大学間連携のための全国共同電子認証基盤(UPKI)構想と米国学術PKIの動向

国立情報学研究所
島岡 政基

本日の概要

- 学術機関の事情と背景
  - 高等教育機関の事情
  - 全国共同利用機関とUPKI
- 米国学術PKIの動向
  - HEPKIプロジェクト
  - ブリッジCAとルートCAのハイブリッド構造
- 連携のアーキテクチャ検討
  - UPKIの3層構造
  - 連携に必要な保証レベル
  - ドメイン構造と信頼点
  - 将来的な連携のアーキテクチャ
- 連携へ向けた体制作り
  - UPKIイニシアティブ(仮)

- 学術機関の事情と背景
  - 高等教育機関の事情
  - 全国共同利用機関とUPKI
- 米国学術PKIの動向
  - HEPKIプロジェクト
  - ブリッジCAとルートCAのハイブリッド構造
- 連携のアーキテクチャ検討
  - UPKIの3層構造
  - 連携に必要な保証レベル
  - ドメイン構造と信頼点
  - 将来的な連携のアーキテクチャ
- 連携へ向けた体制作り
  - UPKIイニシアティブ(仮)

高等教育機関の基礎統計

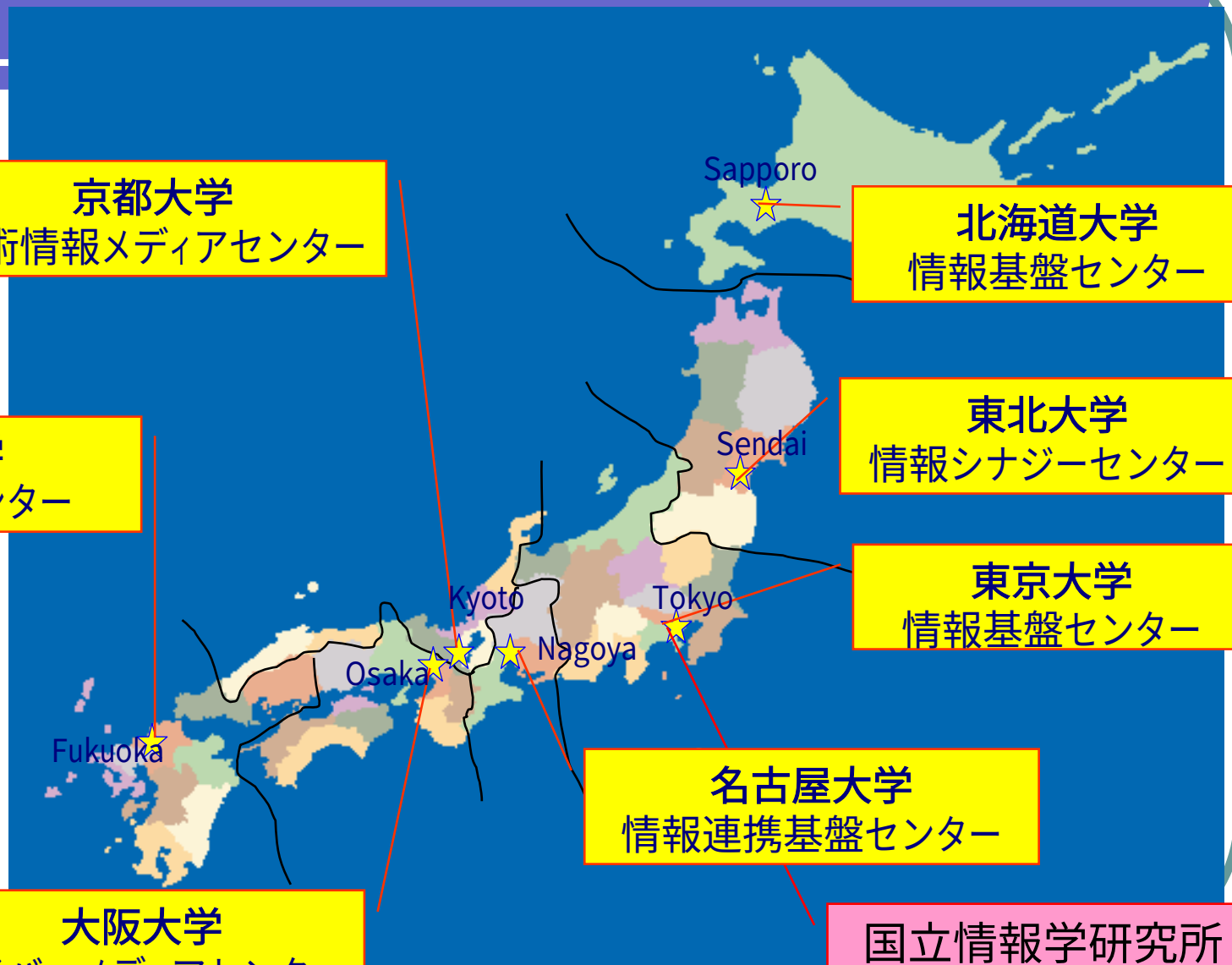
		学校数	学生数	教員数	職員数	総人数
大学		726	2,865,051	161,690	179,521	3,206,262
	国立	87	627,850	60,937	56,470	745,257
	公立	86	124,910	11,426	11,940	148,276
	私立	553	2,112,291	89,327	111,111	2,312,729
短期大学		488	219,355	11,960	6,635	237,950
	国立	10	1,643	244	140	2,027
	公立	42	14,347	1,209	361	15,917
	私立	436	203,365	10,507	6,134	220,006
高等専門学校		63	59,160	4,469	2,903	66,532
	国立	55	52,210	3,952	2,713	58,875
	公立	5	4,594	363	154	5,111
	私立	3	2,356	154	36	2,546
総数		1,277	3,143,566	178,119	189,059	3,510,744

文部科学省 平成17年度学校基本調査より

大学の特殊事情

- 少子化と全入時代
  - 格差の拡大
  - 全国共同利用機関
- 大学の財政基盤
  - 国立は運営費交付金1%シーリング
  - 私学助成金は?
- 大学の情報セキュリティ対策
  - 偏差値や志望者数との関連性は?

全国共同利用情報基盤センター



京都大学
学術情報メディアセンター

北海道大学
情報基盤センター

九州大学
情報基盤センター

東北大学
情報シナジーセンター

東京大学
情報基盤センター

名古屋大学
情報連携基盤センター

大阪大学
サイバーメディアセンター

国立情報学研究所
(NII)

全国共同利用情報基盤センター間の連携の歴史

- 1965～70
  - 全国共同利用大型計算機センタ、7大学に設置
- 1981
  - X.25（DDX-P商用パケットサービス）によるセンター間接続
- 1986
  - 学術情報センター(NACSIS)設置
  - N-1ネットワーク
    - 大学間を結ぶ専用X.25網
    - 共通利用番号制（～2004）
- 1988
  - JAIN プロジェクト開始
    - IP over X.25
- 1992
  - 学術情報センターによるSINETサービス提供開始
- 1999～2003
  - 情報基盤センターへ改組
- 2000
  - 国立情報学研究所(NII)設立
- 2001
  - 大学の情報セキュリティポリシーに関する研究会
- 2002
  - スーパーSINET運用開始
- 2003
  - NAREGI（National Research Grid Initiative） プロジェクト開始
  - グリッドコンピューティング研究会
- 2004
  - 認証研究会
- 2005
  - NIIに学術情報ネットワーク運営・連携本部を設置
    - ネットワーク作業部会
    - 認証作業部会

7大学センターとNIIの連携を強化

スパコン ＋ネットワーク ＋教育用計算機 ＋… ⇒ 情報基盤

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

大学間連携のための全国共同電子認証基盤(UPKI)構築事業

- 目的
  - 大学が有する教育研究用計算機，電子コンテンツ，ネットワークを安全･安心に有効活用するための電子認証基盤の構築
- 7大学とNIIの連携
  - 大学内･大学間認証基盤の国家的なモデル作り
    7大学：大学内認証基盤 ＋ (地域)
    NII　：大学内認証基盤の相互接続
- 効果
  - 大学間の相互認証
    → 研究資源、教育コンテンツの有効活用 (e-learning, 単位互換)
  - 電子署名･暗号化
    → 情報漏洩、なりすましの防止によるセキュリティ強化
    研究成果の真正性の証明
    電子決済･電子回覧による効率化
  - ネットワークローミング → 無線LAN, 公衆Web端末
  - グリッドコンピューティング
    → 7大学スパコンリソースをCSI上に統合
    京速コンピュータ時代へ向けての利用者管理基盤

平成１８年度予算
特別教育研究経費
(大学間連携経費)

大学間連携のための全国共同電子認証基盤（UPKI）：「全国共同」の意義

- 大学間連携の強化
  - 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
- 各大学における効果
  - 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
- 国際連携、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

『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

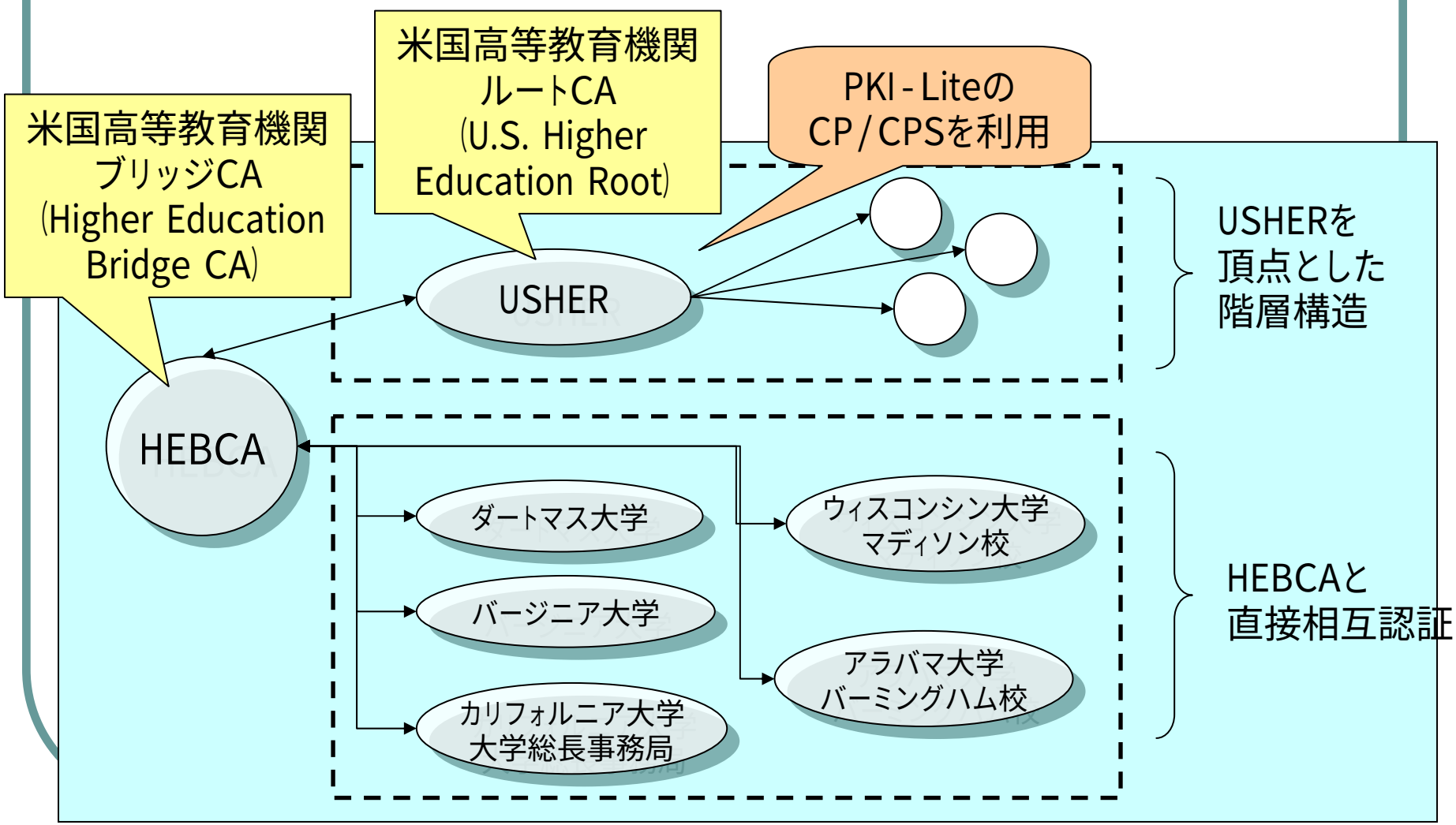
日本版SOX法への対応？

- 学術機関の事情と背景
  - 高等教育機関の事情
  - 全国共同利用機関とUPKI
- 米国学術PKIの動向
  - HEPKIプロジェクト
  - ブリッジCAとルートCAのハイブリッド構造
- 連携のアーキテクチャ検討
  - UPKIの3層構造
  - 連携に必要な保証レベル
  - ドメイン構造と信頼点
  - 将来的な連携のアーキテクチャ
- 連携へ向けた体制作り
  - UPKIイニシアティブ(仮)

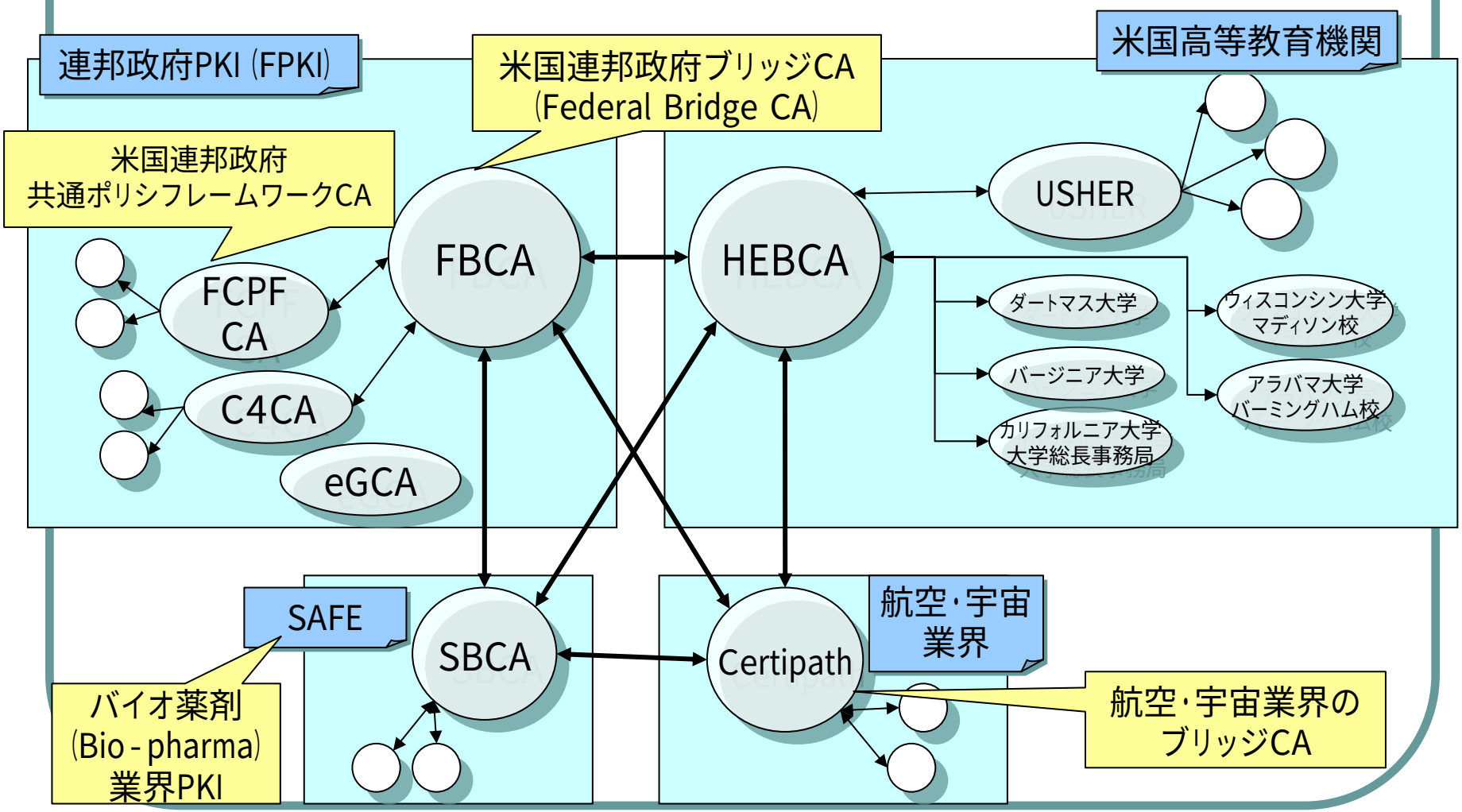
Higher Education PKI（HEPKI）

- 高等教育機関におけるPKIの構築促進を目的としたプロジェクト
  - EDUCAUSEとInternet2の協力事業
  - PKI構築を促進するツールやリファレンス仕様の開発･提供
  - HEBCAやUSHERの設計･構築･運用
- 成果物
  - モデルキャンパス証明書ポリシ（雛形）
  - 証明書プロファイル作成ツール
- PKI Lite
  - 学術機関への軽量なPKI導入を可能にするための活動
  - PKI-Lite Recipe
  - PKI-Lite CP/CPS
    - 学術機関向けのCP/CPS雛形
    - USHER（後述）、InCommon Federation、South California Universityで利用されている

米国学術機関PKI鳥瞰図

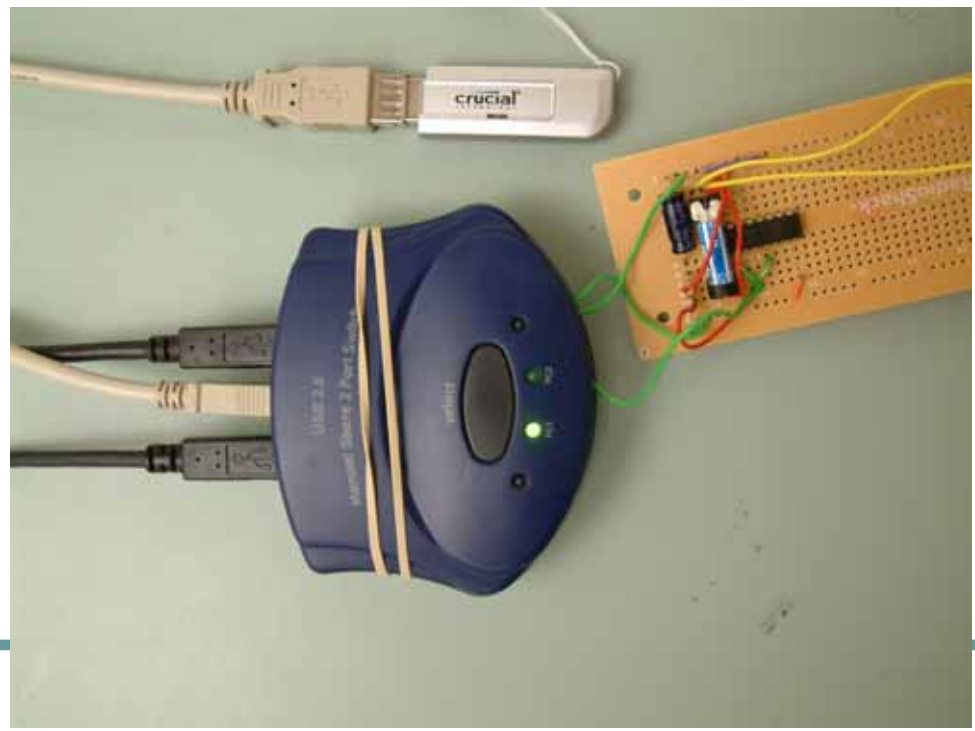


米国学術機関PKI：他の大規模PKIとの接続



FBCAのクライテリアに準拠するための秘密兵器。。。

- 6時間毎のCRL発行 vs. HEBCAのオフライン運用
  - Pre-generated CRLs
  - AirGap Mk II: USB based switch



IMSP
(Identity Management Services Program)

- EDUCAUSEによる加盟組織を対象としたプログラム
- プログラムに登録することにより、さまざまな参加ベンダが提供するアイデンティティ管理製品やサービスを安価に受けることができる
- IMSP加入費用(Subscription Cost)として2,000ドルが必要
  - 利用可能な製品やサービスは認証ベンダによって様々

参加ベンダ
Aladdin
CertAlert
Cybertrust
Geotrust
VeriSign

IMSP加入組織
ノーザンウェスタン大学
サンタクララ大学
ネバダ大学ラスベガス校
イェール大学

PKI先進大学比較（1）

		ダートマス大学	テキサス大学医学部	マサチューセッツ工科大学	アラバマ大学バーミング校
統計情報	ユーザ数	8000	13000	30000	30000
	コスト	30000ドル/年	60000ドル/年	雇用者0.5人＋ハードウェア	（未回答）
	動機	VPN	S/MIME	Web認証	エンタープライズ認証
	CA運用	自己運用	アウトソース	自己運用	アウトソース
発行枚数		1000	500	全学生＋75%の職員	（未回答）
運用期間		1年	3年試用＋半年実運用	8年	3年以上
利用者登録		ローカルログイン	対面登録	Kerberosクレデンシャルが必要	（未回答）
サポート体制		ヘルプデスク PKI研究所	デスクトップ	通常サポート	（未回答）
利用アプリケーション		VPN,Webアプリ、認証、S/MIME、SSL	Webアプリ、認証、S/MIME、SSL	Webアプリ、SSL	文書署名、S/MIME、SSL、Grid

PKI先進大学比較（2）

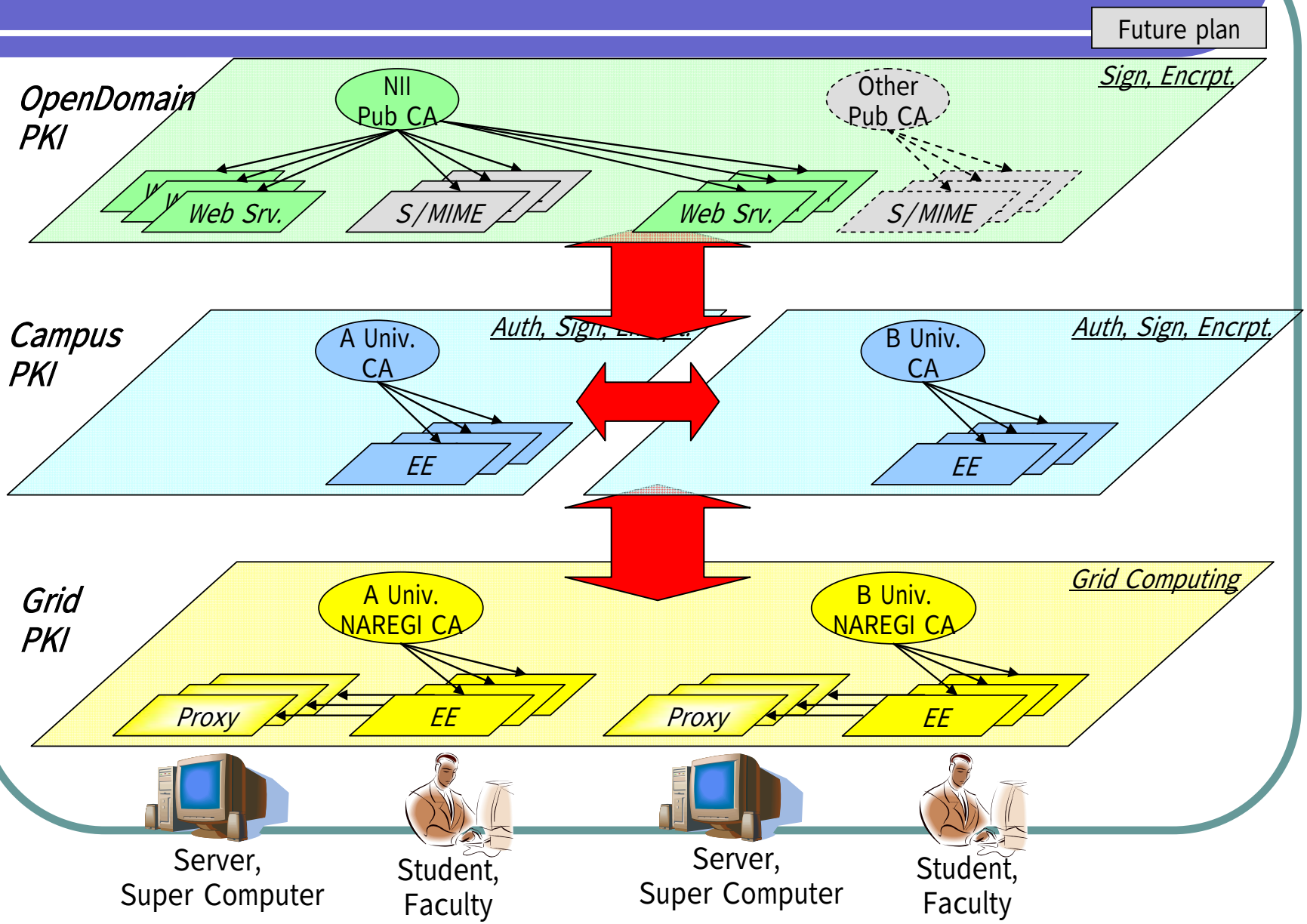
		テキサス・ウェズリアン大学	バージニア大学	テキサス大学ヒューストン健康科学センター
統計情報	ユーザ数	4500	30000	10000
	コスト	（未回答）	雇用者1人＋ハードウェア	50000ドル/年
	動機	ID管理	セキュリティ	文書署名
	CA運用	自己運用	自己運用	アウトソース
発行枚数		（未回答）	5000	2000
運用期間		試用期間1年	2年	5年
利用者登録		（未回答）	保証レベルにより異なる	対面登録
サポート体制		Help Desk（24時間体制）	通常サポート	Help Desk メール&電話 自宅ユーザサポート
利用アプリケーション		デスクトップクライアント認証、文書送信	Webアプリ、EAP/TLS認証、SSH、SSL、S/MIME、Grid	VPN、Webアプリ S/MIME、SSL

- 学術機関の事情と背景
  - 高等教育機関の事情
  - 全国共同利用機関とUPKI
- 米国学術PKIの動向
  - HEPKIプロジェクト
  - ブリッジCAとルートCAのハイブリッド構造
- 連携のアーキテクチャ検討
  - UPKIの3層構造
  - 連携に必要な保証レベル
  - ドメイン構造と信頼点
  - 将来的な連携のアーキテクチャ
- 連携へ向けた体制作り
  - UPKIイニシアティブ(仮)

大学に関係する様々な認証基盤

	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	WebSSO, VPN, 802.1X, 申請・署名アプリなど	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	大学 or アウトソース・ホスティング	全国共同利用センター

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
Campus PKI
A Univ. CA
Auth, Sign, Encrpt.
B Univ. CA
Auth, Sign, Encrpt.
EE
EE
Grid PKI
A Univ. NAREGI CA
Grid Computing
B Univ. NAREGI CA
Proxy
EE
Proxy
EE
Server, Super Computer
Student, Faculty
Server, Super Computer
Student, Faculty

キャンパスPKIを中心とした連携案

- 証明書発行における本人性確認
  - 対面確認、(写真付)IDの提示、e-mailの到達確認、自己申請、紹介制度?などなど
- キャンパスPKIの利点
  - 本人性確認レベルの高い対面確認を行いやすい
    - 登録機関と加入者の地理的関係が近い
- オープンドメインPKI、グリッドPKIなどへの連携
  - 本人性確認の簡易化
  - 本人性確認にキャンパスPKIの証明書を利用可能

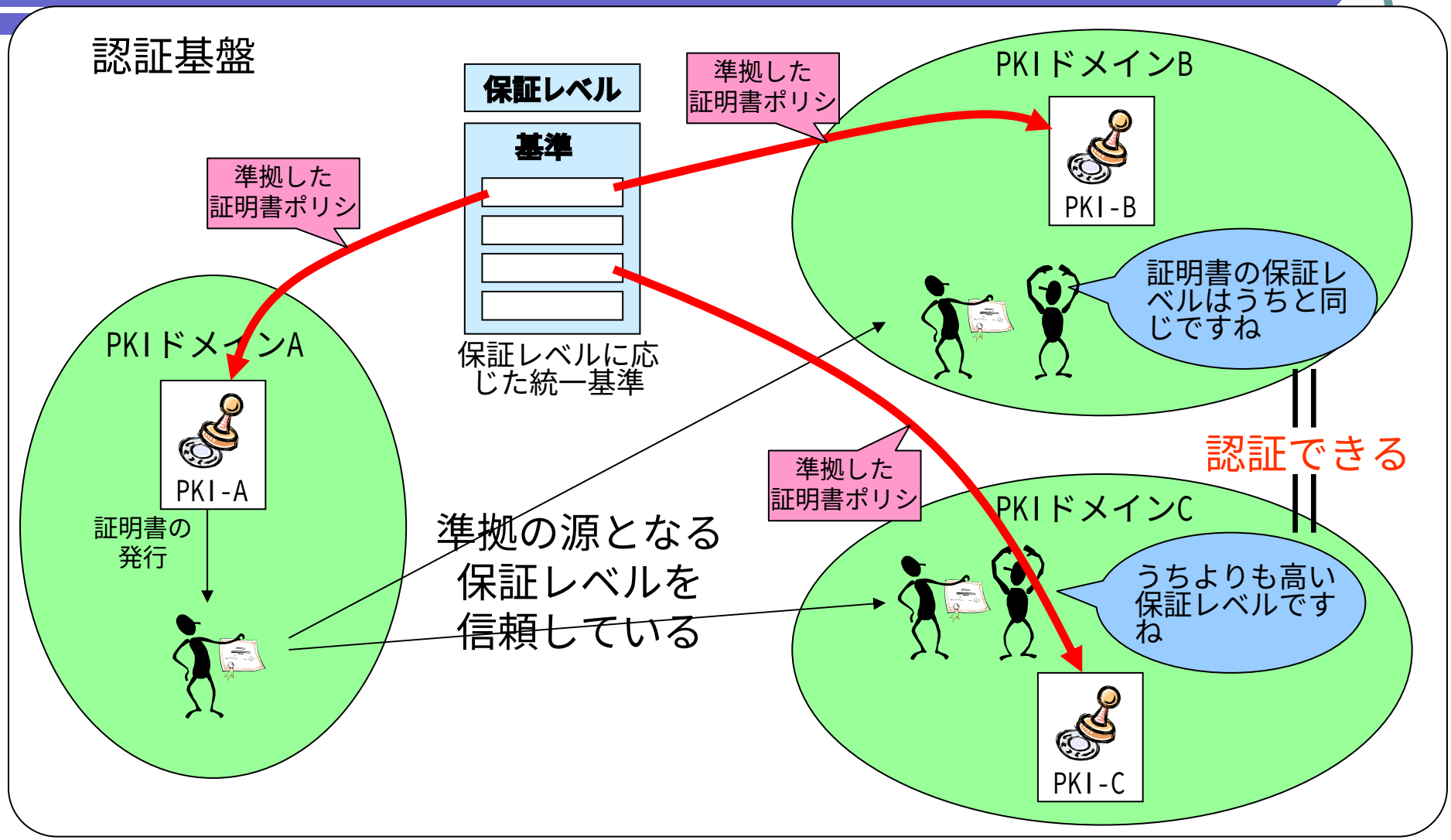
キャンパスPKI同士の連携案

- 大学間連携の最大のポイント
  - ニーズは？プライオリティは？
  - アプリケーションは？
  - 連携方式は？
- 連携方式について
  - PKIベースの相互認証
    - 数が増えればブリッジ接続→パス検証の難しさ
  - ID連携
    - 認証・認可だけなら選択肢に
    - SSOの恩恵もあるが、別途モジュールが必要
- どちらが優れている、というものではない
  - ニーズにあわせて選択していく
- いずれも相互の信頼を確立するためのフレームワークづくりが必要

連携に不可欠な保証レベル

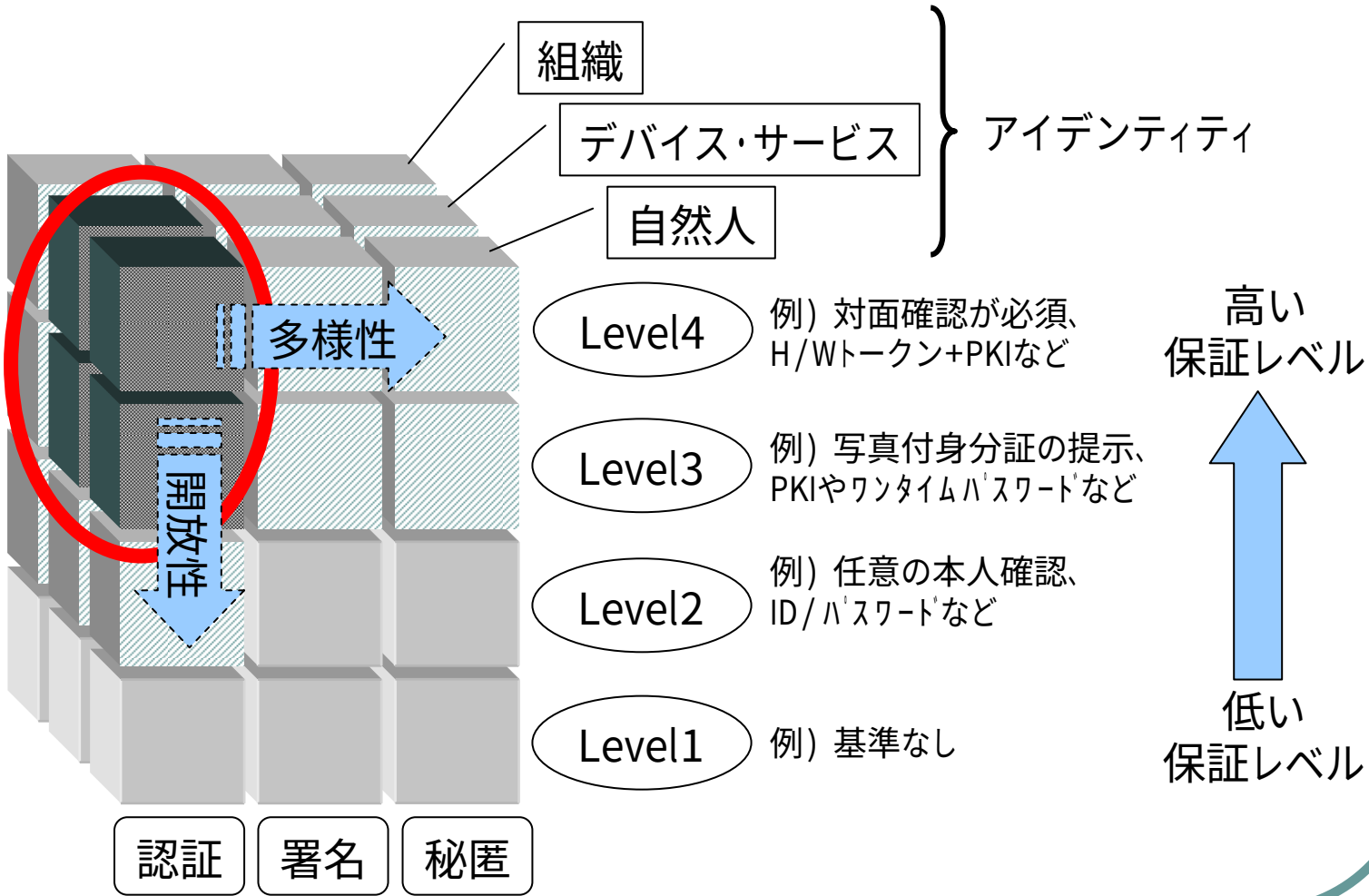
保証レベル	定義	適用例
レベル1	Little or no confidence	自己登録のID/パスワードを用いる運用
レベル2	Some confidence	登録時に何かしらのアイデンティティ確認を求める運用
レベル3	High confidence	高い本人確認を求める運用 cf. 知財情報の取り扱いなど
レベル4	Very high confidence	より高い本人確認を求める運用 cf. 犯罪情報の取り扱いなど

証明書の保証レベルを共有する



各PKIドメインを超えて認証することが可能

松本キューブで示すUPKI。。。

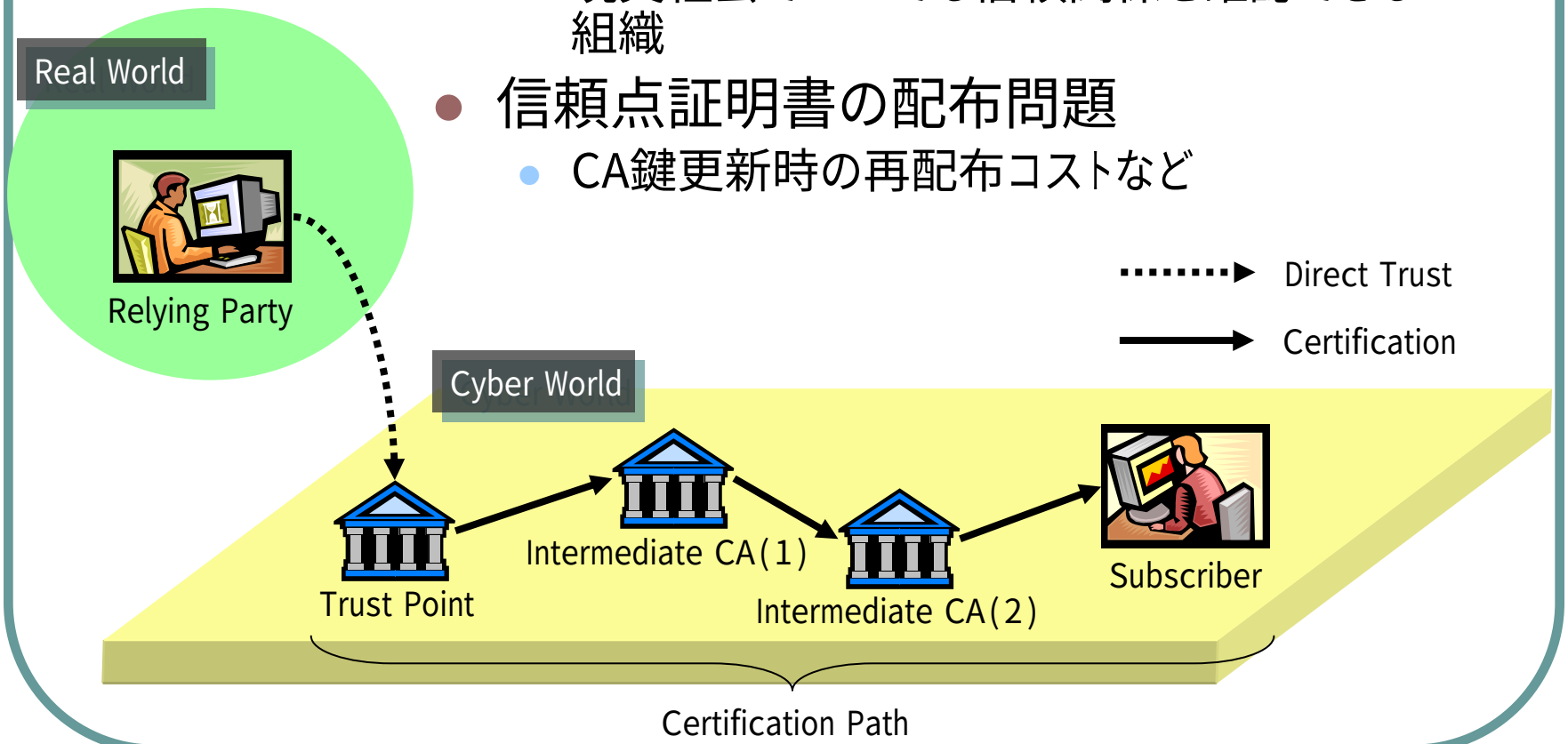


ドメイン構造の分類

	特徴	ドメイン規模	期待されるドメインの信頼点	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･各研究機関	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.

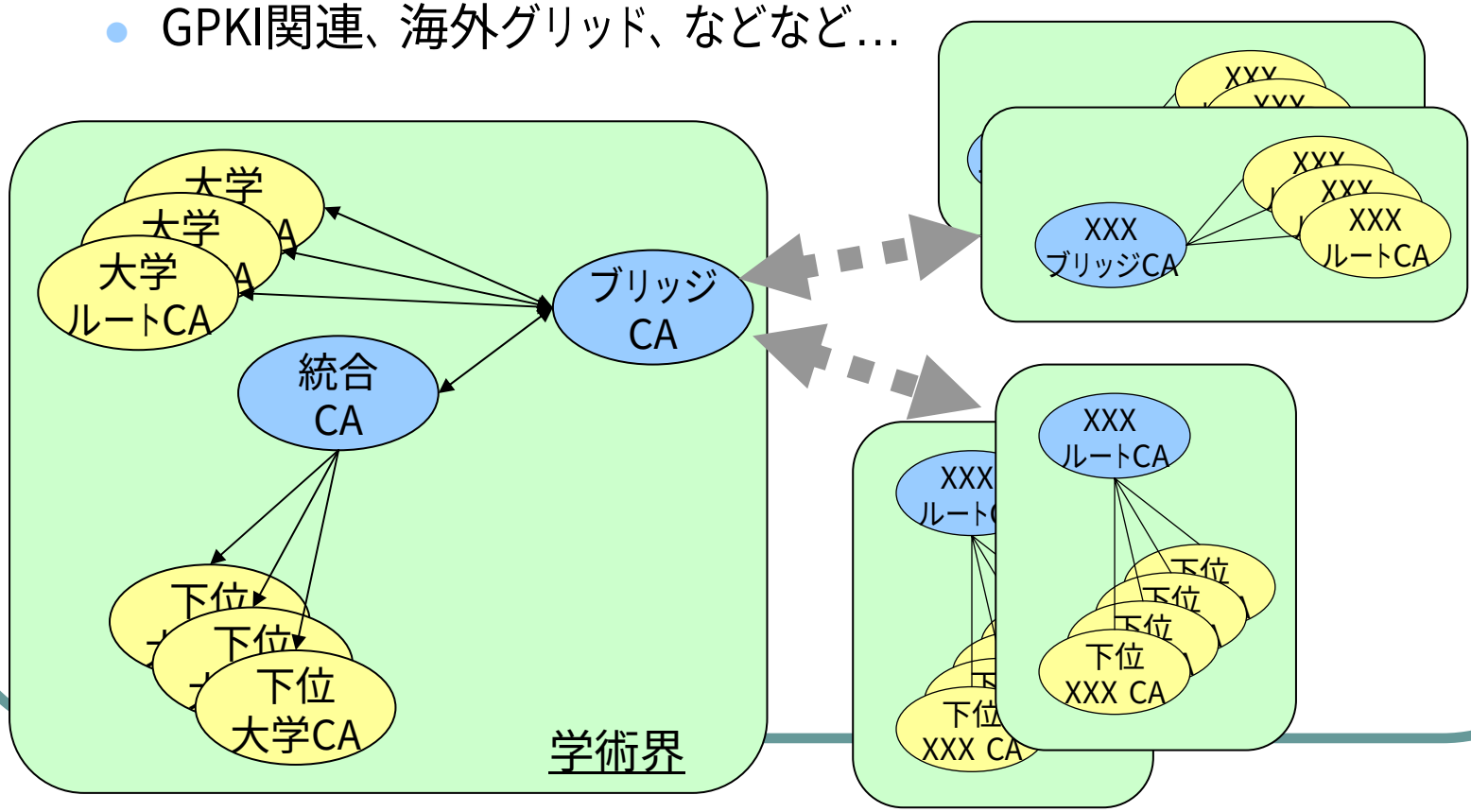
信頼点と認証パス

- 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



将来的なUPKIアーキテクチャ(検討中)

- ブリッジCA and 統合CAによるハイブリッド
- ブリッジ経由で他業界と相互接続
  - GPKI関連、海外グリッド、などなど…



他業界との相互接続を実現するブリッジCA

- 他業界PKIとの相互接続には不可欠な存在
  - ID連携が実現できるのは認証の連携のみ
  - 署名や秘匿用途にはPKIレベルでの相互接続が必要
- 学術界におけるポリシと他業界のポリシをマッピング
  - 学術PKIのPrincipal CAとして位置づけられる

簡易なキャンパスPKIを実現する統合CA

- 学内認証局を広く導入させるにはコスト軽減の工夫が不可欠
  - ポリシ策定などの設計コスト→簡易な汎用ポリシ開発によるコスト共有
  - CA、リポジトリなどの運用コスト→CAホスティングなどによるコスト共有
  - 本人性確認などのRA業務コスト→効率化・最適化によるコスト削減
- ある典型的なポリシに基づく統合CAを構築し、その傘下に下位大学CAを収容可能にする
  - 傘下に入る大学は統合CAの「典型的なポリシ」に従属しなければならない

連携のアーキテクチャ ～まとめ～

- 3層の認証基盤をうまく活用する
  - オープンドメインPKI、キャンパスPKI、グリッドPKI
- 連携に必要な保証レベルを共有する
  - 特定の保証レベルから徐々に拡張
- ドメイン構造と信頼点を考える
  - 現実的なドメイン構造は果たして？
- 将来的なアーキテクチャ
  - 先人の例を学びながら

- 学術機関の事情と背景
  - 高等教育機関の事情
  - 全国共同利用機関とUPKI
- 米国学術PKIの動向
  - HEPKIプロジェクト
  - ブリッジCAとルートCAのハイブリッド構造
- 連携のアーキテクチャ検討
  - UPKIの3層構造
  - 将来的な連携のアーキテクチャ
- 連携へ向けた体制作り
  - UPKIイニシアティブ(仮)

UPKIシンポジウム

- NIIで今年の2月15日に開催
  - 文部科学省と7センターによる共催
- 参加者からの意見
  - 大学以外との連携はどうやっていくのか
  - ノウハウや事例を共有したい
  - アプリへの親和性も考慮して欲しい
  - オープンに議論できる場が欲しい
    - …という意見をいただきました。

UPKIイニシアティブ(仮)の要件

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可能な限り活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

UPKIイニシアティブ(仮)(案)

- UPKIの仕様等検討
  - 各大学認証基盤の相互運用性仕様の設計
  - 関連技術の調査研究
  - 法的整備の検討
  - 認証技術のテスト環境提供と実証実験
- UPKI情報の外部発信(Web公開)
  - 運用事例、仕様書等の情報収集と公開
  - 意見の収集と仕様への反映
  - UPKIの活動報告

メーリングリスト、Webサイトなどを通じて情報発信・交換可能なコミュニティを目指す。

今後のToDoなど

- 各大学の意見を吸収できるオープンコミュニティ作り
- コミュニティで議論する色々なたたき台作り
- コミュニティをリードしていく大学有志

UPKI成功へ向けて
皆様のご協力をお願いします。

国立情報学研究所
島岡 政基