全国大学電子認証基盤（UPKI）とその先にあるもの

京都大学学術情報メディアセンター
岡部　寿男

JNSA PKI Day 2008 〈PKIの標準から実装まで最新動向〉
2008年7月3日

岡部寿男　自己紹介

- 略歴
  - 1988年京都大学大学院工学研究科修士課程情報工学専攻修了
    並列計算の理論
  - 1988年京都大学工学部情報工学教室 助手
  - 1994年京都大学大型計算機センター研究開発部 助教授
    スーパーコンピュータ用基本ソフトウェア
  - 1998年京都大学大学院情報学研究科 助教授
    並列・分散アルゴリズム
  - 2002年より京都大学学術情報メディアセンター教授
    ネットワーク研究部門

- 履歴書には書けない経歴
  - 1985年、研究室へのUNIXマシンの導入の手伝い
  - 同年、教室内Ethernetの敷設、JUNETによる対外接続（電子メールおよびネットニュース）、学内内線電話によるUUCP接続、…
  - 1988年、WIDEプロジェクトによるインターネットへの接続（国内3番目）、BITNET接続
  - 同年、学内LAN　KUINSの運用開始
    - トラブルの嵐
  - 1990年、KUINSユーザグループ創設、初代会長
  - 1994年以降、学内ネットワークKUINSの運用担当
    - NTTマルチメディア実験 OLUプロジェクトなど…
  - 2002年より、学内ネットワーク運用の責任者
    - セキュリティ関係の業務負担増大

PKIに対する想い

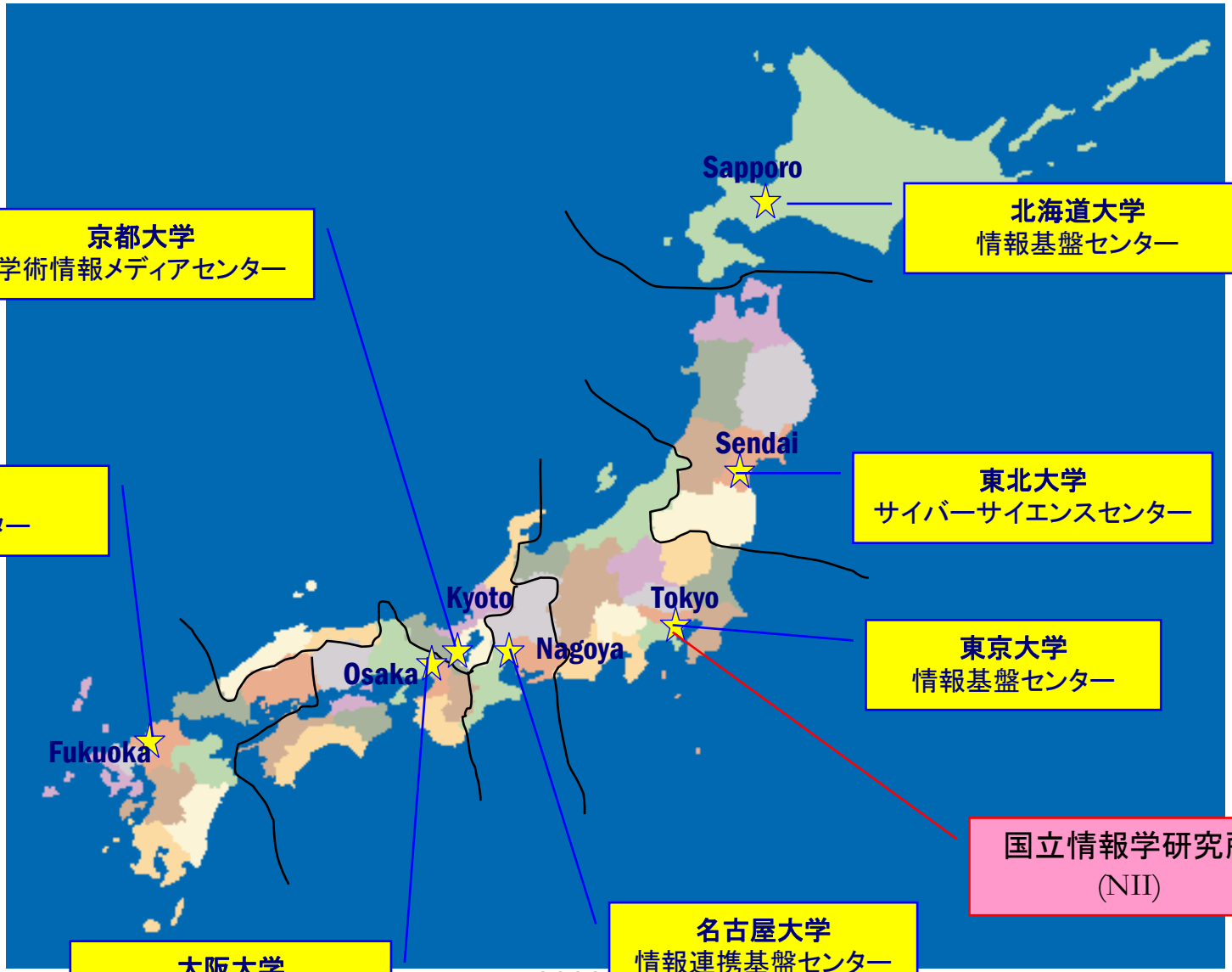
（昔）インターネット：どんどんつなげ！ (^_^)
- 1988年、WIDEプロジェクト開始
- 草創期は、あらゆる手立てを使ってとにかくつなぐことが重要だった
  - 性善説・相互扶助精神
- 接続性が無条件に善
  - 品質は二の次，best effort，セキュリティ意識希薄

（今）セキュリティ：つながっているものを切る (T_T)
- ファイアウォール、フィルタ、IDS、…

匿名性が問題

（これから） PKI: 信頼の絆をつなぐ
- どんどんつなげ！ (^_~)

全国共同利用情報基盤センター



CSI：サイバー・サイエンス・インフラストラクチャ（最先端学術情報基盤）

最先端の学術情報基盤が、今後の学術・産業分野での国際協調・競争の死命を制す

産業・社会貢献

国際貢献・連携

バーチャル研究組織

世界的ソフトウェア及びDBの形成

人材育成及びノウハウの蓄積

NIIと大学図書館等との連携による
学術コンテンツの構築・提供，機関リポジトリの形成

次世代スパコンを含む大学・研究機関の計算リソースの整備

ミドルウェア

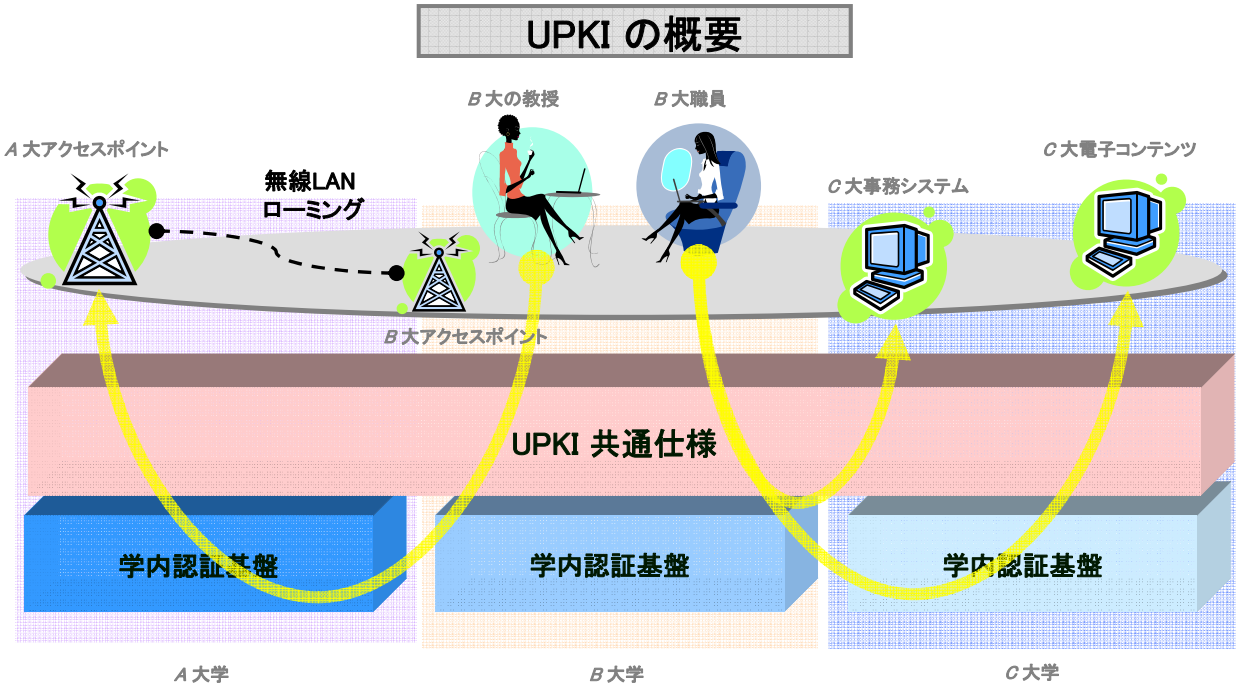
連携ソフトウェアとしての研究グリッドの実用展開

大学・研究機関としての認証システムの開発と実用化

NIIと大学情報基盤センター等との連携による
次世代学術情報ネットワークの構築・運用（SINET3）

大学間連携のための
全国共同電子認証基盤（UPKI）とは

- 最先端学術情報基盤(Cyber Science Infrastructure)実現のため，大学等が保有する，教育・研究用計算機，電子コンテンツ，ネットワークおよび事務システムなどの学術情報資源を安心・安全かつ有効に活用するための電子認証基盤
- PKI（公開鍵認証基盤）を活用



UPKIのこれまでの経緯

- 平成16年度：

  全国共同利用情報基盤センター長会議（構成：7大学情報基盤センター＋NII）の下に「認証研究会」を設置

- 平成17年度：

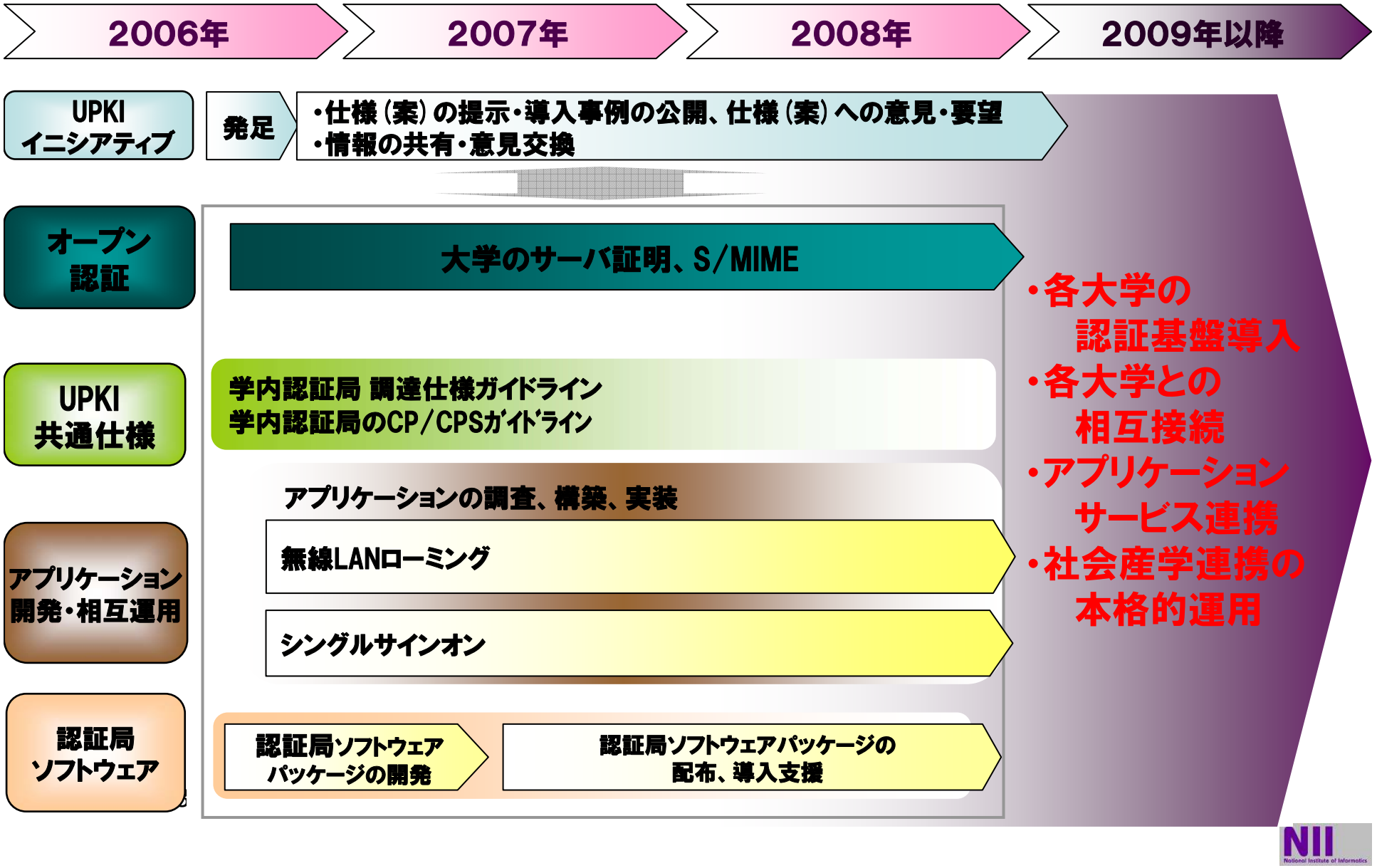
  国立情報学研究所 ネットワーク運営・連携本部の下に「認証作業部会」を設置（構成：7大学情報基盤センター，東工大，KEK，NII）

- 平成18年度：

  文部科学省特別教育研究経費（大学間連携経費）
  「大学間連携のための全国共同電子認証基盤構築事業」
  （平成18年度～平成20年度）がスタート
  - 7大学+NIIで認証基盤とアプリケーションの開発等を開始

  認証作業部会を中心として，UPKIの構築を推進
  UPKIイニシアティブの設立

UPKI構築の全体スケジュール



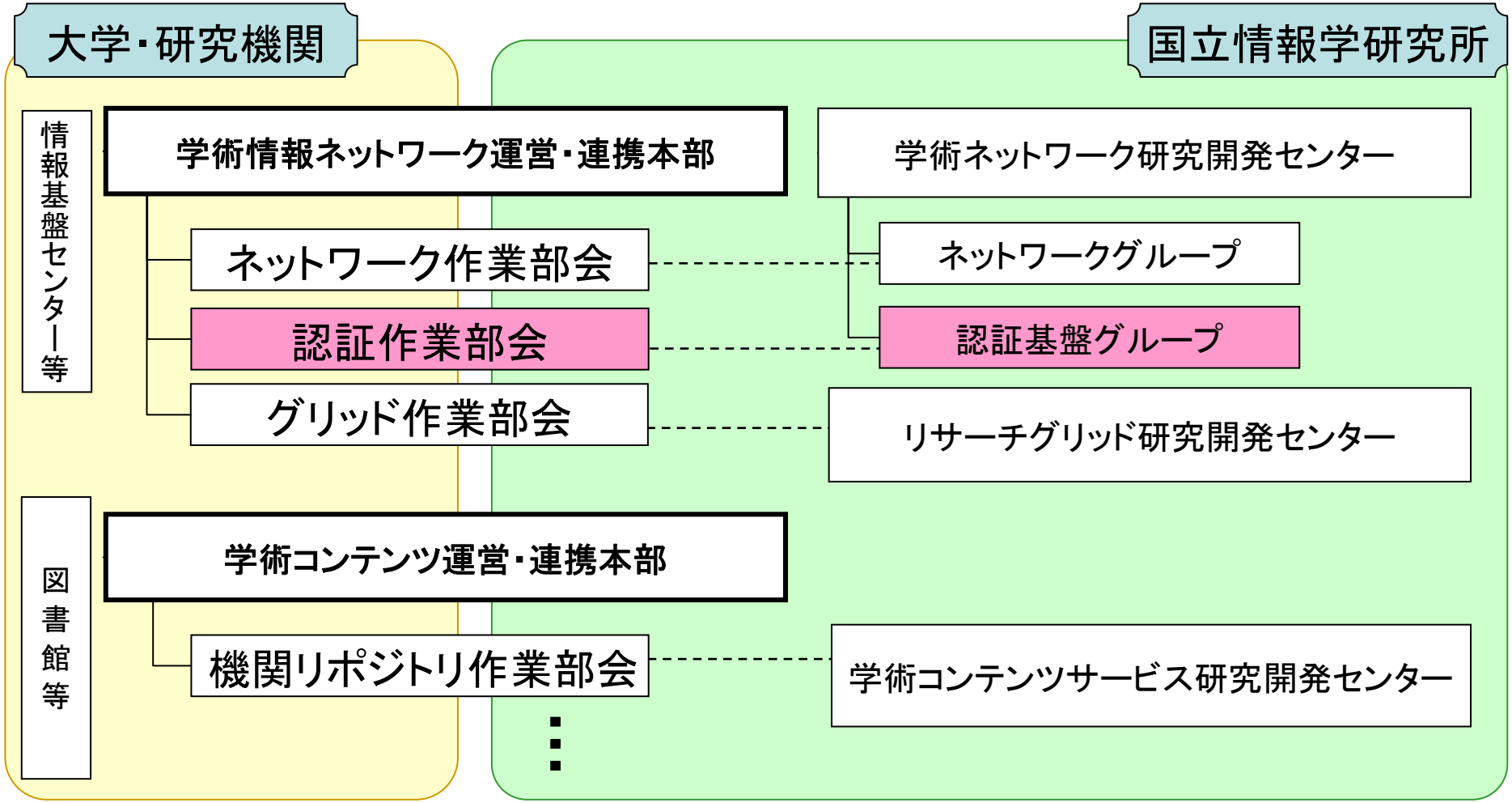
国立情報学研究所
ネットワーク運営・連携本部　認証作業部会

（委員）
- 岡部 寿男（京都大学学術情報メディアセンター 教授）… 主査
- 曽根原 登（国立情報学研究所 教授）…… 幹事
- 高井 昌彰（北海道大学情報基盤センター 教授）
- 曽根 秀昭（東北大学サイバーサイエンスセンター 教授）
- 佐藤 周行（東京大学情報基盤センター 准教授）
- 平野　 靖（名古屋大学情報連携基盤センター 准教授）
- 馬場 健一（大阪大学サイバーメディアセンター 准教授）
- 鈴木 孝彦（九州大学情報基盤センター 准教授）
- 飯田 勝吉（東京工業大学学術国際情報センター 准教授）
- 湯浅 富久子（高エネルギー加速器研究機構計算科学センター 准教授）

- 中村 素典（国立情報学研究所 特任教授）
- 後藤 英昭（東北大学サイバーサイエンスセンター 准教授）

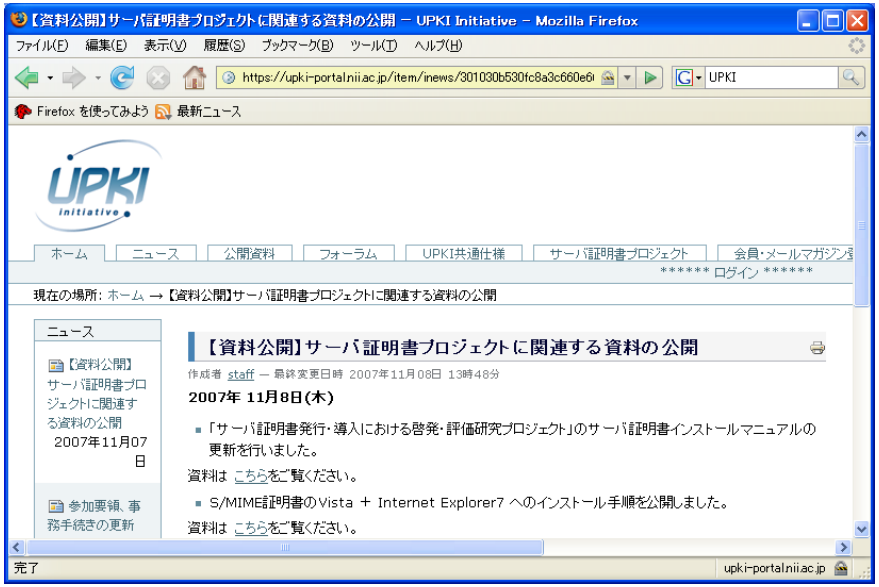
（オブザーバ）
- 谷本 茂明（国立情報学研究所 客員教授）
- 片岡 俊明（国立情報学研究所 特任准教授）
- 島岡 政基（国立情報学研究所 特任准教授）

CSIの実施体制


大学・研究機関
国立情報学研究所
情報基盤センター等
学術情報ネットワーク運営・連携本部
学術ネットワーク研究開発センター
ネットワーク作業部会
ネットワークグループ
認証作業部会
認証基盤グループ
グリッド作業部会
リサーチグリッド研究開発センター
図書館等
学術コンテンツ運営・連携本部
機関リポジトリ作業部会
学術コンテンツサービス研究開発センター
学協会
関連機関

UPKIイニシアティブの発足

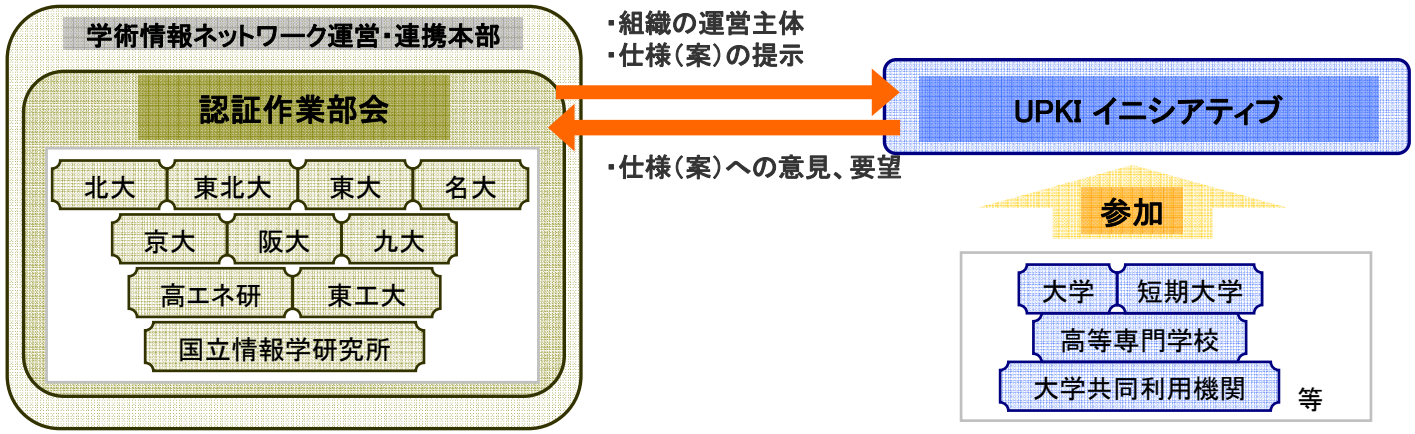
- UPKIの相互運用性，利用促進に関しての意見交換や技術的な検証を行う場として設立（2006年8月16日）
- 運営主体は認証作業部会
- UPKIイニシアティブの活動は，主にホームページ上のUPKIポータルを使用（https://upki-portal.nii.ac.jp/）
- ポータル内にフォーラムを設置し，テーマ毎に議論を実施
- オフラインでの勉強会等も計画中



UPKIの研究開発・連携体制

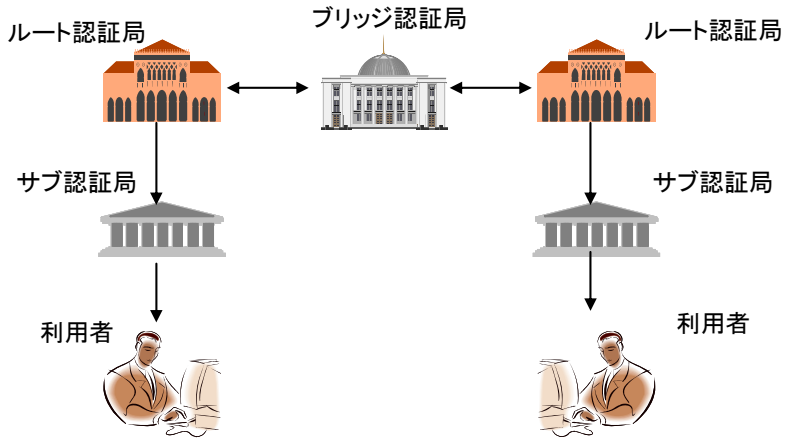
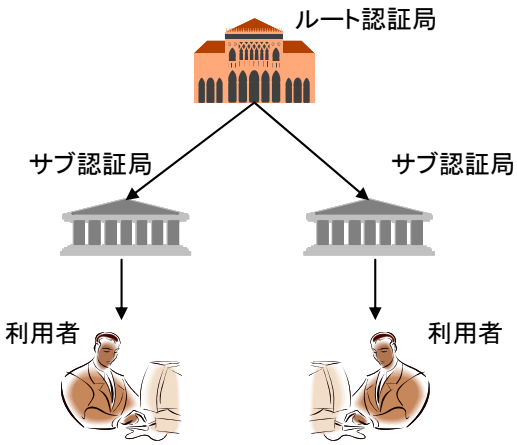
- 「大学間連携のための全国共同電子認証基盤構築事業」
  文部科学省（平成18年度～平成20年度）

- 国立情報学研究所内に設置した学術情報ネットワーク運営・連携本部内の認証作業部会を中心として研究開発を推進。
- 認証作業部会が検討した仕様案をUPKI イニシアティブに公開し、イニシアティブ参加者の意見や要望を取入れ認証基盤の構築を進める。



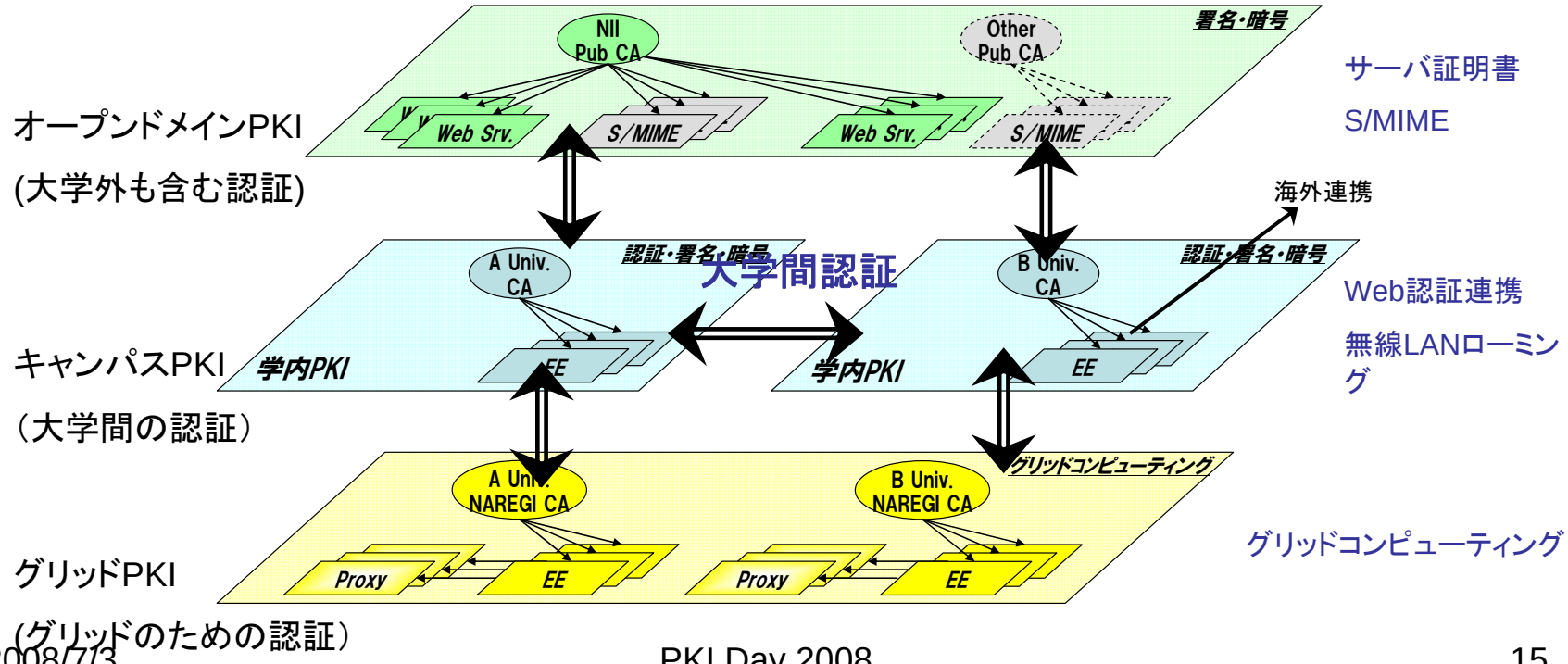
UPKIの基本アーキテクチャ

ブリッジ型とルート型（階層型）の比較

	ブリッジ型	ルート型（階層型）
イメージ		
代表事例	F-PKI（米国）/GPKI、JPKI　等	企業内認証局/証明書発行サービス会社　　等
メリット	・トラストアンカーが一つのため、信頼ドメインの拡張が容易 ・各ドメインの独立性が高い ・機関ごとにCP/CPSが策定可能	・簡単でわかりやすい ・証明書検証が簡単
デメリット	・信頼ドメイン構築にポリシーマッピング等の専門知識が必要なため導入しにくい ・ブリッジCAの製品仕様にブリッジによる信頼ドメイン構築の制約を受ける	・ルートCAの認証ポリシー及び証明書ポリシーに無条件で従う ・サブCA独自の認証ポリシーは定義できない。 ・ルートの署名鍵が危胎化したらルートCA以下の証明書が無効になり、再発行を余儀なくされる。

UPKIの基本アーキテクチャ

- 3階層のPKI (Public Key Infrastructure)による役割分担と連携



各PKI層のコンセプト

- オープンドメインPKI
  - いわゆるパブリックPKI
  - ルート証明書が予め配布されたPKI
  - 皆が信頼しているPKI、誰でも検証できるPKI
- キャンパスPKI
  - 各大学が個別のポリシに合わせて構築するプライベートPKI
  - その大学のユーザ(教職員and/or学生)であることを証明する
  - ユーザ(教職員and/or学生)への厳格な(対面等の)配付が可能

  ☆キャンパスPKI間の横の連携には別の仕掛けが必要
- グリッドPKI
  - AP Grid PMAなどグリッド独自のセキュリティレベル
  - プロキシ証明書など一般的なPKIとは明らかに異なる概念

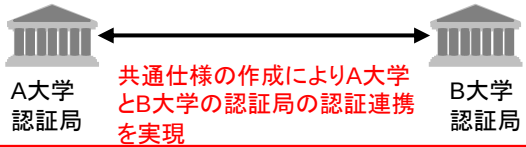
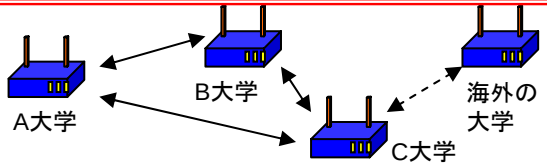
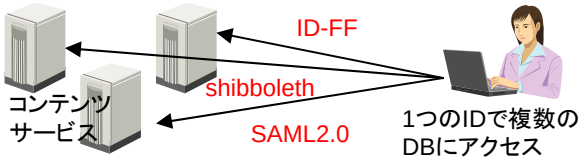
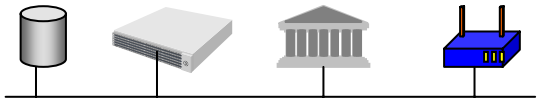
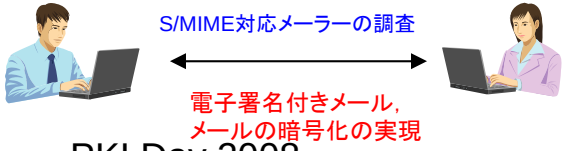
用途に応じたPKI層の使い分け

領域	用途	利用する証明書	ポイント
学外(公衆)	サーバ認証	オープンドメインPKIによるパブリックなサーバ証明書	誰でも検証できること
	クライアント認証	キャンパスPKIによるユーザ証明書をベースとしたID連携	保証レベルの担保
	S/MIME(署名・暗号)	オープンドメインPKIによるパブリックなS/MIME証明書	誰でも検証できること
学内	サーバ認証	オープンドメインPKIによるパブリックなサーバ証明書	ルート証明書の配布
	クライアント認証	キャンパスPKIによるプライベートなユーザ(教職員and/or学生)証明書	特定の認証局からのみ検証できること
	暗号	学外同様S/MIMEを利用、または共通鍵による暗号化＋クライアント認証等によるアクセス制御	鍵預託・鍵更新
	署名	キャンパスPKIによるプライベートなユーザ(教職員and/or学生)証明書	本人による鍵生成 または認証局による厳密な鍵ペア配
グリッド	MyProxy認証	グリッドPKIによるグリッドユーザ(グリッド利用者)証明書	
	Delegation	グリッドPKIのグリッドユーザ鍵ペアによるプロキシ証明書	ユーザによる権限委譲

各PKI層の位置づけ

	オープンドメインPKI	キャンパスPKI	グリッドPKI
適用領域	インターネット	各大学内	全国共同利用センター
目的	インターネット上での認証、署名・暗号など	学内NW・システムへの安全なアクセス	計算機資源の安全な共有
用途	主にSSL/TLS認証、その他S/MIME署名・暗号など	Web SSO、VPN、無線LAN（802.1X）、申請・署名アプリ（成績証明書、事務ペーパレス化等）	プロキシ証明書の発行など
証明書発行対象	サーバ、自然人など	教職員、学生など	各地域の計算機資源、計算機利用者など
信頼者（Relying Party）	不特定多数	主に学内関係者	計算機利用者
認証局の運用	オープンドメイン認証事業者など	アウトソース 、インソースなど	全国共同利用センター

これまで実現したUPKIの成果

項番	事項	内容
1	「UPKI共通仕様」の作成と配布	 「UPKI共通仕様」の利用により大学での ・学内認証局の構築 ・CP/CPS等の規程の整備 が容易に実現可能に
2	オープンドメイン認証局の構築とサーバ証明書の発行	 オープンドメイン認証局の構築により，全世界に通用するサーバ証明書を発行し，大学のWebサーバの実在性証明と通信の暗号化を実現
3	大学間無線LANローミングの実現	 eduroamによる大学間無線LANローミングを実現。海外のeduroam参加機関との連携も実現
4	コンテンツサービスのシングルサインオン実験	 各種データベースサーバへのシングルサインオンを実現するため，shibboleth，SAML2.0等の仕様を調査し，UPKIにふさわしい方式を検討
5	NAREGI-CAを利用した認証局ソフトウェアパッケージの開発	 オープンソースの認証局ソフトウェアあるNAREGI-CAを用いて，認証局を簡単に構築し，無線LAN認証を容易に実現できるソフトウェアを開発 これにより，大学の認証局構築を促進する
6	S/MIME証明書の試験利用	 S/MIME証明書を，認証関係者間で試験利用するとともに，対応メーラーの調査，WebメールでのS/MIME利用の調査研究を実施

(1) UPKI共通仕様の制定

UPKI共通仕様の制定

「UPKI共通仕様」では、各大学において、キャンパスPKIを導入する際の参考となる**共通仕様（キャンパスPKI共通仕様、相互運用性仕様）**を作成し、PKI導入に対する将来の**連携性確保***や**コスト削減****等を狙いとする。

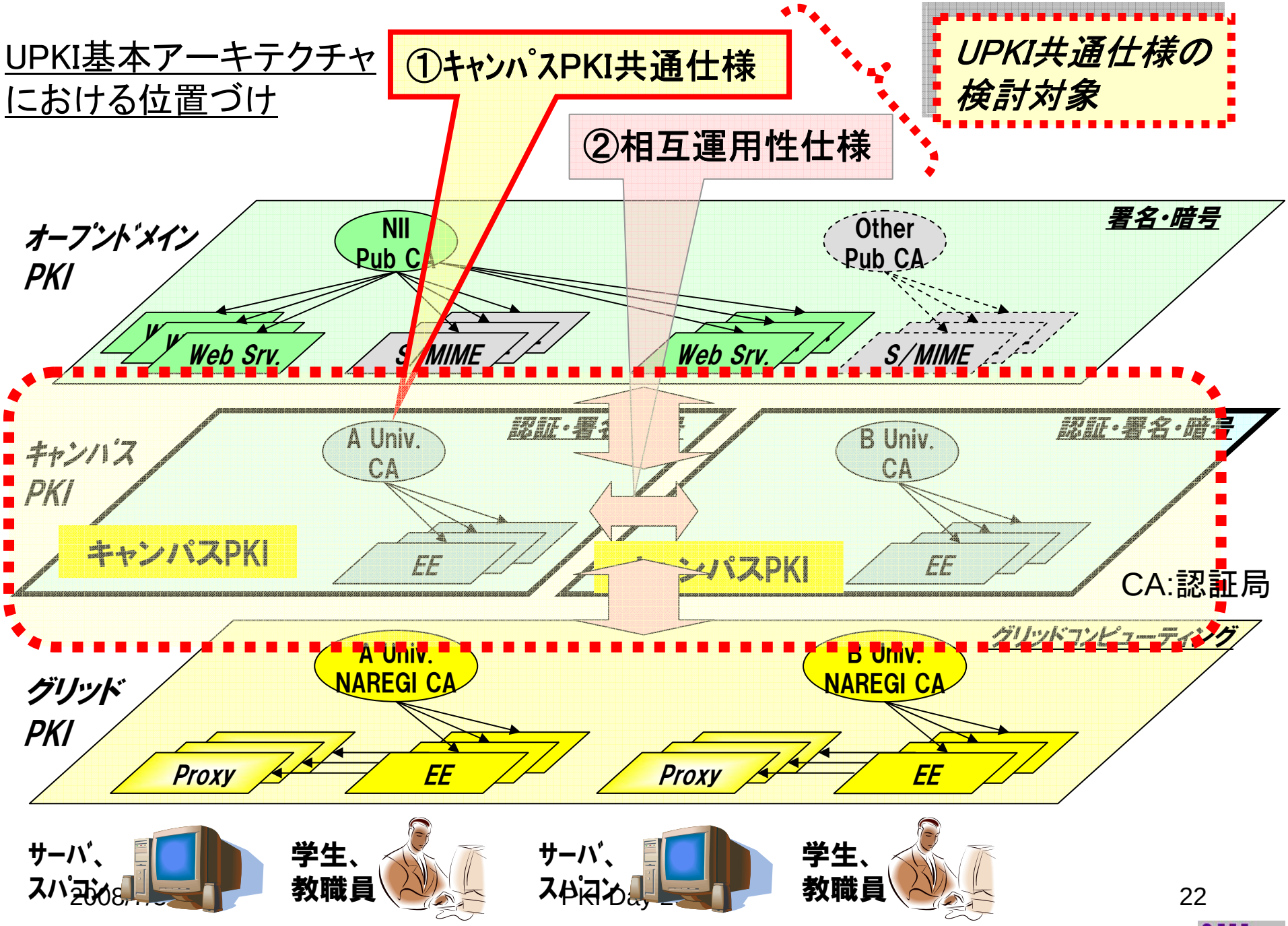
＊：連携性確保
- 大学間の相互運用性を考慮した共通仕様の採用
- 保証レベルの平準化 ⇒連携時の情報セキュリティの問題を解消

＊＊：コスト削減
- キャンパスPKI導入検討・構築コストの削減
- CP/CPS策定コスト・運用コストの削減

⇒各大学での認証局構築における金銭的・人的コストを低減

ガイドライン公開により
キャンパスPKI導入を促進！！

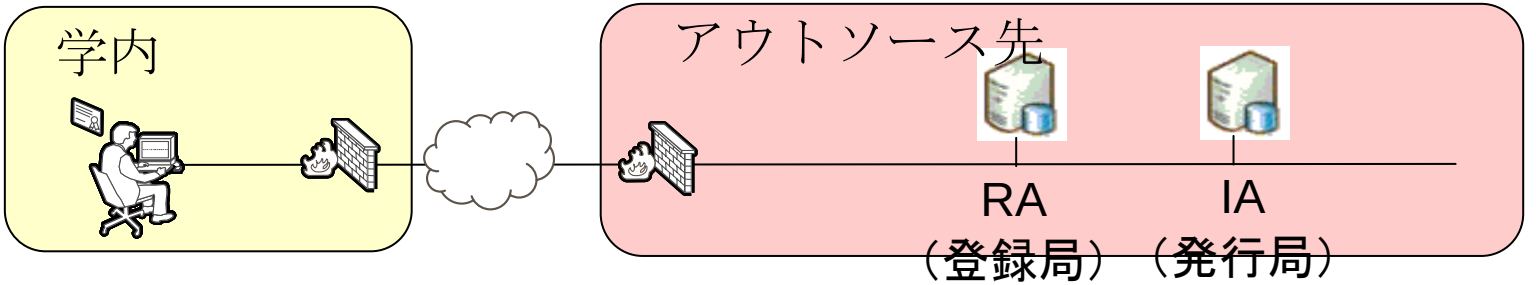
UPKI基本アーキテクチャにおける位置づけ



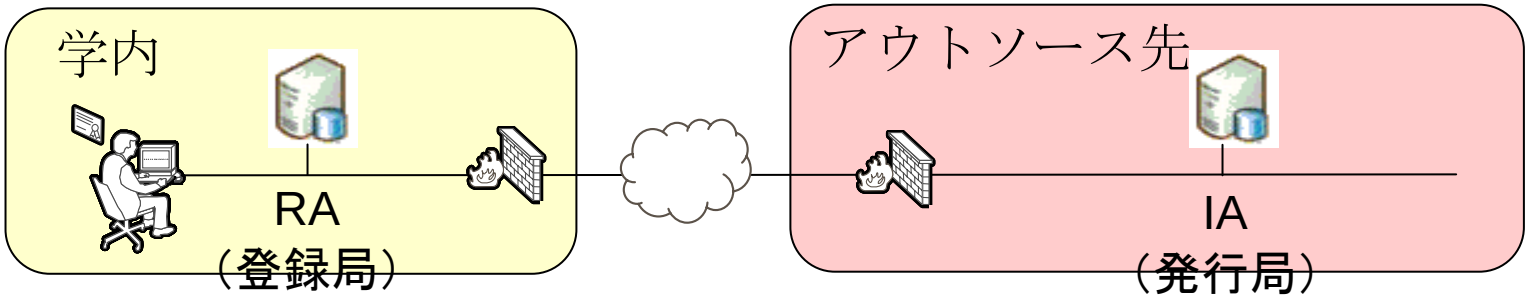
認証局(CA)の運用モデルの検討

H18年度、アウトソースモデルの共通仕様を公開

フルアウトソースモデル

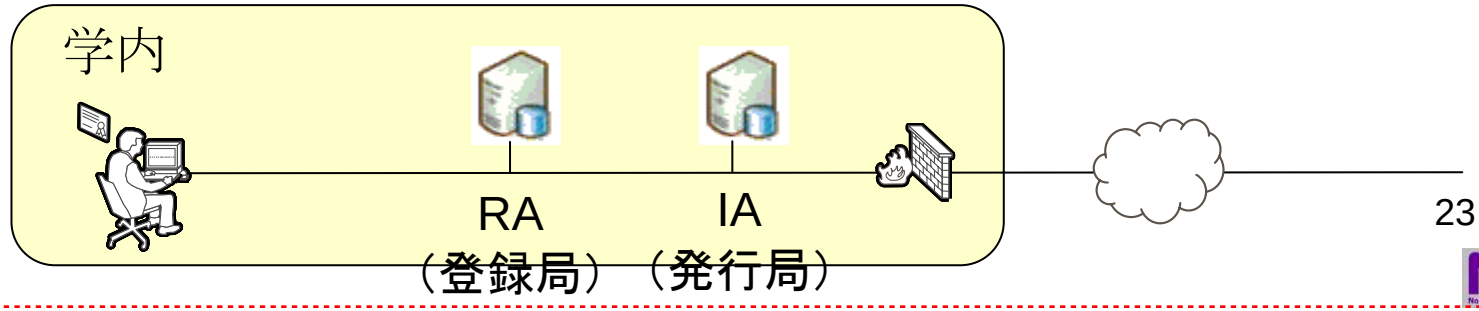


IAアウトソースモデル



インソースモデル

H19年度は、インソースモデルの共通仕様を公開



キャンパスPKI共通仕様（ガイドライン）の作成

先行大学の調査結果を踏まえて、**キャンパスPKI共通仕様**として以下に示すガイドラインを作成した。

(1)作成にあたって：キャンパスPKIガイドラインの作成にあたっては、以下の点に留意した。

- 各大学の調達・設計における参考資料、たたき台、雛形として活用できること
- 必ずしも準拠性を求めるものではないが、将来的に相互接続を想定している場合には本仕様に準拠することが望ましい

(2)ガイドラインの構成：

キャンパス PKI共通仕様

- **(1)ガイドライン利用の手引き**
- **(2)キャンパス PKI 調達仕様ガイドライン**
  - ①キャンパス PKI調達仕様ガイドライン編
  - ②キャンパス PKI調達仕様テンプレート編
- **(3)キャンパス PKI CP/CPSガイドライン**
  - ①キャンパス PKI CP/CPSガイドライン編
  - ②キャンパス PKI CP/CPSテンプレート編

■調達仕様ガイドラインでの記述例

3.2.2　RAサーバアプリケーション要件

(2)ログ収集機能
★登録局サーバを操作した全てのログについて操作日時、アクセス元端末特定情報、操作者、操作時刻、リクエスト先、イベント内容、リクエスト結果が分かる記録を取得できること
★操作者を認証し、ログの検索、参照を可能とすること
★ログの改ざん検知が可能であること
(3)個人情報連携機能
★利用者の情報を予め信頼しているデータベース等と照合するかCSV形式で入出力し、その存在性、同一性の確認ができること
(4)メールによるサーバ証明書配付、通知機能
☆指定された申請者のメールアドレスに対し、証明書の取得方法、あるいは証明書ファイルを送付できること＊（主に機器に対して証明書を発行した場合で機器の管理者に対して配付する方法として）

本章は認証システム及びICカードに関して必要（★）、ある方が望ましい（☆）と思われる要件を示す。各大学の要件に応じて追加すべき内容及び相互認証を行う上で将来的に調整が必要な内容が含まれることに留意すること。

■CP/CPSガイドラインでの記述例

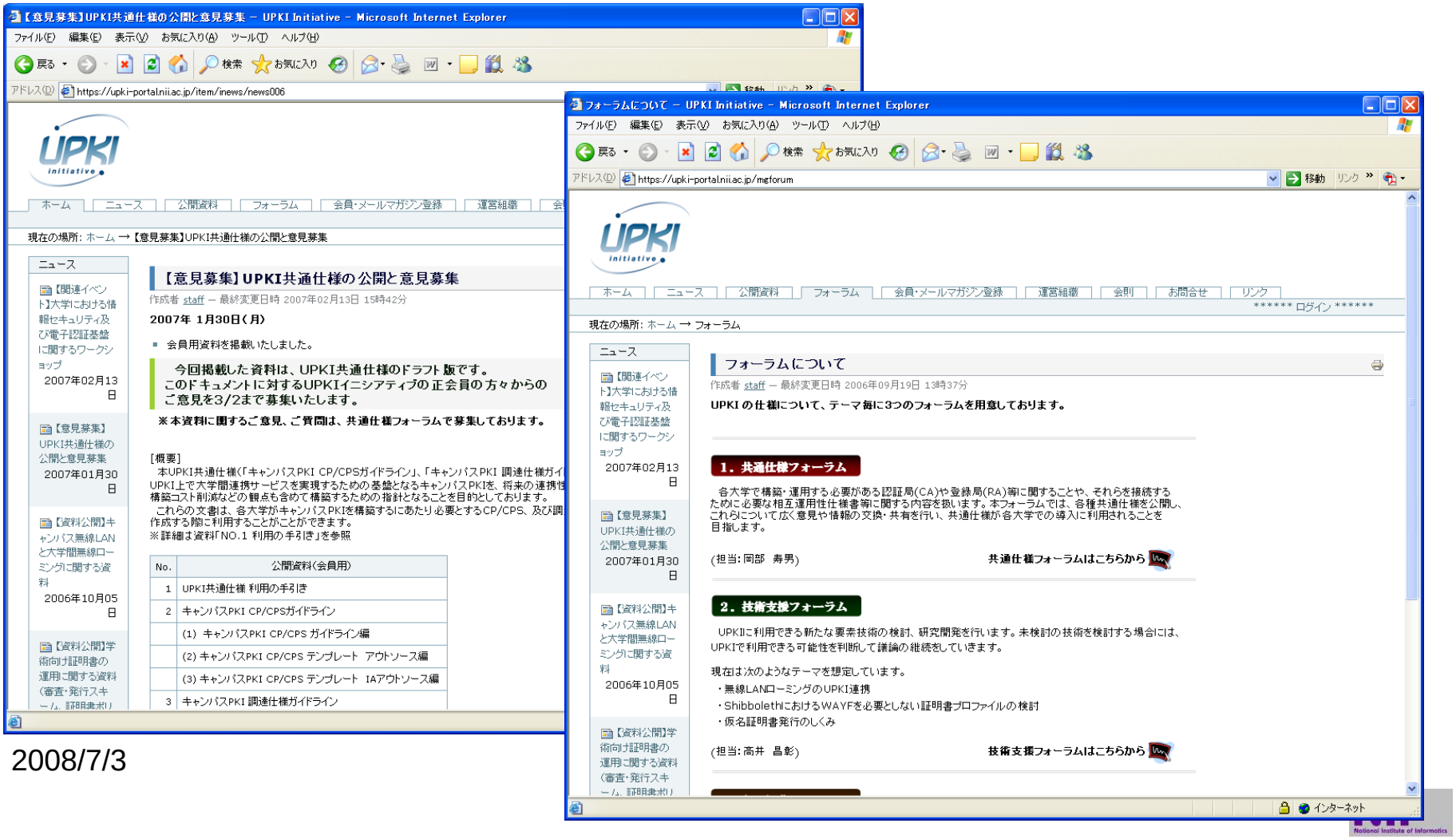
4.1.1　概要
【解説】
本節では認証局の名前、サービス名、大枠のサービス内容、相互認証を行う等の宣言を行い、認証局の概要について記す。また、相互認証の方式についても簡単に定義しておくことが望ましい。

【記述例】
1　はじめに
〇〇電子認証局は、〇〇大学により運営され、〇〇大学内及び大学間のサービスにおける電子認証のために必要となる電子証明書（以下、「証明書」という）を発行する。
本文書において、「〇〇 電子認証局（以下、「本認証局」という）」の権利または義務は国立大学法人たる〇〇大学 に帰属することを意味する。
本認証局は、大学間のサービスを共有するために相互認証接続を行う 。

上記のように、ガイドラインの各章において、それぞれ解説と記述例を示し、理解し易いようにしている。

UPKIイニシアティブにて公開

UPKIイニシアティブホームページで一般公開
（https://upki-portal.nii.ac.jp/）



2008/7/3

効果（想定）

- 共通仕様化による効果
  - 費用削減：最初から作成する場合に比べ、調達仕様、CP/CPSに関わる費用を約半分に削減可能
  - 期間短縮：先行大学の共通項をモデル化した標準モデル提供により、大学固有部分の検討に集中できるため、構築期間短縮が可能
- 連携性確保による効果
  - 保証レベルの平準化：単位互換等、大学間連携の際における情報セキュリティ面の問題を解消できる
  - 国際接続：国際的に通用するグリッド用利用者証明書の発行審査にキャンパスPKIから発行された証明書が利用可能に（現在、検討中）

（参考）「国立大学法人等における情報セキュリティポリシー策定作業部会と電子情報通信学会 ネットワーク運用ガイドライン」の規程群のうち，認証に関わる部分については，『UPKI共通仕様』が参照されている。

- http://www.nii.ac.jp/csi/sp/doc/sp-sample-fy2007.pdf

（参考） 国立大学法人等における情報セキュリティポリシー策定

～高等教育機関の情報セキュリティ対策のためのサンプル規程集～

国立情報学研究所
国立大学法人等における情報セキュリティポリシー策定作業部会
電子情報通信学会
ネットワーク運用ガイドライン検討WG

http://www.nii.ac.jp/csi/sp/

大学の情報セキュリティポリシー策定に関する背景

【背景】

•大学における情報セキュリティレベルの向上は急務

↓

•セキュリティポリシー、実施規程、教育テキストの作成が必要

↓

•大学における教育・研究との関係および組織・運営の考慮や、広範な専門知識が求められる

↓

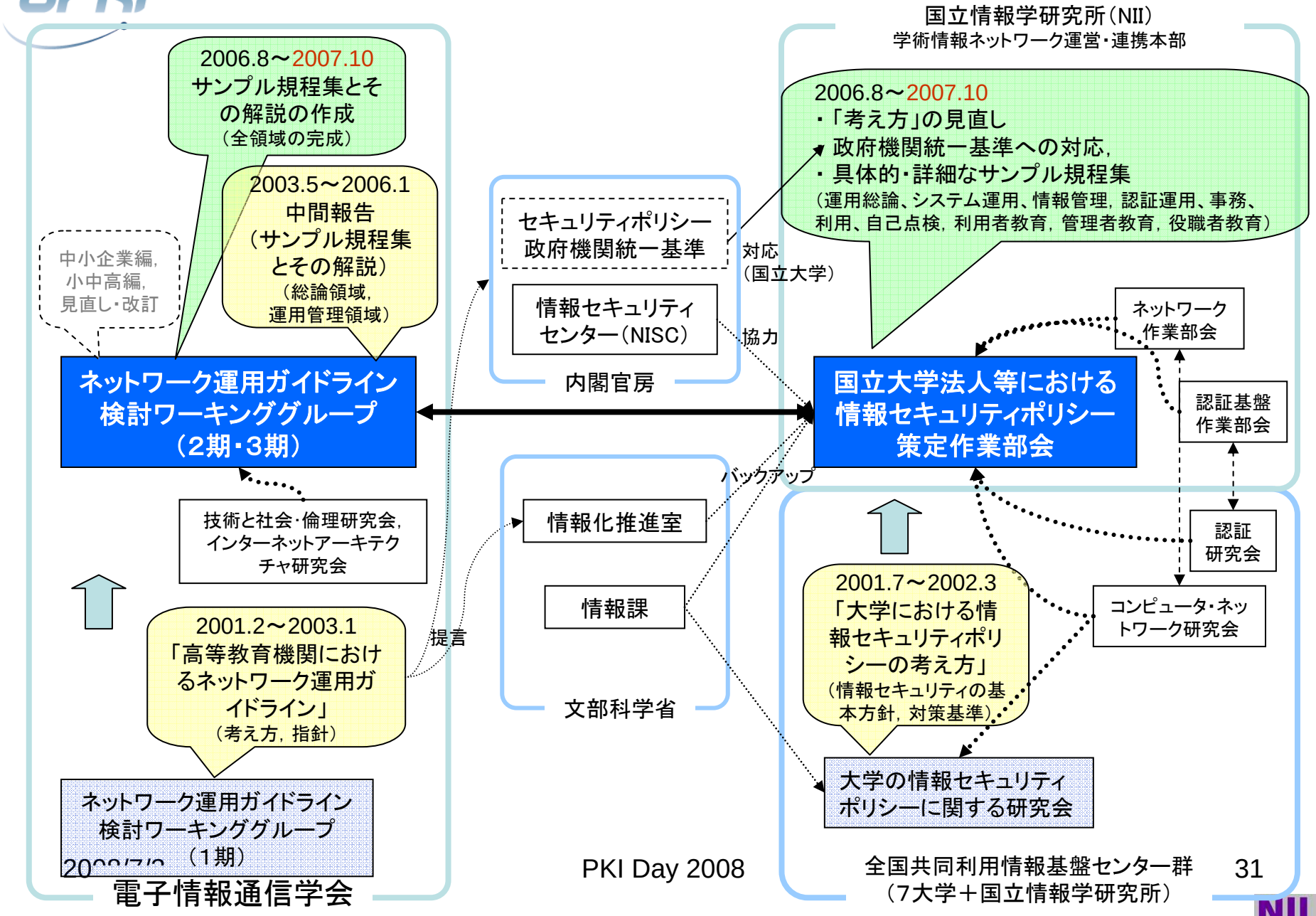
•情報セキュリティ対策の政府機関統一基準の制定、個人情報保護法の施行、国立大学の法人化、セキュリティ水準の高度化

【要請】

雛型となるポリシー規程集を制定すべき必要性

専門家集団 ⇒ セキュリティの高度化・専門化に対応した作業
（全国共同利用情報基盤センター群，電子情報通信学会）

大学における情報セキュリティポリシーの策定の動き



策定したサンプル規程集の構成

赤字は平成19年度の追加・改称文書，§は策定手引書
(*) UPKI共通仕様を参照，(**) 各大学にて策定することを想定

ポリシー	実施規程	手順等
A1000 情報システム運用基本方針 A1001 情報システム運用規程	A2101 情報システム運用・管理規程 A2102 情報システム運用リスク管理規程 A2103 情報システム非常時行動計画に関する規程 A2104 情報格付け規程	A3100 情報システム運用・管理手順の策定に関する解説書 A3101 情報システムにおける情報セキュリティ対策実施規程§ A3102 例外措置手順書； A3103 インシデント対応手順 A3104 情報格付け取扱手順； A3105 情報システム運用リスク評価手順 A3106 セキュリティホール対策計画に関する様式§ A3107 ウェブサーバ設定確認実施手順§ A3108 メールサーバのセキュリティ維持手順§ A3109 人事異動の際に行うべき情報セキュリティ対策実施規程 A3110 機器等の購入における情報セキュリティ対策実施規程§ A3111 外部委託における情報セキュリティ対策実施手順 A3112 ソフトウェア開発における情報セキュリティ対策実施手順§ A3113 外部委託における情報セキュリティ対策に関する評価手順 A3114 情報システムの構築等におけるセキュリティ要件及びセキュリティ機能の検討に関する解説書(*) A3115 情報システムの構築等におけるST 評価・ST 確認の実施に関する解説書(*)
	A2201 情報システム利用規程	A3200 情報システム利用者向け文書の策定に関する解説書 A3201 PC取扱いガイドライン A3202 電子メール利用ガイドライン； A3203 ウェブブラウザ利用ガイドライン A3204 ウェブ公開ガイドライン； A3205 利用者パスワードガイドライン A3211 学外情報セキュリティ水準低下防止手順 A3212 自己点検の考え方と実務への準備に関する解説書
	A2301 年度講習計画	A3300 教育テキストの策定に関する解説書 A3301 教育テキスト作成ガイドライン(利用者向け) A3302 (部局管理者向け)； A3303 (CIO/役職者向け)
	A2401 情報ｾｷｭﾘﾃｨ監査規程	A3401 情報セキュリティ監査実施手順
	A2501 事務情報セキュリティ対策基準	A3500 各種マニュアル類の策定に関する解説書； A3501 各種マニュアル類(**) A3502 責任者等の役割から見た遵守事項
	A2601 証明書ポリシー(*) A2602 認証実施規程(*)	A3600 認証手順の策定に関する解説書 A3601 情報システムアカウント取得手順

効果1.　ポリシー策定の効率化

【従来】　各大学で個々に『政府統一基準』の論点を検討

人的資源:　学内外から各領域の専門家を集める

基礎調査:　・法令集の解釈
・政府統一基準の解釈
・他大学事例の理解

時間費用:　委員10名 × 300時間　と仮定した場合、
⇒　人件費換算　3000時間相当／大学

【今回】　ポリシー規程集を活用した場合、

基礎調査:そのまま適用可能　→　不要
あてはめ:カスタマイズが必要な部分　→　短時間

→想定削減効果:　きわめて短期での作業を可能に

効果2.　ポリシー策定の高品質化

【従来】　各大学で個々に『政府統一基準』の論点を検討

人的資源：　各領域の専門家は全国でも限られている
⇒　専門家を集められないおそれ

調査範囲：　多岐にわたる専門的領域の調査を要する
⇒　検討漏れ事項が生じるおそれ

検討期間：　基礎調査の作業に長期間を要する
⇒　喫緊の課題に対応できないおそれ

→全論点の検討には、2年程度の検討期間が必要

【今回】　ポリシー規程集を活用した場合、

調査・検討：　全論点を各領域の専門家が検証済み

→効果：　セキュリティ対策を早期かつ高品質で実現

「情報セキュリティの日 功労者表彰」を受賞

表彰状

国立情報学研究所
電子情報通信学会 殿

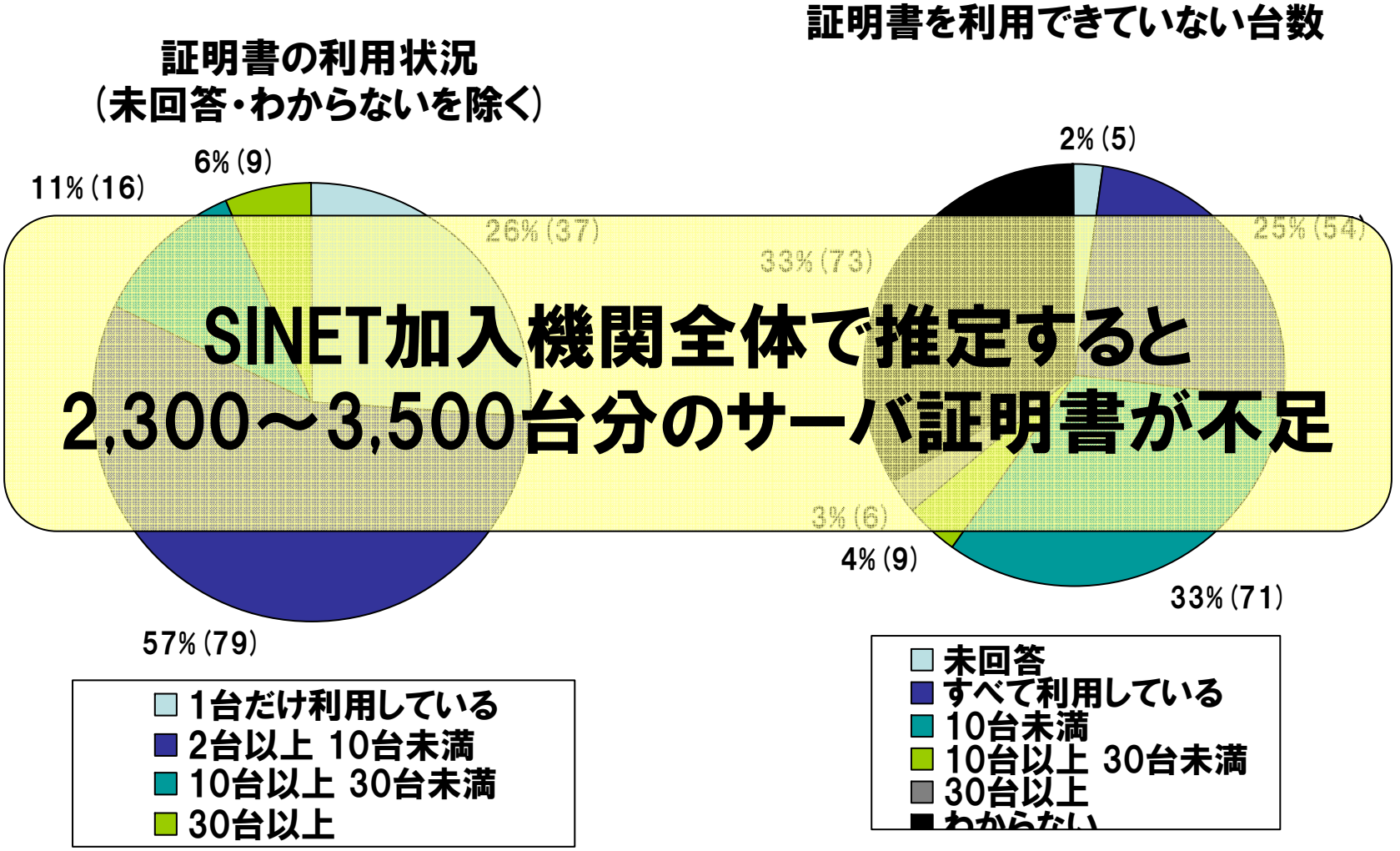
貴団体は我が国における情報セキュリティへの取組に尽力されその功績は極めて顕著でありますよってここに表彰します

平成二十年二月四日

情報セキュリティ政策会議議長
内閣官房長官 町村信孝

(2) サーバ証明書発行・導入の啓発・評価研究プロジェクト

大学等におけるサーバ証明書の実態

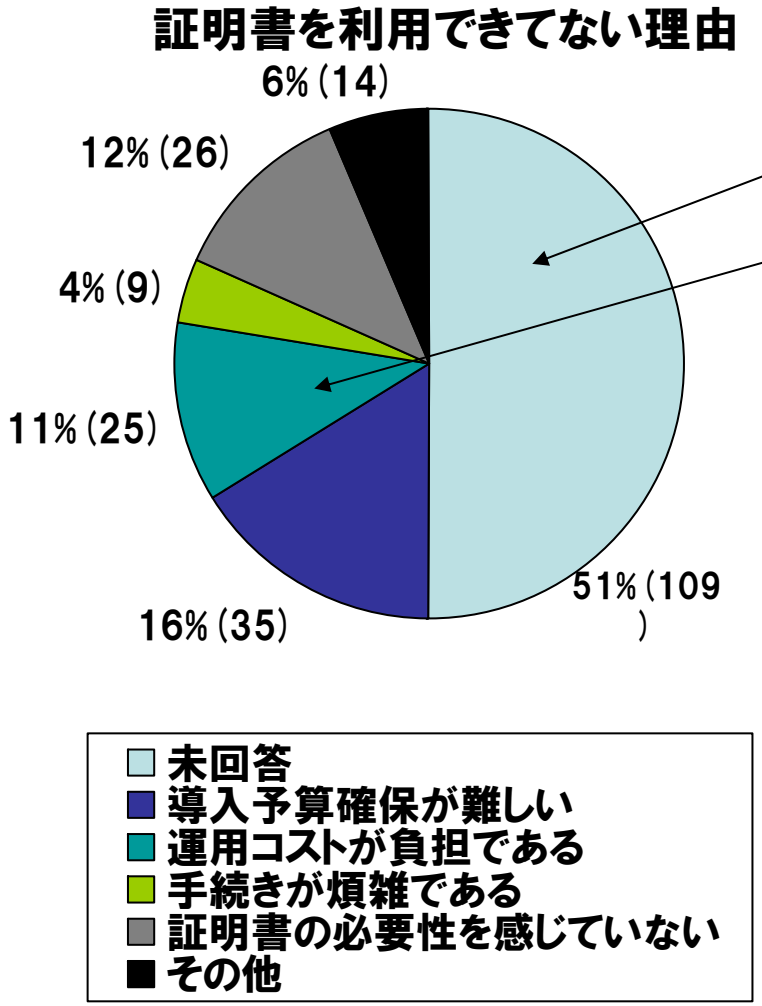


SINET加入機関全体で推定すると
2,300～3,500台分のサーバ証明書が不足

H18年度「大学等における電子証明書の利用状況に関する実態調査」より

対象: SINET加入機関818件、うち有効回答218件

普及が進まない理由



- 理由がわからない!!
- 運用コストの負担
  - 実際に生じる負担は?

実際に使ってもらって確認してはどうか?

プロジェクトの概要

- 目的
  - 大学等のサーバ証明書の普及を推進
  - 認証局を用いた研究開発 ⇒ 登録発行業務の改善
  - 学術機関のWebサーバ信頼性向上
  - サーバ証明書の導入・運用ノウハウの共有
  - 参加者のサーバに対してのサーバ証明書無償配布
- 期間
  - 2007/04/01～2009/06/30
- ゴール
  - H19年度: サーバ証明書の普及が進まない理由・課題の整理
  - H20年度: サーバ証明書の普及促進の仮説・立証
  - 将来的に: キャンパスPKI層を活用した証明書発行業務の自動化
- 主な作業
  - プロジェクト参加機関の募集
  - 各登録担当者へのS/MIME証明書発行
  - 参加機関が管理するサーバに対するサーバ証明書の発行
  - 参加機関加入者によるサーバ証明書の導入・運用
  - 発行手続、導入手順などに対する改善案・Tipsのフィードバック
  - 改善案・Tipsなどの整理・公開など

認証局を用いた評価研究

体験を通じて啓発

H19年度作業

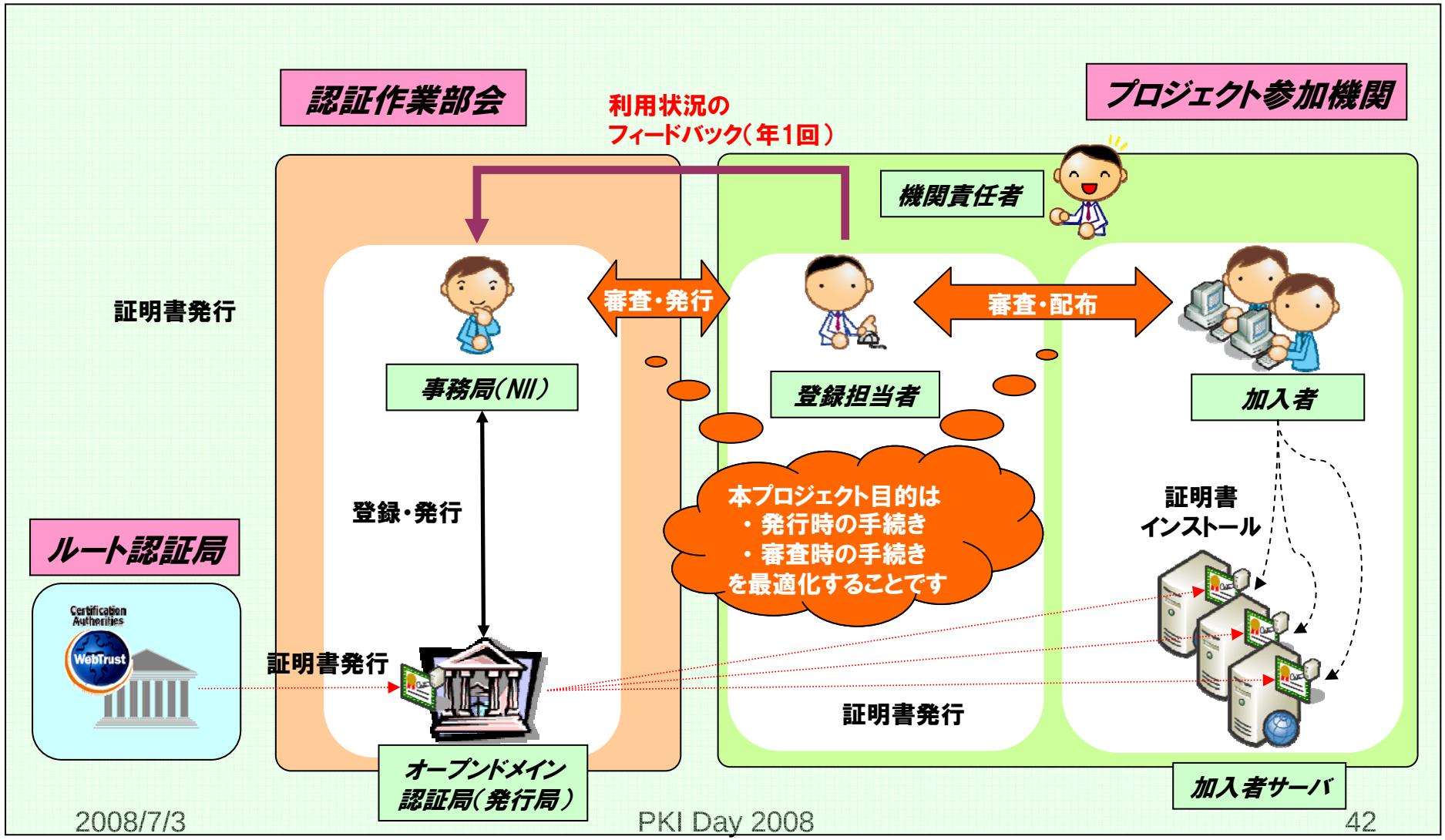
証明書発行の基本方針

- 用語の定義
  - 本人性確認: なりすましや否認を防止するために本人意思を確認する作業
  - 実在性確認: 証明書に記載する組織に実在することを確認する作業
- 審査項目の分担による発行業務の最適化
  - その審査を一番手早く実現できるのは誰か?
  - 認証局が最低限責任を負うべき項目は?
- 商用サービスと同等の保証レベル
  - 機関の実在性認証まで含めた審査項目→分担して実現

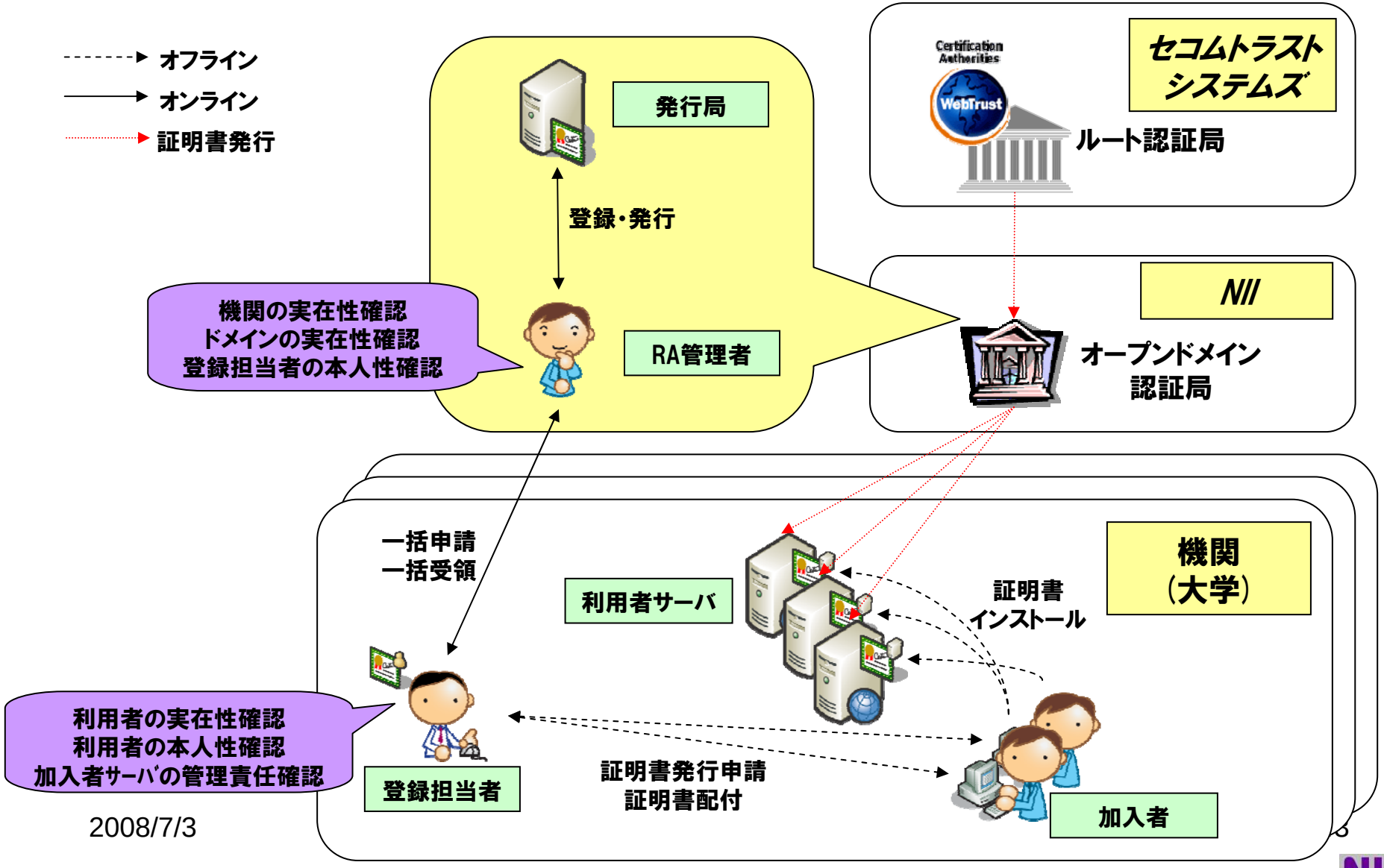
プロジェクト参加者の役割

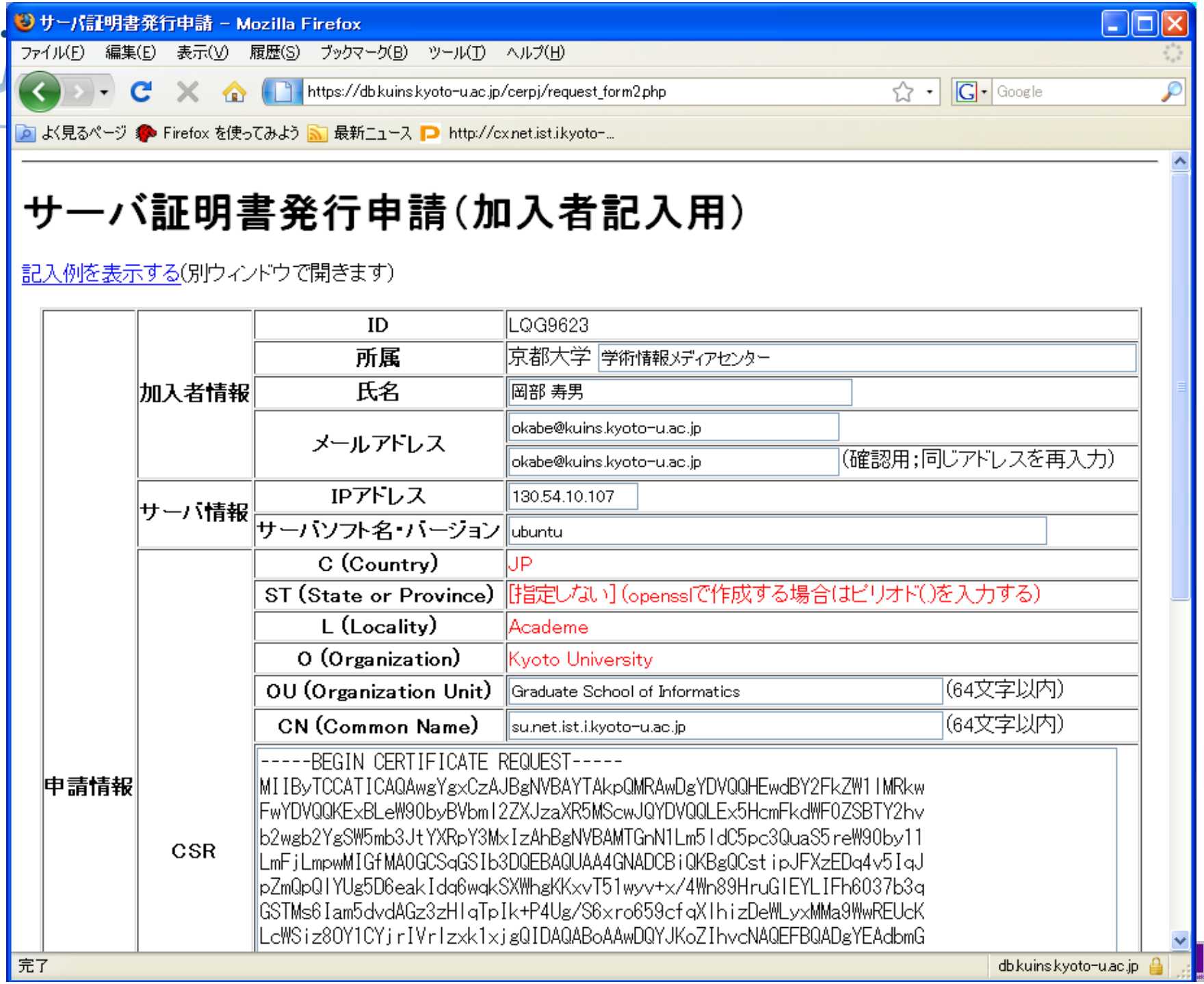
組織	役割	説明
NII	発行局	認証局の鍵管理、サーバ証明書発行など セコムトラストシステムズへ運用委託
	事務局	プロジェクト参加申請、証明書発行申請にあたり、審査業務を行う
機関 (大学)	機関責任者 (1機関1名)	本プロジェクト参加にあたり、各機関で選出した代表者。 課長職相当または准教授以上
	登録担当者 (複数名可)	本プロジェクトの参加機関側の事務的な窓口。 大学の規模等に応じて複数名選出可。
	加入者	Webサーバを管理し、本プロジェクトのサーバ証明書を利用する。 機関に所属する教職員。
不特定多数	利用者	加入者サーバへアクセスし、その証明書を検証する。

プロジェクト概念図


認証作業部会
利用状況の
フィードバック（年1回）
プロジェクト参加機関
機関責任者
証明書発行
審査・発行
審査・配布
事務局（NII）
登録担当者
加入者
登録・発行
本プロジェクト目的は
・発行時の手続き
・審査時の手続き
を最適化することです
証明書
インストール
ルート認証局
Certification Authorities
WebTrust
証明書発行
証明書発行
オープンドメイン
認証局（発行局）
加入者サーバ

証明書発行の流れ


オフライン
オンライン
証明書発行
発行局
登録・発行
RA管理者
機関の実在性確認
ドメインの実在性確認
登録担当者の本人性確認
セコムトラスト
システムズ
ルート認証局
NII
オープンドメイン
認証局
一括申請
一括受領
利用者サーバ
証明書
インストール
機関
（大学）
利用者の実在性確認
利用者の本人性確認
加入者サーバの管理責任確認
登録担当者
証明書発行申請
証明書配付
加入者

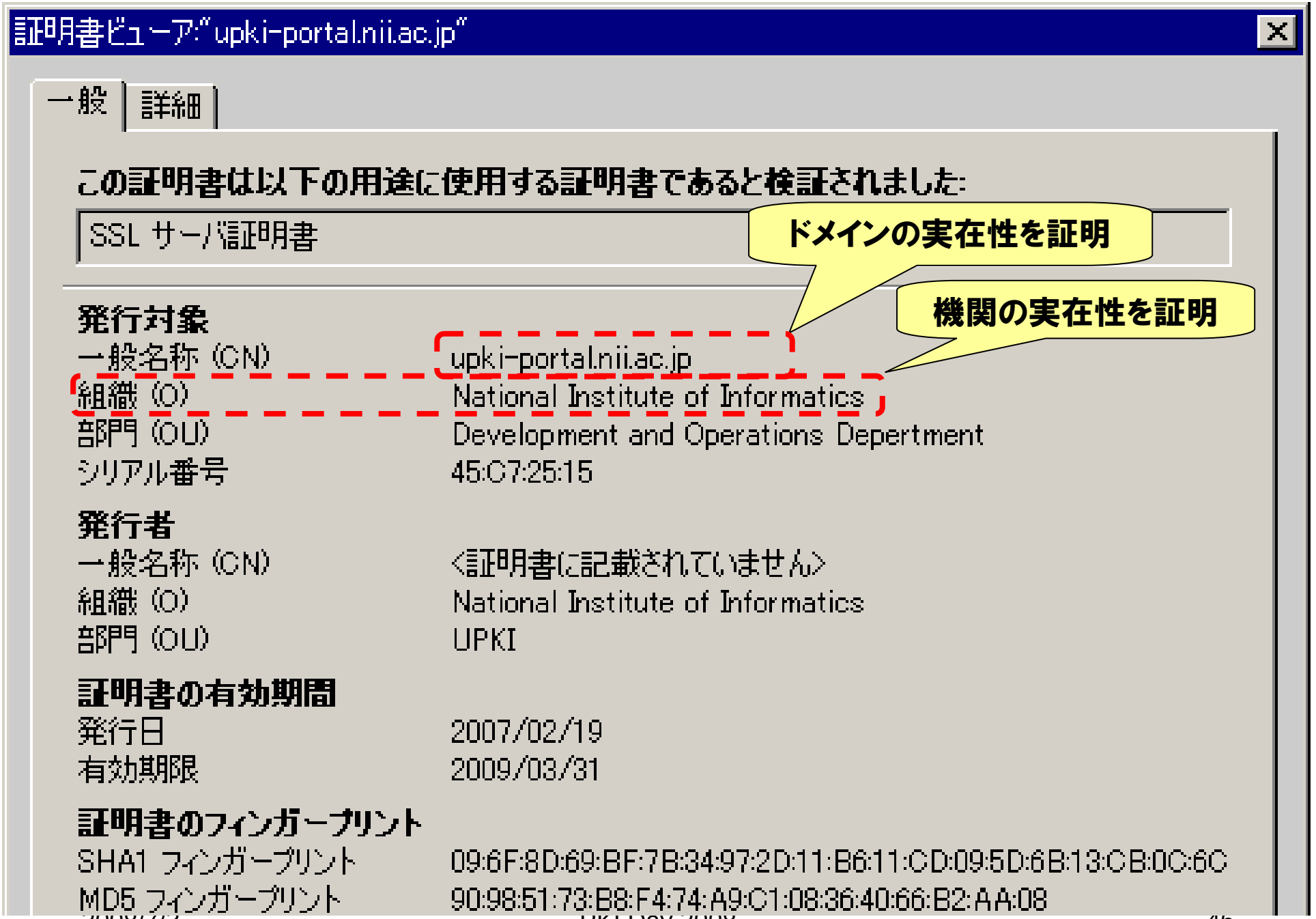

サーバ証明書発行申請 - Mozilla Firefox
ファイル(F) 編集(E) 表示(V) 履歴(S) ブックマーク(B) ツール(T) ヘルプ(H)
https://db.kuins.kyoto-u.ac.jp/cerpj/request_form2.php
Google
よく見るページ Firefox を使ってみよう 最新ニュース http://cx.net.ist.i.kyoto-...
サーバ証明書発行申請(加入者記入用)
記入例を表示する(別ウィンドウで開きます)
申請情報
加入者情報
ID
LQG9623
所属
京都大学 学術情報メディアセンター
氏名
岡部 寿男
メールアドレス
okabe@kuins.kyoto-u.ac.jp
okabe@kuins.kyoto-u.ac.jp (確認用;同じアドレスを再入力)
サーバ情報
IPアドレス
130.54.10.107
サーバソフト名・バージョン
ubuntu
C (Country)
JP
ST (State or Province)
[指定しない] (openssl で作成する場合はピリオド(.)を入力する)
L (Locality)
Academe
O (Organization)
Kyoto University
OU (Organization Unit)
Graduate School of Informatics (64文字以内)
CN (Common Name)
su.net.ist.i.kyoto-u.ac.jp (64文字以内)
CSR
-----BEGIN CERTIFICATE REQUEST-----
MIIByTCCATICAQAwgYgxCzAJBgNVBAYTAkpQMRAwDgYDVQQHEwdBY2FkZW1IMRkw
FwYDVQQKExBLeW90byBVbmI2ZXJzaXR5MScwJQYDVQQLEx5HcmFkdWF0ZSBTY2hv
b2wgb2YgSW5mb3JtYXRpY3MxIzAhBgNVBAMTGnN1Lm5IdC5pc3QuaS5reW90by11
LmFjLmpwMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCstipJFXzEDq4v5IqJ
pZmQpQIYUg5D6eakIdq6wqkSXWhgKKxvT51wyv+x/4Wn89HruGIEYLIFh6037b3q
GSTMs6Iam5dvdAGz3zHIqTpIk+P4Ug/S6xro659cfqXIhizDeWLyxMMa9WwREUcK
LcWSiz8OY1CYjrIVrIzxk1xjgQIDAQABoAAwDQYJKoZIhvcNAQEFBQADgYEAdbmG
db.kuins.kyoto-u.ac.jp
完了

商用証明書との比較
～審査項目の違い～

機関側の審査項目は確認手順調査表でチェック

審査項目	審査者	商用サービス				本プロジェクト			
		オンライン認証		機関認証					
		登録局	利用者	登録局	利用者	登録局	機関責任者	登録担当者	利用者
機関	本人性確認	×		○					
	実在性確認	×		○		○			
ドメイン	本人性確認	○		○		× →	○		
	実在性確認	○		○		○			
機関責任者	本人性確認					○			
	実在性確認					○			
登録担当者	本人性確認					○			
	実在性確認					× →	○		
加入者	本人性確認	×		○		× →		○	
	実在性確認	×		○		× →		○	
加入者サーバ	本人性確認		○		○				○
	管理責任確認		○		○			○ ←	×

「認証方法の違いによる役割と活用場面（企業の実在性認証とオンライン認証）」より
http://www.verisign.co.jp/server/first/difference.html


証明書ビューア:"upki-portal.nii.ac.jp"
一般
詳細
この証明書は以下の用途に使用する証明書であると検証されました:
SSL サーバ証明書
ドメインの実在性を証明
機関の実在性を証明
発行対象
一般名称 (CN) upki-portal.nii.ac.jp
組織 (O) National Institute of Informatics
部門 (OU) Development and Operations Depertment
シリアル番号 45:C7:25:15
発行者
一般名称 (CN) <証明書に記載されていません>
組織 (O) National Institute of Informatics
部門 (OU) UPKI
証明書の有効期間
発行日 2007/02/19
有効期限 2009/03/31
証明書のフィンガープリント
SHA1 フィンガープリント 09:6F:8D:69:BF:7B:34:97:2D:11:B6:11:CD:09:5D:6B:13:CB:0C:6C
MD5 フィンガープリント 90:98:51:73:B8:F4:74:A9:C1:08:36:40:66:B2:AA:08

プライベート認証局と プライベート証明書

- プライベート認証局
  - ユーザがクライアントアプリケーションに後から登録する必要がある
- プライベート証明書
  - 認証局からの信頼を何らかの追加手順なしには確認することができない

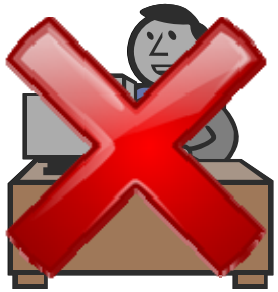
これらは信頼してもらうには、利用者に何らかの設定や操作をしてもらう必要がある。

ここの確認手順を省略してしまうのがいわゆる「オレオレ証明書」

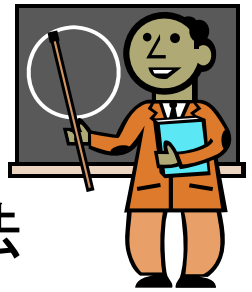
プライベート証明書は、たとえ組織内であっても多くのユーザが利用するサーバ側での利用は困難

オレオレ証明書と大学教育

- 誤った理解
  - 警告が出ても無視していい
    - 何かしらの理由がなければ警告は出ません
  - 警告を回避するには証明書を登録すればいい
    - どんな証明書でも登録していいわけではありません



- 必要な教育
  - 警告の理由と無視してもよい状況の説明
  - 登録してよい証明書といけない証明書の識別方法



十分な教育なしにプライベート証明書を使うことは最高学府として学生にさせるべきではない

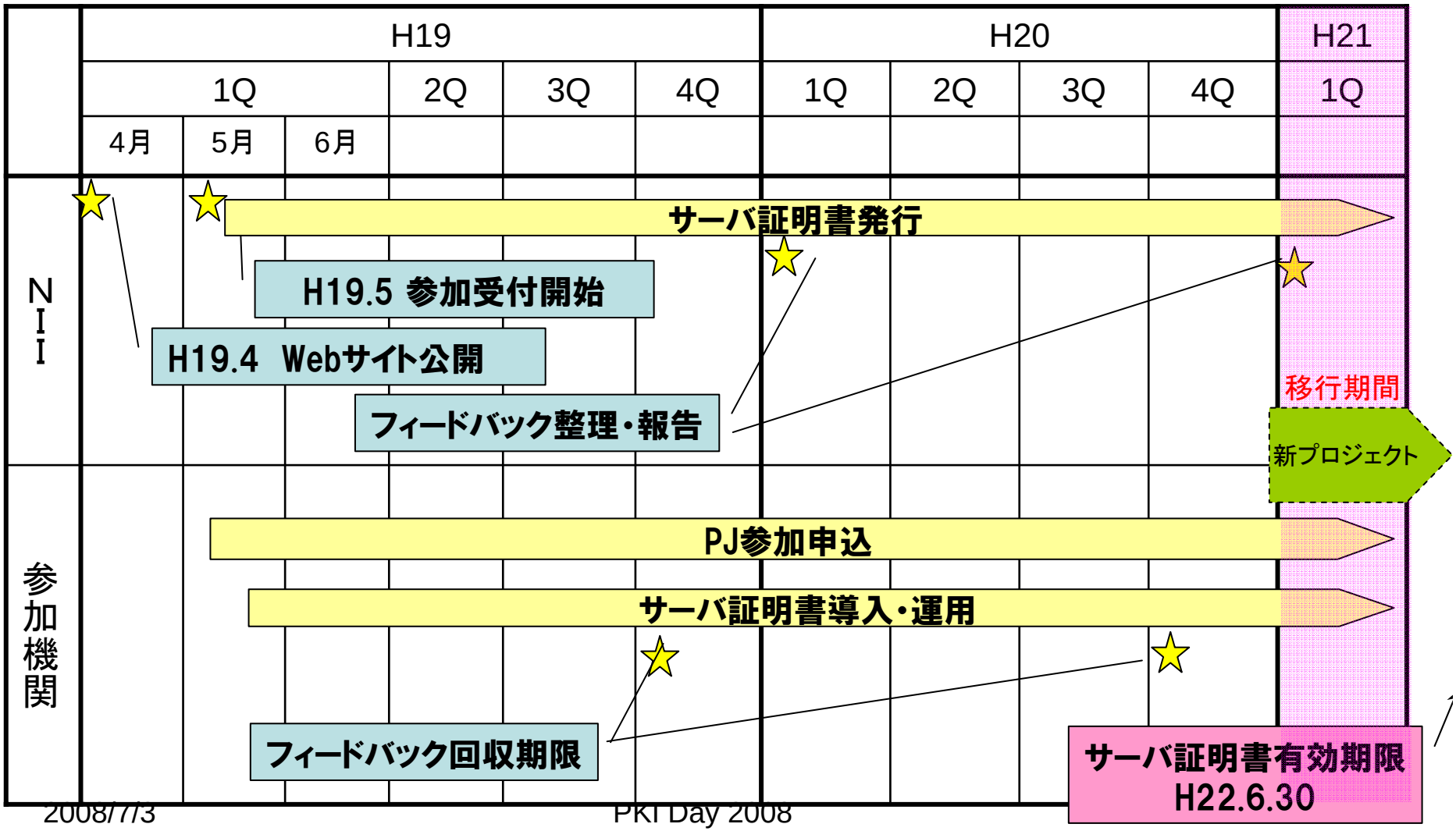
プロジェクトへの参加条件
サーバ証明書の発行条件

- 対象
  - SINET加入機関のうち、
    - 大学，短期大学，高等専門学校，大学共同利用機関
    - 独立行政法人，公益法人，大学共同利用機関法人，学校法人，地方独立行政法人
    - 本プロジェクト参加対象機関の長が設置する組織
  - 日本学術会議協力学術研究団体のうち、
    - 本プロジェクトが対象とするドメイン名を保有し部会が認めた団体
- 対象サーバ
  - 属する機関が所有または管理するサーバ
  - サーバ認証を必要とするサーバ
- ドメイン
  - 属する機関の主たるドメイン
    - 原則としてac.jpドメイン
    - プロジェクト参加申込時に指定

参加機関数	70機関
証明書発行枚数	1,200枚

〔H20.6月中旬時点での実績値〕

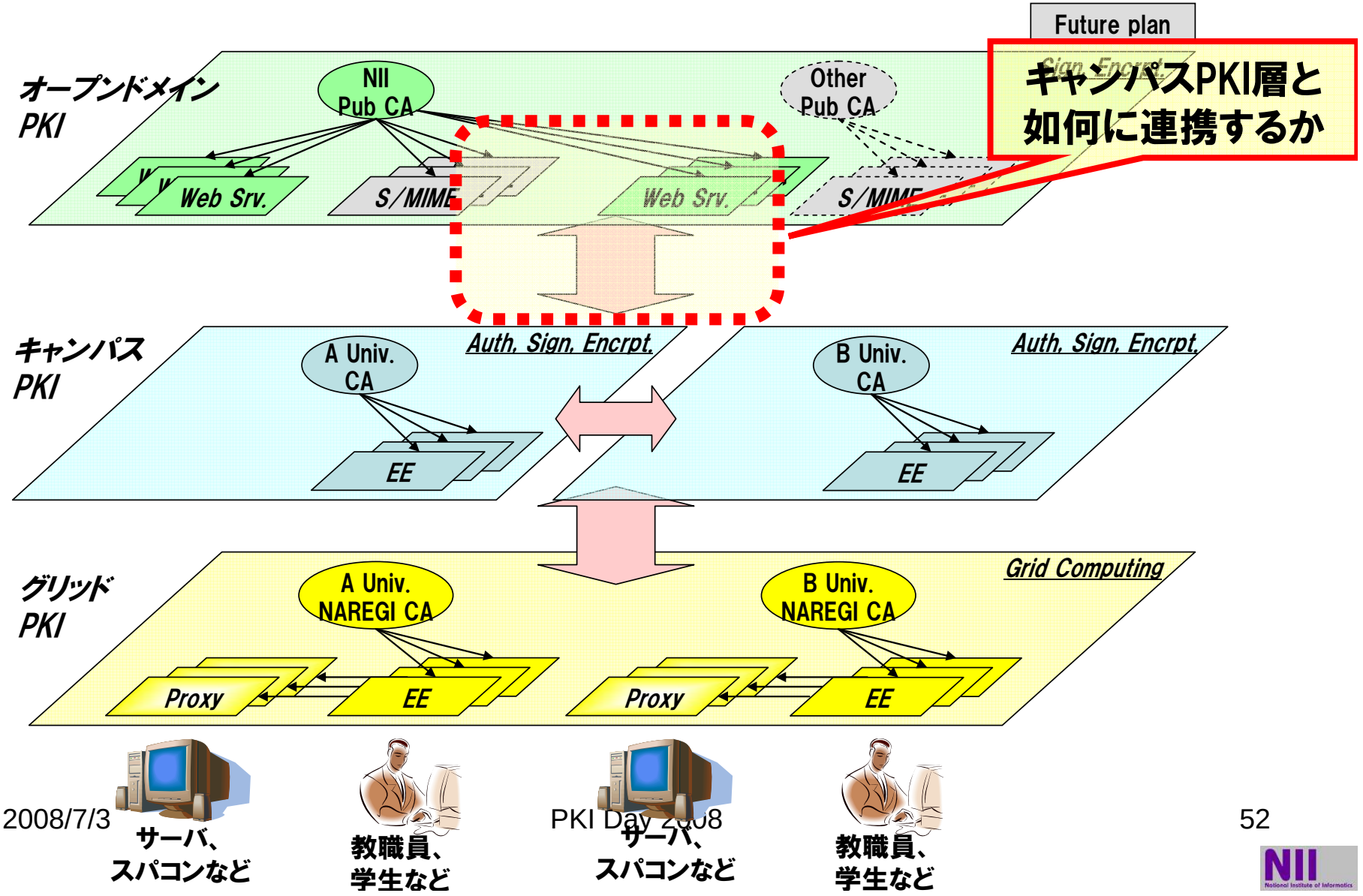
プロジェクトスケジュール



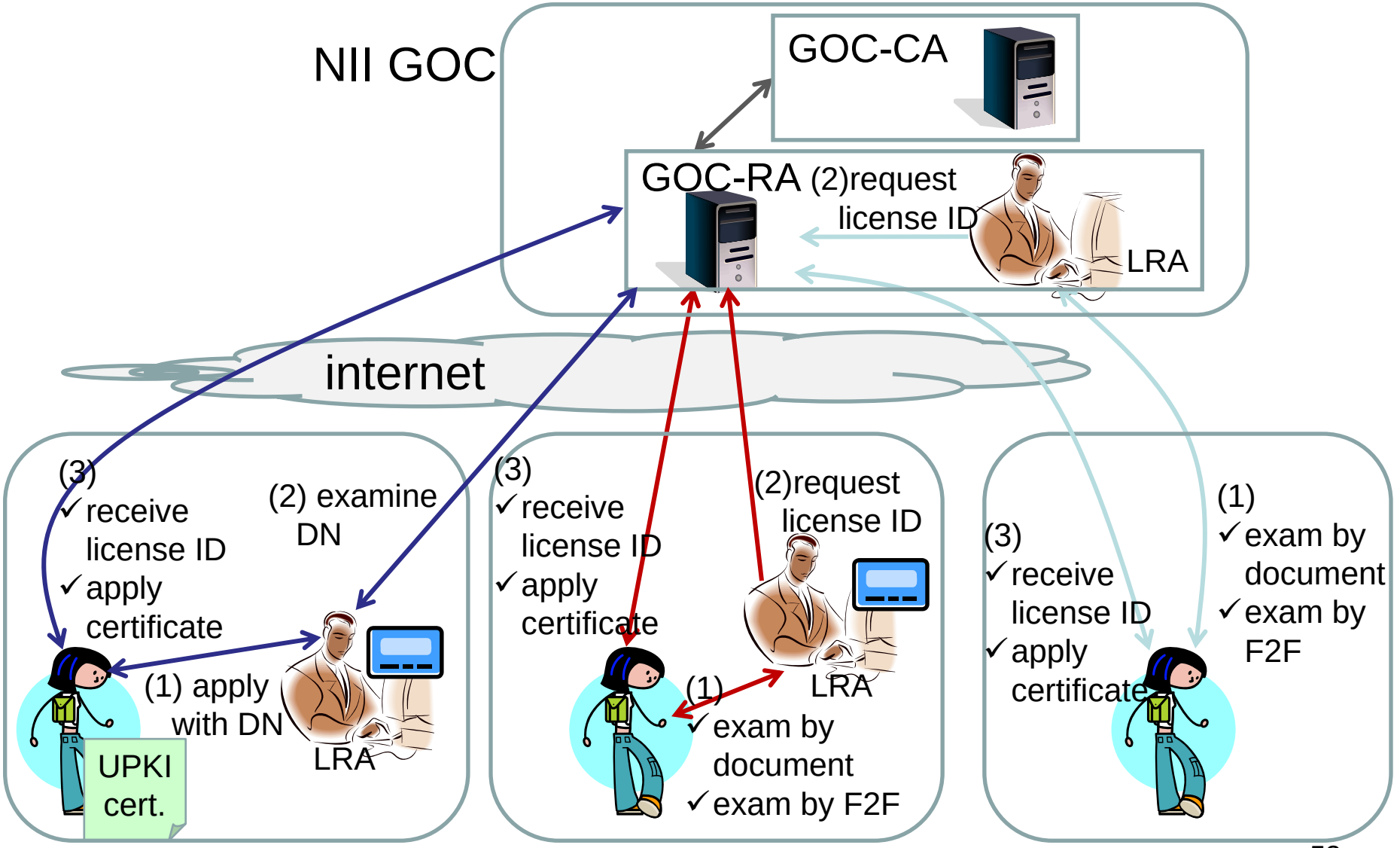
〔関連研究〕

- 平野・内藤: “UPKIイニシアティブ『サーバ証明書発行・導入における啓発・評価研究プロジェクト』と名古屋大学における事例”,
  - 名古屋大学情報連携基盤センターニュース Vol.6 No.4
    - http://www2.itc.nagoya-u.ac.jp/pub/pdf/contents/contents06_04.htm
- 西村・佐藤:“東京大学におけるサーバ証明書発行体制の構築と課題”,
  - 情報処理学会第48回DSM研究会・第26回QAI研究会（平成20年3月、北陸先端大）
- J. Meijer (UNINETT, Norway), “Community SSL/TLS Server Certificate”
  - APAN 25th Workshop (Hawaii)
    - http://www.apan.net/meetings/hawaii2008/proposals/middleware.html

UPKIにおける位置づけ(ゴール)



GOC（グリッドオペレーションセンター）における ユーザ証明書の発行



(3) UPKI認証連携基盤 (UPKI-Federation)による シングルサインオン

～Shibboleth/SAMLとキャンパスPKIによる コンテンツサービスのシングルサインオン～

Shibboleth

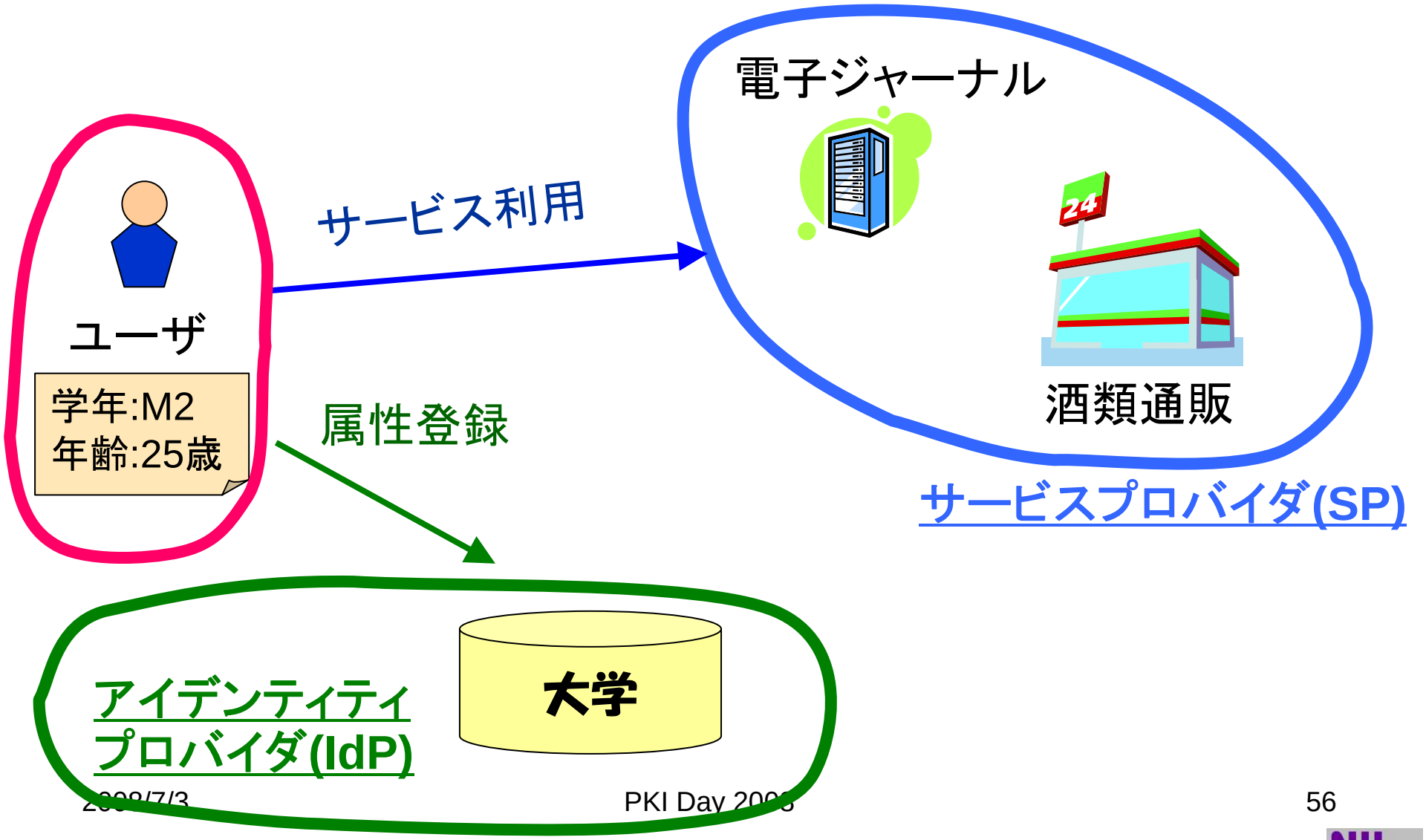
Shibboleth

Shibboleth.

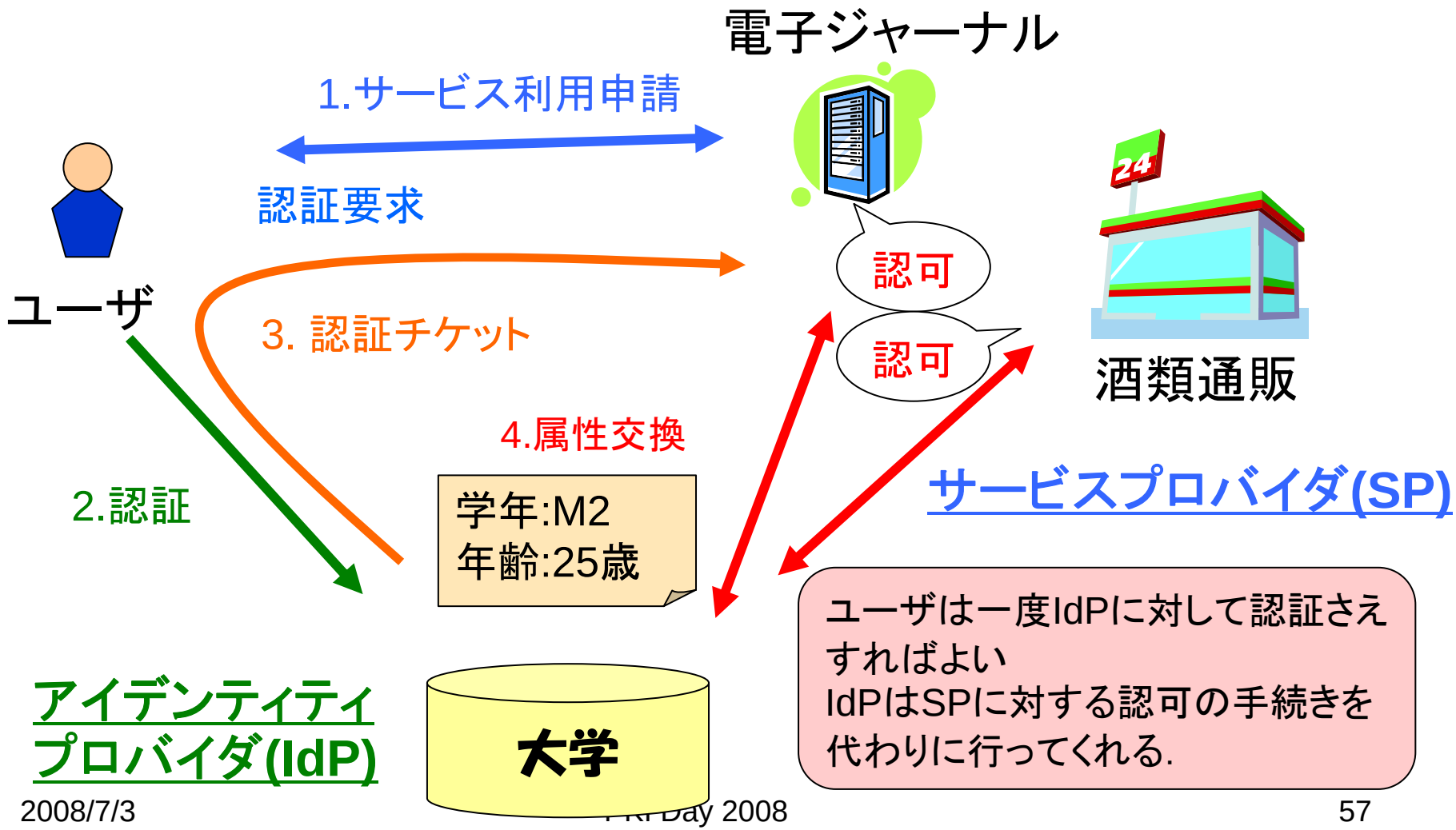
- Internet2/MACEプロジェクト
- SAMLをベースとした、FIMを実現するオープンソースの開発
  - SAML2.0準拠の実装であるShibboleth2.0が最新版(H20.3)
- 欧米の図書館・大学等での利用

[URL] http://shibboleth.internet2.edu/

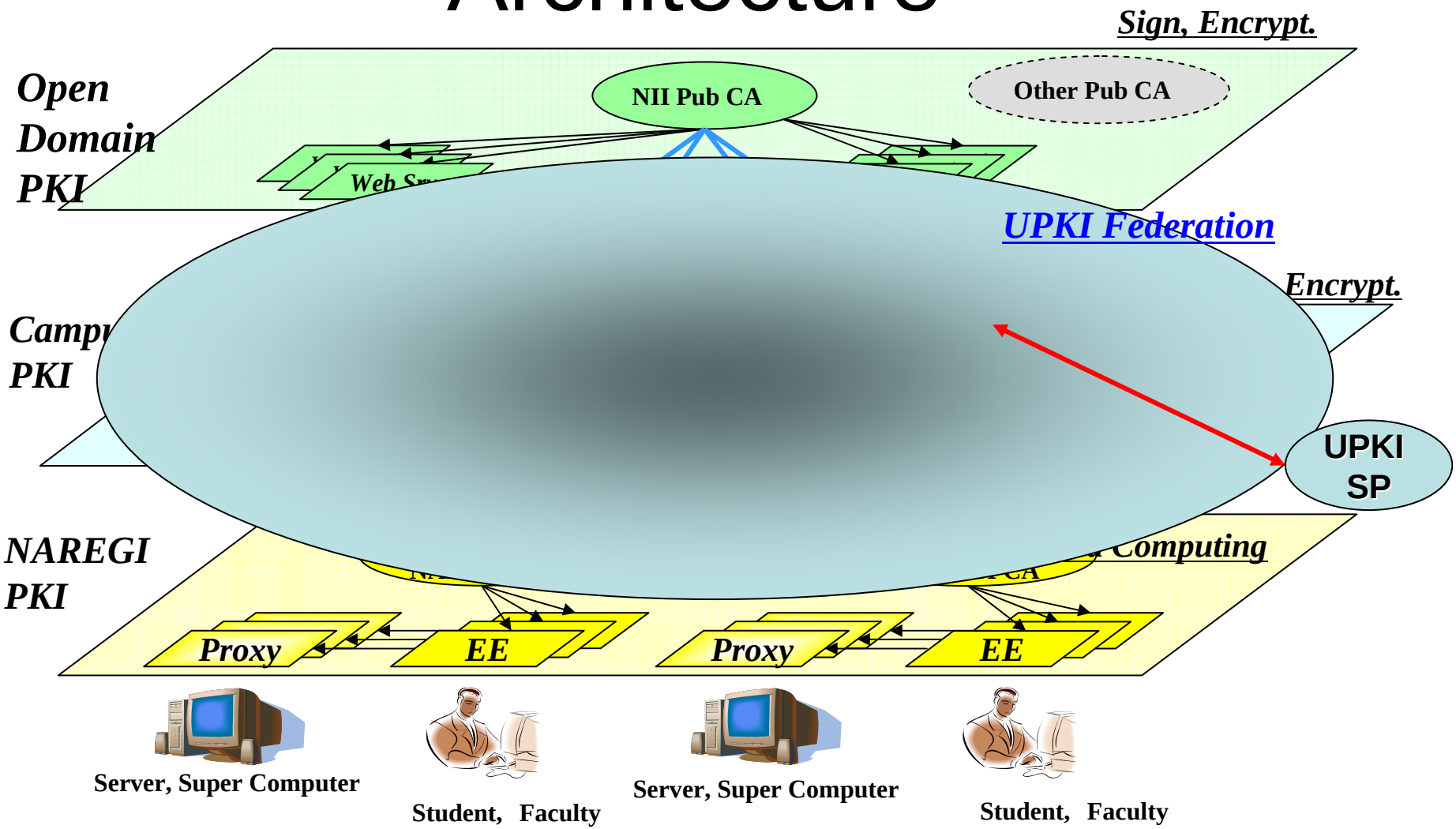
Shibbolethのアーキテクチャ

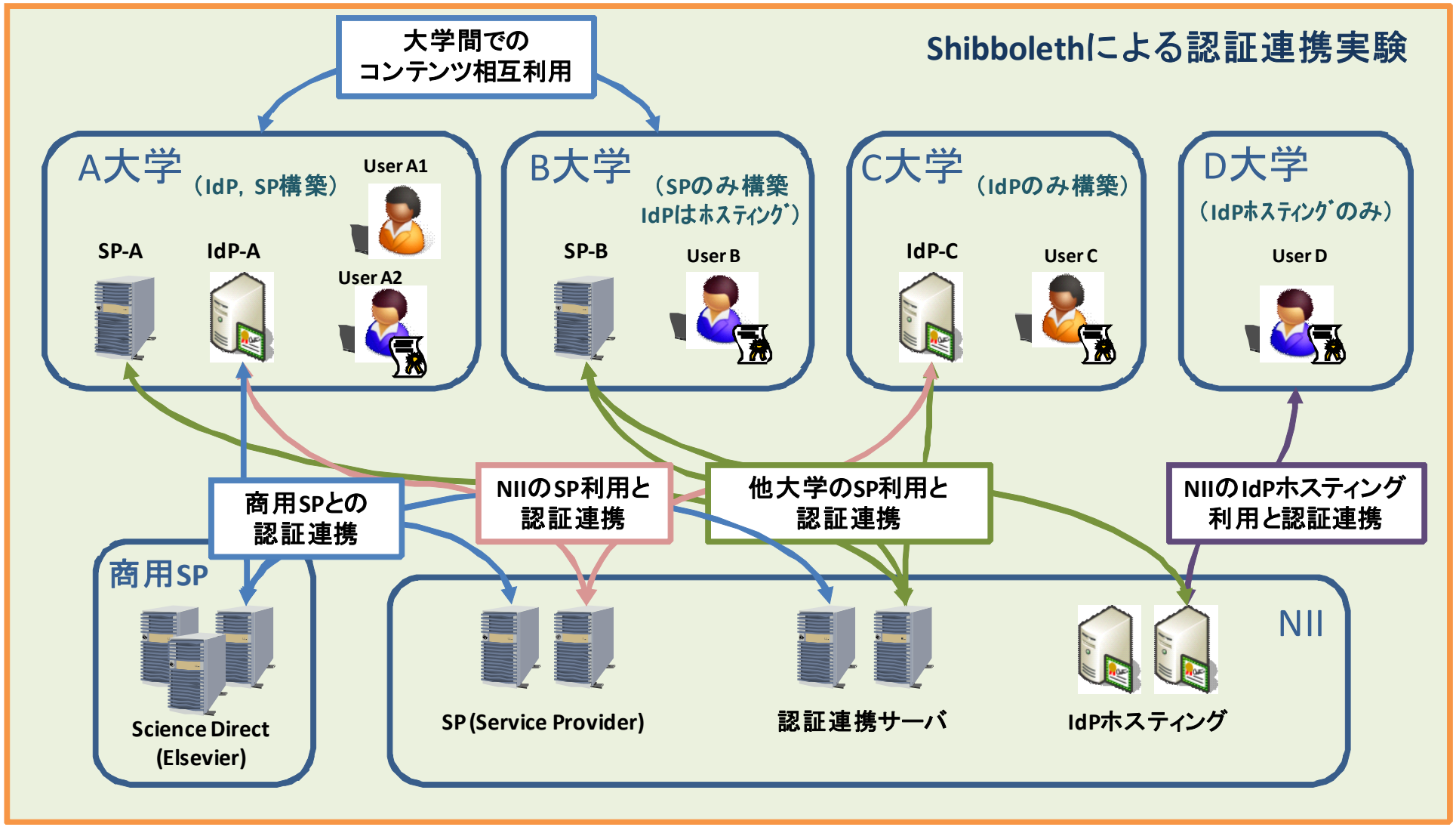


Shibbolethの認証・認可の流れ

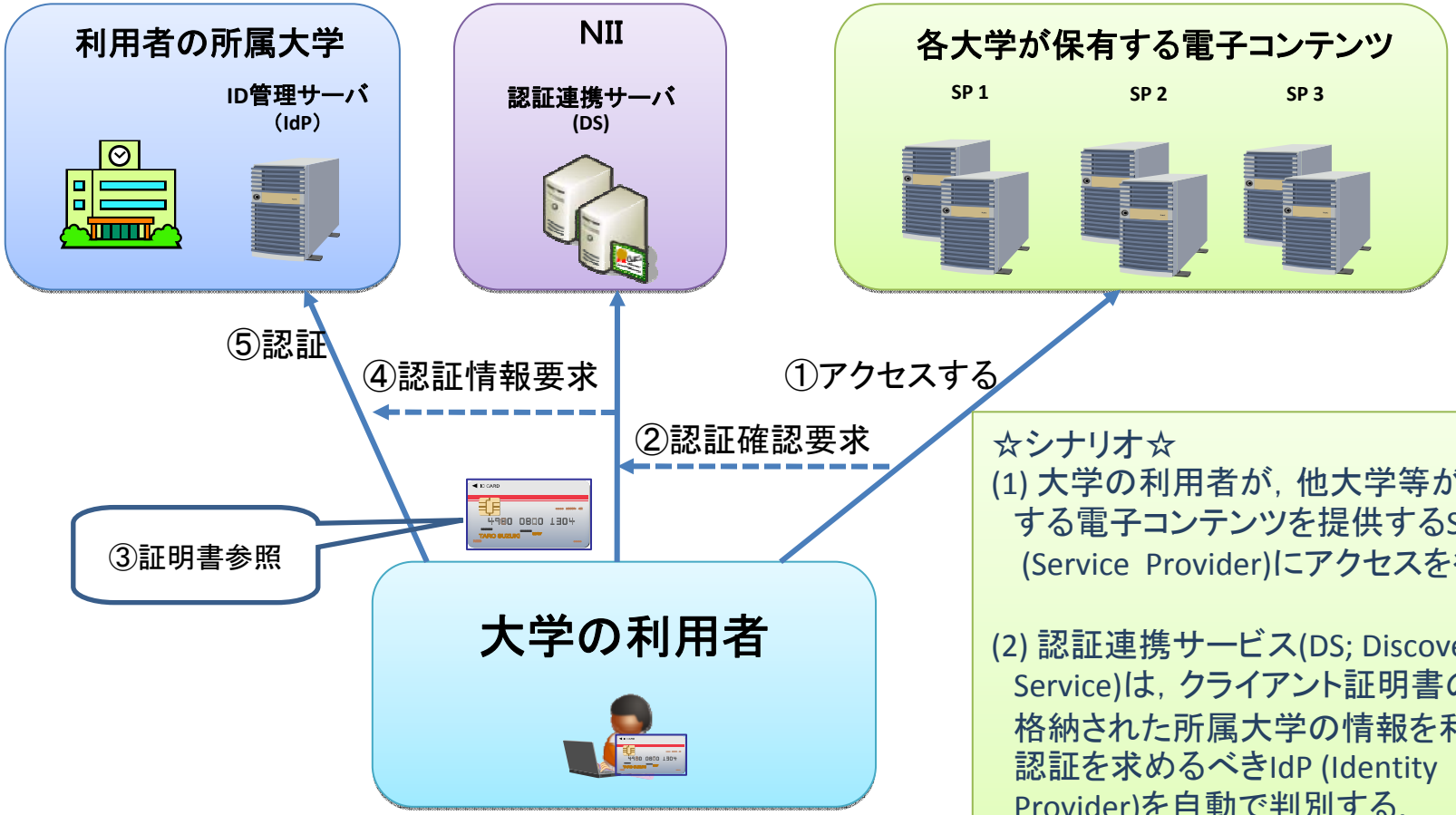


Shibboleth on UPKI Architecture




大学間での
コンテンツ相互利用
Shibbolethによる認証連携実験
A大学
（IdP，SP構築）
User A1
SP-A
IdP-A
User A2
B大学
（SPのみ構築
IdPはホスティング）
SP-B
User B
C大学
（IdPのみ構築）
IdP-C
User C
D大学
（IdPホスティングのみ）
User D
商用SPとの
認証連携
NIIのSP利用と
認証連携
他大学のSP利用と
認証連携
NIIのIdPホスティング
利用と認証連携
商用SP
Science Direct
(Elsevier)
SP (Service Provider)
認証連携サーバ
IdPホスティング
NII

認証とシングルサインオン



☆シナリオ☆

(1) 大学の利用者が，他大学等が保有する電子コンテンツを提供するSP (Service Provider)にアクセスを行う.

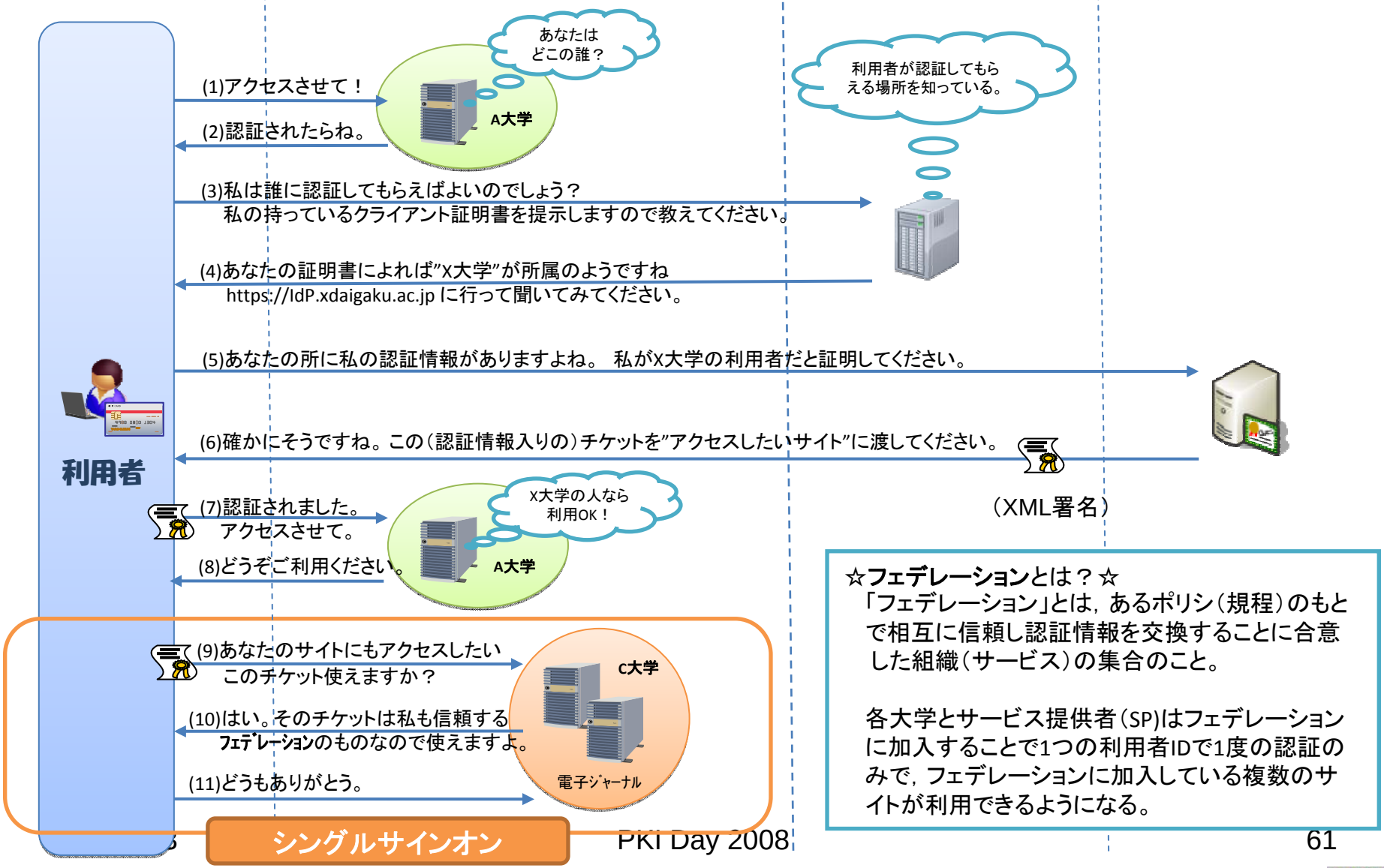
(2) 認証連携サービス(DS; Discovery Service)は，クライアント証明書の中に格納された所属大学の情報を利用して，認証を求めるべきIdP (Identity Provider)を自動で判別する.

(3) 認証情報を確認できた場合は利用者は電子コンテンツにアクセスすることができるようになる.

☆ポイント☆

・自分の所属する大学の認証情報（ID）を利用して，他大学等のWebサイトや電子コンテンツに，シングルサインオンできる

認証とシングルサインオンの処理の流れ（例）

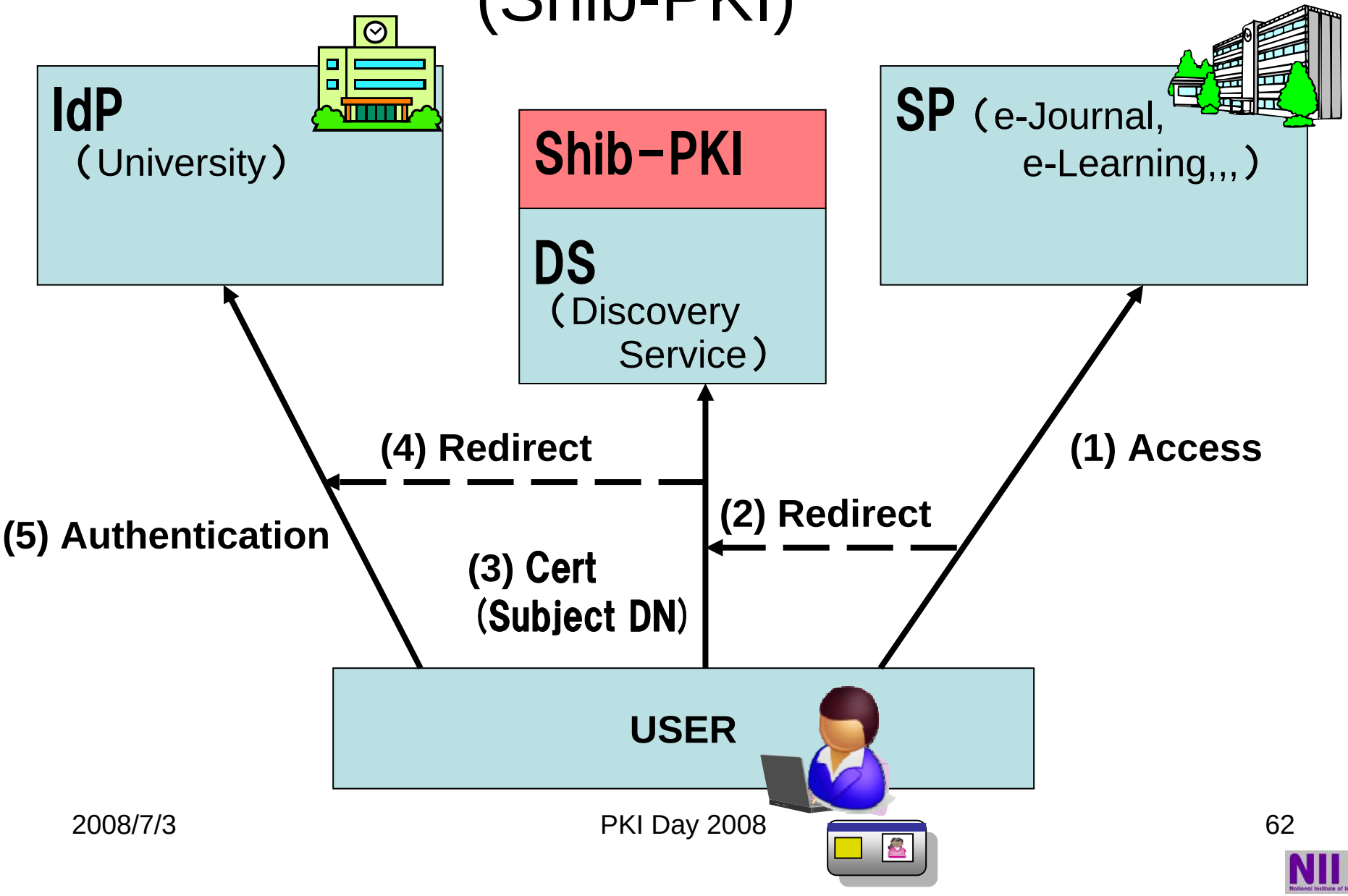


☆**フェデレーション**とは？☆

「フェデレーション」とは，あるポリシ（規程）のもとで相互に信頼し認証情報を交換することに合意した組織（サービス）の集合のこと。

各大学とサービス提供者（SP)はフェデレーションに加入することで1つの利用者IDで1度の認証のみで，フェデレーションに加入している複数のサイトが利用できるようになる。

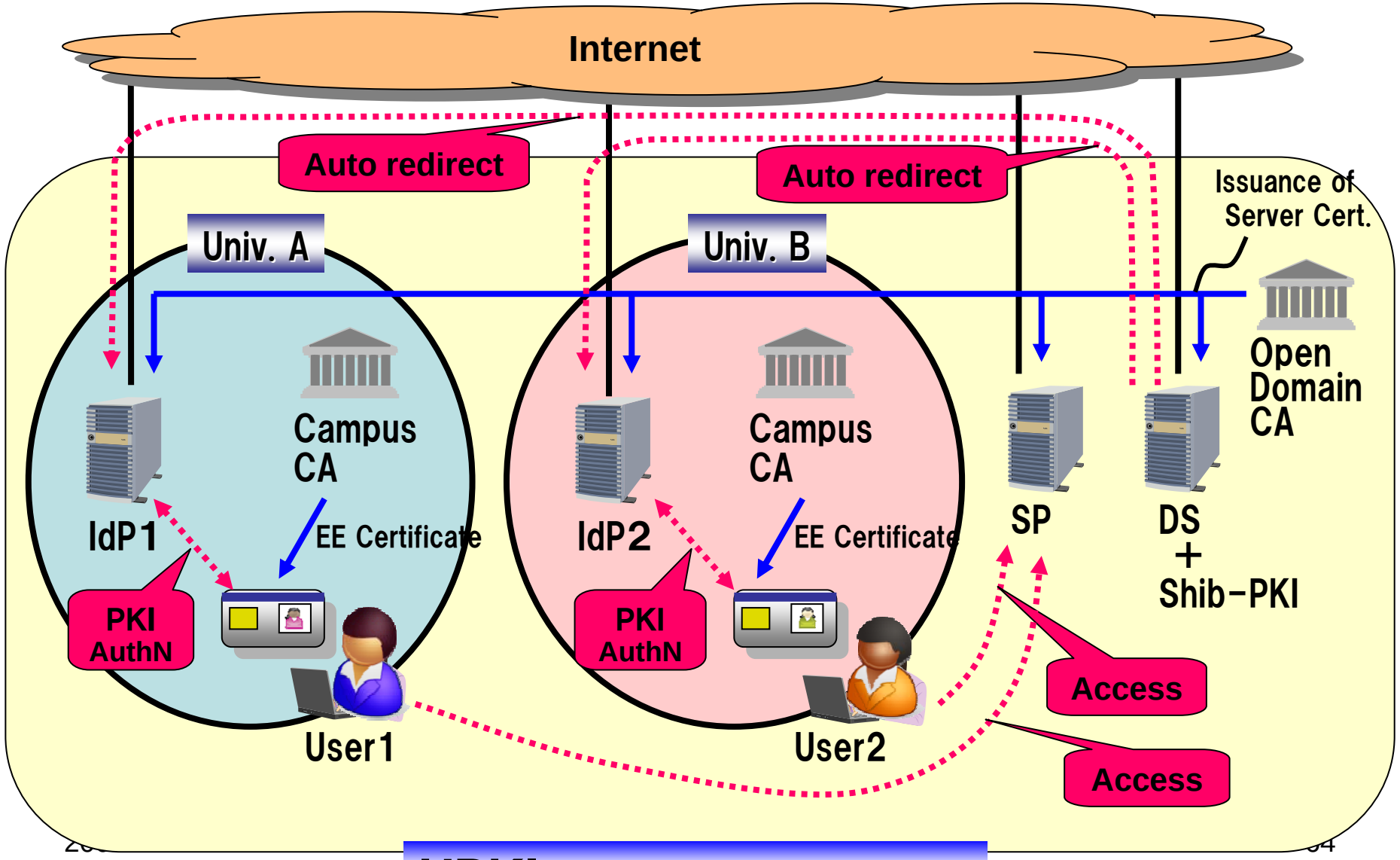
Shibboleth とUPKIの連動 (Shib-PKI)



UPKI認証連携基盤による シングルサインオン実証実験

- 参加機関
  - 国立七大学を中心とする大学図書館、情報基盤センター等
- 期間
  - 平成20年7月～12月
- 実施体制
  - IdPは各大学で準備
    - NIIでホスティングサービスを提供
  - SPとして以下を想定して設計
    - 電子ジャーナル(CiNii，電子ジャーナル)、電子図書館
    - E-learningシステム
    - サーバ証明書発行、グリッド証明書発行
    - 無線LANローミング用一時アカウント発行
  - 認証認可で用いられる属性情報の共通仕様策定が鍵

UPKI-Fedrationテストベッド

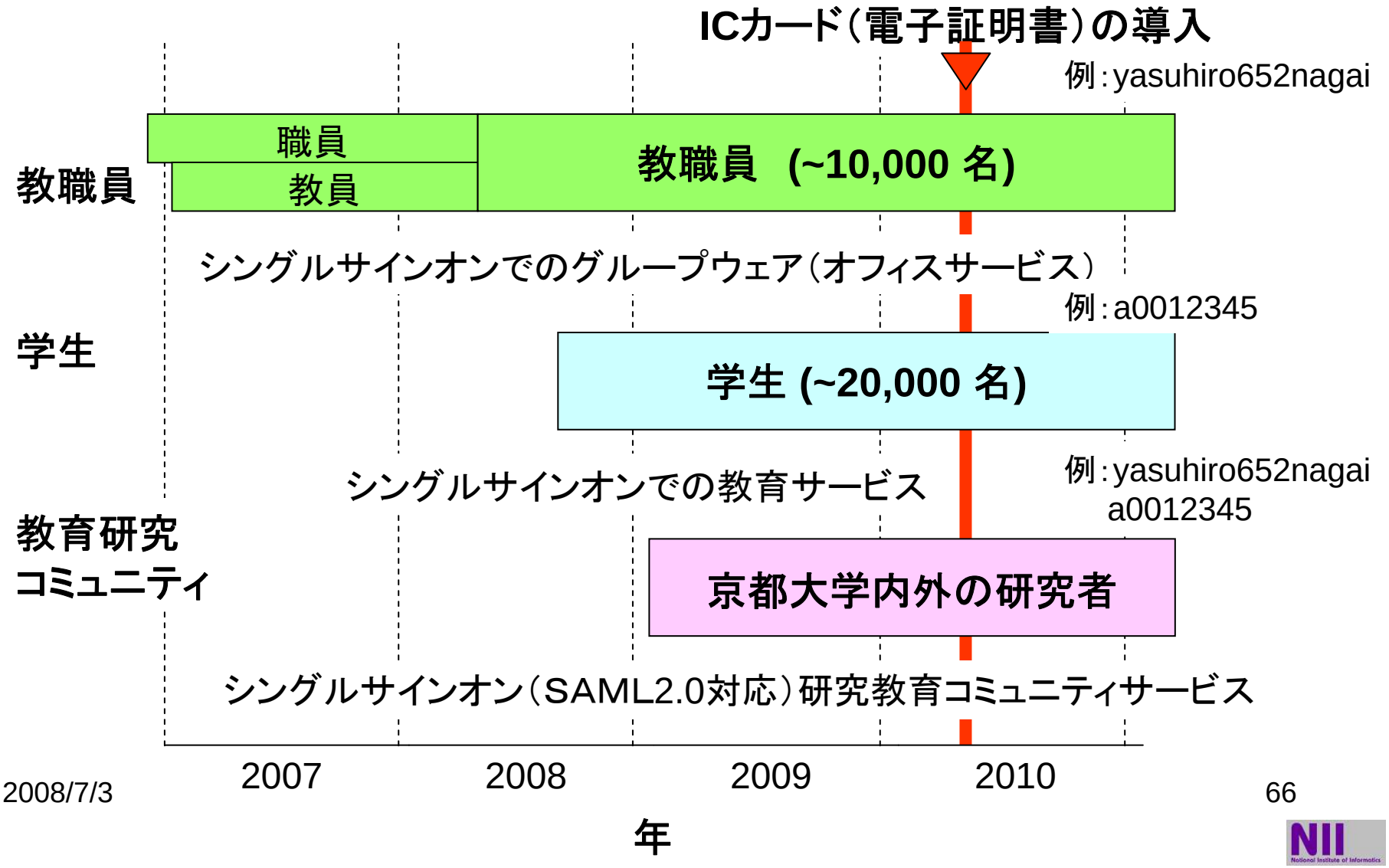


UPKI-Federation Testbed

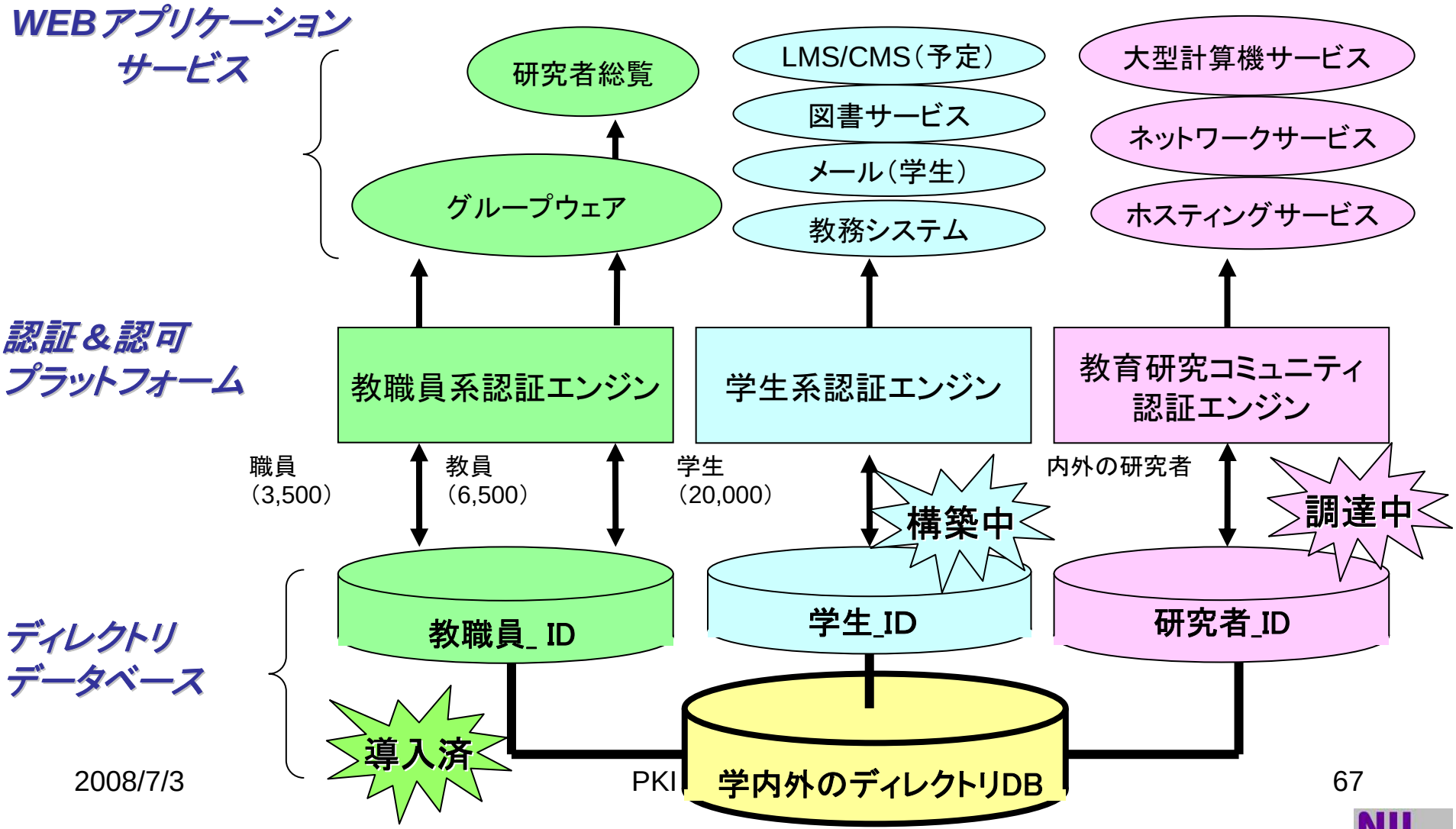
(4) 京都大学での統合認証の現状と今後

認証基盤の構築スキーム

※H20年度4月時点で全学オーソライズされた実施スキーム

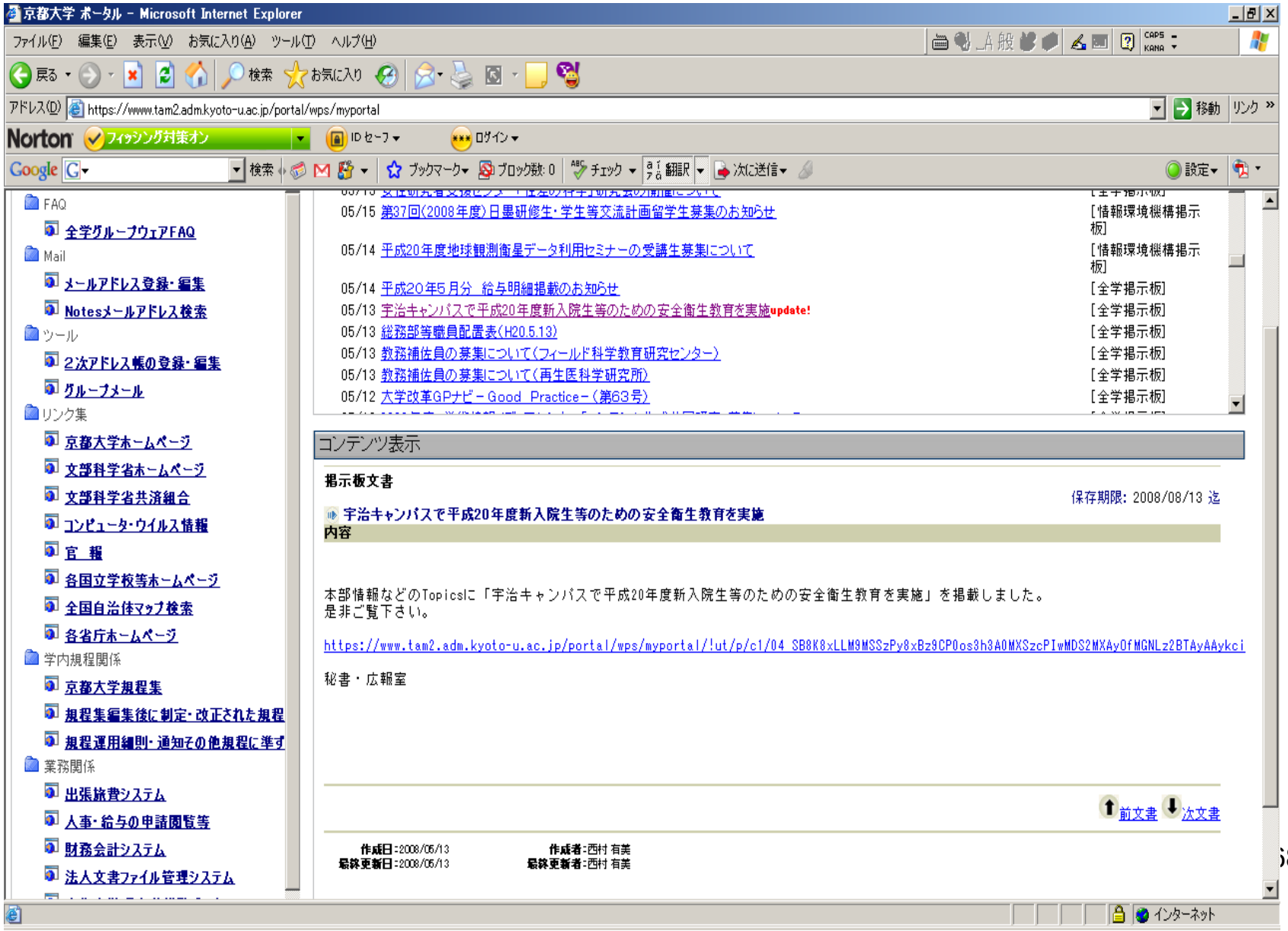


認証基盤全体イメージ


WEBアプリケーション
サービス
研究者総覧
グループウェア
LMS/CMS（予定）
図書サービス
メール（学生）
教務システム
大型計算機サービス
ネットワークサービス
ホスティングサービス
認証＆認可
プラットフォーム
教職員系認証エンジン
学生系認証エンジン
教育研究コミュニティ
認証エンジン
職員
（3,500）
教員
（6,500）
学生
（20,000）
内外の研究者
構築中
調達中
ディレクトリ
データベース
教職員_ ID
学生_ID
研究者_ID
導入済
学内外のディレクトリDB

UPKI 教職員用グループウェア認証（例）

※H20年度4月時点で既に稼動中



UPKI PKIトライアルと得られた知見

※H19年度CSI経費にて物品など購入・契約、本件はそれに対する結果報告

■概要：

・情報環境機構の常勤の教職員を中心に、H19年7月30日より約90名にPKIトライアルのICカード＆リーダライタを配布（MAC対象外）
・NII-CP/CPSをカスタマイズして運用（本番と同様、CRLは未対応）
・検証用SAML対応ポータルのログイン認証にて、サービス利用検証
・60名のアンケートを回収し（約70%）、結果を集計して考察

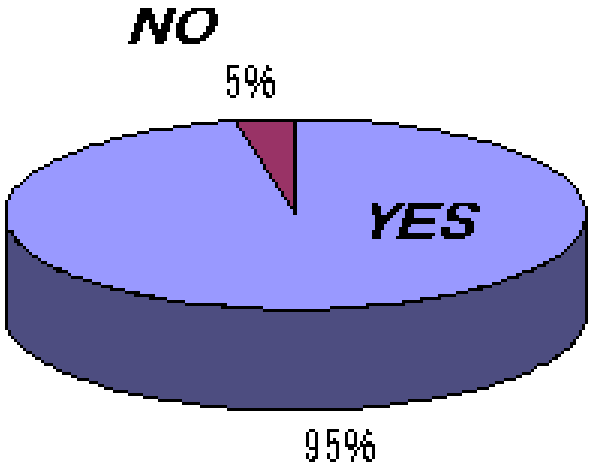
■結果と得られた知見：

(1)リーダライタやPKIドライバのインストール、証明書PIN変更から内容確認まで実施（95%）
⇒インストールからPIN変更まで利用者にやってもらう事は可能
但し、OS、ブラウザ毎の細かな対応が必要、FAQも必要
(2)電子証明書での認証、PIN変更できた利用者は実施（100%）
(3)S／Mimeと電子証明書インポートは35%前後の利用者が成功
⇒今回、利用者が少ないのは、アドレスがない、メーラが違う、適当な証明書が無い等が主な理由

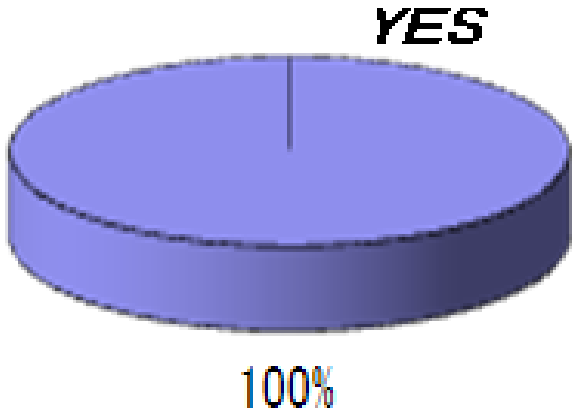
NII National Institute of Informatics

アンケート結果（抜粋）

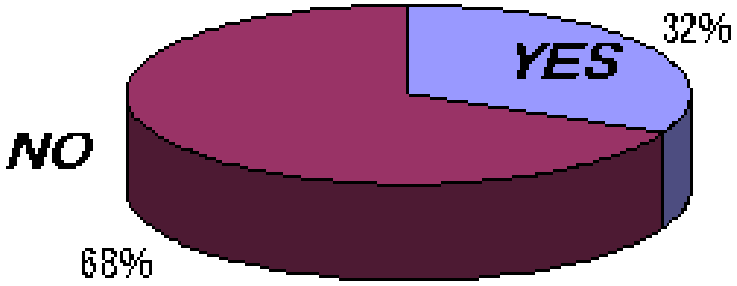
問題なくPIN変更できた



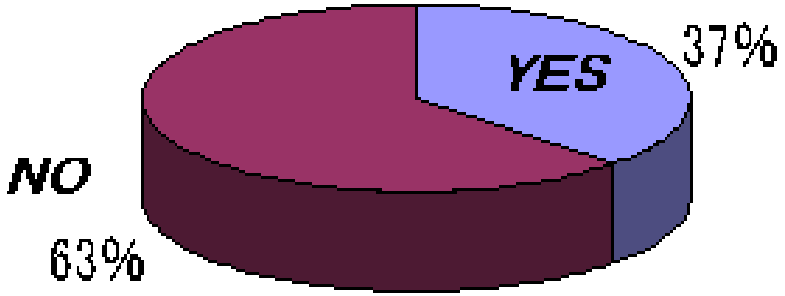
問題なくポータルへログインできた



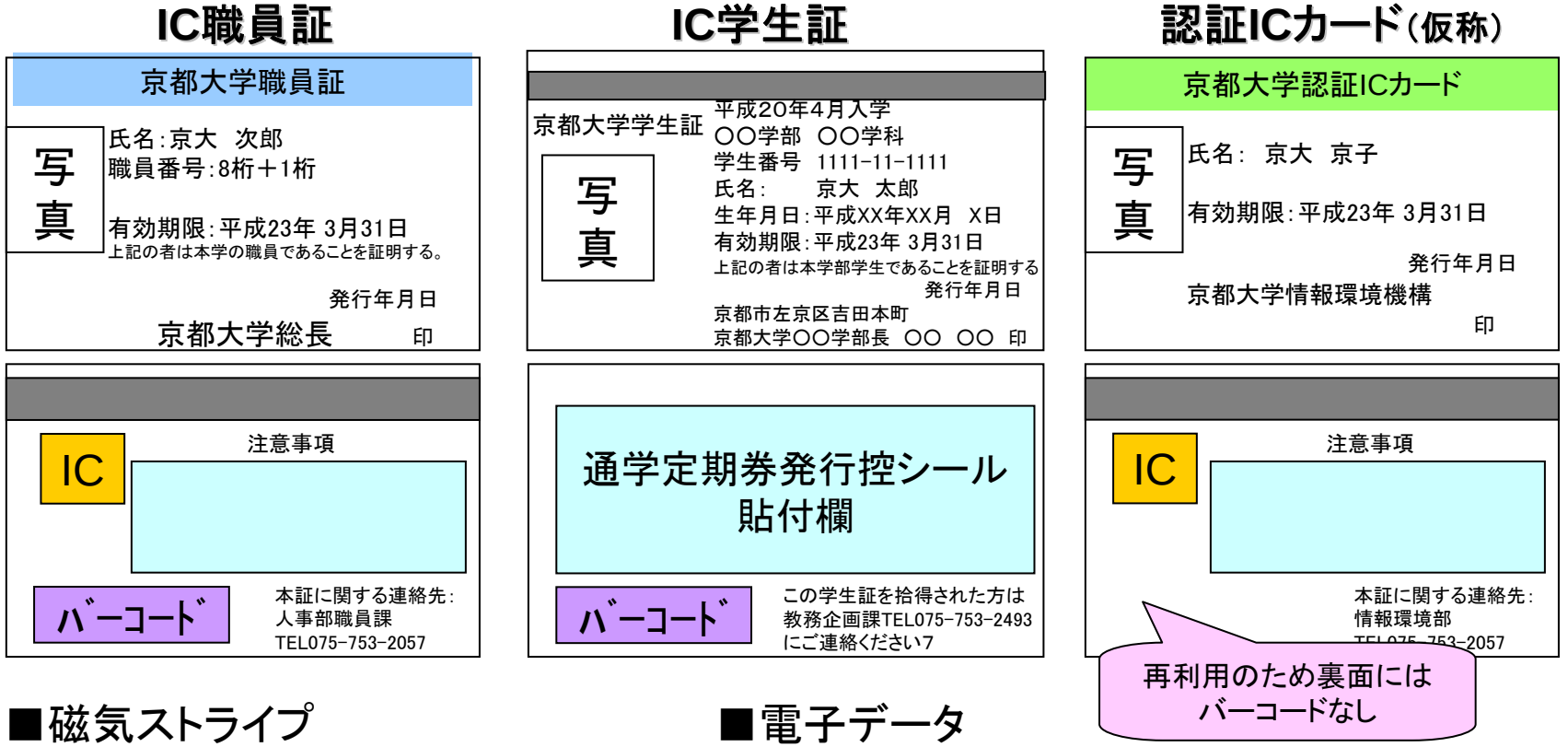
S/MIMEを利用できた



他の電子証明書をカードに書き込めた



ICカードの券種イメージ



■磁気ストライプ

・個人番号＋再発行回数（現行とおり）

■バーコード（病院等で利用し実績有り）

・個人番号（10桁、NW7）

■電子データ

・認証用識別名（DN）、利用者ID（CN）（接触ICチップに搭載）

・基本ID情報（FCFフォーマットに準拠（※1）

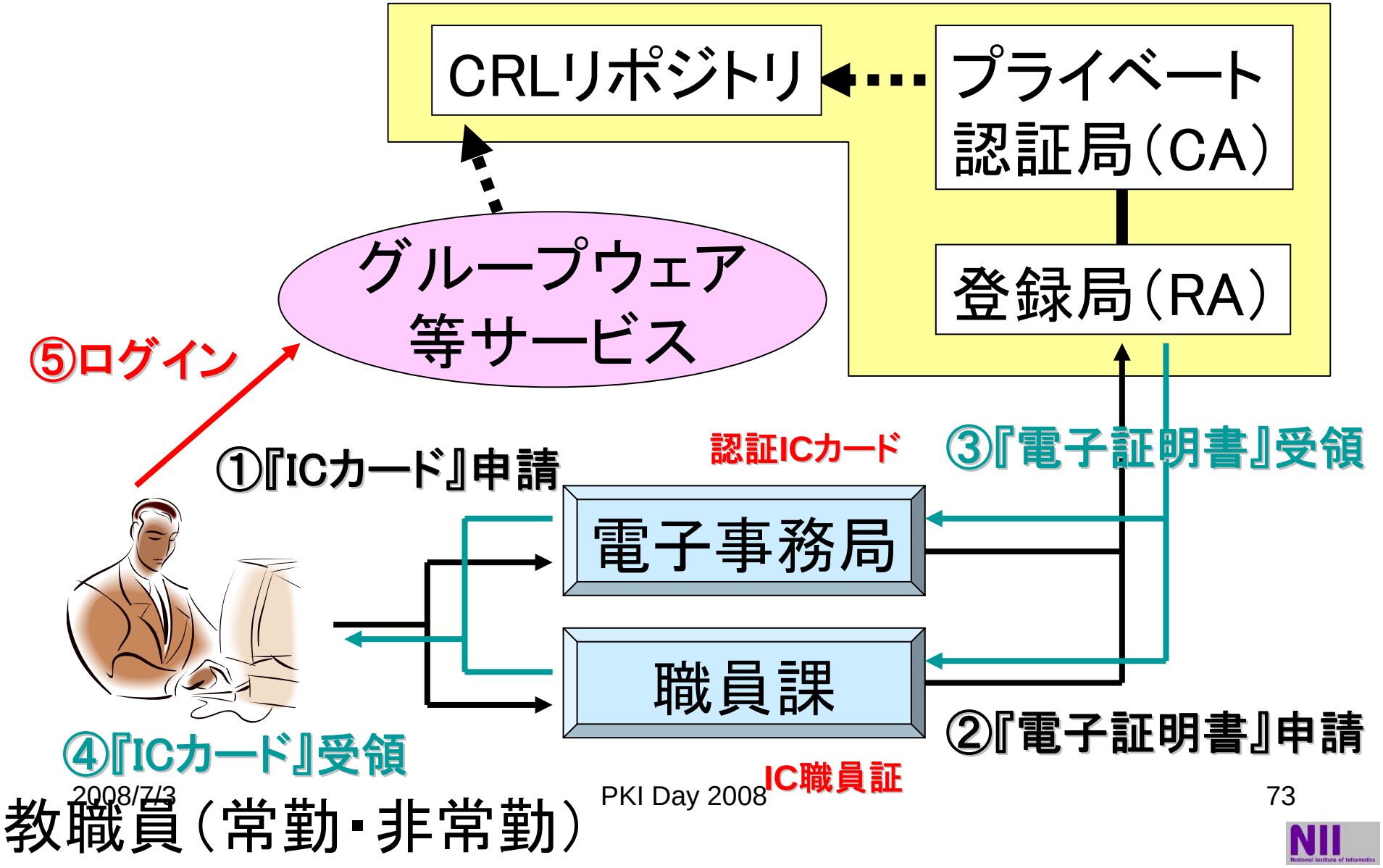
（※1）利用者区分（2Byte）＋ID番号（個人番号12Byte）＋再発行フラグ（1Byte）
＋氏名（半角カタカナ／英字）＋学校識別コード＋発行年月日＋有効期限

利用サービスのイメージ

主な対象者	教職員（常勤）	教職員（非常勤）	学生	その他
証の名称	職員証	認証ICカード	学生証	施設利用証
導入後の利用サービス（共通）	**物理的セキュリティ** （例：建物への入退館、図書館、サーバ室、研究室、事務室など）			
	・グループウェアの**個人認証** ・**電子メール暗号化** （外部へはパブリック証明書利用を推奨） ・**セキュアな印刷とコピー**		**証明書自動交付**	
4年後を目処に収容するサービス	生協など**少額決済** 電子ロッカー 施設利用システム連携			
	グループウェア以外の**セキュアな業務への認証／暗号化**（PKI利用）		**教育利用** （出欠、レポート）	
5年以降に収容を検討するサービス	**部局の業務、サービスへの適用**（例：システムログインなど）			
	他大学との研究・教育リソースの共有（認証など）		他大学と単位互換 OBカード利用など	

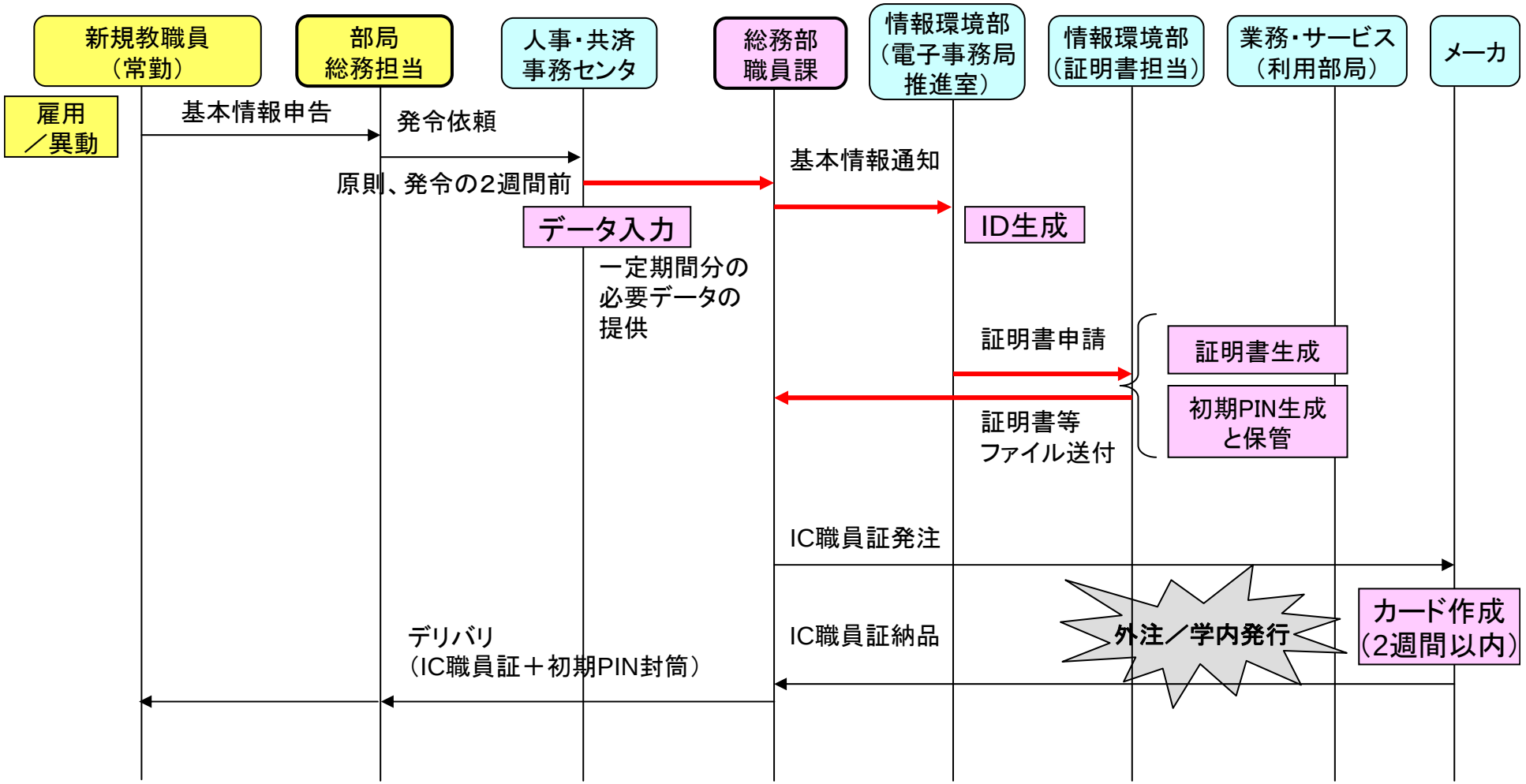
認証局等運用イメージ

※H20年度6月より調達中



IC職員証発行イメージ（例）

※H20年度6月より調達中



代理入力方式の提案と評価

※企業との共同研究を一部含む

■SSO、ID名寄せで運用の問題が懸念される

-現実運用中の代理入力、ポジションIDの『認可』対処

■SSO環境で、電子証明書を利用して権限委譲による『認可』処理（代理入力）を考案

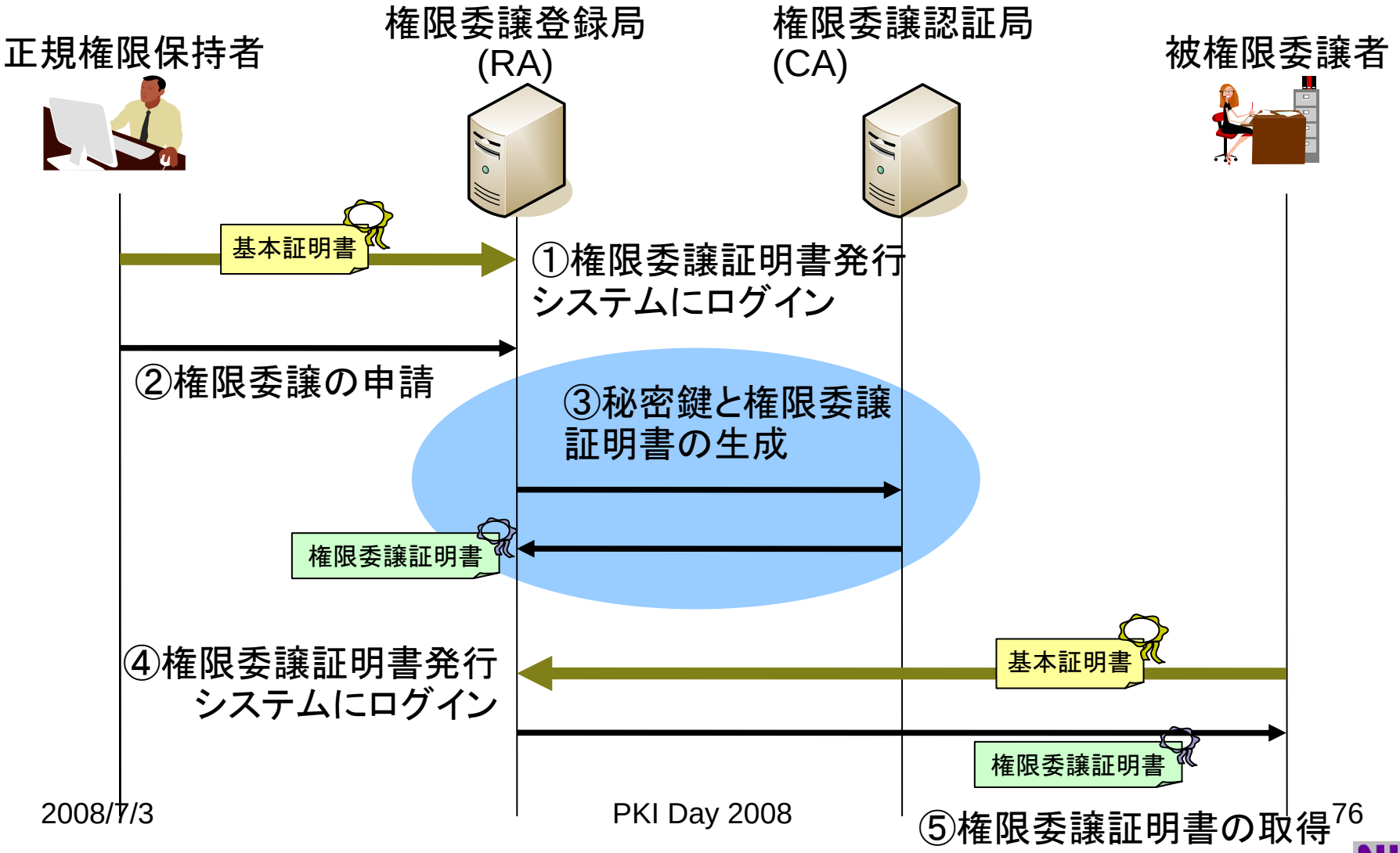
-『認証』で基本証明書（ICカード）を利用するのであれば
権限委譲の『認可』も同じ作法で利用

■『認可』対応は原則バックエンド側（代理入力）だが必要な『認可』情報をICカードで分散管理

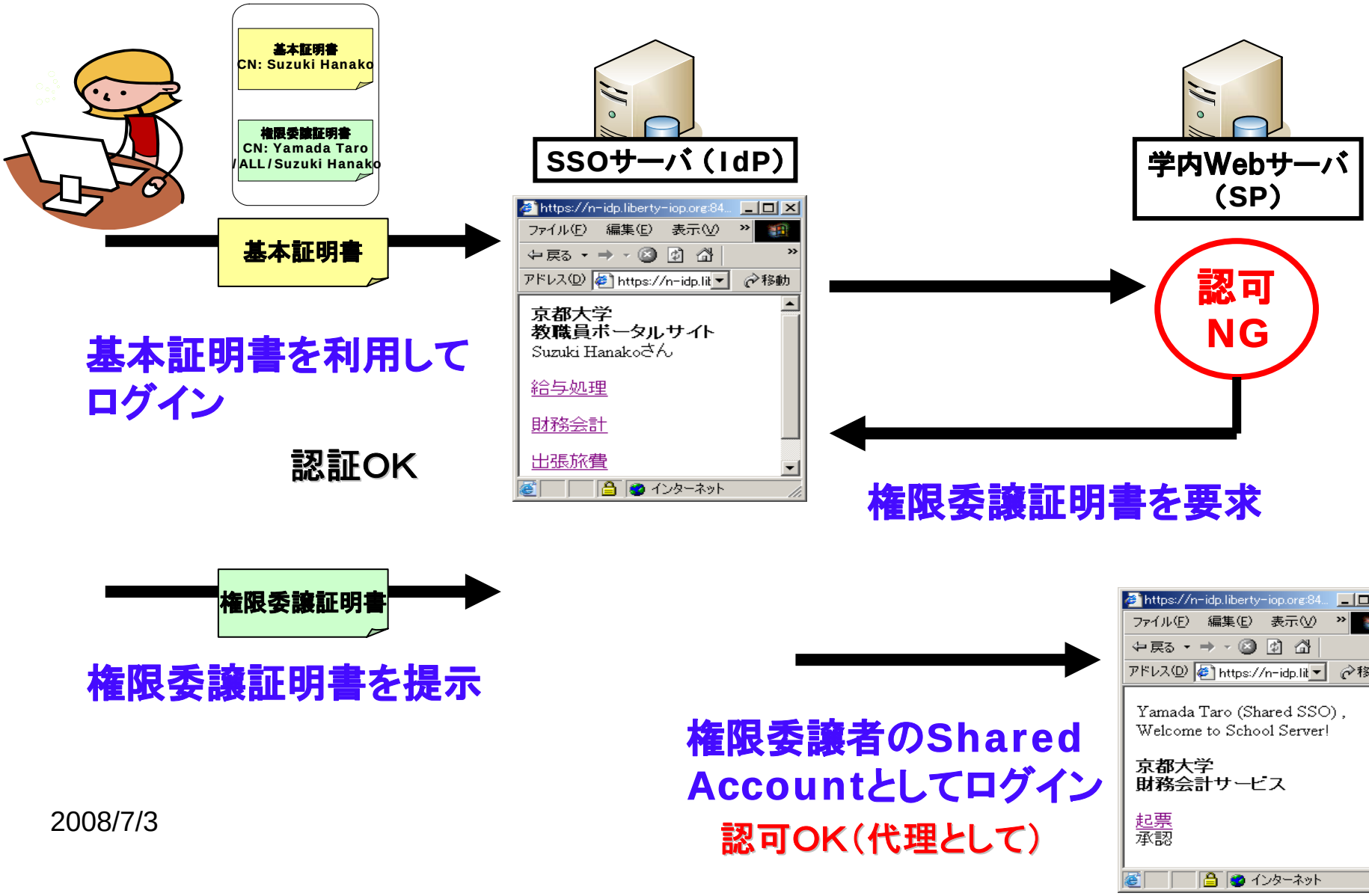
-委譲情報（属性情報）をサーバに格納するのではなく、利用者が
権限委譲証明書として保管

-『認証』の基本証明書と共にICカードに格納して利用

権限委譲証明書の発行の流れ



権限委譲時の認証・認可処理



2008/7/3

まとめ

海外機関の調査・国際連携

- **海外の大学等の認証基盤構築を調査**
  2005年11月（米国 Stanford大学, VeriSing社他、カナダ EnTrust社）
  2006年　7月（オーストラリア クイーンズランド大学, AARNet他）
  2006年11月（米国 ウイスコンシン大学Madison校）
  2007年 7月（スイス SWITCH, オランダ Terena）
  学内認証基盤, PKI運用, eduroam, Shibbolethの動向等を調査
- **国際会議での発表・活動**
  - APAN (Asia Pacific Advanced Network) Meeting
    - 2005夏・台北, 2006冬・東京, 2006夏・Singapore, 2007冬・ Manila, 2007夏・西安
    - Middleware WG (2006～）
  - SAINT2007 Workshop on Middleware Architecture in the Internet (Hiroshima)
  - AP Grid PMA meeting (Osaka, 2006)
  - TERENA 9th TF-EMC2 (Prague, 2007)

今後の展開

- 平成20年度
  - 18年度に行った調査，研究および基本設計、19年度の詳細設計とプロトタイプシステム開発に基づき、実証実験を実施
  - 認証アプリケーションの開発と公開
  - 大学間連携の前提となる，各大学での認証基盤構築の支援
  - 21年度以降の新プロジェクトの提案

オープンドメインPKI
  - オープンドメイン認証局の運用とサーバ証明書の啓発・評価研究
  - S/MIMEの活用、クライアント証明書発行方式の検討

キャンパスPKI
  - 7大学とNIIにプロトタイプ認証局を構築し，相互接続性の検証，試行運用等を実施
  - Webシングルサインオンの実験システム構築
  - eduroamをベースに、PKIによりセキュリティを強化した、大学間無線LANローミング方式の開発

グリッドPKI
  - NAREGIおよび8センターグリッド研究会との連携
  - NAREGI CAソフトウェアの活用

UPKIの先にあるもの？

- 20年前のインターネットとの類似性
  - 大学が主導して（電気通信事業法すれすれのところで）「とにかくつなげ！」
    - **性善説・相互扶助精神**
  - そのころ電話会社はB-ISDNに注力していた…
    - QoS保証、セキュリティ、…
  - 現在はすべてがインターネット化
    - 矛盾も顕在化

  ⇒新世代ネットワークの研究

- UPKIの考え方
  - PKIにこだわらず、認証を「とにかくつなぐ」
    - Shibboleth, raduis, …
  - 軽いPKIを指向
    - “なんちゃってPKI”と従来型PKIとの間を狙う
- 20年後の夢
  - UPKI型の軽いPKIがはびこって社会問題化？

UPKIの今後にご期待(?)ください

ご清聴ありがとうございました