UPKI共通仕様の活用について
～CP/CPSガイドライン詳細解説～

H20.9.2

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/

Agenda

1. UPKI概要
   - 1.1 計画概要（位置づけ、体制、基本ｱｰｷﾃｸﾁｬ）
   - 1.2 主なプロジェクト（共通仕様、ｻｰﾊﾞ証明、SSO連携等）
   - 1.3 UPKIイニシアティブ

2. UPKI共通仕様
   - 2.1 背景・目的・位置づけ
   - 2.2 キャンパスPKIモデル
   - 2.3 キャンパスPKIガイドライン
   - 2.4 （想定）効果

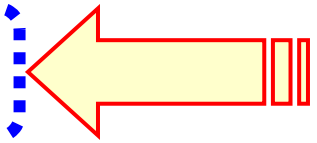
3. CP/CPSガイドライン詳細（インソース編）
   - 3.1 CP/CPSガイドラインの主な項目
   - 3.2 RFC3647との比較
   - 3.3 CP/CPSガイドライン

4. まとめ

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）」

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

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

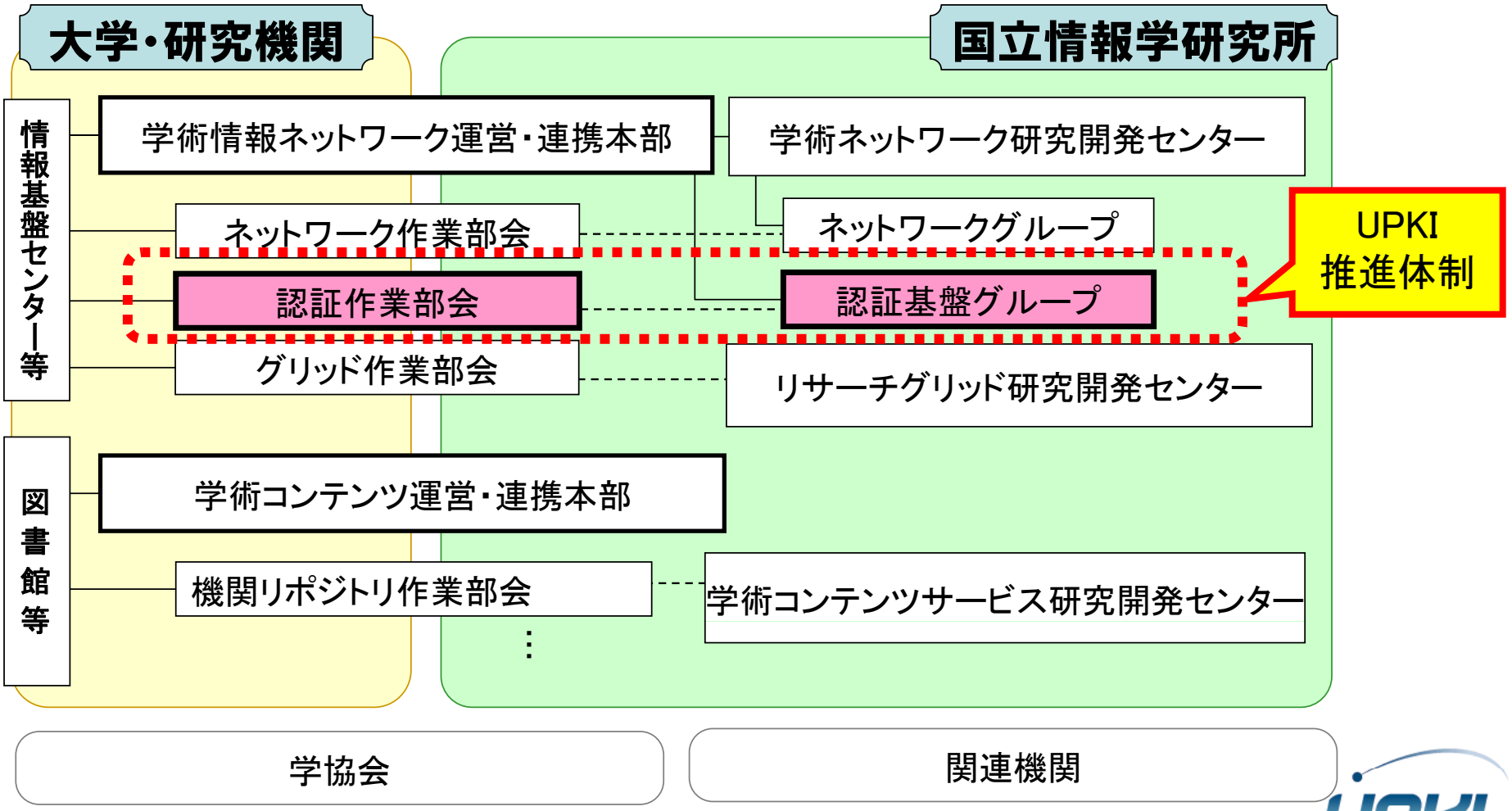
NIIと大学情報基盤センター等との連携による
次世代学術情報ネットワークの構築・運用

産業・社会貢献

国際貢献・連携

UPKI initiative

CSIの研究開発・実施体制



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

オープンドメインPKI

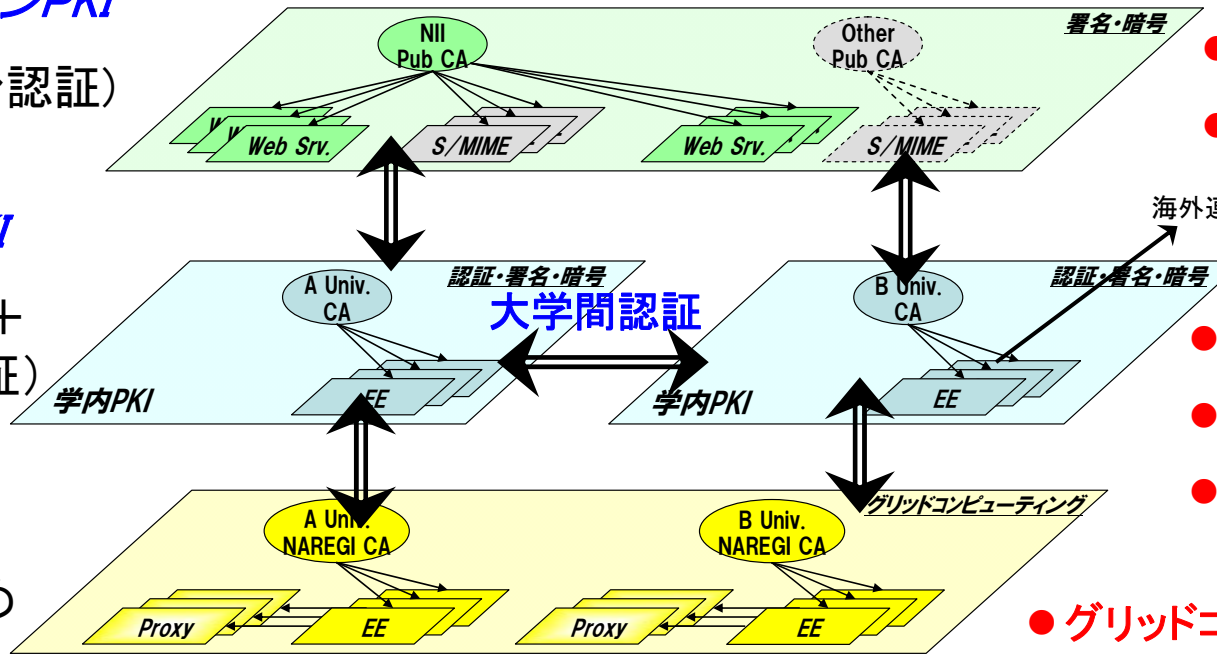
(大学外も含む認証)

キャンパスPKI

(大学内認証＋大学間の認証)

グリッドPKI

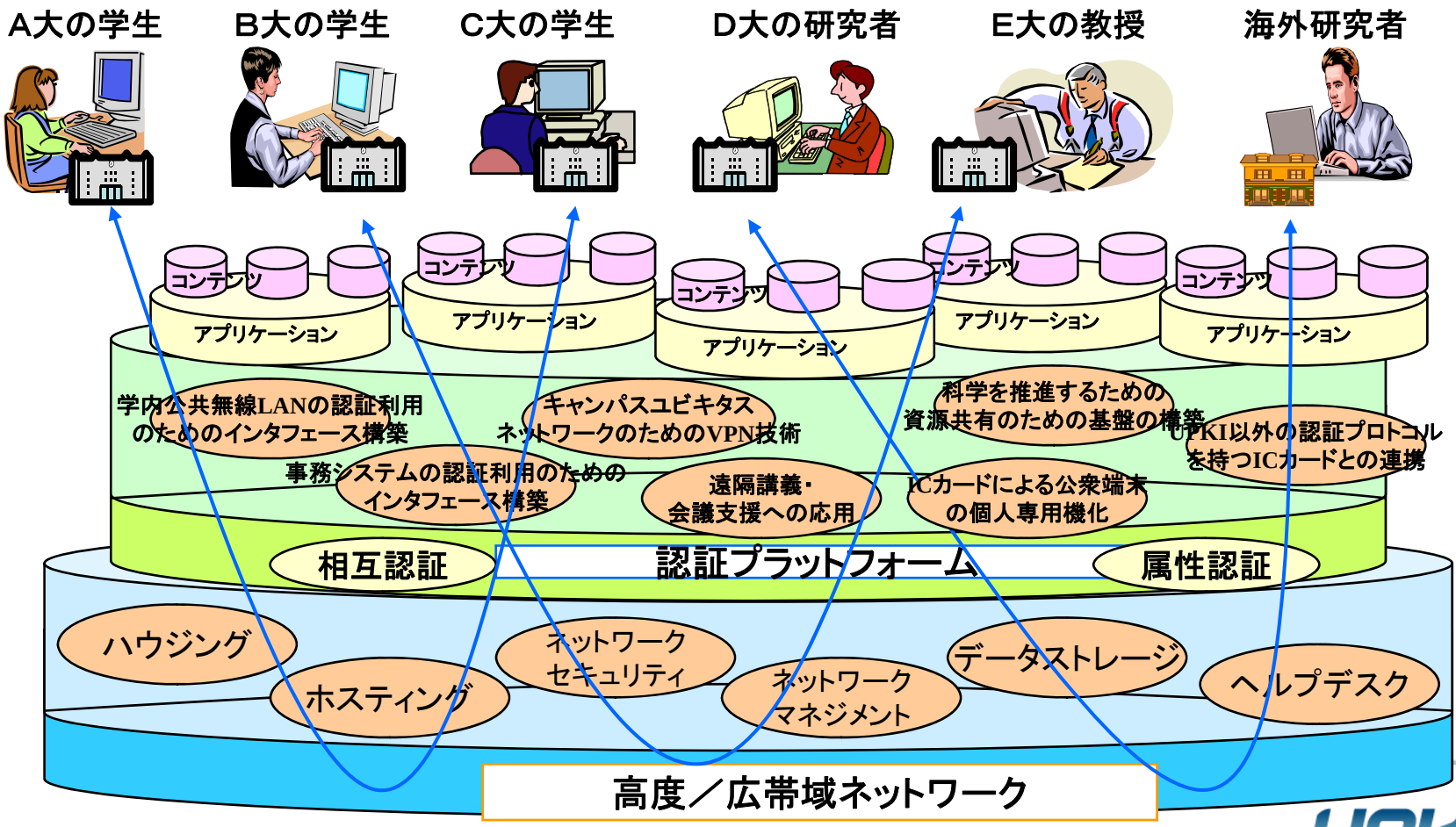
(グリッドのための認証)



- サーバ証明書
- S/MIME
- 身分証明書
- 無線LAN
- 事務ペーパレス
- グリッドコンピューティング

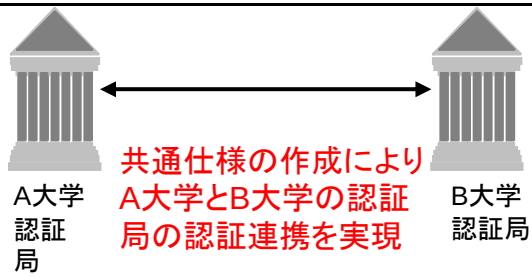
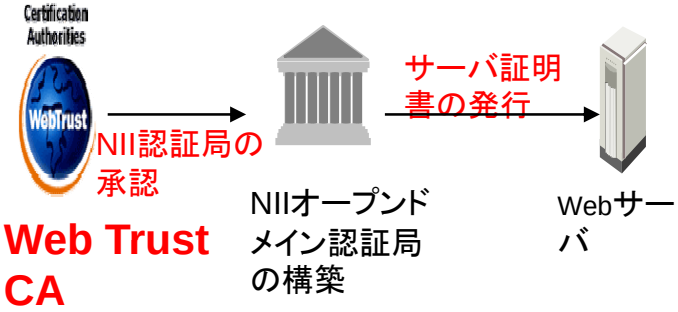
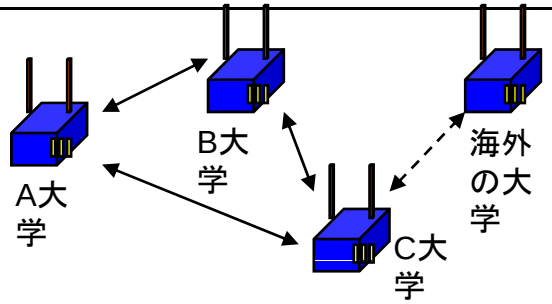
認証基盤の形成例

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！



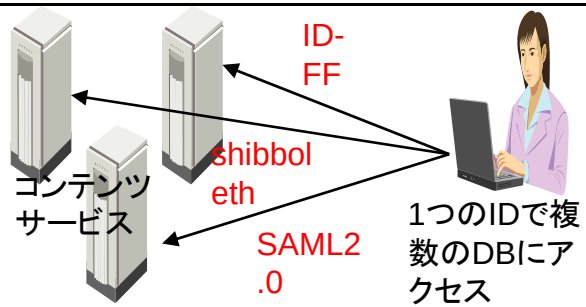
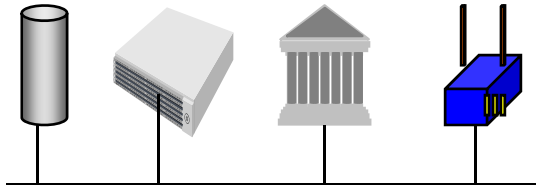
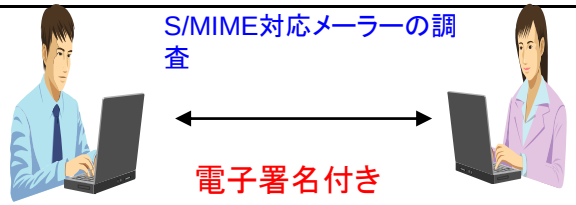
セキュリティを確保した連携を行うには、個人を認識するための認証機能は不可欠

1.2 主なUPKIプロジェクト(1/2)

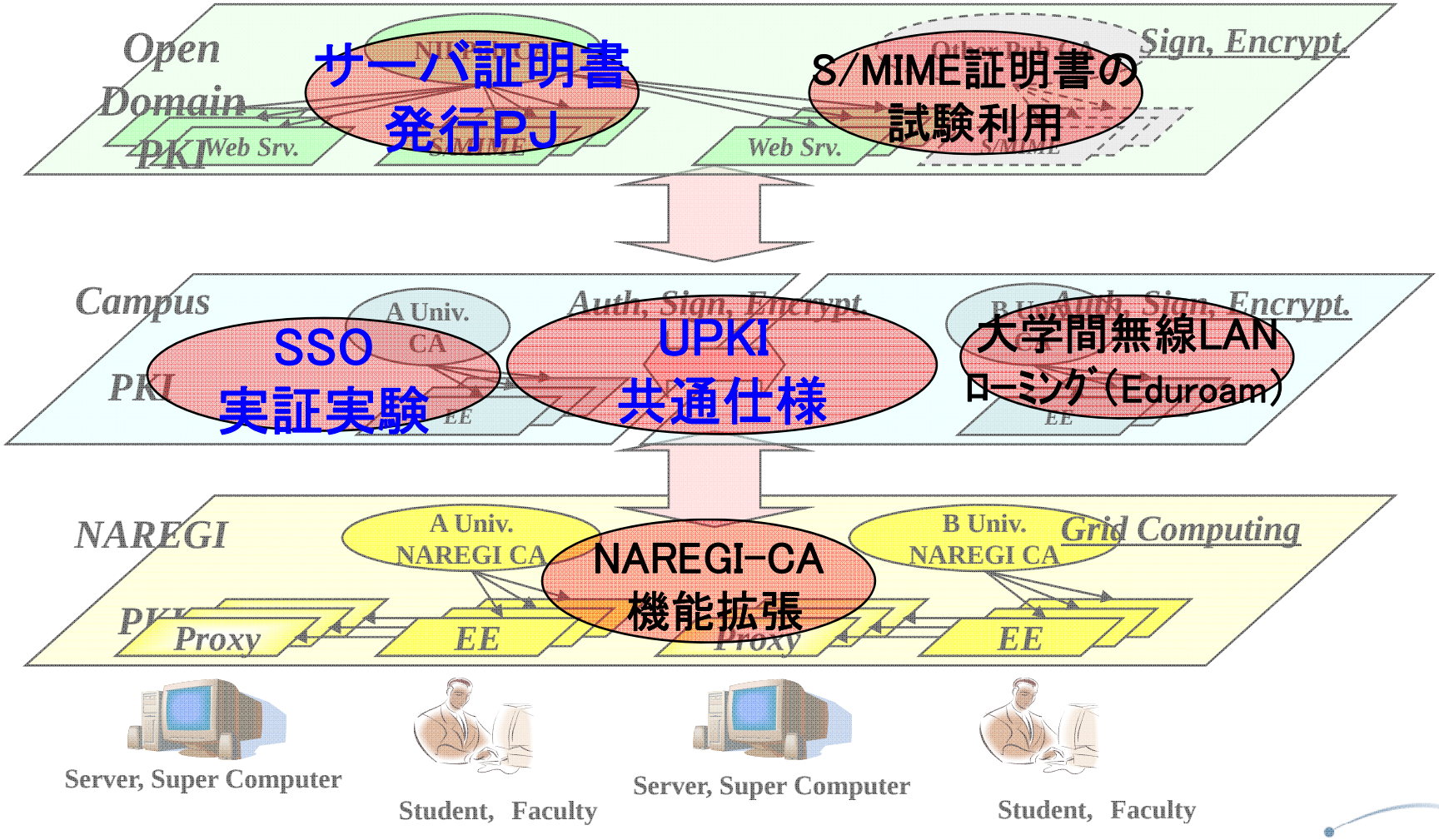
項番	事項	内容
1	「UPKI共通仕様」の作成と配布	 「UPKI共通仕様」の利用により大学での ・学内認証局の構築 ・CP/CPS等の規程の整備 が容易に実現可能に
2	オープンドメイン認証局の構築とサーバ証明書の発行	 オープンドメイン認証局の構築により，全世界に通用するサーバ証明書を発行し，大学のWebサーバの実在性証明と通信の暗号化を実現
3	大学間無線LANローミングの実現 （東北大学が中心）	 eduroamによる大学間無線LANローミングを実現。海外のeduroam参加機関との連携も実現

UPKI initiative

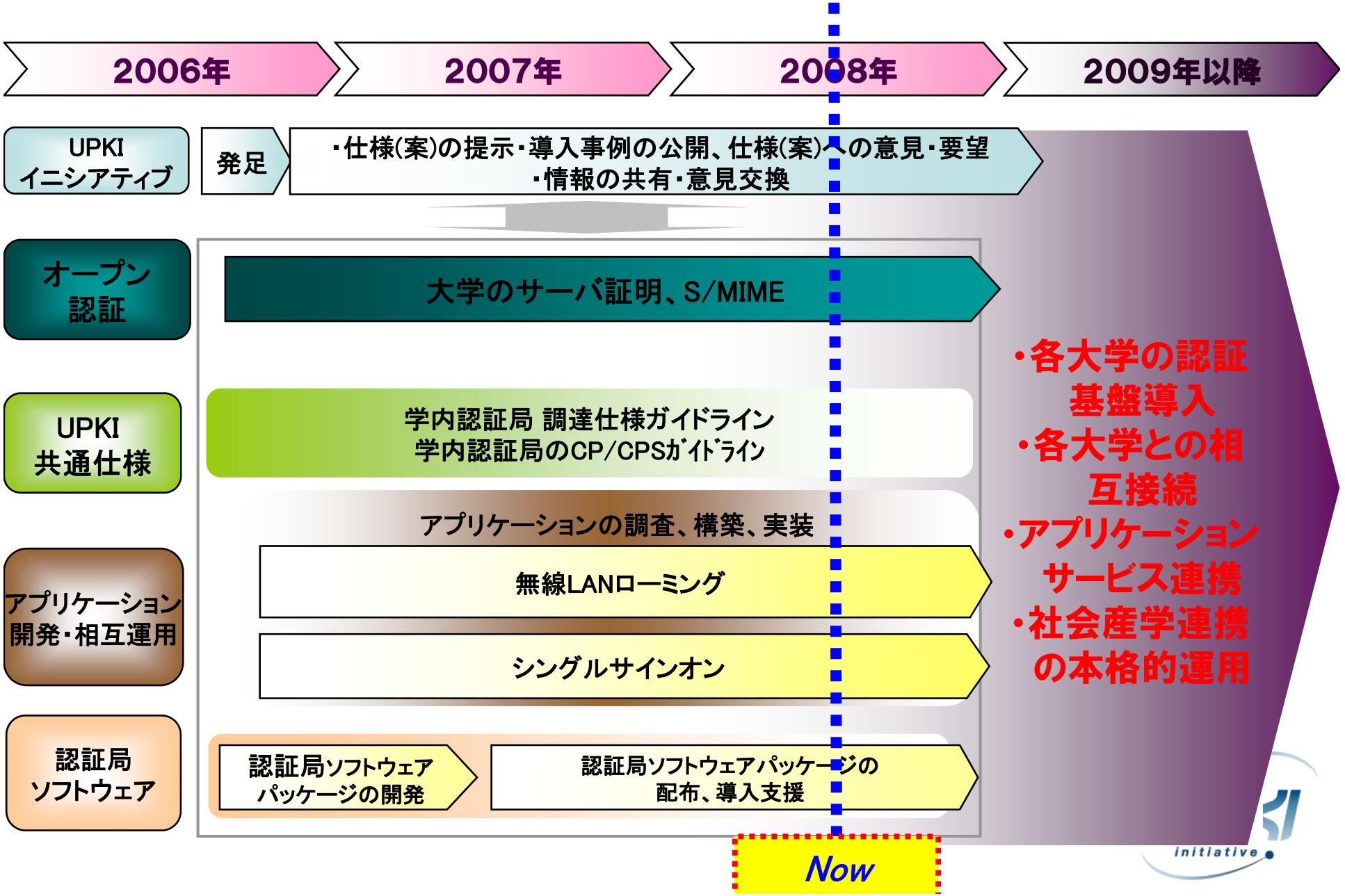
1.2 主なUPKIプロジェクト(2/2)

項番	事項	内容
4	**UPKI認証連携基盤によるシングルサインオン実証実験**	 電子ジャーナル等の利用に用いられているシングルサインオンの技術を用いて，大学間の認証連携の実現する「UPKI認証連携基盤」の構築を計画している。
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

1.2 主なUPKIプロジェクト（アーキテクチャ上にマッピング）



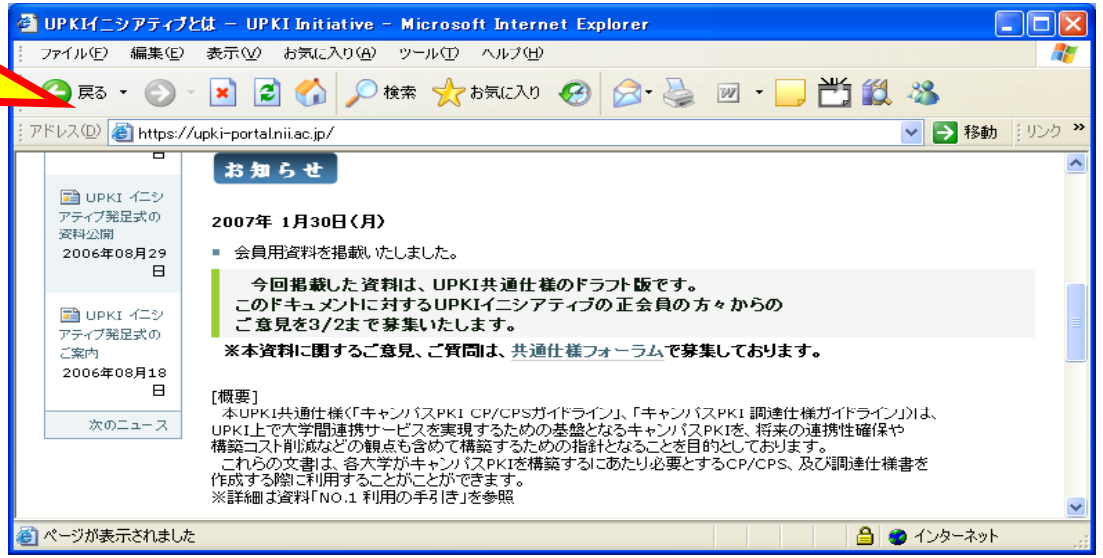
■ UPKI構築の全体スケジュール



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
- オフラインでの勉強会等（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



Agenda

1. UPKI概要
   - 1.1 計画概要（位置づけ、体制、基本ｱｰｷﾃｸﾁｬ）
   - 1.2 主なプロジェクト（共通仕様、ｻｰﾊﾞ証明、SSO連携等）
   - 1.3 UPKIイニシアティブ

2. UPKI共通仕様
   - 2.1 背景・目的・位置づけ
   - 2.2 キャンパスPKIモデル
   - 2.3 キャンパスPKIガイドライン
   - 2.4 （想定）効果

3. CP/CPSガイドライン詳細（インソース編）
   - 3.1 CP/CPSガイドラインの主な項目
   - 3.2 RFC3647との比較
   - 3.3 CP/CPSガイドライン

4. まとめ

2.1 背景・目的・位置づけ

- 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

2.1 背景・目的・位置づけ

「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

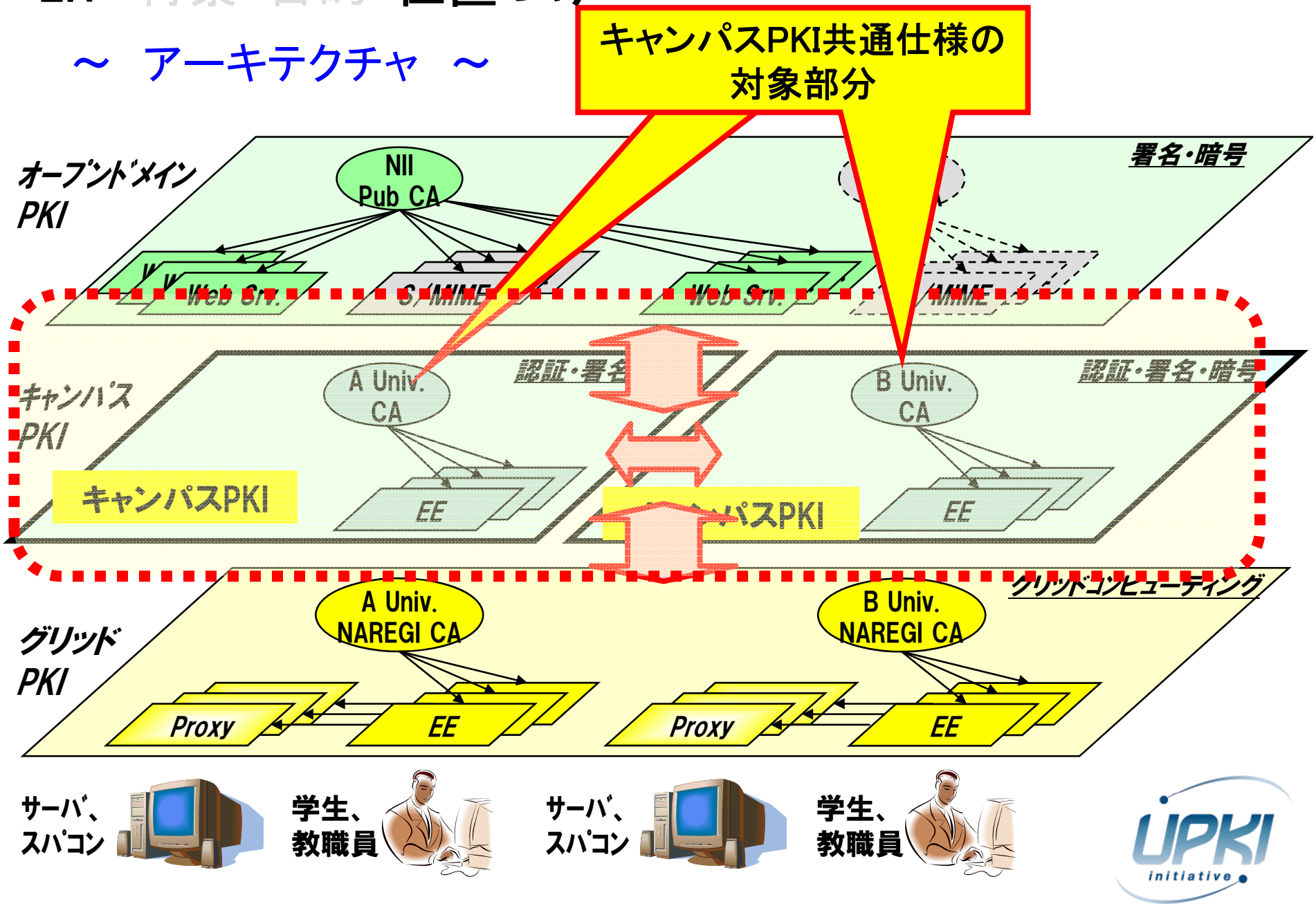
＊＊：コスト削減
- キャンパスPKI導入検討コストの削減
- CP/CPS策定コストの削減

⇒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！！

2.1 背景・目的・位置づけ

～ アーキテクチャ ～



2.1 背景・目的・位置づけ

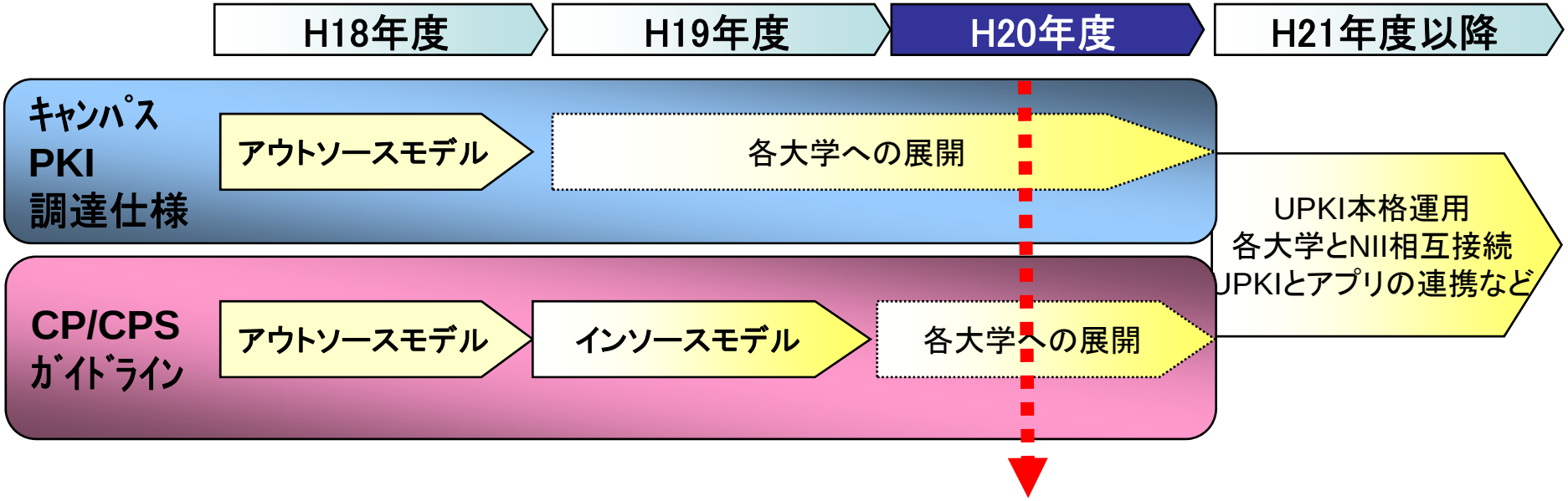
～ 適用領域等 ～

	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

2.1 背景・目的・位置づけ ～ スケジュール ～

- 段階的に展開（3年計画）
  - ◆ これまでにキャンパスPKI共通仕様（アウトソースモデル、インソースモデル）を作成（H18, 19年度）
  - ◆ 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/）

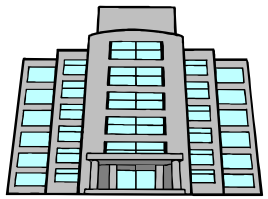


- 今年度は、作成したモデルを大学へ展開するための活動を実施中！

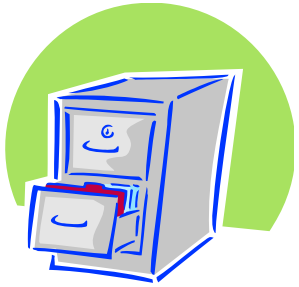
2.2 キャンパスPKIモデル

■ PKIの主な構成要素（1/3）：
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

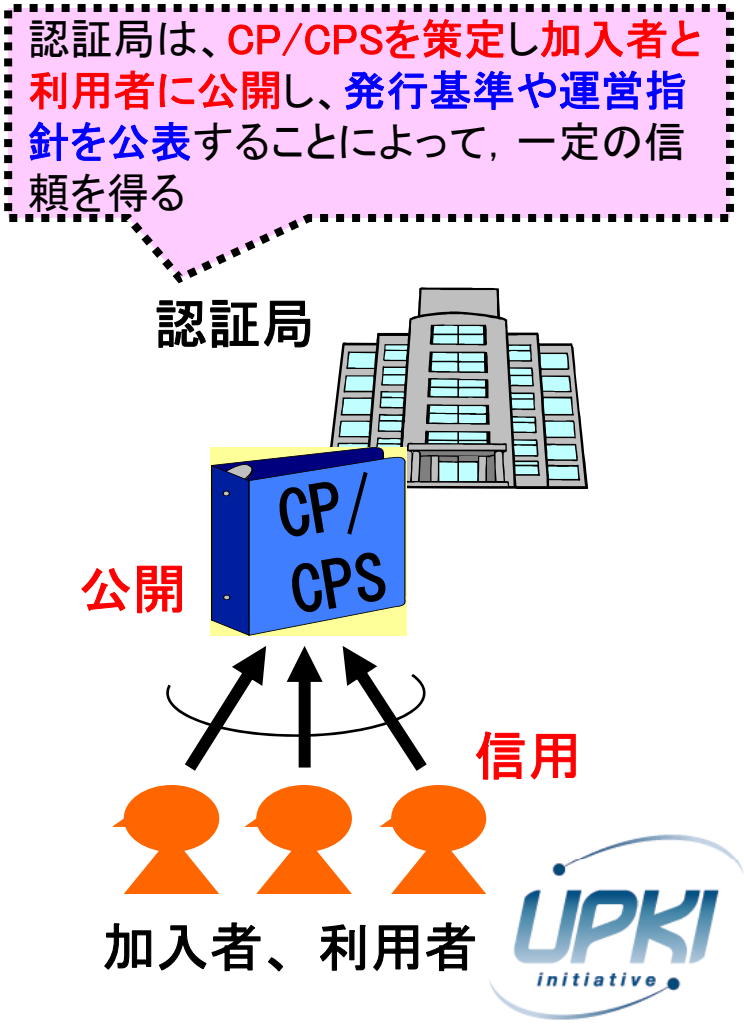
UPKI initiative

2.2 キャンパスPKIモデル

■ PKIの主な構成要素（2/3）：
CP/CPS（証明書ポリシーと認証局運用規程）

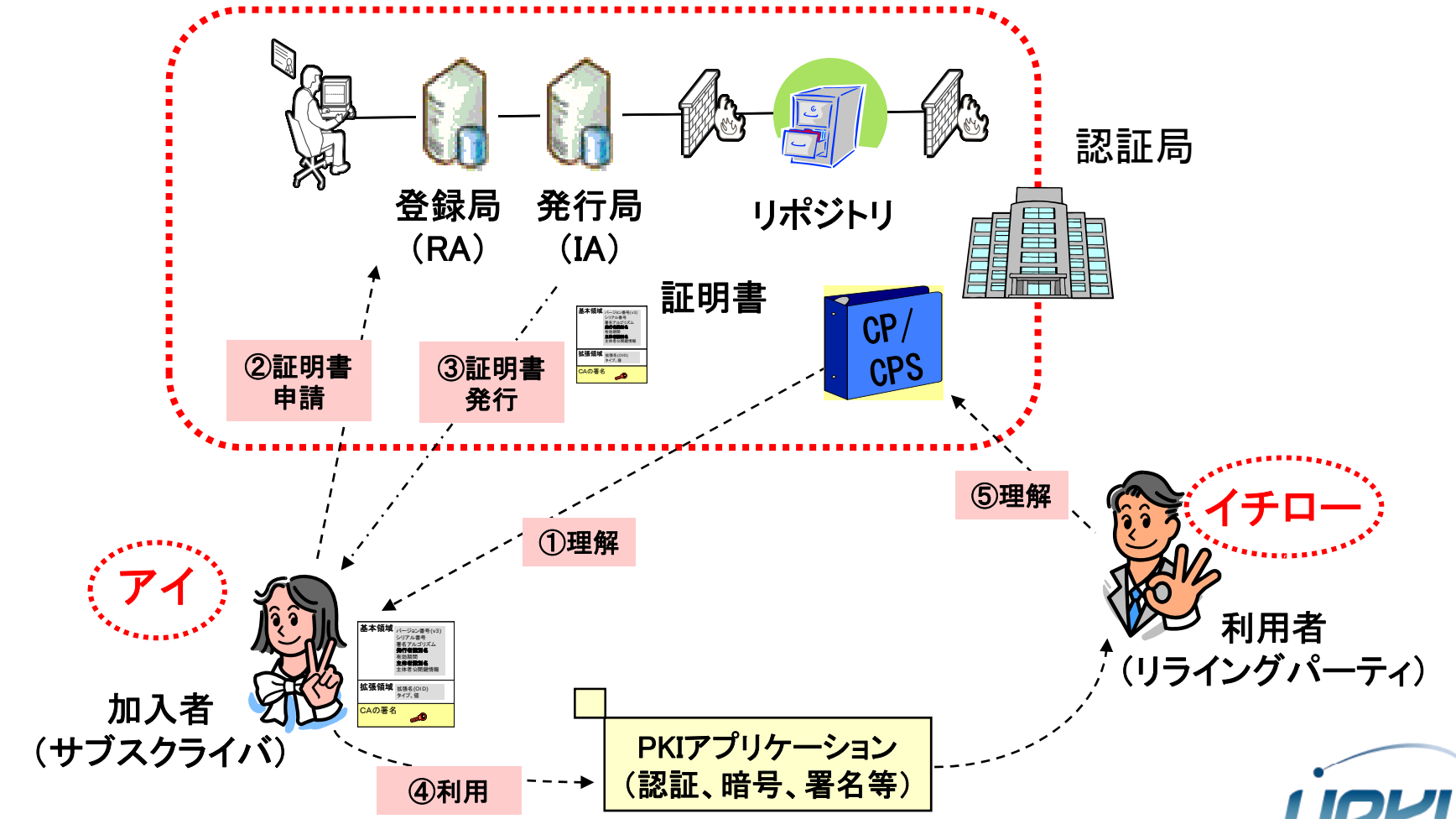
●CP（Certificate Policy）：証明書ポリシー
- 証明書を発行する際の基準。
  身元確認方法や鍵ペアの生成方法、想定するアプリケーションなどを記述したもの。
  一般的には、証明書を発行する認証局毎に定義して用いる。

●CPS（Certification Practice Statement）：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



2.2 キャンパスPKIモデル

■ PKIの主な構成要素（3/3）：
証明書、認証局、リポジトリ、CP/CPS、加入者、利用者



参考：企業システムのためのPKI　公開鍵インフラストラクチャの構築・導入・運用、塚田孝則、日経BP企画、2001

2.2 キャンパスPKIモデル

■ キャンパスPKIの一般的な運用モデル(1/2)

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	●	●	●	△

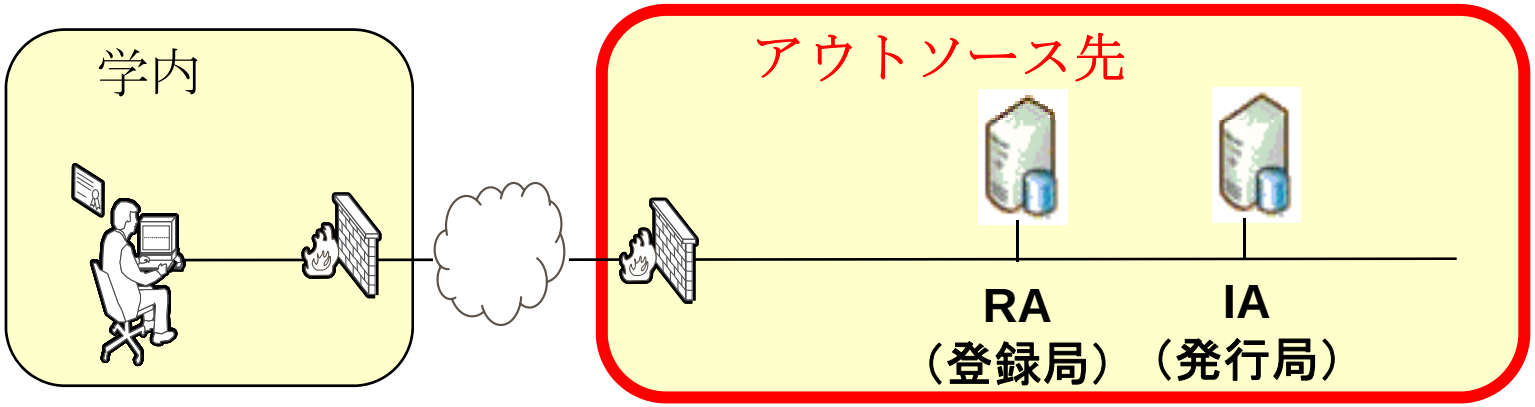
○:アウトソースする、●:インソースする、△:オプションでアウトソースする

※ 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。

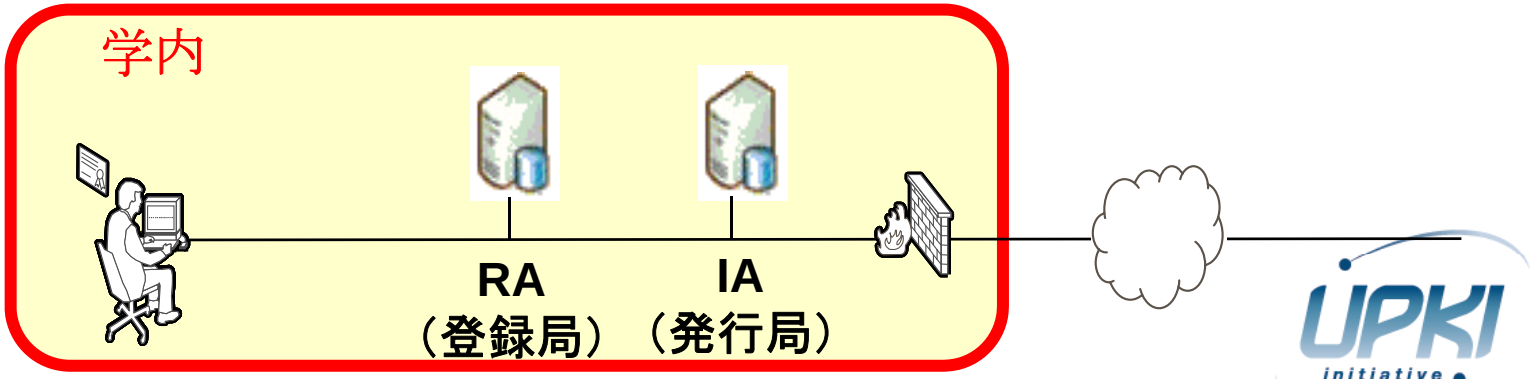
2.2 キャンパスPKIモデル

■ キャンパスPKIの一般的な運用モデル（2/2）

アウトソースモデル（H18年度作成）



インソースモデル（H19年度作成）



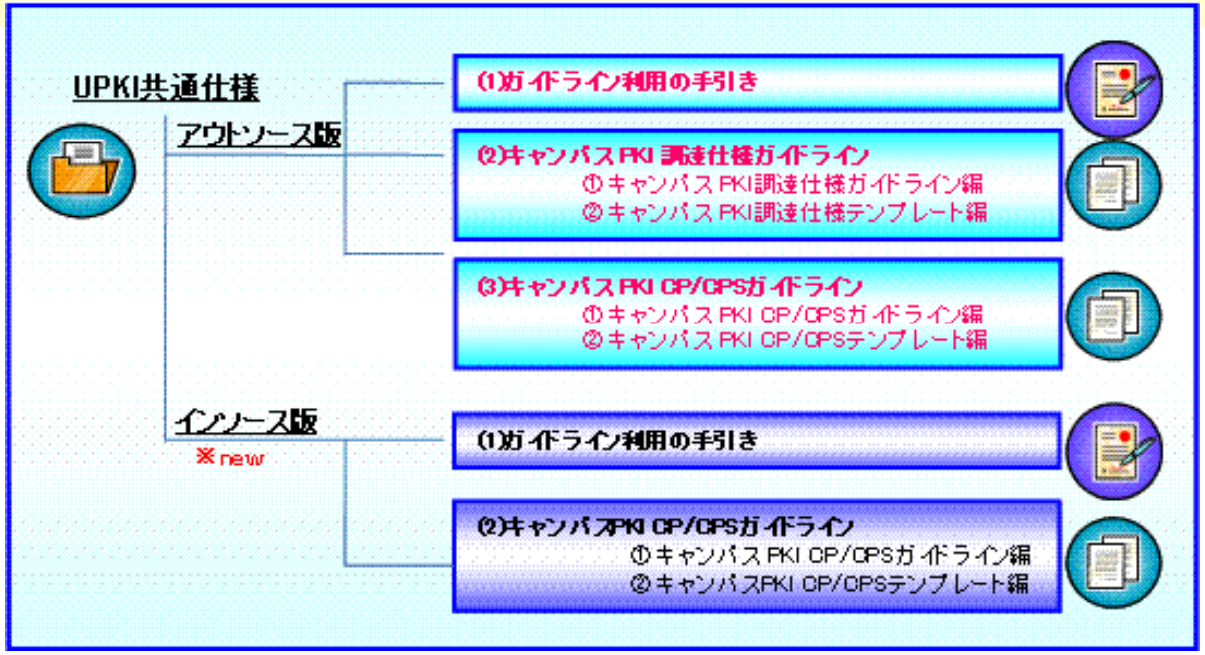
2.3　キャンパスPKIガイドライン

●アウトソースモデル、インソースモデルを対象に、先行大学の調査結果を踏まえ、**UPKI共通仕様**として以下に示すガイドラインを作成した。

(1)特徴：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**

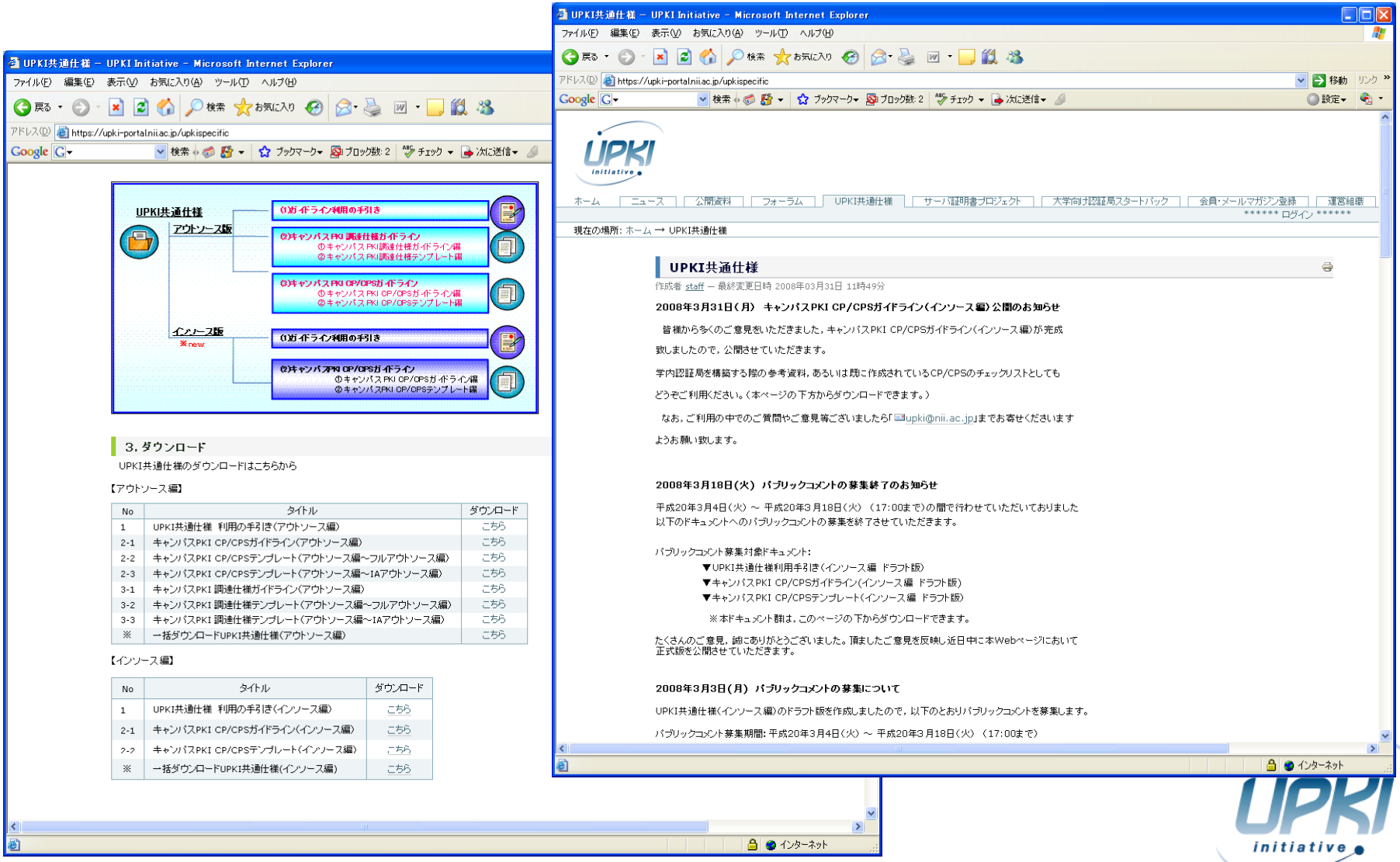
(2) 構成：ガイドラインの構成は、下記のとおり。



2.3 キャンパスPKIガイドライン

■ ダウンロード先（再掲）

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



2.3 キャンパスPKIガイドライン

■ 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、**アウトソースモデル、インソースモデル**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　キャンパスPKIガイドライン

◆　先行大学の調査

アウトソース、インソース共に、**先行大学の調査**を基にして、キャンパスPKIガイドラインの作成を行った。

主な調査項目

1. 認証局階層構造
2. 発行対象者と証明書利用用途
3. 利用者の本人確認と審査登録
4. 利用者の鍵ペア生成と格納媒体
5. 利用者への配付
6. 証明書有効期間
7. 失効情報の提供方法と有効期間
8. 認証局秘密鍵管理
9. 運営に関する指揮命令系統と内部牽制
10. 認証局の職員に対する教育訓練
11. 物理的管理
12. 認証設備室（物理的アクセス）
13. 認証設備室（ファシリティ）
14. ICカード発行室
15. 登録端末設置室
16. 媒体保管場所
17. 施設外のバックアップ
18. 記録する情報とその管理
19. 監査

■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。

2.3 キャンパスPKIガイドライン

■ 調達仕様ガイドライン：主な記述内容（アウトソースのみ）

(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

2.3　キャンパスPKIガイドライン

■（実際の）調達仕様ガイドラインでの記述例

付.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）

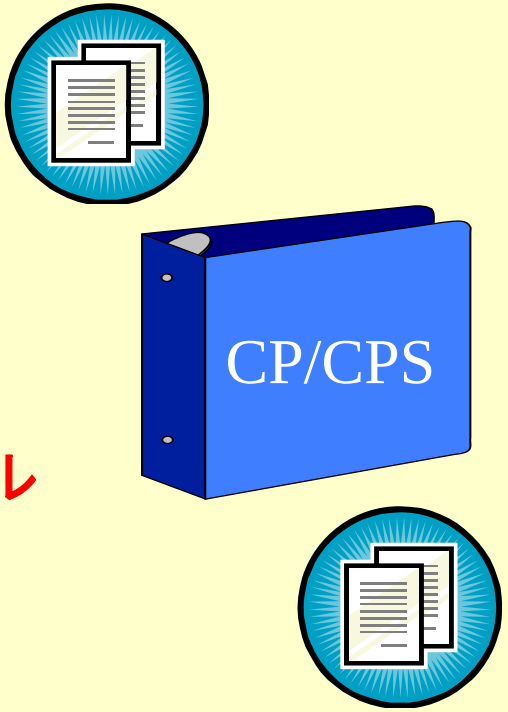
本ガイドラインでは、**認証システム及びICカードに関して必要（★）、ある方が望ましい（☆）**、と思われる要件を示す。各大学の要件に応じて追加すべき内容及び相互認証を行う上で将来的に調整が必要な内容が含まれることに留意すること。

2.3　キャンパスPKIガイドライン

■　CP/CPSガイドライン：主な記述内容

本ガイドラインの記述内容は、**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。主な内容を下記に示す

（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



2.3　キャンパスPKIガイドライン

■（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。

2.4 （想定）効果

- 共通仕様化による効果
  - 費用削減：最初から作成する場合に比べ、調達仕様、CP/CPSに関わる費用削減が可能
  - 期間短縮：先行大学の共通項をモデル化した標準モデル提供により、大学固有部分の検討に集中できるため、大幅に構築期間短縮が可能
- 連携性確保による効果
  - 保証レベルの平準化：単位互換等、大学間連携の際における情報セキュリティ面の問題を解消できる
  - 国際接続：国際的に通用するグリッド用利用者証明書の発行審査にキャンパスPKIから発行された証明書が利用可能に（現在、検討中）

（参考）「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電子情報通信学会 ネットワーク運用ガイドライン」の規程群のうち，認証に関わる部分については，『UPKI共通仕様』が参照されている。

- http://www.nii.ac.jp/csi/sp/doc/sp-sample-fy2007.pdf

Agenda

1. UPKI概要
   - 1.1 計画概要（位置づけ、体制、基本ｱｰｷﾃｸﾁｬ）
   - 1.2 主なプロジェクト（共通仕様、ｻｰﾊﾞ証明、SSO連携等）
   - 1.3 UPKIイニシアティブ

2. UPKI共通仕様
   - 2.1 背景・目的・位置づけ
   - 2.2 キャンパスPKIモデル
   - 2.3 キャンパスPKIガイドライン
   - 2.4 （想定）効果

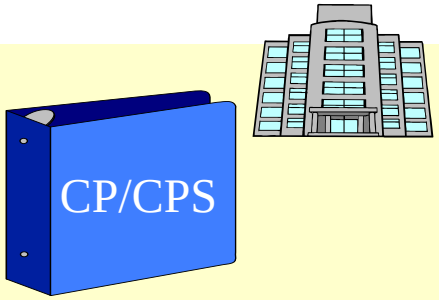
3. CP/CPSガイドライン詳細（インソース編）
   - 3.1 CP/CPSガイドラインの主な項目
   - 3.2 RFC3647との比較
   - 3.3 CP/CPSガイドライン詳細

4. まとめ

3.1　CP/CPSガイドラインの主な項目

■　主な項目（CP/CPSガイドライン）

各項目に対して、CP/CPSガイドラインの解説編を基に説明する。



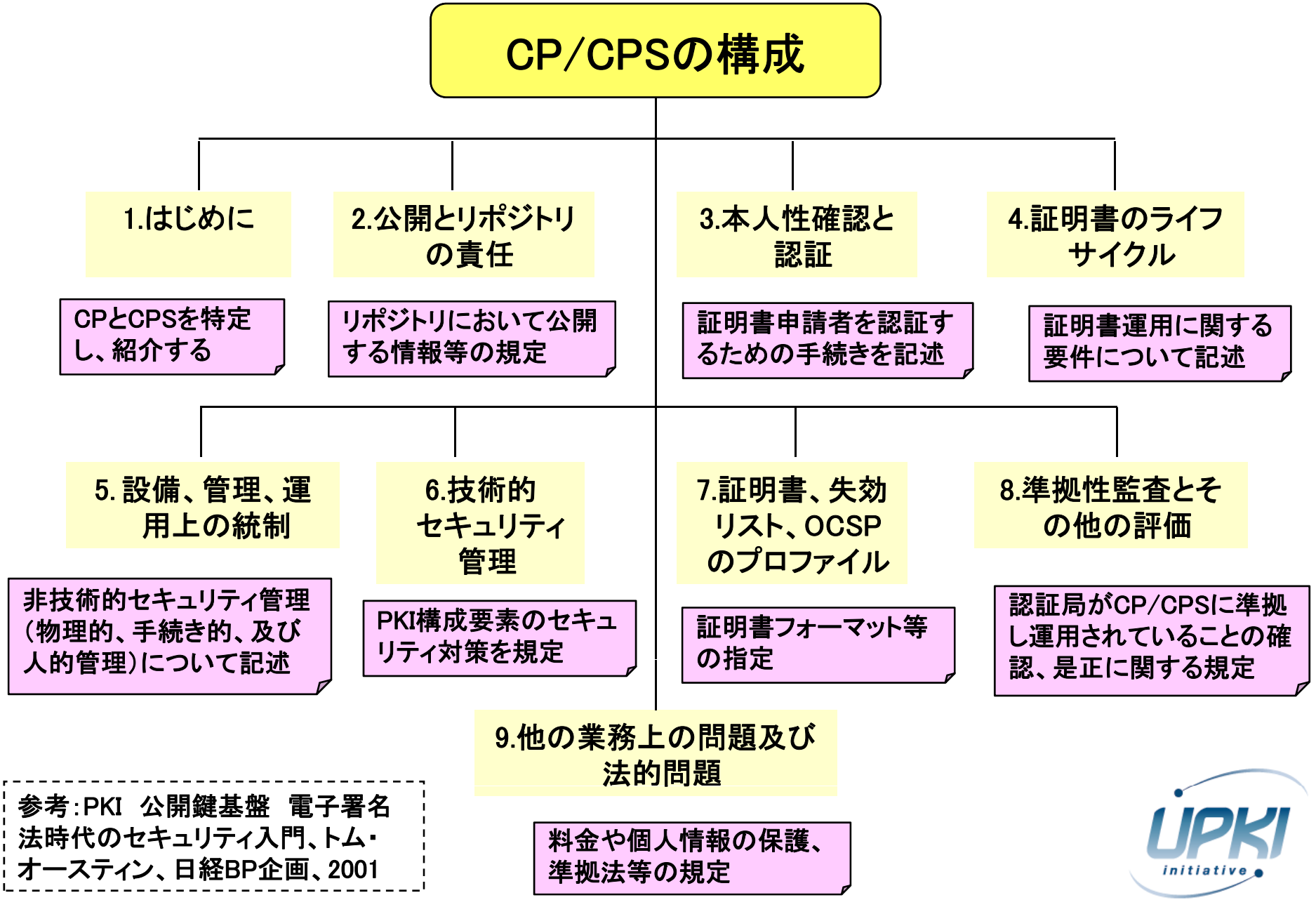
1. はじめに
2. 公開とリポジトリの責任
3. 本人性確認と認証
4. 証明書のライフサイクル
5. 設備、管理、運用上の統制
6. 技術的セキュリティ管理
7. 証明書、失効リスト、OCSPのプロファイル
8. 準拠性監査とその他の評価
9. 他の業務上の問題及び法的問題

3.2　RFC3647との比較

■キャンパスPKI　CP/CPSガイドライン（https://upki-portal.nii.ac.jp/upkispecific）	■IETF RFC3647*（http://www.ietf.org/rfc/rfc3647.txt）
1. はじめに	1. Introduction
2. 公開とリポジトリの責任	2. Publication and Repository Responsibilities
3. 本人性確認と認証	3. Identification and Authentication (I&A)
4. 証明書のライフサイクル	4. Certificate Life-Cycle Operational Requirements
5. 設備、管理、運用上の統制	5. Facility, Management, and Operational Controls
6. 技術的セキュリティ管理	6. Technical Security Controls
7. 証明書、失効リスト、OCSPのプロファイル	7. Certificate, CRL, and OCSP Profiles
8. 準拠性監査とその他の評価	8. Compliance Audit and Other Assessment
9. 他の業務上の問題及び法的問題	9. Other Business and Legal Matters

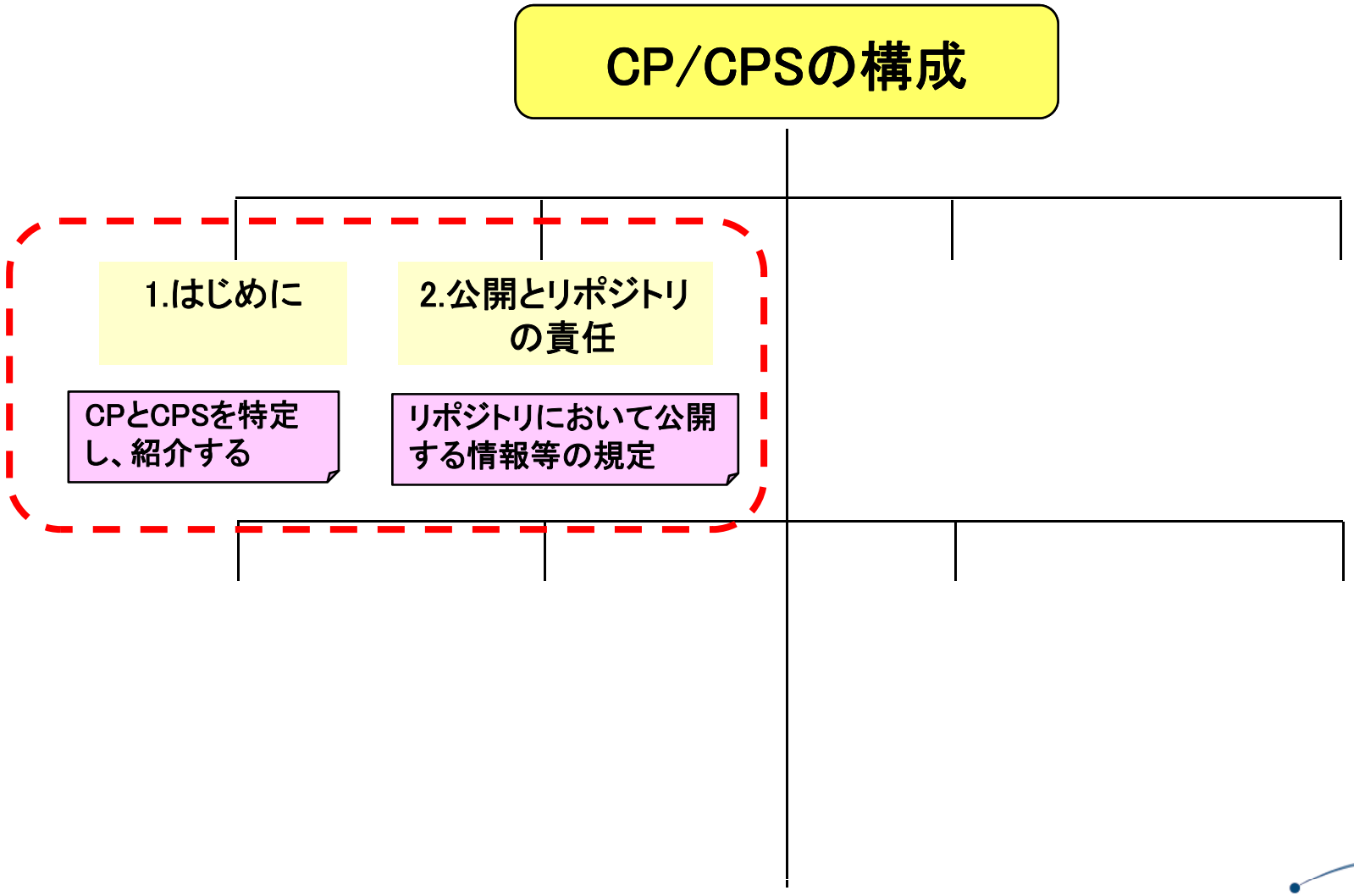
＊：CP/CPSのフレームワークを規定

3.3　CP/CPSガイドライン詳細



参考：PKI　公開鍵基盤　電子署名法時代のセキュリティ入門、トム・オースティン、日経BP企画、2001

3.3　CP/CPSガイドライン詳細



3.3 CP/CPSガイドライン詳細

1. はじめに

IETF RFC3647
1. Introduction

①概要
　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。

②文書名称と定義
　CP/CPSの正式名称を定め、そのポリシーのオブジェクト識別子（OID：Object Identifier）を規定する。

③PKIの関係者
　トラストドメインに登場する関係者を規定し（図解することが望ましい）、また、証明書の発行を受ける者（利用者）の窓口となる部署、連絡先、サポート時間等の規定を行う。

④証明書の用途
　認証局が発行する全ての証明書の種類及び用途や禁止されている用途について規定する。

⑤ポリシー管理
　CP/CPSの管理組織、窓口、ポリシーに対するCPSの準拠性調査担当者、CPSの承認手続きについて規定する。

⑥定義と略称
　用語及び略語の定義を行う。

3.3　CP/CPSガイドライン詳細

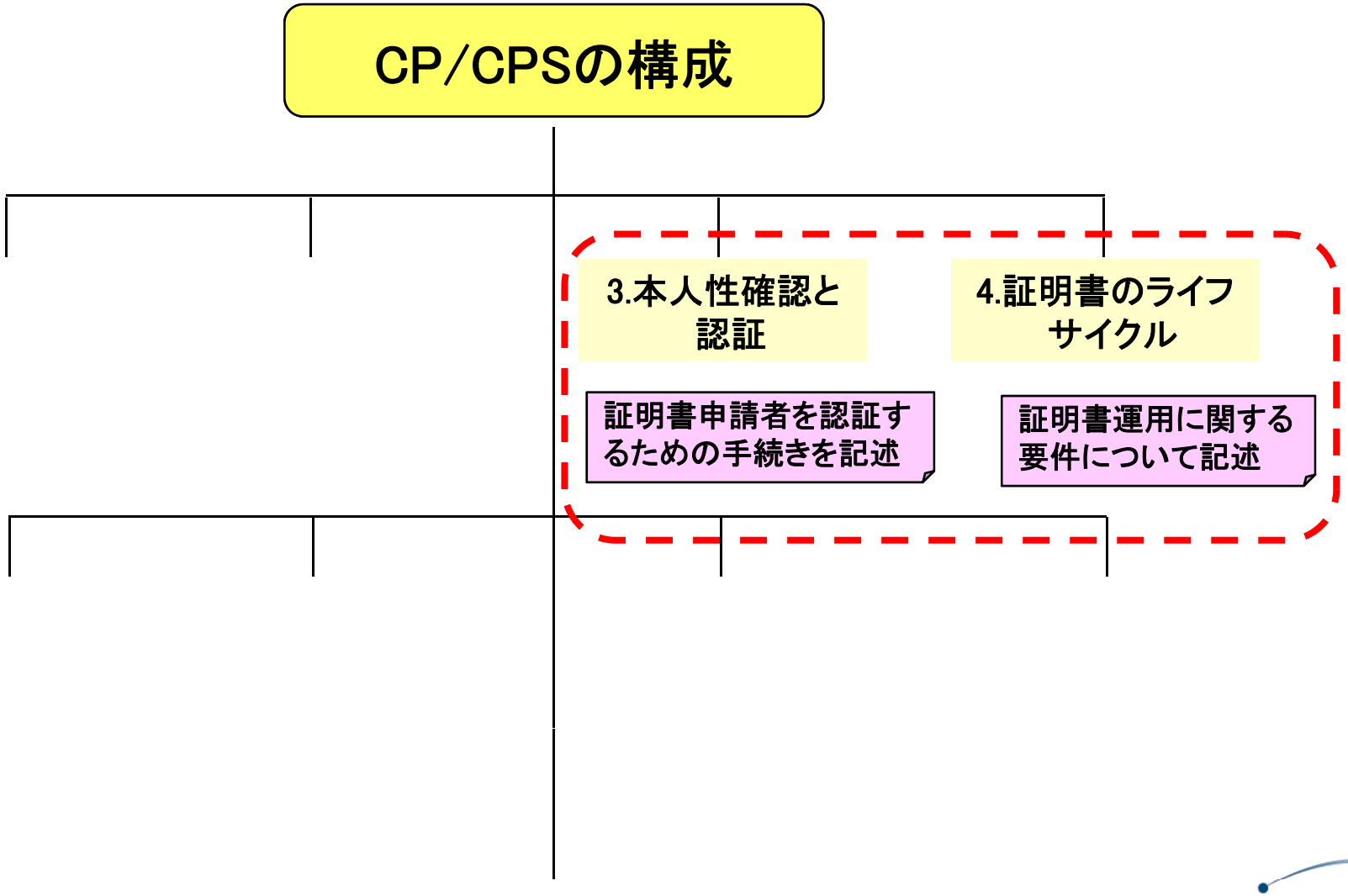
2. 公開とリポジトリの責任

IETF RFC3647
2.　Publication and Repository Responsibilities

- リポジトリにおいて公開する情報、リポジトリのサービス時間、アクセスコントロール等について規定する。

- リポジトリは認証局が利用者及び信頼者に対して公開、通知するために設置されるWebサーバやLDAPサーバ、OCSPサーバ等である。失効情報の公開は通常、Webサーバ、LDAPサーバ、OCSPサーバのどれか、あるいは組合せで実施される。

3.3　CP/CPSガイドライン詳細



3.3　CP/CPSガイドライン詳細

３．本人性確認と認証（1/3）

IETF RFC3647
3.　Identification and Authentication (I&A)

①名称

●利用者証明書に記載するissuerDN及びsubjectDNについて準拠する規格、subjectDNに規定する個人を特定できる情報、利用者の匿名・仮名の許可・不許可等について規定する。

●subjectDNは、認証局の存続期間を通じて同じDNが複数の利用者に使われることがないよう、一意にしなければならない。また、相互認証を行う上で、証明書のみで利用者の氏名あるいは学籍番号を把握するニーズがなければ、subjectDNは一意性が保たれればよく、CN（Common Name）に氏名や学籍番号を記載する必要はない。

3.3 CP/CPSガイドライン詳細

3. 本人性確認と認証(2/3)

② 初回の利用者の本人性確認

- 初回の利用者の確認方法、権限確認、相互運用性基準、更新時の本人性確認について規定する。
- 本人確認時において利用者の秘密鍵の保持を確認する場合があるが利用者に鍵ペアの生成、証明書発行リクエスト(PKCS#10、PKCS#7形式)を実施させず、認証局側で実施する方が利用者に無用な混乱を生じさせないメリットがある。従って、認証局内でセキュアなファシリティ、デュアルコントロールの下で、安全に利用者用鍵ペアを生成する方法を推奨する。
- 利用者の本人確認は、証明書申請時に対面で行うことを推奨するが、入学や採用の際に利用者の本人確認が行われ、利用者本人を特定する情報が学内の信頼できるデータベースにより管理されている場合、そのデータベースを信頼することにより利用者の確認を行うことでも問題ない。

☆ 本人確認において対面審査を実施していれば、より利用者証明書の信頼性が上がり、例えば国際的に通用するグリッド用利用者証明書の発行審査にキャンパスPKIから発行された証明書を利用できる可能性がある。

3.3　CP/CPSガイドライン詳細

3．本人性確認と認証(3/3)

③ 失効申請時の本人性確認と認証

- 利用者が証明書の失効申請を行う場合の利用者の本人性確認と認証について規定する。失効に際しては、ICカードの紛失といった緊急性の高い場合とそうでない場合が存在するため、両方の場合について規定する。

- 緊急失効の際、電話での受付けを行い、コールバックで本人確認を行うことを規定した場合、予め利用者に連絡するための電話番号(研究室電話番号、携帯電話等)を認証局が知る必要があるため、これを安全に入手、管理しておく必要がある。

3.3 CP/CPSガイドライン詳細

4. 証明書のライフサイクル(1/6)

IETF RFC3647
4. Certificate Life-Cycle Operational Requirements

①証明書申請
証明書の申請者、申請方法、登録手続きと責任について規定する。利用者に申請書を提出させ、認証局が登録を行う場合と、利用者が申請したものとみなし、認証局が登録を行う場合とが想定されるが、いずれも発行すべき利用者本人に対し、確実に証明書の発行を行えるよう規定する必要がある。

②証明書申請手続き
申請手続きの際の本人性確認について規定する。更に、証明書申請の承認または却下の条件、証明書申請の処理時間について規定する。

3.3 CP/CPSガイドライン詳細

4. 証明書のライフサイクル(2/6)

③ 証明書発行

- 証明書発行時の認証局、登録局の行為及び利用者に対する証明書の発行通知に関して規定する。
- 利用者の証明書格納媒体として、ICカード、利用者の利用するコンピュータ、PKIに対応したUSBトークン等が考えられる。しかし、利用者PCではその利用が固定的になる等の問題があり、USBトークンではパーソナライズや大量発行に向かないといった問題が生じる。本ガイドラインでは認証局において利用者の鍵生成を行い、証明書発行後、ICカードへの格納を行うことを推奨している。
- ICカード及びICカードPINの配布方法は、対面もしくは配送が考えられるが、配送で行う場合には配送手段(学内便、郵送)についても詳細に規定しなければならない。郵送の場合には、配達記録郵便や書留郵便などの配送記録が確認できるサービスを利用することが必要であり、学内便の場合には、配送途中の紛失や盗難等が生じないような対策をとるとともに、郵送の場合と同様に本人に確実に届くような工夫が必要である。

3.3　CP/CPSガイドライン詳細

4．証明書のライフサイクル（3/6）

④証明書受領
- ●利用者が証明書を受領した際の受領確認手続き、認証局が発行した利用者証明書をリポジトリ等で公開するか否か、利用者以外に証明書の発行の通知を行うかを規定する。

⑤鍵ペアと証明書の用途
- ●利用者が自身の利用者秘密鍵と証明書の使用を行う際の用途、信頼者が利用者の公開鍵と証明書を使用する際の用途について規定する。

⑥鍵更新を伴わない証明書の更新
- ●鍵更新を伴わない証明書の更新は混乱を伴うことが予想されるため、一般的には実施されることは少ない（リンク証明書の場合実施しているケースがある）。従って、明確な理由がない限り、本節は鍵ペアを更新することを規定する。

3.3　CP/CPSガイドライン詳細

4．証明書のライフサイクル（4/6）

⑦鍵更新を伴う証明書の更新
　鍵更新及び証明書の更新時の手続きについて規定する。

⑧証明書の変更
　基本的には証明書の変更に関して規定するが、ICカードの券面の変更に際しても同様の処理を行う場合は、変更条件として明記する。
　本人を特定できることが前提であるが、証明書及びICカードの券面情報の変更は必須事項でなく、希望者のみという運用でも問題ないと考えられる。

3.3　CP/CPSガイドライン詳細

4．証明書のライフサイクル（5/6）

⑨証明書の失効と一時停止

- ●証明書は、利用者、認証局のそれぞれの失効事由により失効するため、それぞれについて規定する。想定されていない失効事由が発生した場合、認証局責任者の判断に基づき証明書を失効できるよう規定しておく必要がある。
- ●また、ICカードの紛失等、緊急を要する失効手続きとそうでない場合の手続きについて違いがある場合は、それについても規定する必要がある。
- ●証明書失効リスト（CRL/ARL）の発行にあたっては、24時間ごとに48時間有効な証明書発行リストを発行することを推奨する。（*1）

*1　既に稼動中の認証局などにおいて、CRLの発行頻度24時間、有効期間48時間とすることが困難な場合には、それに限りなく近い時間で運用するよう努めることが望ましい。尚、将来的な相互認証にあたって、相互認証先とCRLの発行頻度及び有効期間に大きな相違がある場合、信頼性に影響を与えることから相互認証の可否や証明書の利用用途等に関して、予め相互認証先との調整が必要となる。

3.3 CP/CPSガイドライン詳細

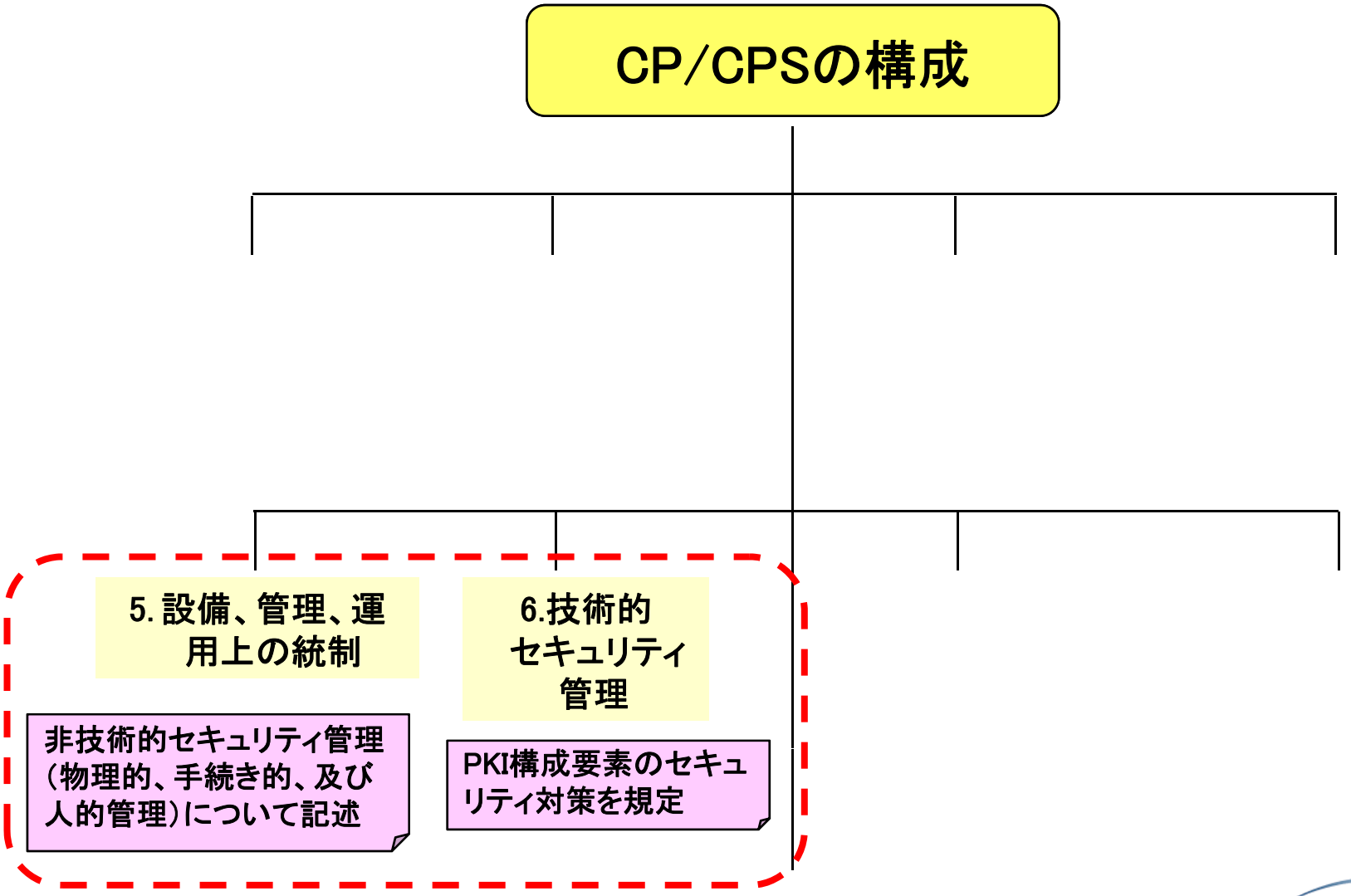
4. 証明書のライフサイクル(6/6)

⑩ 証明書のステータス確認サービス
- CRL/ARL及びOCSPレスポンダによる証明書のステータス確認について規定する。

11 利用の終了
- 利用者が退職、退学等により証明書の利用を終了する際の手続きについて規定する。

12 キーエスクローとリカバリ
- 利用者の鍵のエスクロー(預託)、リカバリ(回復)について規定する。キーエスクローとリカバリのサービスは、認証局が利用者の鍵の複製を保管し、利用者、あるいは大学が認めた者に対し、必要な時(鍵データが破損した場合、暗号を復号したい場合等)に複製を提供するサービスである。
- キャンパスPKIを暗号の用途で用いていない現状では、このようなサービスを提供する意義は少なく、安全性を一定レベルに維持するためには、運用上も煩雑であるため、提供しないことが望ましい。

3.3　CP/CPSガイドライン詳細



3.3 CP/CPSガイドライン詳細

5. 設備、管理、運用上の統制(1/4)

IETF RFC3647
5. Facility, Management, and Operational Controls

①物理的管理

- ●認証局を構成する重要な設備の設置場所について、その立地や構造、様々な設備について規定する。インソースで運用する場合、以下の例に示すセキュリティレベルやファシリティの施設を備えることが必須である。
- ●認証局を構成する重要な設備(認証設備)は、隔壁により独立した専用の部屋に設置することが望ましい。他システムとの共通の部屋内に設置する場合には、共用の部屋(認証設備室)及び認証設備へのアクセス管理を行う必要がある。
- ●認証設備を収容する建物及び部屋は、停電対策、空調管理、水害対策、火災対策及び地震対策を施すことが必要である。
- ●オフサイトバックアップについては必須としないが、大規模な障害や災害に備える必要はある。オフサイトバックアップに加え、ローカルでのバックアップや二重化等の要件は各大学において判断する必要がある。

3.3 CP/CPSガイドライン詳細

5. 設備、管理、運用上の統制(2/4)

②手続き的管理
- ●認証局における役割に応じ、必要な最低人数、兼務の可否等を規定する。フォーカスすべきポイントは、内部牽制が出来ているかどうかであり、不正が起こりえる手続きを回避する必要がある。
- ●認証局の運営に責任を持つ者として認証局責任者を配置し、認証局の運営に関する最高意思決定機関を設置することは必須である。

③人事的管理
- ●CP/CPSで規定(手続き的管理)した職制の要員に対する要件及び教育に関する要件を規定する。

④監査ログの手続き
- ●監査対象となる記録の種類、保管期間、記録の保護等について規定する。証明書の発行及び失効といった重要なイベントに関する記録、運用規程や下位文書に関する記録、体制及び契約に関する記録、監査に関する記録は重要な記録であるため、これらの保管期間、バックアップ、保護について規定する必要がある。

3.3 CP/CPSガイドライン詳細

5. 設備、管理、運用上の統制(3/4)

⑤ 記録のアーカイブ
- 監査ログとして定義された記録に加え、保管対象となるデータ、文書を規定し、規定したそれぞれについて保管期間及び保護に関する規定を行う。

⑥ 鍵の切り替え
- 認証局の秘密鍵に関する鍵更新について規定する。認証局は鍵更新に際して新たな証明書の発行を行うが、この時リンク証明書を発行し、認証局の世代管理を行う場合がある。リンク証明書は、古い鍵で新しい証明書に電子署名を行い、新しい鍵で古い証明書に電子署名を行った2つの証明書からなる。リンク証明書が発行されれば、旧認証局と新認証局が同じ認証局であることを表明することができ、操作についても新しい認証局で古い認証局から発行された証明書を失効する等が出来る。

3.3　CP/CPSガイドライン詳細

５．設備、管理、運用上の統制（4/4）

⑦危殆化及び災害からの復旧
- ●システム的な障害、自然災害、認証局の秘密鍵の危殆化といった障害、災害が発生した際の手続き及び復旧に関する手続きについて規定する。
- ●重要な認証設備及び失効情報を提供するリポジトリ等については、各大学において、バックアップ要件、二重化要件を定め、障害復旧のための手続きを規定しておくことを推奨する。

⑧認証局の業務終了
- ●認証局が業務を終了する際の手続きについて規定する。
  （例）本認証局が認証業務を廃止する場合、廃止日の3 ヶ月前までにリポジトリ上で告知、あるいは利用者に対し書面による通知を行う。

3.3 CP/CPSガイドライン詳細

6. 技術的セキュリティ管理

IETF RFC3647
6. Technical Security Controls

① 鍵ペアの生成及びインストール
利用者及び認証局の鍵生成、秘密鍵、及び公開鍵の配付、認証局証明書の配付、鍵サイズや品質検査について規定する。

② 秘密鍵の保護及び暗号モジュール技術の管理
認証局秘密鍵及び利用者の秘密鍵についての保護、エスクロー、バックアップ、活性化・非活性化、破棄について規定する。

③ その他の鍵ペア管理
認証局証明書並びに利用者証明書のアーカイブ及び使用期間に関して規定

④ 活性化データ
認証局及び利用者の秘密鍵の活性化情報の作成、設定、保護等に関し規定

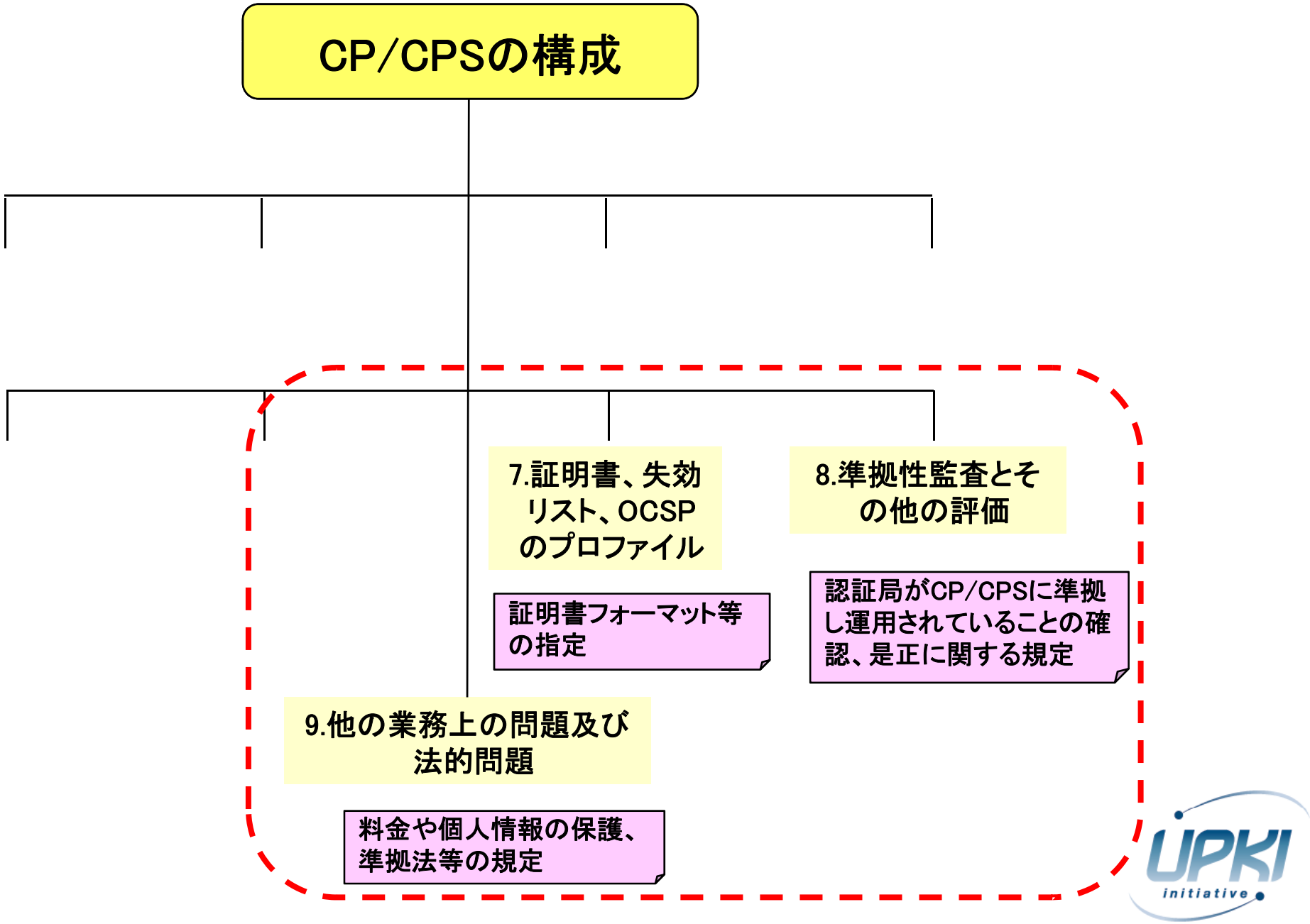
⑤ コンピュータのセキュリティ管理
認証設備等に用いられるソフトウェアに関する技術的要件等の要件を規定

⑥ ライフサイクルの技術上の管理
システム開発におけるライフサイクル、運用管理、当に関する要件を規定

⑦ ネットワークセキュリティ管理
ネットワークセキュリティに関する要件を規定する。

⑧ タイムスタンプ
日時の記録に関する要件を規定する。

3.3　CP/CPSガイドライン詳細



3.3　CP/CPSガイドライン詳細

7．証明書、失効リスト、OCSPのプロファイル（1/2）

IETF RFC3647
7.　Certificate, CRL, and OCSP Profiles

①証明書プロファイル
　認証局証明書、利用者証明書のプロファイルに関する要件を規定する。
　本節で規定せず、付録や別紙として記載することも可能である。
②CRL、ARLプロファイル
　ARL/CRLのプロファイルに関する要件を規定する。
③OCSPプロファイル
　OCSPのプロファイルに関する要件を規定する。OCSPを利用しない認証局は規定する必要はない。

3.3 CP/CPSガイドライン詳細

7. 証明書、失効リスト、OCSPのプロファイル(2/2)

【記述例】 **証明書プロファイル**

7.1.1 バージョン番号

本認証局は、X.509 バージョン3 に準拠した自己署名証明書、相互認証証明書、利用者証明書を発行する。

7.1.2 証明書拡張領域

本認証局は、X.509 で定義された拡張領域を利用する。利用する拡張領域については別紙に示す。

7.1.3 アルゴリズムオブジェクト識別子

本認証局が発行する自己署名証明書、相互認証証明書、利用者証明書、CRL/ARL における電子署名アルゴリ ズムはSHA-1WithRSAEncryption (OID=1 2 840113549 1 1 5)である。各証明書に記載される主体者の公開鍵のアルゴリズムは、RSA(OID=12 840 113549 1 1 1)である。

▪

▪

▪

3.3 CP/CPSガイドライン詳細

8. 準拠性監査とその他の評価

IETF RFC3647
8. Compliance Audit and Other Assessment

- 認証局がCP/CPSに準拠し運用がなされていることを確認、是正するために行う準拠性監査について規定する。具体的には、監査の頻度、監査人の要件、監査の範囲、是正処置等について規定する。

9. 他の業務上の問題及び法的問題

IETF RFC3647
9. Other Business and Legal Matters

- 料金や個人情報の保護、トラストドメイン内の関係者毎の保証内容、補償、改訂手続き、紛争時の解決手段、準拠法等について規定する。

Agenda

1. UPKI概要
   - 1.1 計画概要（位置づけ、体制、基本ｱｰｷﾃｸﾁｬ）
   - 1.2 主なプロジェクト（共通仕様、ｻｰﾊﾞ証明、SSO連携等）
   - 1.3 UPKIイニシアティブ

2. UPKI共通仕様
   - 2.1 背景・目的・位置づけ
   - 2.2 キャンパスPKIモデル
   - 2.3 キャンパスPKIガイドライン
   - 2.4 （想定）効果

3. CP/CPSガイドライン詳細（インソース編）
   - 3.1 CP/CPSガイドラインの主な項目
   - 3.2 RFC3647との比較
   - 3.3 CP/CPSガイドライン

4. まとめ

4. まとめ

■UPKIの概要
- ➢H18年度から3年計画
- ➢主なプロジェクト
  - ➢UPKI共通仕様
  - ➢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
  - ➢UPKI認証連携基盤によるシングルサインオン実証実験
- ➢UPKIイニシアティブ

■UPKI共通仕様
- ➢キャンパスPKIモデル
  - ☆アウトソースモデルとインソースモデル
  - ☆調達仕様、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～:アウトソース編
  - ☆H20/3/31～:インソース編

■CP/CPSガイドライン詳細(インソース編)
- ➢CP/CPSガイドラインの各項目について紹介