学内認証局の構築･運用にむけて
～概要および基礎知識～

平成20年度情報処理軽井沢セミナー

2008.9.2

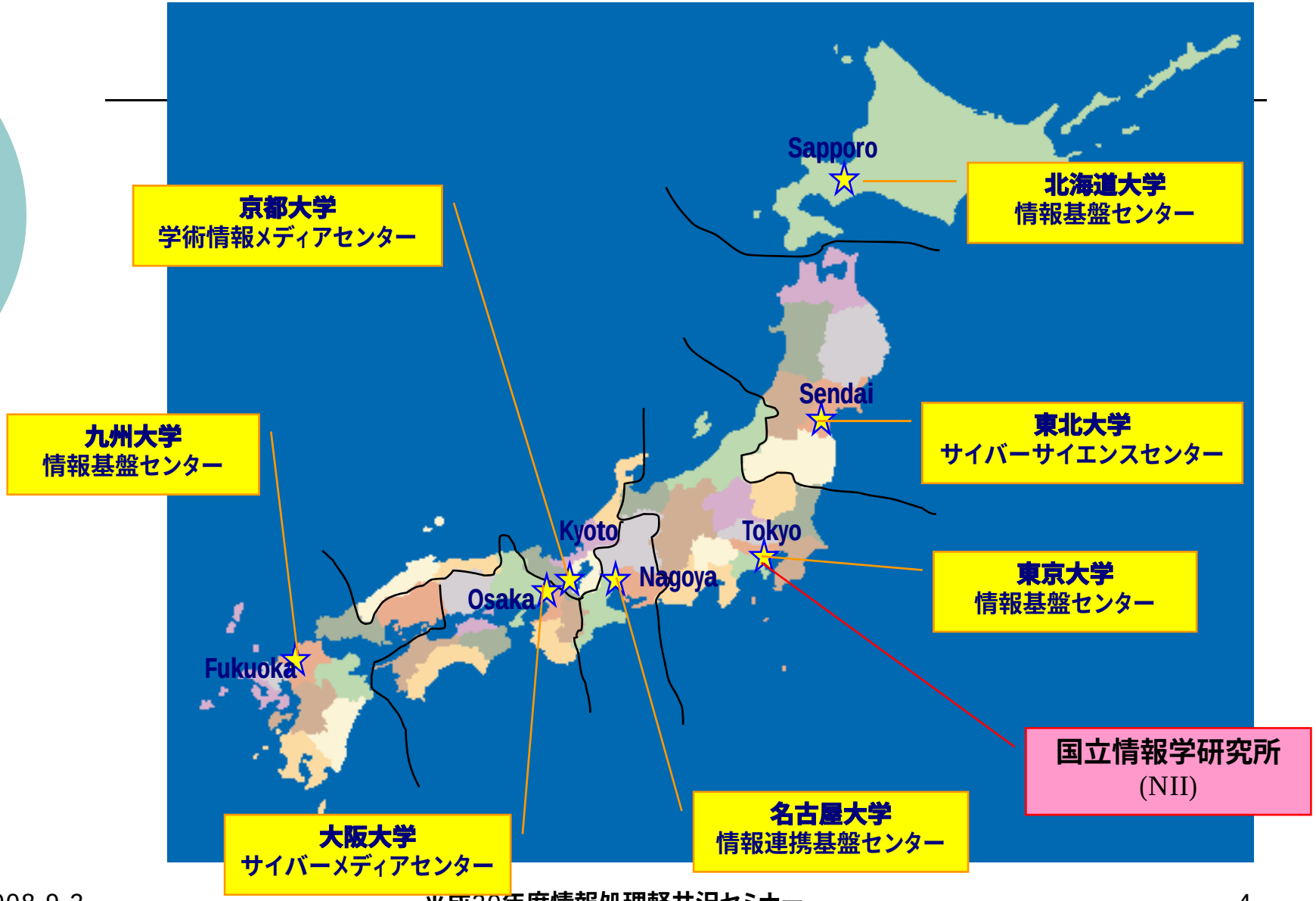
国立情報学研究所　中村素典

内容

- 概要：認証技術の活用事例
  - 大学間認証連携(UPKI)
  - 認証局構築支援
  - オープンドメインサーバ証明書発行
  - 無線LANローミング
- PKIによる認証基盤構築のための基礎知識
  - 信頼性の確保
  - 証明書の概要
  - 認証局の運用

認証技術の活用事例

全国共同利用情報基盤センター



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ー、7大学に設置**
- 1986
  - **学術情報センター**(NACSIS)**設置**
  - **共通利用番号制** (〜2004)
- 1992
  - **学術情報センターによる** SINET**サービス提供開始**
- 2000
  - **国立情報学研究所**(NII)**設立**
- 2002
  - SuperSINET**運用開始**
- 2003
  - NAREGI (National Research Grid Initiative) **プロジェクト開始**
- 2004
  - **国立大学法人化**
- 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
- 2008
  - SINET3**運用開始**

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

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(SINET3)

国際貢献・連携

Cyber Science Infrastructure (= e-Science) の目的

1. **学術ネットワークの強化･国際化：** SINET3
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**

学術力（情報力・研究力・教育力・文化力）の強化

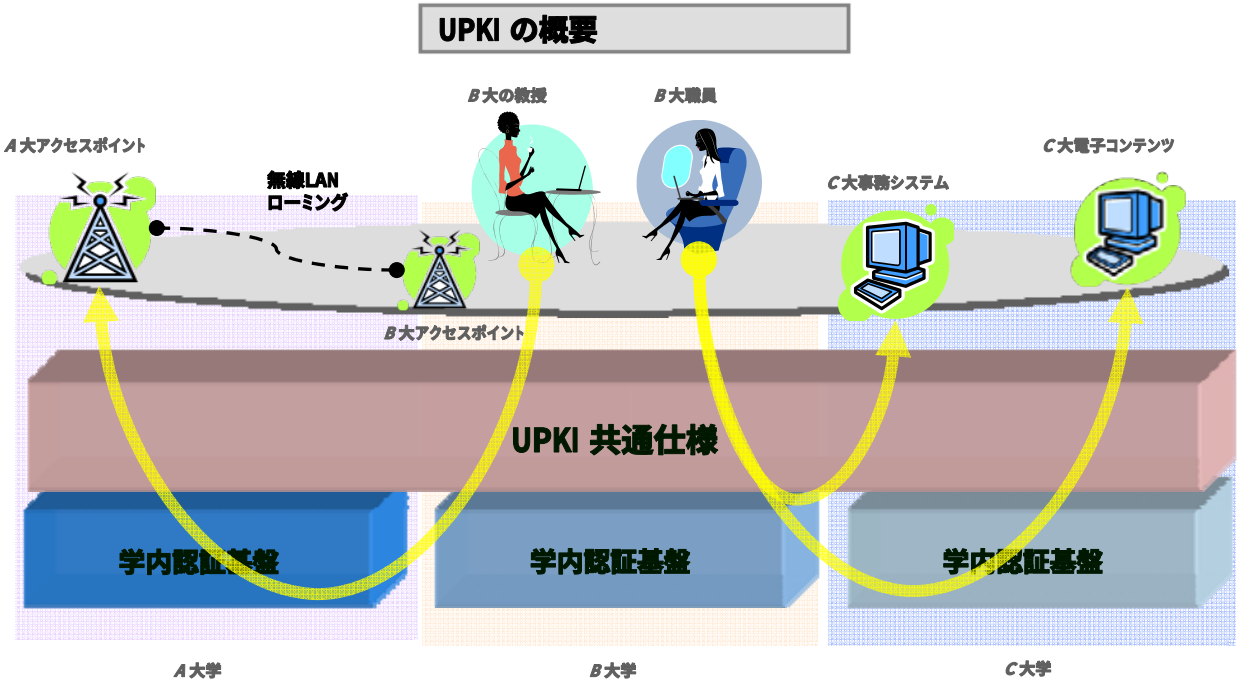
- ３０年前は、大型計算機、大型実験設備の保有が研究力・教育力の差に
- １０年前から、インターネットが情報力・研究力・教育力の差に
- ５年前ころから、コンテンツ発信・探索が情報力・研究力・教育力・文化力の差に
- これからは、フェデレーション・コラボレーション・コミュニティのための認証基盤が学術力の差になるのでは・・・・

連携 (Federation) がキーワード

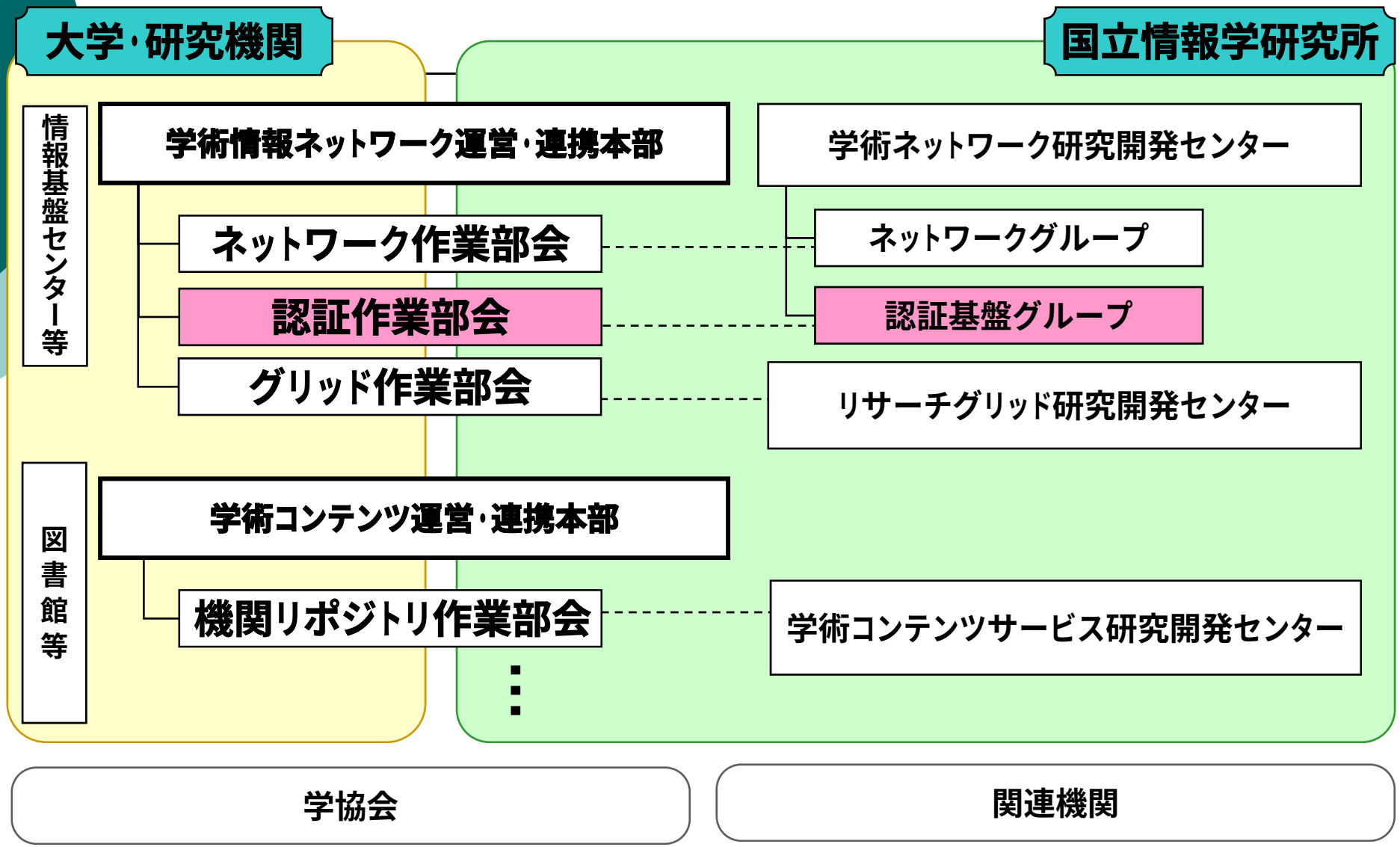
1. **学術基盤連携 (科学技術の進展)**
   - ドライ系　ネットワーク・コンテンツ・コンピュータ・データベース
   - ウエット系　**信頼関係**など
2. **高等教育連携 (分野と専門を超えた交流)**
   - ＩＣＴ人材育成、トップＳＥ、単位互換、研究倫理な
3. R&D連携 (**イノベーションダイナミクスの**創出)
   - 産学共同研究開発、学術知財管理など
4. **社会連携 (学術から知流社会への転換)**
   - 大学の情報社会基盤
   - 市民講座、生涯学習、公共スペース活用など

大学間連携のための
全国共同電子認証基盤（UPKI）とは

- 最先端学術情報基盤(Cyber Science Infrastructure)実現のため，大学等が保有する，教育･研究用計算機，電子コンテンツ，ネットワークおよび事務システムなどの学術情報資源を安心･安全かつ有効に活用するための電子認証基盤
- PKI（公開鍵認証基盤）を活用



CSIの実施体制


大学・研究機関
国立情報学研究所
情報基盤センター等
学術情報ネットワーク運営・連携本部
学術ネットワーク研究開発センター
ネットワーク作業部会
ネットワークグループ
認証作業部会
認証基盤グループ
グリッド作業部会
リサーチグリッド研究開発センター
図書館等
学術コンテンツ運営・連携本部
機関リポジトリ作業部会
学術コンテンツサービス研究開発センター
学協会
関連機関

国立情報学研究所
学術情報ネットワーク運営・連携本部
認証作業部会

- 岡部　寿男（京都大学学術情報メディアセンター）… 主査
- 曽根原　登（国立情報学研究所）…… 幹事
- 高井　昌彰（北海道大学情報基盤センター）
- 曽根　秀昭（東北大学サイバーサイエンスセンター）
- 後藤　英昭（東北大学サイバーサイエンスセンター）
- 佐藤　周行（東京大学情報基盤センター）
- 平野　　靖（名古屋大学情報連携基盤センター）
- 馬場　健一（大阪大学サイバーメディアセンター）
- 鈴木　孝彦（九州大学情報基盤センター）
- 飯田　勝吉（東京工業大学学術国際情報センター）
- 湯浅　富久子
  （高エネルギー加速器研究機構計算科学センター）
- 中村　素典（国立情報学研究所）
- 山地　一禎（国立情報学研究所）

国立情報学研究所
学術ネットワーク研究開発センター
認証基盤グループ

- 曽根原　登　　教授 (情報社会相関研究系 研究主幹) ……主査
- 岡部　寿男　　客員教授 (京都大学教授) ……副主査
- 中村　素典　　教授 (学術ネットワーク研究開発センター)
- 谷本　茂明　　客員教授 (学術ネットワーク研究開発センター)
- 岡田　仁志　　准教授 (情報社会相関研究系)
- 山地　一禎　　准教授 (学術ネットワーク研究開発センター)
- 島岡　政基　　特任准教授 (学術ネットワーク研究開発センター)
- 片岡　俊幸　　特任准教授 (学術ネットワーク研究開発センター)
- 樋口　秀樹　　基盤企画課副課長
- 夏目　典大　　基盤企画課係長 (連携システムチーム)

UPKI:体制と効果

- 体制：7大学情報基盤センターと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
      グリッド、共同研究、e-learning、単位互換、電子図書館
  - 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、利用者管理基盤
  - 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

文部科学省
特別教育研究経費
(大学間連携経費)
平成18年度～20年度

〔参考〕諸外国の状況

- Webサービス
  - Shibboleth（米欧）
    - 米国Internet2 MACE (Middleware Architecture Committee for Education) のプロジェクト
    - SAMLの標準化とオープンソース実装に寄与
    - 米欧で採用例多数
      - 図書館系の大学間認証ですでに実用化
- PKI構築
  - HEPKI（米国）
    - Internet2のプロジェクト
    - 1994年頃からスタート
- ネットワークローミング
  - eduRoam （欧州）
    - キャンパス無線LAN (Wi-Fi) の大学間ローミング
    - 欧州発、Asia-Pacificへ展開中
    - Shibbolethとの連携を検討中
- グリッド
  - TeraGrid（米国）
    - GridShibによるShibbolethとの連携
  - EGEE（欧州）

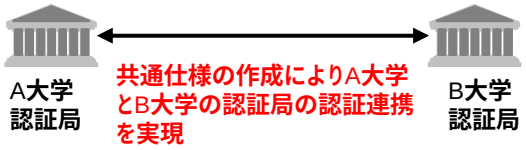
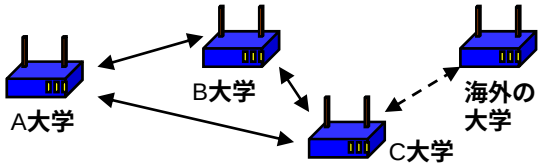
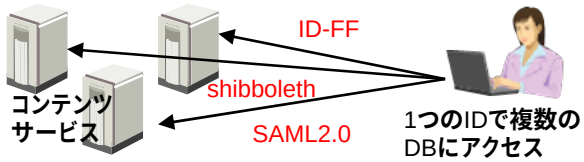
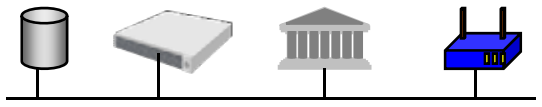
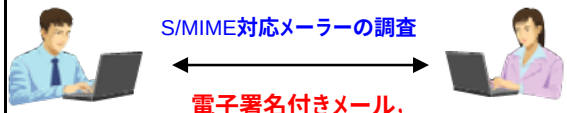
事業の概要

- UPKIアーキテクチャの設計と構築･運用
  - 公開鍵認証基盤(PKI)をベース
  - 多様なアプリケーションに対応したアーキテクチャ設計

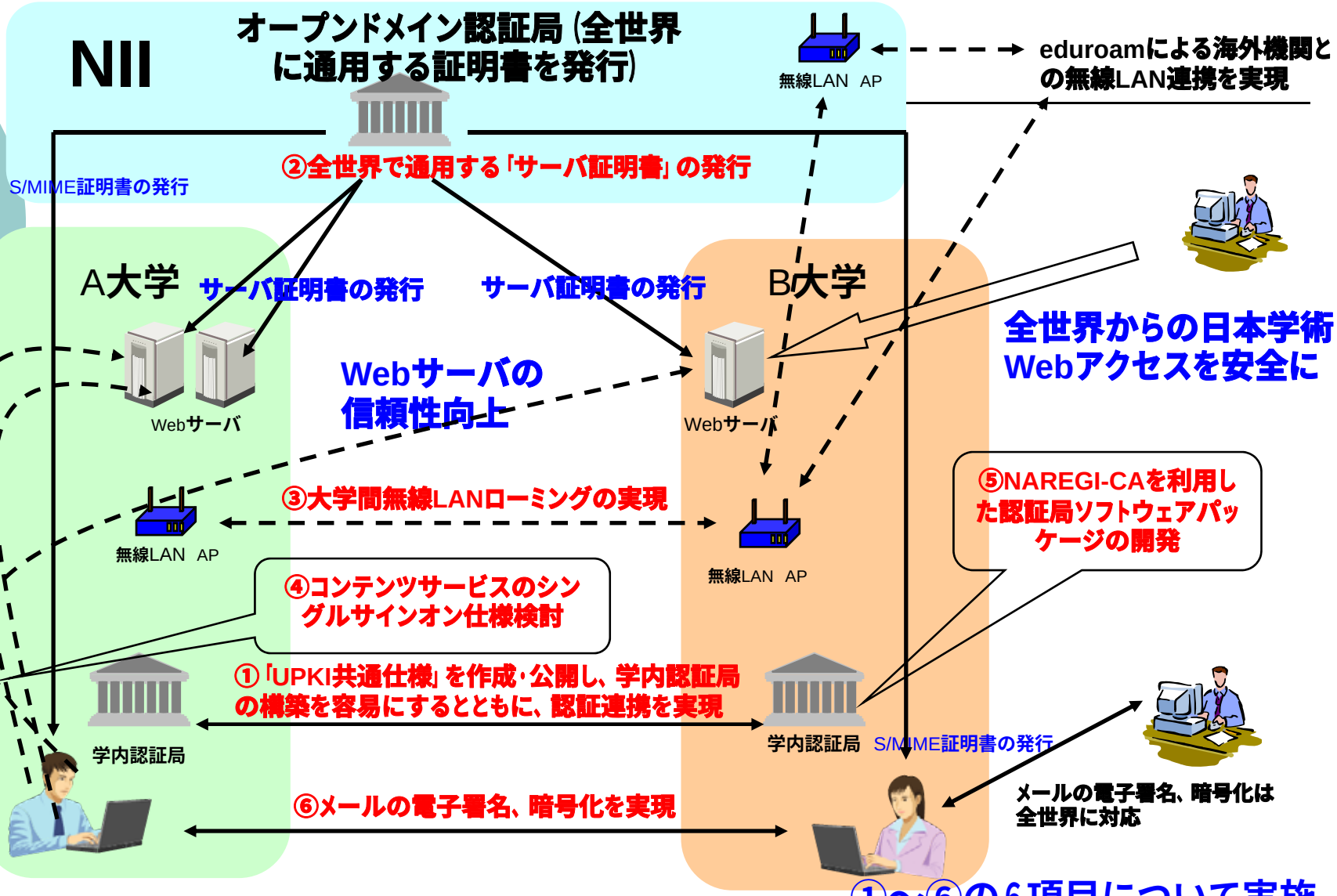
  ⇒Public系とprivate系の併用

  実印･銀行印･認印モデル
- スキーム･ポリシーのガイドライン策定･公開
  - 大学等の実務に即した証明書発行スキームの確立
  - CP/CPSガイドラインの制定
  - 大学等における情報セキュリティポリシー制定と連動
    - 共通ガイドラインの設計を行い，大学へ公開
- 大学における個人認証技術の検討
  - ICカード
  - バイオメトリックセキュリティ
- 認証ミドルウェアの設計･開発
  - ＯＳＳ (Open Source Software) の活用推進
  - NAREGI-CAのOSS化を支援
- アプリケーション技術の開発
  - WebサービスSSO
    - Shibboleth/SAML2.0
  - 電子メール暗号･署名 (S/MIME)
  - ネットワークローミング
    - eduroam
  - グリッド技術を活用した計算機環境の構築
    - NIIがGOC (Grid Operation Center) としての役割を担い，運用
- 国際連携、産官学連携、…
  - APGRID
  - APAN Middleware WG, Internet2 Shibboleth
  - GPKI、日本PKIフォーラム、…

これまで実現したUPKIの成果

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
4	コンテンツサービスのシングルサインオン仕様検討	 各種データベースサーバへのシングルサインオンを実現するため，shibboleth，SAML2.0等の仕様を調査し，UPKIにふさわしい方式を検討
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

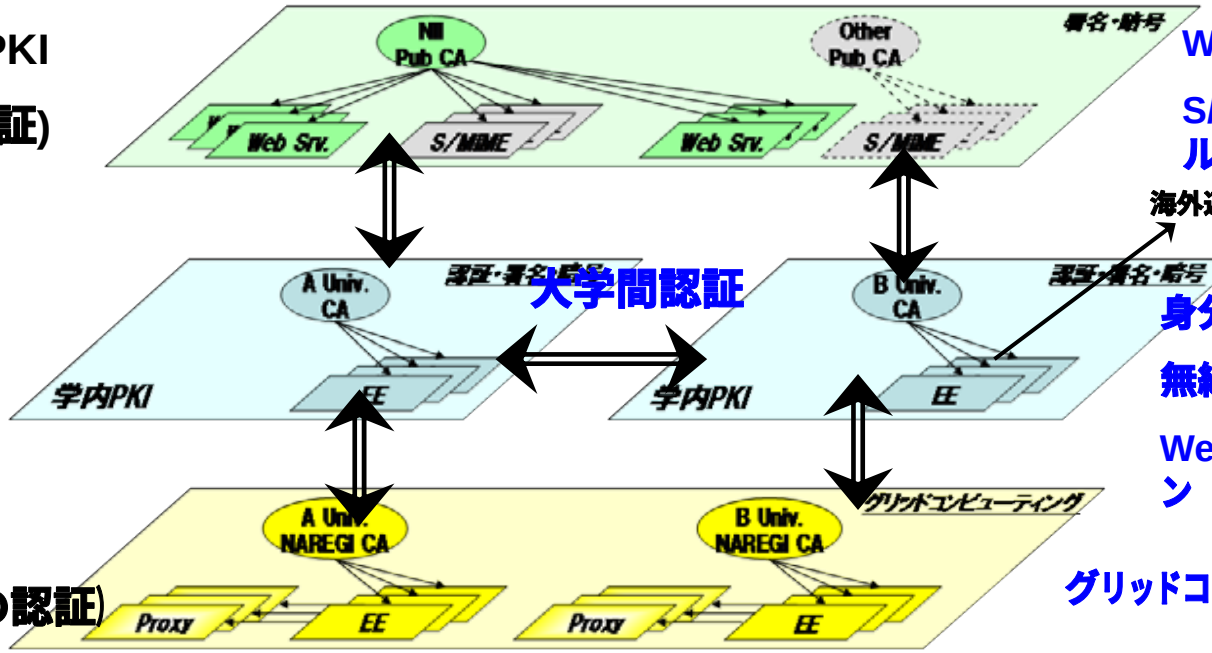
UPKIで開発中のアプリケーション等



UPKI構築の全体スケジュール

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



各PKI層のコンセプト

- オープンドメインPKI
  - いわゆるパブリックPKI
  - ルート証明書が予め配布されたPKI
  - 皆が信頼しているPKI、誰でも検証できるPKI
- キャンパスPKI
  - 各大学が個別のポリシに合わせて構築するプライベートPKI
  - その大学のユーザ(教職員and/or学生)であることを証明する
  - ユーザ(教職員and/or学生)への厳格な(対面等の配付が可能)
- グリッドPKI
  - AP Grid PMAなどグリッド独自のセキュリティレベル
  - プロキシ証明書など一般的なPKIとは明らかに異なる概念

用途に応じたPKI層の使い分け

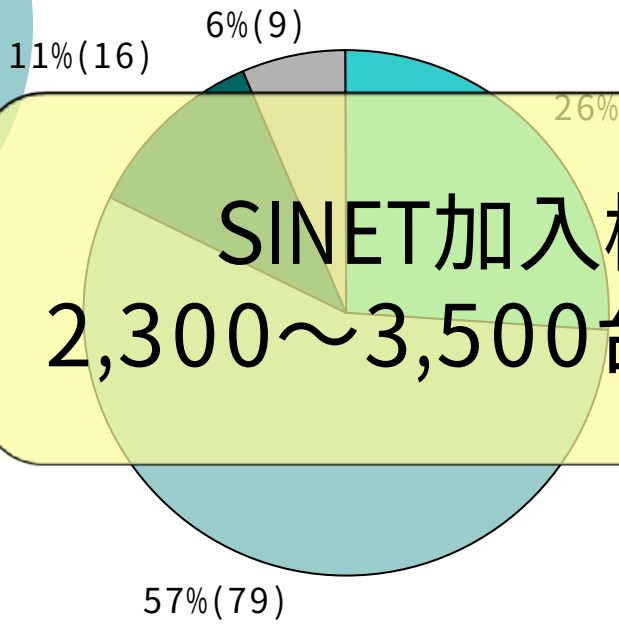
領域	用途	利用する証明書	ポイント
学外(公衆)	サーバ認証	オープンドメインPKIによるパブリックなサーバ証明書	誰でも検証できること
	クライアント認証	キャンパスPKIによるユーザ証明書をベースとしたID連携	保証レベルの担保
	S/MIME(署名･暗号)	オープンドメインPKIによるパブリックなS/MIME証明書	誰でも検証できること
学内	サーバ認証	オープンドメインPKIによるパブリックなサーバ証明書	ルート証明書の配布
	クライアント認証	キャンパスPKIによるプライベートなユーザ(教職員and/or学生)証明書	特定の認証局からのみ検証できること
	暗号	学外同様S/MIMEを利用、または共通鍵による暗号化＋クライアント認証等によるアクセス制御	鍵預託･鍵更新
	署名	キャンパスPKIによるプライベートなユーザ(教職員and/or学生)証明書	本人による鍵生成 または認証局による厳密な鍵ペア配付
グリッド	MyProxy認証	グリッドPKIによるグリッドユーザ(グリッド利用者)証明書	
	Delegation	グリッドPKIのグリッドユーザ鍵ペアによるプロキシ証明書	ユーザによる権限委譲

各PKI層の位置づけ

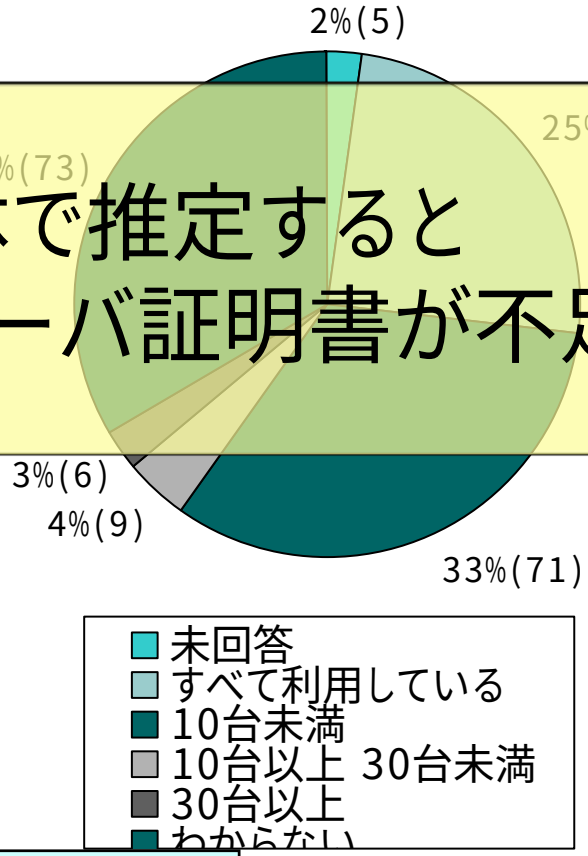
	オープンドメインPKI	キャンパスPKI	グリッドPKI
適用領域	インターネット	各大学内	全国共同利用センター
目的	インターネット上での認証、署名・暗号など	学内NW・システムへの安全なアクセス	計算機資源の安全な共有
用途	主にSSL/TLS認証、その他S/MIME署名・暗号など	Web SSO、VPN、無線LAN（802.1X）、申請・署名アプリ（成績証明書、事務ペーパレス化等）	プロキシ証明書の発行など
証明書発行対象	サーバ、自然人など	教職員、学生など	各地域の計算機資源、計算機利用者など
信頼者（Relying Party）	不特定多数	主に学内関係者	計算機利用者
認証局の運用	オープンドメイン認証事業者など	アウトソース 、インソースなど	全国共同利用センター

大学等におけるサーバ証明書の実態

証明書の利用状況
(未回答･わからないを除く)



証明書を利用できていない台数

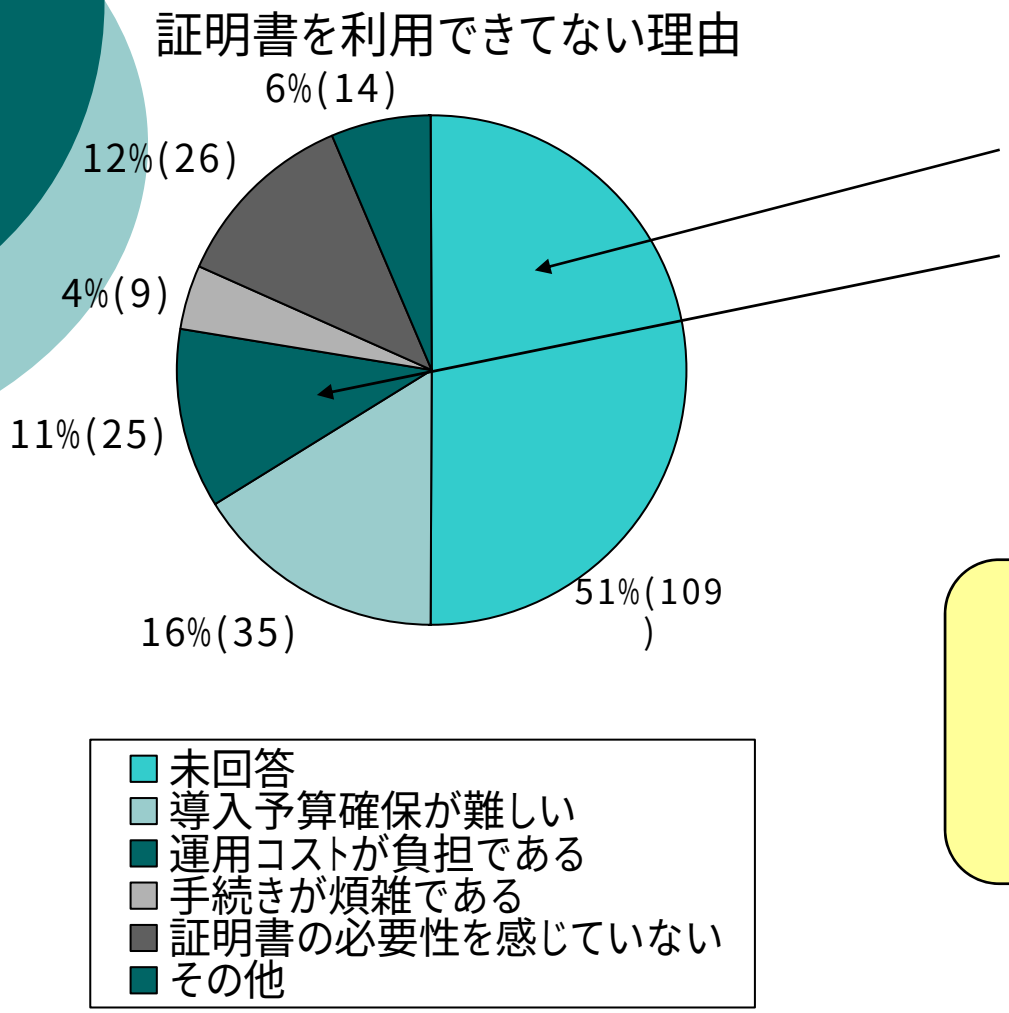


SINET加入機関全体で推定すると
2,300～3,500台分のサーバ証明書が不足

H18年度「大学等における電子証明書の利用状況に関する実態調査」より

対象: SINET加入機関818件、うち有効回答218件

普及が進まない理由



- **理由がわからない!!**
- **運用コストの負担**
  - **実際に生じる負担は?**

実際に使ってもらって
確認してはどうか?

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

認証局を用いた評価研究

体験を通じて啓発

- **目的**
  - **大学等のサーバ証明書の普及を推進**
  - **認証局を用いた研究開発 ⇒ 登録発行業務の改善**
  - **学術機関のWebサーバ信頼性向上**
  - **サーバ証明書の導入･運用ノウハウの共有**
  - **参加者のサーバに対してのサーバ証明書無償配布**
- **期間**
  - 2007/04/01～2009/03/31

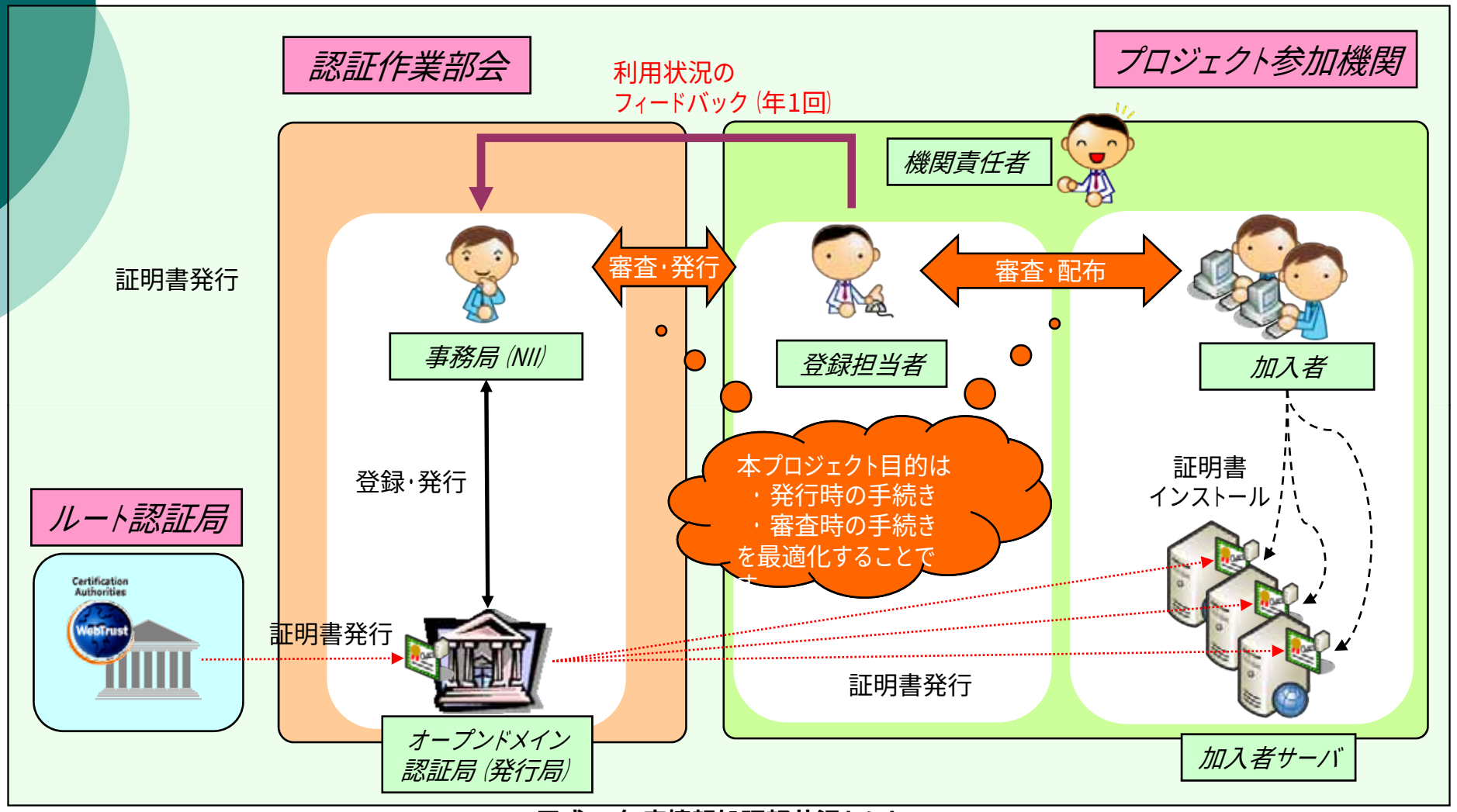
2010/06/30まで有効

- **ゴール**
  - H19年度: **サーバ証明書の普及が進まない理由･課題の整理**
  - H20年度: **サーバ証明書の普及促進の仮説･立証**
  - **将来的に: キャンパスPKI層を活用した証明書発行業務の自動化**
- **主な作業**
  - **プロジェクト参加機関の募集**
  - **各登録担当者へのS/MIME証明書発行**
  - **参加機関が管理するサーバに対するサーバ証明書の発行**
  - **参加機関加入者によるサーバ証明書の導入･運用**
  - **発行手続、導入手順などに対する改善案･Tipsのフィードバック、整理･公開**

証明書発行の基本方針

- 用語の定義
  - **本人性確認**：なりすましや否認を防止するために本人意思を確認する作業
  - **実在性確認**：証明書に記載する組織に実在することを確認する作業
- 審査項目の分担による発行業務の最適化
  - その審査を一番手早く実現できるのは誰か?
  - 認証局が最低限責任を負うべき項目は?
- 商用サービスと同等の保証レベル
  - 機関の実在性認証まで含めた審査項目→分担して実現

プロジェクト概念図


認証作業部会
利用状況の
フィードバック（年1回）
プロジェクト参加機関
機関責任者
証明書発行
審査・発行
審査・配布
事務局（NII）
登録担当者
加入者
登録・発行
本プロジェクト目的は
・発行時の手続き
・審査時の手続き
を最適化することで
証明書
インストール
ルート認証局
Certification Authorities
WebTrust
証明書発行
証明書発行
オープンドメイン
認証局（発行局）
加入者サーバ

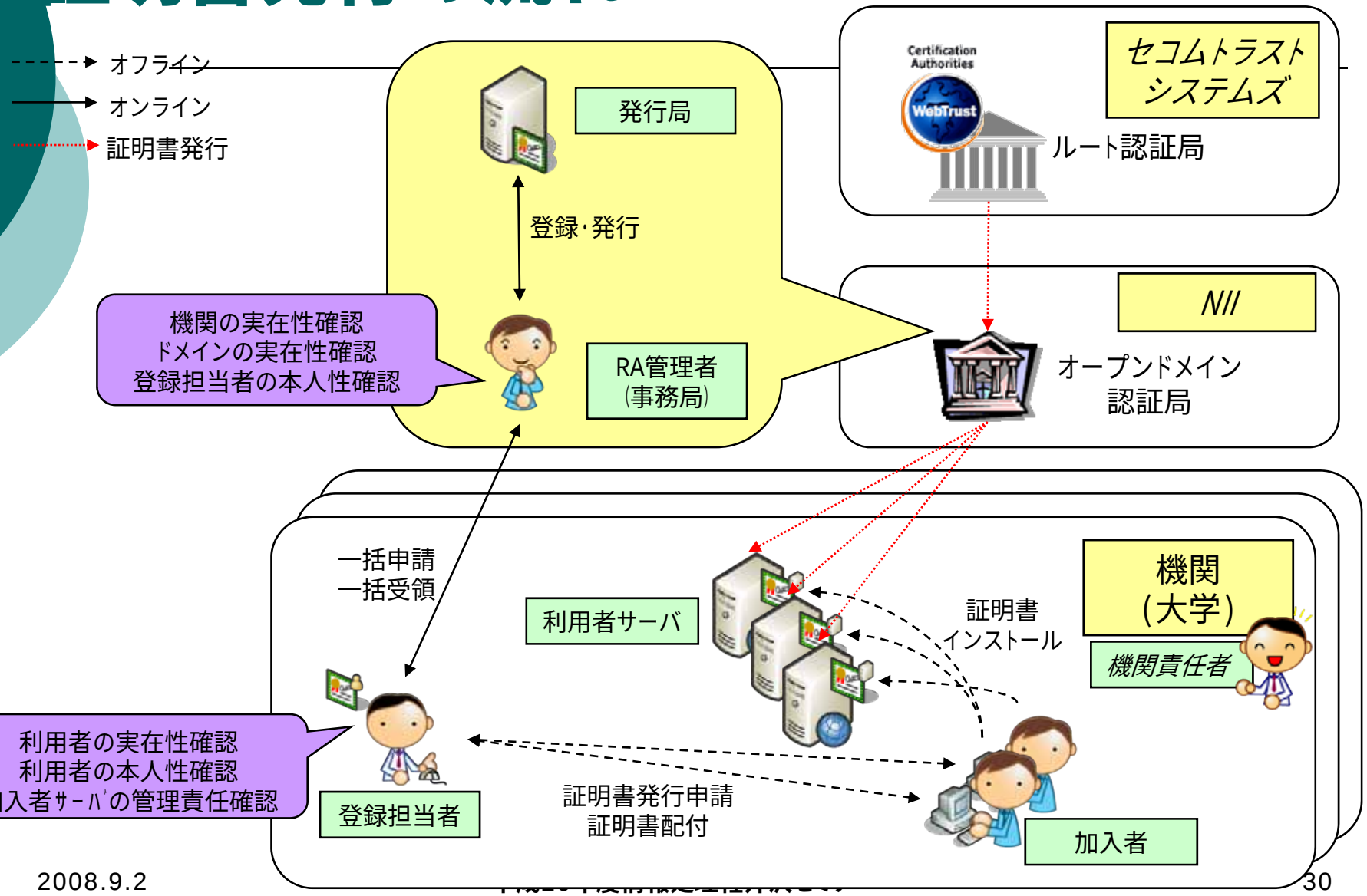
商用証明書との比較
～審査項目の違い～

機関側の審査項目は
確認手順調査表で
チェック

審査者 / 審査項目		商用サービス				本プロジェクト			
		オンライン認証		機関認証					
		登録局	利用者	登録局	利用者	登録局	機関責任者	登録担当者	利用者
機関	本人性確認	×		○					
	実在性確認	×		○		○			
ドメイン	本人性確認	○		○		× →	○		
	実在性確認	○		○		○			
機関責任者	本人性確認					○			
	実在性確認					○			
登録担当者	本人性確認					○			
	実在性確認					× →	○		
加入者	本人性確認	×		○		× →		○	
	実在性確認	×		○		× →		○	
加入者サーバ	本人性確認		○		○				○
	管理責任確認		○		○			○ ←	×

「認証方法の違いによる役割と活用場面（企業の実在性認証とオンライン認証）」より
http://www.verisign.co.jp/server/first/difference.html

証明書発行の流れ


オフライン
オンライン
証明書発行
発行局
登録･発行
RA管理者
(事務局)
機関の実在性確認
ドメインの実在性確認
登録担当者の本人性確認
Certification Authorities
WebTrust
セコムトラスト
システムズ
ルート認証局
NII
オープンドメイン
認証局
一括申請
一括受領
利用者サーバ
証明書
インストール
機関
(大学)
機関責任者
利用者の実在性確認
利用者の本人性確認
加入者ｻｰﾊﾞの管理責任確認
登録担当者
証明書発行申請
証明書配付
加入者

無線LANにおける個人認証方式

- 802.1x
  - **パスワード認証**
    - EAP-TTLS, EAP-PEAP
  - PKI**認証 (クライアント)**
    - EAP-TLS
- RADIUS**サーバ間で認証連携させる**
  - EduRoam
    - **世界規模の大学間認証連携**
    - http://www.eduroam.jp/

(参考) IEEE802.1Xの認証プロトコル

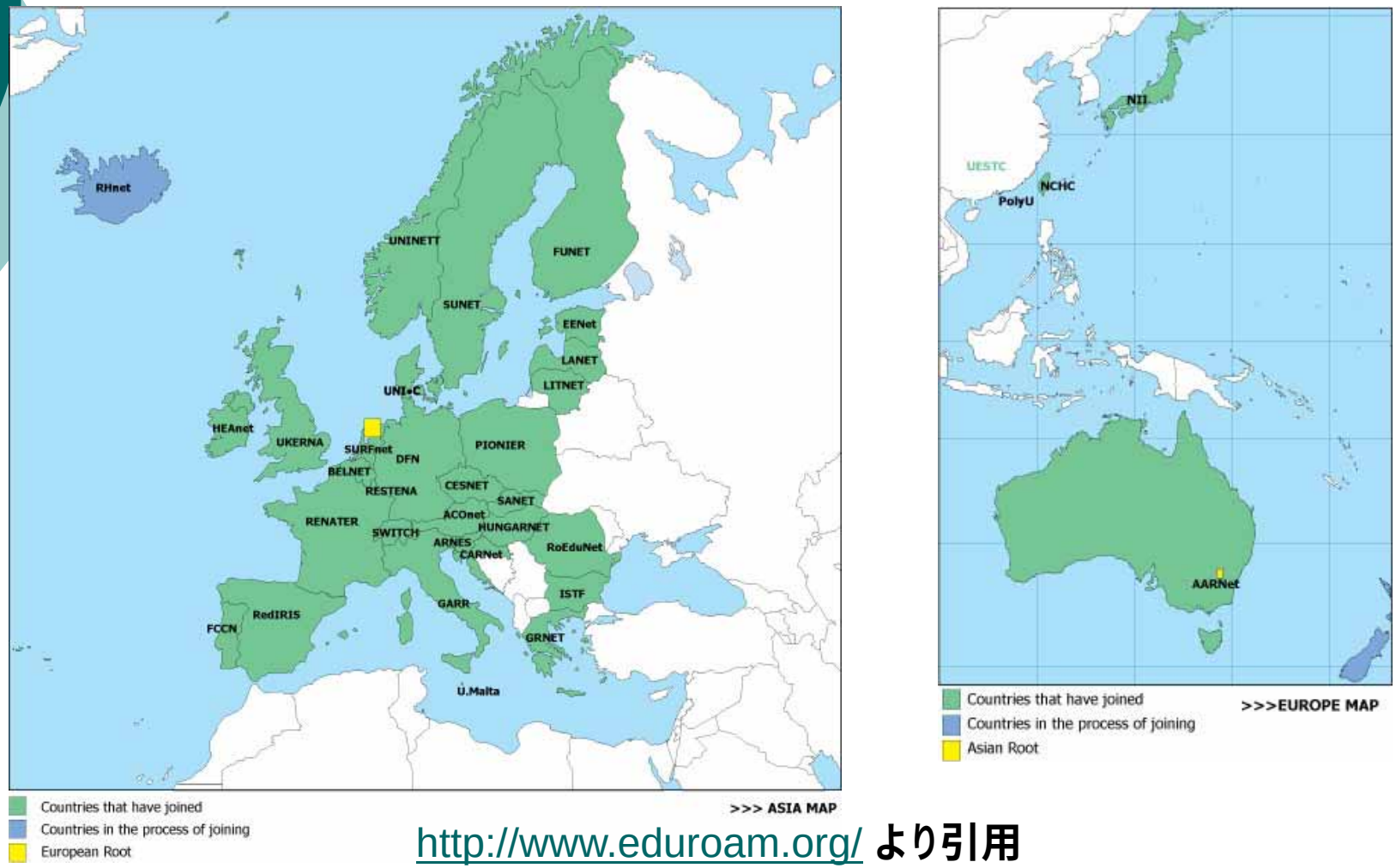
- EAP (Extensible Authentication Protocol)の種類

方式	クライアント認証方式	サーバ認証方式	セキュリティレベル	運用工数
EAP-TLS	証明書	証明書	高	高
EAP-TTLS	ID/パスワード	証明書	中	中
EAP-PEAP	ID/パスワード	証明書	中	中
LEAP	ID/パスワード	ID/パスワード	低	低
EAP-MD5	ID/パスワード	無し	低	低

EduRoamとは

- ヨーロッパを中心とした学術組織による無線LANローミング方式
  - ヨーロッパのデファクトスタンダード
  - オーストラリア、香港、台湾なども参加
- 参加組織に所属する利用者は、他の参加組織で無線LANローミングを利用可能
- 国立情報学研究所(NII)を中心に国立七大学等で導入作業中

EduRoamに参加している国

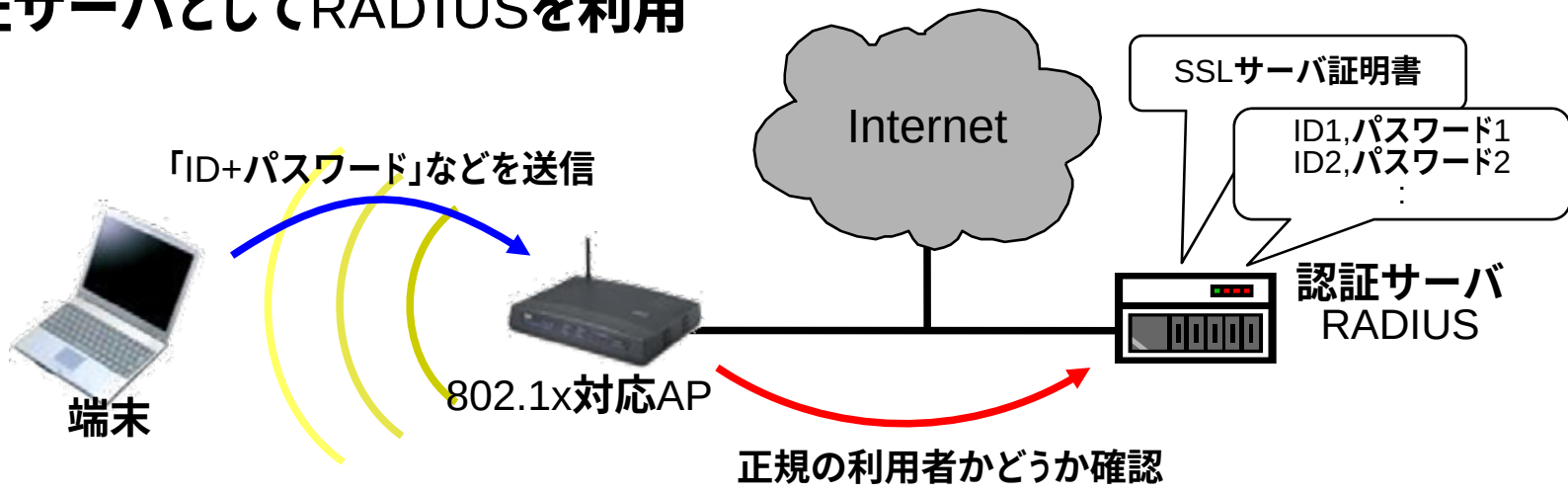


http://www.eduroam.org/ より引用

EduRoamの仕組み(1/2)

IEEE 802.1x を利用

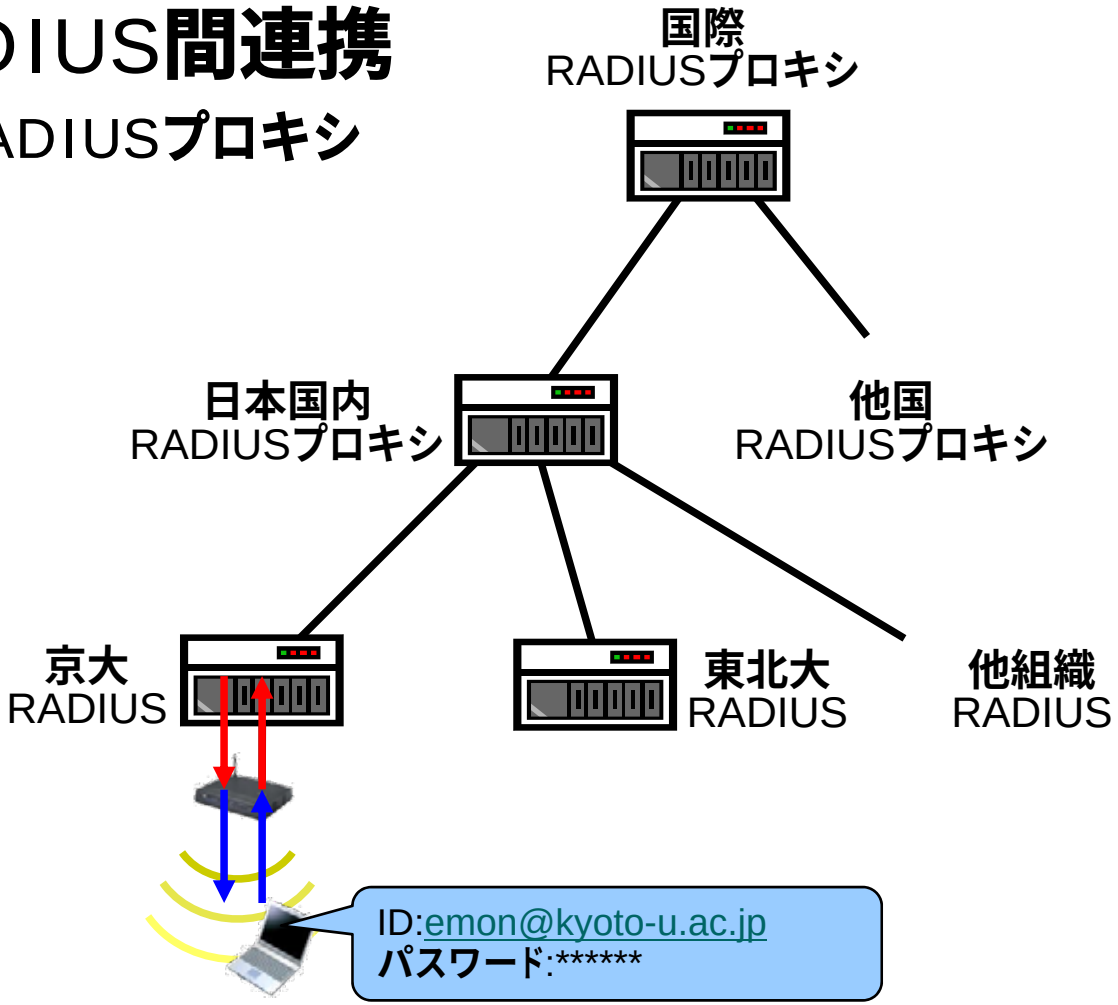
- 無線アクセスポイント(AP)やLANスイッチで
  ユーザを認証するための仕組み
- 「SSLサーバ証明書」でネットワーク(AP)を認証
- 「ID＋パスワード」や「SSLクライアント証明書」で
  端末を認証
- 認証サーバとしてRADIUSを利用



EduRoamの仕組み(2/2)

RADIUS間連携

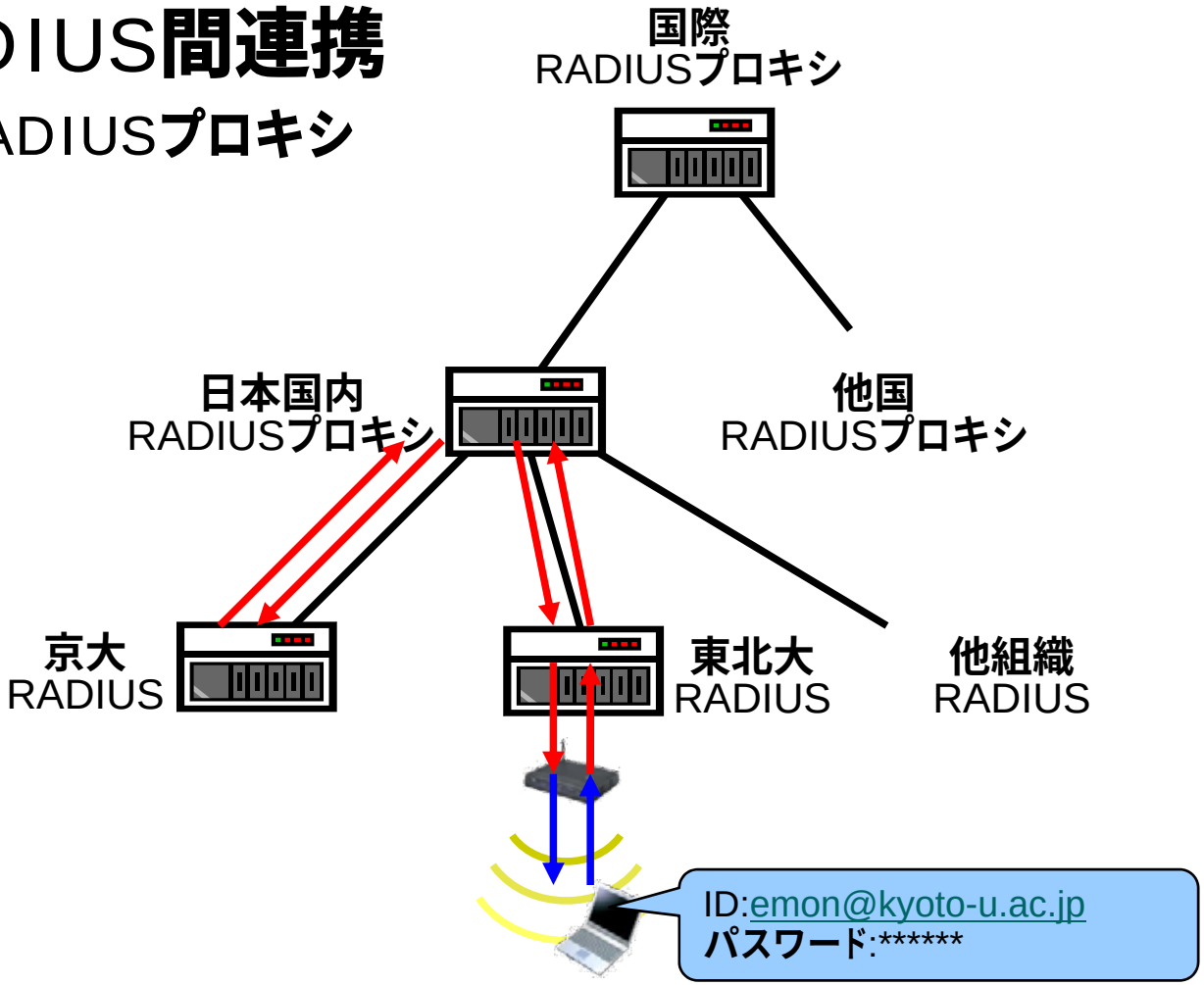
- RADIUSプロキシ



EduRoamの仕組み(2/2)

RADIUS間連携

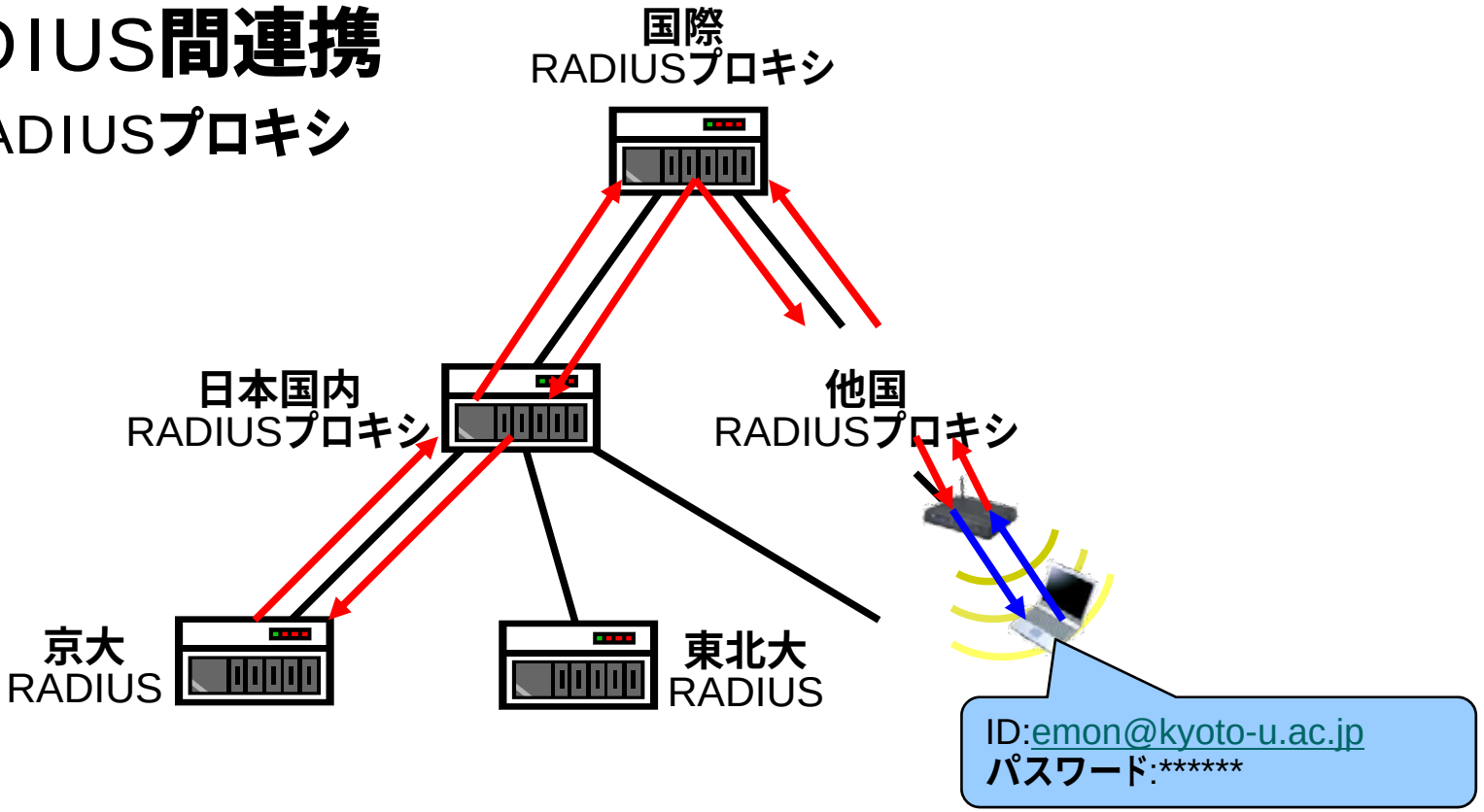
- RADIUSプロキシ



EduRoamの仕組み(2/2)

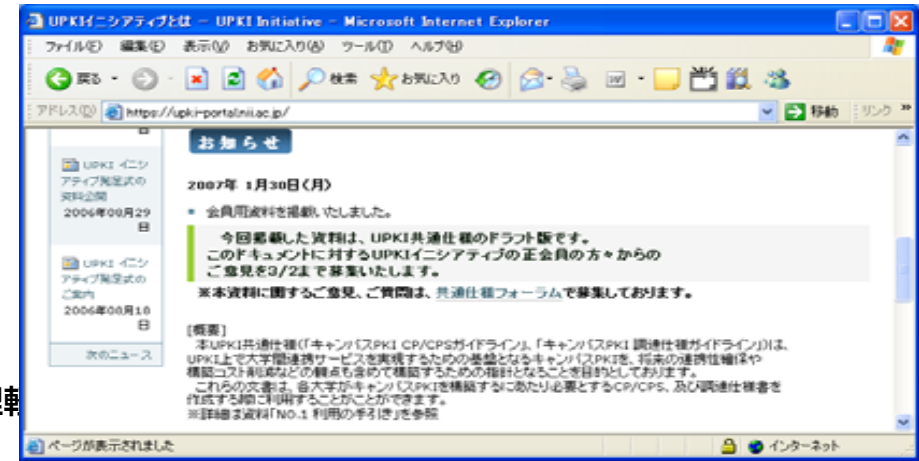
RADIUS間連携

- RADIUSプロキシ



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）
- UPKIイニシアティブの活動に関する情報は，ホームページ上のUPKIポータルから提供
  https://upki-portal.nii.ac.jp/



PKIによる認証基盤構築のための基礎知識

ネットワークセキュリティにおける4つの脅威

- 盗聴
- 改竄（かいざん）
- 成りすまし
  - フィッシング、Man-in-the-middle
- 否認

→ 対策は暗号化と署名（認証）

2つの暗号方式

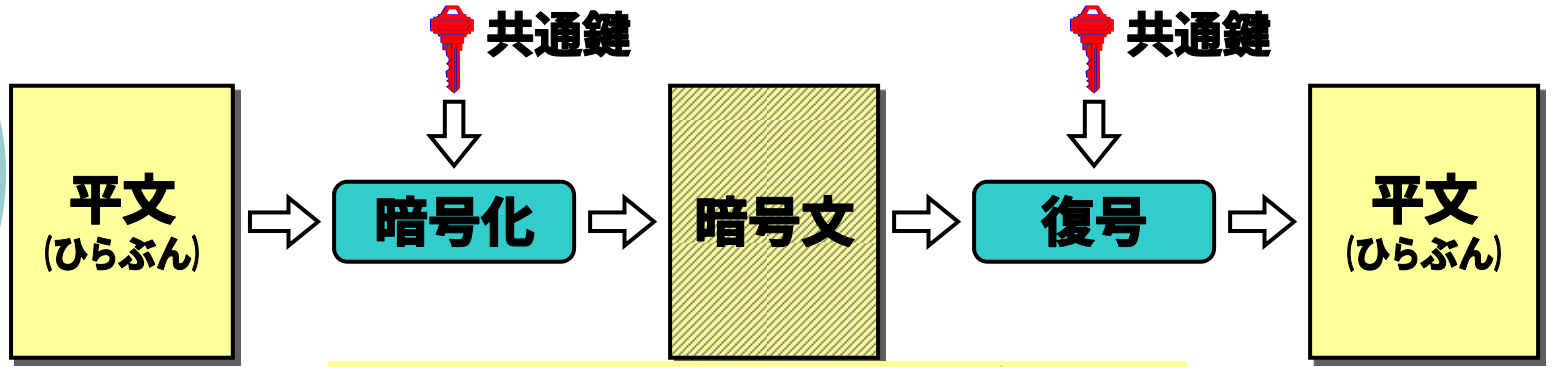
- 共有鍵方式
  - パスワード
    - サーバに生パスワード保存?
    - ネットワークに復号容易なパスワードが流れる?
    - 認証可能な回数に制約? (ワンタイムパスワード)
- 公開鍵方式
  - 公開(public)鍵と私有(private)鍵の2つを用いる
    - 私有鍵は本人のみが持つ
    - 公開鍵は相手を問わず広く公開
  - 暗号化に加えて**署名**を実現

暗号方式の使い分け

- 鍵の数
  - O(n×n) ⇔ O(2n)
- 処理速度
  - 公開鍵暗号の計算は共有鍵暗号より遅い
- 発行のコスト
  - 有効期限の設定
  - 再発行のコスト(失効処理など)
- その他の制限との組み合わせ
  - IPアドレスによる制限等
    - Brute forceアタックの回避

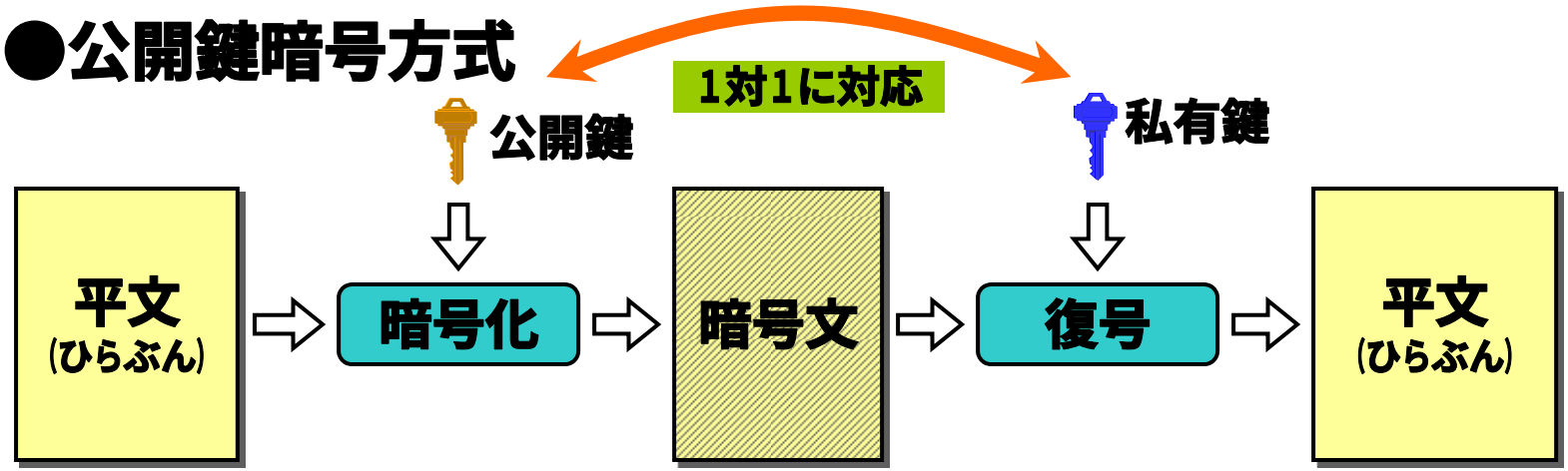
■共通鍵暗号方式と公開鍵暗号方式

●共通鍵暗号方式



→暗号化と復号の鍵が同一

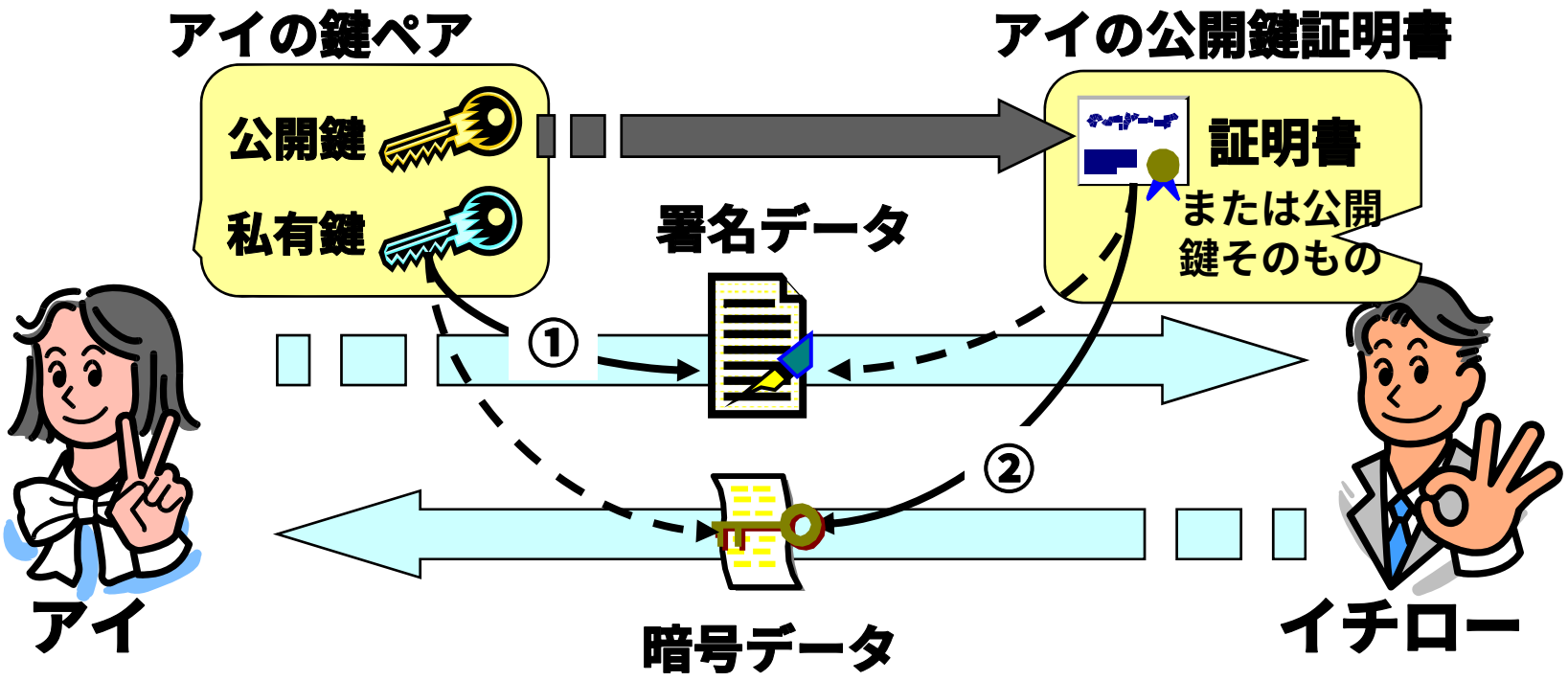
●公開鍵暗号方式



→暗号化と復号の鍵が異なる

■　暗号化と署名

- 以下の仕組みを利用して署名/暗号を実現
  - ①　署　名：私有鍵でエンコード→公開鍵でデコード
  - ②　暗号化：公開鍵でエンコード→私有鍵でのみデコード



公開鍵方式を利用する際の考慮点

- 私有鍵の配布
  - 本人だけに確実に渡す方法
  - 漏洩対策
- 公開鍵の配布
  - 信頼性の確保（なりすまし防止）
- 鍵長
  - 鍵の強度：現在は1024bit以上を推奨

いかに安全に鍵を受け渡すか

- 私有鍵
  - 対面による本人確認
  - 別チャンネルの利用
    - 例：クレジットカード情報はFAXや電話で？
  - 別の認証システムを信頼
- 公開鍵
  - Finger Printを事前に公知
    - 別チャンネルで
  - CA (認証局) による
    - 信頼関係のリンクが切れないよう配慮が必要

公開鍵の利用：SSLサーバ証明書

- https://.....
- **効果**
  - **盗聴防止、改ざん防止（通信の暗号化）**
    - **公開鍵を利用した共有鍵の受け渡し**
      - **処理効率の問題**
  - **（サーバの）なりすまし防止**
    - **サーバ証明書の検証が重要**
    - **サーバ名の確認も重要**
      - **表示とリンクのURLが異なる場合**
        - <A HREF="SITE B">SITE A</A>
      - **フィッシングサイトも正しい証明書を持っているかも**

公開鍵の信頼性の確保

- 事前に安全に配布し、クライアントにインストールさせる
- 認証局(CA: Certificate Authority)による署名、ルートからのパスの確認 (信頼のおける第3者)

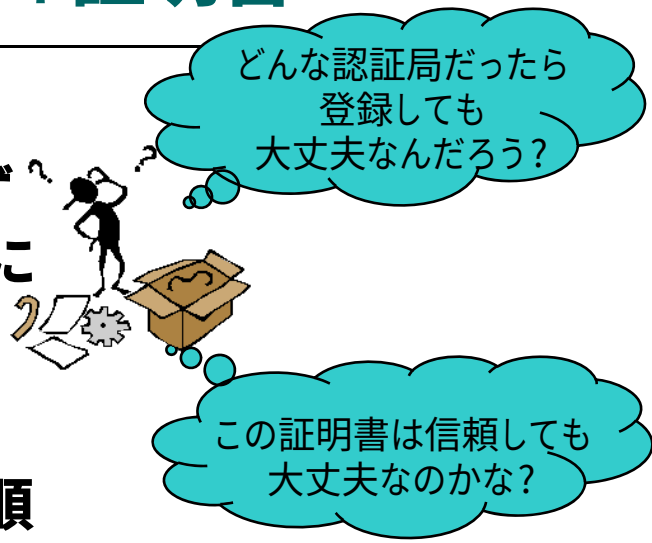
- 信頼性を提供する範囲
  - オープン ドメイン
    - インターネット全域
  - クローズド ドメイン (プライベート認証局)
    - 組織ごと、独自のルート認証局
  - オレオレ証明書 (自己署名のみ)
    - サーバ単位

公開鍵の信頼性の確保（続き）

- 鍵の紛失、盗難、廃止等への対応
  - 廃棄証明書リストの管理
    - CRL: Certificate Revocation List

プライベート認証局とプライベート証明書

- **プライベート認証局**
  - **事前にクライアントに登録されておらずユーザがクライアントアプリケーションに後から登録する必要がある**
- **プライベート証明書**
  - **認証局からの信頼を何らかの追加手順なしには確認することができない**



これらは信頼してもらうには、利用者に何らかの設定や操作をしてもらう必要がある。

ここの確認手順を省略してしまうのがいわゆる「オレオレ証明書」

プライベート証明書は関係者限定の用途以外の利用は困難

オレオレ証明書と大学教育

- 誤った理解
  - 警告が出ても無視していい
    - 何かしらの理由がなければ警告は出ません
  - 警告を回避するには証明書を登録すればいい
    - どんな証明書でも登録していいわけではありません
- 必要な教育
  - 警告の理由と無視してもよい状況の説明
  - 登録してよい証明書といけない証明書の識別方法

十分な教育なしにプライベート証明書を使うことは最高学府として学生にさせるべきではない

オープンドメイン認証局とは?

- **国際規準**WebTrust for CA**に準拠**
  - **認証局の運用の厳格さを審査する規準**
    - **定期的に外部監査を受けているか?**
    - **認証局の鍵ペアは安全に管理されているか?** など
  - **さらに厳密な**EV (Extended Validation)**証明書もある**
- Web**サーバに関する実在性を確認**
  - Web**サーバのドメイン**
  - Web**サーバを所管する機関**
- **主要な**PKI**アプリケーションの証明書リストに予め登録済。**

客観的で公平な規準

証明書用途に適した確認内容

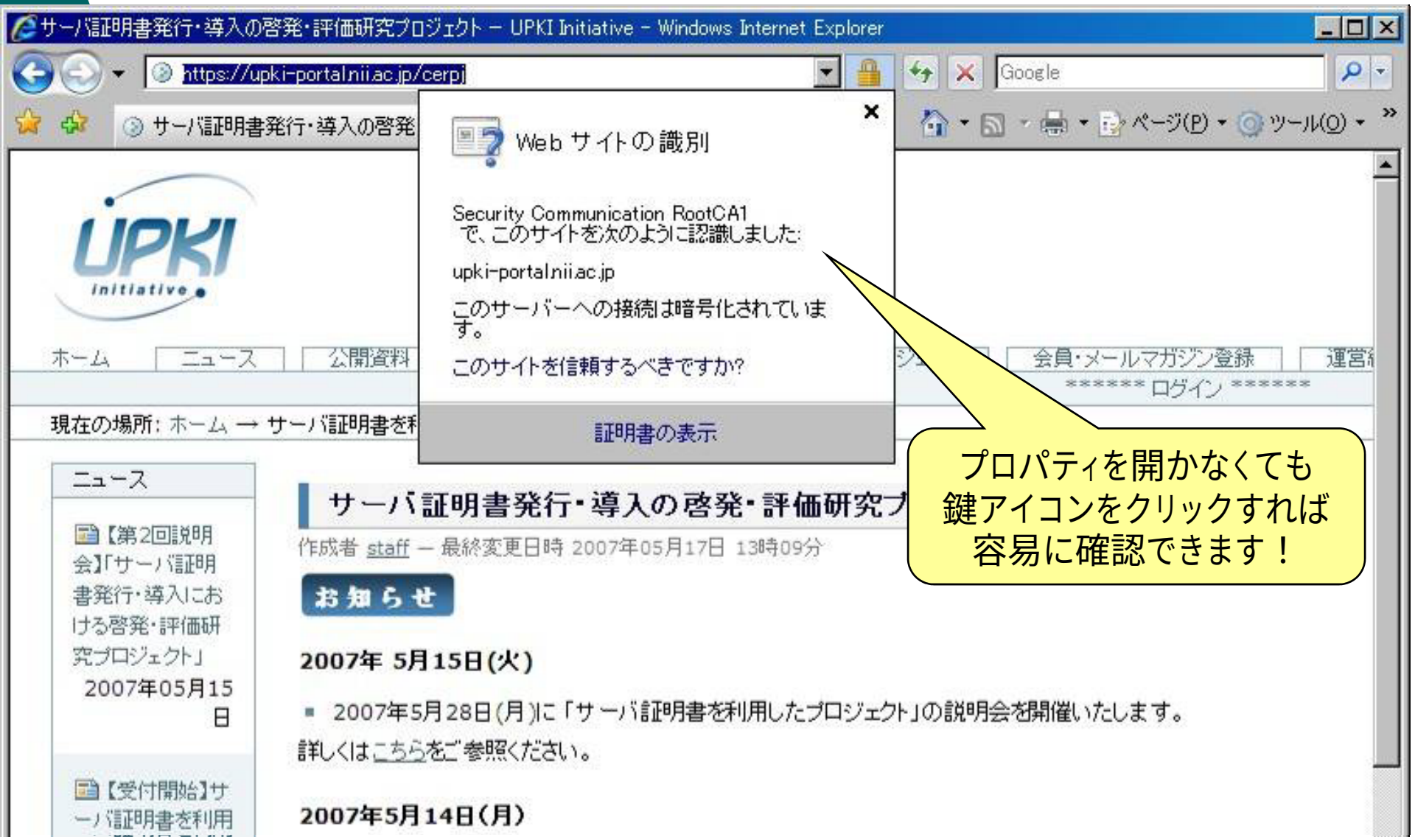
認定された認証局だから安心だね！
何も操作しなくても信頼できるから簡単だね！

オレオレ証明書の区分（高木浩光氏による）

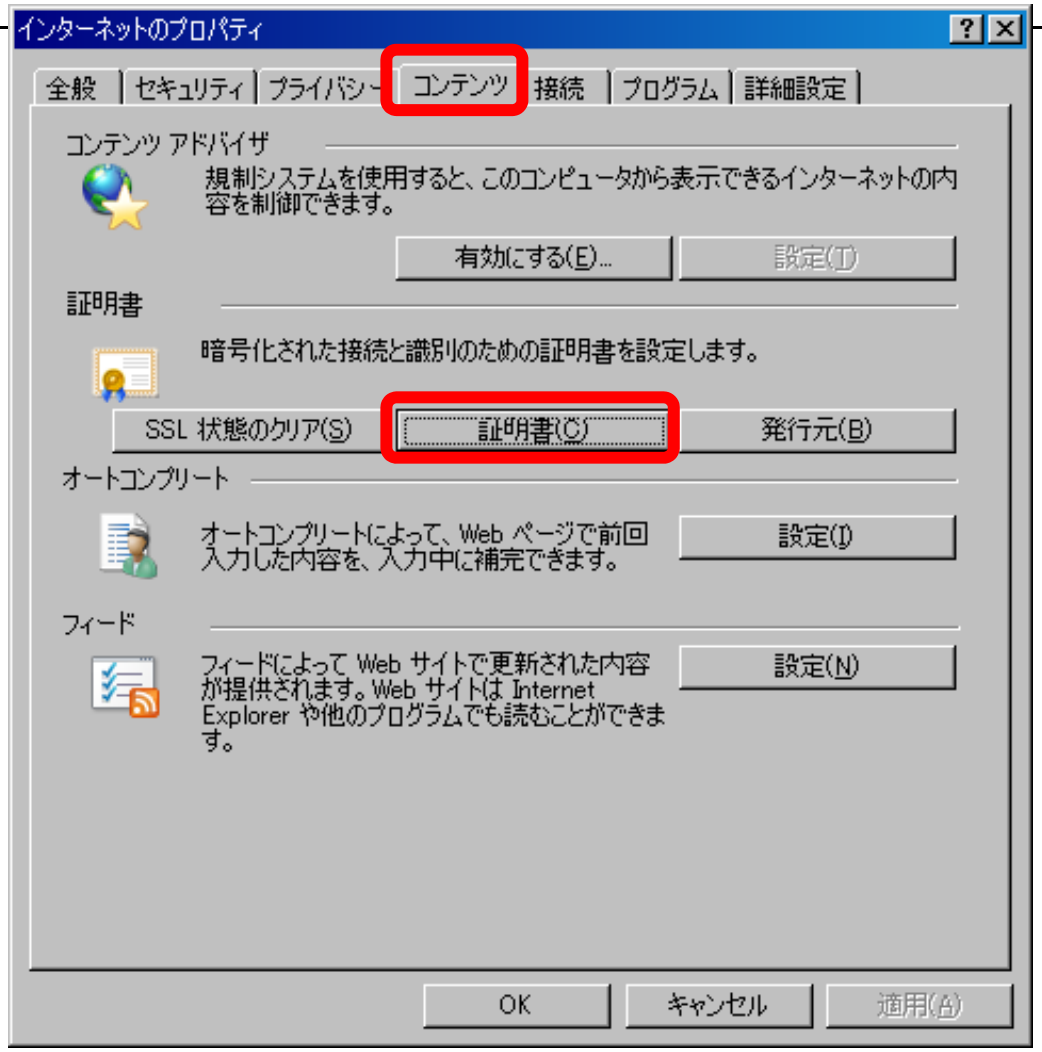
http://takagi-hiromitsu.jp/diary/20051118.html#p01　より

- 第一種オレオレ証明書
  - 不特定多数に利用させることを想定していて、ルート証明書もサーバ証明書もインストールさせるつもりのないもの。
- 第二種オレオレ証明書
  - 不特定多数に利用させることを想定していて、ルート証明書かサーバ証明書をインストールするよう促しているが、インストール方法として安全な手段が用意されていないもの。
- 第三種オレオレ証明書
  - 不特定多数に利用させることを想定していて、ルート証明書かサーバ証明書をインストールするよう促しており、安全なインストール方法が用意されているもの。
- 第四種オレオレ証明書
  - 特定の者だけに利用させることを想定しているもの。
- 第五種オレオレ証明書
  - 正規の認証局から取得したサーバ証明書であるが、一部のクライアントでその認証局がルートとして登録されていないもの。
- 第六種オレオレ証明書
  - 正規の認証局（中間認証局）から取得したサーバ証明書であるが、中間認証局の証明書をサーバに設置していないため、クライアントが認証パスを検証できないもの。

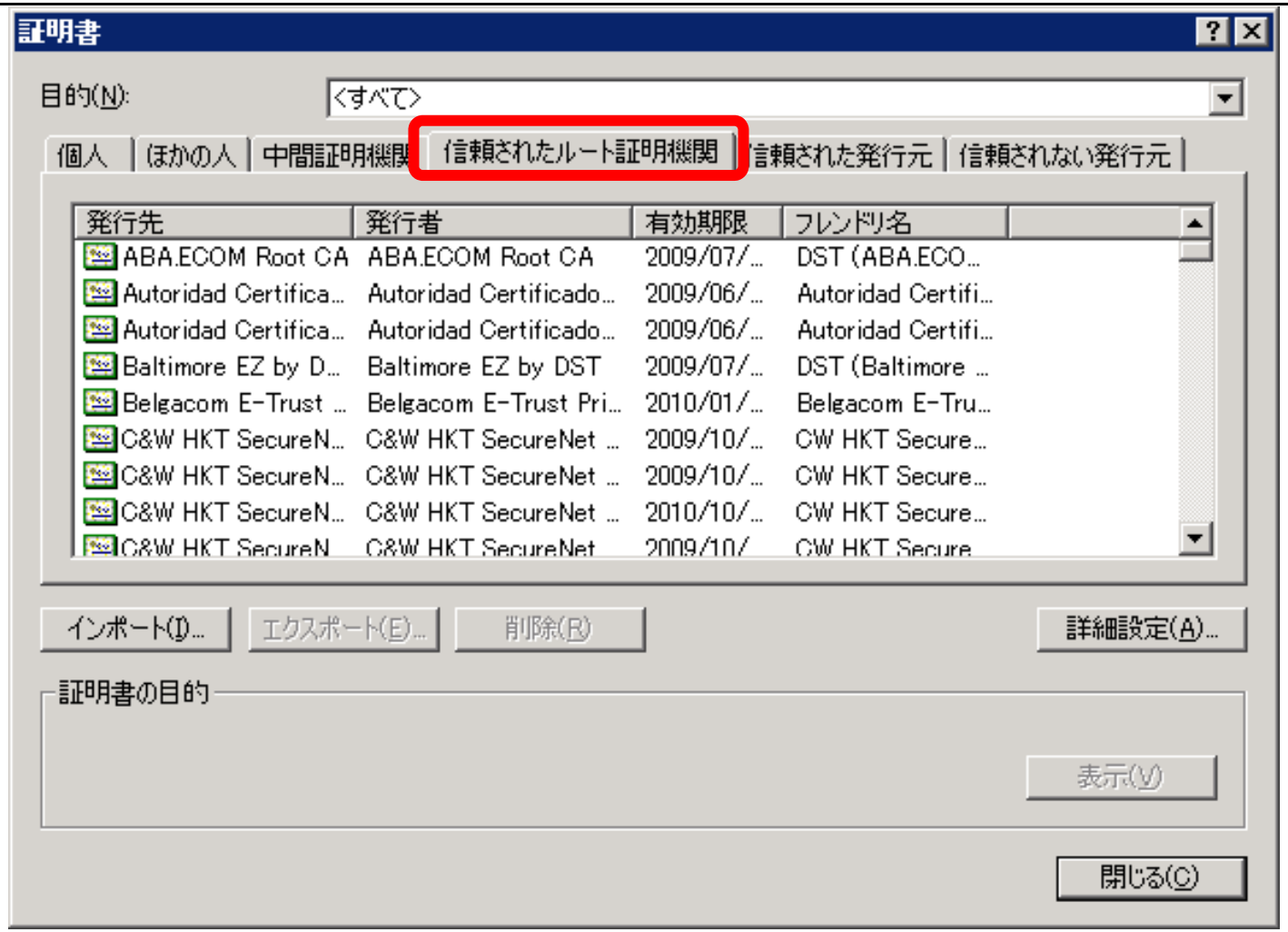
IE 7.0で見るサーバ認証



登録されているルート認証局の確認(1)

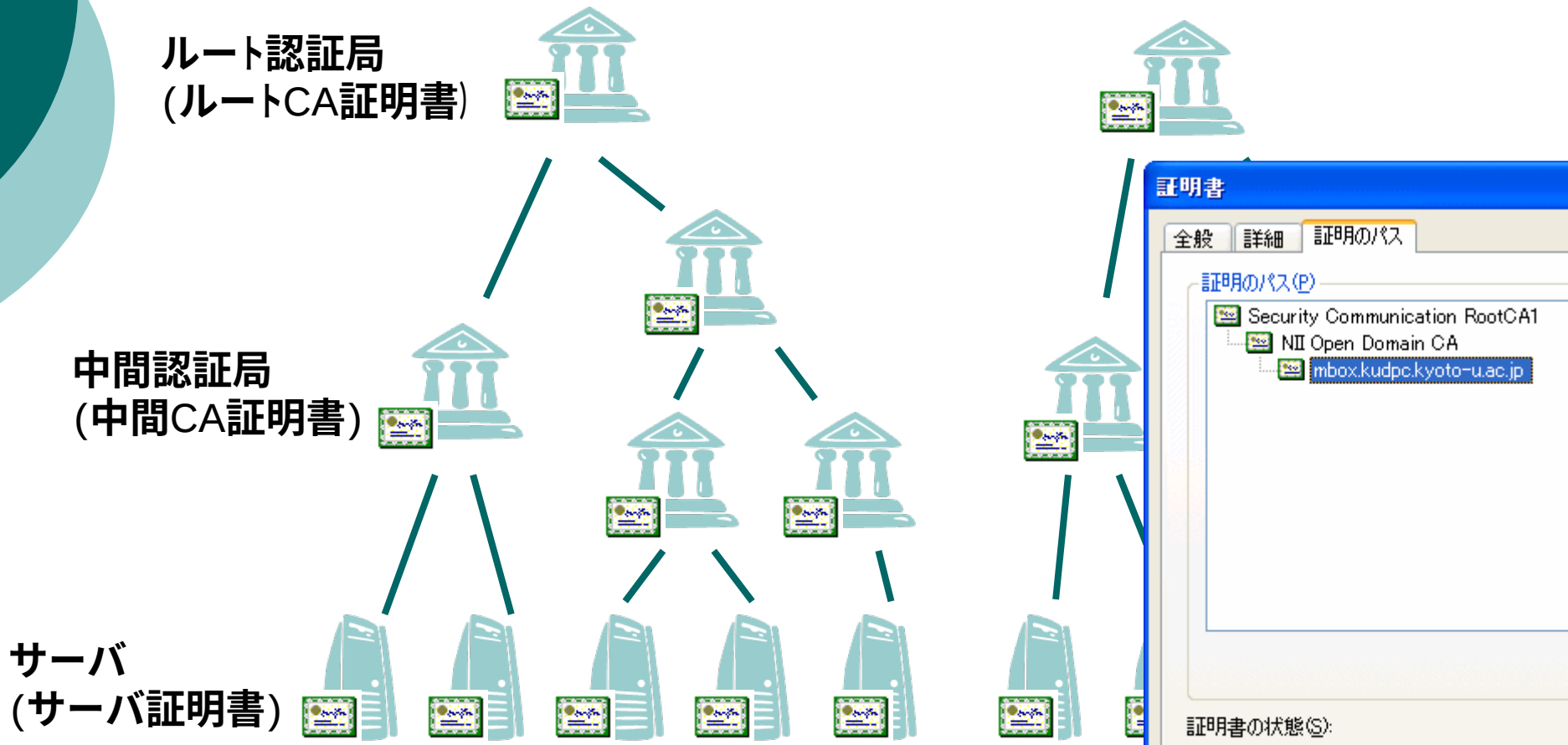


登録されているルート認証局の確認(2)



(クライアントの種類やバージョンで内容が異なることがある)

認証局による署名のパス



サーバから送られる証明書の確認

```
$ openssl s_client -connect mbox.kudpc.kyoto-u.ac.jp:443 –showcerts
depth=2 /C=JP/O=SECOM Trust.net/OU=Security Communication RootCA1
verify error:num=20:unable to get local issuer certificate
verify return:0
---
Certificate chain
 0 s:/C=JP/L=Academe/O=Kyoto University/OU=ACCMS/CN=mbox.kudpc.kyoto-u.ac.jp
   i:/C=JP/L=Academe/O=National Institute of Informatics/OU=UPKI/OU=NII Open Domain CA
-----BEGIN CERTIFICATE-----
MIIFDjCCA/agAwIBAgIERcclAjANBgkqhkiG9w0BAQUFADB3MQswCQYDVQQGEwJK
(中略)
DDMqiKrdxKTa0TTDqYSuSKFDcZiefjMajzFoqbdm4MicEUGMWmdgzTUdUmbUv6q1
j2s=
-----END CERTIFICATE-----
 1 s:/C=JP/O=SECOM Trust.net/OU=Security Communication RootCA1
   i:/L=ValiCert Validation Network/O=ValiCert, Inc./OU=ValiCert Class 1 Policy Validation
   Authority/CN=http://www.valicert.com//emailAddress=info@valicert.com
-----BEGIN CERTIFICATE-----
MIID7zCCA1igAwIBAgICJxIwDQYJKoZIhvcNAQEFBQAwgbsxJDAiBgNVBAcTG1Zh
(中略)
BbA14zB2my/qUSkSJP/l0vkwixtep37CYg8onF/NmzDrK8/uqZeANCHWovBkWMiB
C2si
-----END CERTIFICATE-----
 2 s:/C=JP/L=Academe/O=National Institute of Informatics/OU=UPKI/OU=NII Open Domain CA
   i:/C=JP/O=SECOM Trust.net/OU=Security Communication RootCA1
-----BEGIN CERTIFICATE-----
MIIETjCCAzagAwIBAgIEErmwtjANBgkqhkiG9w0BAQUFADBQMQswCQYDVQQGEwJK
(中略)
2rSrUmGX0HCJNFAK5BlQkUWE5XFn0zRWoZmsGbGKgIBDwSGhsvWR3IU6KamOwqE4
gVs=
-----END CERTIFICATE-----
```

-CApathを指定していないので警告がでている

(送信順)
サーバ証明書

ルートCA証明書

中間CA証明書

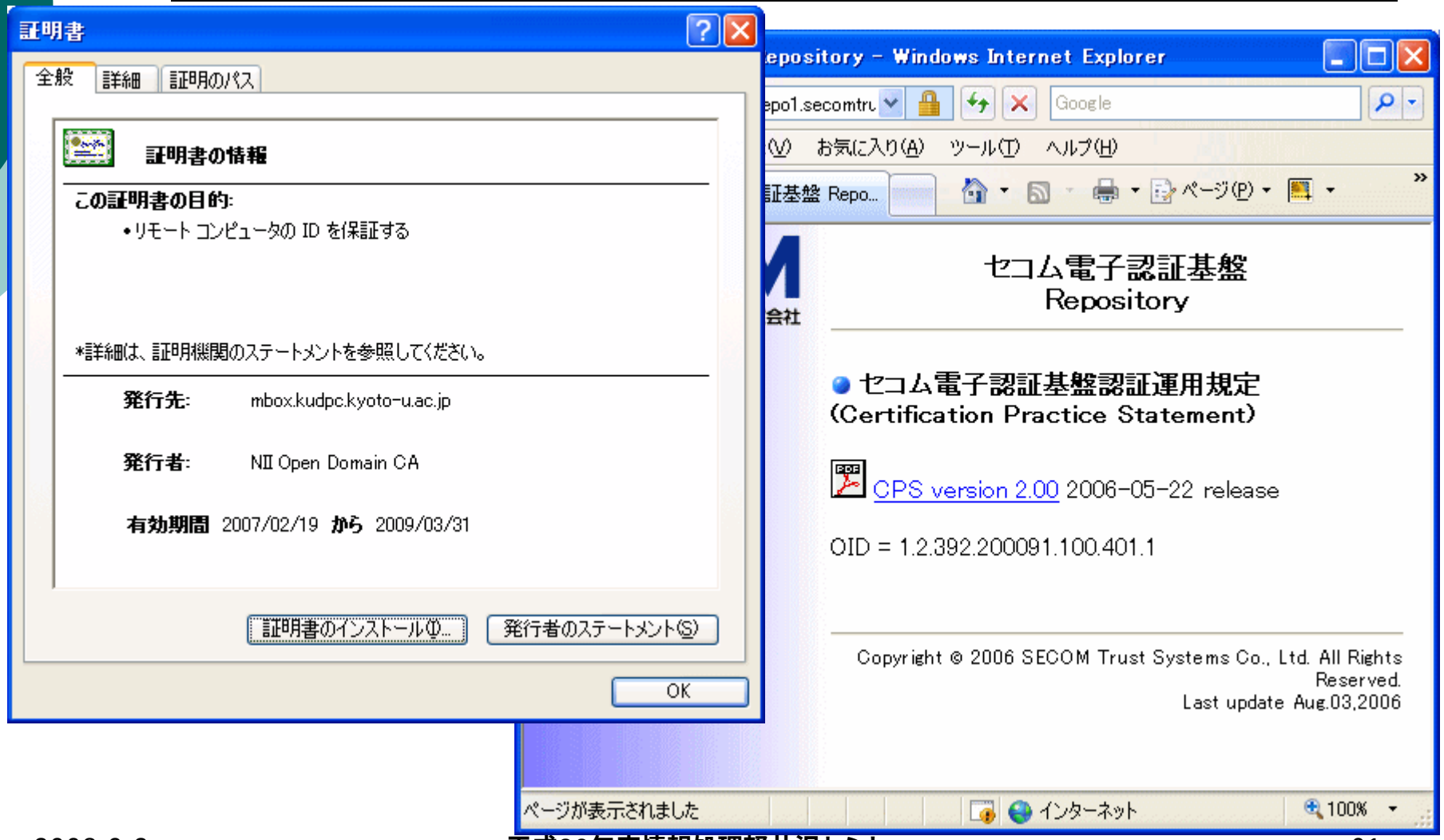
サーバから送られる証明書の確認 (続き)

サーバ証明書に関する情報

SSLセッション情報

```
---
Server certificate
subject=/C=JP/L=Academe/O=Kyoto University/OU=ACCMS/CN=mbox.kudpc.kyoto-u.ac.jp
issuer=/C=JP/L=Academe/O=National Institute of Informatics/OU=UPKI/OU=NII Open Domain CA
---
No client certificate CA names sent
---
SSL handshake has read 3977 bytes and written 332 bytes
---
New, TLSv1/SSLv3, Cipher is EDH-RSA-DES-CBC3-SHA
Server public key is 1024 bit
SSL-Session:
    Protocol  : TLSv1
    Cipher    : EDH-RSA-DES-CBC3-SHA
    Session-ID: D44700F8E1CF3C636DCDB3266A1771FF427C20BD79B261BF6582EB93E9E333D3
    Session-ID-ctx:
    Master-Key: C61D395A6D79968473ADB96995FC1078F1C2DE2DD924AE51B3FC5BF9B43C131
      8B6F9EE4DA5EE95E9CC2CA0E9B04BD003
    Key-Arg   : None
    Start Time: 1219784761
    Timeout   : 300 (sec)
    Verify return code: 20 (unable to get local issuer certificate)
---
(Control-D)
DONE
>
```

証明書の情報と、発行者のステートメント



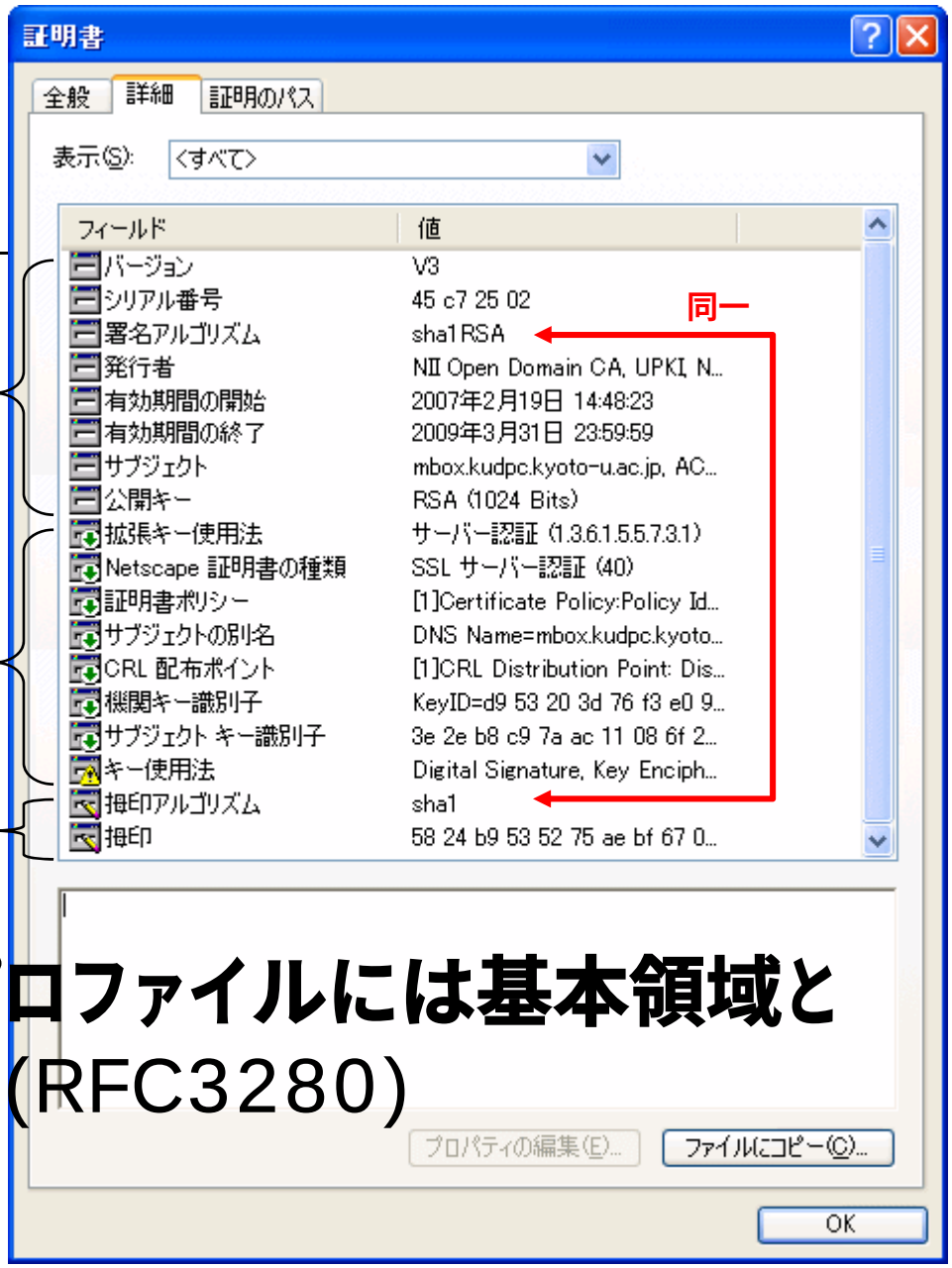
証明書の詳細

これらに対して
署名（押印）
アルゴリズムを
用いて計算し、
CAの私有鍵で
暗号化したものが
署名（押印）

基本領域

拡張領域

基本領域



- X.509**証明書プロファイルには基本領域と拡張領域がある**(RFC3280)

証明書の主な項目 (1)

- Issuer (**発行者**)
- subjectDN(**サブジェクト**) :**所有者識別子**
  DN (Distinguished Name)**で表現**
  - CN = mbox.kudpc.kyoto-u.ac.jp (commonName)
    DNS**の**FQDN**に一致**
  - OU = ACCMS (organizationUnit)
  - O = Kyoto University (organizationName)
  - L = Academe (localityName)
  - C = JP (country)
- validity (**有効期間**:**開始、終了**)
  - **有効期間外のものは無効**
- serialNumber (**シリアル番号**)
  - CA**で管理される通し番号、失効処理に必要**

証明書の主な項目（2）

- keyUsage（**キー使用法**）
  - digitalSignature（**デジタル署名**）、nonRepudiation（**否認防止**）、keyEncipherment（**鍵配布**）、dataEncipherment（**データ暗号化**）、keyAgreement（**鍵の検証**）、keyCertSign（**鍵署名**）、cRLSign（**証明書失効リストの検証**）、encipherOnly（**暗号化のみ**）、decipherOnly（**復号化のみ**）**の組み合わせ**
- extendedKeyUsage（**拡張キー使用法**）
  - serverAuth（**サーバ認証**）、clientAuth（**クライアント認証**）、codeSigning（**コード署名**）、emailProtection（S/MIME**など**）、timeStamping（**タイムスタンプ**）**などの組み合わせ**
- CRLDP（CRL**配布ポイント**）
  - CRL**へのアクセス方法**
- certificatePolicies（**証明書ポリシー**）
  - CPS**の**ODI、URL**など**

証明書等のファイル形式

表現（エンコーディング）

- DER (Distinguished Encoding Rules)**形式**(.der)
  - X.509**等のバイト配列形式によるバイナリ**
- PEM (Privacy Enhanced Mail)**形式**(.pem)
  - DER**を**base64**でテキストにしたもの**
  - **秘密鍵・公開鍵を**base64**でテキスト形式にしたもの**(.key?, .pub?)

内容

- X.509 (.cer, .crt)**形式**
  - ASN.1 (Abstract Syntax Notation One)**形式（バイナリ）**
- PKCS#7 (.p7c, .p7s, .p7m)**形式**
  - S/MIME**など暗号メッセージ構文**(CMS: Cryptographic Message Syntax)**として利用される（公開鍵、証明書、署名のやりとりなど）**
- PKCS#10 (.p10, .csr)**形式**
  - CSR**の格納に使われる**
- PKCS#12 (.p12, .pfx)**形式**
  - **秘密鍵と公開鍵を一つのファイルで扱うことができる**
  - **パスワードで保護可能**

PKCS: Public-Key Cryptography Standards (RSA Security**社**)

CSR: Certificate Signing Request
証明書署名要求

- 証明書発行に必要な情報を申請者から認証局に通知するためのもの
  - 公開鍵と秘密鍵の鍵ペアを生成し
  - 申請者識別子（サブジェクト）と公開鍵などの情報をCSRに含め
  - 秘密鍵で署名する
- 認証局に確実に渡し、認証局は証明書を発行してもよいかどうか審査する（実在性確認、本人性確認）

CRL: Certification Revocation List
証明書失効リスト

- 当該認証局により発行した証明書のうち
  失効済みの証明書の一覧
  - シリアル番号
  - 失効理由 (失効:Revoked、停止:Hold)
  - CRL発行日時
  - CRL発行者

  など
- 証明書と同様に認証局が署名
- 証明書の有効性確認のため参照される
- 定期的に更新

サーバ証明書の検証 (クライアントで)

- 用途(フラグがcriticalの場合)
- 有効期限
- commonNameとFQDNの一致
- 上位CAの証明書 (公開鍵) を用いたサーバ証明書の改竄の確認
- CAの証明書のチェインの確認
  - 中間CA証明書はサーバが提供
  - ルート (既知の) CAまでたどれるか？
- 各CA証明書の改竄確認
- 各CAのCRL確認、CRLの改竄確認

PKIシステムの運用

- 認証局の運用
  - インソース
    - 自前でサーバを設置･運用
      - 認証局の安全性の確保も自前で
  - アウトソース
    - 外部委託
      - 全て / IA:Issuing Authorityのみ
- 登録局(RA: Registration Authority)
  - 証明書発行依頼業務（審査）
    - ユーザの実在性確認
    - ユーザの本人性確認
- 信頼性の担保
  - 運用ポリシーの策定、公開と、それに基づく運用、監査

運用コストの問題

- オープンドメイン⇔クローズドドメイン
  - 利便性･信頼性
- インソース⇔アウトソース
  - 初期費用と維持費用のトレードオフ
- RAをどこまで展開するか (分散ー集中)
- 有効期限
  - 鍵の更新、再配布
- CP/CPSをどこまで厳密に定めるか

運用ポリシー：CP/CPS

- **証明書ポリシー** (CP: Certificate Policy)
  - 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
- **認証局運用規定**
  (CPS: Certification Practice Statement)
  - 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

PKIの応用

- ネットワークアクセスローミング
- 別サービス用アカウント等の自動発行
- GRIDのアクセス認証
- 共有データベースの認証
- 大学間単位互換
- シングルサインオン
- フェデレーション
- タイムスタンプ、長期署名
  - 実験ノート、知財
  - ：

まとめ

- PKIの活用事例：UPKIのとりくみ
  - 共通仕様
  - オープンドメインサーバ証明書発行
  - 無線LANローミング
  - シングルサインオン
  - 認証局ソフトウェアパッケージ
  - S/MIME
- PKIによる認証基盤構築のための基礎知識
  - 信頼性確保の重要性
  - PKIシステム運用のコスト

各大学での様々な取り組み(1)

- **東北大学**
  - http://www2.he.tohoku.ac.jp/center/risyuu/pamphlet.pdf
- **東京大学**
  - http://www.pki.itc.u-tokyo.ac.jp/
- **東京工業大学**
  - http://portal.titech.ac.jp/
- **名古屋大学**
  - http://www.icts.nagoya-u.ac.jp/nuid/index.htm
- **京都大学**
  - https://upki-portal.nii.ac.jp/item/idata/odatao/csi20060517/CSIsession4.pdf/download
- **大阪大学**
  - http://repository.cmc.osaka-u.ac.jp/ja/index.html
- **九州大学**
  - http://www.slrc.kyushu-u.ac.jp/japanese/project/iccard/

各大学での様々な取り組み(2)

- **筑波大学**
  - https://account.tsukuba.ac.jp/index.html
- **群馬大学**
  - http://account.media.gunma-u.ac.jp/
- **名古屋工業大学**
  - http://www.cc.nitech.ac.jp/news/20070324_01_i.html#pagetop
- **広島大学**
  - http://auth.hiroshima-u.ac.jp/
- **高知大学**
  - http://www.iic.kochi-u.ac.jp/ipc/system/ldap.htm
- **福岡大学**
  - http://www.ipc.fukuoka-u.ac.jp/service/index.html#ninsho

- **文部科学省**
  - https://shinsei-cert.mext.go.jp/guide/ninsyo/index.html
- **政府認証基盤**(GPKI)
  - http://www.gpki.go.jp/documents/gpki.html