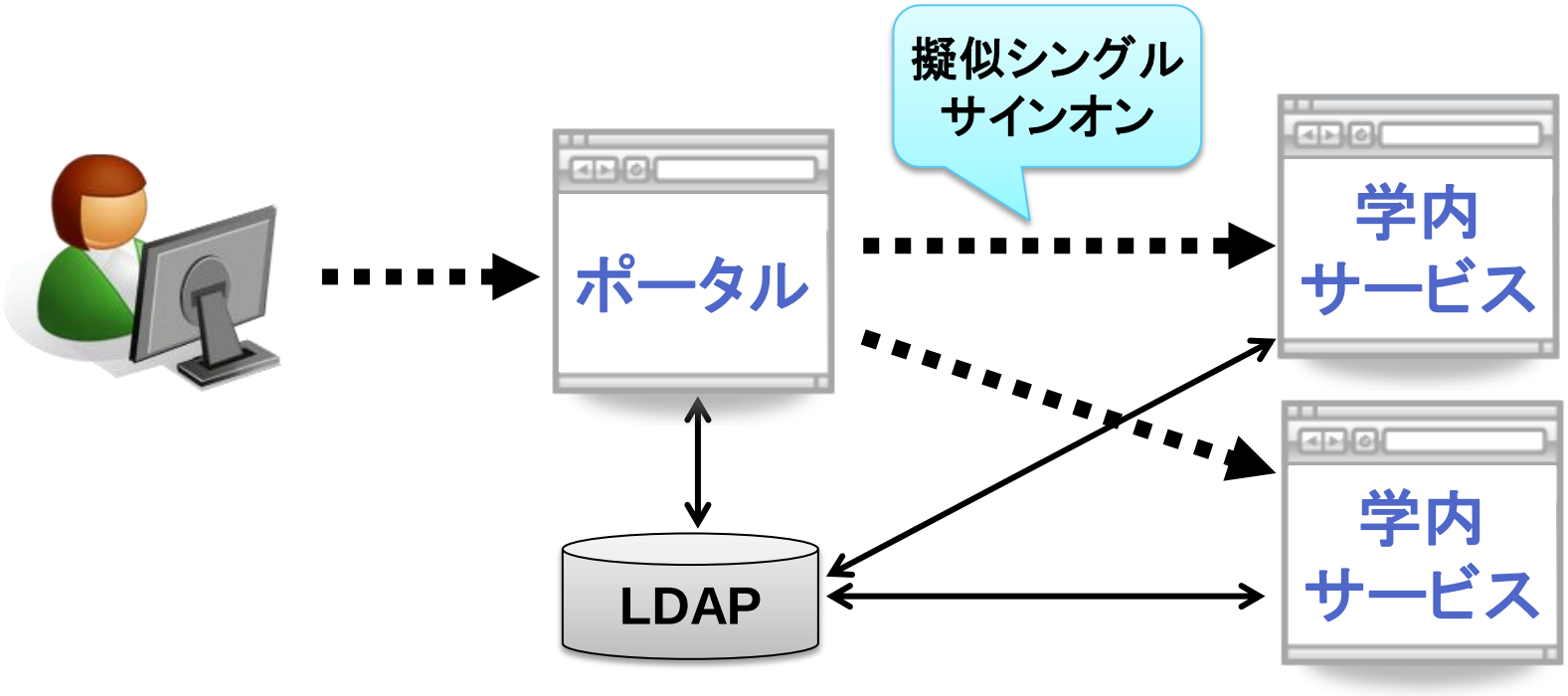
- 受け渡し先は単位互換を申請するシステム
- 学生証番号，大学メールアドレスの受け渡しは説明可

◆アクセスする際に説明画面を表示すればよい

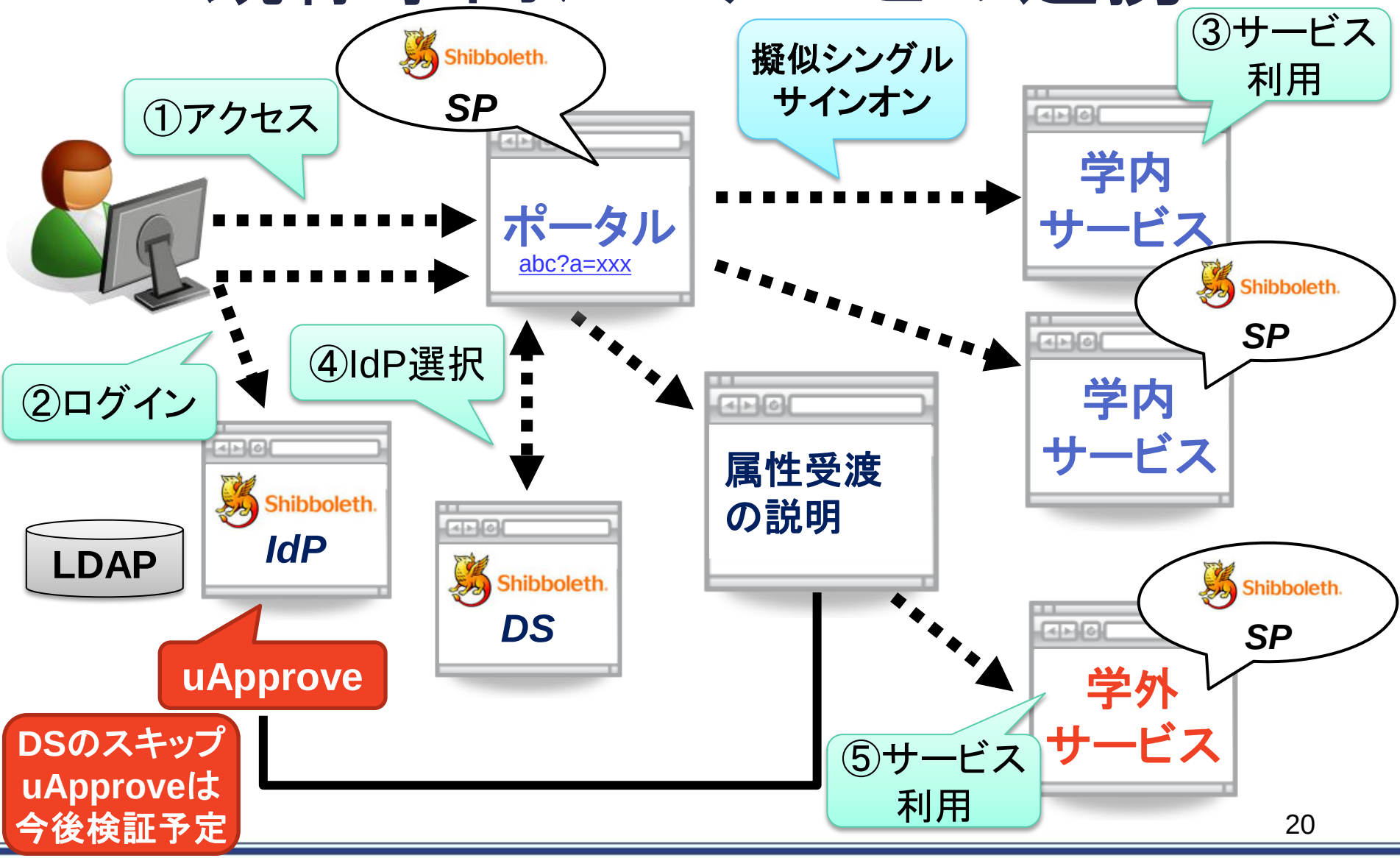
- 今回の事例では未実装
- uApproveというシステムを学認で実装中
  - SPへの属性受け渡し時に確認画面を提示
  - 必要に応じてユーザが受け渡し属性を選択可

◆利用しない人の情報は一切渡らない

既存学内システムとの連携



既存学内システムとの連携



具体的な設定

◆学内SP利用時にDS画面は不要
- 学内SPはデフォルト認証を学内IdPに向ける

◆DSがトラブルを起こしても学内は動く
- 学内IdPに学内SPのメタデータを固定でセット
- 学内SPに学内IdPのメタデータを固定でセット
- （加えて学認メタデータを自動更新設定）

◆学外SPはデフォルト認証がNIIのDSに向いている
- この場合は，IdP認証を済ませていても，アクセスするときにDS画面が出る
- ただし、学内ポータルから学外サービスへのリンクにパラメータを指定することでDS画面もスキップ可能

構築コスト

- ハードウェアは通常のサーバ
- ソフトウェアはオープンソースなので構築を内部の人間が対応できれば低コスト
  - 「学認」の方からの強力な支援もあります

- （必要に応じて）LDAPの属性追加
- 業者に委託すると…x百万？
- 学内の承認を取り付ける障壁
  - メリットの共有による障壁の低減
- 利用者へのシステム切替の説明

運用コスト

◆IdPの設定変更
- 利用したいSPが増えた時に，そのSPに渡す属性の設定
- 署名証明書の更新

◆LDAPの設定変更
- 利用したいSPから要求される属性がLDAPに登録されていなければ追加
- 既存の属性をShibbolethの機能で変換して提示することで解決できるケースもある

◆ハードウェアの保守
- 通常のサーバと同じ

◆各ソフトウェアのセキュリティアップデート
- 通常のサーバと同じ

学外連携の状況

- ◆学認SP（利用中のもの）
  - ➢FaMCUs（テレビ会議用MCUサービス）
  - ➢Eduroam-Shib（eduroam仮名アカウント発行システム）
- ◆SAML(Shibboleth) SP
  - ➢Google Apps（コンピュータ理工学部のみ）
- ◆今後の予定
  - ➢IOP（電子ジャーナル）連携
  - ➢DSのスキップ、uApproveは今後検証予定

まとめ

◆京都産業大学の事例報告

- 統合認証基盤整備と大学間共有eラーニングシステムとの連携

◆今後の展開

- 他の大学間連携事業に必要なシステムにも適用可能
- 学認は大学間共有のシステムを作成する基盤として期待できる

◆学認への期待

- 色々な学術SPの登場に期待
- クラウド事業での利用
  - すでに利用可能な例
    edubase、Google Apps