





# 「UPKI電子証明書利活用について」 セッション概要

学術情報基盤オープンフォーラム  
2015.2.3

- ▶ CSI実現に向けての、大学等の学内および大学間連携のための電子認証基盤
  - ▶ 学術ネットワーク運営・連携本部 認証作業部会 (2005年設置)
    - ▶ 7大学情報基盤センター、東工大、KEK、NIIで構成
    - ▶ 「大学間連携のための全国共同電子認証基盤構築事業」として活動開始
      - 文部科学省 (2006年度～2008年度)
- ▶ PKI技術の普及・活用のための6つの課題を設定

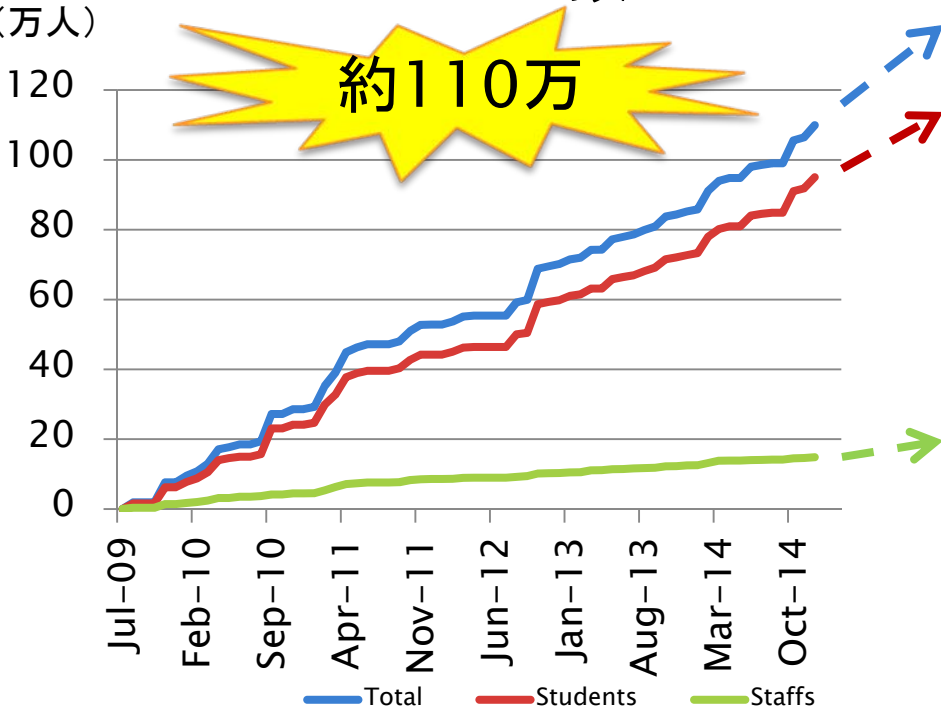
1	UPKI共通仕様の作成・配布	学内認証局構築のためのCP/CPSおよび調達仕様書の雛形を提供 (済)
2	オープンドメインサーバ証明書発行	「UPKIオープンドメイン証明書自動発行検証プロジェクト」で300以上の機関に対して無償で提供中 (のべ15000枚以上を発行)
3	大学間無線LANローミング	国際学術無線LANローミング基盤eduroamとして展開 
4	シングルサインオン検討	学術認証フェデレーション「学認」として運用中 
5	認証局ソフトウェアパッケージ開発	無線LAN認証等に適用可能なNAREGI-CAをベースとしたスタートパックを提供 (済)
6	S/MIME証明書の試験利用	実用化に向けてオープンドメインクライアント証明書の配布コストが懸案

# 学認参加IdPの推移(2015/1/1現在)

## 機関数



## ユーザ数



試行

本格運用

参考: 高等教育人口は350万人(文部科学省)

学生の割合は、80%強

	国立大学	公立大学	私立大学	短期大学	高等専門学校	共同利用機関	その他	合計
学認参加数	49	6	35	0	51	1	7	149
カバー率	57%	7%	6%	0%	89%			
総機関数	86	92	603	352	57			

# 学認参加SPの推移(2015/1/1現在)

メタデータ登録数(公開準備中を含む)

- ▶ コンテンツ系サービス
  - ▶ 電子ジャーナル
  - ▶ 機関リポジトリ
  - ▶ 文献検索
  - ▶ 論文・業績情報管理
  - ▶ 開発環境(ソフトウェア)
  
- ▶ 基盤系サービス
  - ▶ 無線ネットワークアクセス
  - ▶ Eラーニング
  - ▶ テレビ会議
  - ▶ ファイル共有
  - ▶ メーリングリスト
  - ▶ クラウド環境

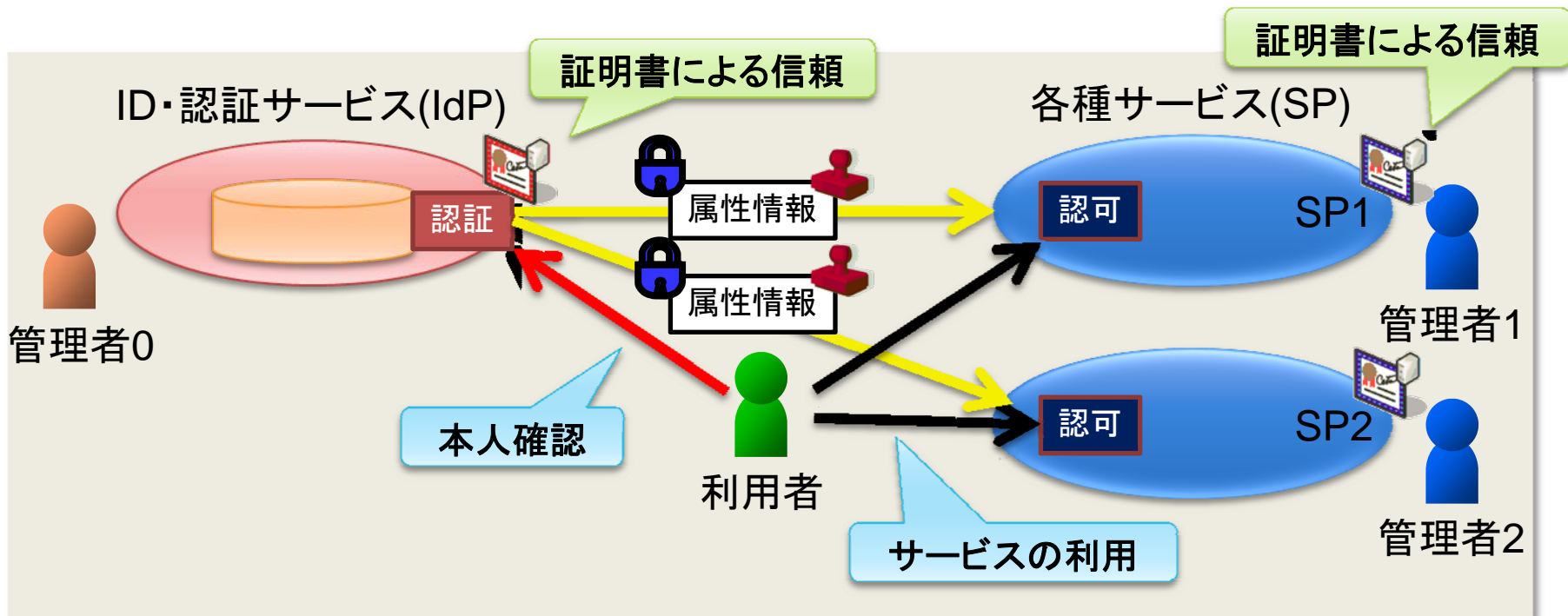


# システム構築・運用における課題

- ▶ コストの削減
  - ▶ 冗長なID管理作業の集約による効率化
  - ▶ 認証処理の高度化にかかるコストの集約 (IDaaS、AaaSの導入)
- ▶ 利便性の向上
  - ▶ 多数のID・パスワード管理からの解放、シングルサインオン
  - ▶ より良い教育・研究基盤の提供、あらゆる業務効率の改善
    - ▶ クラウドサービスの活用、サービス間連携、マッシュアップ
- ▶ 安全性の向上
  - ▶ 様々なシステムに対する、認証の安全性の底上げ
  - ▶ 高度な認証方式への対応が容易
    - ▶ サービスごとに異なる認証レベルの提供
  - ▶ 集中的なアクセス記録と監査 (不正アクセスの発見と対策)

# クラウド環境活用のためのID連携

- ▶ 「認証」と「認可」の分離
  - ▶ **認証**: 本人確認 (Authentication)
  - ▶ **認可**: その人に利用させるかどうかの判断 (Authorization)
- ▶ 学認とeduroamはプロトコルは異なるが、枠組みはほぼ同じ



# 電子証明書の種類と用途

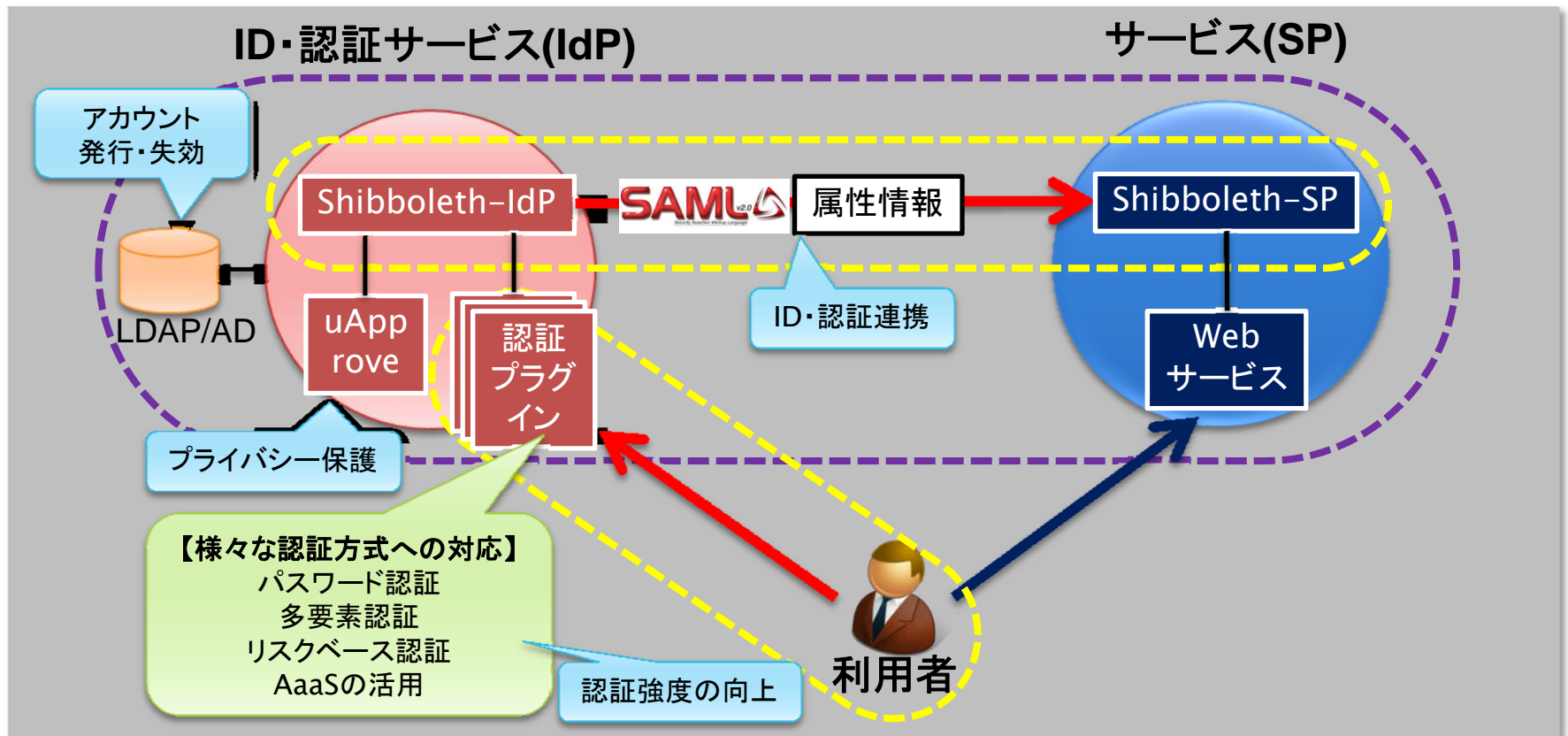
- ▶ サーバ証明書(正当性確認、暗号化)
  - ▶ Domain Validation (ドメイン所有者であることの確認)
  - ▶ Organization Validation (組織の実在性の確認)
  - ▶ Extended Validation (法的実在性等の確認、**緑色**)
- ▶ クライアント証明書(認証、暗号化、署名)
  - ▶ 電子メール(S/MIME)での利用の有無
- ▶ コードサイニング証明書
  - ▶ タイムスタンプを付与することで有効期限の延長が可能
- ▶ タイムスタンプ局証明書
  - ▶ タイムスタンプ、長期署名

高度な認証手段の提供

新サービスにて提供

# IdPにおける運用管理のイメージ

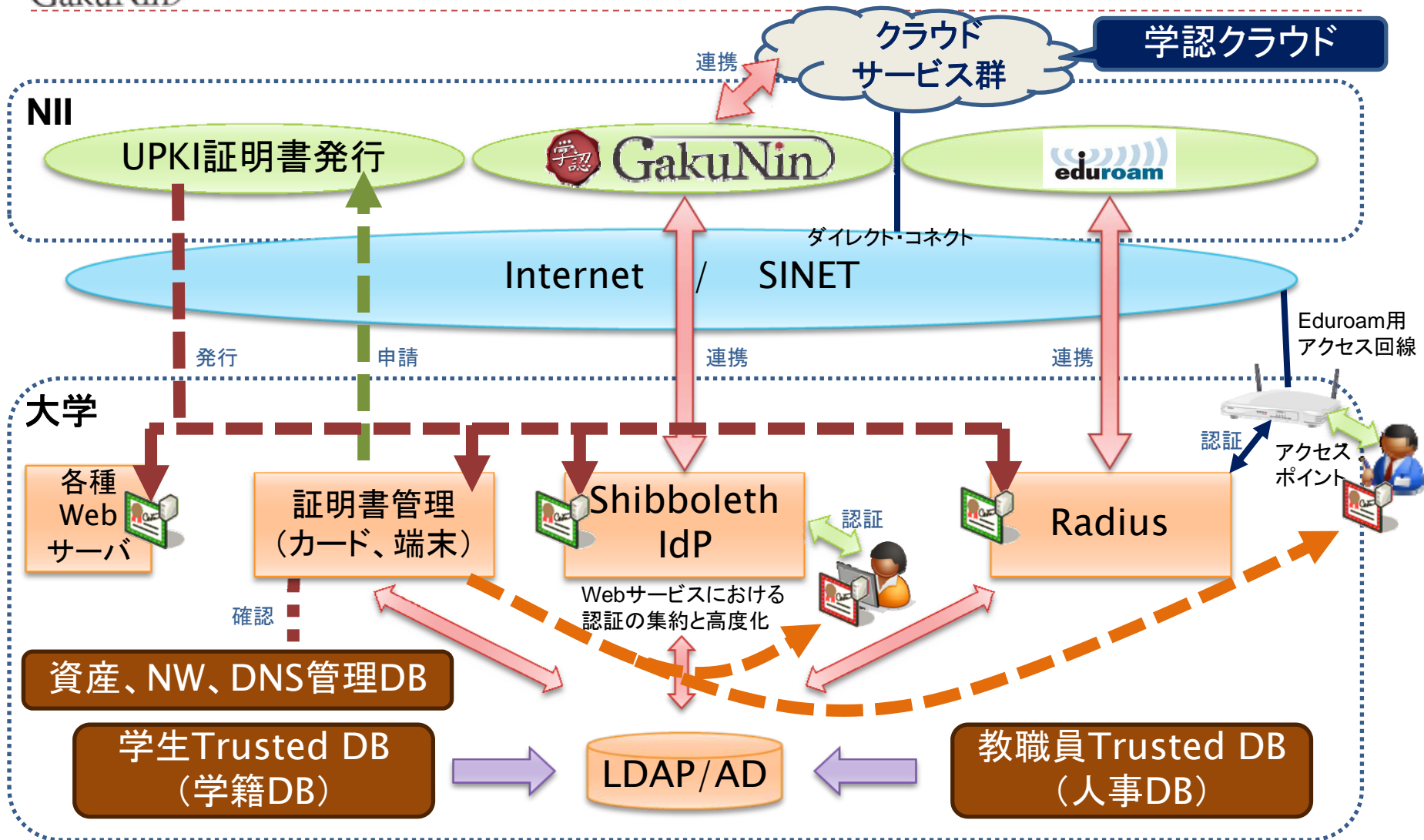
- ▶ Shibboleth IdPでは、多様な認証方式やプライバシー保護をプラグインにより柔軟にサポート



AaaS: Authentication as a Service



# 大学における情報基盤の 認証を中心としたイメージ



# 「UPKI電子証明書利活用について」

- ▶ UPKI電子証明書サービスのご案内
  - ▶ 国立情報学研究所 学術基盤課 水元 明法
- ▶ 大学統合認証基盤における多要素認証について
  - ▶ 金沢大学 情報化推進室 松平 拓也
- ▶ UPKIパスシステムとUPKIパス(カード)発行サービス
  - ▶ (株)高見沢サイバネティックス 増井 正宏
  - ▶ トップラン・フォームズ(株) 竹内 範幸
- ▶ EV証明書の意義
  - ▶ セコム(株)IS研究所 島岡 政基
- ▶ 電子署名とタイムスタンプ
  - ▶ セイコーソリューションズ(株) 柴田 孝一