全国の大学をつなぐ認証基盤「UPKI」

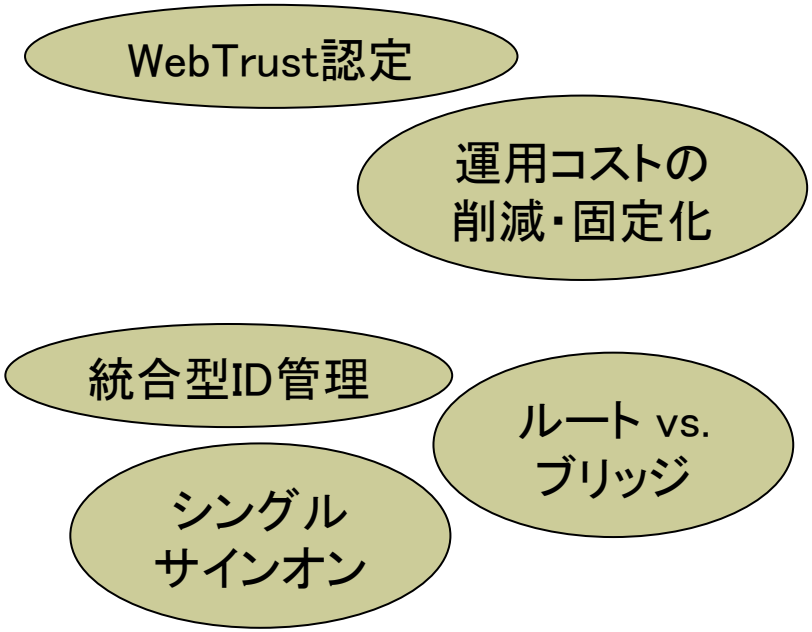
国立情報学研究所
学術ネットワーク研究開発センター
島岡　政基

UPKIの背景

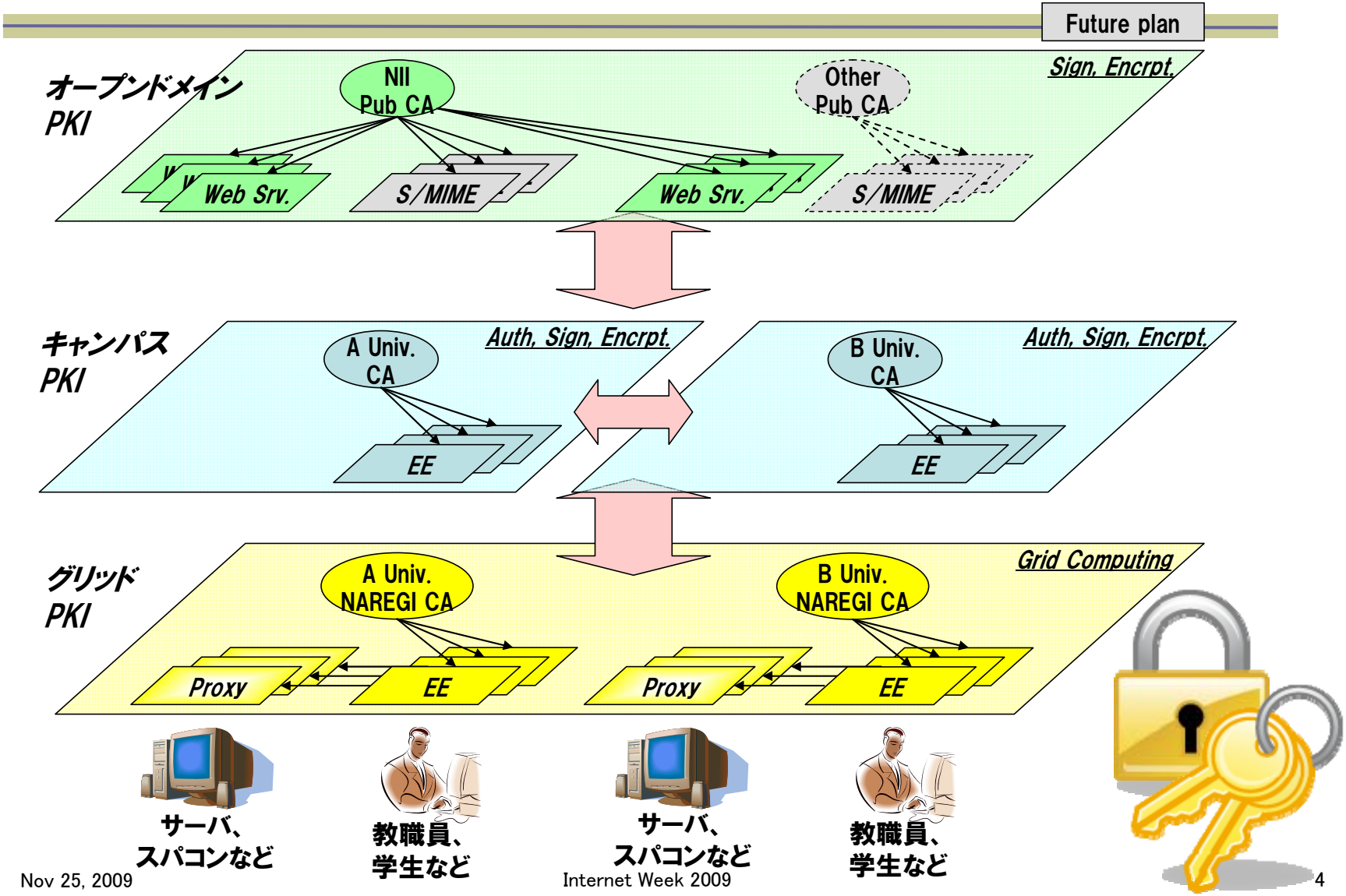
- 各大学の認証基盤導入
  - 共通仕様、運用標準など
- 各大学との相互接続
  - 単位互換など
- 大学間アプリケーションサービス連携
  - IT人材育成など
- 社会・産学連携の本格的運用
  - サービスや情報連携
- 国際連携
  - 学術情報格差の克服

UPKI初期のトピック

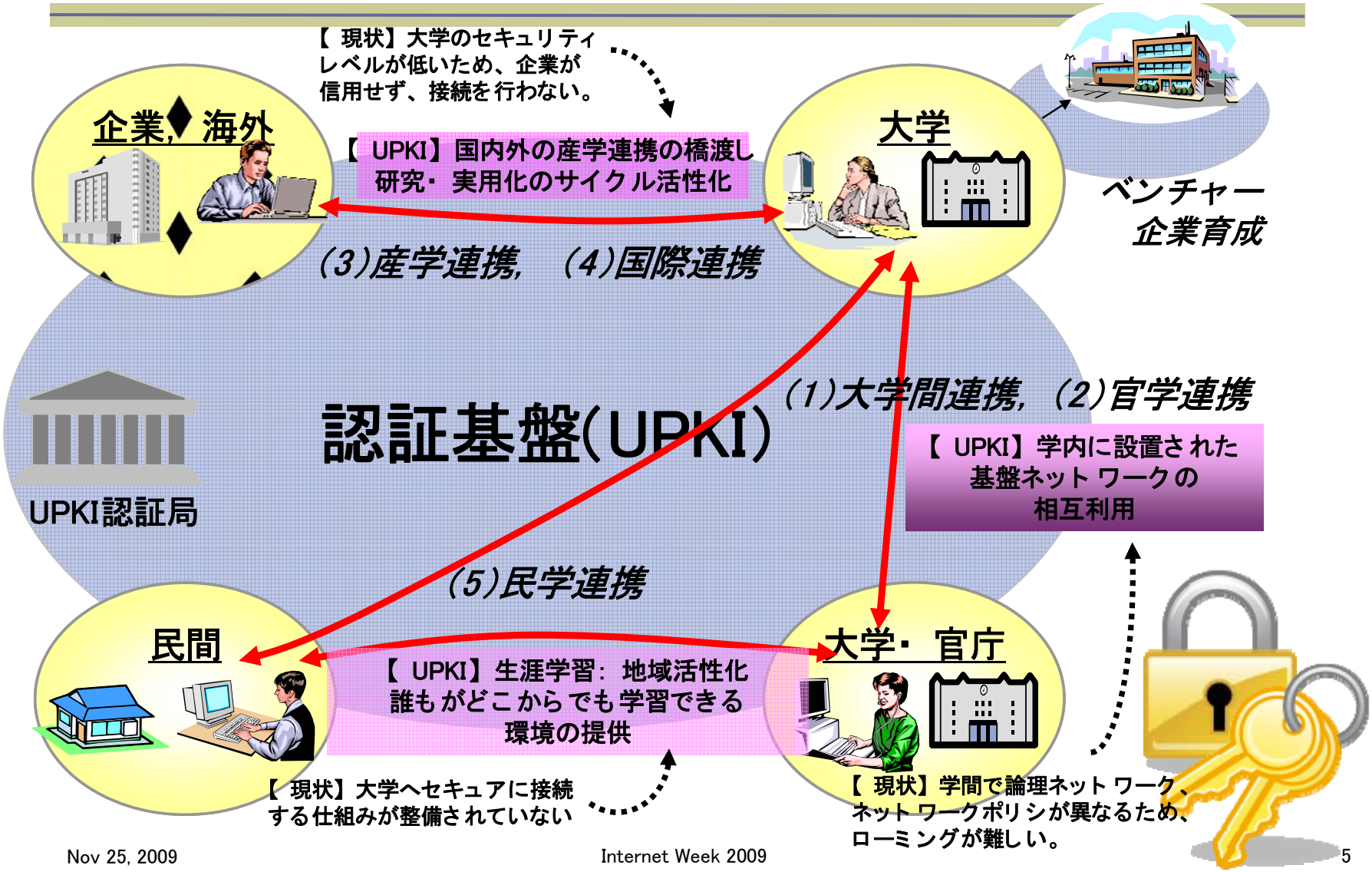
- パブリック証明書
  - サーバ証明書
  - S/MIME証明書
- 学内認証基盤
  - 大学間相互接続
  - CP/CPS
- グリッド認証局
  - PKI的には異端児(プロキシ証明書)
  - 学内認証基盤との連携



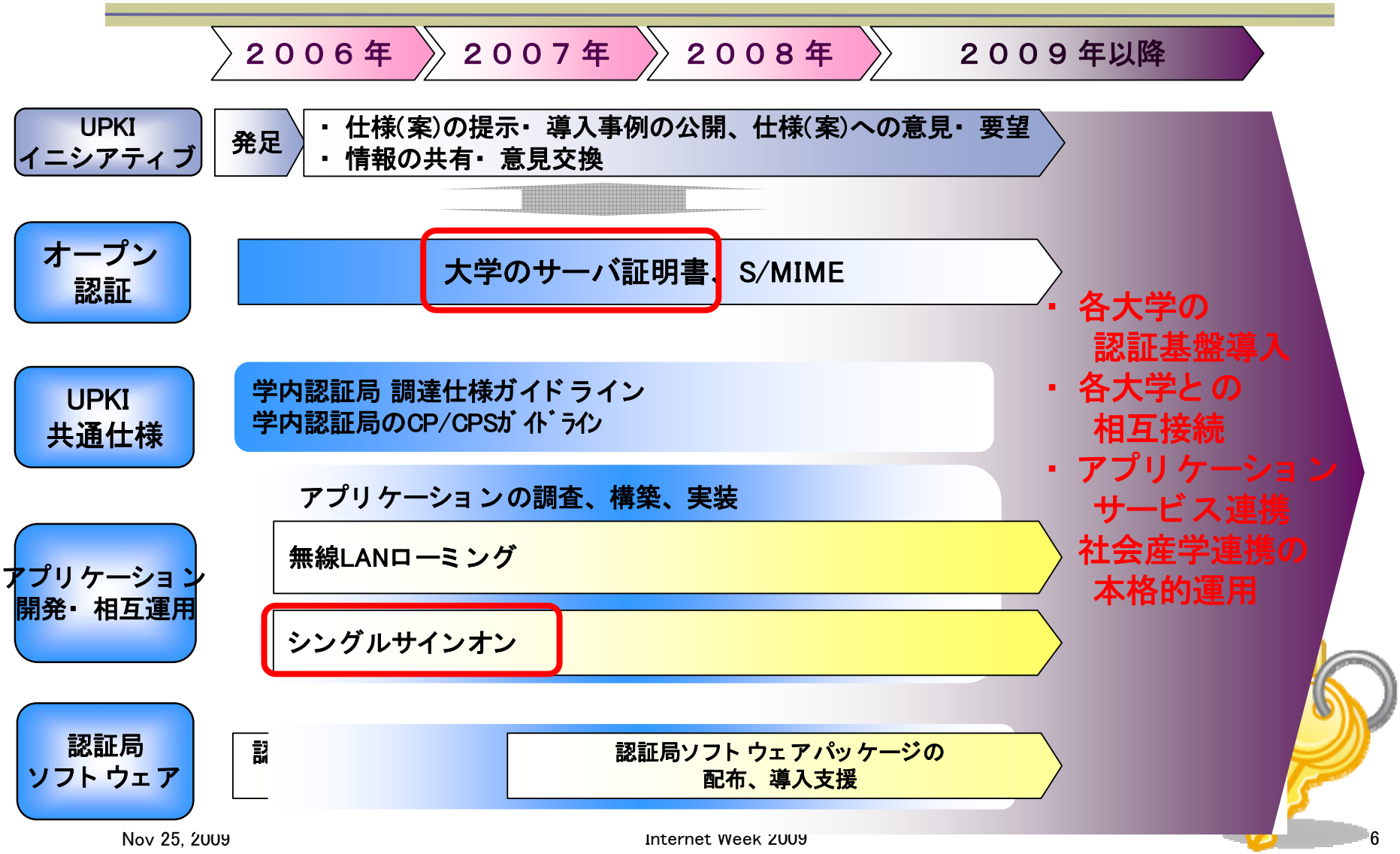
UPKIの3層構造


Future plan
オープンドメイン PKI
NII Pub CA
Other Pub CA
Sign, Encrpt.
Web Srv.
S/MIME
Web Srv.
S/MIME
キャンパス PKI
A Univ. CA
Auth, Sign, Encrpt.
EE
B Univ. CA
Auth, Sign, Encrpt.
EE
グリッド PKI
A Univ. NAREGI CA
Grid Computing
B Univ. NAREGI CA
Proxy
EE
Proxy
EE
サーバ、スパコンなど
教職員、学生など
サーバ、スパコンなど
教職員、学生など

UPKIが描く連携サービス



UPKIの歩み


２００６年
２００７年
２００８年
２００９年以降
UPKI
イニシアティブ
発足
・仕様(案)の提示・導入事例の公開、仕様(案)への意見・要望
・情報の共有・意見交換
オープン
認証
大学のサーバ証明書、S/MIME
UPKI
共通仕様
学内認証局 調達仕様ガイドライン
学内認証局のCP/CPSガイドライン
アプリケーション
開発・相互運用
アプリケーションの調査、構築、実装
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
認証局ソフトウェアパッケージの
配布、導入支援
・各大学の
認証基盤導入
・各大学との
相互接続
・アプリケーション
サービス連携
社会産学連携の
本格的運用

サーバ証明書プロジェクト

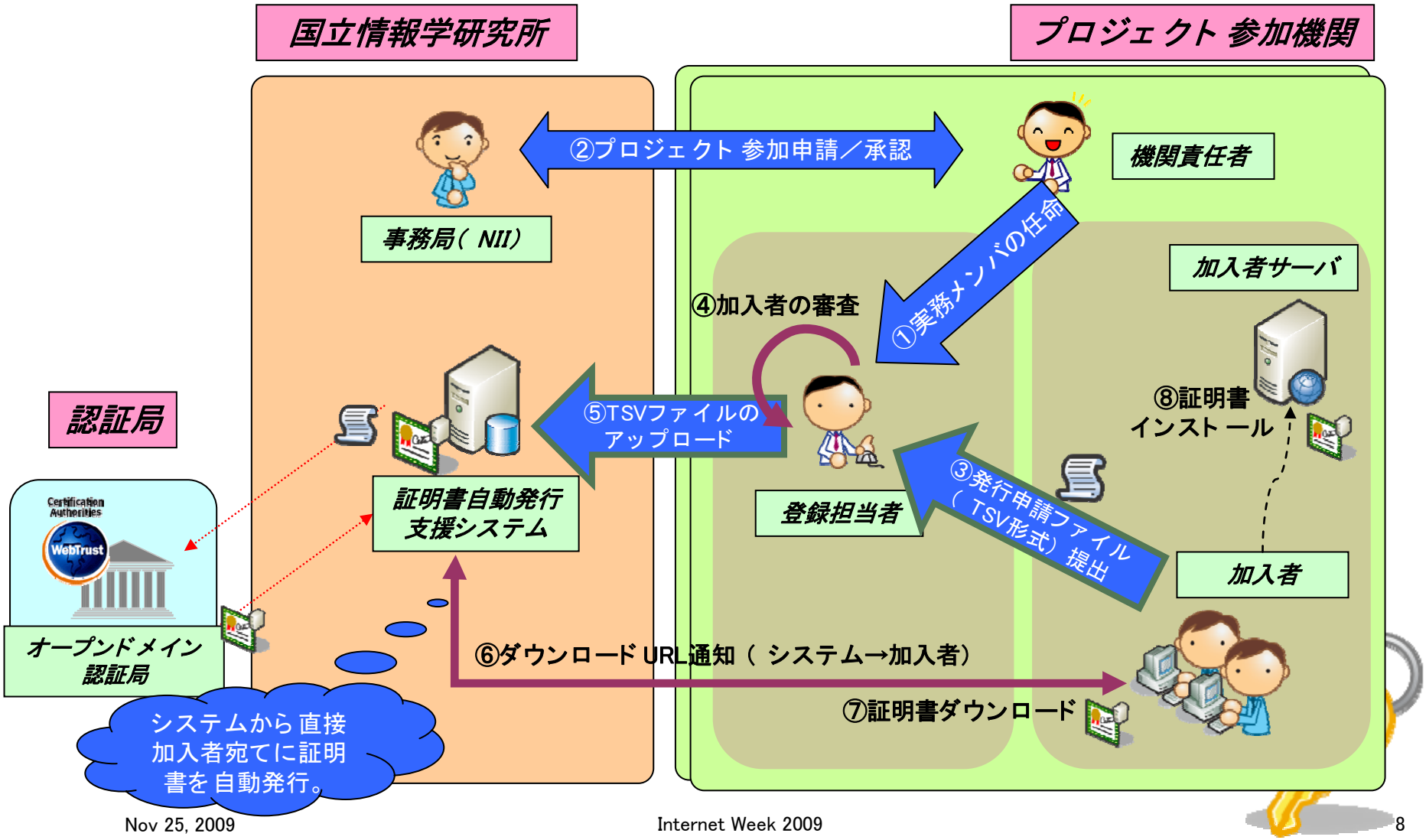
- 大学向けサーバ証明書の普及推進と証明書発行プロセスの研究

’09/11/06現在

	旧ﾌﾟﾛｼﾞｪｸﾄ	新ﾌﾟﾛｼﾞｪｸﾄ
期間	‘07/05～’09/06末	’09/04～’12/03末
機関数	97	112
発行枚数	2,413枚 （失効92）	1,982枚 （失効48）

- いわゆるパブリック証明書を発行
  - WebTrust for CAに準ずる審査
- 機関単位での参加→機関認証を担保
- 各大学へのLRA権限委譲
  - 機関毎に異なるネットワーク管理を緩衝
  - 証明書発行・審査作業の効率化
  - 機関単位の失効というハリセンボンマシン

(新) 証明書自動発行検証プロジェクト



確認実施手順調査表の記入例

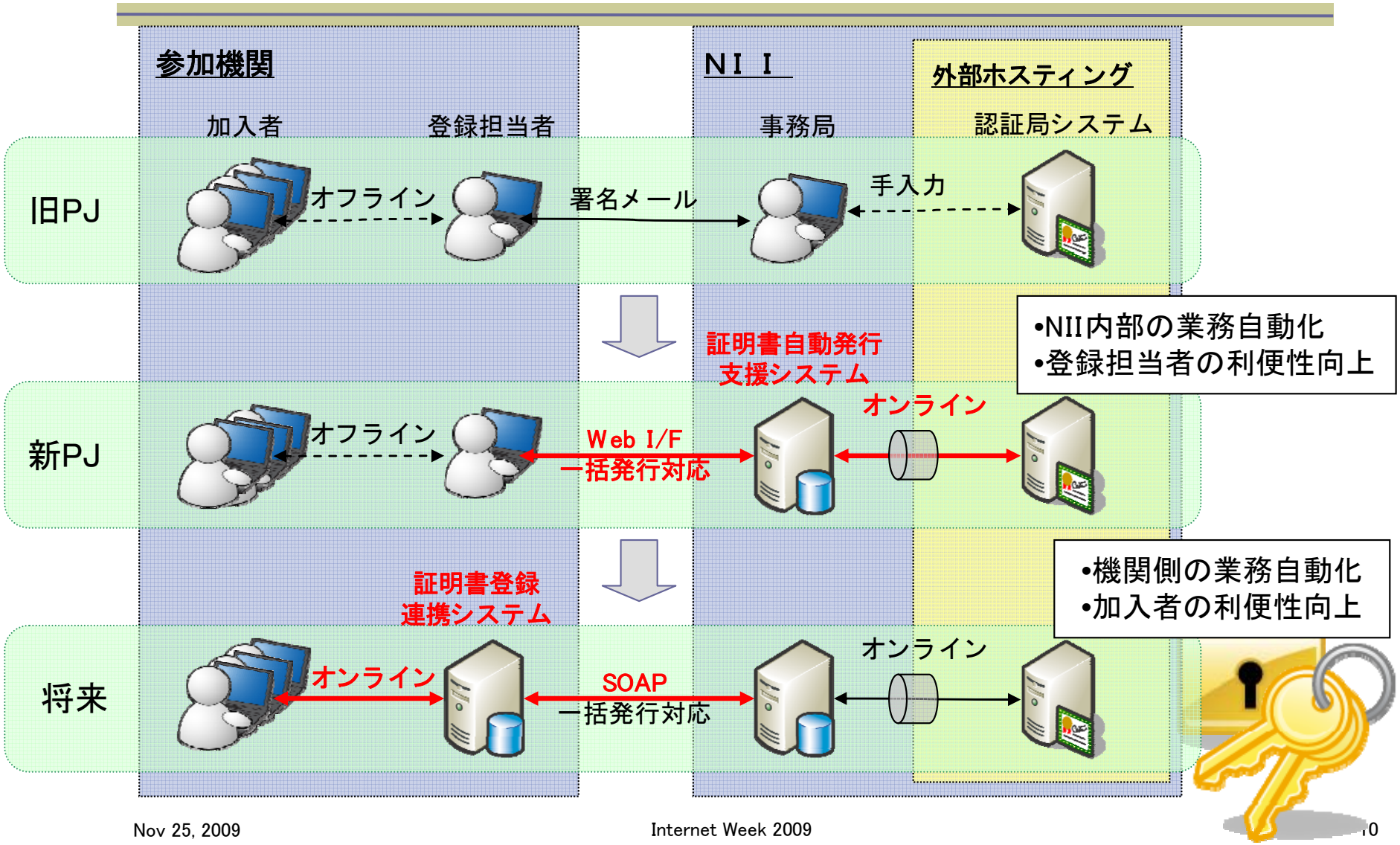
凡例
○　適切な判断規準
×　不適切な判断規準

1　参加申請書について
機関責任者が参加申請書を記述するにあたって、以下の項目をどのように確認したのかを教えてください。

1-1　ドメインが組織の保有であることの確認
申請するドメインが組織の所有であることを、「どのような情報」をもとに、「どのような方法で」確認を行い、「どのように承諾を得た」かを教えてください。

○	「Whoisデータベースでxxx.ac.jpのドメイン名管理者」を確認し、「管理者へ直接対面で問い合わせて」許
○	本学の広報委員会が「公式のWebページで利用しているドメインであることを確認」し、「LAN管理委員会会議で当該ドメインに対して証明書を発行することの承諾」を得ました。
○	機関責任者自身がドメイン管理者であり、自組織の所有であることに間違いない。
×	xxx.ac.jpのxxxが、組織名と一致していることを確認した。 *名称の確認だけでは、機関の所有するドメインであることを確認したことにはなりません。*

ゴール: 学内認証基盤との連携

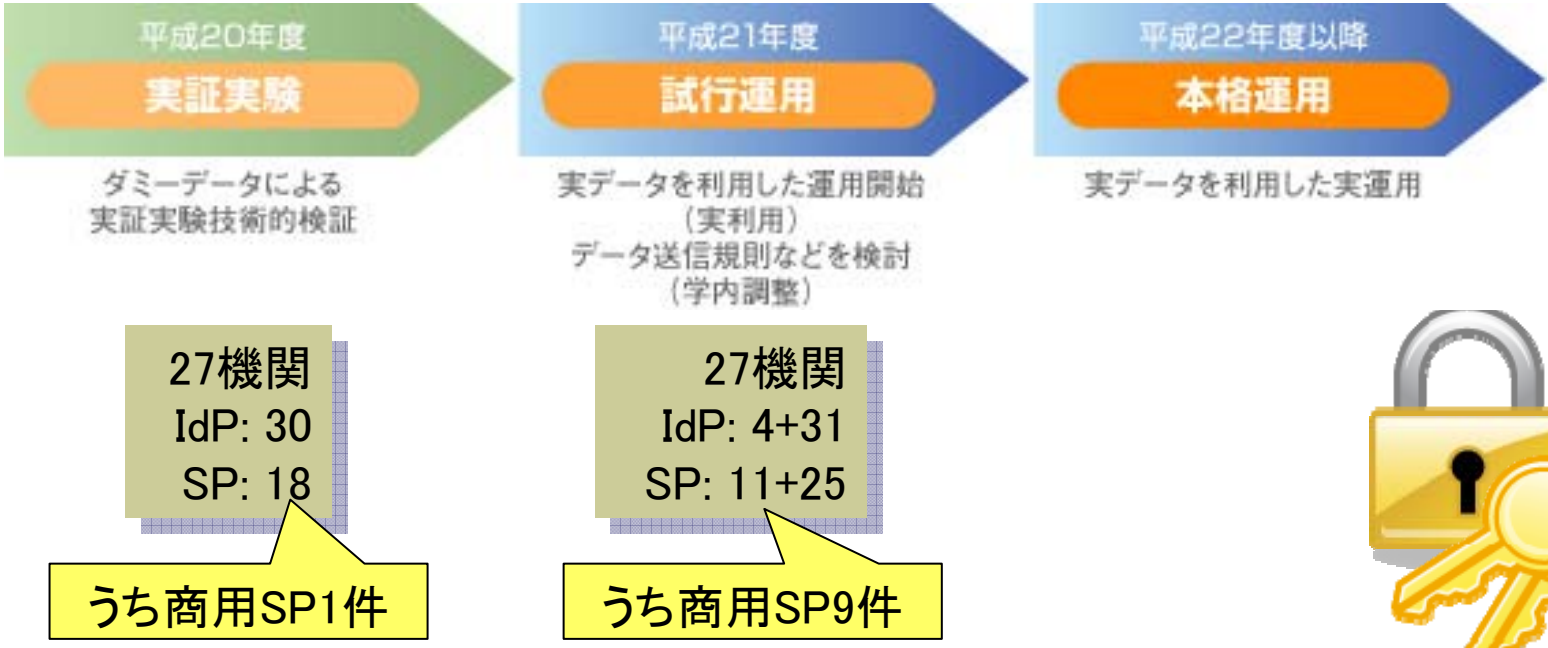


サーバ証明書プロジェクト成功への鍵

- LRAに対するガバナンス→機関単位の失効
  - LRAの義務と責任
  - 審査規程の明文化(確認実施手順調査票の提出)
- 機関認証の担保→目下実証中
  - 法人登記のない学術機関
  - 公印という呪縛
- 運用業務の省力化→PDCAサイクル
  - 既成手続きの見直し・ルーチン化
  - 参加機関の業務省力化支援

学術認証フェデレーション

- Shibbolethを利用した大学間認証連携の実現
  - 電子ジャーナル等の利便性向上
  - 海外との連携促進
- 学術リソースを利用する大学(IdP)と、学術リソースを提供する大学・企業等(SP)で連合体を構成

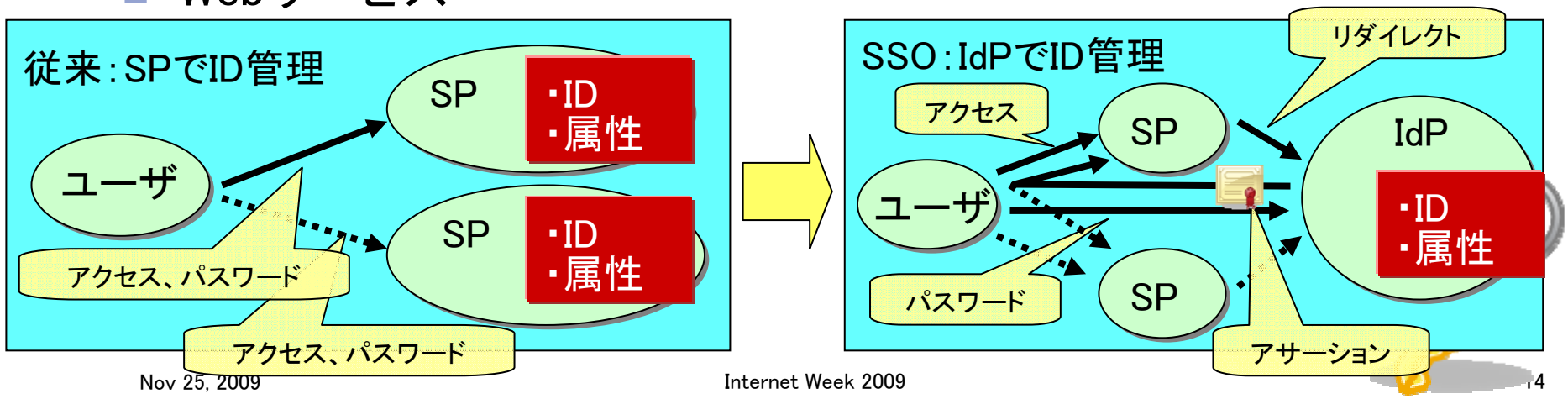


Shibboleth（シボレス）

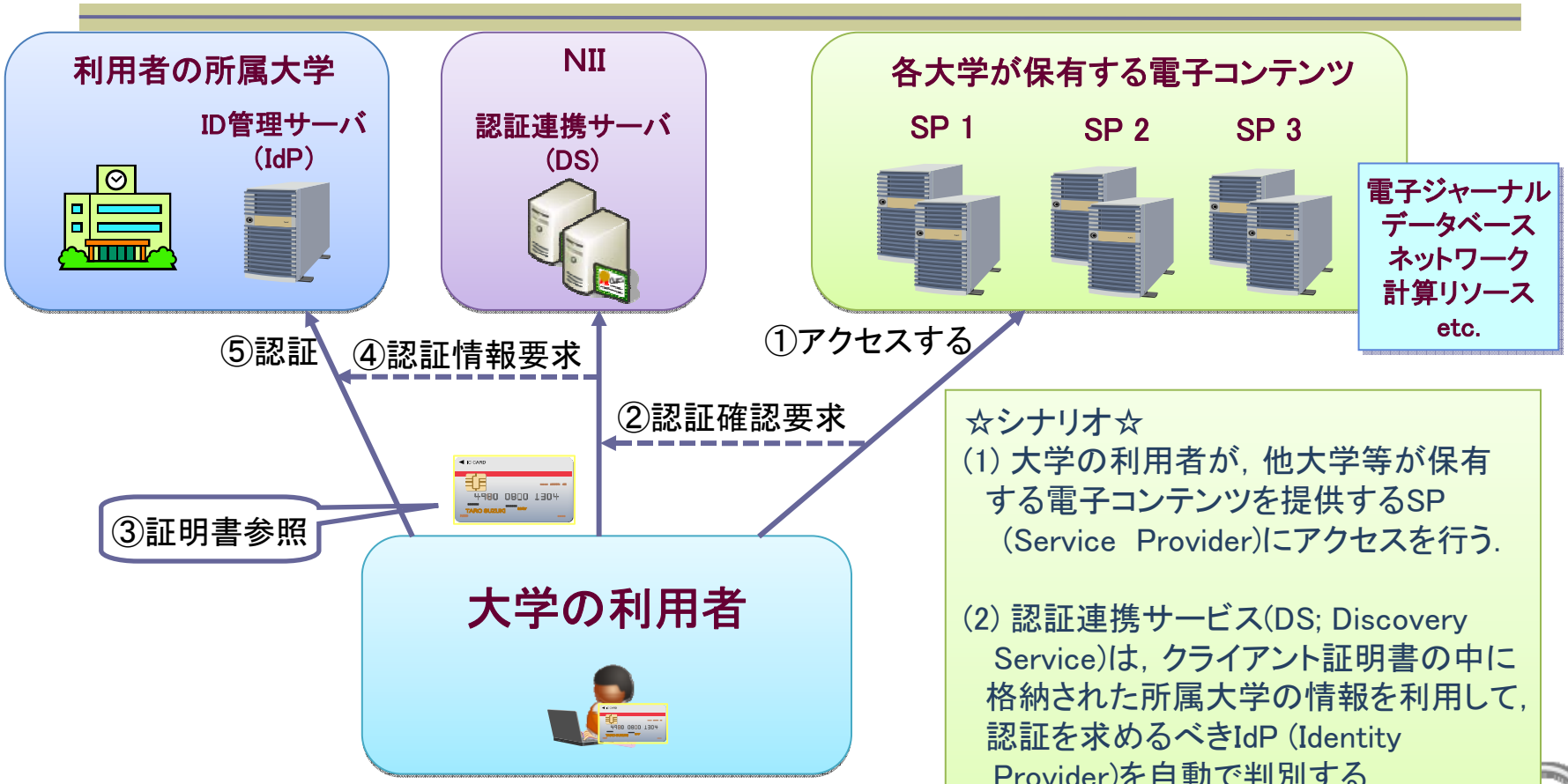
- 米国EDUCAUSE／Internet2にて2000年に発足したプロジェクト
  - http://shibboleth.internet2.edu/
- SAML、eduPerson等の標準仕様を利用した、認可のための属性交換を行う標準仕様とミドルウェア（オープンソースソフトウェア）
- 最新はShibboleth V2.1
- 米国、欧州でShibbolethによるFederationが運用、拡大

Shibbolethによるフェデレーション構築

- プライバシ保護
  - ユーザのユニークネスを保証しつつ個人情報は出さない
  - SPは必要な情報のみをIdPに要求
  - ユーザは各SPに対する各属性の公開を制御可能
- シングルサインオン技術の組織外への展開
  - 属性の分散管理＝Federation
  - IdP（大学）がIDと属性を管理して、SPがこれを利用
  - Webサービス



フェデレーションにおける認証フロー



☆シナリオ☆

(1) 大学の利用者が，他大学等が保有する電子コンテンツを提供するSP (Service Provider)にアクセスを行う.

(2) 認証連携サービス(DS; Discovery Service)は，クライアント証明書の中に格納された所属大学の情報を利用して，認証を求めるべきIdP (Identity Provider)を自動で判別する.

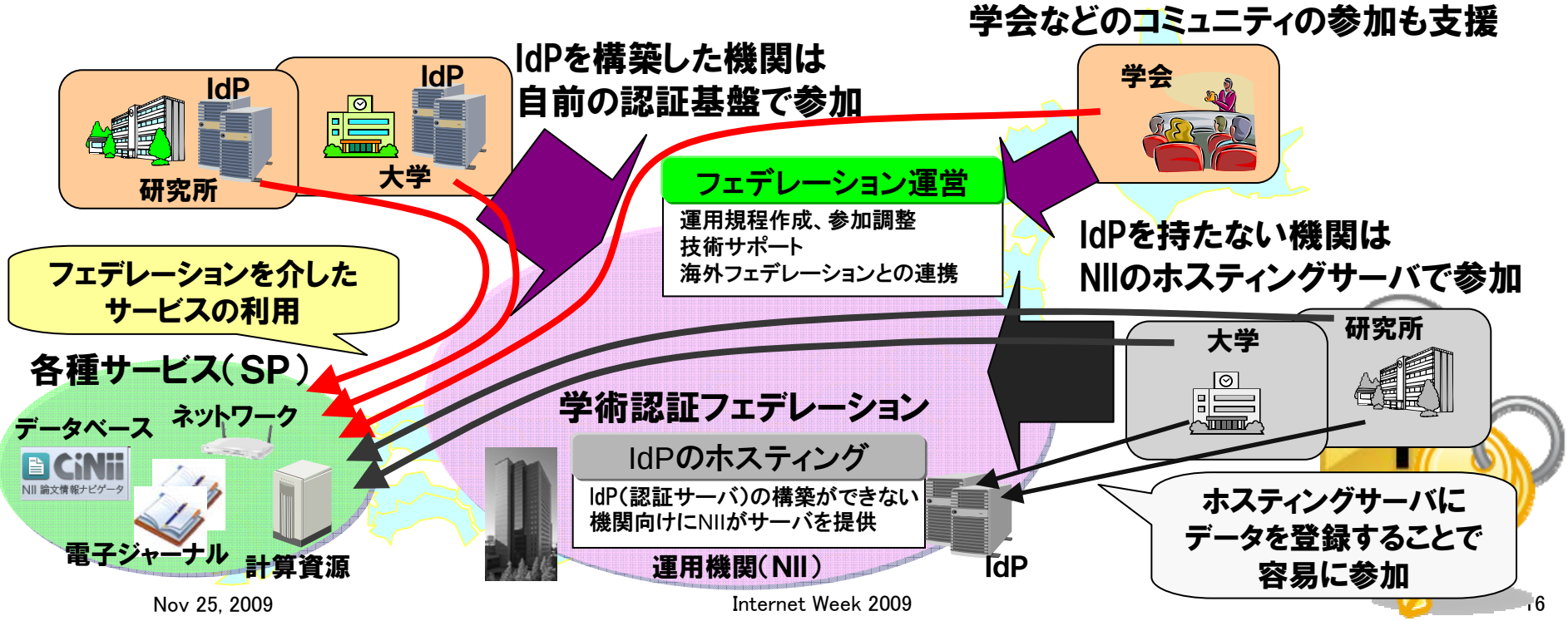
(3) 認証情報を確認できた場合は利用者は電子コンテンツにアクセスすることができるようになる.

☆ポイント☆

・自分の所属する大学の認証情報(ID)を利用して，他大学等のWebサイトや電子コンテンツに，シングルサインオンできる

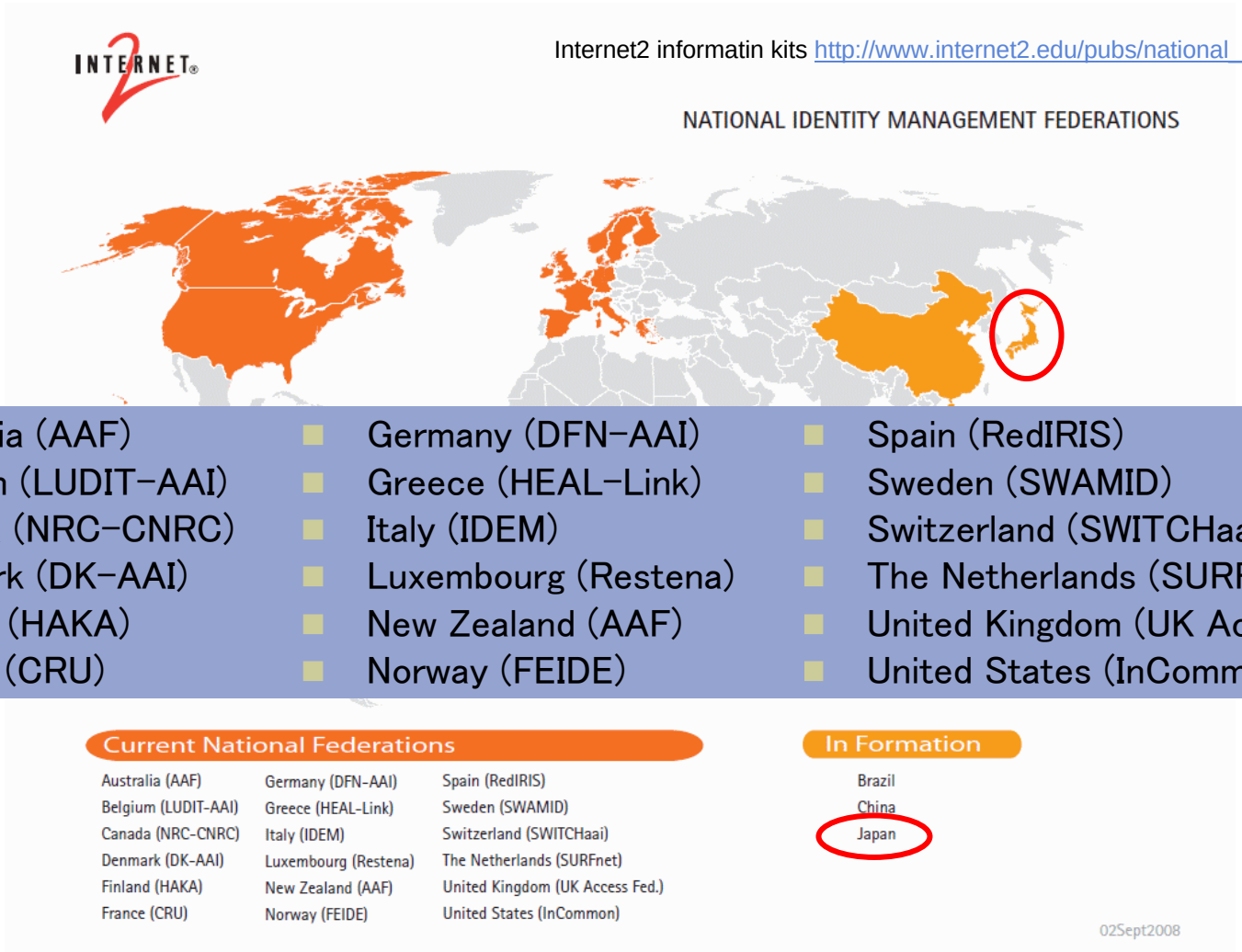
学術認証フェデレーション普及に向けて

- 大学全体のIdP構築には学内調整等の時間が必要
  - フェデレーションの早期拡大のため，調整がついた学部単位や一部のユーザグループでの参加も可能とする
- IdPの構築・運用の負担が大きい可能性
  - NIIでIdP用のホスティングサーバを用意(準備中)
  - 参加希望の機関は，データのメンテナンスのみでも参加可能



海外の学術認証フェデレーション

Internet2 informatin kits http://www.internet2.edu/pubs/national_federations.pdf から引用



- Australia (AAF)
- Belgium (LUDIT-AAI)
- Canada (NRC-CNRC)
- Denmark (DK-AAI)
- Finland (HAKA)
- France (CRU)
- Germany (DFN-AAI)
- Greece (HEAL-Link)
- Italy (IDEM)
- Luxembourg (Restena)
- New Zealand (AAF)
- Norway (FEIDE)
- Spain (RedIRIS)
- Sweden (SWAMID)
- Switzerland (SWITCHaai)
- The Netherlands (SURFnet)
- United Kingdom (UK Access Fed.)
- United States (InCommon)

学術認証フェデレーション成功への鍵

- IdPへの動機付け
  - 電子ジャーナル以外の付加価値
  - 学内認証基盤整備の動機付け
  - 統合管理による業務分析のためのIT武装
- SPへの動機付け
  - プライバシ情報管理からの解放
  - 組織単位の認可など
- 新たなサービス、新たな枠組みへの発展可能性
  - 学術コミュニティ(VO)の推進
  - 大学間、国際間でのサービス展開
- 効率的なワークフロー設計
  - フェデレーションへの参加手続き
  - IdP/SP間の契約支援
  - 運用サイクルの確立

日々勉強中です！

全国の大学をつなげるために（1）

- 継続的な啓発・広報活動
  - 全国キャラバン3回(’05, ’07, ’09)
  - 単体イベント10件、関連イベント3件、外部講演多数
  - 海外学術機関等との連携調整、民間SPとの折衝
- 各機関との合意形成
  - ポリシ、運用ガイドライン、etc.
- サーバ証明書の普及推進
  - Webサイトの信頼性向上
  - サーバとの安全な通信経路の提供
  - 認証連携に欠かせない要素

全国の大学をつなげるために(2)

- 学内認証基盤の整備支援
  - LDAPベースの統合ID管理
  - スモールスタートのサポート
  - 投資メリットのあるセンターサービス拡充
- キーパーソンの見極めと動機付け
  - 認証基盤: 情報基盤センター
  - 学術コンテンツ: 図書館
- 安定運用・事業継続性
  - 基盤として求められる重要な要件
  - # これはNIIが頑張るしかない!?

最後に

- 全国の様々な機関をつなげるには年月が必要
  - 各機関への啓発、気運の醸成
  - 各機関の内部調整
  - 機関同士での合意形成
- 一番の推進力・触媒は目的の共有
  - 共通のビジネスメリット
    - サーバ証明書の入手
    - 電子ジャーナル　など
  - これさえ明確なら話は早い