大学間連携のための全国共同電子認証基盤 UPKIにおける認証連携方式の検討

2006年5月24日

国立情報学研究所
島岡　政基
谷本 茂明、片岡 俊幸、峯尾 真一、曽根原 登
寺西 裕一、飯田 勝吉、岡部 寿男

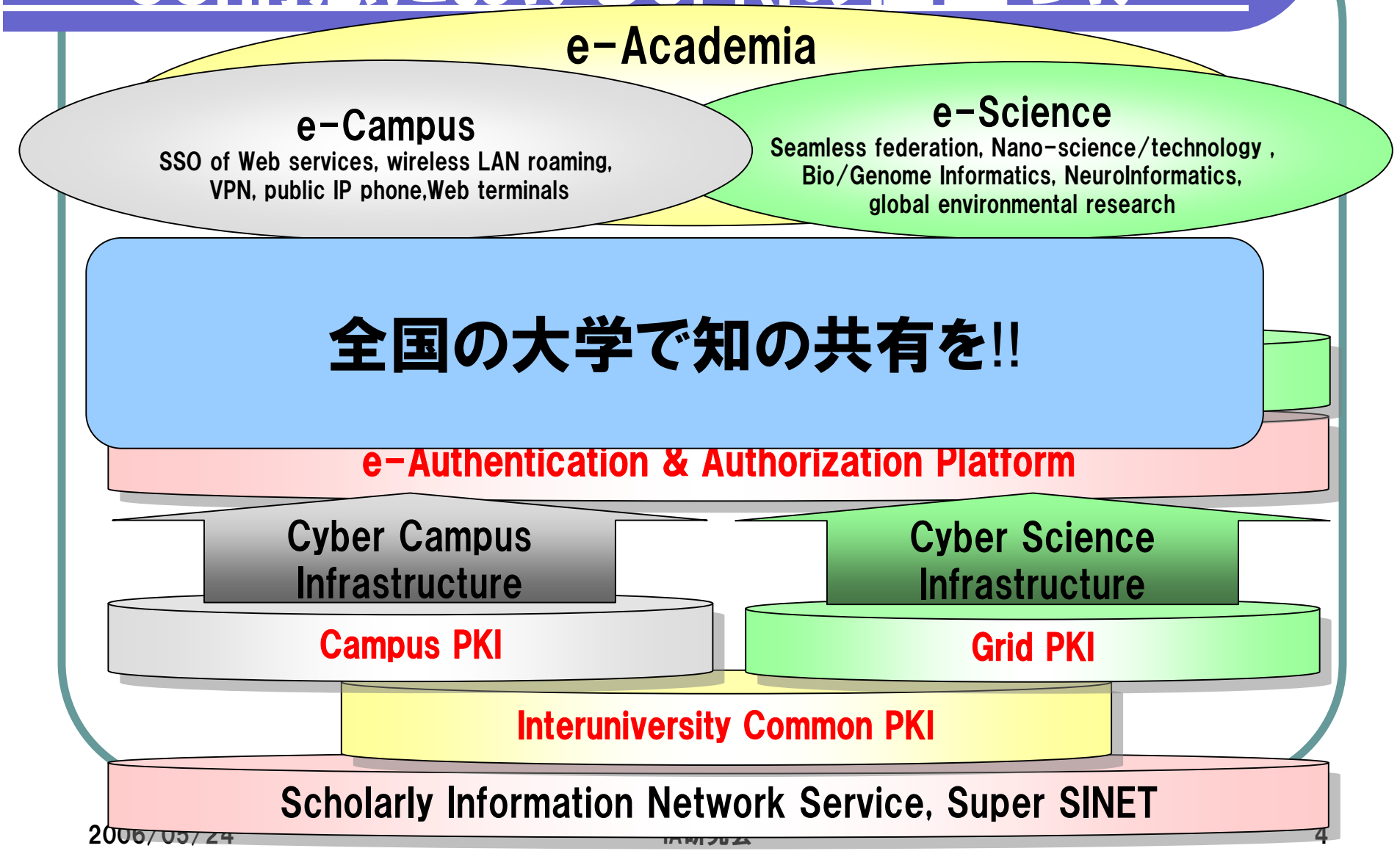
本日の概要

- UPKIの背景とモチベーション
  - CSIを支えるUPKI
  - UPKIにおけるサービス展開
- 大学界へPKIを適用していくには?
  - 大学特有の課題が沢山
  - 様々な多様性への対応
    - セキュリティポリシ、セキュリティレベルの多様性
    - 認証基盤の多様性、などなど
- 具体的な課題の抽出
  - 信頼点の設定、ドメイン構造、認証連携方式
- 今後のアプローチ
  - UPKI相互運用フレームワークの確立を目指して

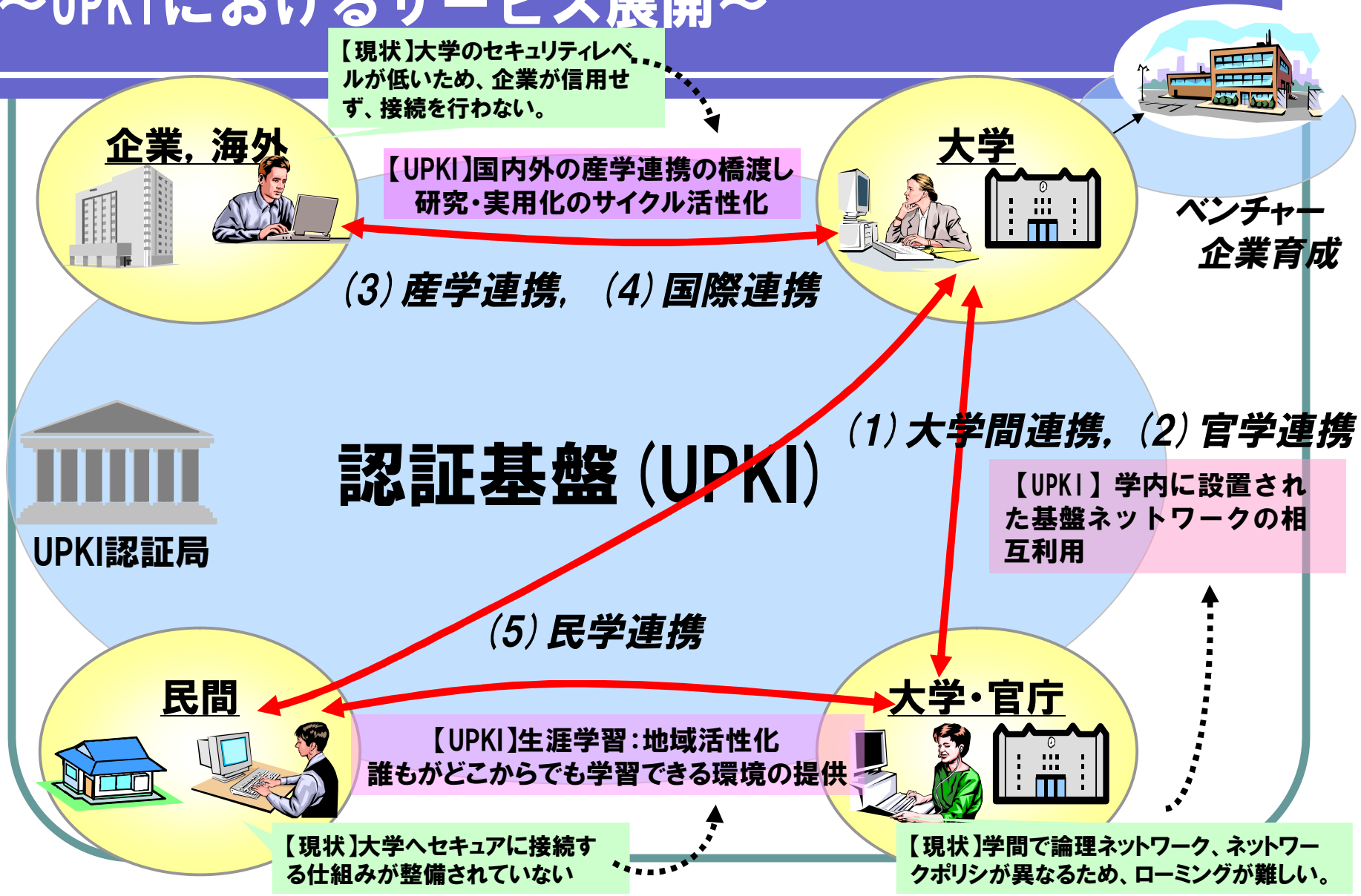
背景とモチベーション（1）

- セキュリティニーズの増加
  - 情報セキュリティポリシとコンプライアンス
  - 大学のセキュリティガバナンス
  - 政府機関の情報セキュリティ対策のための統一基準
- ID・パスワードからPKIへ
  - 銀行などでは2要素認証への移行が進みつつある
    - 記憶だけでなく、所持と記憶

背景とモチベーション(2)
～CSI構想におけるUPKIの位置づけ～



背景とモチベーション(3)
～UPKIにおけるサービス展開～



大学へ適用していくには…

- 大学特有の背景
  - 大学特有の事情・文化…
    - 少子化、産学連携、セキュリティコンプライアンス
  - 大学間の多様性

PKIと多様性の難しさを克服するために皆でノウハウを共有

- 認証レイヤでの課題
  - 高価な研究施設の共同利用
    - NW経由での利用には認証連携が不可欠
  - UPKIのアプリケーション
    - 科学技術計算、学術コンテンツ、高等教育、学術ネットワーク
  - 3層の認証基盤
    - グリッド認証基盤、キャンパス認証基盤、オープンドメイン認証基盤

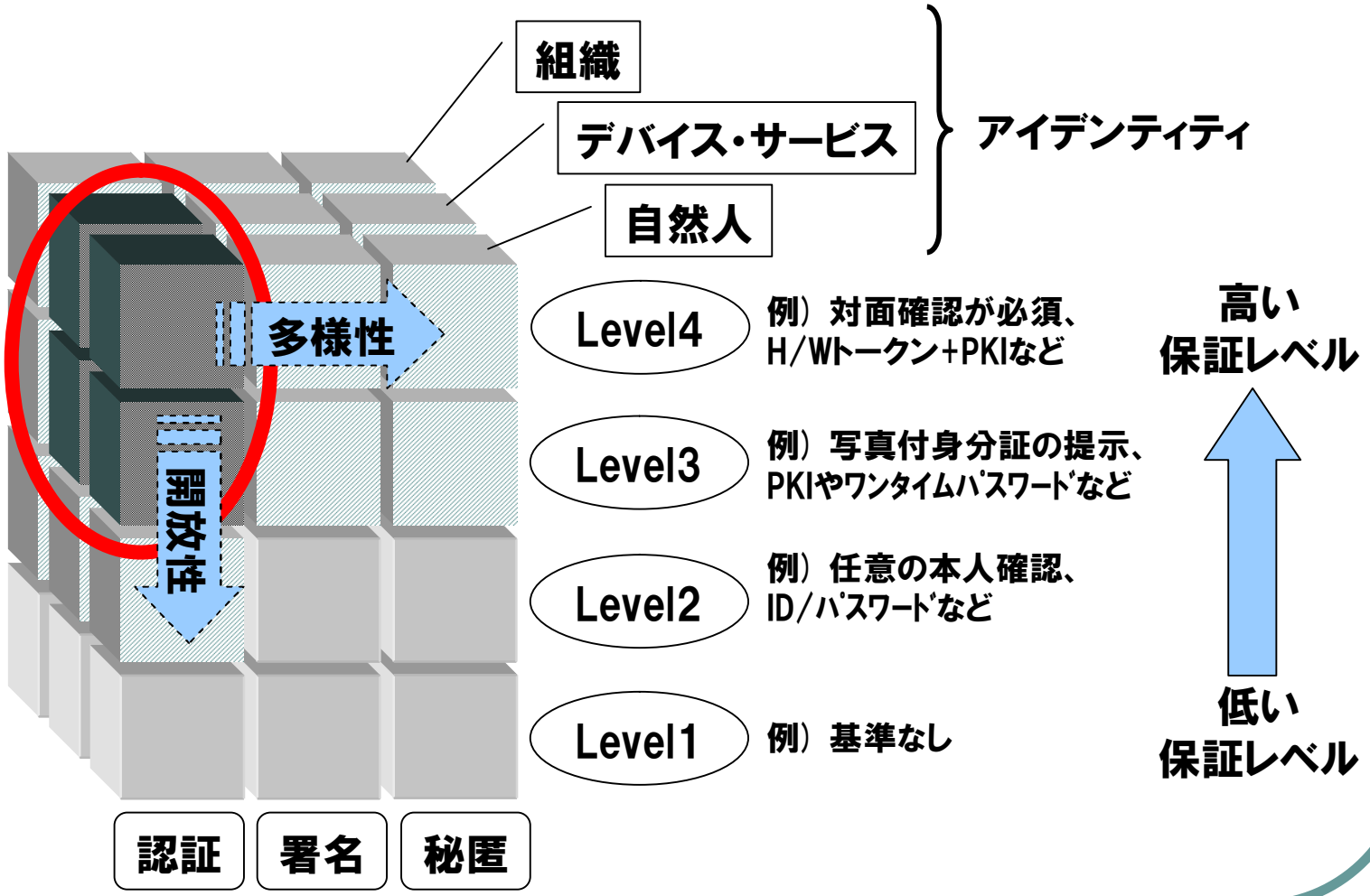
セキュリティポリシを揃えていくには

- 多様なセキュリティポリシ
  - 大学によってセキュリティポリシは様々
  - 高価な研究施設を共同利用するには認証連携が必要
  - 連携するには合意できる要素が必要
- 何が合意できればいい??
  - PKIであれば、本人性が信頼に直結する
- 本人性を保証する考え方: 保証レベル

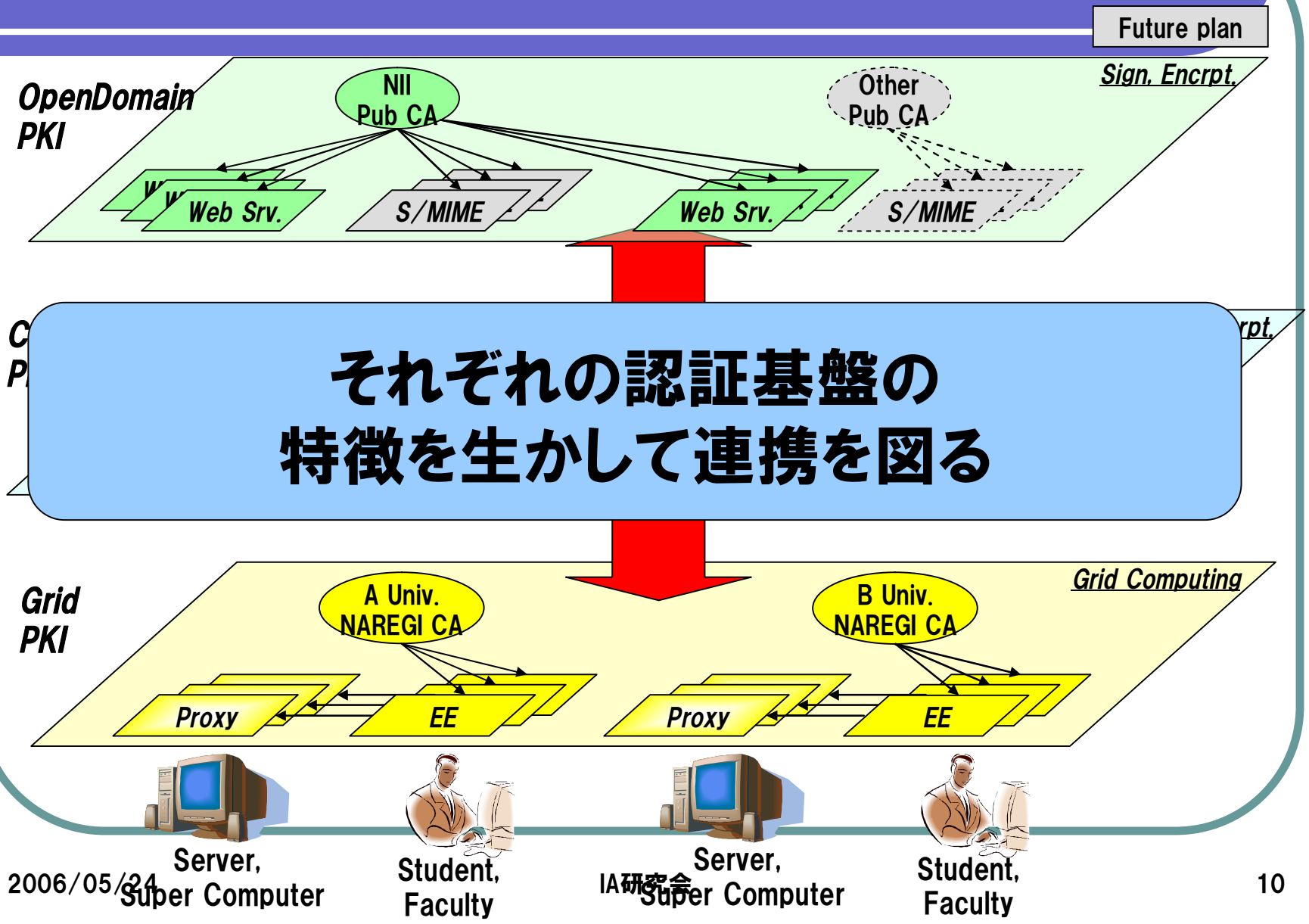
信用度を示す保証レベル（例）

保証レベル	定義	適用例
レベル1	Little or no confidence	自己登録のID/パスワードを用いる運用
レベル2	Some confidence	登録時に何かしらのアイデンティティ確認を求める運用
レベル3	High confidence	高い本人確認を求める運用 cf. 知財情報の取り扱いなど
レベル4	Very high confidence	より高い本人確認を求める運用 cf. 犯罪情報の取り扱いなど

保証レベルのキューブ


組織
デバイス・サービス
自然人
アイデンティティ
多様性
信頼性
Level4
例）対面確認が必須、
H/Wトークン+PKIなど
Level3
例）写真付身分証の提示、
PKIやワンタイムパスワードなど
Level2
例）任意の本人確認、
ID/パスワードなど
Level1
例）基準なし
高い
保証レベル
低い
保証レベル
認証
署名
秘匿

UPKIの3層構造


Future plan
OpenDomain PKI
NII Pub CA
Other Pub CA
Sign, Encrpt.
Web Srv.
S/MIME
Web Srv.
S/MIME
それぞれの認証基盤の
特徴を生かして連携を図る
Grid PKI
A Univ. NAREGI CA
B Univ. NAREGI CA
Grid Computing
Proxy
EE
Proxy
EE
Server, Super Computer
Student, Faculty
Server, Super Computer
Student, Faculty

具体的な課題の抽出

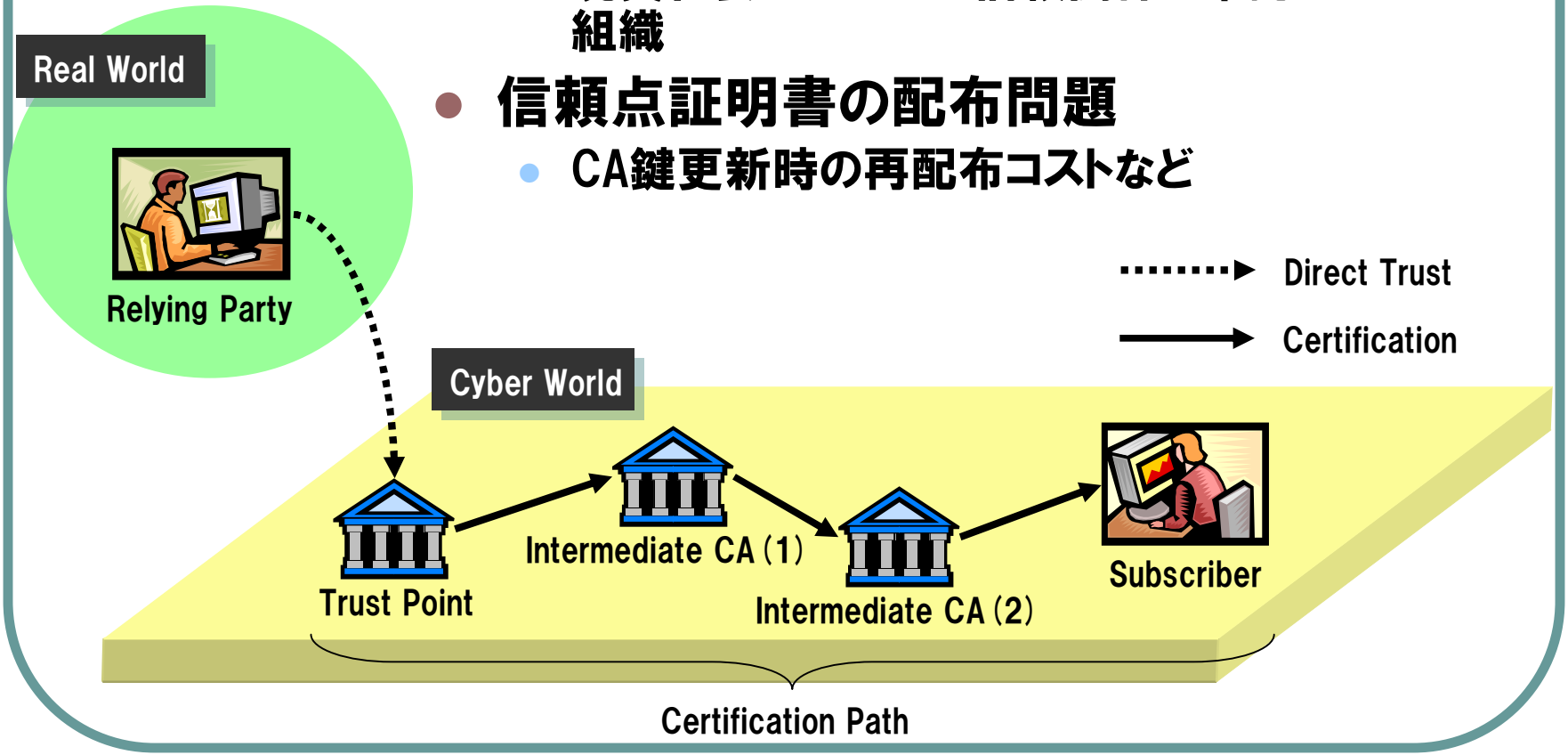
- UPKIドメイン構造の検討
  - ドメイン構造の分類、PMAの確立
  - ハイブリッドなドメイン構造
- UPKIにおける信頼点の検討
  - 信頼点は現実世界との紐付け
  - 利用者への（物理層での）安全な配布
- 学間連携のアーキテクチャ
  - マルチドメイン問題
  - ブリッジ、統合ドメイン、ID連携

ドメイン構造の分類

	特徴	ドメイン規模	期待されるPMA組織	備考
単一ドメイン構造	全ての大学・研究機関でポリシを共有	全国一元の大規模ドメイン	文部科学省，大学共同利用機関法人など	全大学・研究機関に対する一定の支配力が必要.
複数ドメイン構造	いくつかの大学・研究機関でポリシを共有	国・公・私，都道府県単位，地域単位など中規模ドメイン	7大学情報基盤センター，国立大学協会など	共有可能なポリシを策定する協調性が不可欠.
個別ドメイン構造	各大学・研究機関で個別にポリシを確立	個々の大学・研究機関毎	各大学・研究機関	重複するポリシ策定コストによる負担増. 連携時の平準化コスト.

信頼点と認証パス

- 信頼点は現実世界との唯一の紐付け
  - 現実社会でいつでも信頼関係を確認できる組織
- 信頼点証明書の配布問題
  - CA鍵更新時の再配布コストなど



信頼点の配付（配布）方法

配付: 銘々にくばりわたすこと。
配布: 広くゆきわたるように配ること。

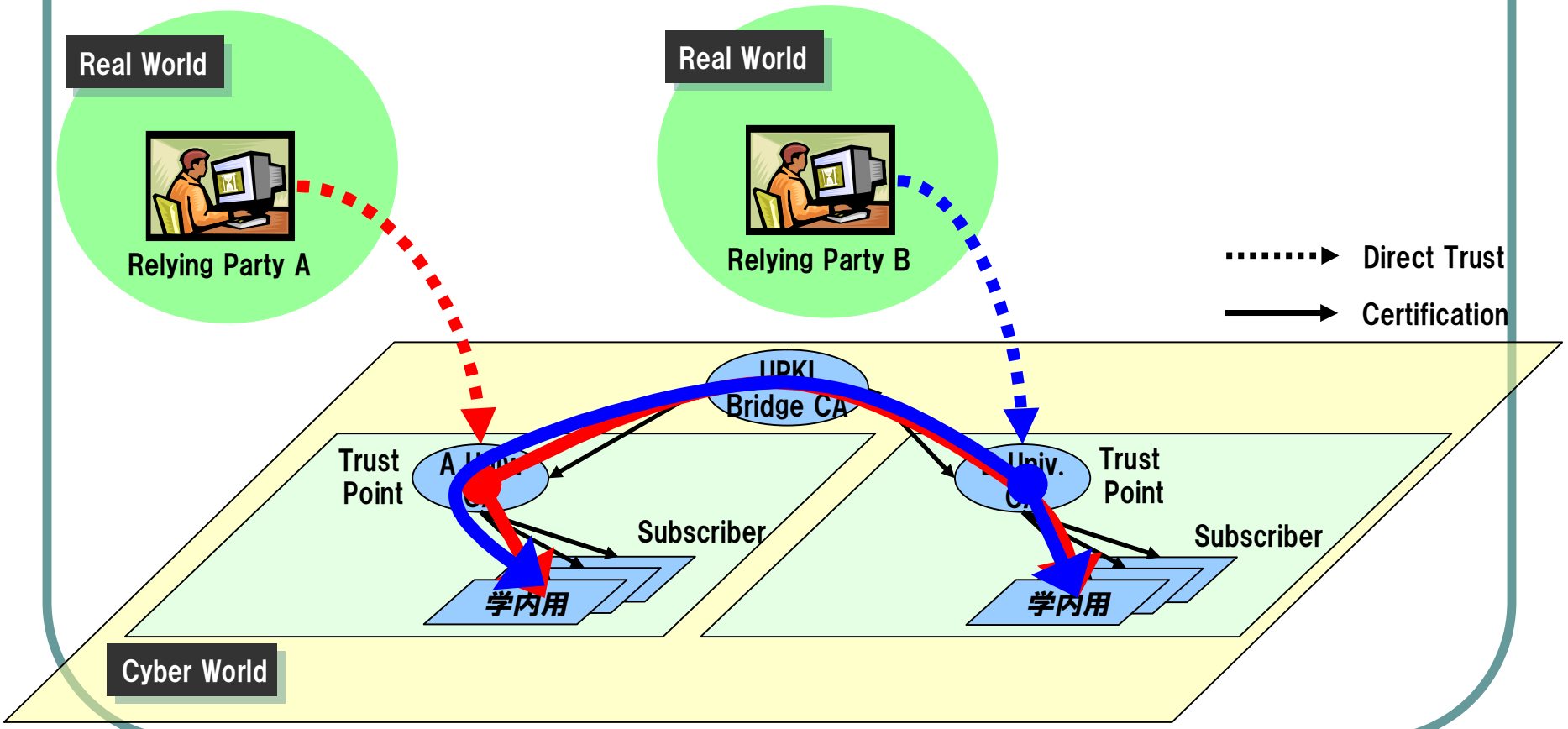
三省堂「大辞林 第二版」より

- **ダウンロード方式**
  - 信頼できる機関が、ネットワーク上で信頼者に信頼点を配る方式
  - 配付（配布）コストそのものは安価
  - 配布するサイト自体の信頼性が必要→鶏卵問題
- **対面配付方式**
  - 信頼できる機関が直接、信頼者に信頼点を配付する方式
  - 信頼できる機関から直接入手できるのできわめて安全
  - 地理的制約が伴う → 配付コストに直結

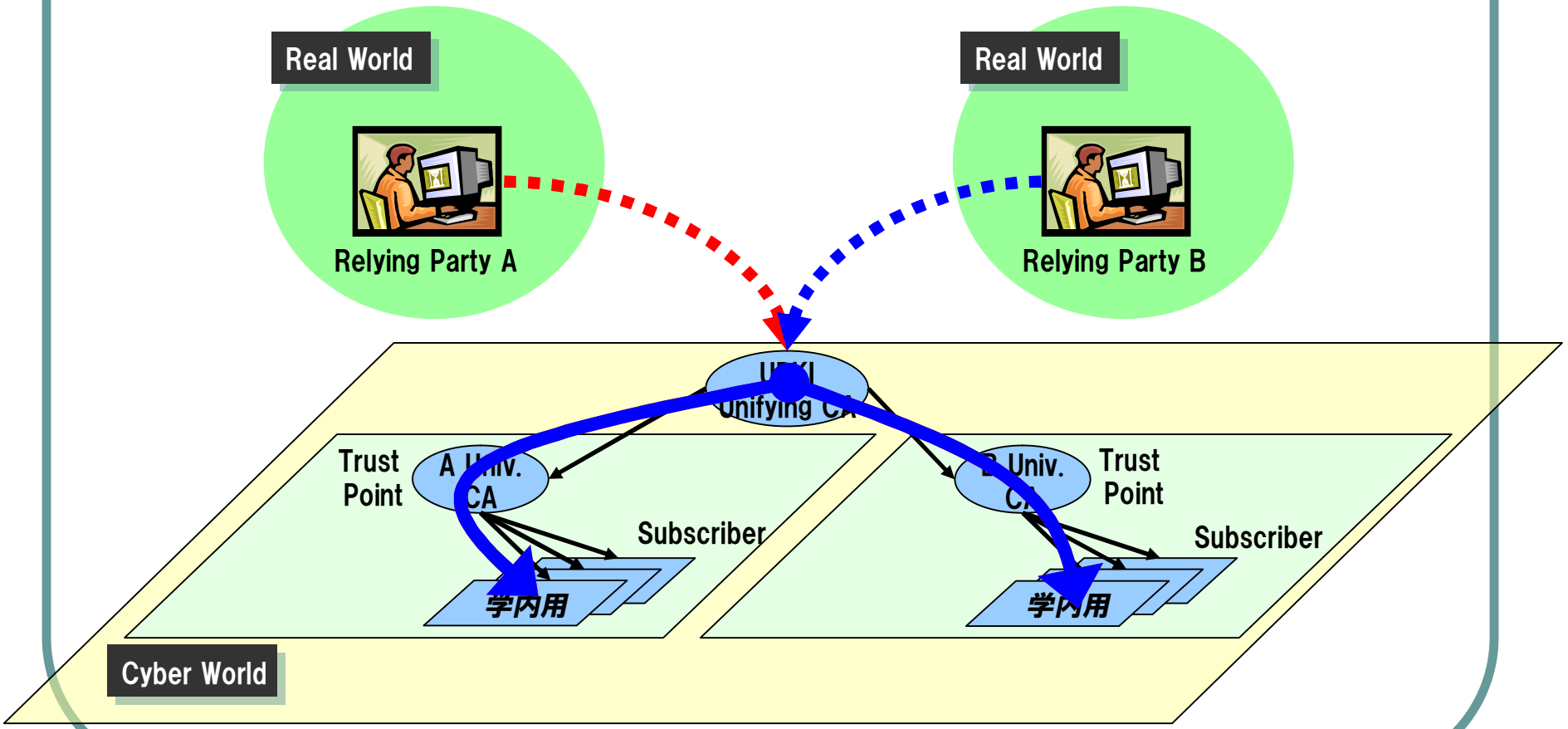
信頼点の配付形態

- アプリケーション組み込み型
  - 信頼点を組み込んだアプリケーションを配付（配布）する形態
  - アプリケーションの配付自体に信頼性が必要
  - アプリケーションによっては登録コストが発生する（登録審査・手続きなど）
  - アプリケーション毎に信頼点を組み込む必要がある
- 直接配付型
  - 信頼点証明書そのものを配付（配布）する形態
  - 配布自体はアプリケーションに依存しないため、自由度が高い
  - 利用するアプリケーションによっては信頼点の登録方法が異なるなどのサポートコストが発生する

ブリッジモデルの信頼点



統合ドメインモデルの信頼点



ここまでのまとめ

- 取り組むべき具体的課題の整理
  - ドメイン構造
  - 信頼点の配付方法と配付形態
  - 学間連携アーキテクチャ
- 大学界全体で検討・合意形成していくべき課題
- 課題解決・合意形成へ向けた「**知の共有**」
- 大学界全体で合意形成していけるフレームワークが必要となる

今後のアプローチ
～UPKI相互運用フレームワークの整備～

- 広く全国の大学に支持・合意を得られる仕組みを持つこと → 全国のUPKI有志がバーチャルに議論を行い，合意形成できるコミュニティ作り
- 広く全国の大学が導入・運用可能なアーキテクチャを持つこと → デファクトスタンダードを多用したリファレンス仕様の策定
- 広く全国の大学が導入可能な経済合理性を実現すること → 全国の大学が効率よく負担できるコスト集中型の運用モデル検討や設計開発
- 広く全国の大学にUPKIの技術や利用事例を啓発すること → UPKIのアーキテクチャ，アプリケーション，ケーススタディのKnowledge Base構築

ありがとうございました

国立情報学研究所
島岡 政基
shimaoka@nii.ac.jp