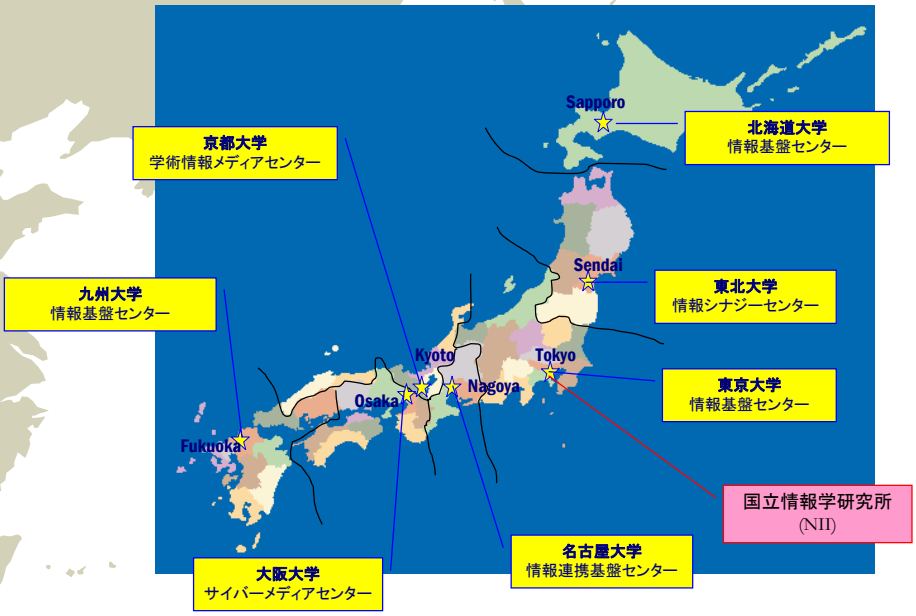
大学間連携のための
全国共同電子認証基盤(UPKI)
構築の構想

岡部寿男
（京都大学学術情報メディアセンター）

平成17年10月27日

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、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
  - NACSISによる大学間を結ぶ専用X.25網のサービス
  - 共通利用番号制 (～2004)
- 1988
  - JAIN (Japan Academic Inter-university Network) 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
- 2000
  - 国立情報学研究所(NII)設立
- 2002
  - SuperSINET運用開始
- 2003
  - NIIのもとでNAREGI (National Research Grid Initiative) プロジェクト開始
- 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**

<u>7大学センターとNIIの連携を強化</u>

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）
- 川端節彌（高エネルギー加速器研究機構計算科学センター）

国立情報学研究所：最先端学術情報基盤の構築に向けて

最先端の学術研究基盤が、今後の学術分野・産業分野での国際協調・競争の死命を制す　！！

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
    - → 教育・研究資源、コンテンツの有効活用（単位互換、e-learning応用）
  - メール内容などの暗号化　→　情報漏洩の防止
  - 電子認証・電子署名
    - → 電子決済・電子回覧による効率化，フィッシング対策などセキュリティ強化
  - 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

UPKI構築事業の背景

- かつての8センター共通利用番号制
  - ID体系を共通化 （素朴な形のFederated Identity Management）
    - W55070 〔数字の最上位が地区別を表す〕
  - 第二センター登録のオンライン申請
    - 印鑑を捺すのは第一センター登録時のみ（原始的なSSO）
    - 利用資格・負担金支払い力を第一センターが保証（認証・認可連携）
- 現状の大学内電子認証システム
  - ID/パスワードの組合せを多用
    ⇒ パスワード漏洩による，情報リソースへの不正アクセスの可能性
  - 様々な部局が独自のID/パスワード体系
    ⇒ 利用者の混乱

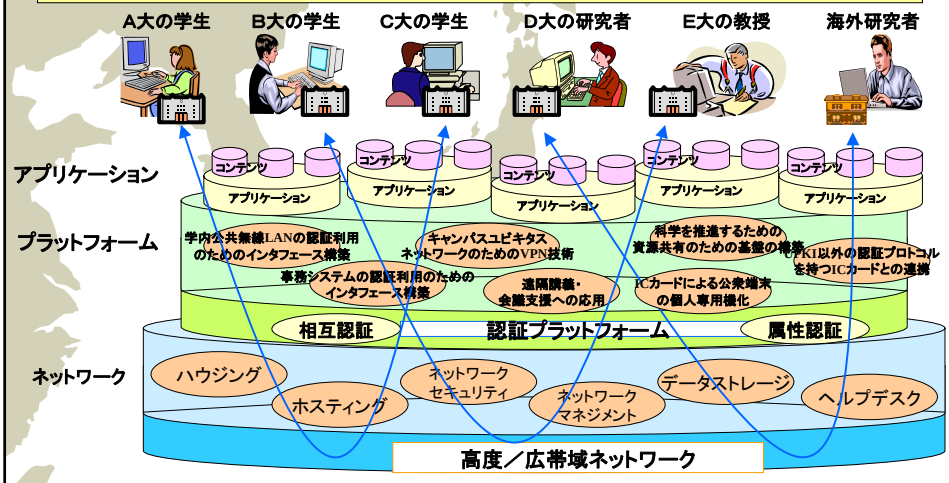
◎現在、全国の大学で、学内認証系の統合とSSO（シングルサインオン）の導入が進められている

- 求められる電子認証システム
  - PKI (Public Key Infrastructure：公開鍵認証基盤)の導入による不正アクセスの防止
    - 電子証明書による本人証明・暗号化通信
    - ICカード等に秘密鍵を格納することにより，詐称不能
    ◎グリッドとの親和性
  - 大学としての一元的な認証システム

各大学ばらばらではなく、全国共通のシステムを！

全国共同電子認証基盤の構築

全国共同電子認証基盤を構築し、大学の先生、研究者、学生、事務職員が、連携している大学のネットワークに自由に入れるようにする。更に共通プラットフォーム上で利用できる機能を活用することで、利便性の向上を図る。



セキュリティを確保した連携を行うには、個人を認識するための認証機能は不可欠

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
  - コンテンツ共有
    - 電子図書館、e-learning
  - 学生・教員の流動化：
    - 学生：単位互換
    - 教員：非常勤講師、共同研究

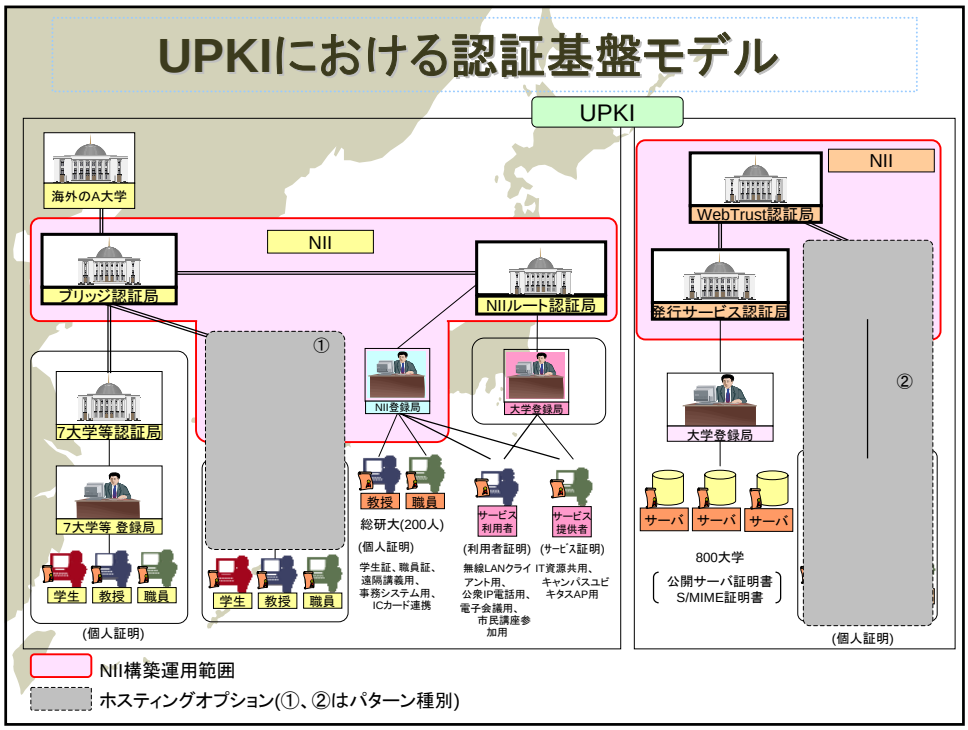
    物理的にも、仮想的にも
  - 法人化後の国立大学間の絆
- 各大学における効果
  - セキュリティレベルの向上
    - ポリシーと実施手順の見直し
  - 導入・開発コストの削減
- 国際連携、産学連携、地域連携
  - 国際標準への対応、標準化への貢献

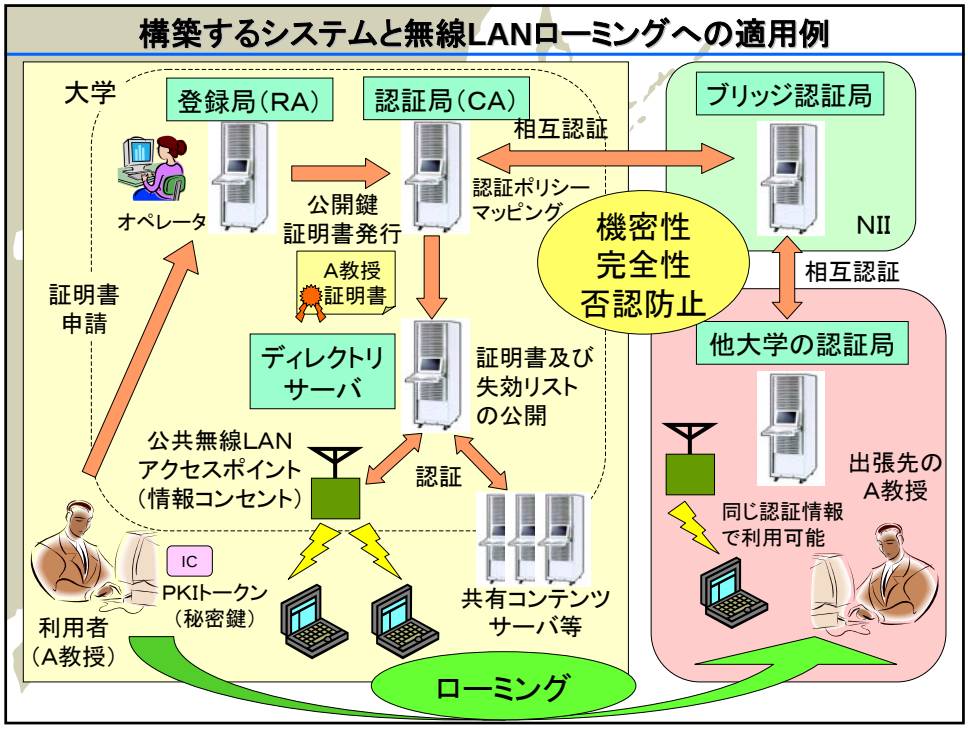
大学におけるPKIの構築

<u>検討課題</u>

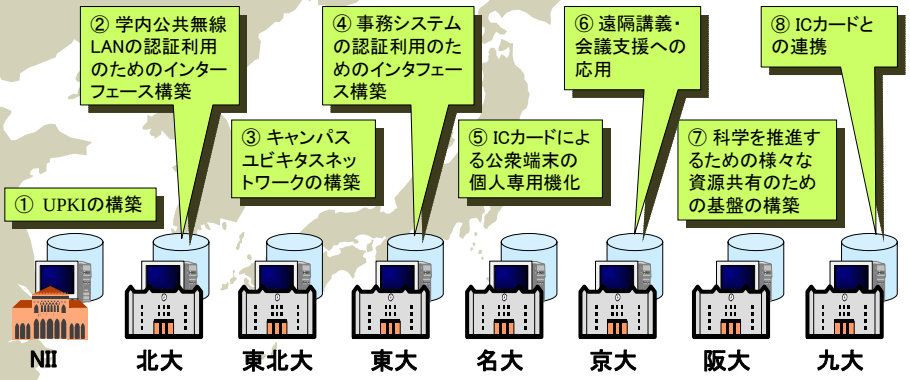
- 認証局の運用方法
  - パブリックCAかプライベートCAか
    - 公開Webサーバにはパブリックな証明書が必須
    - 学生を含む全構成員のクライアント証明書をパブリックにするのは高コスト

    ⇒（当面）パブリック系とプライベート系を併用
      - コンピュテーショングリッドはプライベート系？
  - プライベート系のアーキテクチャ
    - 7大学がCAを持ち、NIIがブリッジ認証局
- 認証局ソフトウェア
  - NAREGI-CAを核
  - 7大学で、マルチベンダー環境でのインターオペラビリティを検証
- 証明書の登録・配布モデル
  - 主体者発行(subscriber enroll)かバルク発行(bulk issuing)か
- 証明の対象
  - クライアント証明書
    - 特に身分証のICカード化


UPKIにおける認証基盤モデル
UPKI
海外のA大学
NII
ブリッジ認証局
NIIルート認証局
①
NII登録局
大学登録局
7大学等認証局
7大学等 登録局
学生
教授
職員
(個人証明)
教授
職員
総研大(200人)
(個人証明)
学生証、職員証、遠隔講義用、事務システム用、ICカード連携
サービス利用者
サービス提供者
(利用者証明)
(サービス証明)
無線LANクライアント用、公衆IP電話用、電子会議用、市民講座参加用
IT資源共用、キャンパスユビキタスAP用
NII
WebTrust認証局
発行サービス認証局
②
大学登録局
サーバ
サーバ
サーバ
800大学
公開サーバ証明書
S/MIME証明書
(個人証明)
NII構築運用範囲
ホスティングオプション(①、②はパターン種別)

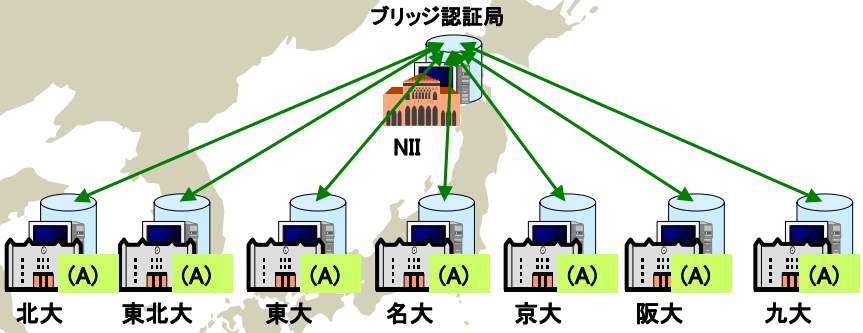

構築するシステムと無線LANローミングへの適用例
大学
登録局(RA)
認証局(CA)
相互認証
ブリッジ認証局
オペレータ
公開鍵
証明書発行
認証ポリシー
マッピング
機密性
完全性
否認防止
NII
相互認証
A教授
証明書
証明書
申請
ディレクトリ
サーバ
証明書及び
失効リスト
の公開
他大学の認証局
公共無線LAN
アクセスポイント
(情報コンセント)
認証
出張先の
A教授
同じ認証情報
で利用可能
IC
PKIトークン
(秘密鍵)
利用者
(A教授)
共有コンテンツ
サーバ等
ローミング

平成18年度　大学連携による共同開発



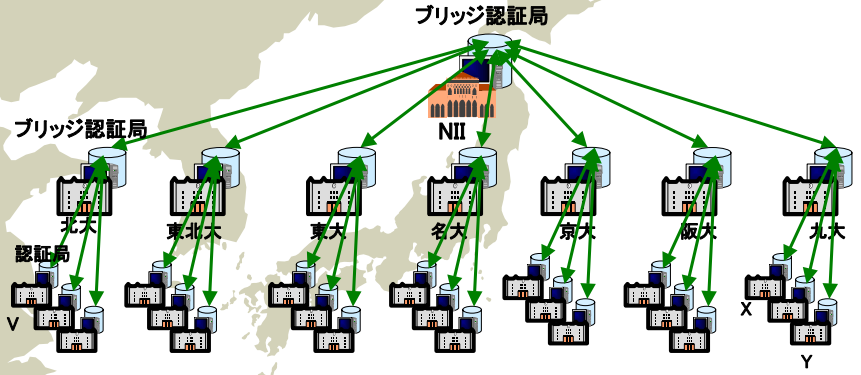
- NIIと7センターは，認証に必要な各システム①～⑧を開発する。
- 各センターは開発したシステムの試験運用を実施する

平成19年度　大学連携による検証実験



- 各センターで開発したシステム①～⑧の統合版(A)を作成する
- 各センターが統合版のインストールを行い，試験運用を実施する
- NIIのブリッジ機能を利用して，各センター間の試験運用を実施する
- NIIにてWTCAの試験運用を開始する

平成20年度　CSIの全国展開



- 統合版(A)の改良を加え，各大学に配付する
- 地域内での大学間のブリッジ機能の試験運用を行う（XとY）
- 7センター配下の大学間のブリッジ機能の試験運用を行う（VとX）
- WTCAの本格運用を実施する

現状と課題

◆現状

【SINETの状況】

- 現在、主要大学間はSINET、スーパーSINETを介して接続されており、バイオ・ゲノムをはじめとした研究テーマに取り組んでいるが、セキュリティレベルの確保は**利用者に依存**している。また、商用の証明書発行サービスを利用するには、**煩雑な事務手続き**が発生する。

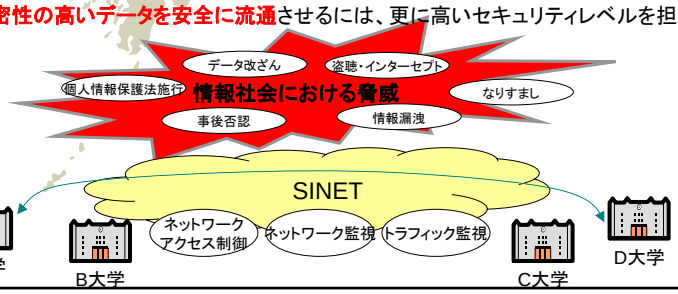
【世の中の状況】

- 情報漏えい、データ改ざん等のネットワーク上の脅威が拡大しており、平成17年4月から個人情報保護法が施行され、大学においてもますます**セキュリティレベルを向上**させる必要性を迫られている。

◆課題

•ネットワークインフラとしての整備および高度化は世界最高水準に達したところだが、今後は**サイバー・サイエンス・インフラ**として利用者（大学・機関）から共同実験や研究における連携を実現するため、更なる期待が寄せられている。

•SINETとしては、ネットワークレイヤの脅威については対策を講じているものの、大学間及び外部（産業界等）と**機密性の高いデータを安全に流通**させるには、更に高いセキュリティレベルを担保する必要がある。

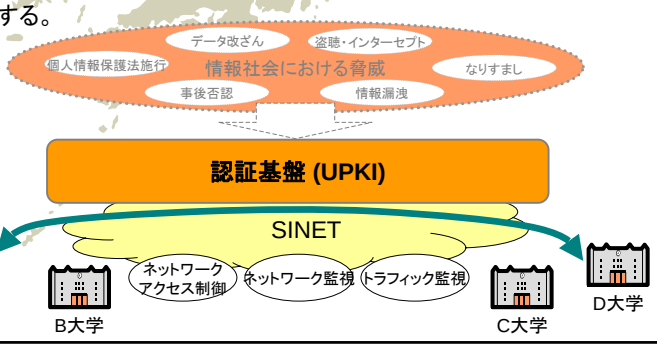


施策と期待される効果

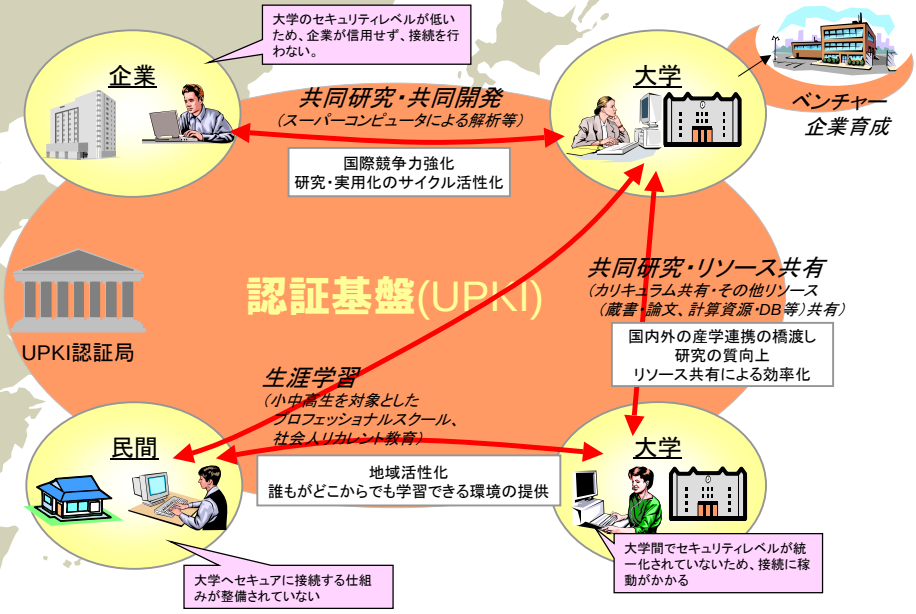
◆施策と期待される効果

•SINETに接続される国公私立大学・学術機関(約800校) の情報交換をセキュアに行うための**社会基盤**としての大学間認証基盤(UPKI)の構築を行うことにより、ネットワークの利用者が安全にデータをやりとりできるようになる。これにより、**サイバー・サイエンス・インフラとしての機能**を強化し、**利用者指向のネットワーク**へと進化する。

•更に、積極的に国内外の産業・学術機関等との連携も実現させることにより、**国内外の「知」を集結**し、研究事業の推進による**国際競争力の強化**、ひいては**経済社会全体の活性化に寄与**する。



UPKIにおける連携モデル



学-学連携（がっちりスクラム）

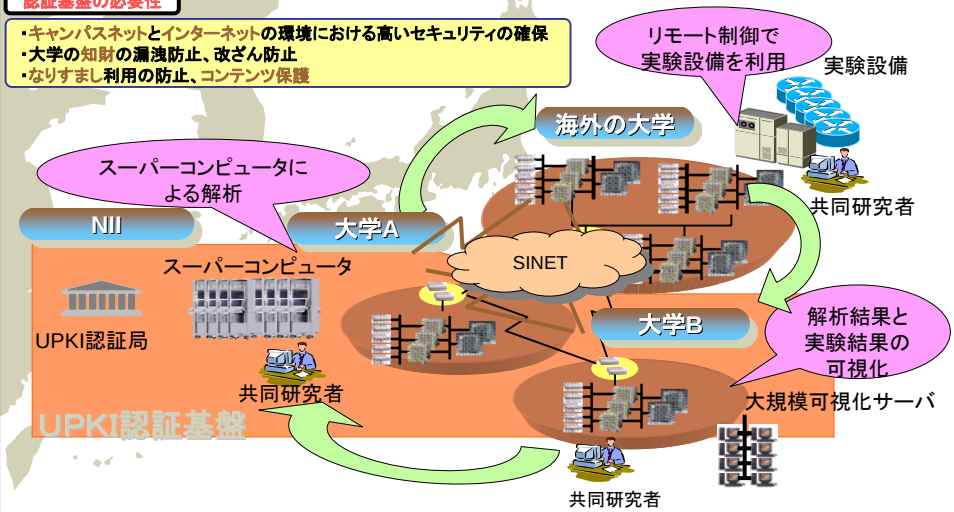
学ー学連携による利用

①大学間連携による共同研究の促進
②リソース共有による研究資源の有効活用

認証基盤の必要性

・キャンパスネットとインターネットの環境における高いセキュリティの確保
・大学の知財の漏洩防止、改ざん防止
・なりすまし利用の防止、コンテンツ保護

連携場面
●バイオインフォマティクス（ゲノム創薬）
●ニューロインフォマティクス（人工知能）
●大規模シミュレーショングリッドコンピューティング



産-学連携（IT国家競争力）

UPKI認証基盤による、安全・安心な産学連携の利用促進。

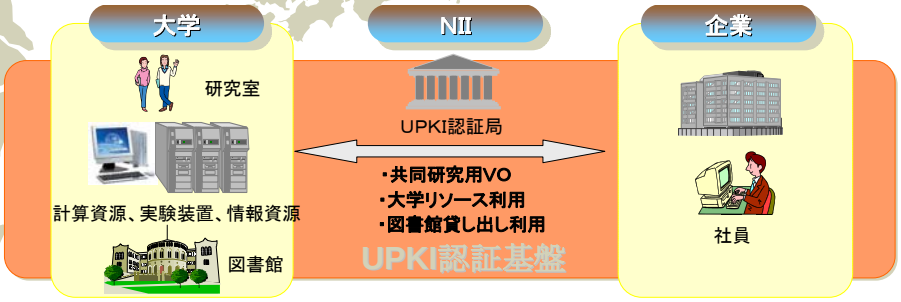
産学連携による利用

①バーチャルオーガニゼーション（VO）構築による共同研究の促進と効率化
②大学リソースのネット利用の促進
③図書館の蔵書、デジタルアーカイブ貸し出しの利用促進

認証基盤の必要性

・キャンパスネットとインターネットの環境における高いセキュリティの確保
・大学の知財の漏洩防止、改ざん防止
・なりすまし利用の防止、コンテンツ保護
・学生、職員、共同研究企業の社員の個人情報保護

認証の役割（確保するセキュリティ）
●共同研究用VOの本人確認
●大学リソース利用の企業確認
●図書館利用の企業確認
●大学の各種サーバ確認
●知財、コンテンツの原本性確認
●利用履歴の確認



民-学連携（大衆の支援）

民ー学連携の目的

地域コミュニティの核として大学が機能し、市民生活の高度化を目指す

目指す社会基盤

① ひとりひとりの個性に対応できる社会基盤
② 人々の内面に根ざした新しいコミュニティ形成を促進する社会基盤

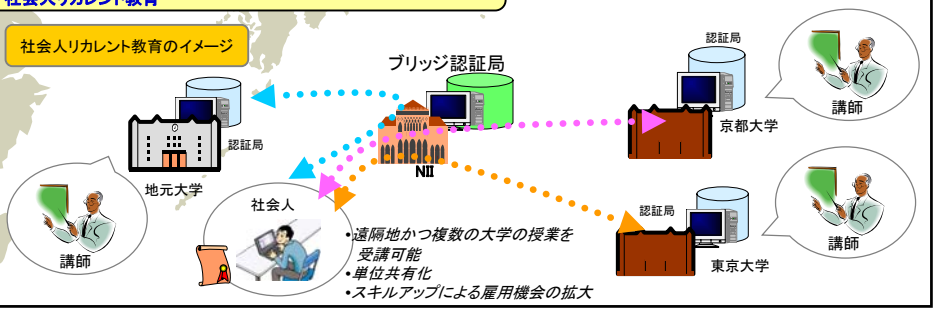
社会基盤による具体的な効果

- 大学院生・社会人の教育への大量参画
- 一般市民からの知識基盤の大学へのリンク
- インターン制度・発展的な各種資格制度の創設
- 小中高生を対象としたプロフェッショナルスクールの設立
- 社会人リカレント教育

認証の役割（確保するセキュリティ）

- 生涯学習講座の受講証
- 地域活性化活動の参加証
- 各種優待措置のための本人確認
- 講師の登録証
- 利用履歴の確認

社会人リカレント教育のイメージ



- *遠隔地かつ複数の大学の授業を受講可能*
- *単位共有化*
- *スキルアップによる雇用機会の拡大*

構築スケジュール

	H18年度	H19年度	H20年度
WebTrust認証基盤の構築	調査・研究・設計 →	開発・構築 →	試験運用 →
ブリッジ認証局の構築	要件定義（ポリシー策定）→ 調査・設計 →	開発・構築 →	試験運用 →
大学のアプリケーション開発	調査・研究・設計 →	開発・構築 →	統合版の開発 → 試験運用 →

まとめにかえて

- 大学間連携のための全国共同電子認証基盤
  - 7大学の、学内での展開に限っても課題山積み
    - 大学間よりもむしろ学内に高い障壁
      - 縦割り事務、部局の自治、…
- いかに先例に学ぶか
  - 諸外国の動き
    - Internet2 Shibboleth
    - EduRoam
  - 企業における社内システム
  - 電子政府系
    - わが国のGPKI, LGPKI, JPKI
    - E-authentication（米国政府）
  - グリッド