# UPKI共通仕様のご紹介

H20.2.19

国立情報学研究所
学術ネットワーク研究開発センター
谷本　茂明

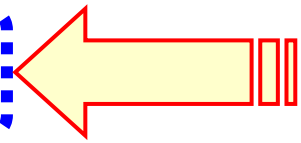
https://upki-portal.nii.ac.jp/

# 目次

# 1.1 計画概要（はじめに）

## Cyber Science Infrastructure (= e-Science) の目的

1. 学術ネットワークの強化・国際化Sinet III
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



*：NAREGIは2003年から文部科学省が進める「超高速コンピュータ網形成プロジェクト（National Research Grid Initiative：通称NAREGI）」

UPKI initiative

# 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

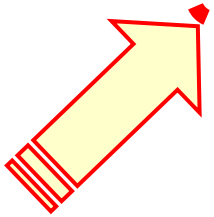
次世代スパコンを含む大学・研究機関の計算リソースの整備

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

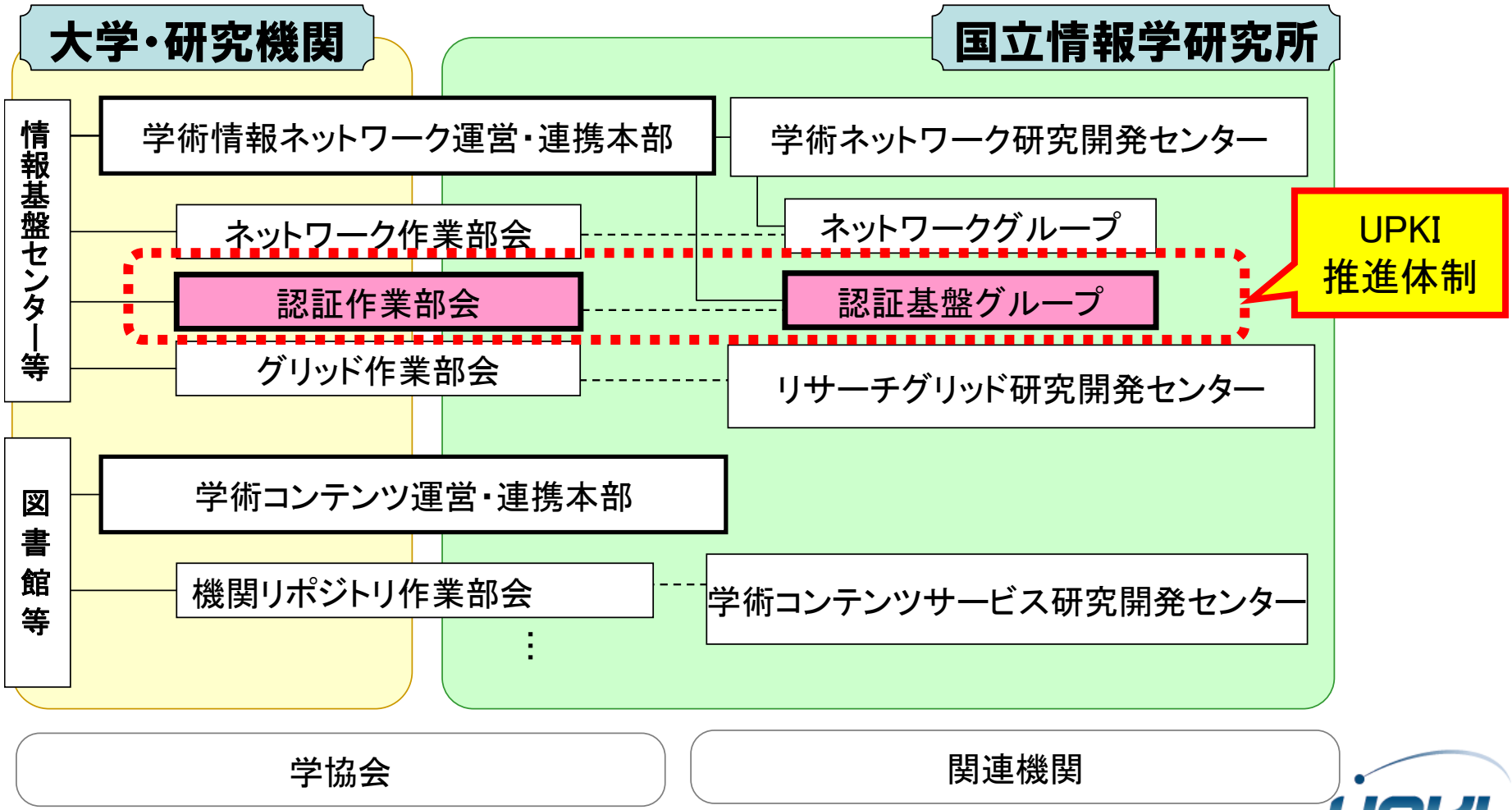
大学・研究機関としての認証システムの開発と実用化

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



UPKI initiative

# CSIの研究開発・実施体制



# 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）

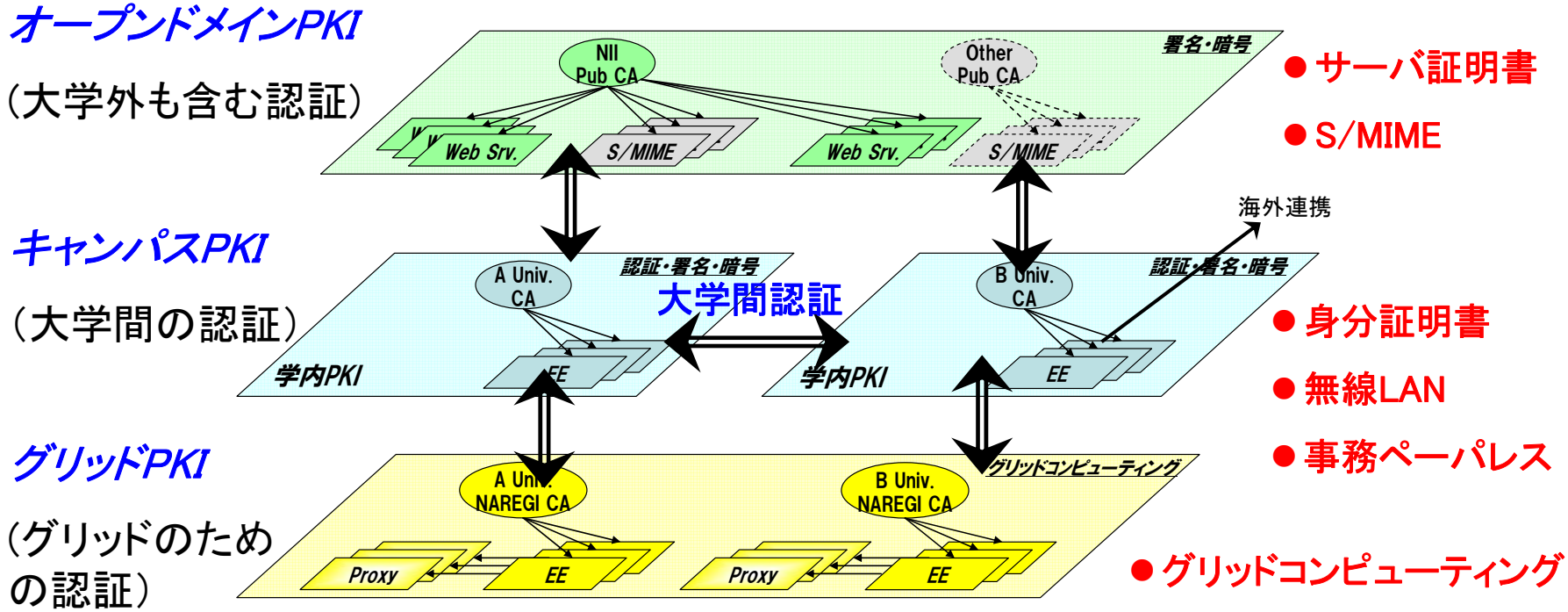
# 学術ネットワーク研究開発センター
# 認証基盤グループ

- 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
- 夏目　典大　　基盤企画課係長（連携システムチーム）

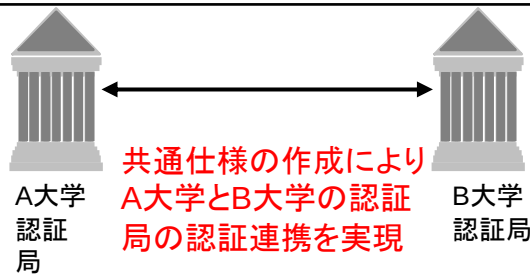
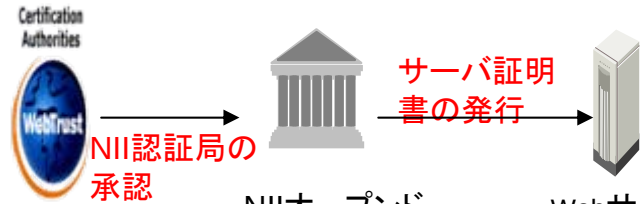
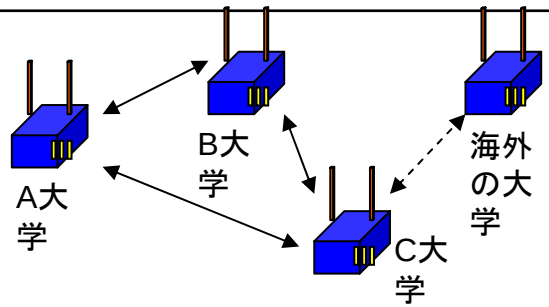
UPKI initiative

# UPKIの基本アーキテクチャ

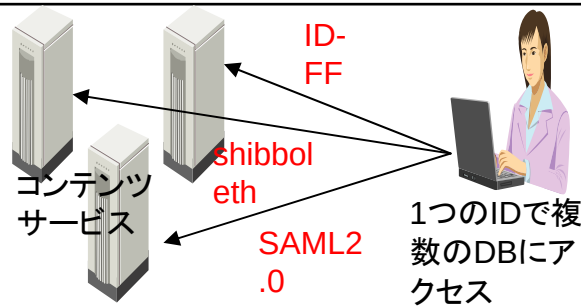
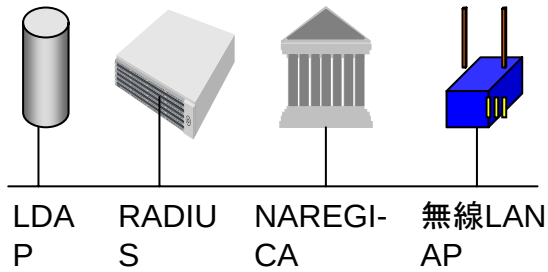
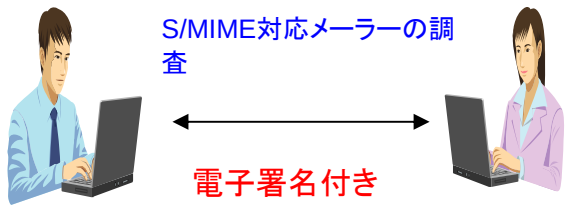
■ 3階層のPKI (Public Key Infrastructure)による役割分担と連携



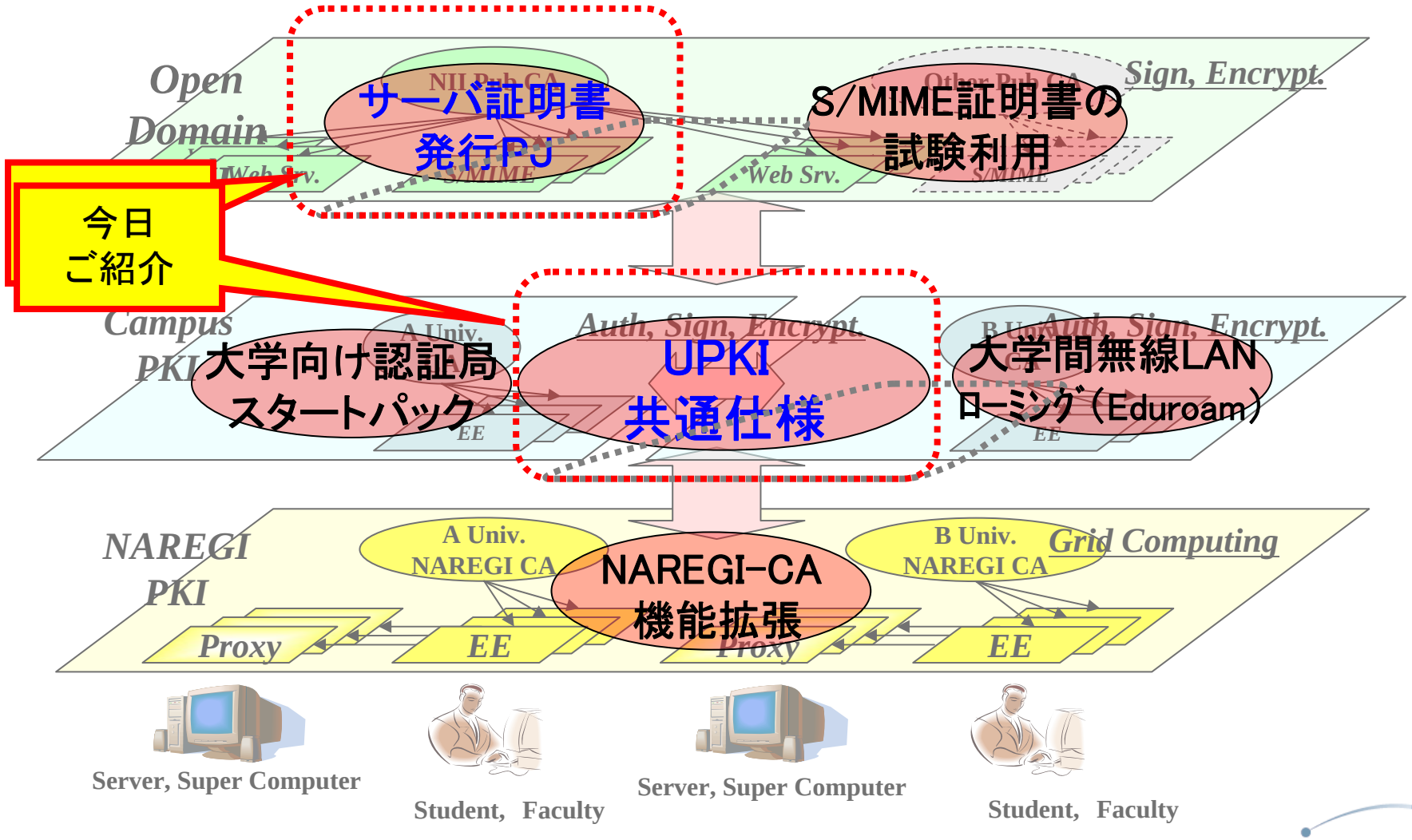
# 1.2 主なUPKIプロジェクト(1/2)

| 項番 | 事項 | 内容 |
|---|---|---|
| 1 | 「UPKI共通仕様」の作成と配布 |  <br>「UPKI共通仕様」の利用により大学での<br>・学内認証局の構築<br>・CP/CPS等の規程の整備<br>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 |  <br>Web Trust CA<br>NIIオープンドメイン認証局の構築<br>Webサーバ<br>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<br>（東北大学が中心） |  <br>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 |

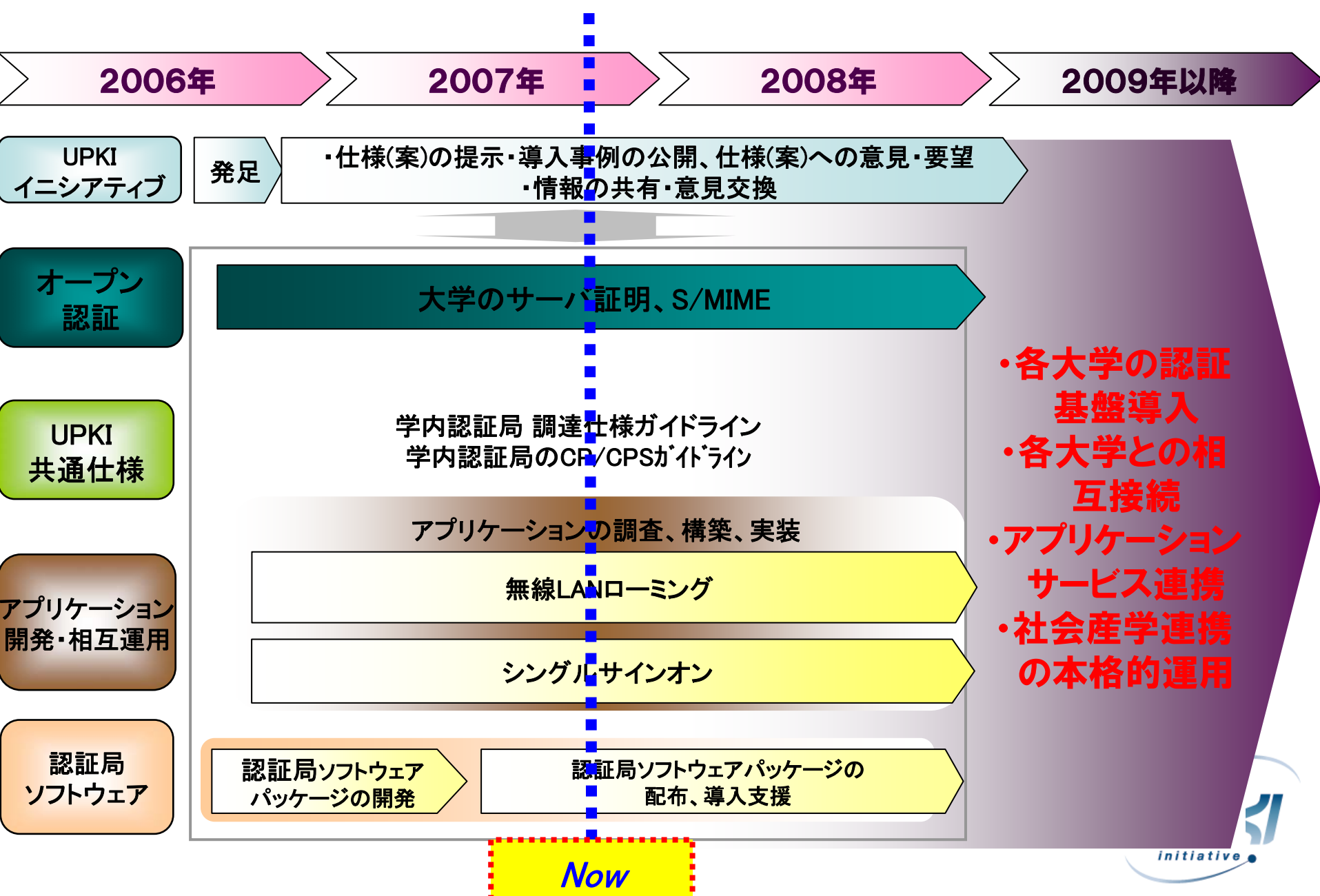
# ■ 主なUPKIプロジェクト(2/2)

| 項番 | 事項 | 内容 |
|---|---|---|
| 4 | コンテンツサービスのシングルサインオン仕様検討<br><br>※昨年の1月の京大セミナーで紹介 |  <br>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 |  <br>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<br><br>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 |  <br>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 Activities（アーキテクチャ上にマッピング）



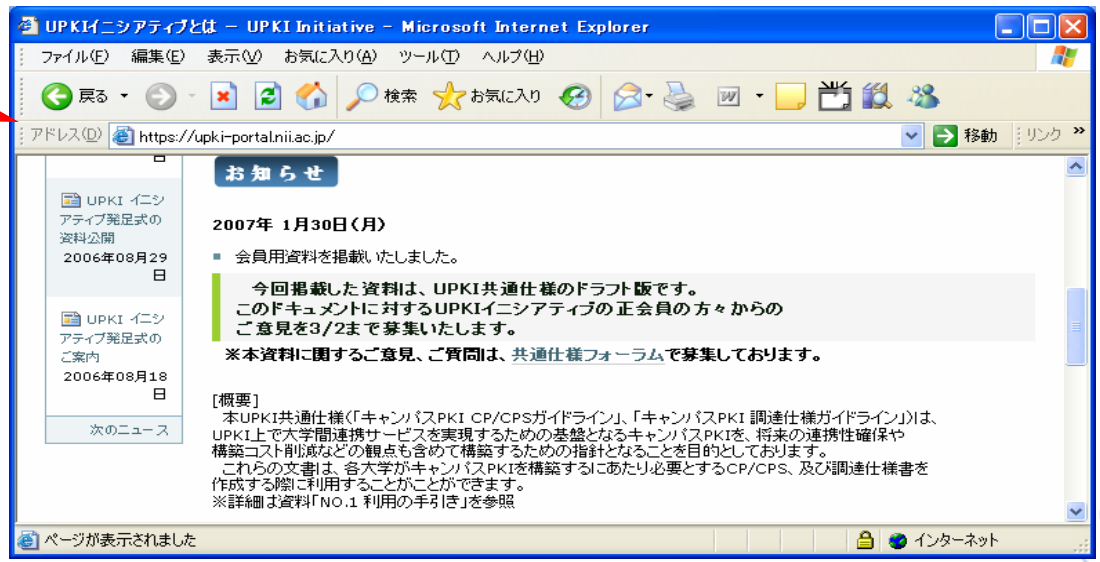
# ■ UPKI構築の全体スケジュール



# 1.3　UPKIイニシアティブ

- 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
- オフラインでのキャラバン等（H19.10：東北、12：東京、京都、広島、名古屋、H20.1：福岡、2:札幌、等）

UPKIイニシアティブのポータル画面



# 目次

# 2.1 背景

- 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

少子化と全入時代
大学の財政基盤（1%シーリング）

- 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

『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

- 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

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

UPKI initiative

# ■ 目的

「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調達仕様、CP/CPSガイドライン）**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 ⇒連携時の情報セキュリティの問題を解消

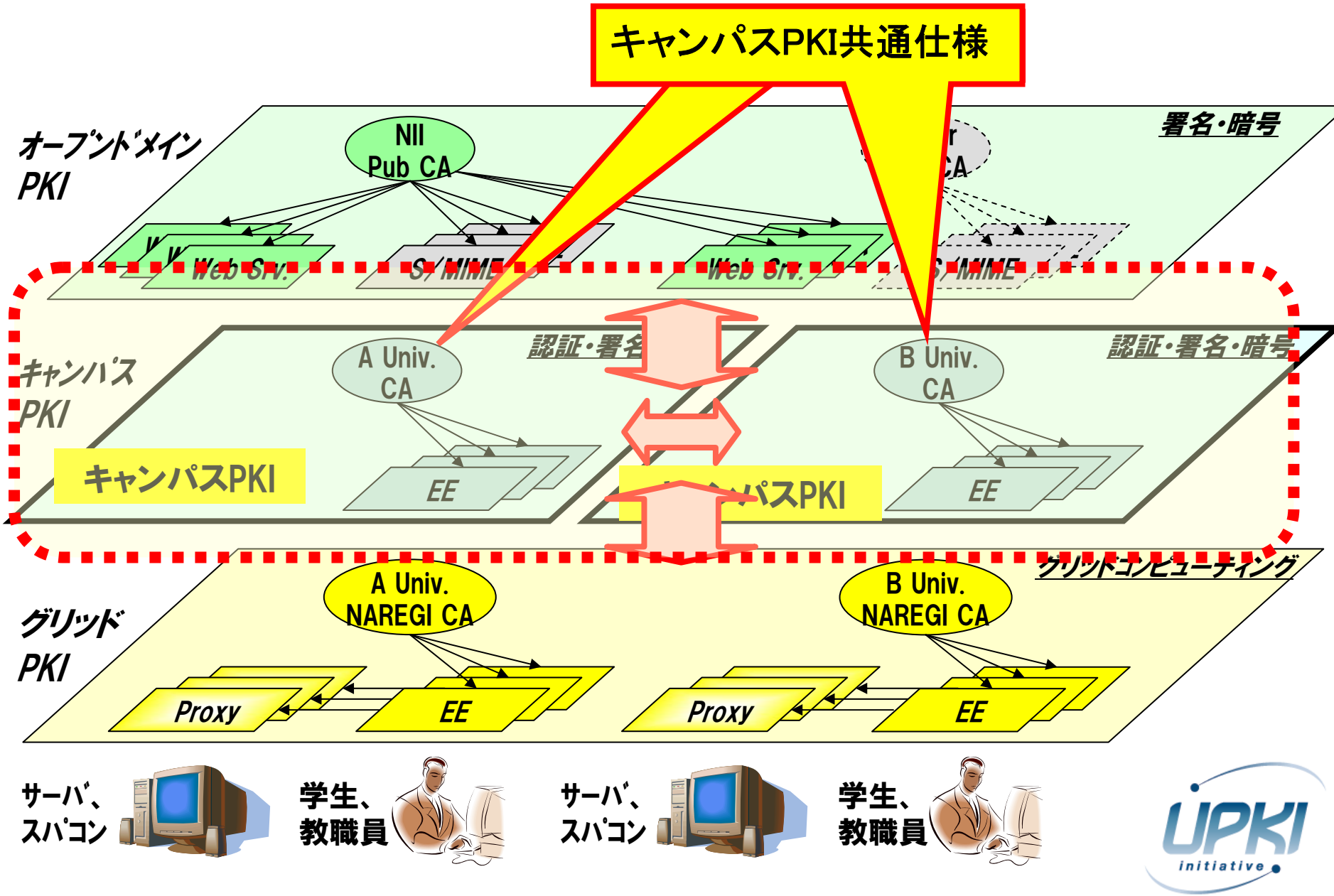
＊＊：コスト削減
- キャンパスPKI導入検討コストの削減
- CP/CPS策定コストの削減

⇒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 initiative

# ■ 位置づけ（アーキテクチャ）



# ■ 位置づけ（適用領域、目的等）

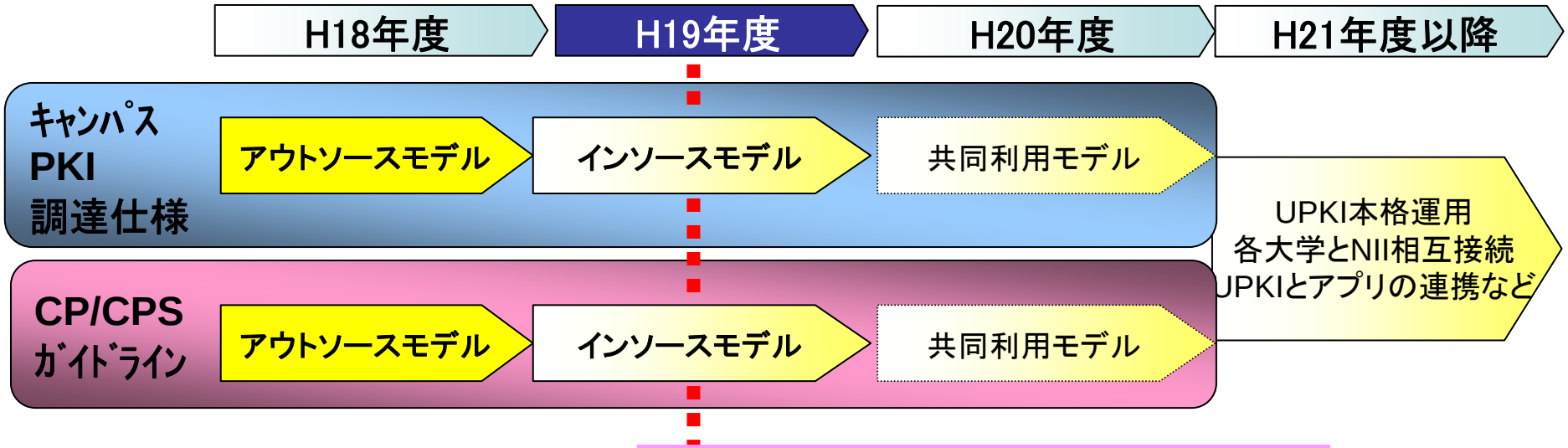
***UPKI共通仕様の検討対象***

| | 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（身分証明書、事務ペーパレス化等） | Proxy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、学内サーバなど | 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 | 全国共同利用センター |

# ■ スケジュール（案）

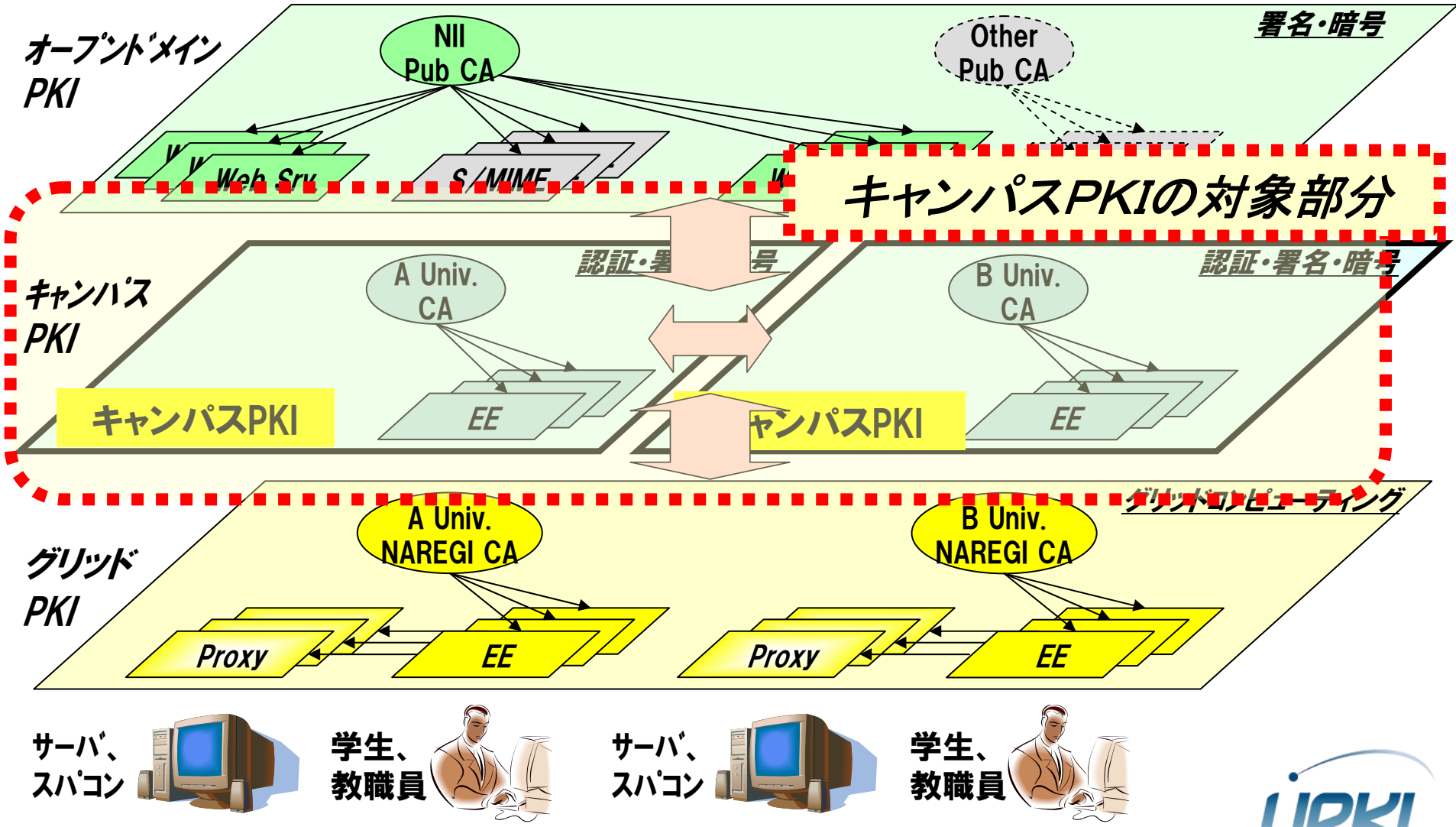
- **段階的に展開（３年計画）**
  - **まずは**キャンパスPKI共通仕様（アウトソースモデル）**を作成（H18年度）**
  - **H19年度以降、順次モデルの拡充を予定**
  - **成果に関しては、順次、**UPKIイニシアティブ※**で公開**

（※：https://upki-portal.nii.ac.jp/upkispecific）



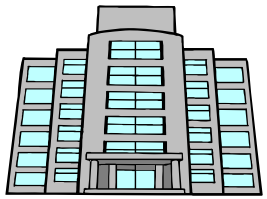

- 今年度は、インソースモデルに着手、作成中（京都大学にもご協力をいただいております）

# 2.2 キャンパスPKIモデル

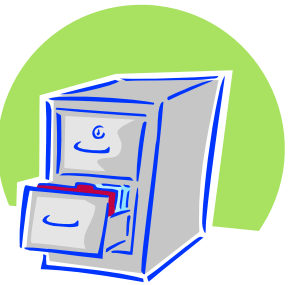


# ■ PKIの主な構成要素：
# 証明書、認証局、リポジトリ、加入者、利用者


**証明書**：鍵ペアの所持者であることを保証した情報。X.509 標準に準拠する公開鍵証明書



**認証局**：証明書を発行する認証機関を指す。認証局（CA ）はユーザの身元と鍵ペアの所有を確認し、その公開鍵証明書を発行



**リポジトリ**：証明書や、証明書の状態に関する情報（失効情報等）等を利用者（リライングパーティ）への情報提供

**加入者（サブスクライバ）：**

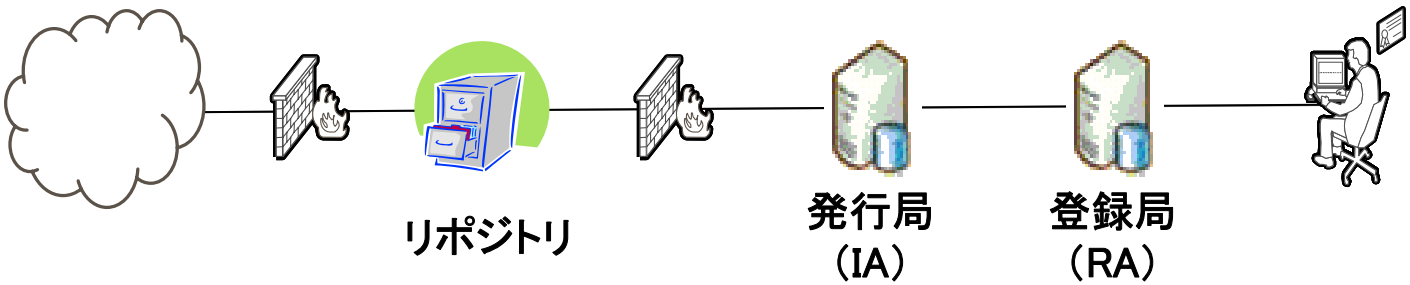

- 認証局から証明書を発行されたエンティティ
- 証明書に記載された公開鍵に紐づけられた秘密鍵を持つ。

**利用者（リライングパーティ）：**


- サブスクライバの証明書を検証するエンティティ

# ■ 認証局 （CA: Certification Authority）

- 基本機能：
  - 公開鍵暗号利用時に、その公開鍵が確かに加入者（サブスクライバ）本人のものであることを証明するための「公開鍵証明書」を発行／管理する
  - 要求に応じて証明書を配布する
  - 証明書の失効リスト（CRL）を管理する
- 主な構成要素：
  - 発行局（IA）：証明書を発行する機関
  - 登録局（RA）：電子証明書発行の申請者の本人を確認し、主として登録業務を行う機関



# ■ 認証局の一般的な運用モデル（その１）

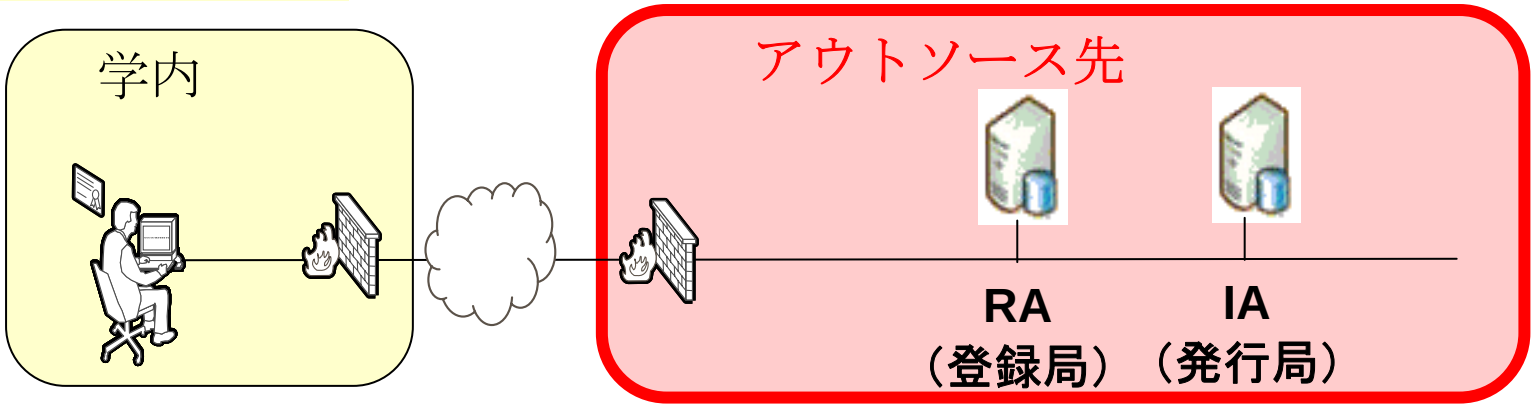
| モデル | 運用形態 | 運用先 | | | |
|---|---|---|---|---|---|
| | | IA：<br>発行局 | RA：<br>登録局 | LRA：<br>登録端末 | ICカード発行 |
| アウトソース | 全てのサーバをアウトソース | ○ | ○ | ○ | ○ |
| インソース | 全てのサーバをインソース | ● | ● | ● | △ |

○：アウトソースする、●：インソースする、△：オプションでアウトソースする

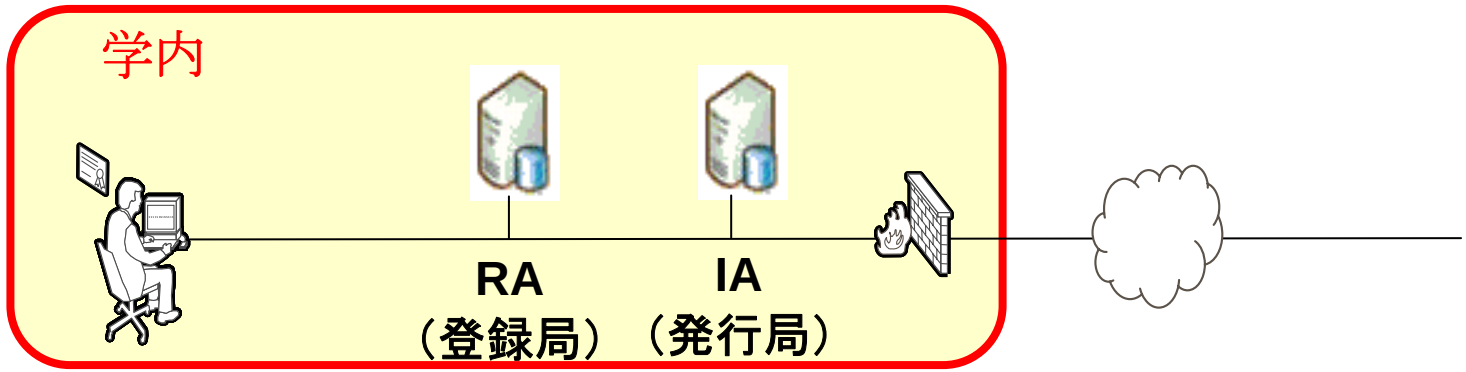
※　共同利用モデルは、いろいろな形態が考えられるが、基本的には、上記の組み合わせとなると想定される。
※　ICカードは、証明書格納媒体として耐タンパ性と持ち運びの容易さ、身分証としての役割、大量発行等を鑑み、活用メリットのあるリソースであることから、運用モデルの検討範囲として入れている。

# ■ 認証局の一般的な運用モデル（その2）

## アウトソースモデル




## インソースモデル




**アウトソースモデルから検討着手（H18年度）**

UPKI initiative

# ■ キャンパスPKIモデル（アウトソース編：H18年度成果）

## ◆ 先行大学の調査

■調達仕様に関して
　認証局システム及びICカード、認証業務を**アウトソースにて調達を実施する上で重要なポイント**を示し、その主なポイント毎に先行大学の調達仕様書の規定内容について比較した結果を示す。

■CP/CPSに関して
　**相互運用性を確立する上で重要なポイント**を示し、そのポイント毎に先行大学のCP/CPSの規定内容について比較した結果を示す。

# ■ 主な調査結果（調達仕様編）

| | A大学 | B大学 | 考察 |
|---|---|---|---|
| ①認証局階層構造 | セルフサイン証明書を持つ認証局。階層構造を持たない | ルート認証局、中間認証局（発行認証局）からなる階層構造を持つ | 運用上、特に階層構造を持つ必要性が低ければ、セルフサイン証明書を持つ認証局を前提にした方が良い |
| ②アウトソース範囲 | 発行局（IAサーバ）及び登録局（RAサーバ）の運用を外部に委託 | 発行局（IAサーバ）の運用のみ外部に委託する | 委託先に期待するホスティングサービスの内容、稼動実績、サービスレベル等について調達仕様書に明記することが必要である |
| ③ 発行対象者と証明書利用用途 | 両大学とも、発行対象者は人（教職員、学生、その他大学が認めた者）としている。共通の証明書の利用用途は、以下の通りである<br>・Webポータルや無線LAN、VPN、SSOにおけるクライアント認証の用途<br>・スマートカードログオン（Windows、MacOS、Linux）の用途 | | |

# ■ 主な調査結果（CP/CPS編）

| | A大学 | B大学 | 考察 |
|---|---|---|---|
| ①利用者の本人確認と審査登録 | ●**両大学共に利用者の本人確認は入学時、あるいは採用時**に行われ、その時に入手したデータがデータベースに登録されている。 | | |
| ②利用者の鍵ペア生成と格納媒体 | ●両大学共にアウトソース先のサーバ内において利用者の鍵ペアを生成し、**鍵ペア及び証明書の格納媒体としてICカードを利用**している。**ICカードは入館証や身分証明書の役割も果たしている**。<br>●また、鍵ペアの生成については、認証局設備と同等の設備内で内部けん制の働く環境において行われるべきであり、**両大学においてもアウトソース先の安全なファシリティ内で複数人コントロールの下で実施**されている。 | | |
| ③利用者への配付 | ●両大学共に**利用者への配付はオリエンテーション時や窓口にて対面で実施**されている。券面に印字された顔写真等を元に本人確認される。A大学については、ICカードの配付と同時に誓約書を利用者に提出させ、学内の情報セキュリティ規則への遵守及び証明書の受領について同意させる方法を用いている。 | | |

# ■ 調査結果（アウトソースモデル）（その１）

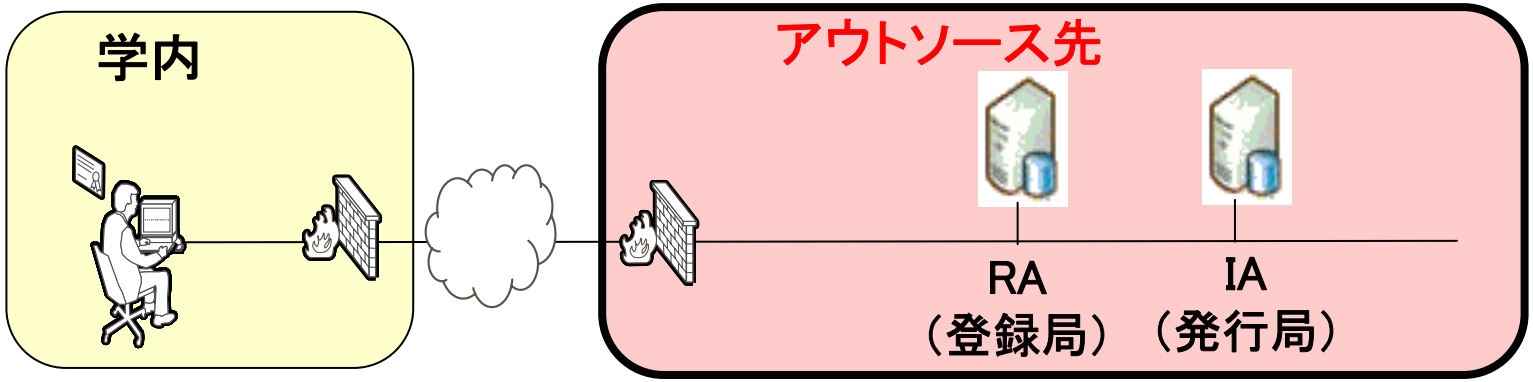
## 二段階のアウトソースモデル

| モデル | 運用形態 | 運用先 | | | |
|---|---|---|---|---|---|
| | | IA：<br>発行局 | RA：<br>登録局 | LRA：<br>登録端末 | ICカード発行 |
| アウトソース | フル<br>アウトソース | ○ | ○ | ● | △ |
| | IA<br>アウトソース | ○ | ● | ● | △ |

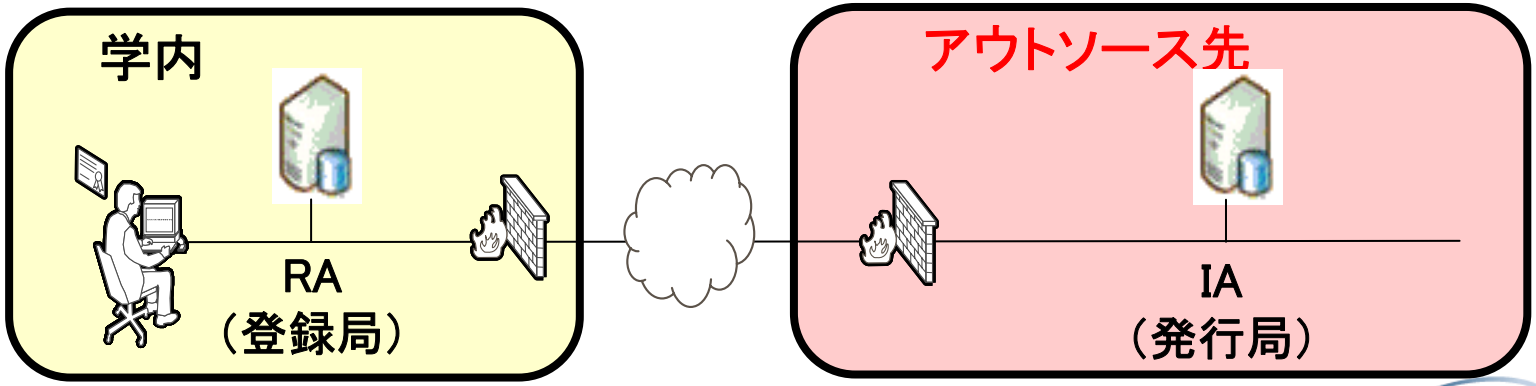
※　○：アウトソースする、●：インソースする、△：オプションでアウトソースする

# ■ 調査結果（アウトソースモデル）（その2）

## フルアウトソースモデル




## IAアウトソースモデル



# 2.3　キャンパスPKIガイドライン概要

アウトソースモデルを対象に、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。

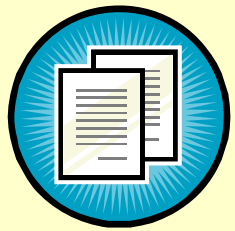
- 各大学の調達・設計における**参考資料、たたき台、雛形として活用できる**こと
- 必ずしも準拠性を求めるものではないが、**将来的に相互接続を想定している場合には本仕様に準拠することが望ましい**

**(2)ガイドラインの構成**：ガイドラインの構成は、下記のとおり。

**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



**ダウンロード先：https://upki-portal.nii.ac.jp/upkispecific**

# ■ ガイドラインの利用法（利用の手引き）

① 「キャンパスPKI CP/CPSテンプレート」、「キャンパスPKI 調達仕様テンプレート」を**各大学にて編集し利用することを想定**。

② テンプレートとして、**フルアウトソースモデル、IAアウトソースモデル**の2種類を用意。

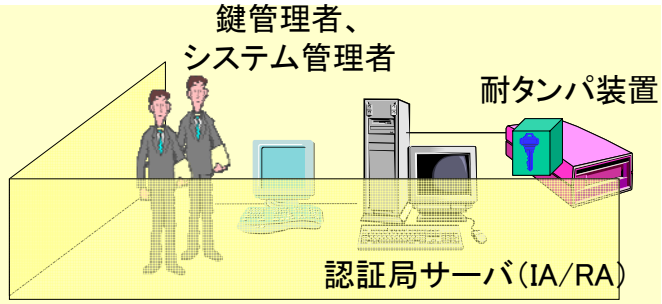
③ 各大学はこれらのモデルから**各大学の運用方針に適するものを選択して**用いることとする。

④ 具体的なテンプレートの利用方法としては、**認証局構築モデル**を選択後、各テンプレート内の空欄を**認証局の運用方針、予算、証明書利用用途に従い項目毎に取捨選択及び空欄を補充**することとする。

⑤ 各大学において本「キャンパスPKI CP/CPSテンプレート」、「キャンパスPKI調達仕様テンプレート」の**改変は自由**に行えるが、将来の大学間連携を見据えて、認証局のポリシーレベルを合わせる観点からも、各大学では**最小限の改変に留めることを推奨**する。

# ■ 主な記述内容（調達仕様ガイドライン）

(1) IAシステム要件
(2) RAシステム要件
(3) RAサーバアプリケーション要件
(4) 登録アプリケーション要件
(5) 認証基盤リポジトリ
　→Webサーバ要件、LDAPサーバ要件、OCSPレスポンダ要件




(6) アウトソース及びインソースでのファシリティ、その他の要件
　→IA/RAサーバの運用をアウトソースする場合
　→IAサーバの運用をアウトソースする場合
　→ICカード発行業務をアウトソースする場合＊（オプション）
(7) ICカードに関する要件＊（オプション）

(8) 認証局運用規程及び運用手順書の提供
(9) 保守、トレーニング要件
(10)費用

# ■（実際の）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）

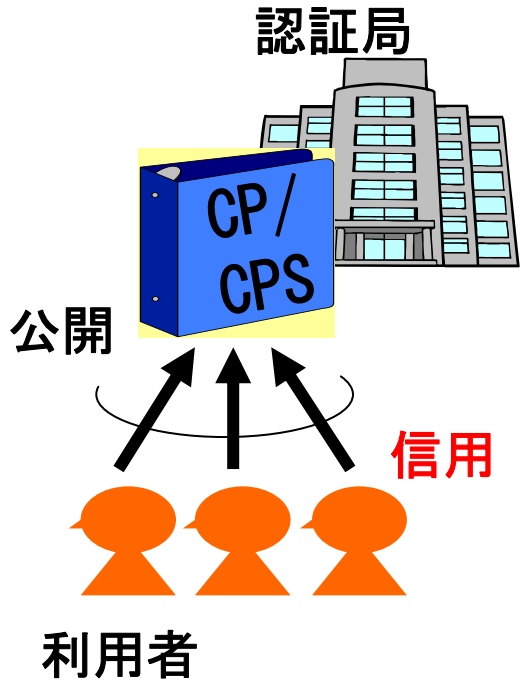
本ガイドラインでは、**認証システム及びICカードに関して必要（★）**、**ある方が望ましい（☆）**、と思われる要件を示す。各大学の要件に応じて追加すべき内容及び相互認証を行う上で将来的に調整が必要な内容が含まれることに留意すること。

# ■ CP/CPS（運用ポリシー）

- **CP：証明書ポリシー**
  - 証明書を発行する際の基準。

    **身元確認方法や鍵ペアの生成方法、想定するアプリケーションなどを記述**したもの。

    一般的には、証明書を発行する認証局毎に定義して用いる。
- **CPS：認証局運用規定**
  - CPの要件を満たすために、**認証局がどのような運用を行うかを規程**したもの

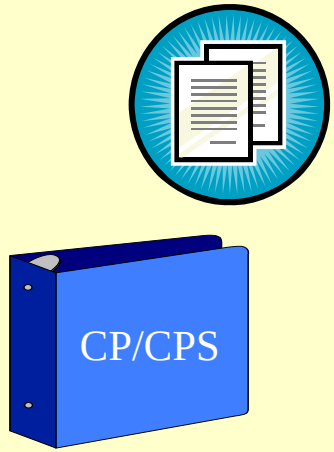



***CP : Certificate Policy***
***CPS: Certification Practice Statement***

# ■　主な記述内容（CP/CPSガイドライン）

本CP/CPSの記述内容は、**先行大学からの調査結果**に加え、**RFC3647**（CP/CPSのフレームワークを規定）を参考に記述している。主な内容は、下記のとおり。

（1） 概要
（2） 公開とリポジトリの責任
（3） **本人性確認と認証**
（4） 証明書のライフサイクル
（5） 設備、管理、運用上の統制
（6） 技術的セキュリティ管理
（7） **証明書、失効リスト、OCSPのプロファイル**
（8） **準拠性監査とその他の評価**
（9） 他の業務上の問題及び法的問題
（10）証明書、ARL/CRLプロファイル例



# ■（実際の）CP/CPSガイドラインでの記述例

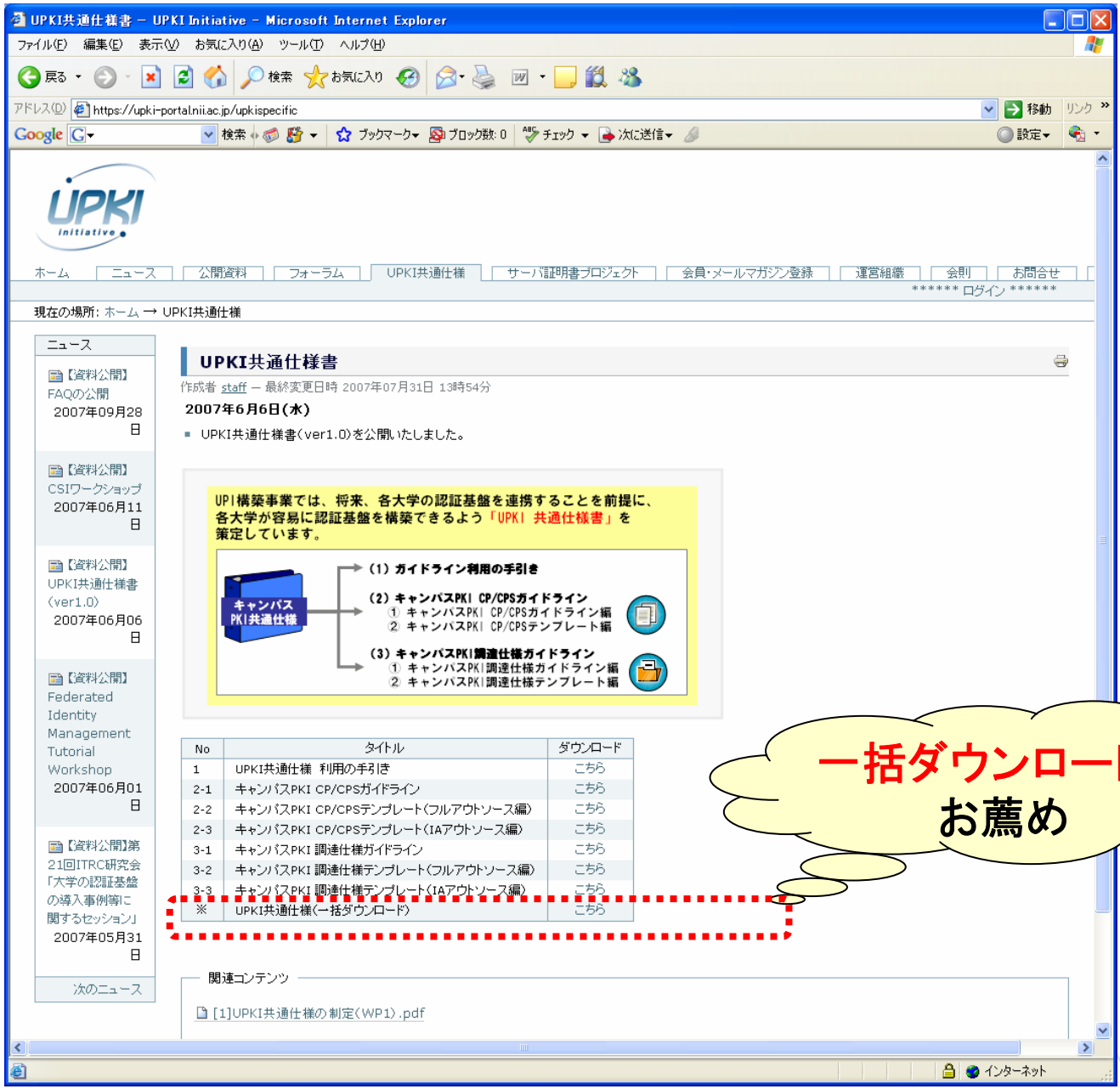
4.1.1　概要
【解説】
本節では認証局の名前、サービス名、大枠のサービス内容、相互認証を行う等の宣言を行い、認証局の概要について記す。また、相互認証の方式についても簡単に定義しておくことが望ましい。

【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。

# ■ ダウンロード先

https://upki-portal.nii.ac.jp/upkispecific



# 2.4　まとめ

■UPKI共通仕様の計画
- ➢H18年度から3年計画

■キャンパスPKIモデル
- ➢二段階のアウトソースモデル化

■共通仕様（アウトソース）ガイドライン作成
- ➢調達仕様ガイドライン、テンプレート
- ➢CP/CPSガイドライン、テンプレート

■UPKIイニシアティブに公開中
- ➢H19/6/6～：UPKI共通仕様書（アウトソース）を公開
- ➢H20/3末～：インソース編を公開予定