UT-CA 講演会資料

2007.04.27

CSIとUPKI
進捗状況と今後の展開

曽根原 登 中村 素典

国立情報学研究所 教授

学術情報NW運営・連携本部 認証作業部会

NII 学術NW研究開発センター 認証基盤G

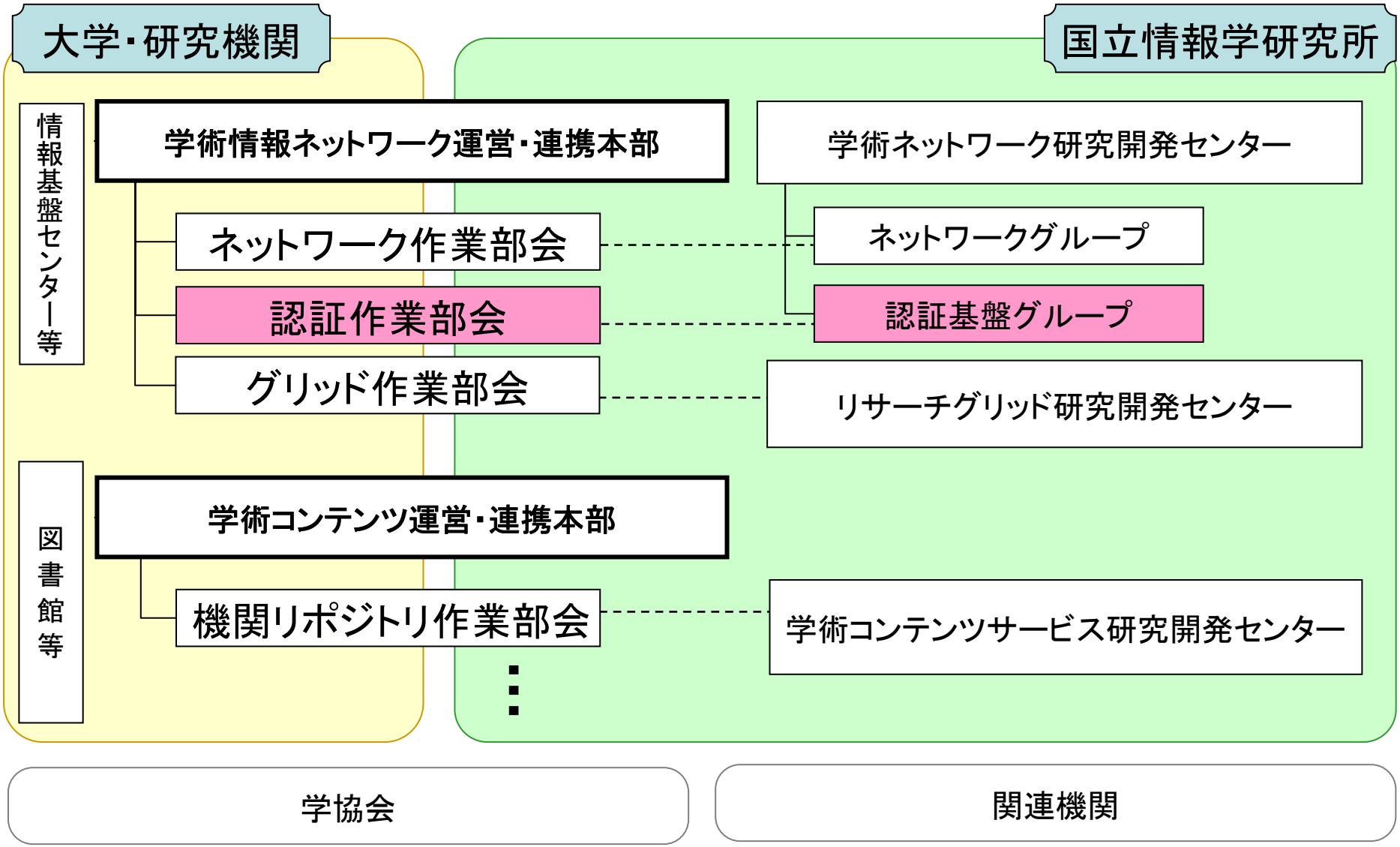
NII 学術基盤推進部 基盤企画課

を代表して

学術情報ネットワーク運営・連携本部
認証作業部会

- 岡部　寿男（京都大学学術情報メディアセンター）主査
- **曽根原　登（国立情報学研究所）幹事**
- 高井　昌彰（北海道大学情報基盤センター）
- 曽根　秀昭（東北大学情報シナジーセンター）
- **佐藤　周行（東京大学情報基盤センター）**
- 平野　　靖（名古屋大学情報連携基盤センター）
- 馬場　健一（大阪大学サイバーメディアセンター）
- 鈴木　孝彦（九州大学情報基盤研究開発センター）
- 飯田　勝吉（東京工業大学学術国際情報センター）
- 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）

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

学術ネットワーク研究開発センター
認証基盤グループ

- 曽根原　登　　教授（情報社会相関研究系 研究主幹）…… 主査
- 岡部　寿男　　客員教授（京都大学教授） …… 副主査
- 中村　素典　　特任教授（学術ネットワーク研究開発センター）
- 谷本　茂明　　客員教授（学術ネットワーク研究開発センター）
- 岡田　仁志　　准教授（情報社会相関研究系）
- 山地　一禎　　特任准教授（学術ネットワーク研究開発センター）
- 島岡　政基　　特任准教授（学術ネットワーク研究開発センター）
- 片岡　俊幸　　特任准教授（学術ネットワーク研究開発センター）
- 鷲崎　弘宣　　助教（アーキテクチャ科学研究系）
- 鈴木　新一　　基盤企画課長
- 樋口　秀樹　　基盤企画課専門員
- 小松　陽一　　基盤企画課係長（連携システムチーム）

学術の情報力・研究力・文化力

- 30年前は、大型計算機、大型実験設備の保有が情報力・研究力・文化力の差に
- 10年前は、インターネットが情報力・研究力・文化力の差に
- 5年前ころから、コンテンツ発信・探索が情報力・研究力・文化力の差に
- これからは、フェデレーション・コラボレーション・コミュニティのための認証・認可基盤の保有が情報力・研究力・文化力の差に

情報リテラシー啓蒙という側面

- 認証やPKIは、素人であってもある程度仕組みを理解しておかないと、
  - フィッシングなどの詐欺にだまされたり、
  - セキュリティ上の懸念をネタに不必要に高い商品を売りつけられたり、
- ということもあるので、学術での啓発活動という側面もあわせもつ。
- その例題としてサーバ証明書をUPKIとして取り組んでいるという側面もある

学術認証基盤グランドチャレンジ（研究開発の対象として進める）

- 学術研究と高等教育の**質の向上**、学術情報**資源の価値を高める**ために
- 研究と教育の**利便性・効率性**と学術情報資源の**安全性**の**両立**という互いに矛盾する難しい課題を解決する
- そのため、情報セキュリティ技術、管理・運営システム、情報セキュリティ遵守などの社会制度等を緻密に強く連携させた**総合的研究開発**を７大学とNIIで進める

学術情報基盤を取り巻く課題

1. 学術無窮
   - 人材育成（教育）、科学技術（研究）、**地域社会の知的情報集積（社会情報基盤）**としての役割

2. 学術連携（ICT国際競争力強化）
   - 少子高齢化社会の到来、死の谷（研究と実用化）克服、産学連携の新たな仕組みを模索
   - **イノベーションダイナミクスの創出**

3. 学術経営（国立大学法人）
   - 法人化後の社会規範・法制度への対応、学問の自由と社会的責任のバランス、**経営効率の改善**

学術の情報社会基盤化の課題

1. 外国人学生、社会人学生、シニア学生が増加
   - 年齢、専門、分野、経験を超えた自己実現欲求の増大
   - 社会人・市民学生の通学時間の負担

2. 学術資源の継承と地域社会・産業還元できる仕組
   - 文化遺産から産業資産へ
   - 地域の情報集積と世界への情報発信

3. ICTを活用した学術・社会知的情報基盤
   - 自宅、職場、公共設備などから学術参加

Cyber Science Infrastructure (= e-Science) の目的

1. 学術ネットワークの強化・国際化
2. 学術資源 (コンテンツ、データベース)の体系化・整備
3. Naregi, UPKI連携ミドル研究開発
4. 具体的な産学連携施策の推進
5. 大学の社会情報基盤化の促進(知の泉)

最先端学術情報基盤（CSI）の構築に向けて

産業・社会貢献

国際貢献・連携

サイバー・サイエンス・インフラストラクチャ（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

学術コンテンツの確保・発信システム

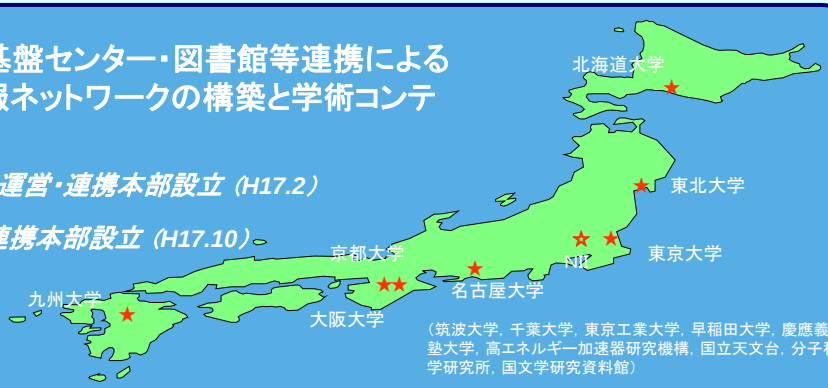
連携ソフトウェアとしての研究グリッドの実用展開

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・図書館等連携による次世代学術情報ネットワークの構築と学術コンテンツ整備

学術情報ネットワーク運営・連携本部設立（H17.2）

学術コンテンツ運営・連携本部設立（H17.10）



（筑波大学，千葉大学，東京工業大学，早稲田大学，慶應義塾大学，高エネルギー加速器研究機構，国立天文台，分子科学研究所，国文学研究資料館）

大学・研究機関の研究リソース整備・研究成果等の発信

中長期計画

- Sinet 3 、学術コンテンツ配信は運用事業フェーズ
- Naregi、UPKI は研究開発フェーズ（本格運用を目指す）
- 大学連携による社会と産学連携、イノベーションダイナミクスの創出を狙う

連携(Federation)がキーワード

1. 学術基盤連携(科学技術の進展)
   - ドライ系　ネットワーク・コンテンツ・コンピュータ・データベース
   - ウエット系　信頼関係など

2. 高等教育連携(分野と専門を超えた交流)
   - ICT人材育成、トップSE、単位互換、研究倫理など

3. R&D連携(イノベーションダイナミクスの創出)
   - 産学共同研究開発、学術知財管理など

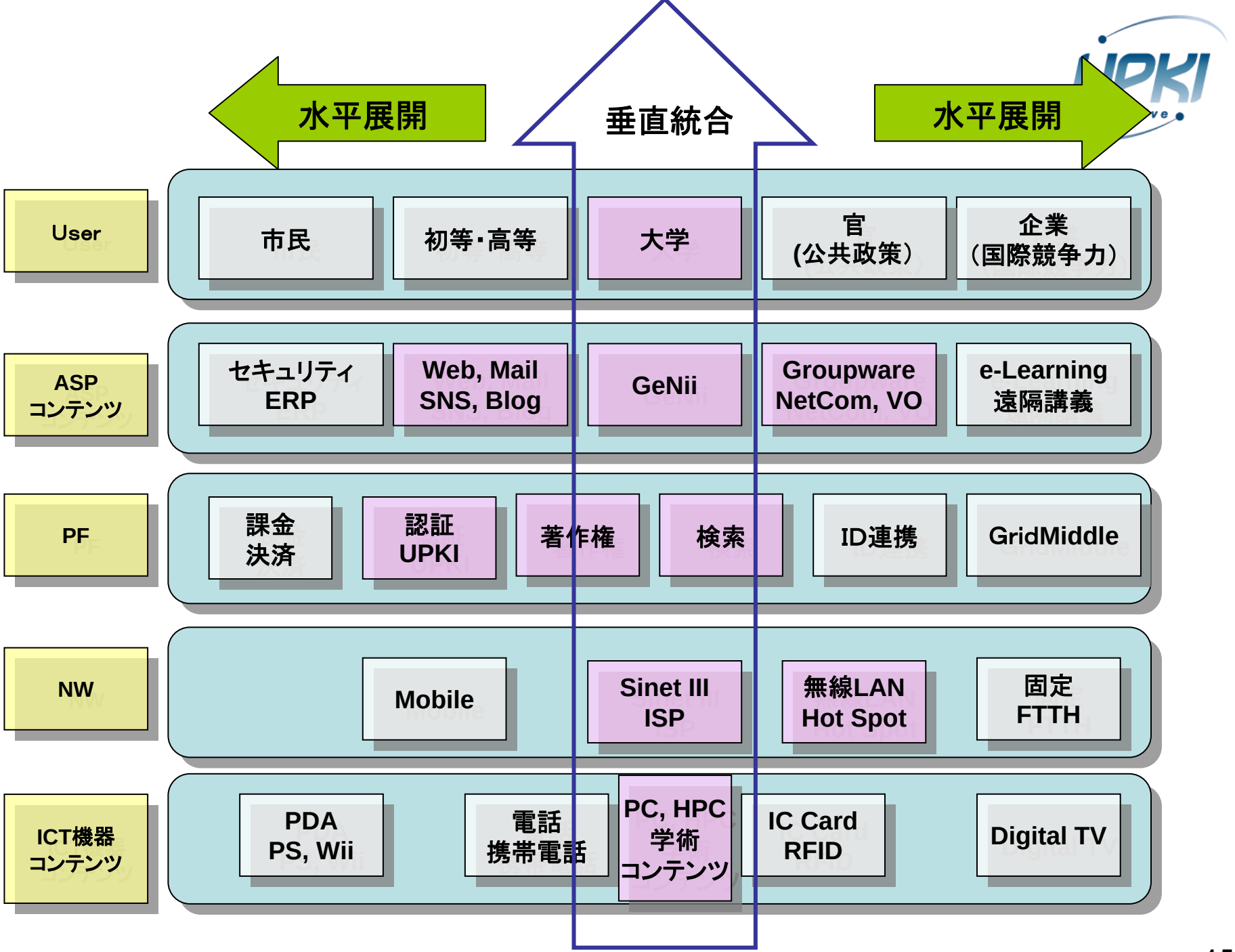
4. 社会連携(学術から知流社会への転換)
   - 大学の情報社会基盤
   - 市民講座、生涯学習、公共スペース活用など

学術サービスをより便利で
使いやすいものに、そして安全に
（企業経験からの提言）

1. 学術データセンタADC
   - Sinet　III、GeNii、Naregi、UPKIを活用し、学術Web、Mail、DBなどをHosting / Housingするデータセンター

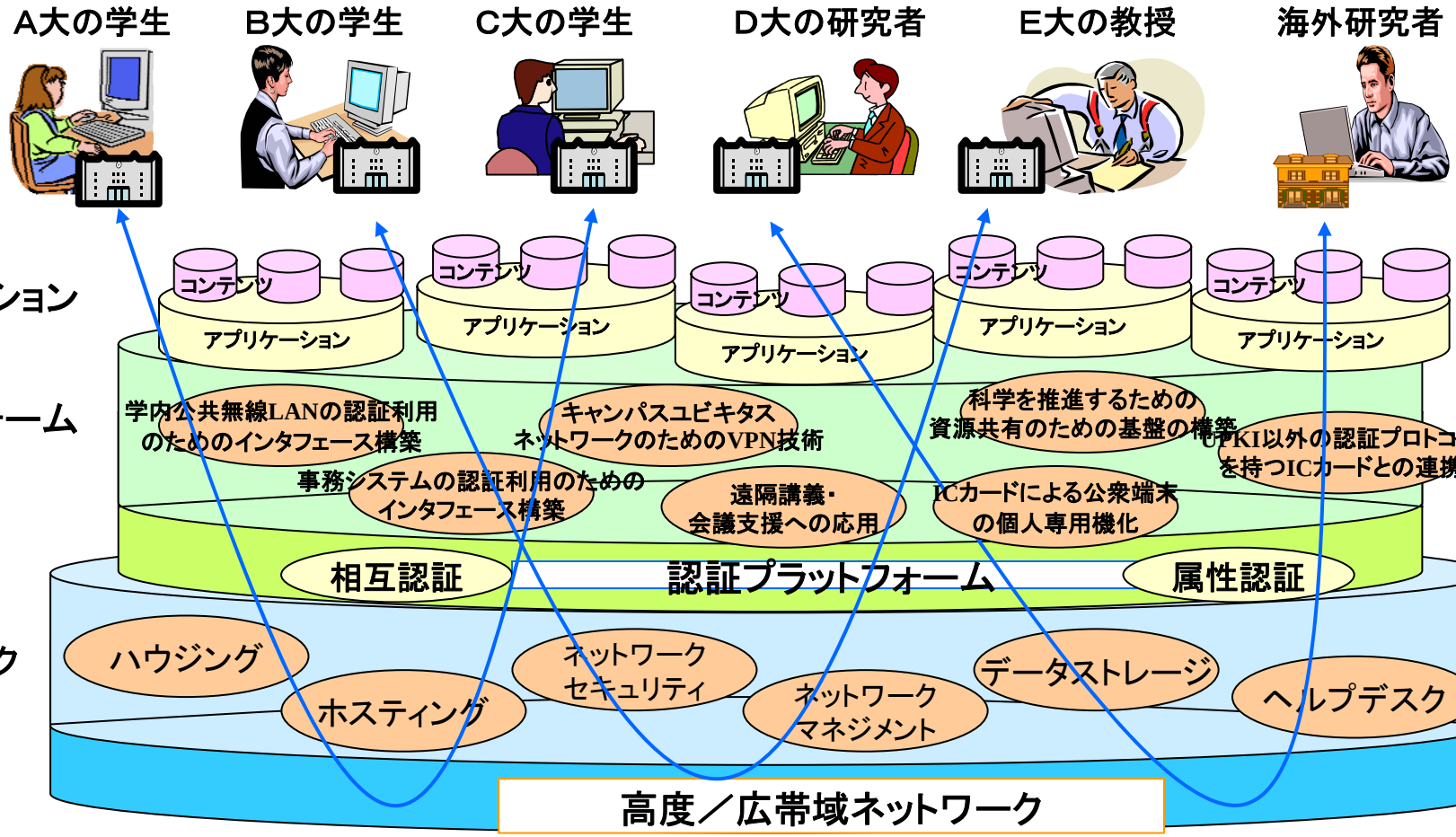
2. 学術サービス・プロバイダAASP
   - e-Learning、遠隔講義、情報セキュリティ、JSOXなどの学術ASP（Application Service Provider）サービス

3. 大学共同ARPサービス
   - 学術経営の効率化
   - 研究と教育の質の向上、学術資源運用企画、持続的運用モデルなど


水平展開
垂直統合
水平展開
User
市民
初等・高等
大学
官
(公共政策)
企業
(国際競争力)
ASP
コンテンツ
セキュリティ
ERP
Web, Mail
SNS, Blog
GeNii
Groupware
NetCom, VO
e-Learning
遠隔講義
PF
課金
決済
認証
UPKI
著作権
検索
ID連携
GridMiddle
NW
Mobile
Sinet III
ISP
無線LAN
Hot Spot
固定
FTTH
ICT機器
コンテンツ
PDA
PS, Wii
電話
携帯電話
PC, HPC
学術
コンテンツ
IC Card
RFID
Digital TV

7大学とNIIの連携による認証基盤の形成

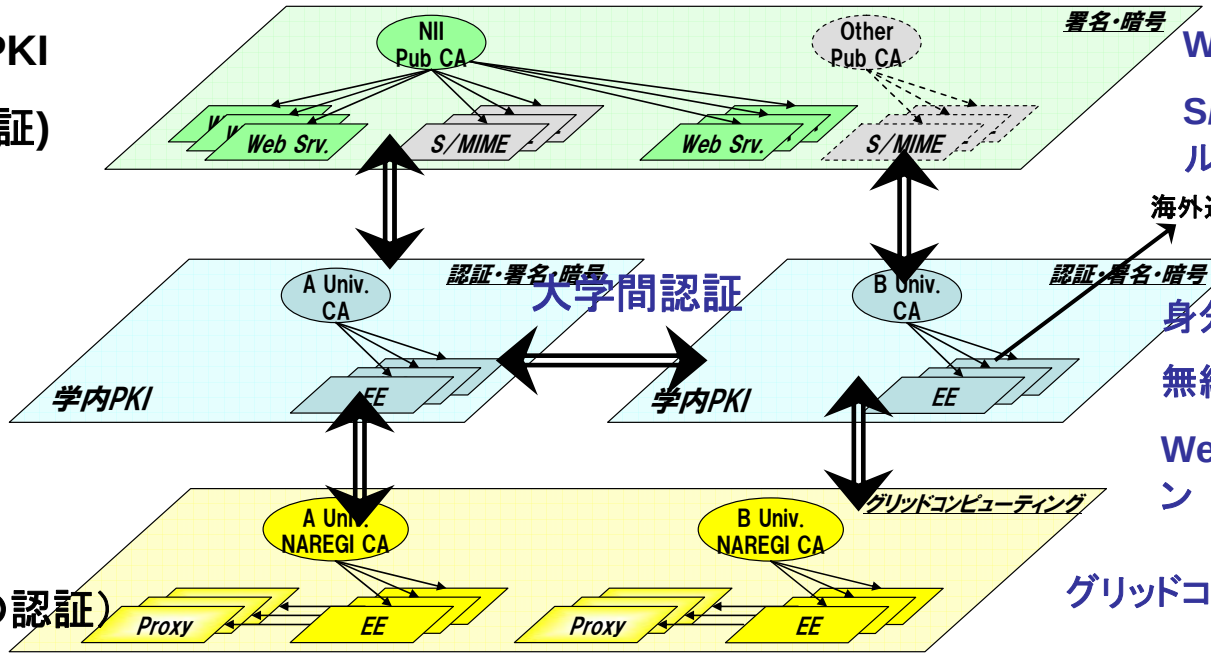
全国共同電子認証基盤を構築し、大学の先生、研究者、学生、事務職員が、連携している大学のネットワークに自由に入れるようにする。更に共通プラットフォーム上で利用できる機能を活用することで、利便性の向上を図る。 2006年スタート



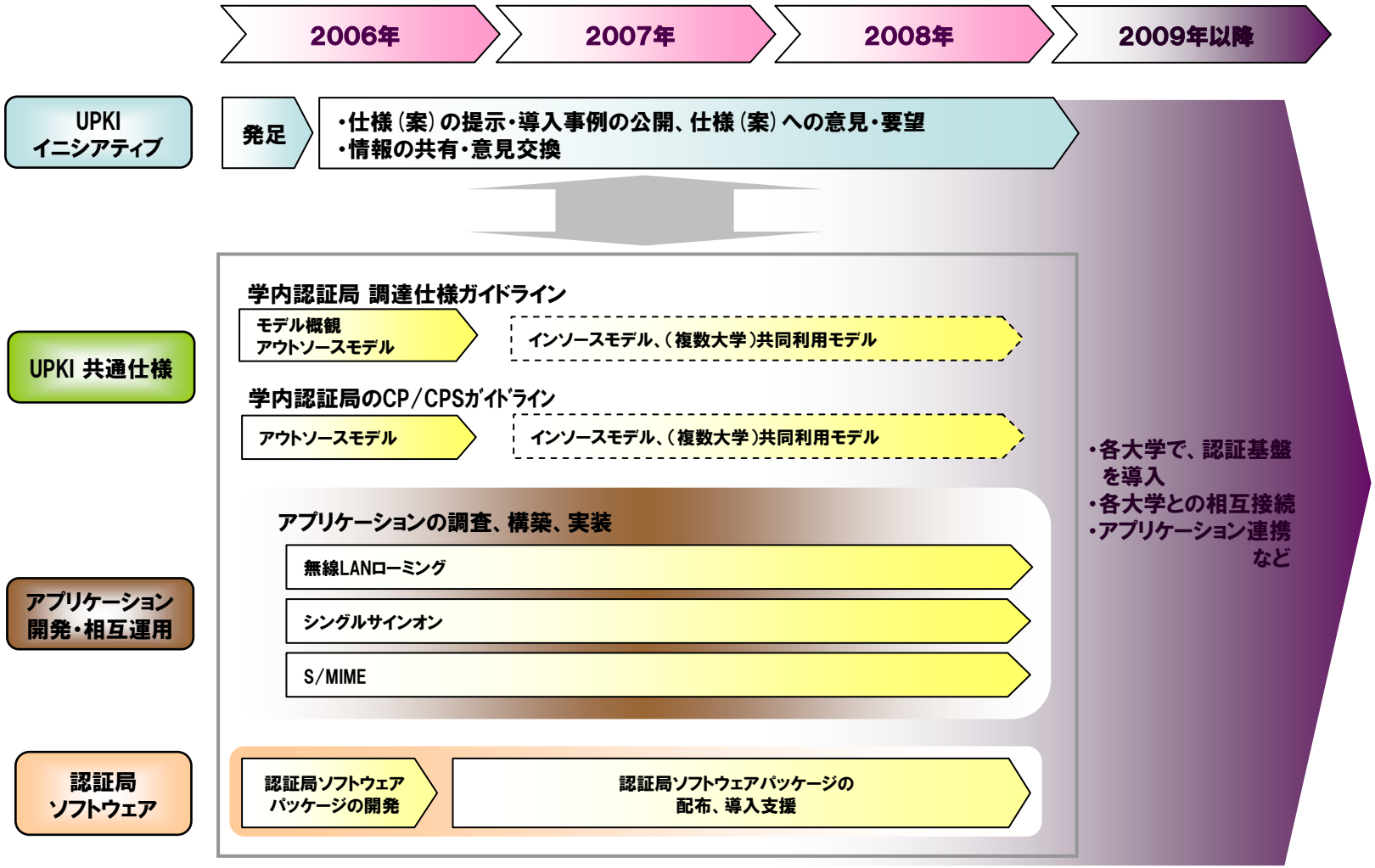
セキュリティを確保した連携を行うには、個人を認識するための認証機能は不可欠

UPKIの基本アーキテクチャ

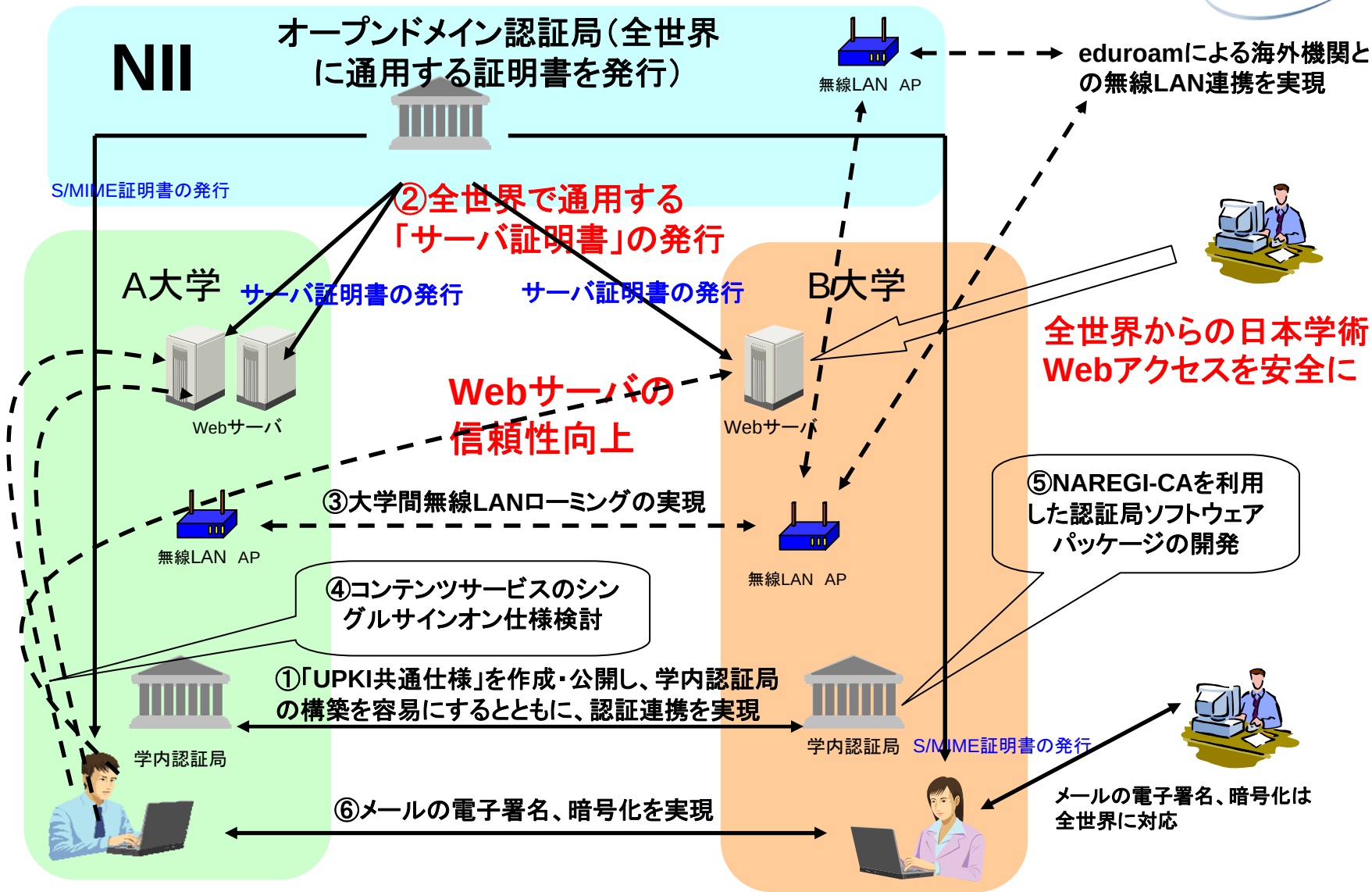
- 3階層のPKI（Public Key Infrastructure）による役割分担と連携



UPKI構築の全体スケジュール

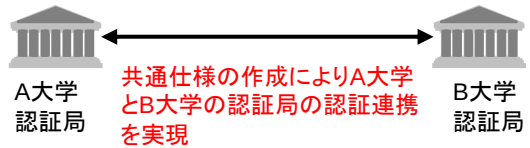
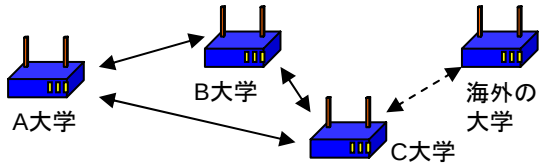
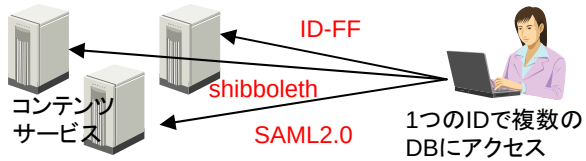
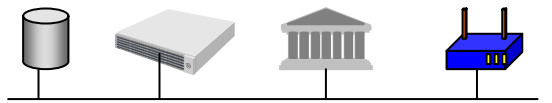
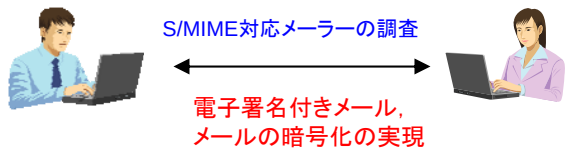


UPKIで開発中のアプリケーション等



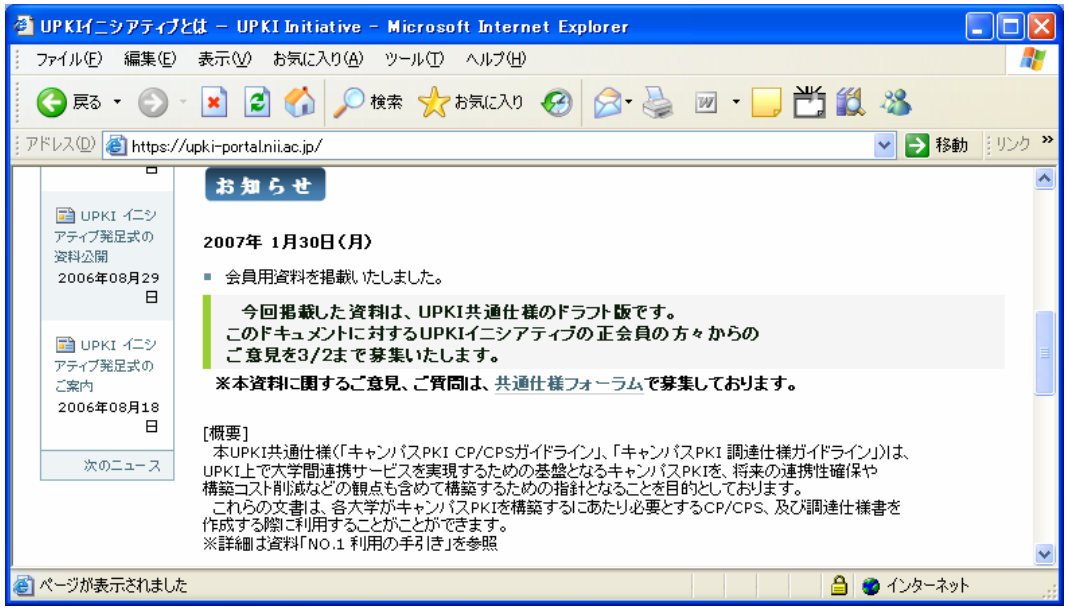
平成18年度は①～⑥の6項目について実施した

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（東北大学が中心：今井、後藤、曽根）	 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仕様検討	 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

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



これまでのUPKIイニシアティブの活動

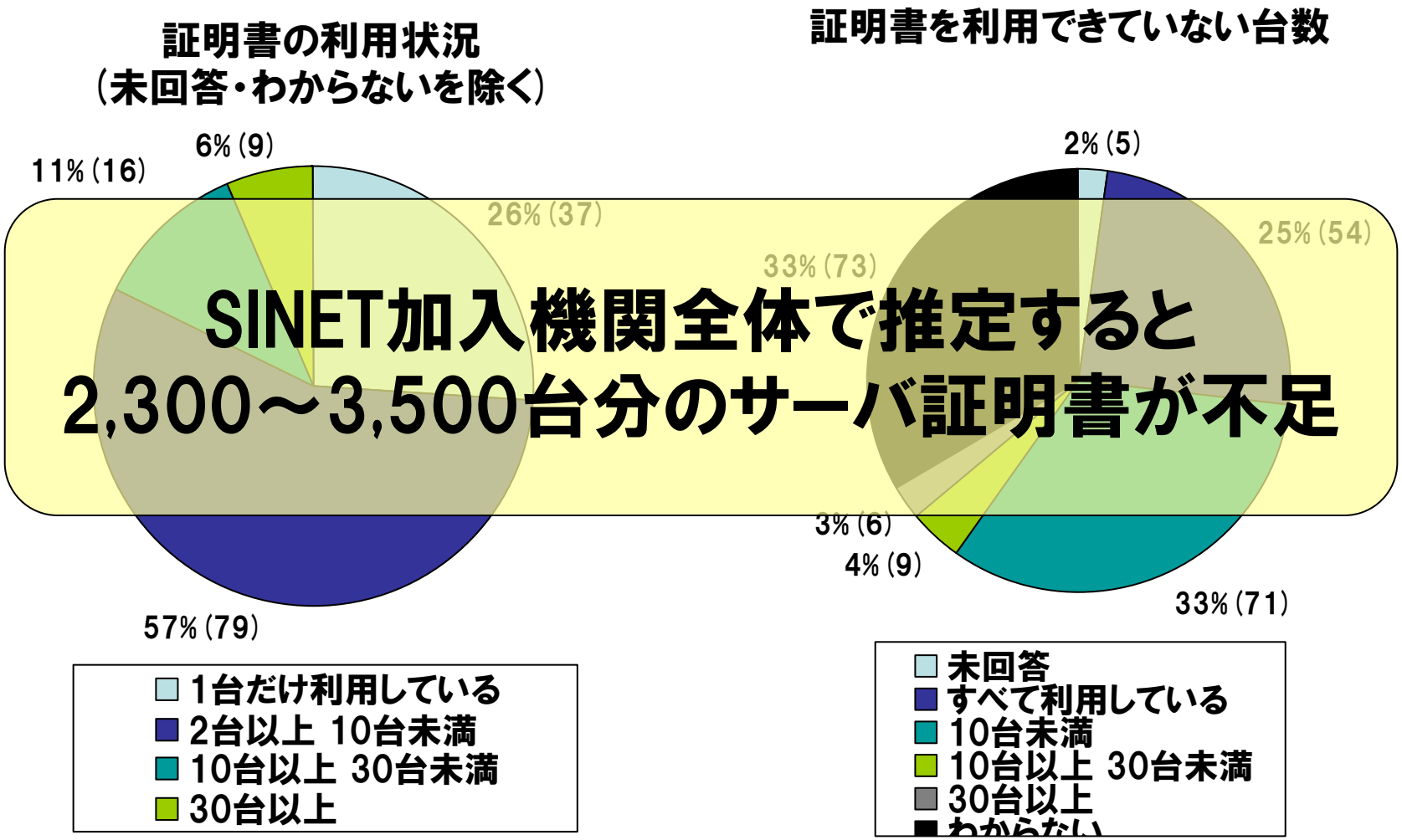
- メールマガジンの発行
  - イベント情報等これまで4回発行
- 各種研究会等の共催
  - ITRC研究会のキャンパス無線LANセッションなど
- 資料の公開(一般公開および会員限定公開)
  - UPKIシンポジウム(2006年2月開催)
  - CSI委託事業報告交流会(2006年5月開催)
  - インターネットアーキテクチャ研究会(2006年6月開催)
  - シンポジウム「最先端学術情報基盤(CSI)構築に向けて(2006年6月開催)
  - ITRC研究会資料(キャンパス無線LAN)(2006年10月開催)
  - その他認証関連のドキュメント多数掲載
- フォーラムでのパブリックコメント募集の実施
  - UPKI共通仕様に対するパブコメ(2007年1月)

会員募集中です！ 皆様の参加をお待ちしております。

社会要請に応える事業
各大学の予想以上に強い期待

1. オープンドメインPKI層
   - サーバ証明書発行サービス
   - S/MIMEクライアント証明書発行サービス
   - キャンパスPKI層とShibbolethによる認証連携
2. キャンパスPKI層
   - 各大学がキャンパスPKIを構築
   - 各大学がアイデンティティプロバイダ (IdP)
   - NIIがコンテンツのサービスプロバイダ(SP)として認証連携
3. グリッドPKI層
   - 京速コンピュータ時代の全国共同利用スパコンサービスを、NAREGIミドルウェアと各大学のグリッド用PKIとを使ってつなぐサービス
   - NIIはGOC (Grid Operation Center) としてAPGrid認定の国際連携グリッド用認証局を運用

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

プロジェクトの概要

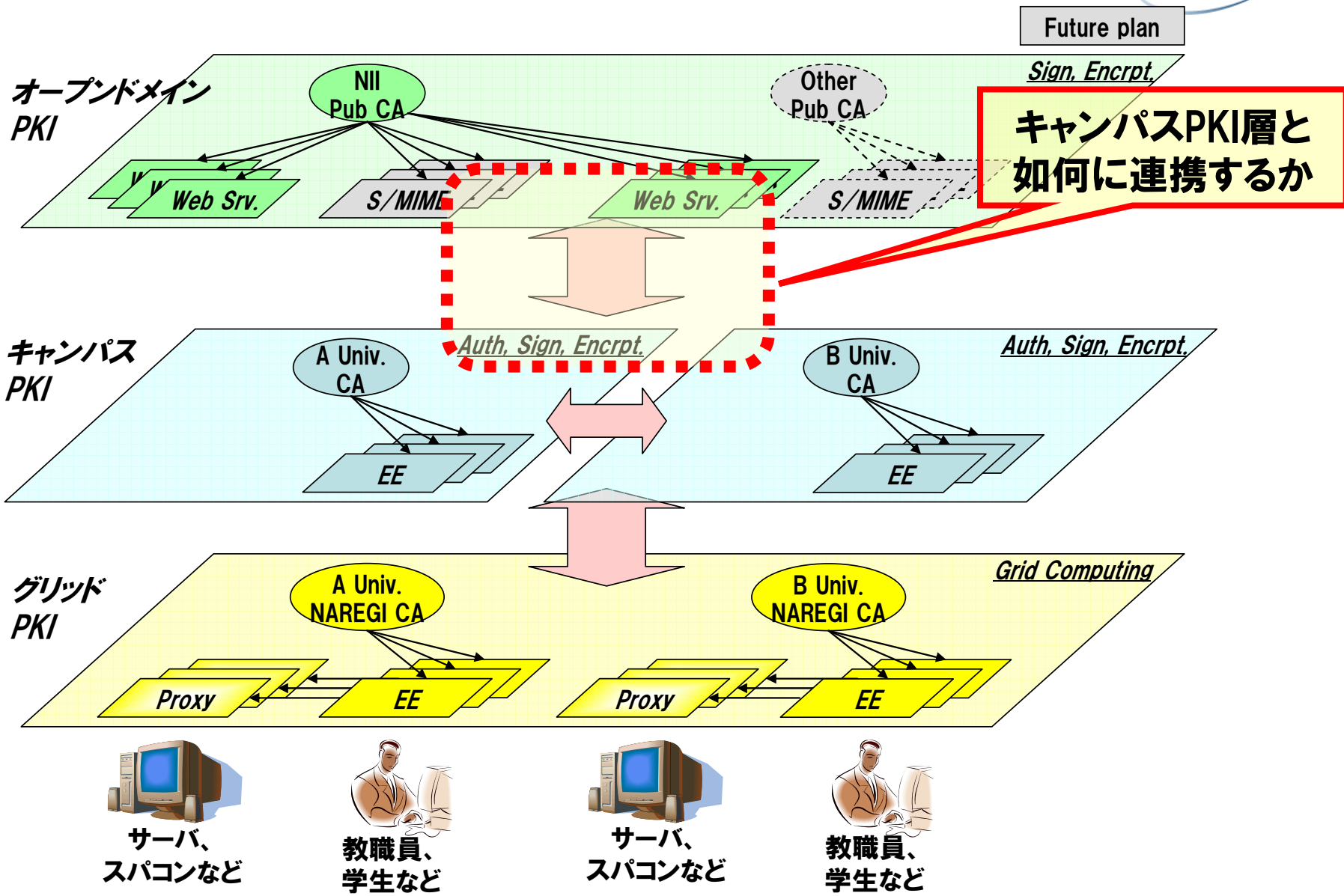
- 目的
  - 大学等のサーバ証明書の普及を推進
  - 認証局を用いた研究開発 ⇒ 登録発行業務の改善
  - 学術機関のWebサーバ信頼性向上
  - サーバ証明書の導入・運用ノウハウの共有
  - 参加者のサーバに対してのサーバ証明書無償配布
- 期間
  - 2007/04/01～2009/03/31
- ゴール
  - H19年度: サーバ証明書の普及が進まない理由・課題の整理
  - H20年度: サーバ証明書の普及促進の仮説・立証
  - 将来的に: キャンパスPKI層を活用した証明書発行業務の自動化
- 主な作業
  - プロジェクト参加機関の募集
  - 各登録担当者へのS/MIME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

UPKIにおける位置づけ(ゴール)



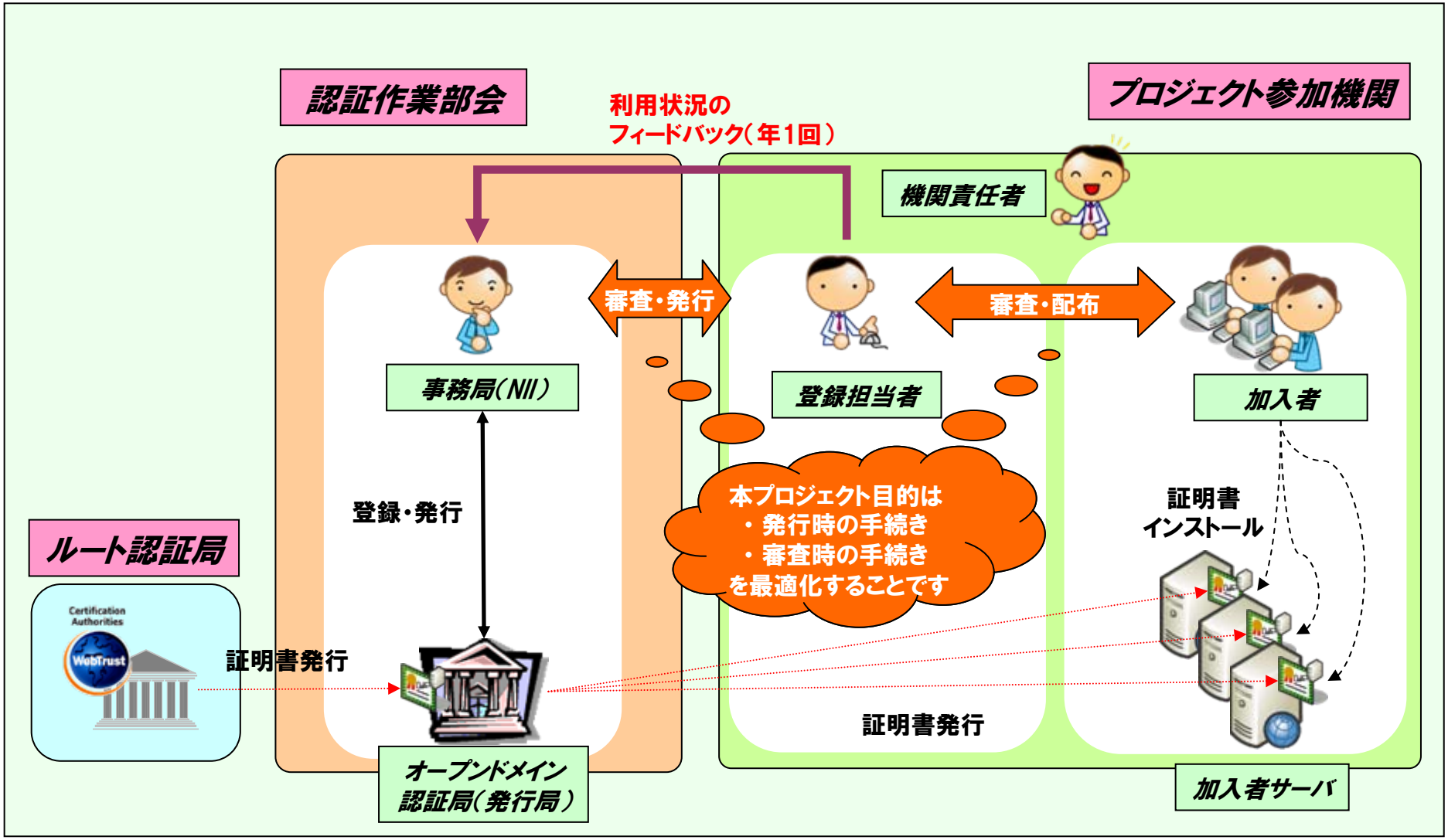
証明書発行の基本方針

- 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

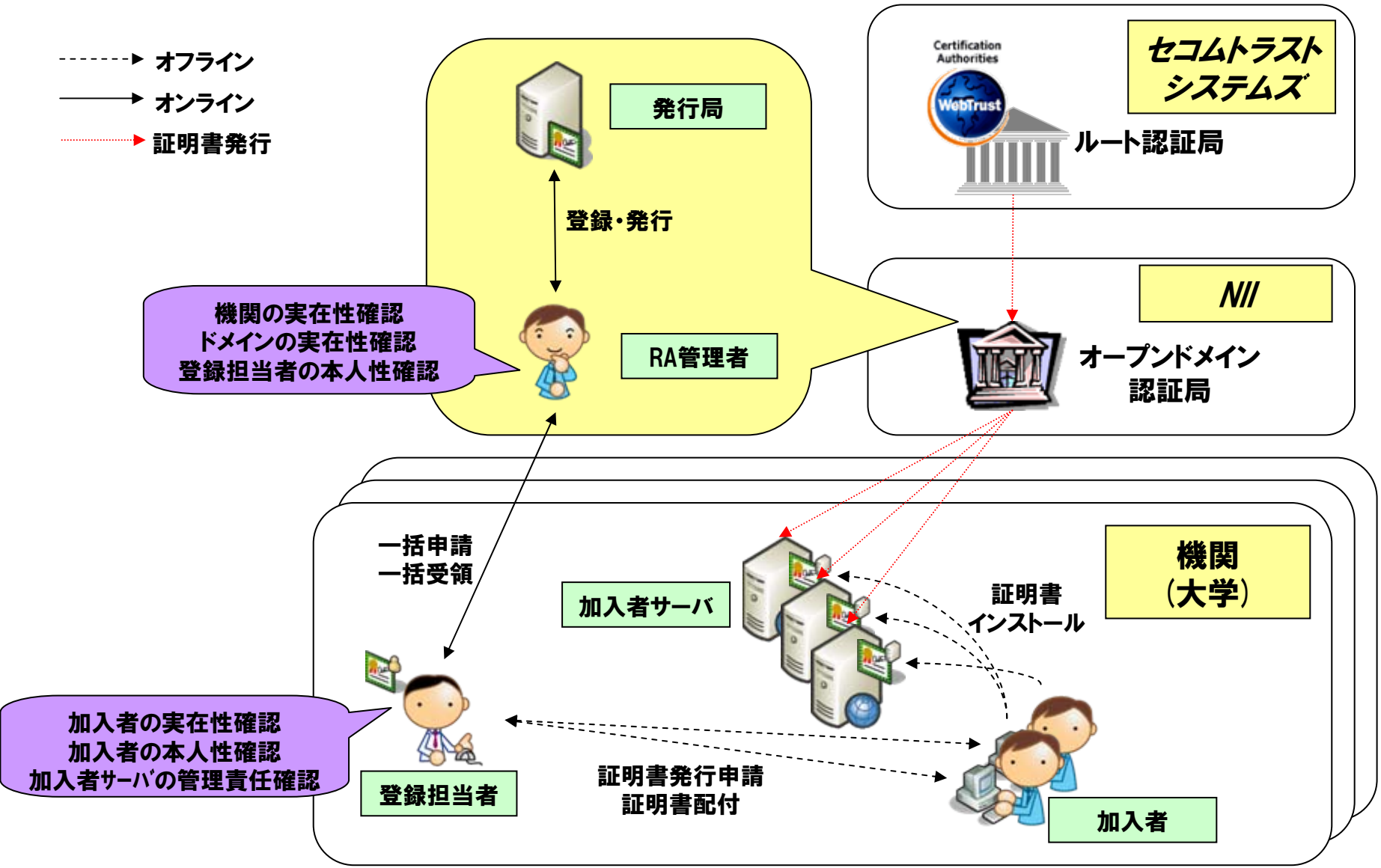
プロジェクトで利用する用語と役割

組　織	用語	説　明
NII	オープンドメイン認証局（発行局）	本プロジェクトで使用する，サーバ証明書を発行するための認証局。Web Trust for CAに準拠しており，世界的に信頼できる証明書の発行が可能です。また，この証明書は，主要なウェブブラウザ等のPKIアプリケーションに標準でルート認証局が搭載されているため、商用のサーバ証明書と同様に利用することができます。
	事務局	プロジェクト参加申請、証明書発行申請にあたり、審査業務を行なうNIIの事務窓口です。
各大学	機関責任者	本プロジェクト参加にあたり，各機関で選出いただく代表者の方。課長職相当または准教授以上の方にお願いいたします。
	登録担当者	本プロジェクトの参加機関側の事務的な窓口をお願いする方。大学の規模に応じて複数名選出していただくことが可能です。
	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される方。プロジェクト参加機関内の教職員の方であれば，どなたでも加入者となれます。
	加入者サーバ	加入者の方が管理するWebサーバ。
不特定多数	利用者	PKI加入者サーバにアクセスする，不特定多数の方々のことを，この説明では利用者と呼びます。利用者は、ウェブブラウザ等の標準の機能を利用して加入者サーバの証明書を検証いたします。

プロジェクト全体概要


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
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

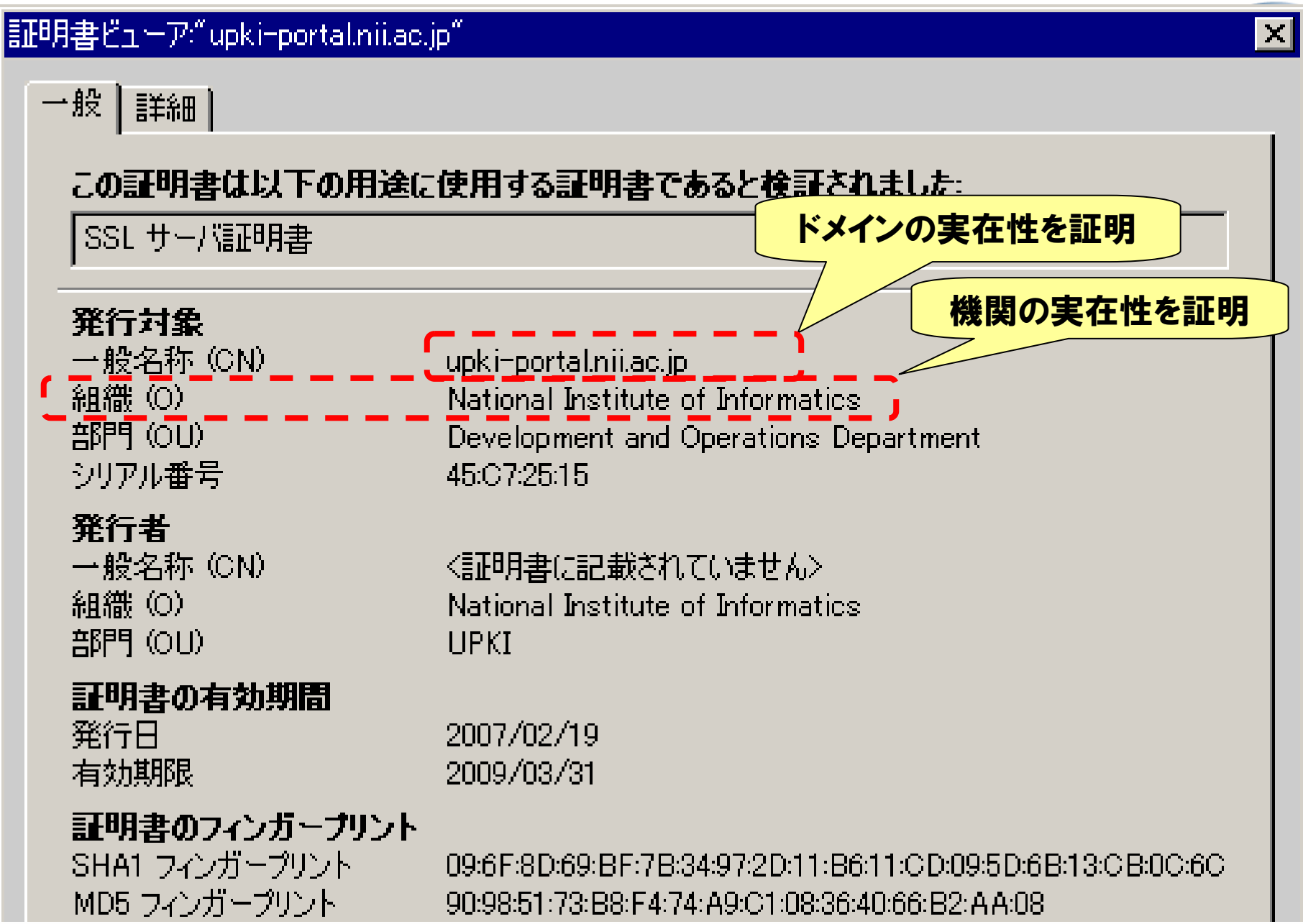
証明書発行の流れ


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
Certification Authorities
WebTrust
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
加入者サーバ
証明書
インストール
機関
（大学）
加入者の実在性確認
加入者の本人性確認
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

商用証明書との比較
～審査項目の違い～

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 Department
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

動作確認済みWebサーバ

- Apache(mod_ssl) ※注1)
- Apache-SSL ※注1)
- Microsoft Internet Information Server 5.0
- Microsoft Internet Information Server 6.0
- IBM HTTP Server 6.0.2 以上
- Jakarta Tomcat ※注2)

※注1)Apacheバージョンについて

Apache(mod_ssl-2.8.25-1.3.34)、apache_1.3.33+ssl_1.55より動作確認を行っています。

古いバージョンにつきましては、深刻な脆弱性が報告されていますので、最新版をご使用いただくことをお勧めいたします。

※注2)Jakarta Tomcatについて

Jakarta Tomcat 4.1.31 と Jakarta Tomcat 5.0.30につきましての動作確認を行っています。

推奨ブラウザ

- Netscape Communicator 4.78 以上
- Netscape Communicator 7 以上
- Microsoft Internet Explorer 5.5 以上
- Microsoft Internet Explorer 5.2 (MacOS) 以上
- Opera 7.6 以上
- FireFox 1.0 以上
- Safari 1.2.2 以上

※SafariはMacのOS X以上に標準搭載されているブラウザ。OS X以前は、
IEなどの利用になります。

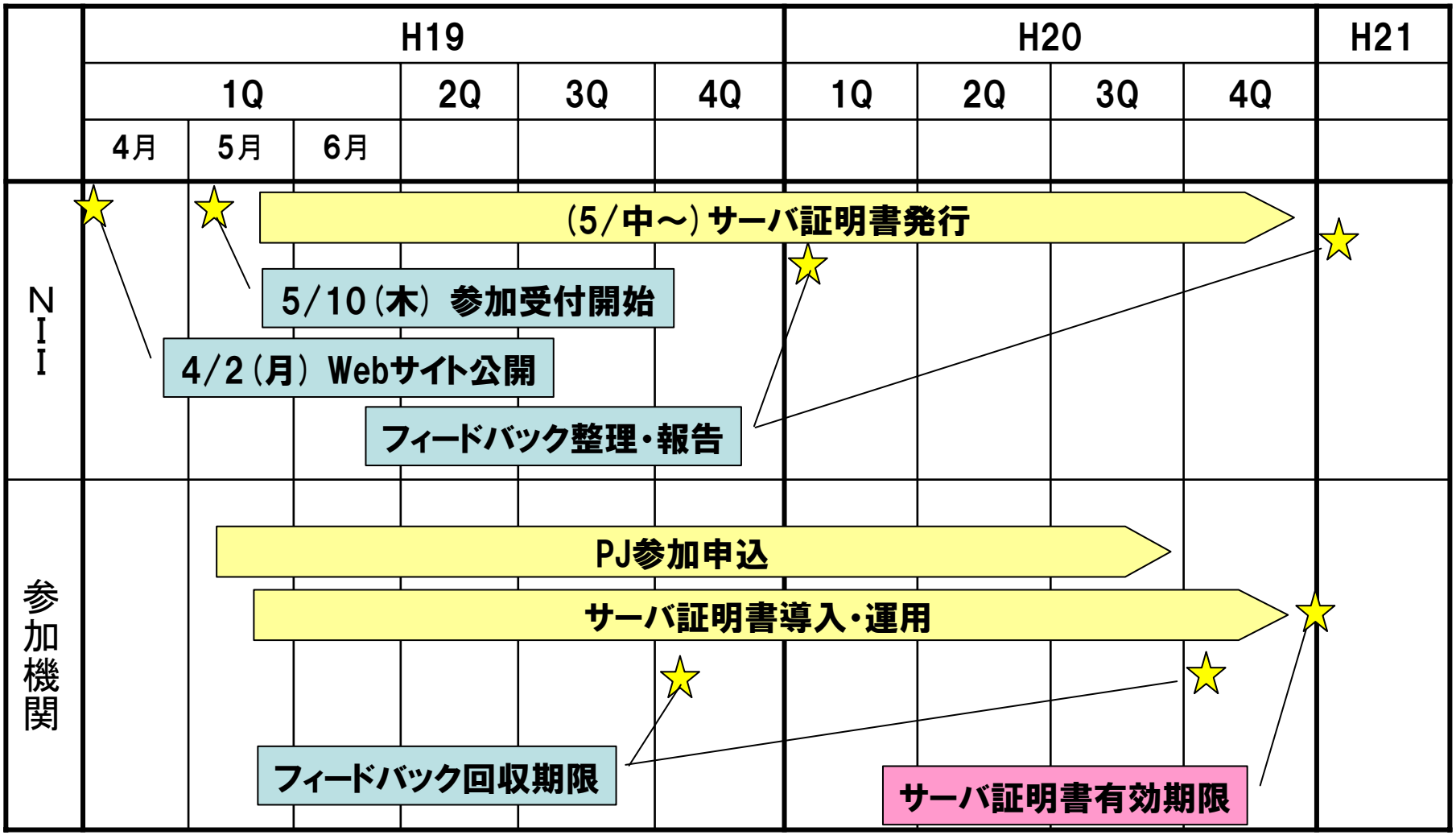
プロジェクトへの参加条件

- 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
    - その他の独立行政法人等
- 参加単位
  - 機関毎に参加申し込みを行う。
    - 異なるドメインを用いる場合には、別途相談。
  - H19年度当初は、審査処理等の都合により、受付機関数に制限あり
- 条件
  - PJ趣旨に賛同し、証明書利用結果についてのフィードバックを行うこと。
  - 証明書申請について責任を全うできること。
    - 加入者の本人性確認、実在性確認、加入者サーバの管理責任確認
    - 申請書類の保管
  - 登録担当者が以下の環境を利用できること。
    - S/MIMEメーラ（申請ファイル送信時のデジタル署名）
    - Office XP以降のExcel（申請ファイルへのデジタル署名）

サーバ証明書の発行条件

- 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
- 注意
  - 次のようなケースは対象外
    - 特定少数の検証者のみを対象としたサーバ
    - 検証者へのルートCA証明書の配布が容易に実現できる場合

プロジェクトスケジュール



まとめにかえて

- 大学の研究力・情報力・文化力の強化に
- 大学共同利用機関の事業化戦略として
- 学術サービスプロバイダー（Academic Service Provider）を目指す

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

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

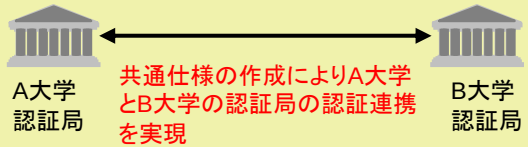
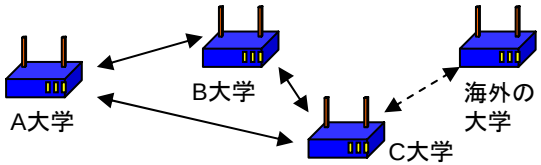
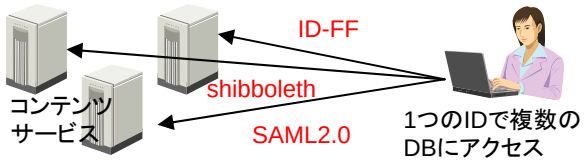
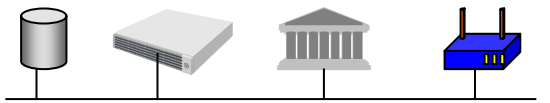
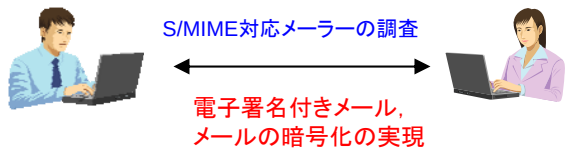
国際貢献・連携

認証基盤による付加価値
学術サービスプロバイダーを目指す

- 認証のない学術ネットワークサービス、認証のない学術コンテンツサービスは？
- SINETの「セキュリティ強化」の具体的サービスとして、SINET加入機関に対するサーバ証明書の発行という付加価値サービスの提供を試みる
- SINET加入とサービス提供によってNIIと大学の協力・信頼関係を構築

ありがとうございました

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仕様検討	 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

UPKI共通仕様の制定

- 大学間連携の必要性
  - リソース共有、コンテンツ共有
    - グリッド、電子図書館、e-learning、…
  - 学生・教員の流動化への対応：
    - 単位互換、共同研究、非常勤・客員の扱いなど
- 情報セキュリティ対策
  - セキュリティレベルの向上
    - ポリシー・実施手順の見直しとの連動
  - 導入・開発コストの削減
- 産学連携、地域連携、…への展開
  - 国際標準への対応、標準化への貢献
  - 学術以外の様々な認証基盤との連携
    - オープンドメインPKI、GPKI関係、海外PKIなど

少子化と全入時代
大学の財政基盤（1%シーリング）

『政府機関の情報セキュリティのための統一基準』への対応
大学によって異なるセキュリティポリシ

企業と大学との組織間連携強化
地域連携、知的クラスタの促進

キャンパスPKI共通仕様・相互運用仕様

社会要請を背景に、「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、**大学へのキャンパスPKI導入を促進する**とともにPKI導入に対する将来の**連携性確保***や**コスト削減****等を狙いとするものである。

＊：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

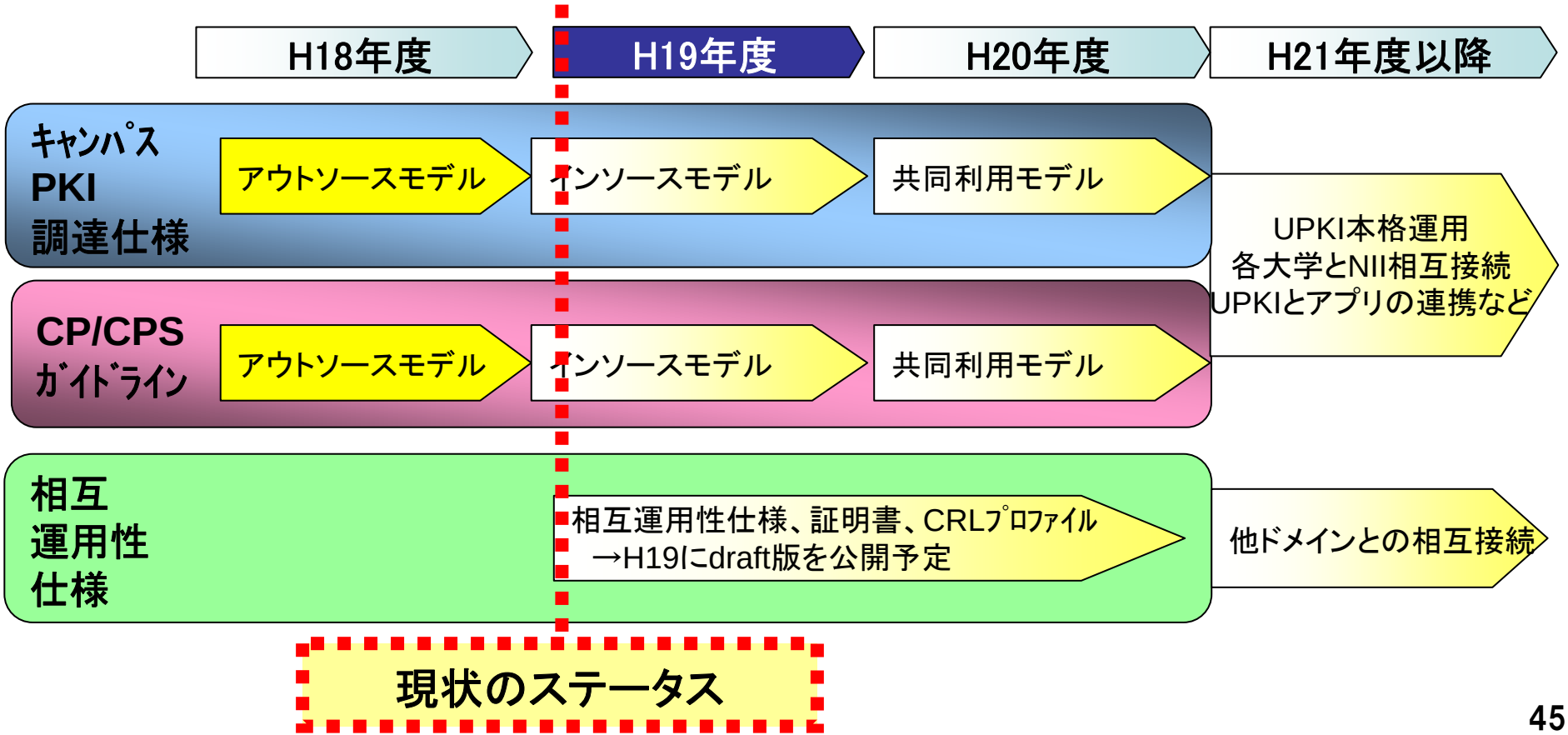
＊＊：コスト削減
- キャンパスPKI導入検討コストの削減
- CP/CPS策定コストの削減

ガイドライン公開により
キャンパスPKI導入を促進！！

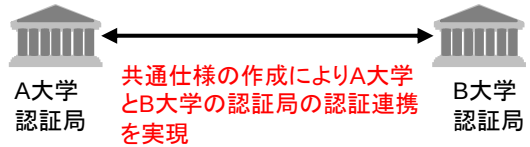
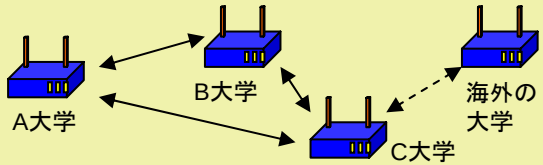
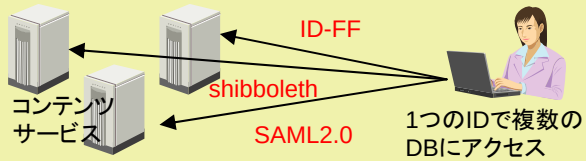
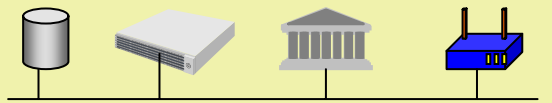
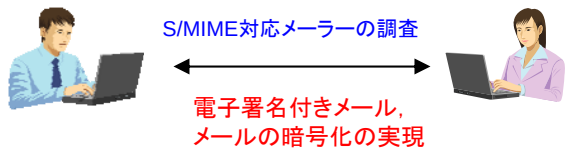
スケジュール

- 段階的に展開（3年計画）
  - H18年度：キャンパスPKI共通仕様（アウトソースモデル）を作成し、UPKIイニシアティブ*で公開中（H18年度成果）
  - H19年度以降、順次モデルの拡充とともに相互運用性仕様を作成

＊：https://upki-portal.nii.ac.jp/item/idata/odatao/CampusPKI/



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仕様検討	 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

UPKI認可フェデレーション方式の研究開発

- UPKI AAI(認証認可基盤)の構築
  - 大学の共通電子認証基盤上で様々なアプリケーションを利用するためには、認証と共に認可を連携することが必要。
  - 大学間連携や、産学連携では、提供するサービス(ポータル、学術DB等)個々にID管理を行っており、管理工数が増加。
  - ID管理を行わず、サイトで管理しているサービスでは、学外からのアクセスができず、外出時、出張時に研究業務の遂行が阻害。
  - 海外(特に欧米)では、Shibbolethを利用したフェデレーションが数多く運用開始されており、Science Direct等の大手サービスプロバイダーや、EGEE、TeraGrid等の大手グリッド・サービスで利用開始。

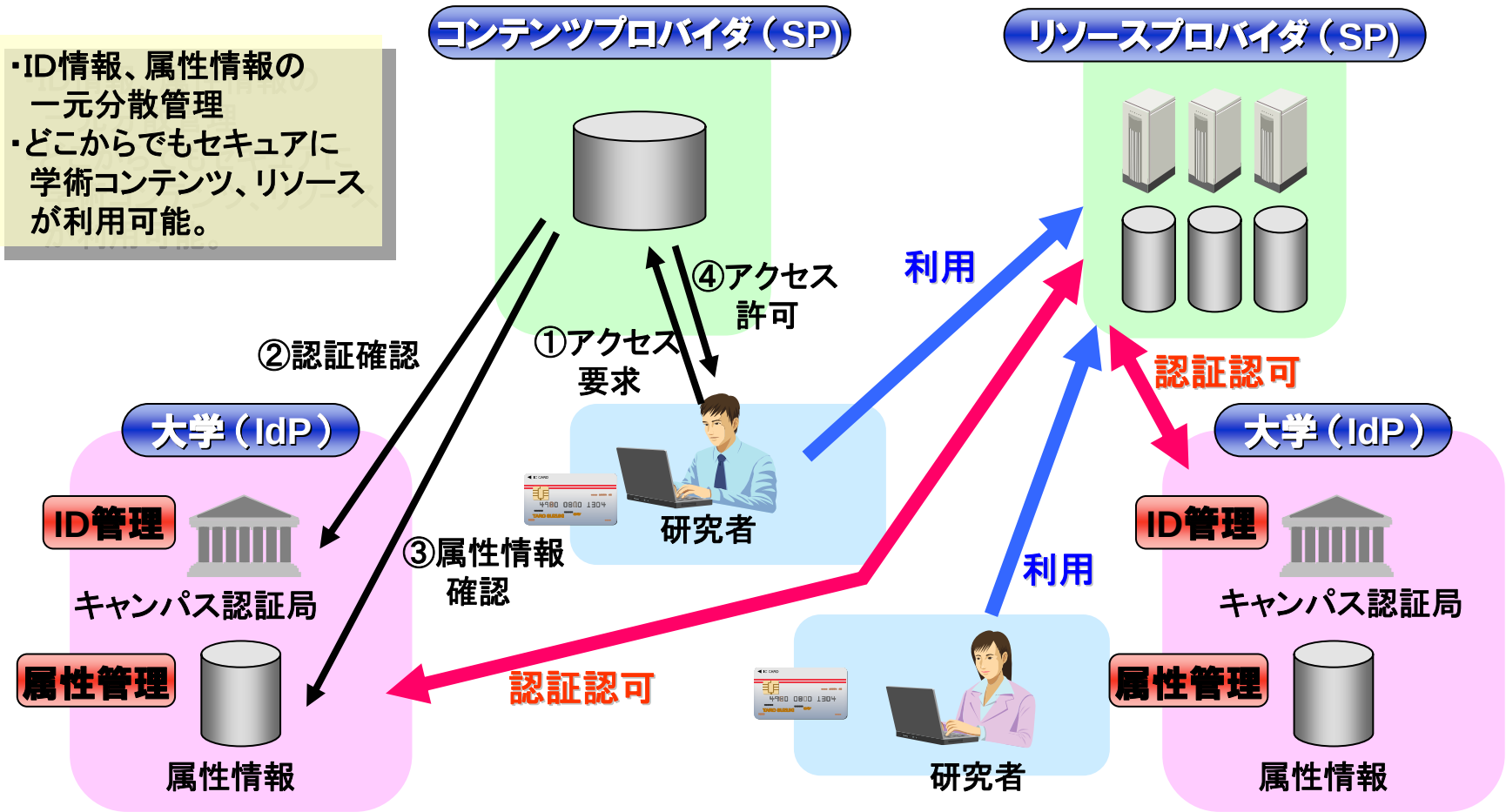
UPKI認可フェデレーション方式の研究開発

- UPKI認可フェデレーションの効果
  - UPKIのキャンパス認証局による認証を基本に、この上で認可連携を行うための大学IdPの方式を検討。
  - フェデレーションにより、大学連携における高いセキュリティを確保したアクセシビリティの向上と、連携する組織全体のID管理工数の削減。
  - システム構築だけではなく、フェデレーション機構のポリシーや契約を含む効率的な運用方式。
  - 学術コンテンツ流通、無線LAN認証連携やグリッド・アクセス等の幅広いサービスへの対応を目指す。

UPKI AAI構想

UPKIフェデレーション

- ID情報、属性情報の一元分散管理
- どこからでもセキュアに学術コンテンツ、リソースが利用可能。



今後のスケジュール

- H19年度：
  - スモールスタートによる、フェデレーション機構の運用方法確立
- H20年度：
  - フェデレーション規模の拡大
    - 参加大学の拡大
    - 対応アプリケーションの品揃え
- H21年度：
  - 海外との連携を含む本格運用開始

情報セキュリティポリシー作業部会

国立大学法人等における情報セキュリティポリシー

□検討体制・メンバー

○　情報・システム研究機構 国立情報学研究所 学術情報ネットワーク運営・連携本部
「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」（2006年8月設置）

飯田勝吉（東京工業大学）、板垣毅（東北大学）、上原哲太郎（京都大学）、
岡田仁志（副主査、国立情報学研究所）、岡部寿男（京都大学）、岡村耕二（九州大学）、
垣内正年（奈良先端科学技術大学院大学）、笠原義晃（九州大学）、金谷吉成（東北大学）、
上岡英史（国立情報学研究所）、貴志武一（千葉大学）、鈴木孝彦（九州大学）、
曽根秀昭（主査、東北大学）、高井昌彰（北海道大学）、高倉弘喜（京都大学）、
竹内義則（名古屋大学）、谷本茂明（国立情報学研究所）、中野博隆（大阪大学）、
中山雅哉（東京大学）、西村浩二（広島大学）、林田宏三（熊本大学）、
布施勇（東京工業大学）、松下彰良（東京大学）、南弘征（北海道大学）、
湯浅富久子（高エネルギー加速器研究機構）

協力：　文部科学省大臣官房政策課情報化推進室、文部科学省研究振興局情報課、
内閣官房情報セキュリティセンター

○　社団法人電子情報通信学会「ネットワーク運用ガイドライン検討ワーキンググループ」

Secure-Japan と 大学の情報セキュリティ

【背景】

- 情報セキュリティ対策の政府機関統一基準の制定 (2005.12.13)

↓

- 国立大学法人等における情報セキュリティレベルの向上は急務

↓

＋ 大学における教育・研究との関係および組織・運営の考慮

＋ 新しい法律・技術に関する広範な専門知識を取り入れる

↓

- 国立大学法人等に適した情報セキュリティポリシーが必要

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

2007.2.26公開

サンプル規程集の策定に向けた活動

総論・体制、NW運用、認証運用、事務、利用、教育の6つの領域から構成

各研究会などのメンバーによる横断的時限組織で、セキュリティポリシーを策定

政府機関統一基準への対応や情報システム運用に関連する規程集の取りまとめ

各領域の優先事項

総論・体制

大学の情報システムの運用組織の設置に始まる運用ポリシー策定のための考え方や考慮点について検討

NW運用

ネットワークの運用と管理各種情報システムの運用や管理に携わる者が遵守すべき規則や運用・管理の面から実際に想定される留意点について検討

認証運用

認証基盤システムの構築・運用・管理

事務

事務組織に関連する情報システムのセキュリティ対策に関する基準について検討

政府統一基準対応の観点からセキュリティポリシーの作成、改訂

利用

利用者の教育に関連する内容大学の情報システムの利用者が遵守すべき規則やネットワーク利用方法について利用者の権利と責任の観点から検討

教育

リテラシー、倫理などの教育利用者への情報システム利用に関する教育と情報倫理教育について検討

サンプル規程集とその解説作成を最優先

策定したサンプル規程集の構成

ポリシー	実施規程	手順
A1000 情報システム運用基本方針 A1001 情報システム運用基準	A2101 運用・管理規程 A2102 リスク管理規程 A2103 非常時行動計画 A2104 情報格付け規程	A3101 運用・管理手順 A3102 情報システムリスク評価手順 A3103 インシデント対応手順 A3104 情報格付け手順 A3105 情報取扱い手順 A3106 外部委託における情報セキュリティ対策実施手順 A3107 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 A3111 ウェブサーバ設定確認実施手順 策定手引書 A3112 メールサーバのセキュリティ維持に関する規程 策定手引書
	A2201 利用規程	A3201 PC取扱い手順 A3202 電子メール手順 A3203 ウェブブラウザ手順　策定手引書 A3204 Web公開手順 A3211 学外情報セキュリティ水準低下防止手順 A3212 自己点検についての解説書
	A2301 年度講習計画	A3301 教育テキスト
	A2401 監査規程	A3401 監査手順
	A2501 事務情報セキュリティ対策基準	A3501 各種マニュアル類
	A2601 証明書ポリシー A2602 認証実施規程	A3601 認証手順
	→	A3001 責任者等の役割から見た遵守事項 A3002 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 A3003 例外措置手順書

青字は平成19年度中に策定する予定の文書

効果.　大学の情報セキュリティポリシーの共通化

【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
⇒　緊急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

情報セキュリティ対策のサンプル規程集を活用

→効果1：　セキュリティ対策を早期かつ高品質で実現

→効果2：　大学間で相互運用可能性のあるポリシー

ありがとうございました