

# 【WP1】UPKI共通仕様の制定

---

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

# 1. 目的

WP1 (UPKI共通仕様制定)では、PKI導入に対する**コスト削減**や**将来の連携性確保**等の観点から、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**)を作成する。

- コスト削減
  - キャンパスPKI構築設計コストの削減
  - 証明書ポリシー設計コストの削減
- 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

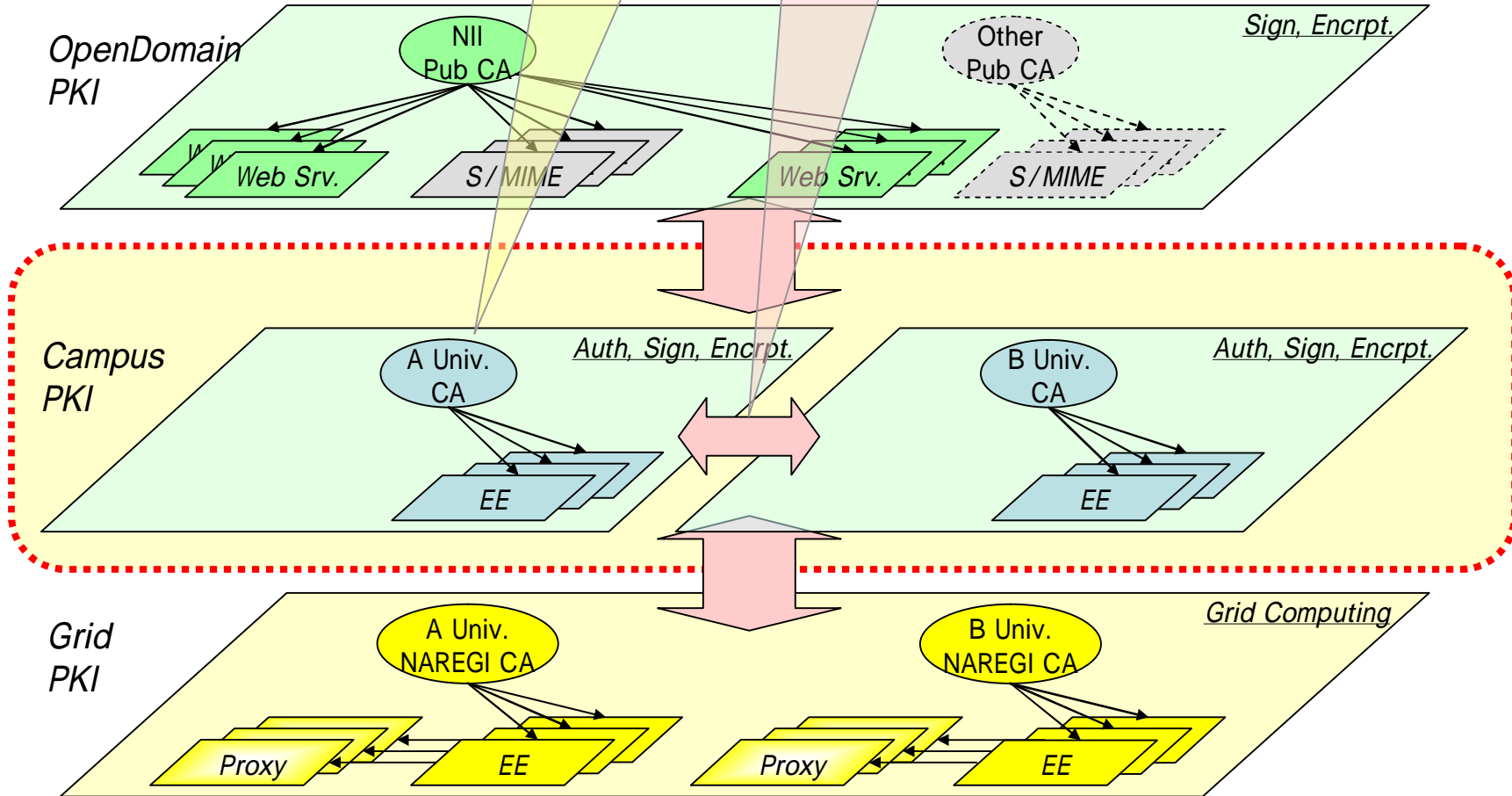
ガイドライン公開により  
キャンパスPKI導入を促進！！

## 2. 位置づけ

キャンパスPKI共通仕様

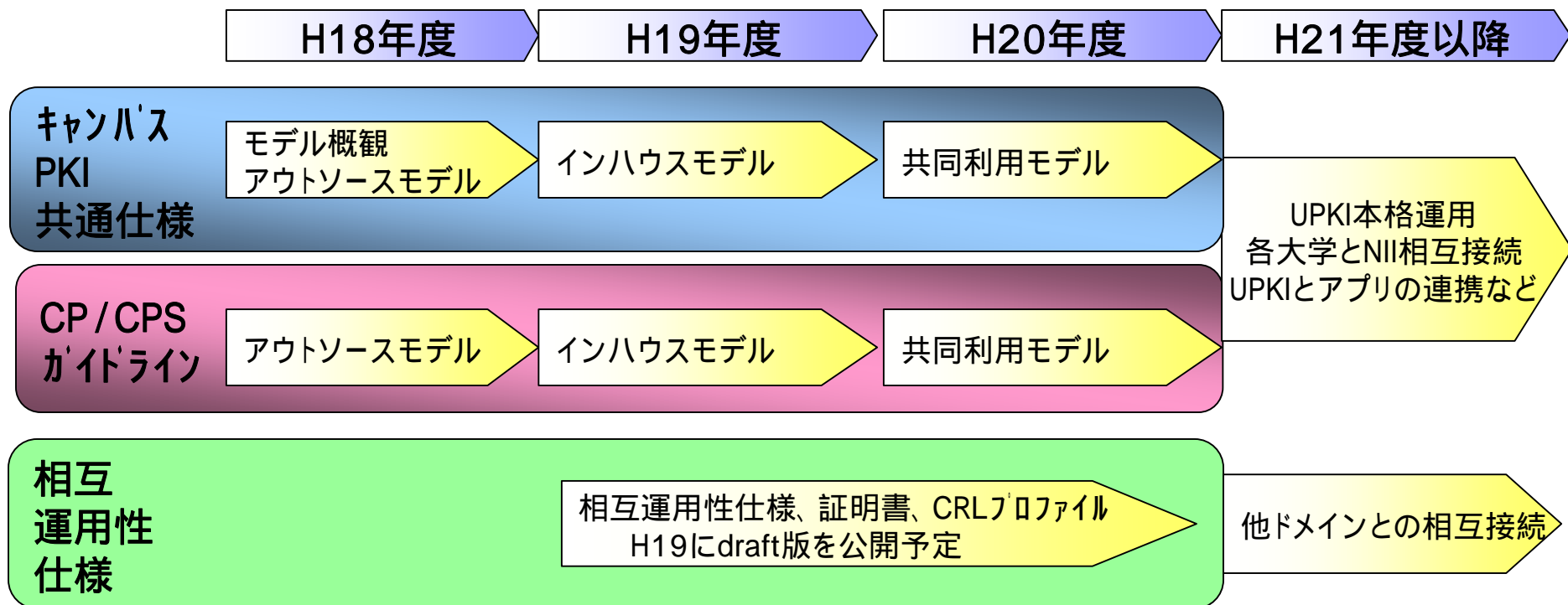
WP1での  
検討対象

相互運用性仕様



### 3. スケジュール案

- 段階的に展開
  - まずは**キャンパスPKI仕様(アウトソースモデル)**を作成(H18年度)
  - 次年度以降、順次モデルの拡充とともに**相互運用性仕様**を作成予定



順次、UPKIイニシアティブで公開予定

## 4 . H18年度計画(案)

### ■ 計画概要

- UPKI共通仕様制定として、キャンパスPKIのモデルの一つである**アウトソースモデル**について、以下を作成する。

キャンパスPKI共通仕様	～アウトソースモデル編～
CP/CPSガイドライン	～アウトソースモデル編～

## 4.1 キャンパスPKI共通仕様 ~アウトソースモデル編~

### (1)内容

- キャンパスPKIで必要となる要件を整理統合し、今後PKIの導入を予定している大学向けに必要な**キャンパスPKI共通仕様**を作成
- 認証局の運用モデルは、一般に3モデル(アウトソース、インハウス、共同利用)考えられる。H18年度は、**アウトソースモデル**から着手

### (2)主な検討課題

- モデル概観
  - ◆ アウトソース型、インハウス型、共同利用型
- 設備要件の確認と整理
  - ◆ 登録局(大学内)設備要件
  - ◆ 建物、部屋、電源、監視カメラ等
- 業務要件の確認と整理
  - ◆ 登録局(大学内)業務要件
  - ◆ 発行登録業務、発行審査業務、証明書発行業務、等
- システム要件の確認と整理
  - ◆ 登録局(大学内)システム要件
  - ◆ 暗号アルゴリズム、システム認証(ISO15408等)、等

## 4.2 CP/CPSガイドライン ~アウトソースモデル編~

### (1)内容

- キャンパスPKIで必要となる要件を整理統合し、今後PKIの導入を予定している大学向けに必要な**CP/CPSのガイドラインを作成**する。H18年度は、**アウトソースモデル**から着手する

### (2)主な検討課題

- CP/CPSの{構成、承認、更新方法等}の検討
- {設備、業務}要件の確認とCP/CPSの記述内容の検討
- システム要件の確認とCP/CPSの記述内容の検討
- CP/CPSの法務的な検討

検討にあたっては、「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」とも連携する