東海地区ＣＳＩ事業報告会
2006年12月15日

大学間連携のための全国共同電子認証基盤（UPKI）構想について

名古屋大学情報連携基盤センター 助教授
国立情報学研究所 客員助教授(連携)
平野 靖

全国共同利用情報基盤センター

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

産業・社会貢献

国際貢献・連携

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

CSI (Cyber Science Infrastructure) の目的

- 知的技術立国化の加速
  - 新たなICT産業の創出、およびICT人材育成
  - 国際・産官学の共同研究
  - 大学の社会基盤化の促進
- 世界最先端の学術研究基盤の実現
  - NAREGI, SINET, GeNiiとの連携
  - 学術資源（計算機，ネットワーク，コンテンツ）の安全・安心な共有・利用・流通基盤の実現

UPKIとは

- **大学間連携のための全国共同電子認証基盤**
  - 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**
    - 最先端学術研究の加速支援
    - 学術人材の（物理的・仮想的）流動への対応
- **U+PKI**
  - University　／Universal　／Ubiquitous
    大学の　汎用の・全世界の　いつでもどこでも
  - PKI（公開鍵認証基盤）
    - ただしPKIに限定せず認証技術を幅広く扱う

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 (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

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

全国共同利用情報基盤センター間の連携の歴史

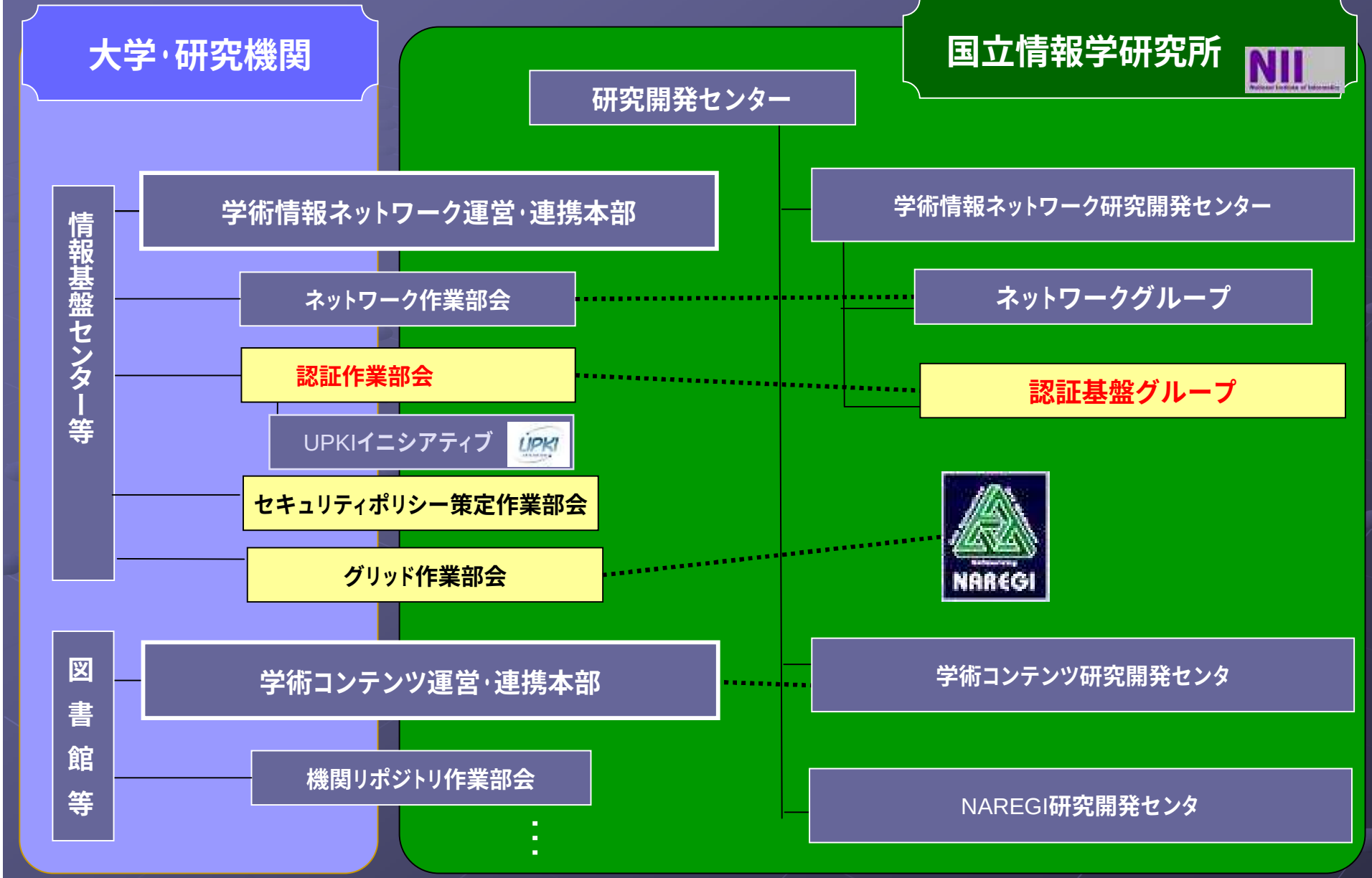
- 1965〜70
  - 全国共同利用大型計算機センター、7大学に設置
- 1986
  - 学術情報センター(NACSIS)設置
  - 共通利用番号制 (〜2004)
- 1992
  - 学術情報センターによるSINETサービス提供開始
- 2000
  - 国立情報学研究所(NII)設立
- 2002
  - SuperSINET運用開始
- 2003
  - NAREGI (National Research Grid Initiative) プロジェクト開始
- 2004
  - 国立大学法人化
- 2005
  - NIIに学術情報ネットワーク運営・連携本部を設置
    - 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
- 2006
  - UPKI構築事業開始 (〜2008)
  - UPKIイニシアティブ発足

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)
- 松岡聡 (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の研究開発・連携体制



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：
    - 学生：単位互換、卒業生サポート
    - 教員：非常勤講師、共同研究(VO)
  - 法人化後の国立大学間の絆
- 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
  - 電子政府用認証基盤（GPKI・LGPKI・JPKI）との連携

『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

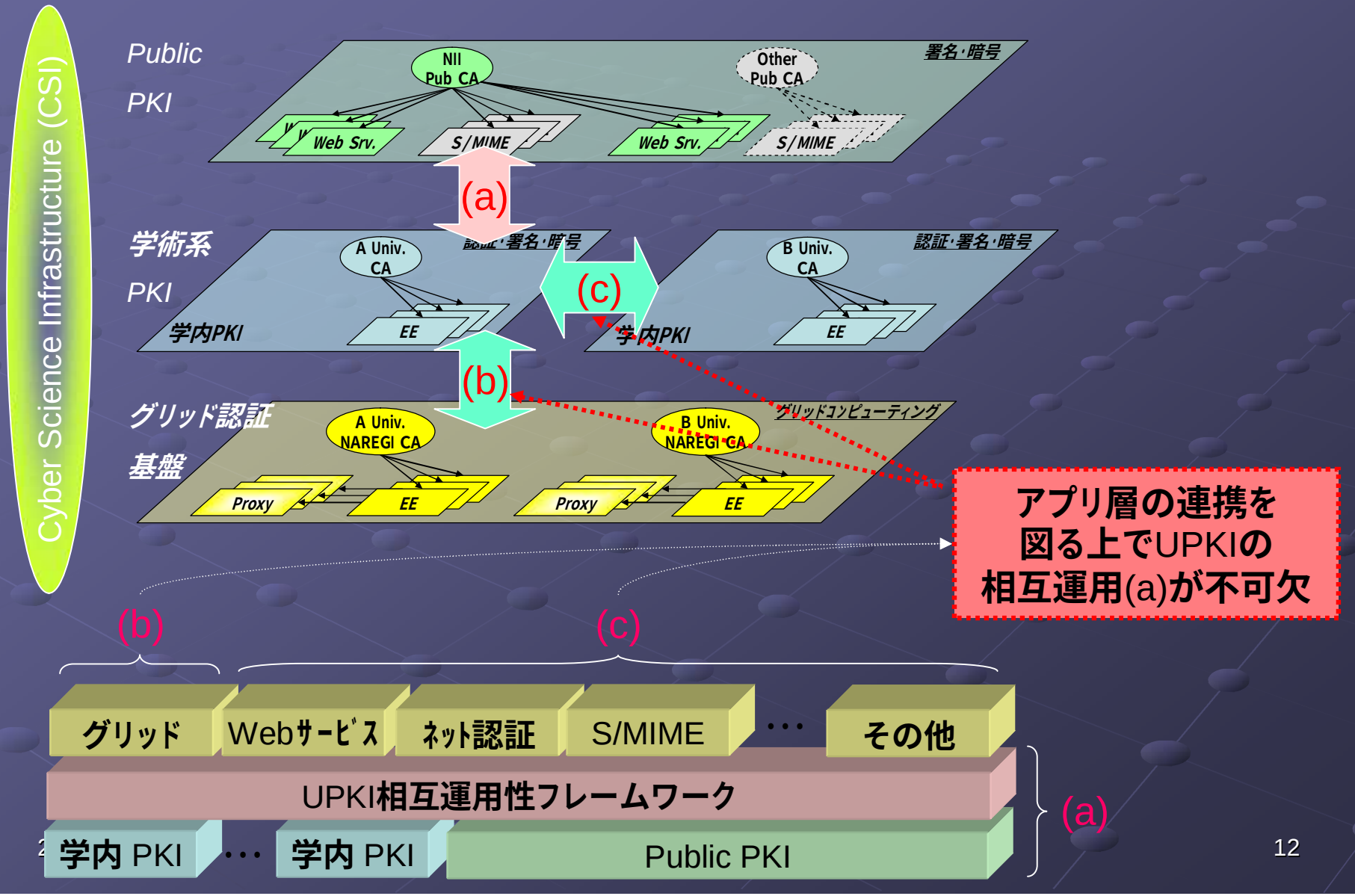
UPKI事業の概要

- 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

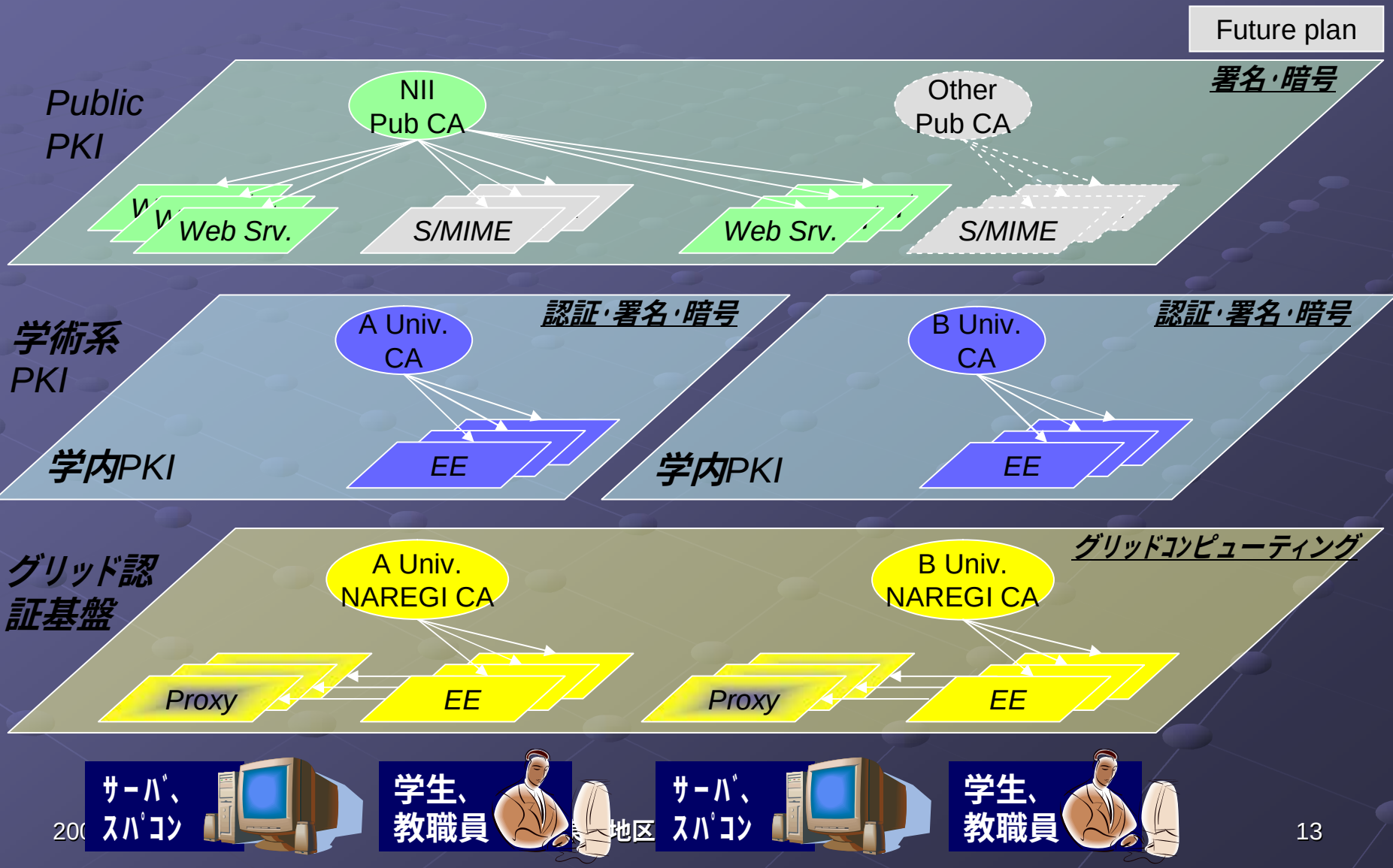
  ⇒Public系とprivate系の併用

  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、…

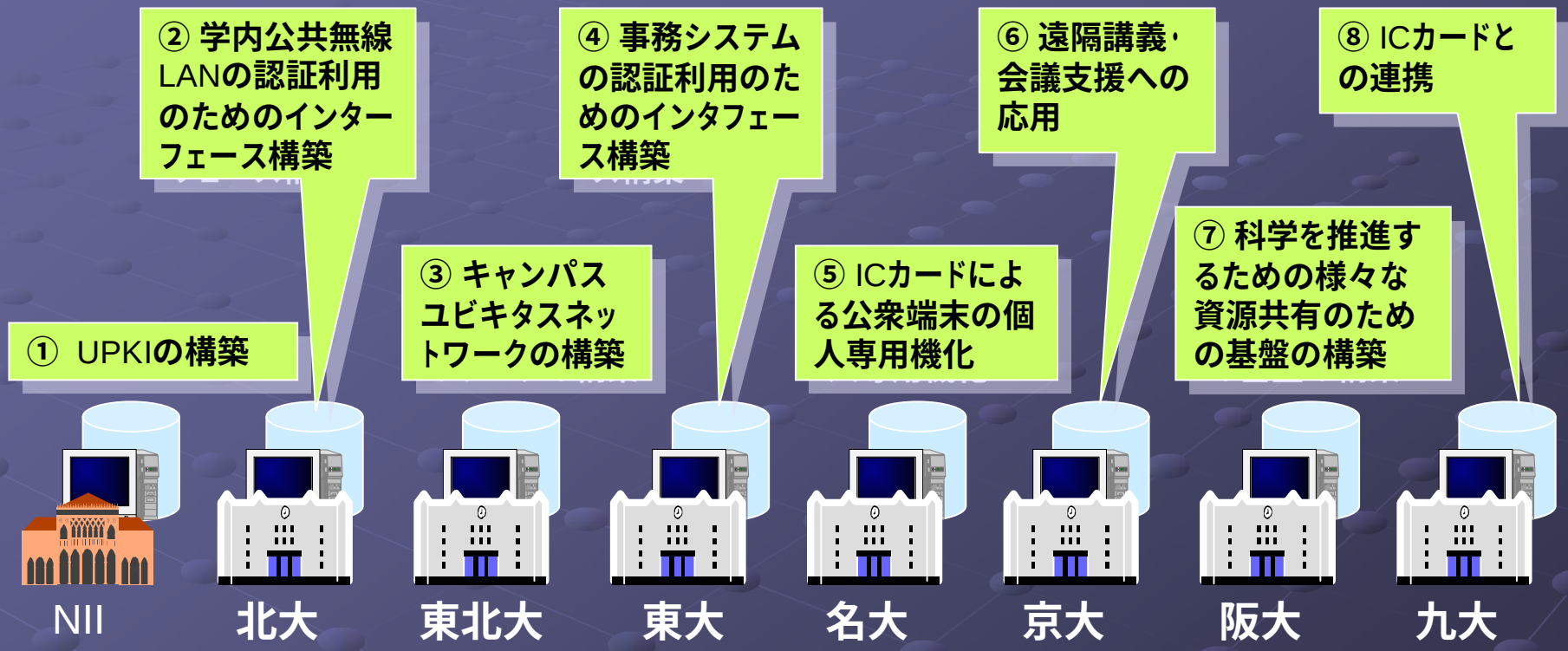
UPKIの相互運用フレームワーク



UPKIのアーキテクチャとドメイン構造



各大学におけるアプリケーション開発



- NIIと7センターは，認証に必要な各システム①～⑧を開発する。
- 各センターは開発したシステムの試験運用を実施する

NII認証基盤グループによる開発項目

- UPKI共通仕様の策定【WP1】
- 外部向けサーバ証明書発行サービス【WP2】
- 大学間無線ローミング【WP3】
- 情報基盤センターおよびNIIコンテンツサービスのシングルサインオン【WP4】
- CSI向け認証局ミドルウェアの開発【WP5】
- S/MIMEによる電子メール署名・暗号化の試験運用【WP6】

大学間無線LANローミング

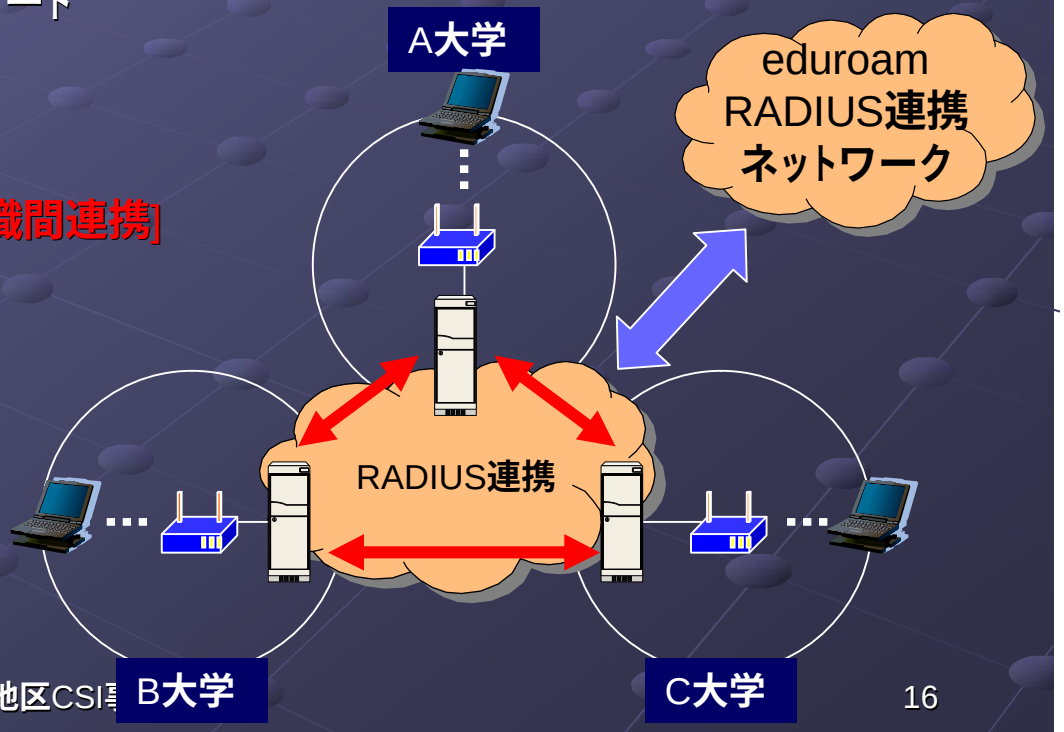
UPKIユーザが，他のUPKI参加機関を訪問した際，UPKIの仕様に基づく認証連携により，その機関が運営している無線LANインフラを利用したインターネットアクセス環境を構築する

本サービスの位置づけ：UPKIにおける組織間認証連携アプリケーション
対象ユーザ：UPKI参加機関の教職員，学生，研究員等

●フェーズ1（2006年度）[組織間連携]
(1) 将来の国際連携も考慮し，
eduroam互換のRADIUS連携方式でスタート
(2) eduroam接続試験
(3) RADIUS方式の問題点整理

●フェーズ2（2007年度以降）[PKIを含む組織間連携]
(1) PKI を用いたRADIUS連携方式の強化
(2) RADIUS連携をUPKIへ移行

テストベッド構築・試験運用



eduroam
・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・インフラストラクチャ
・RADIUSサーバ連携による認証方式
(ID/Password利用)

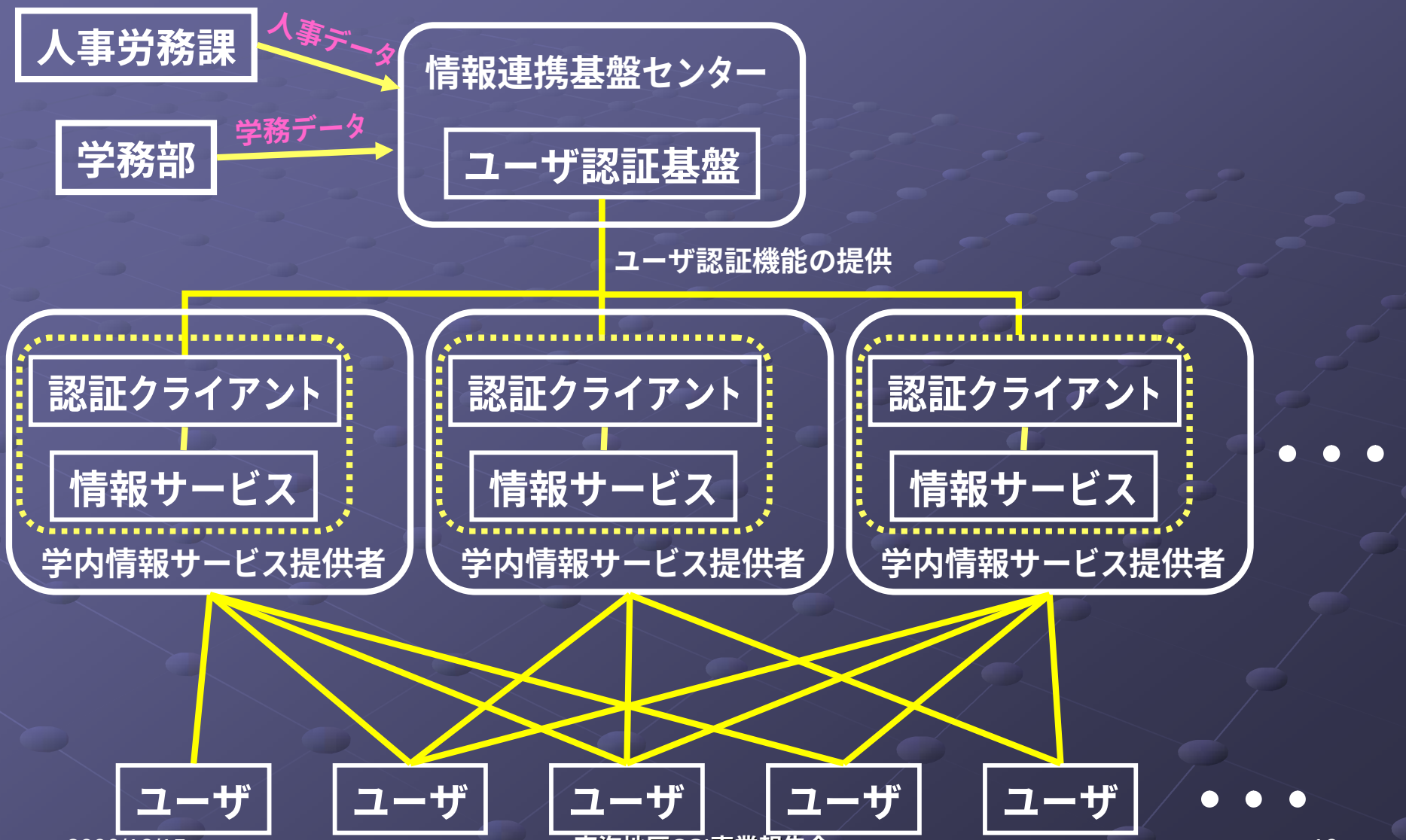
UPKIイニシアティブ
https://upki-portal.nii.ac.jp

- 目的
  - UPKI構築推進のための認証技術及び利用等に係る仕様検討，意見交換及び情報公開
- 組織
  - 代表：岡部（認証作業部会・主査）、副代表：曽根原（同・幹事）
  - 会員：
    大学，短期大学，高等専門学校又は大学共同利用機関等の教職員
  - 準会員：一般
- 活動
  - メールマガジン、UPKIイニシアティブフォーラム（掲示板）による情報公開と意見交換
  - 認証技術全般に関する普及・啓発活動、研究支援

名古屋大学の場合

- 全学ユーザ認証基盤
  - 全学ID：全学生，全職員に発行
  - LDAP CAS
- 職員証・学生証のICカード化の検討
  - PKIの導入
- ICカードによるWindows端末へのログオン実験
  - 直接LDAPサーバにアクセス

一元的な認証基盤


人事労務課
人事データ
学務部
学務データ
情報連携基盤センター
ユーザ認証基盤
ユーザ認証機能の提供
認証クライアント
情報サービス
学内情報サービス提供者
認証クライアント
情報サービス
学内情報サービス提供者
認証クライアント
情報サービス
学内情報サービス提供者
ユーザ
ユーザ
ユーザ
ユーザ
ユーザ

名古屋大学の規模(1)

- 学部学生　9,800名
- 大学院学生　6,000名
- 研究生　1,000名
- 教員　1,800名
- 事務職員･技術職員　1,500名
- 非常勤職員　3,000名

平成17年5月1日現在

名古屋大学の規模(2)

- 新規卒業生　2,200名
- 新規修了生　2,500名

- 既卒業生(新制)　76,500名
- 既卒業者(旧制)　4,100名
- 既修了生　41,000名

平成16年度現在

(注：現在は16，17年度卒業生・修了生にのみ全学IDの付与を行っている)

名古屋大学のユーザ認証システム

- 学内情報サービスの種類に応じた2つのユーザ認証システム
  - LDAP　(UNIXやWindowsのログインなど)
  - CAS　　(主にWebアプリケーション向け)

*CASサーバが用いるユーザ情報はLDAPサーバに格納されているため，認証用データベースは同一

CASとは(1)

- Central Authentication Serviceの略
- 米国Yale大学が開発
- Single Sign-On (SSO)を実現可能
- 標準的なWeb技術だけを用いて実装可能
- ユーザインタフェースとしてWebブラウザを利用
- Java，PHP，Perl，PL/SQL，Pythonなどのための CASクライアント構築用のライブラリ
- 北米を中心に豊富な採用実績(2005年6月現在，30を越える大学で採用)

CASとは(2)

- 認証情報はユーザ・CASサーバ間で通信
- 暗号化すべきは

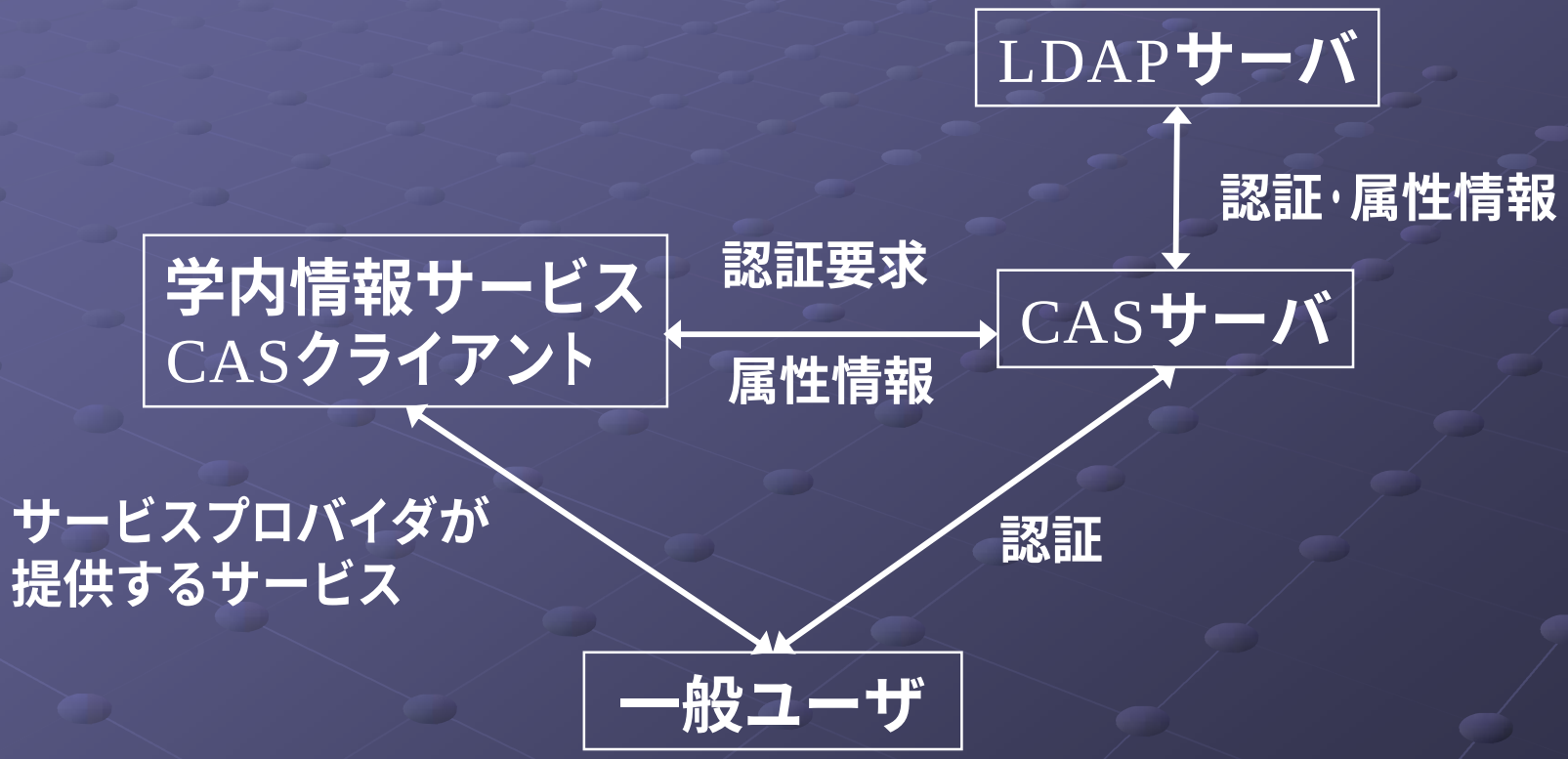
  ユーザ・CASサーバ間と，

  学内情報サービス・CASサーバ間

  → CASサーバにのみサーバ証明書が必要

  →コスト削減可能

CASとは(3)


LDAPサーバ
認証・属性情報
学内情報サービス
CASクライアント
認証要求
属性情報
CASサーバ
サービスプロバイダが
提供するサービス
認証
一般ユーザ

名大版CAS

- 強力な権限管理機構を付加

  CAS^2 (Central Authentication and Authorization Service)
- 権限管理情報は任意のデータベースに格納可能(名大ではLDAPサーバに格納)

LDAPを利用する
学内情報サービスプロバイダ

利用実績(15):

- 本部(3)
- 附属図書館(1)
- 情報科学研究科(2)
- 情報メディア教育センター(2)
- 情報連携基盤センター(7)

利用例:

教育用計算機システム(情報メディア教育センター)

図書館システム(附属図書館)

CAS²を利用する
学内情報サービスプロバイダ

利用実績(8):

- 本部(2)
- 法学部(3)
- 情報メディア教育センター(2)
- 情報連携基盤センター(1)

利用例:

WebCT(情報メディア教育センター)
教務システム(学務情報システム推進委員会)
大学ポータル(情報連携基盤センター)

まとめ

- 大学間連携のための全国共同電子認証基盤(UPKI)構築事業
  - 事業主体
    - NII + 7大学情報基盤センター
    - 7大学（先行/限定）ではありません！
  - 事業期間：平成18年度～20年度
    - 7大学にとっては全学認証基盤の構築が急務
- UPKIイニシアティブへの参加のお願い
  - 先例に学び、経験を共有することで、認証基盤を早期に低コストで構築しましょう！