UPKI共通仕様の制定について

H19.2.26

国立情報学研究所
学術ネットワーク研究開発センター

目次

1．計画概要
  1.1　目的
  1.2　スケジュール

2．H18年度成果
  2.1　キャンパスＰＫＩモデル
  2.2　キャンパスＰＫＩモデル：アウトソース編
  2.3　ガイドラインの作成
  2.4　主な記述内容
  2.5　コメント募集中
  2.6　まとめ

3．今後の予定

【参考】UPKIイニシアティブ

1.1 目的

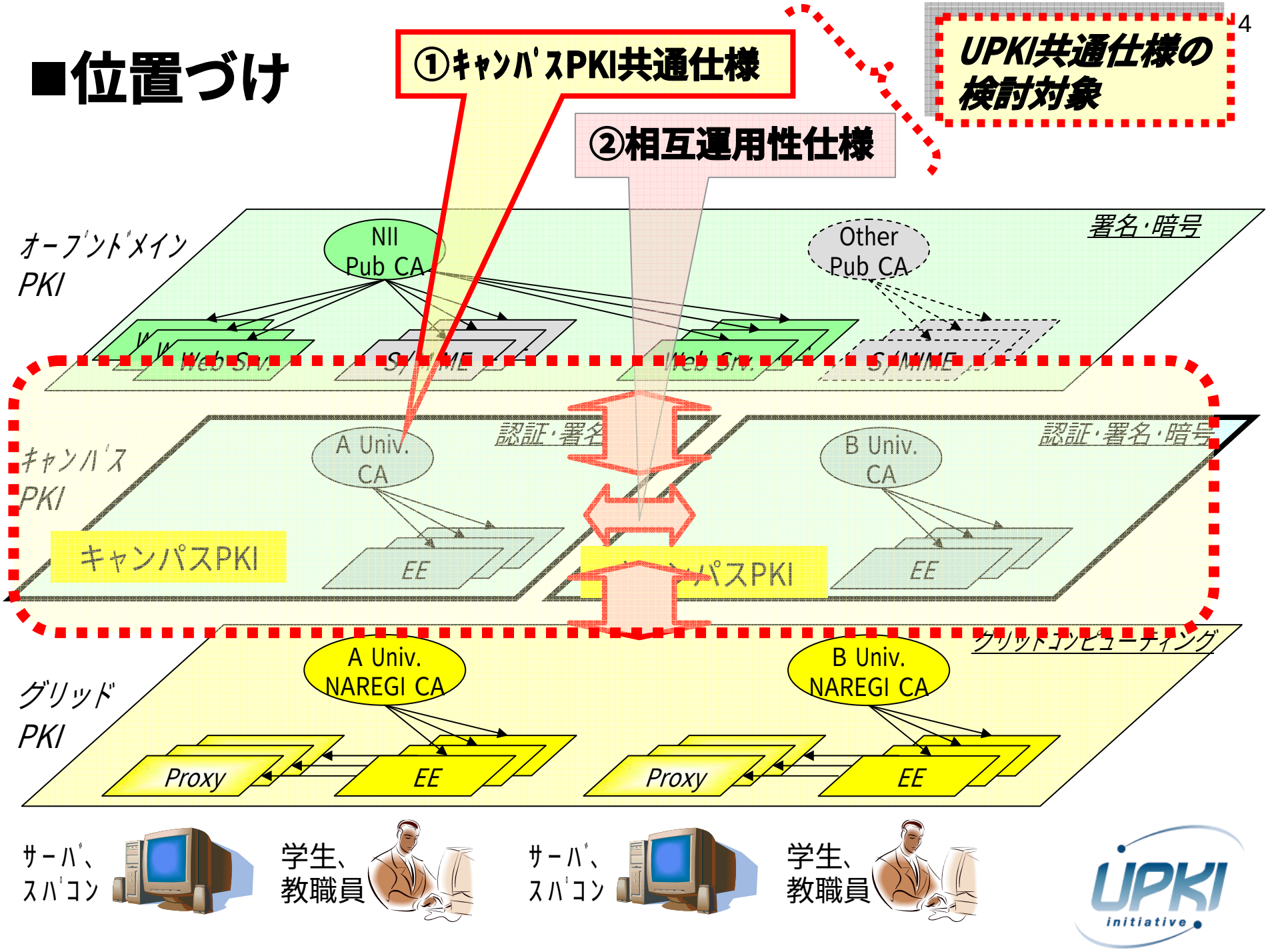
「UPKI共通仕様」では、各大学において、キャンパスPKIを導入する際の参考となる**共通仕様（キャンパスPKI共通仕様、相互運用性仕様）**を作成し、**大学へのキャンパスPKI導入を促進する**とともにPKI導入に対する将来の**連携性確保***や**コスト削減****等を狙いとするものである。

＊：**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！！

■位置づけ


①ｷｬﾝﾊﾟｽPKI共通仕様
②相互運用性仕様
UPKI共通仕様の検討対象
オープンドメイン PKI
NII Pub CA
Other Pub CA
署名・暗号
Web Srv.
S/MIME
Web Srv.
S/MIME
ｷｬﾝﾊﾟｽ PKI
A Univ. CA
認証・署名
B Univ. CA
認証・署名・暗号
キャンパスPKI
EE
キャンパスPKI
EE
グリッドコンピューティング
グリッド PKI
A Univ. NAREGI CA
B Univ. NAREGI CA
Proxy
EE
Proxy
EE
ｻｰﾊﾞ、ｽﾊﾟｺﾝ
学生、教職員
ｻｰﾊﾞ、ｽﾊﾟｺﾝ
学生、教職員

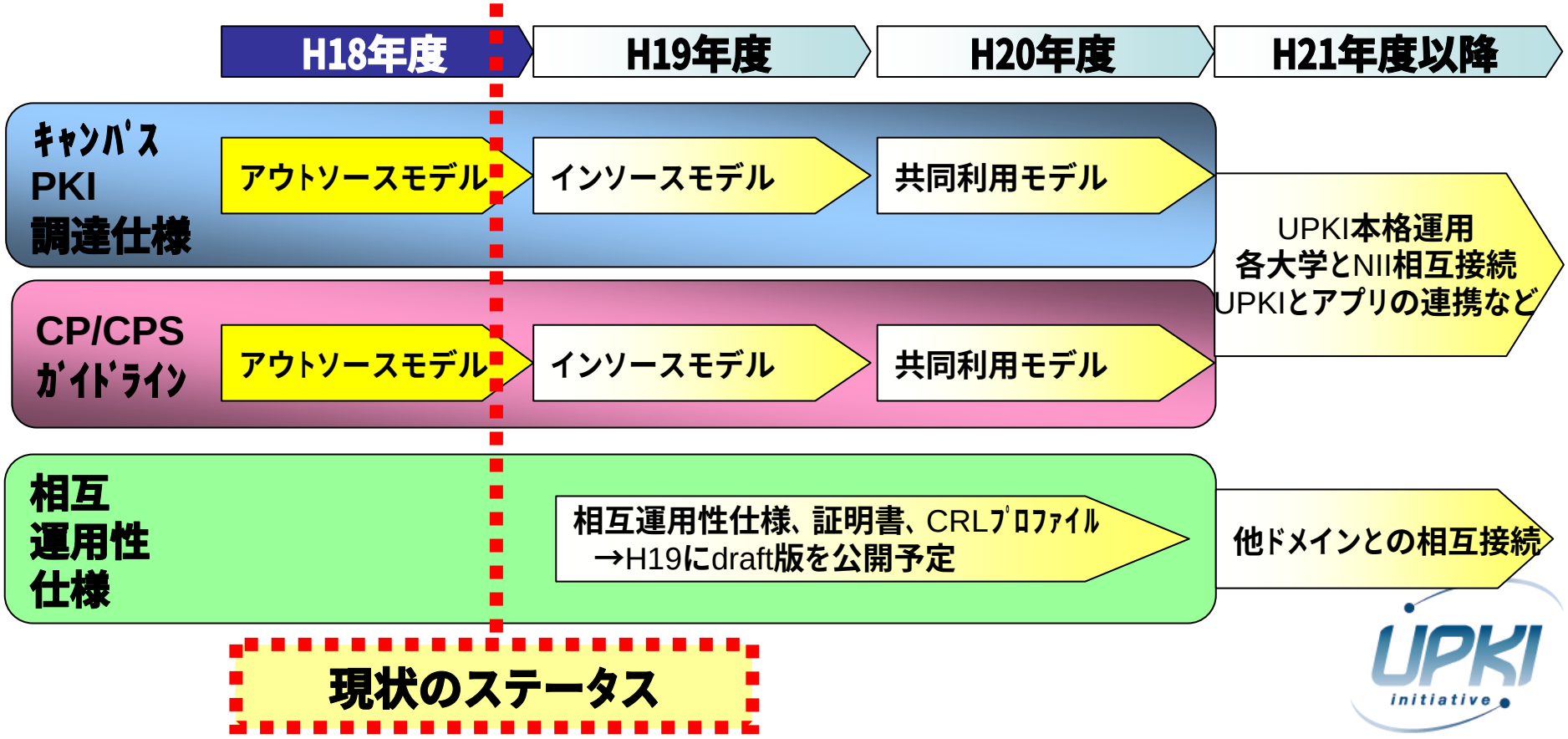
■位置づけ

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

1.2 スケジュール (案)

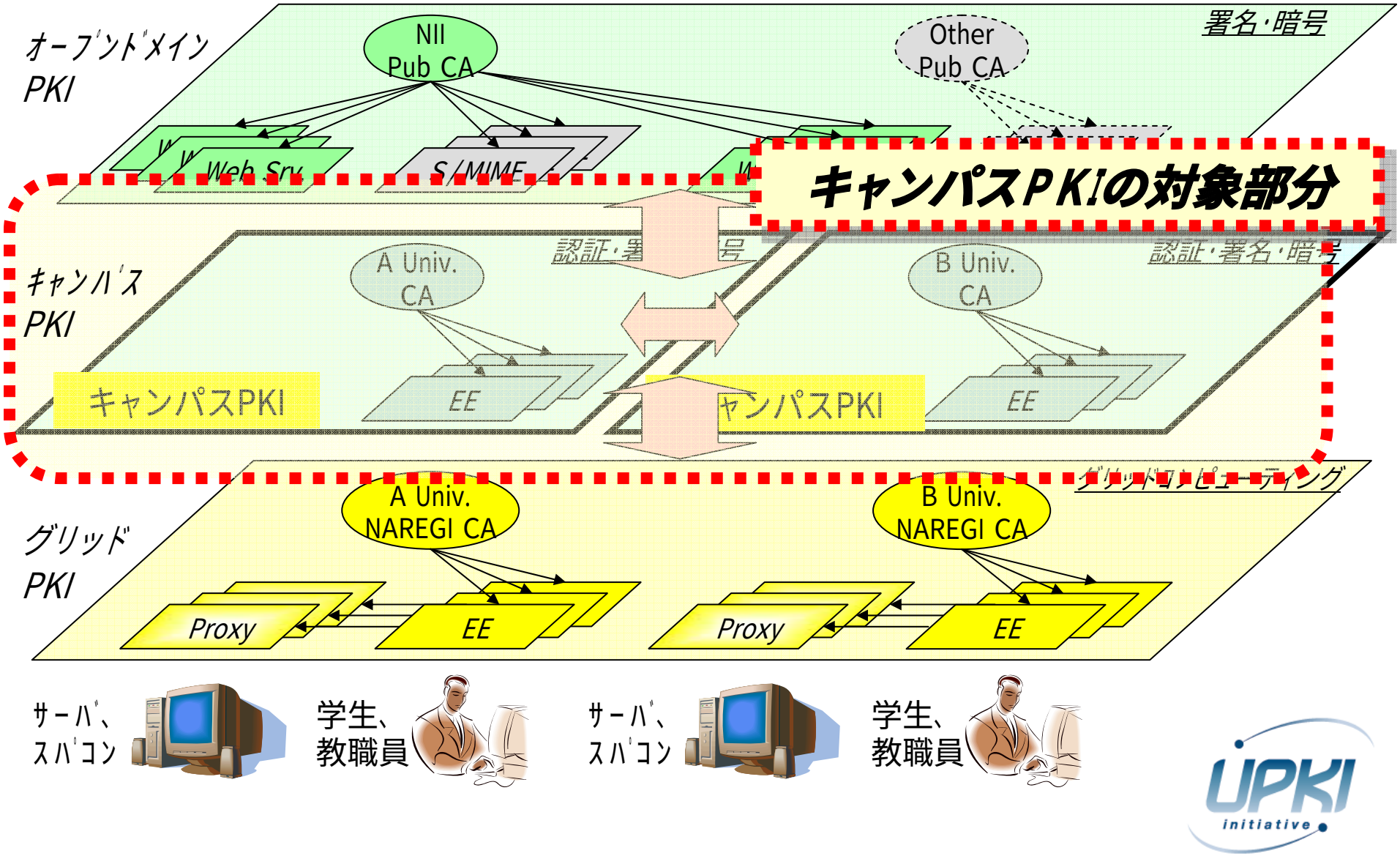
- 段階的に展開 (3年計画)
  - まずはｷｬﾝﾊﾟｽPKI共通仕様 (ｱｳﾄｿｰｽﾓﾃﾞﾙ) を作成 (H18年度)
  - 次年度以降、順次モデルの拡充とともに相互運用性仕様を作成予定
  - 成果に関しては、順次、UPKIイニシアティブで公開予定



2．H18年度成果

2.1　キャンパスＰＫＩモデル
2.2　キャンパスＰＫＩモデル：アウトソース編
2.3　ガイドラインの作成
2.4　主な記述内容
2.5　コメント募集中
2.6　まとめ

2.1 キャンパスPKIモデル



2.1.1 認証局の一般的な運用モデル（その1）

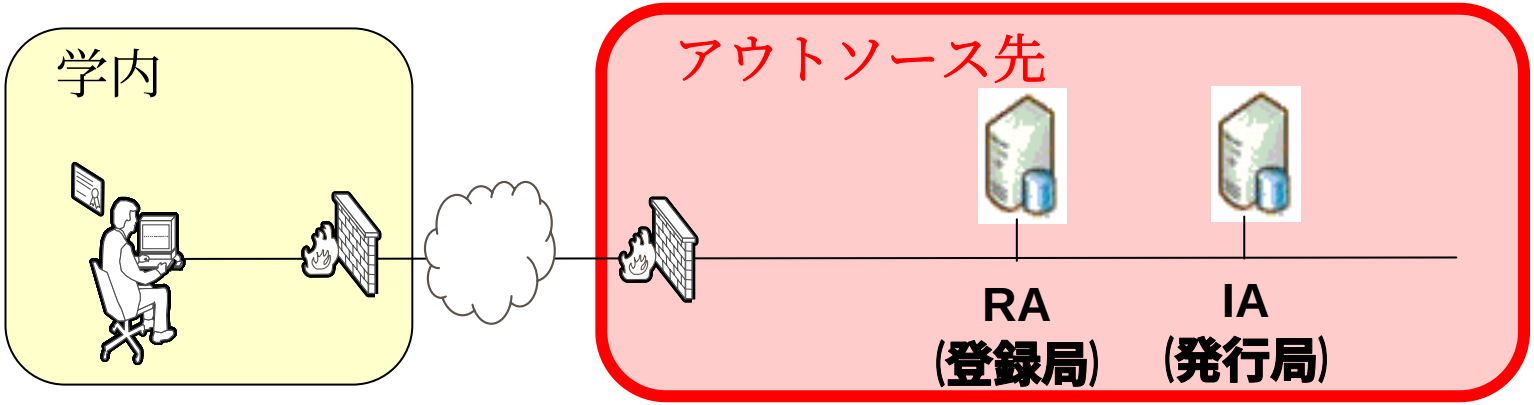
モデル	運用形態	運用先			
		IA： 発行局	RA： 登録局	LRA： 登録端末	ICカード発行
アウトソース	全てのサーバをアウトソース	○	○	○	○
インソース	全てのサーバをインソース	●	●	●	●

○：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

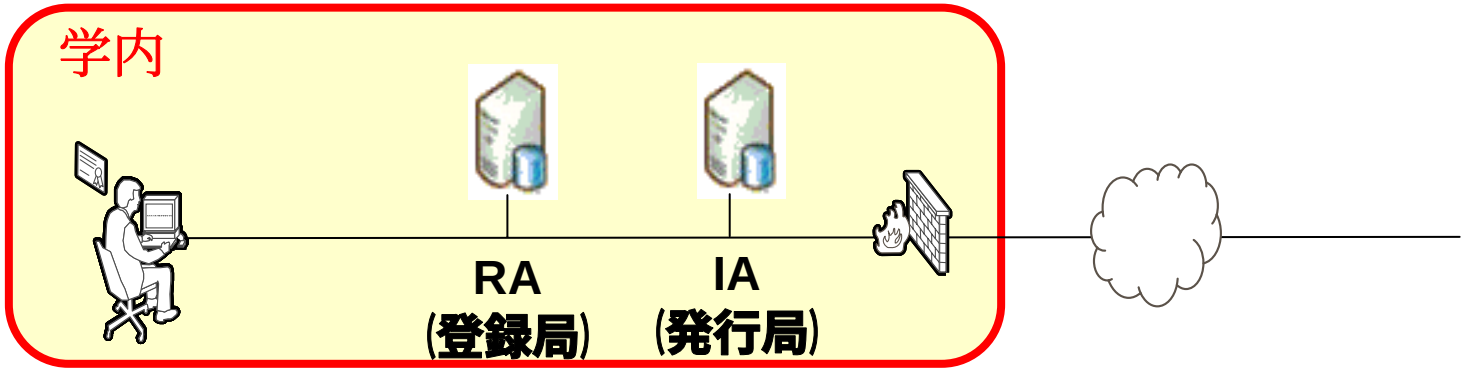
※ 共同利用モデルは、いろいろな形態が考えられるが、基本的には、上記の組み合わせとなると想定される。
※ ICカードに関しては、キャンパスPKI導入の際に必須のものではないが、入退室管理や学生証等との併用に見られるように、**活用メリットのあるリソース**である ことから、運用モデルの検討範囲として入れている。

■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



H18年度は、アウトソースモデルから検討着手

UPKI initiative

2.2 キャンパスPKIモデル：アウトソース編

2.2.1 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。

2.2.2 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 ・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 ・スマートカードログオン（Windows、MacOS、Linux）の用途		

2.2.3 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**。 ●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。		

2.2.4 調査結果（アウトソースモデル）（その1）

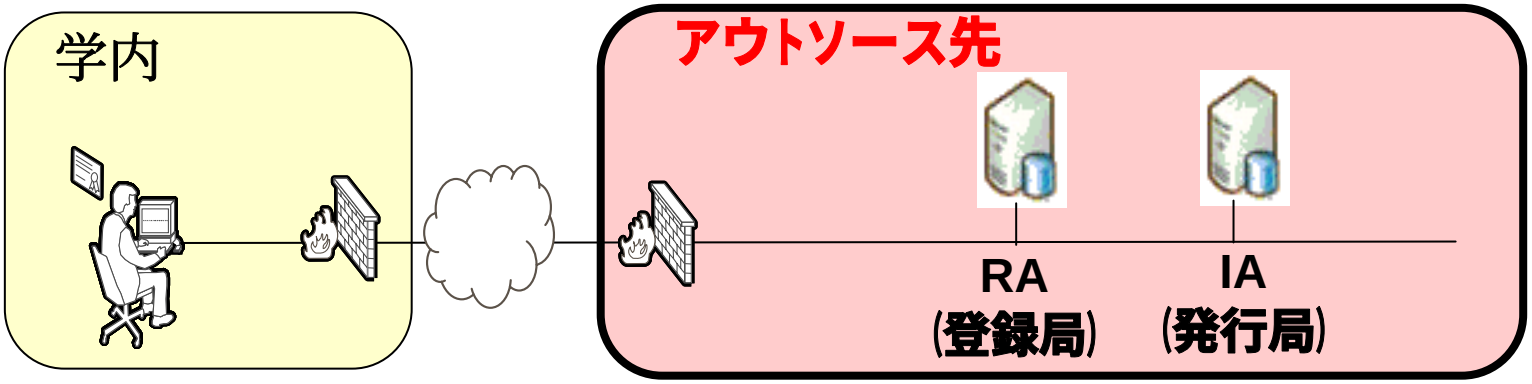
二段階のアウトソースモデル

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

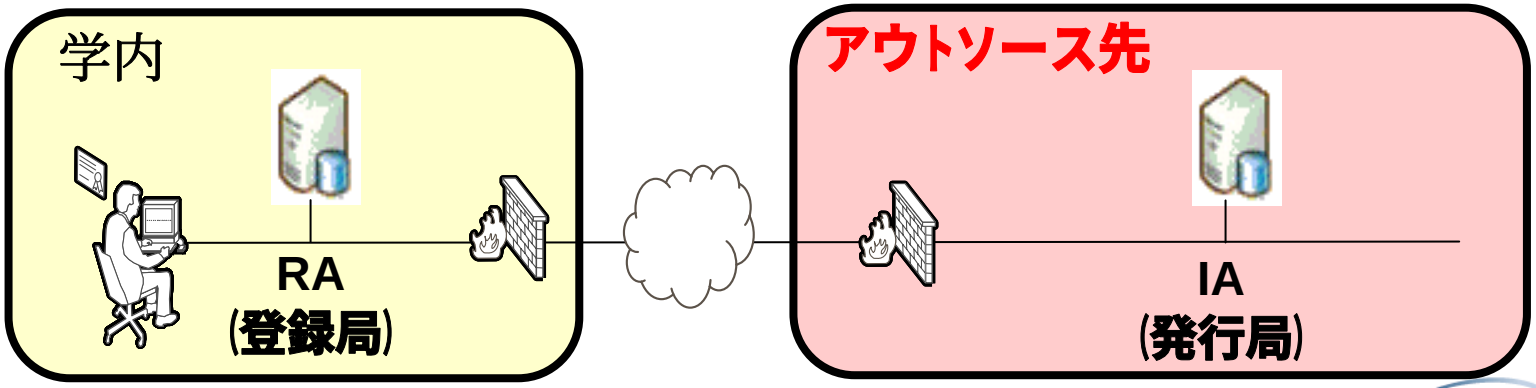
※ ○：アウトソースする、●：インソースする、△：オプションでアウトソースする

2.2.5 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 ガイドラインの作成

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。

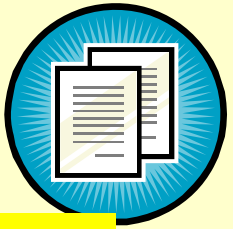
(1)作成にあたって：キャンパスPKIガイドラインの作成にあたっては、以下の点に留意した。

- 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/item/idata/mdatam/Interop-d/CampusPKI/

2.3.1 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。

2.3.2　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

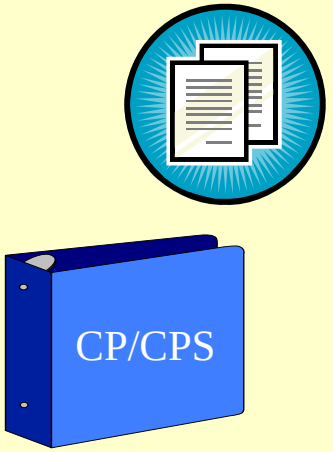
(2)ログ収集機能
★登録局サーバを操作した全てのログについて操作日時、アクセス元端末特定情報、操作者、操作時刻、リクエスト先、イベント内容、リクエスト結果が分かる記録を取得できること
★操作者を認証し、ログの検索、参照を可能とすること
★ログの改ざん検知が可能であること
(3)個人情報連携機能
★利用者の情報を予め信頼しているデータベース等と照合するかCSV形式で入出力し、その存在性、同一性の確認ができること
(4)メールによるサーバ証明書配付、通知機能
☆指定された申請者のメールアドレスに対し、証明書の取得方法、あるいは証明書ファイルを送付できること＊（主に機器に対して証明書を発行した場合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

2.4　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
○○電子認証局は、○○大学により運営され、○○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、「○○ 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○○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 。

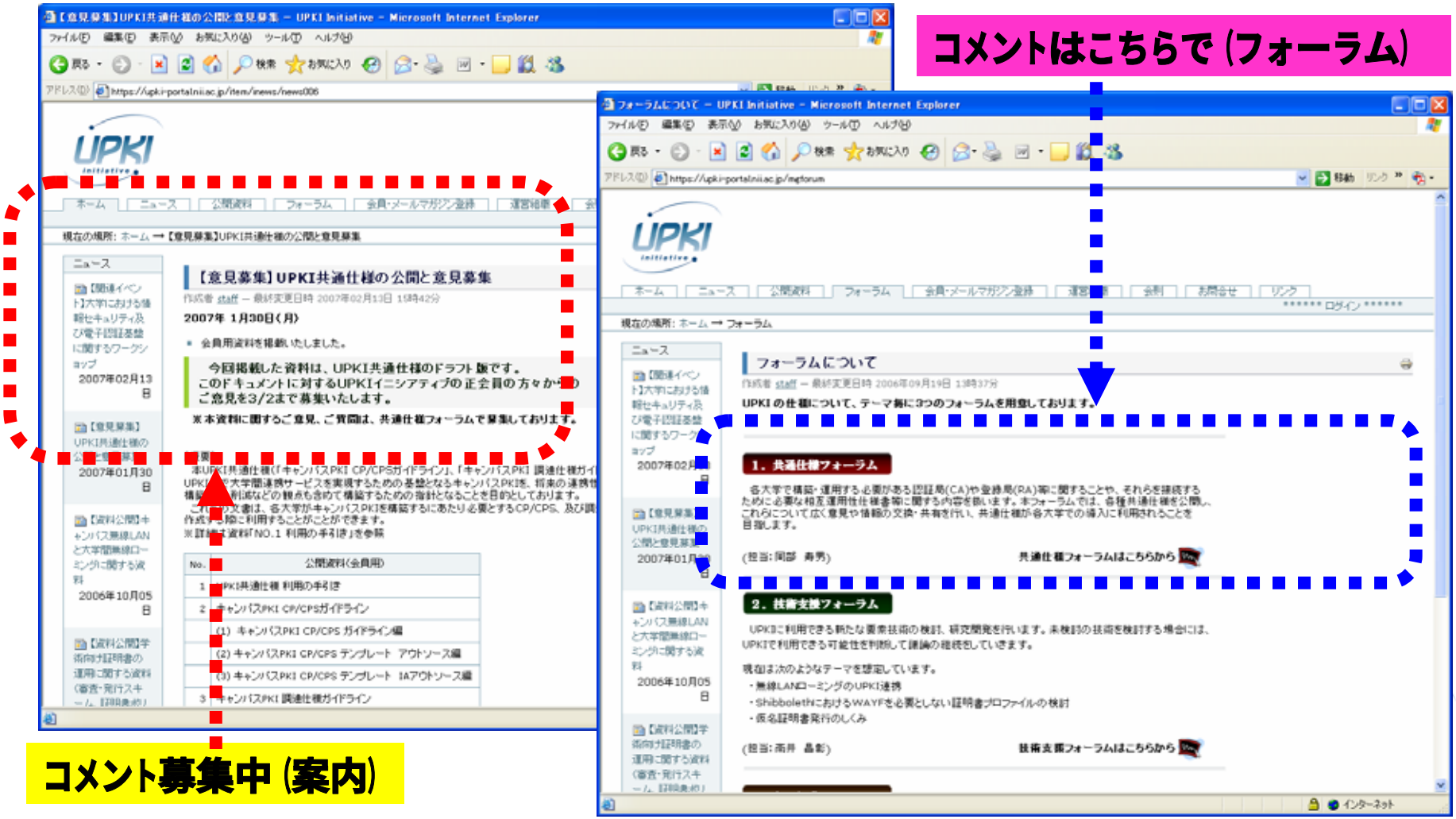
上記のように、ガイドラインの各章において、それぞれ解説と記述例を示し、理解し易いようにしている。

■ダウンロード先：
https://upki-portal.nii.ac.jp/item/idata/mdatam/Interop-d/CampusPKI/

➢**一括ダウンロード**がお薦め

2.5　コメント募集中

UPKIイニシアティブで公開し（https://upki-portal.nii.ac.jp/）、パブリックコメント募集中（1/30～3/2）



2.6　まとめ

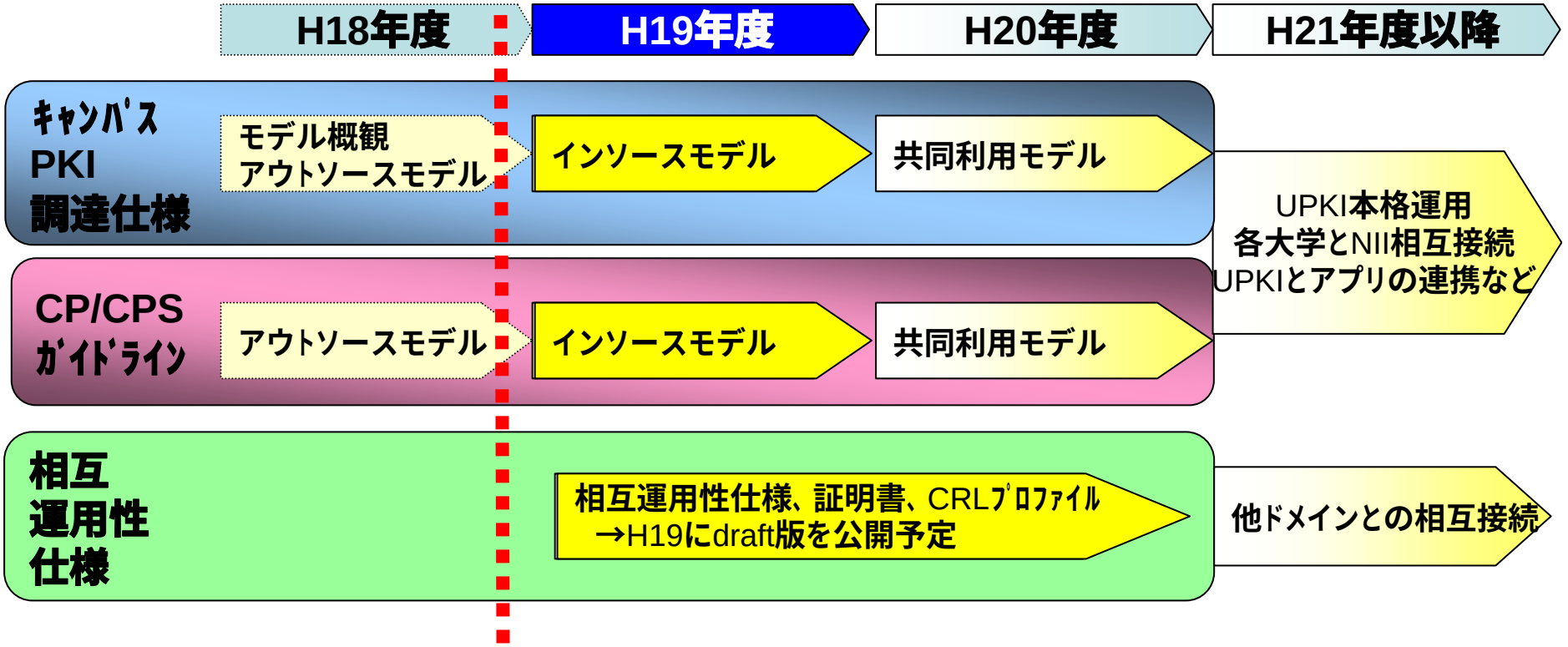
■UPKI共通仕様の計画
- ➢H18年度から**3年計画**

■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
- ➢1/30～3/2：**パブリックコメント募集中**

3. 今後の予定



- UPKIイニシアティブで公開し（https://upki-portal.nii.ac.jp/）、パブリックコメントを募集中（1/30～3/2）
- インソースモデルに着手

【参考】

■UPKIイニシアティブ (https://upki-portal.nii.ac.jp/)