UPKI構築事業の概要

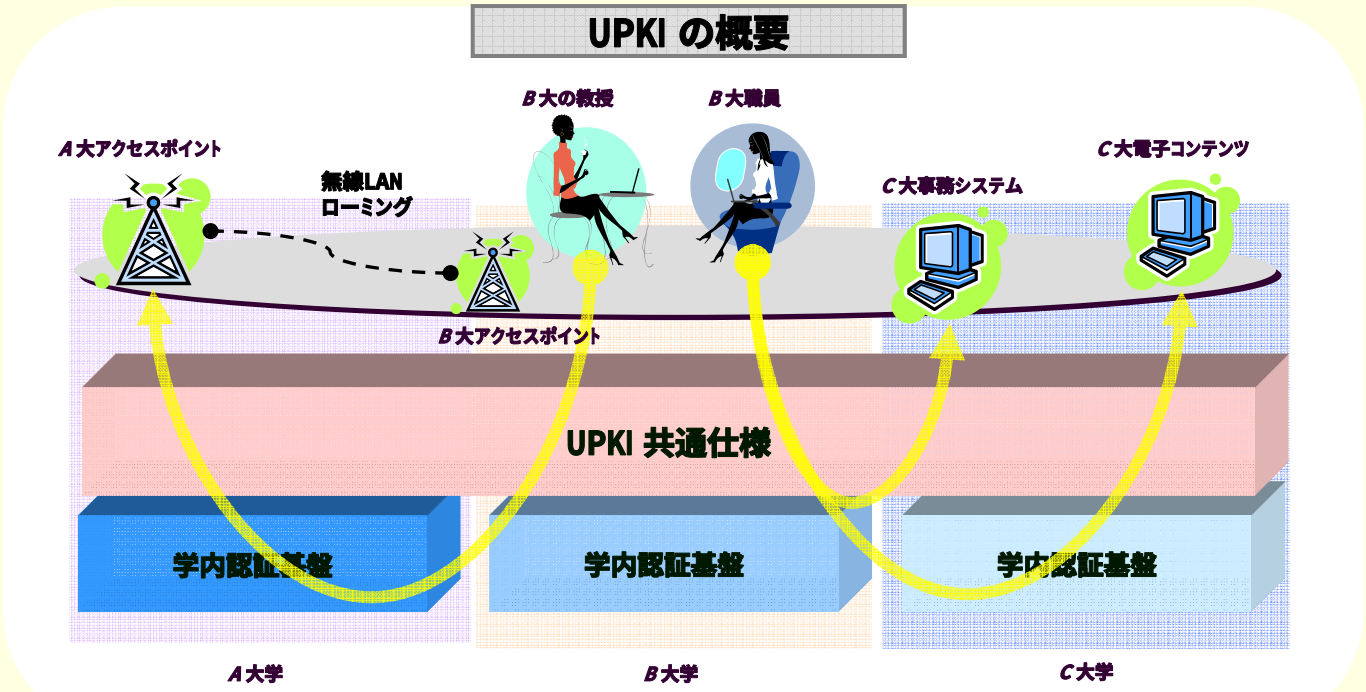
岡部寿男

国立情報学研究所 学術情報ネットワーク運営・連携本部 認証作業部会主査

京都大学学術情報メディアセンター教授

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を安心･安全かつ有効に活用するための電子認証基盤**



UPKIのこれまでの経緯

- **平成16年度：**

  全国共同利用情報基盤センター長会議（構成：7大学情報基盤センター＋NII）の下に「認証研究会」を設置

- **平成17年度：**

  国立情報学研究所 ネットワーク運営・連携本部の下に「認証作業部会」を設置（構成：7大学情報基盤センター，東工大，KEK，NII）

- **平成18年度：**

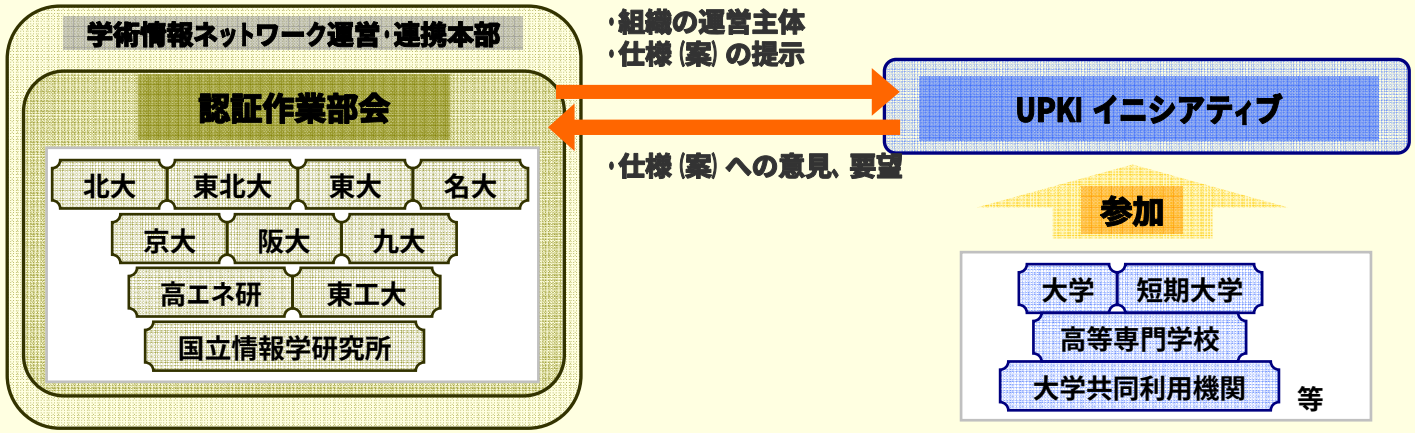
  文部科学省から「大学間連携のための全国共同電子認証基盤構築事業」が3年計画として予算が認められる

  - **7大学+NIIで認証アプリケーションの開発等を開始**

  認証作業部会を中心として，UPKIの構築を推進

UPKIの研究開発・連携体制

- 国立情報学研究所内に設置した学術情報ネットワーク運営・連携本部内の認証作業部会を中心として研究開発を推進。
- 認証作業部会が検討した仕様案をUPKI イニシアティブに公開し、イニシアティブ参加者の意見や要望を取入れ認証基盤の構築を進める。



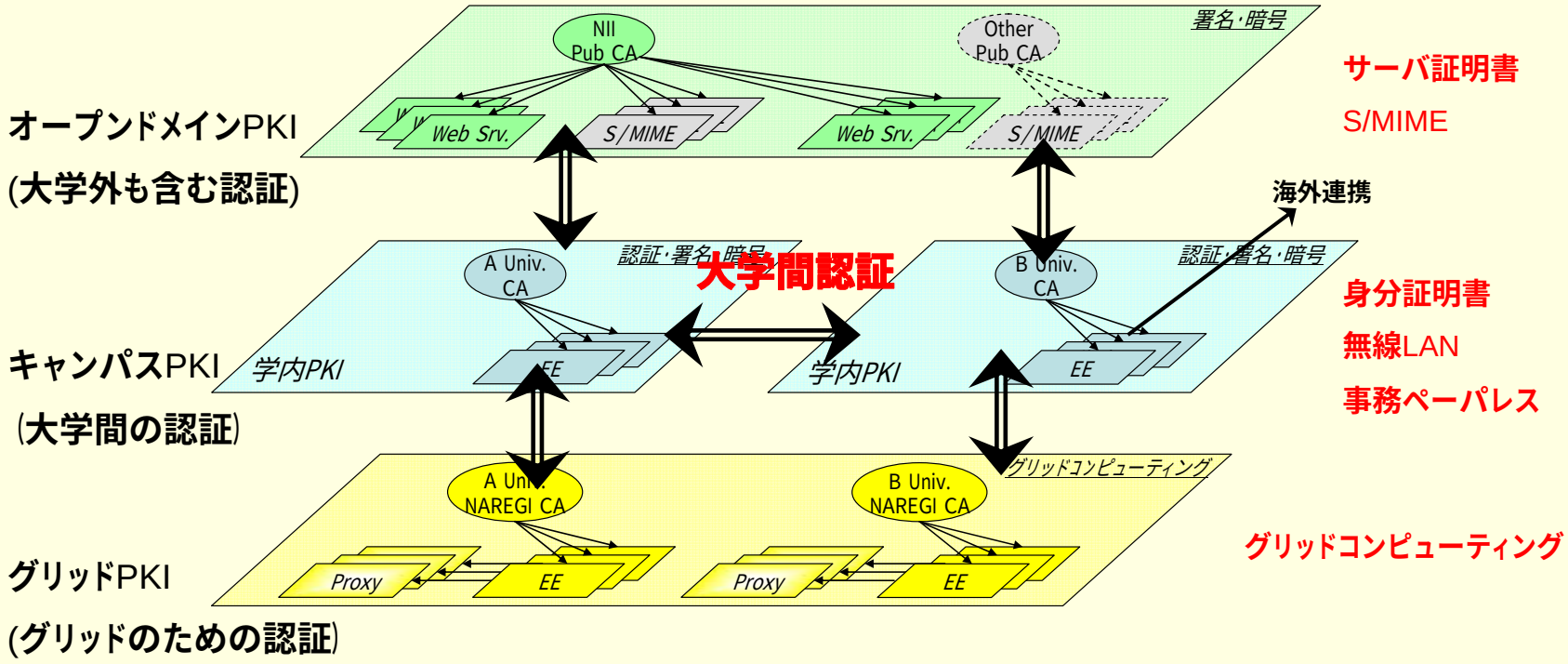
国立情報学研究所
ネットワーク運営･連携本部　認証作業部会

- 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（東北大学情報シナジーセンター）
- 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）

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**



平成18年度の成果

- 今年度は「調査研究」「基本設計」を中心に実施
- 本年度の成果
  (1) UPKI共通仕様の制定
  (2)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
  (3) 大学向け認証局スタートパックの開発
  (4) eduroamによる無線LAN国際連携
  (5) SAML, Shibboleth等のSSO調査・検討
  (6) S/MIME証明書の実証実験
- UPKIイニシアティブの発足

(1)〜(4)については，このあと講演があります。

(5) SAML, Shibboleth等のSSO調査・検討

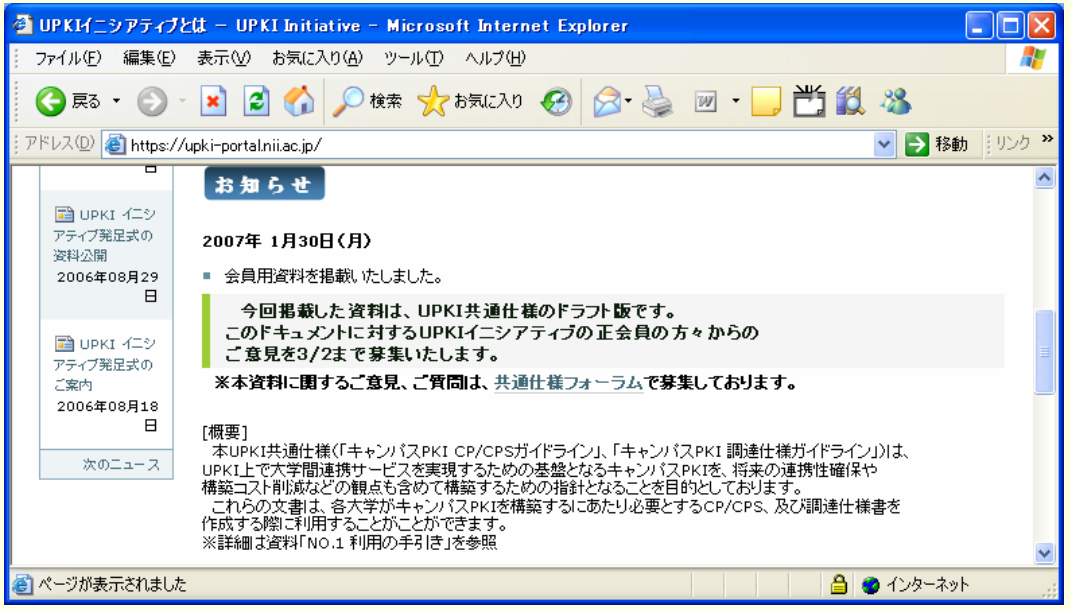
- **Webサービスのシングルサインオンと認証連携のアーキテクチャ検討のため，SAML2.0, Shibboleth等の調査**
  - SAML (Security Assertion Markup Language)
    - Webサービス標準化団体OASIS (Organization for the Advancement of Structured Information Standards)によって策定された、IDやパスワードなどの認証情報を安全に交換するためのXML仕様。
  - Shibboleth
    - **Internet2 MACE** (Middleware Architecture Committee for Education) プロジェクトによって開発されている、SAMLベースの連携型ID管理のアーキテクチャ、およびオープンソースの実装
- **大学におけるコンテンツサービスの現状の調査**
  - 大学で公開されているデータベースの認証方式や，提供範囲，利用申請時に集めている情報等
  - 国内先進事例の調査
    - CAS^2 によるポータル (名古屋大学)
    - PKIを用いた簡易SSO (東京大学)
- これらの調査から，大学の公開データベースに適したシングルサインオン方式とキャンパスPKIの活用、大学間認証連携の方式を検討
- 次年度は、この方式を実証するための実験システムを構築、UPKIとしての共通仕様を確立へ

(6) S/MIME証明書の実証実験

- **S/MIME (Secure Multipurpose Internet Mail Extensions) とは**
  - **電子メールの署名・暗号化の方式の1つで、PKIに基づく**
  - **政府機関統一基準などで推奨**
    - 3.2.4 **情報の移送** (3) **移送手段の選択** (a)
      - **行政事務従事者は、要機密情報を移送する場合には、安全確保に留意して、当該要機密情報の移送手段を決定し、…**
        - **〔解説〕送信については府省庁内通信回線、信頼できるプロバイダ、VPN及び暗号メール(S/MIME)等、運搬については…**
- **S/MIME証明書の発行手順の検証**
  - **個人情報を含むメールアドレス等の申請情報のやり取りや，パスコードの安全なやり取り方法について検証し，大学における安全な発行方式を確立**
- **S/MIME証明書の利用実験**
  - **認証作業部会の10機関を対象に実証実験を実施**
  - **認証作業部会メンバー間の連絡などでも積極活用**
  - **「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」でも利用予定**
- **実験の評価**
  - **S/MIME非対応のメーラー利用者やWebメール利用者が予想以上に多く、想定外のトラブルあり。当初の期待ほどの利用実績は得られず。**
- **今後の検討**
  - **「S/MIMEゲートウェイ」によるS/MIME非対応メーラやウエブメール利用者のサポートの検討。来年度に向けて実証実験を準備中。**

UPKIイニシアティブの発足

- 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も計画中



海外機関の調査・国際連携

- **海外の大学等の認証基盤構築を調査**

  2005年11月 (米国 Stanford大学, VeriSign社他、カナダ EnTrust社)
  2006年 7月 (オーストラリア クイーンズランド大学, AARNet他)
  2006年11月 (米国 ウイスコンシン大学Madison校)
  学内認証基盤, PKI運用, eduroam, Shibbolethの動向等を調査

- **国際会議での発表・活動**
  - APAN (Asia Pacific Advanced Network) Meeting
    - 2005夏・台北, 2006冬・東京, 2006夏・Singapore, 2007冬・ Manila
    - Middleware WG (2006～)
  - SAINT2007 Workshop on Middleware Architecture in the Internet (Hiroshima)
  - AP Grid PMA meeting (Osaka, 2006)
  - AEARU (Association of East Asian Research Universities)
    - 3rd Workshop on Network Education (Seoul National University, 2005)
    - 7th Workshop on Web Technology and Computer Science (National Taiwan University, 2006)

- **eduroamへの接続**

  海外機関との無線LANローミングにより、目に見える形での国際連携を実現

  現在, 北海道大学, 東北大学, 京都大学, 九州大学, 高エネルギー加速器研究機構, 国立情報学研究所が接続または接続準備中

今後の課題

- 平成19年度
  - 18年度に行った調査，研究および基本設計に基づき，詳細設計とプロトタイプシステム開発を実施
  - その他，認証アプリケーションの開発と公開
  - 大学間連携の前提となる，各大学での認証基盤構築の支援

オープンドメインPKI

  - オープンドメイン認証局の運用とサーバ証明書の啓発･評価研究
  - S/MIMEの活用

キャンパスPKI

  - 7大学とNIIにプロトタイプ認証局を構築し，相互接続性の検証，試行運用等を実施
  - Webシングルサインオンの実験システム構築など，目に見える形での認証基盤プロトタイプの構築
  - eduroamをベースに、PKIによりセキュリティを強化した、大学間無線LANローミング方式の開発

グリッドPKI

  - NAREGIおよび8センターグリッド研究会との連携
  - NAREGI CAソフトウェアの活用

「セキュア・ジャパン２００６」 http://www.nisc.go.jp/active/kihon/pdf/sjf_2006.pdf

(平成１８年６月１５日情報セキュリティ政策会議決定)

第２章 対策実施４領域における情報セキュリティ対策の強化

第１節 政府機関・地方公共団体

ア 政府機関

③中長期的なセキュリティ対策の強化・検討

(ウ) 政府機関への成りすましの防止

悪意の第三者が政府機関に成りすまし、一般国民や民間企業等に害を及ぼすことが無いよう、正統な政府機関であることを容易に確認可能とするため、電子証明書の広範な活用や、政府機関のドメインであることが保証されるドメイン名の利用を推進する。

【具体的施策】

ア) **政府機関のドメイン名であることが保証されるドメイン名の利用の促進** (総務省及び全府省庁)

政府機関のドメイン名であることが保証されるドメイン名を利用していないサイトについては、原則として２００６年９月までに、同ドメイン名の利用を開始する。

また、政府機関のドメイン名であることが保証されるドメイン名を用いることについて、各府省庁は国民に対し広く周知を行う。

イ) **政府機関から発信する電子メール及び政府機関のホームページからダウンロードされる電子文書に係るなりすまし及び改ざんの防止** (内閣官房、総務省、及び全府省庁)

政府機関に係る電子文書の成りすまし及び改ざん防止のため、政府機関から発信する電子メール及び政府機関のホームページからダウンロードされる電子文書に電子署名を付すことにより、一般国民や民間企業等の利用者が安心して利用できる環境の整備、具体的には電子署名を付すための政府内情報システムの共通仕様の検討を2006年度に開始する。