



UPKI全体報告

国立情報学研究所 認証作業部会主査

京都大学学術情報メディアセンター教授

岡部 寿男

-
- 1 . UPKIについて
 - 2 . UPKI3年間の成果
 - 3 . 今後の計画

1 . UPKIについて

全国大学共同電子認証基盤 (UPKI) とは

- 平成17年頃から、7大学情報基盤センターとNIIで、大学の資源を共有するための認証基盤を検討
- 平成18年2月15日にキックオフのシンポジウムを開催
- 大学が保有するスパコン、電子コンテンツ、ネットワーク等の学術情報資源を、安心・安全かつ有効な活用が可能な基盤を目標にする
- 先行する海外の学術機関の事例、PKI以外の技術も積極的に取り入れて研究・開発する
- 7大学情報基盤センター群とNIIで概算要求を行い、平成18～20年度の3年間、特別教育研究経費(研究推進:大学間連携)が認められた。



最先端学術情報基盤を構成するUPKI

最先端学術情報基盤 (Cyber Science Infrastructure: CSI)

人材育成及び推進体制の整備
(推進組織・人材確保等)

バーチャル研究組織/ライブ
コラボレーションの育成・支援

学術コンテンツの確保・発信システム

コンピュータ資源を結ぶグリッドの実用展開

大学・研究機関のための認証システムの開発と実用化

学術情報ネットワーク(SINET3)の運用

【NIIと大学の情報基盤センターや図書館等連携による
学術情報ネットワークの運用と学術コンテンツ整備・発信】

- 学術情報ネットワーク運営・連携本部 (H17.2設置)
- 学術コンテンツ運営・連携本部 (H17.10設置)



大学・研究機関の研究リソース整備・研究成果等の発信

産業・社会貢献

国際貢献・連携

UPKI実施体制

大学・研究機関

国立情報学研究所

学術情報ネットワーク運営・連携本部

ネットワーク作業部会

認証作業部会

グリッド作業部会

高等教育機関における
情報セキュリティポリシー推進部会

学術コンテンツ運営・連携本部

図書館連携作業部会

学術ネットワーク研究開発センター

ネットワークグループ

認証基盤グループ

リサーチグリッド研究開発センター

学術コンテンツサービス研究開発センター

学会・関連機関

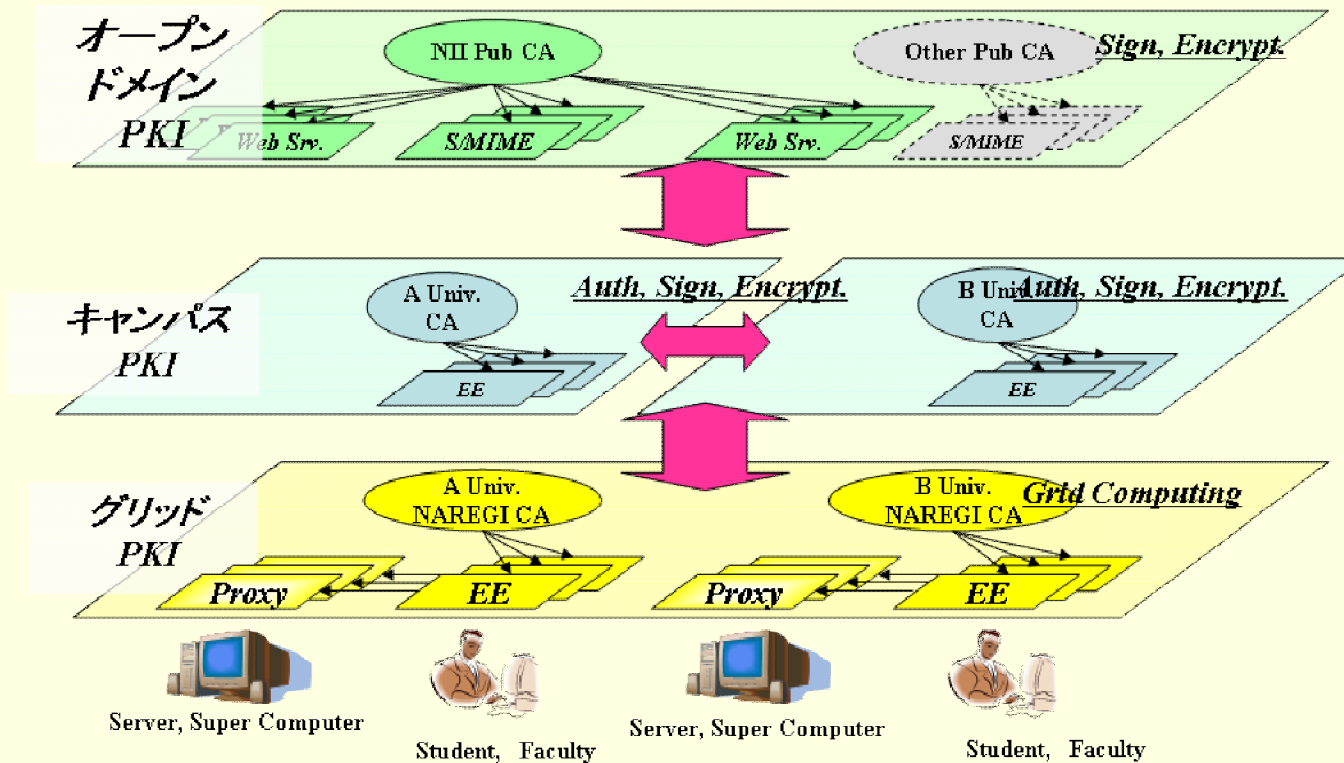
UPKIの構想段階では

- プライベート認証局の連携による，大学間連携を模索
- 大学の認証局を用いて，「サーバ証明書」「S/MIME証明書」「コード証明書」「官職証明書」を発行し，大学間連携，産学連携に活用
- このため，認証局間の連携方式の調査・分析を実施

| | イメージ | 長所 | 短所 |
|--------------|------|--|---|
| ルートモデル | | <ul style="list-style-type: none"> ・ユーザ規模，用途により下位CAを増やせる ・認証パスの構築が容易 ・ウェブブラウザ等の製品が標準でサポート | <ul style="list-style-type: none"> ・ルートCAに権限が集中する ・ルートCAの鍵が危殆化した場合，前証明書の再発行が必要 |
| ブリッジモデル | | <ul style="list-style-type: none"> ・他CAの追加が容易 ・他ドメインのCA鍵危殆化の影響範囲が局所的 | <ul style="list-style-type: none"> ・認証パスの構築，検証が複雑になる ・ウェブブラウザ等が対応していない |
| Pear to pear | | <ul style="list-style-type: none"> ・他CAの追加が容易 ・ポリシーによる制約が可能 | <ul style="list-style-type: none"> ・他CAとの連携維持管理及び認証パス構築が難しい ・相互認証証明書の登録が必要 ・ウェブブラウザ等が対応していない |

UPKI 3層アーキテクチャ

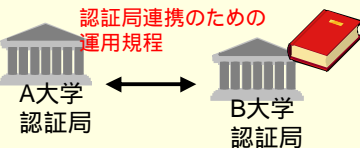
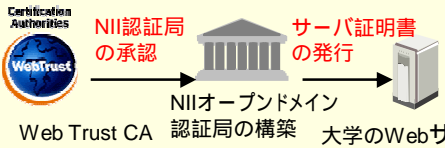
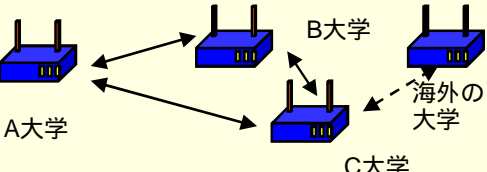
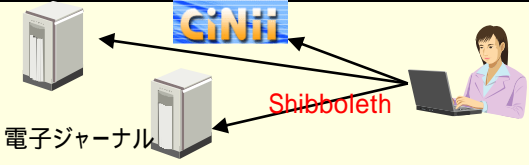

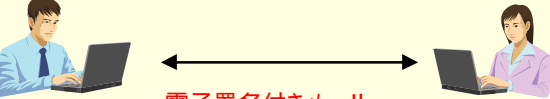
- PKIの階層を3つに分け, 認証局の用途や強度レベル等を分けて検討
- 階層内, 階層間の認証技術, 認証アプリケーションの研究・開発を実施
- あわせて, 大学で利用できるアプリケーションも開発



各階層のコンセプト

- オープンドメインPKI層
 - 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層
 - 各大学が個別のポリシー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)
- グリッドPKI層
 - 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

6つの項目に基づく取り組み

| 項番 | 実施項目 | 内容 | 実績 |
|----|-----------------------------------|--|--|
| 1 | 「UPKI共通仕様」の作成と配布 |  <p>認証局連携のための運用規程</p> <p>A大学認証局 ↔ B大学認証局</p> <p>大学の認証局のための「認証局運用規程」のひな形を作成 セキュリティレベルを統一して認証局連携を容易にする</p> | 平成18年度, 19年度に作成し, Webで公開中 |
| 2 | オープンメイン認証局の構築とサーバ証明書の発行 |  <p>NII認証局の承認</p> <p>サーバ証明書の発行</p> <p>Web Trust CA → NIIオープンメイン認証局の構築 → 大学のWebサーバ</p> <p>オープンメイン認証局の構築 サーバ証明書の発行</p> | 平成19年度から, 「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」を開始 → 21年度から新プロジェクト開始 |
| 3 | 大学間無線LANローミングの実現 |  <p>A大学 ↔ B大学 ↔ C大学 ↔ 海外の大学</p> <p>認証を用いた大学間の無線LANローミングの実現</p> | 平成18年度から, eduroam方式による無線LANローミングを開始 |
| 4 | コンテンツサービスのシングルサインオン実現(フェデレーション構築) |  <p>電子ジャーナル</p> <p>Shibboleth</p> <p>CILogon</p> <p>1つのIDで複数のDBにアクセスを可能とする仕様を検討</p> | 平成20年度, 27機関の協力により, シングルサインオン実証実験を実施 → 21年度から試行運用を開始 |
| 5 | NAREGI-CAを利用したキャンパスPKIスタートパックの開発 |  <p>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, 大学認証局を簡単に構築できるソフトウェアを開発</p> | 平成18年度に開発し, Webで公開中 |
| 6 | S/MIME証明書の試験利用 |  <p>電子署名付きメール, メール暗号化の実現</p> <p>S/MIMEを関係者間で使用するとともに, 発行方法等の検討を実施</p> | 平成18年度から試験利用を開始 一部はサーバ証明書発行のための本人確認に利用 |

UPKIイニシアティブ

- UPKIの相互運用性, 利用促進に関する意見交換や技術的な検証を行う場として設立(平成18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/>)
- 各活動のページから関連情報、資料を発信

UPKIポータルの
トップページ

各活動のページが
並んでいます。

UPKI Initiative

ホーム news 公開資料 フォーラム 共通仕様 サーバ証明書PJ 認証局スタートパック SSO実証実験 会員登録 運営組織
***** ログイン *****

現在の場所: ホーム

ニュース

シングルサイ
ンオン実証実験中
間報告会資料公
開
2008年11月26

UPKIイニシアティブとは

作成者 staff - 最終変更日時 2008年10月21日 20時27分

UPKIイニシアティブは、最先端学術情報基盤(サイバー・サイエンス・インフラストラクチャ: CSD)を
実現するために構築中である大学間連携のための全国大学共同電子認証基盤構築事業(UPKI:
University Public Key Infrastructure)の仕様や利用方法について、公開資料の掲載、

2 . UPKI 3 年間の成果

UPKI共通仕様の作成

■ 目的

- 大学認証局のセキュリティレベルを揃え，連携を容易にする
→ キャンパスPKI層の大学連携
- CP/CPSのサンプル，仕様書のサンプルを作成し，運用コスト，調達コストを低減する

■ 概要

- 認証局を調達するための「仕様書」
- 認証局のCP/CPSのひな形
- CP/CPSは，アウトソース版とインソース版を作成
- 情報セキュリティポリシーサンプル規程集の一部としても活用

UPKI共通仕様

キャンパス PKI 調達仕様ガイドライン(アウトソース版)

キャンパス PKI調達仕様ガイドライン編
キャンパス PKI調達仕様テンプレート編



キャンパス PKI CP/CPSガイドライン(アウトソース版)

キャンパス PKI CP/CPSガイドライン編
キャンパス PKI CP/CPSテンプレート編



キャンパス PKI CP/CPSガイドライン(インソース版)

キャンパス PKI CP/CPSガイドライン編
キャンパス PKI CP/CPSテンプレート編

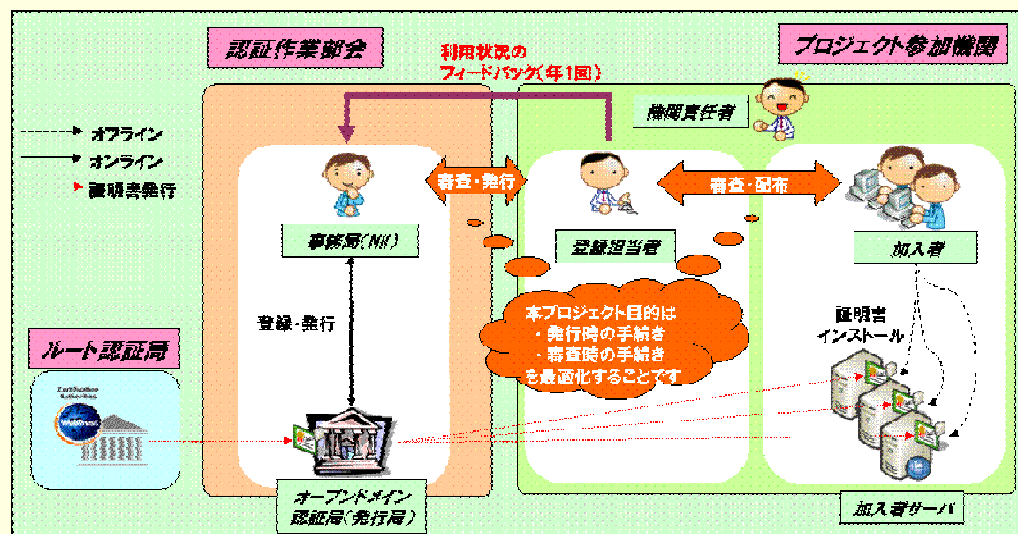
サーバ証明書発行・導入における啓発・評価 研究プロジェクト

■ 目的

- オープンドメイン層の認証基盤の構築
- 大学等における、サーバ証明書発行時の審査・証明書配付方式の最適化
- サーバ証明書の重要性の啓蒙活動

■ 概要

- サーバ証明書発行業務(審査)の一部を大学で実施
- プロジェクトではあるが、発行する証明書は“本物”のサーバ証明書
- 1月末現在、90機関が参加し、1900枚の証明書を発行
- 現在のプロジェクトは6月で終了し、新プロジェクトを4月から開始
→ 詳細は午後の講演で説明します



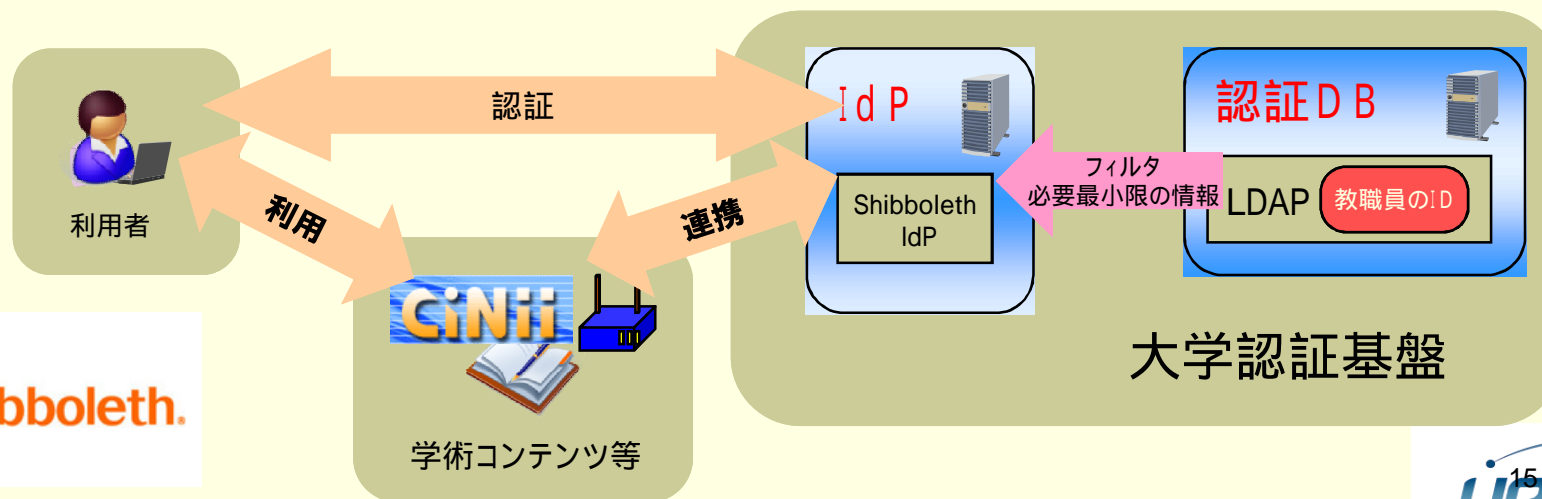
シングルサインオン(フェデレーション構築)

■ 目的

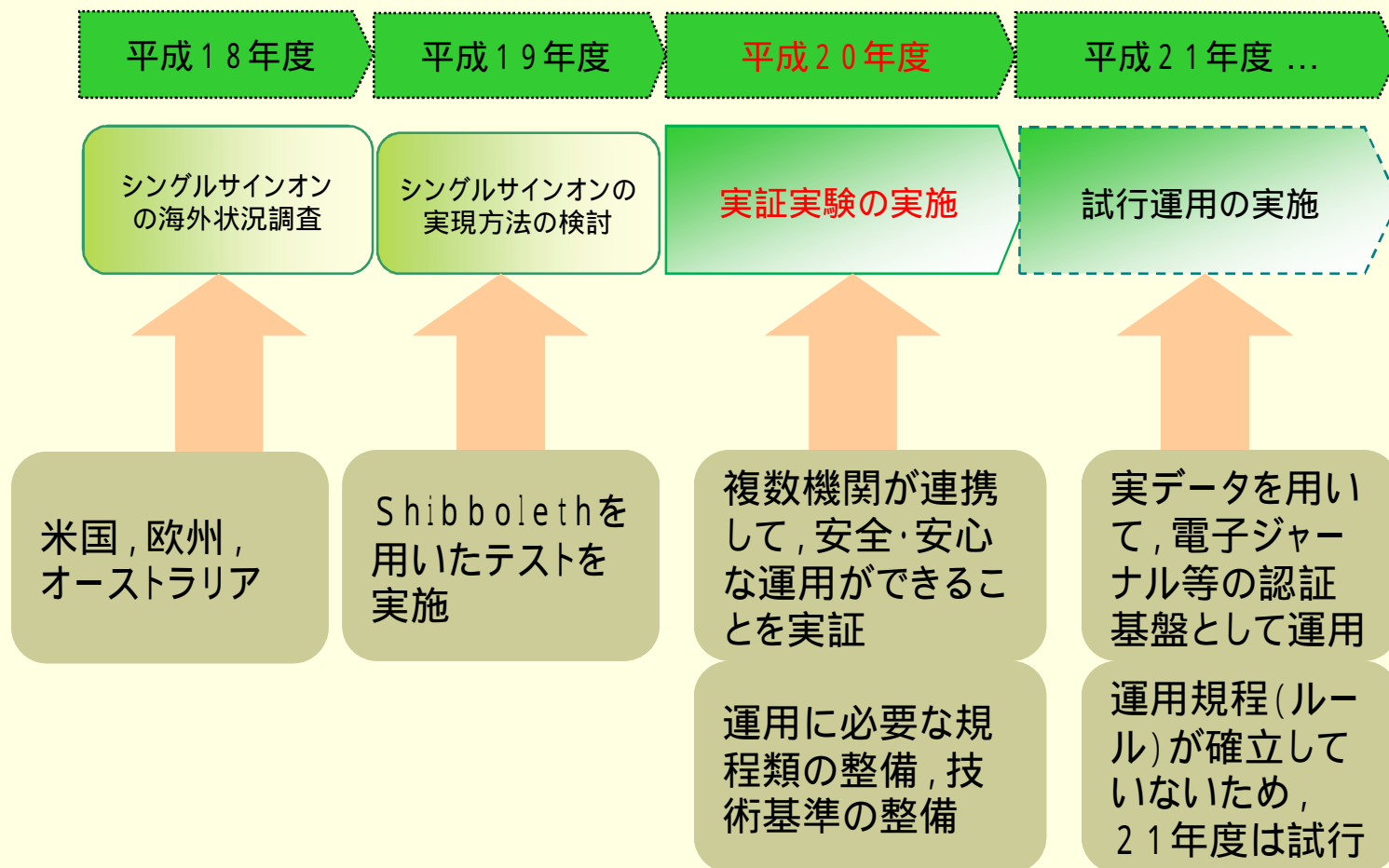
- キャンパスPKI層の学内認証と, 大学間の認証連携を実現
- コンテンツサービス利用を中心とした認証基盤の構築

■ 概要

- Internet2が開発したShibbolethを利用
- 学内に, LDAP等で構築したデータベースがあれば, そのまま利用可能
- 欧米の図書館を中心に, 電子ジャーナル利用等に普及
- 平成20年7月から, 27機関により実証実験を開始
- Science Direct(Elsevier)との利用実験を実施



シングルサインオン実証実験 (平成20年度)



日本のフェデレーションを構築することが目的

無線LANローミング

■ 目的

- 大学間で無線LANを共有し, 安心・安全にインターネット環境を提供する

■ 概要

- 欧州, アジア・オセアニア等で普及しているeduroam方式により, 無線LANローミングを実現
- RADIUS連携で実現できることから構築が容易
- 海外のeduroam機関との連携により, 海外の学術機関とも相互利用
- 平成21年2月現在, 国内10機関が運用



キャンパスPKIスタートパックの開発

■ 目的

- オープンソースの認証局ソフトウェアであるNAREGI - CAを活用し、低コストでの認証局構築をサポートする

■ 概要

- NAREGI - CAをコンパイル、インストールするためのスクリプト群から構成されている
- 難しい設定をしなくても、無線LAN向け認証局として利用できる環境が自動的に設定される
- 本格利用のためには、手動で環境設定が必要
- UPKIイニシアティブのサイトからダウンロード可能

The screenshot shows the NAREGI-CA RA Management Site. The header includes the NAREGI-CA logo and the text "National Research Grid Initiative". Below the header, there is a table with the following information:

| | | | |
|-----------|--------------|------------|--|
| NAREGI CA | RAオペレータ管理サイト | 操作者名 | CN=RAAdmin003, |
| | | 識別ID | e6144984ebbbe476b081e5Jfb37b8dc08cb30a |
| サイト操作 | RA管理者操作 | RAオペレーター操作 | |

Below the table, there are several navigation links:

- ▶ RAアドミニストレータ情報
 - ◉ RAアドミニストレータ証明書詳細 / RAアドミニストレータ証明書ダウンロード
 - ◉ RA CA設定表示
 - ◉ CA証明書詳細 / CA証明書ダウンロード / ORLダウンロード
- ▶ RAオペレーター操作一覧
 - ◉ RAオペレーター登録申請
 - ◉ RAオペレーター申請状況 / RAオペレーター申請一覧 / RAオペレーター更新申請一覧 / RAオペレーター有効申請一覧
 - ◉ RAオペレーター検索 / RAオペレーター一覧

At the bottom of the page, there is a copyright notice: "(c) 2008 National Research Grid Initiative" and "NAREGI-CA RA Management".

グリッドとの連携

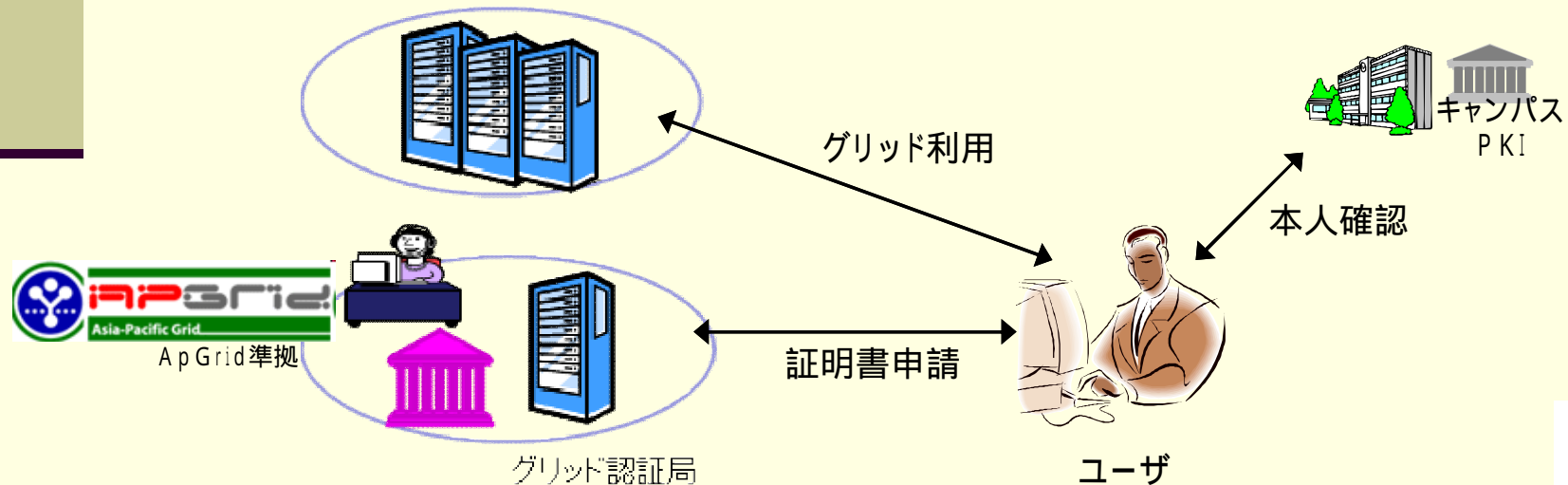
■ 目的

- 大学の認証基盤を用いて、グリッドコンピュータ利用に必要な証明書発行を行う

■ 概要

- UPKI3層の、グリッド層とキャンパスPKI層の連携
- グリッド用の証明書は、厳格な管理と本人確認を求められている
- アジア太平洋地区は”ApGrid”の基準を満たす必要がある
- この実現のための、ポリシー検討等を実施した

グリッドコンピュータ



3. 今後の計画

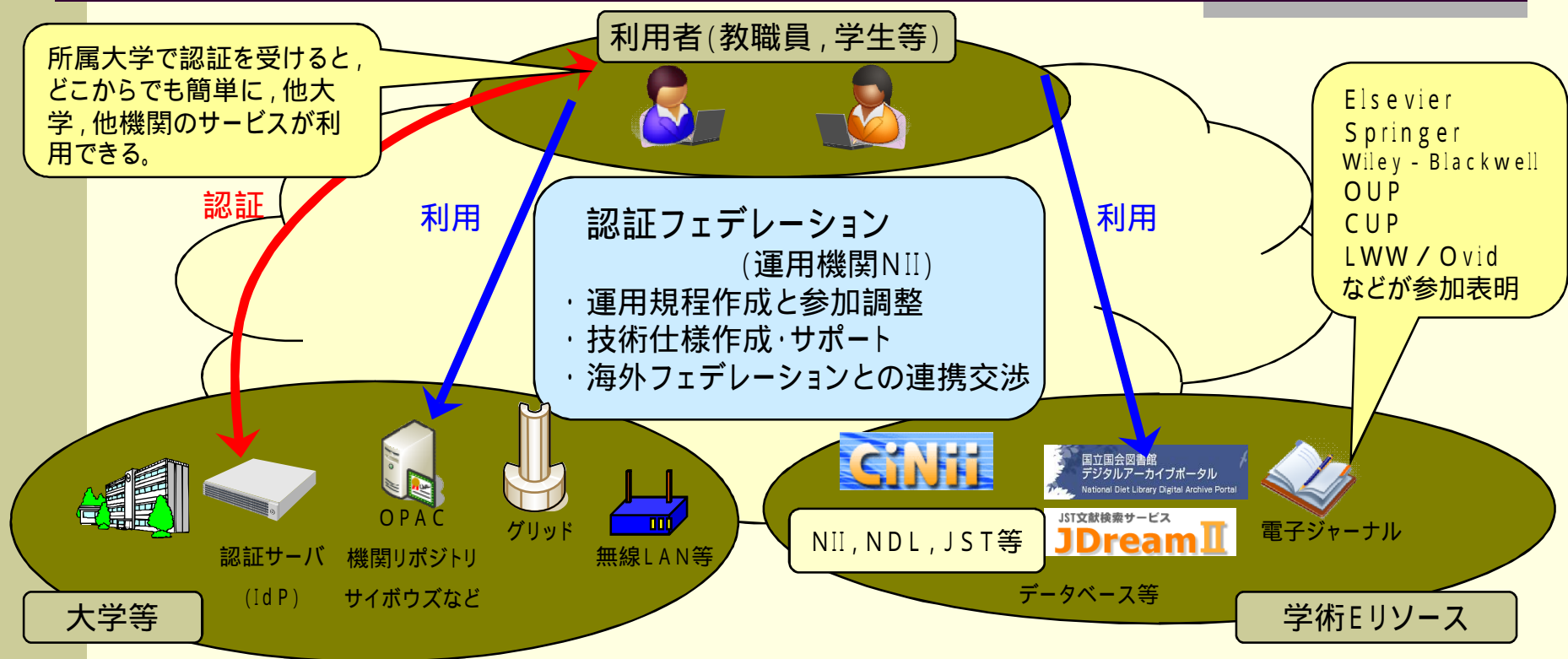
平成21年度以降のUPKI

21年度から、UPKIは研究開発のフェーズから運用フェーズに向けて一歩前進します。これまでの成果を生かして、次の2つの項目を実施します。

- サーバ証明書プロジェクトの継続
 - 現プロジェクトは、平成21年6月末で終了
 - 平成21年4月～24年3月までの3年間、新プロジェクトを実施
 - 平成21年4月～6月の3ヶ月間は移行期間
 - 新プロジェクトは、ウェブ画面からの証明書発行申請を可能に
 - 自動発行の技術的検証を実施

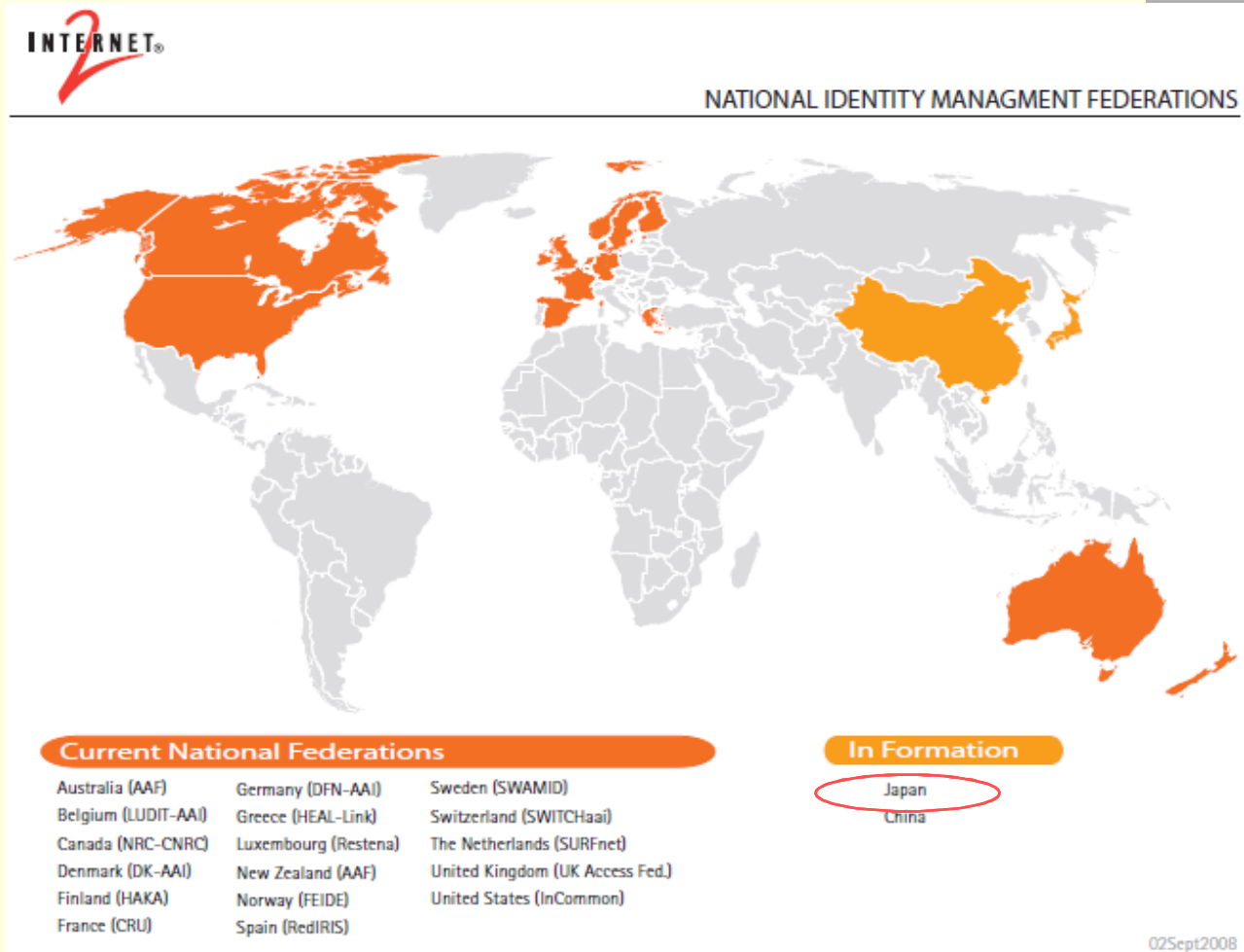
- 認証フェデレーション試行運用
 - 実証実験の成果を利用し、日本での認証フェデレーション運用を開始
 - まずは、実証実験参加機関を中心に、実利用可能な認証基盤の構築
 - 電子ジャーナル等の実利用を実現
 - NIIのコンテンツサービスであるCiNiiも対応
 - フェデレーション運用のためのルール(規程等)の整備をあわせて実施
 - グリッド、ネットワーク利用のための認証基盤として利用

認証フェデレーションの構築



- 大学等とNIIが連携して「認証フェデレーション」を構築・運用する
- 2009年4月からフェデレーション試行運用を開始
- 2009年4月時点で、複数の大学、NII内でのシングルサインオン実現
- 2010年4月からの本格運用を目指す

世界のフェデレーション



Internet2 informatin kits http://www.internet2.edu/pubs/national_federations200809.pdf から引用

日本はまだ準備中，世界に遅れないためにもフェデレーションの運用開始は重要

まとめにかえて

■ 午後の講演

- 14:00 ~ 認証を用いたセキュリティ対策
岡田 仁志 (情報社会相関研究系准教授, 高等教育機関における
情報セキュリティポリシー推進部会副主査)
- 14:20 ~ 電子証明書の意義とサーバ証明書新プロジェクトの計画
島岡 政基 (学術ネットワーク研究開発センター特任准教授)
- 14:40 ~ Shibbolethを用いたフェデレーション構築計画
片岡 俊幸 (学術ネットワーク研究開発センター特任准教授)
Nate Klingenstein (Internet2 Technical analyst)
- 15:10 ~ 認証基盤を活用したコンテンツサービスの展開
阿藪品 治夫 (学術基盤推進部学術コンテンツ課係長)