NIIオープンハウス
CSIワークショップ
平成19年6月8日(金)

これからのPKI:
～ さまざまな大学内サービスの認証・認可の統合 ～

国立情報学研究所
学術ネットワーク研究開発センター
片岡 俊幸

目次

1. さまざまな大学のサービス
2. 大学向け認証局パックの開発
3. 大学知財保護システムの実証実験
4. これからの方向性

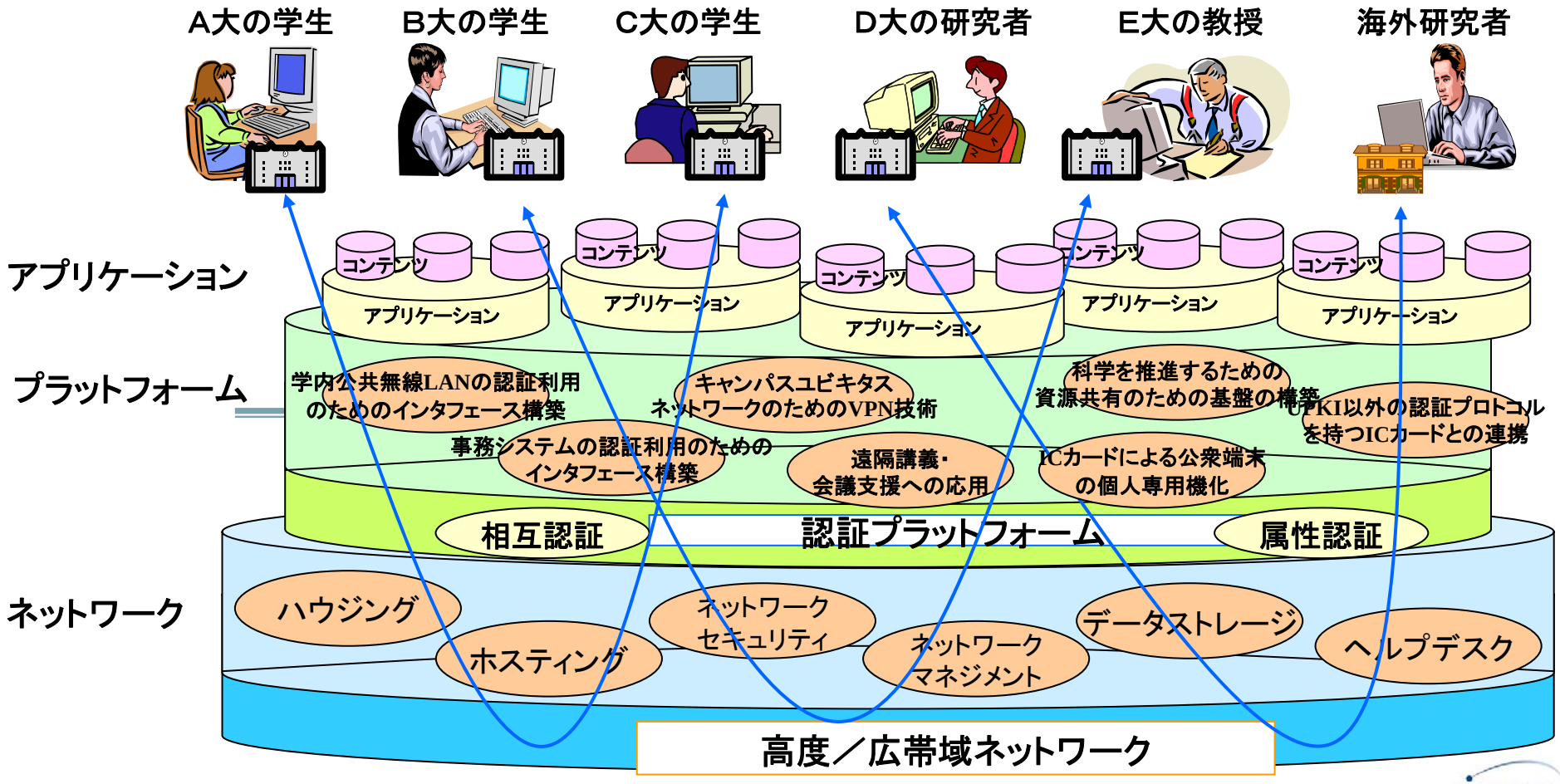
1．さまざまな大学のサービス

1-1 さまざまな大学のサービス(学内、学間)

- 認証を必要とする大学のサービス例
  - 施設管理:入退出管理、施設予約、駐車場ゲート、、、
  - 情報管理:PCログイン、ネットワークログイン、コンテンツアクセス(DB、電子ジャーナル、遠隔授業)、リモートアクセス、プリント印刷、、、
  - 事務管理:人事管理、会計管理、電子決済、、、
  - 教務事務:証明書発行、電子掲示板、履修登録、出席管理、、、
  - キャンパス:食堂キャッシュレス、売店キャッシュレス、健管センター管理
  - 図書館:貸出サービス、端末アクセス、印刷サービス
  - 他サービス:卒業生カード、卒業生コミュニティ、地域ポイントカード連携、、、
- PKIを利用すると、より安全に、安心にサービスが利用可能に!

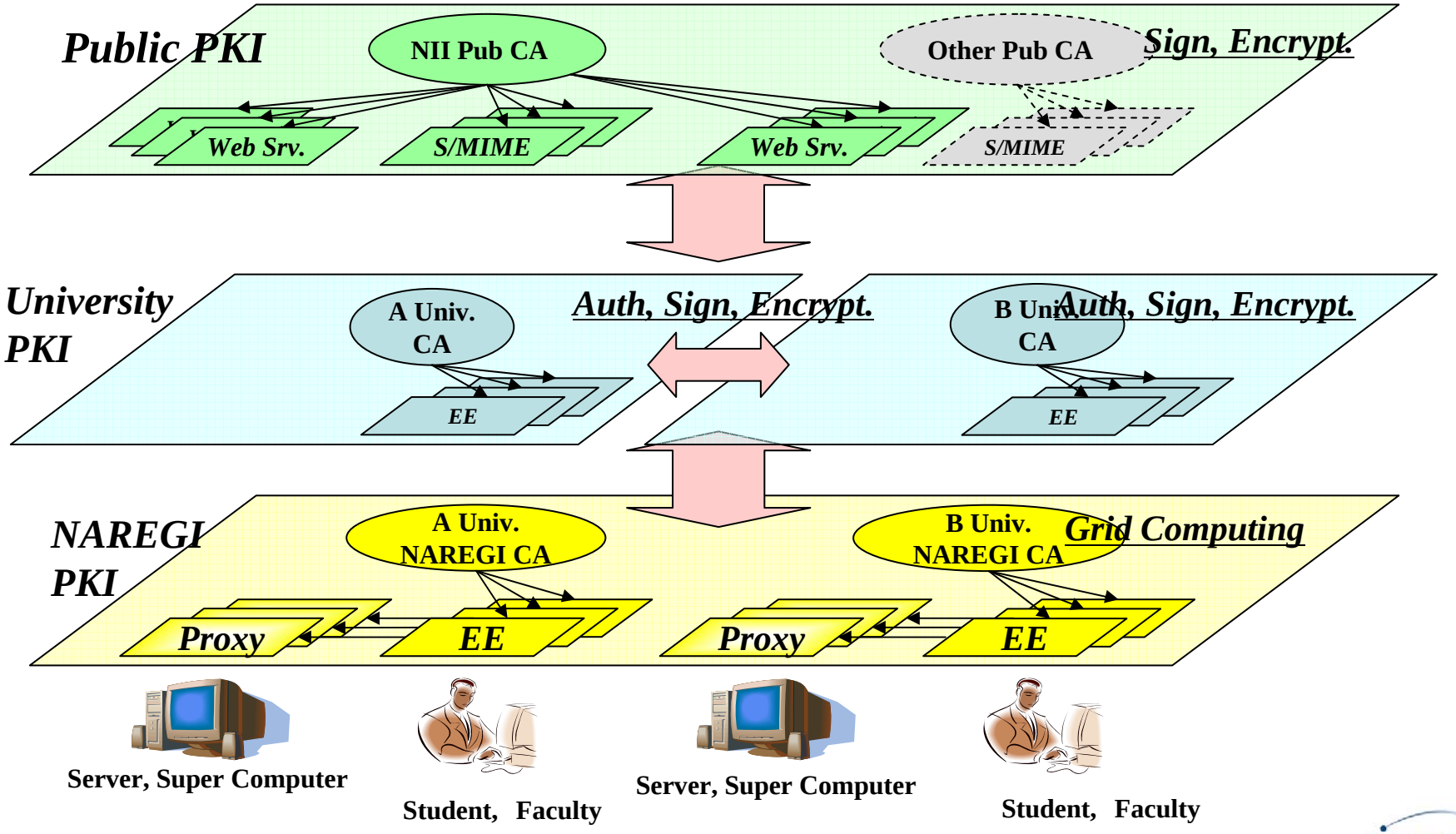
1-2 UPKI認証を利用するアプリケーション

全国共同電子認証基盤を利用した様々な個別プラットフォームを利用することで、セキュリティを確保した大学内・大学間連携のアプリケーションを安全・安心に利用することが可能となる。

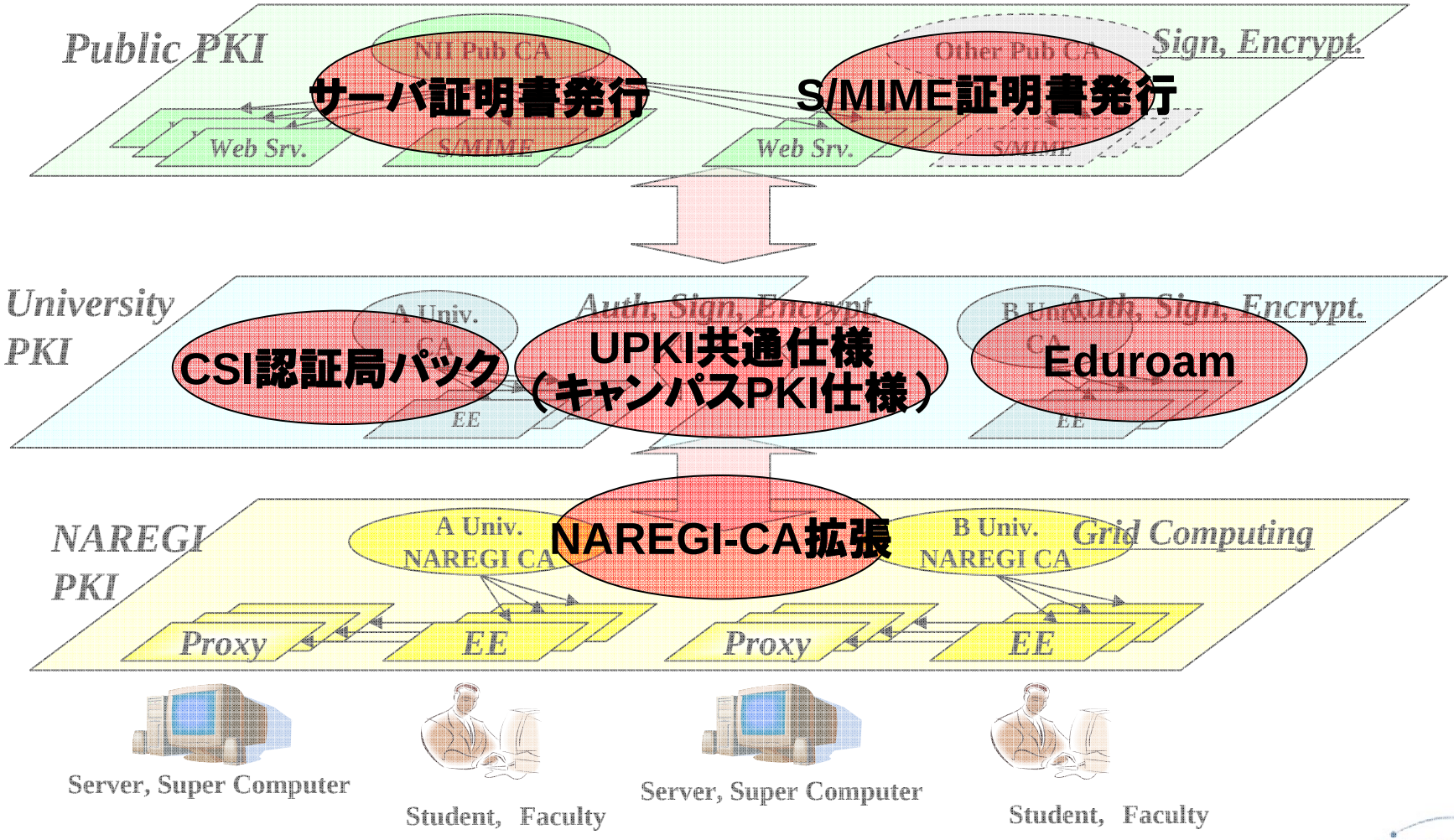


セキュリティを確保した連携を行うには、個人を認識するための認証機能は不可欠

1-3 UPKIのアプローチ



1-3 UPKIのアプローチ



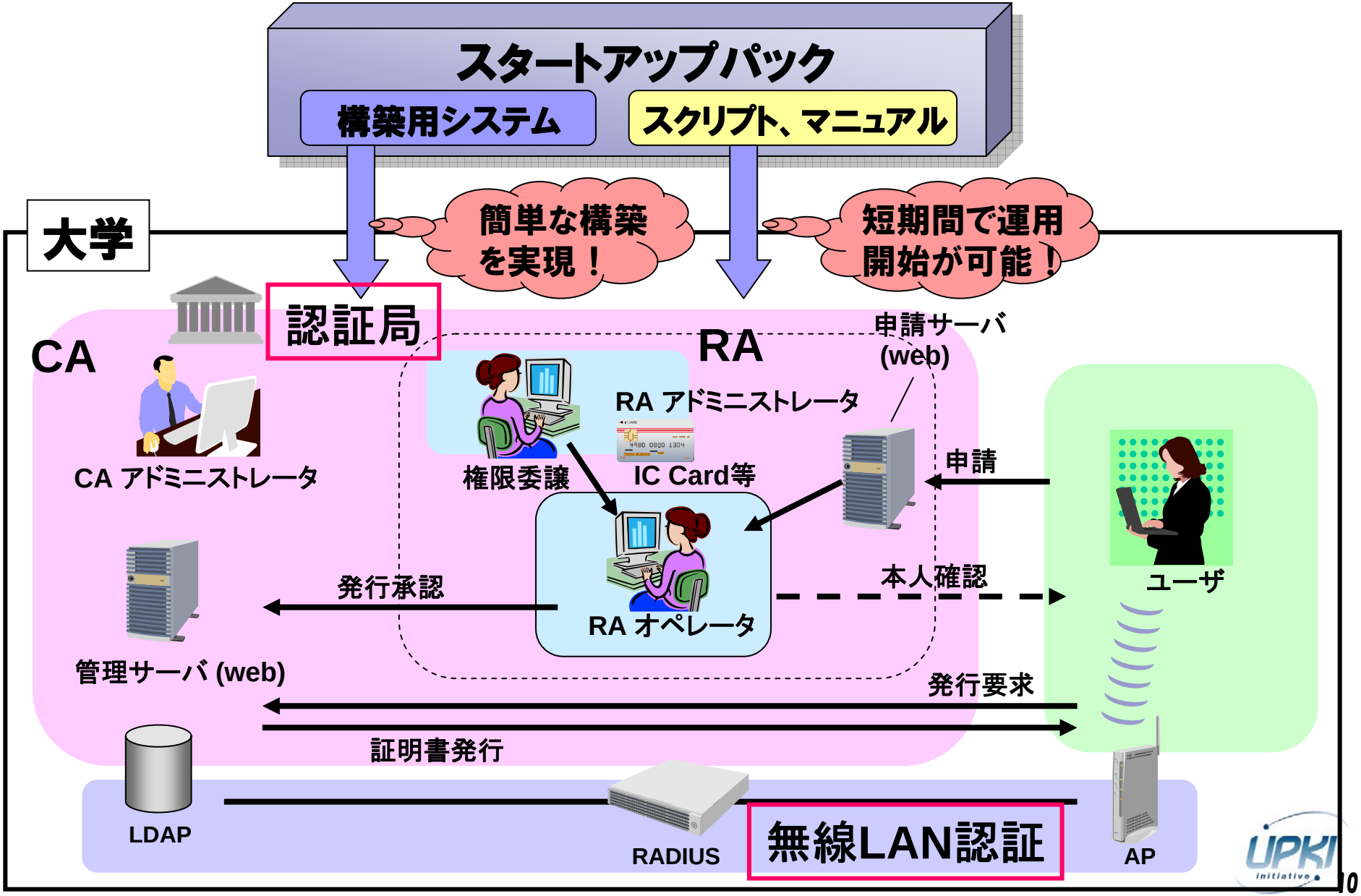
2. 大学向け認証局スタートパックの開発

2-1 大学向け認証局スタートパックとは？

学内認証局と無線LAN認証システムを簡単に構築して運用するためのパック（オープンソース、構築スクリプト、マニュアル）。

- **証明書を利用するアプリケーション**
  - 学内無線LAN認証のための証明書発行に特化した、認証局スタートパックを実現する。
  - 認証方式はサーバ証明書とクライアント証明書を利用するIEEE802.1X EAP-TLS方式とする。
- **認証局システム**
  - NAREGI(National Research Grid Initiative)で開発され、運用実績のあるNAREGI-CAを利用。
  - オープン・ソースであり、商用CA製品と同レベルの運用が可能なシステム。
  - 昨年度UPKIで開発した権限分離機能の拡張を含む。
- **無線LANシステム**
  - FreeRadiusとOpenLDAPを利用する構成。

2-2 スタートアップパックのイメージ



2-3 スタートパック内容

- スクリプト
  - インストール・スクリプト：
    - 認証局を簡単に構築するためのスクリプトを添付。
  - プロファイル：
    - 無線LAN認証の証明書発行のためのプロファイル、および、設定テンプレートを添付。
- ドキュメント
  - CSI認証局スタートアップガイド：
    - 認証局のインストール、および、無線LANと連携した認証に関する構成、設定を含めた構築方法を説明。
  - 無線LAN用認証局運用手順書：
    - 認証局の運用手順を説明。
  - 利用者用マニュアル：
    - 学内ユーザが構築した認証局を利用して証明書を取得し、これを用いて無線LANを利用する手順を説明。
- システム
  - NAREGI-CA Ver2.2

3. 大学知財保護システムの実証実験

3-1 長期署名とは？

- 電子署名
  - 研究者が執筆した論文に電子署名を行うことで、下記が可能。
    - 執筆者であることを証明。（署名証明）
    - 改ざんされていないことを証明。（非改ざん証明）
- タイムスタンプ
  - 論文にタイムスタンプを行うことで、下記が可能。
    - いつ作成した論文であるかを証明。（時刻証明）
    - 改ざんされていないことを証明。（非改ざん証明）

☑ 電子署名、タイムスタンプだけだと、、、

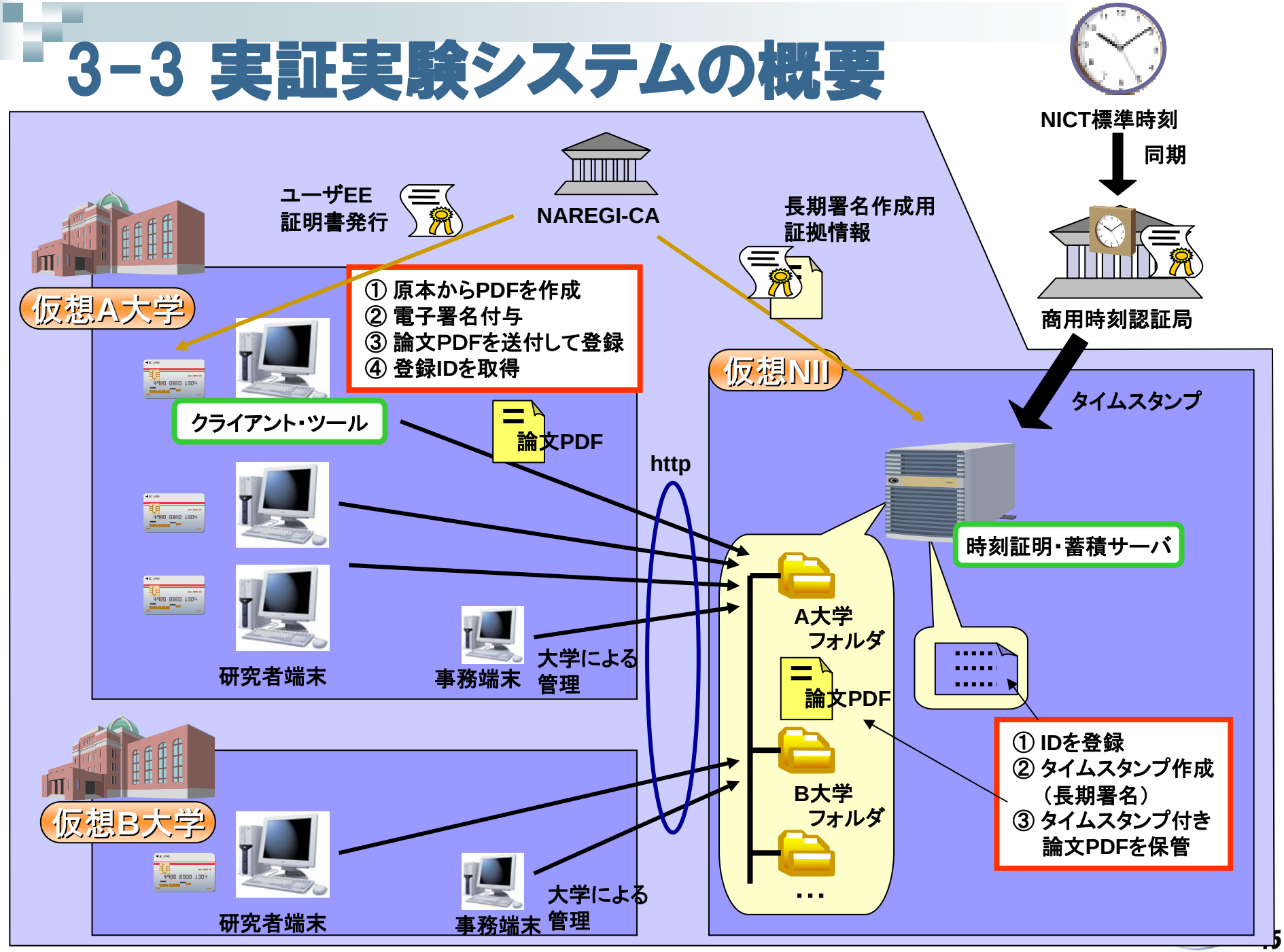
✓ どちらもデジタル署名技術を利用しており、アルゴリズム脆弱化や鍵漏洩への対応として、有効期限や失効機能を持っている。つまり、長期的に証明力を保持できない。 これを解決するために、、、

- 長期署名
  - 長期署名を行うことで、下記が可能。
    - 証明可能な期間を延長することができる。（長期証明）
  - 有効期間内に電子署名、タイムスタンプを検証するための全ての検証情報を収集、この情報を含めたデータにタイムスタンプを付与する方式。
  - 長期署名フォーマットは国際標準RFC3126に準拠。

3-2 研究知財保護システムとは？

- **研究知財保護の必要性**
  - 研究のグローバル化、論文発行数の急速な増加、研究開発競争の激化により、研究業績の確保が重要となってきた。
  - 研究業績の確証は、学会誌による論文公開。しかし、論文は学会への提出後、半年以上の査読期間の後に学会誌として発行されるため、タイムラグが生じる。
  - 大学は機関リポジトリによる研究知財の公開を進めており、今後は公開する研究知財の信頼性保証が重要。
  - 確保するべき研究知財は論文、研究アイデア、研究データ等、様々な形態で日々、大量に生成される。
- **研究知財保護システム**
  - 誰がいつ創造した研究知財かを担保する確証として、デジタル署名とタイムスタンプを利用した長期署名（国際標準RFC3126）により、上記課題を解決することを目指す。
  - 署名には大学で発行する職員証／学生証ICカードに格納された証明書の利用を想定。
  - タイムスタンプは商用時刻認証局から発行。

3-3 実証実験システムの概要



3-4 検討課題

- 信頼性のレベル
  - 署名に用いる証明書の信頼レベル？
  - タイムスタンプの信頼レベル？
  - 長期署名の信頼レベル？
- 適用範囲
  - プレプリント、論文、実験ノート、実験データ、、、？
- 研究知財保護システム
  - 長期署名の延長方法？
  - 共著者による電子署名の必要性と、その方法？
  - 機関リポジトリ等との連携？
  - 原本ファイル、長期署名付きファイルの管理方法？

4. 今後の方向性

4-1 認証と認可

- 認証と認可
  - 認証：本人性を確認すること。
  - 認可：本人の属性（所属やタイトル等）を確認して、
    資源へのアクセス制御等の判断を行うこと。

・認可の例

→ 無線LAN認証では、

無線LANにログイン後、インターネットのみ利用許可とするか、キャンパス内イントラネットの利用を許可するかの認可制御が必要。

→ タイムスタンプでは、

知財保護サーバにログイン後、各論文への署名や閲覧を許可するかの認可制御が必要。

4-2 AAI（Authentication and Authorization Infrastructure）

- AAI ＝ 認証・認可基盤
  - アプリケーションを利用するには認証に加え、認可も必要。
  - 認可の方式はアプリケーションに強く依存する。
  - 認可属性を交換する世界標準仕様として
    SAMLやShibboleth等が欧米で広く利用されており、UPKIでも調査、検討中。
  - 認可基盤は利用するアプリケーションに適応したものとすることが重要。
  - 今後、3層構造の認証基盤をベースに学内サービス、および、大学間サービスのための認可連携方式を統合したAAIを検討していくことが重要。

4-3 Shibbolethとは？

- 米国EDUCAUSE／Internet2にて2000年に発足したプロジェクト
- SAML、eduPerson等の標準仕様を利用した、認可のための属性交換を行う標準仕様とオープンソフト
- 米国、欧州の大学で利用拡大中。
- Federation例（IdP）;
  - 米国：InCommon
  - 英国：The UK Access Management
  - スイス：SWITCH
  - オーストラリア：MAMS
  - フィンランド：HAKA
  - フランス：CRU
  - ノルウェイ：FEIDE
  - デンマーク：DK-AAI
- Federation例（SP）;
  - ScienceDirect、 Ovid Technologies、JSTOR、ExLibris、 Digitalbrain、Thomson Gale等
  - Blackboard、WebCT、Moodle、OLAT、WebAssign等
  - DSpace, uPOrtal, Napster, Sharepoint, Symplicity, TWiki, Zope+Plone, eAcademy等

4-4 Shibbolethの特徴

（１）属性の分散管理＝Federation

IdP（大学）がIDと属性を管理して、SPがこれを利用

（２）プライバシ保護

ユーザの識別情報をIdP外部に公開しない仕組み

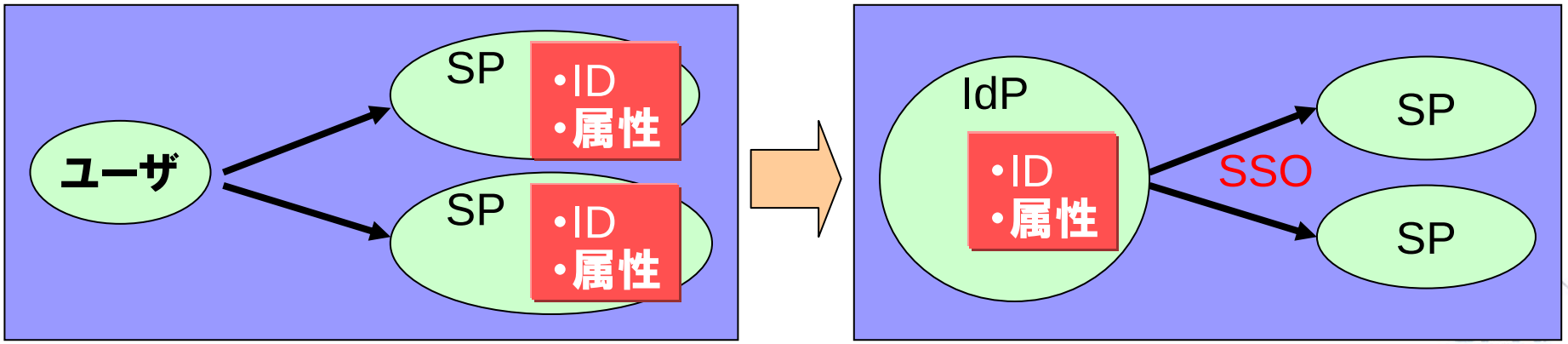
ユーザは各SPに対する各属性の公開を制御可能

（３）SSO

Webサービスのシングルサインオン

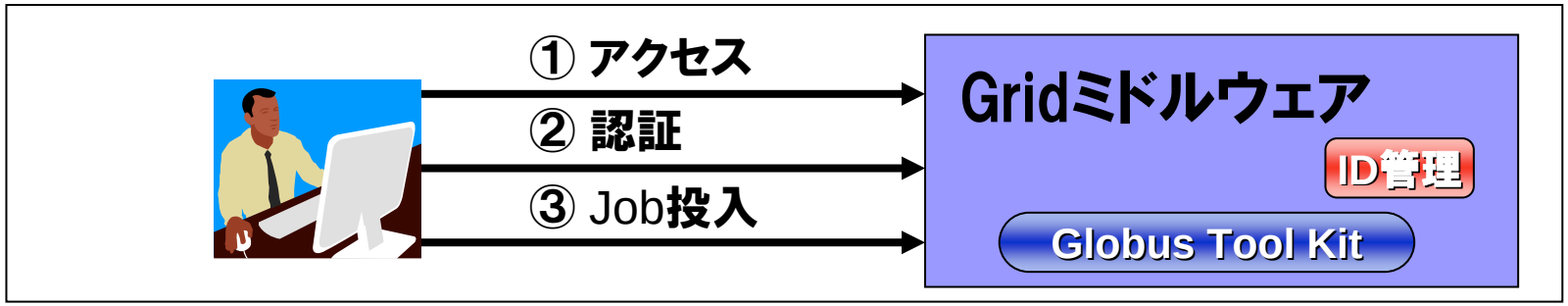
（４）学外アクセス

学外からもSPにアクセスが可能。



4-5 Gridとの連携

- Gridミドルウェアでユーザ管理を行う。



- 大学のShibbolethフェデレーションを利用。