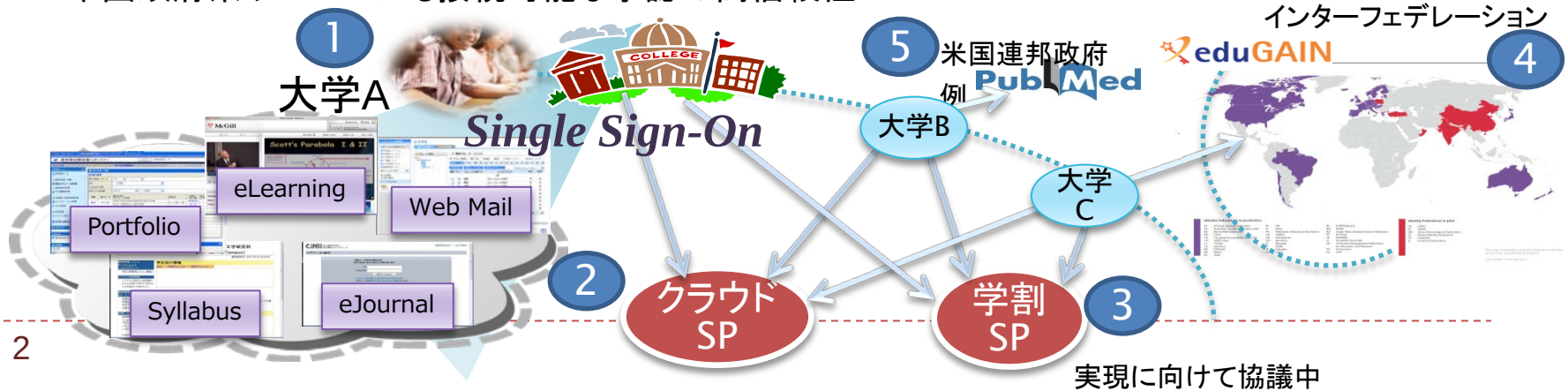
魅力的な学認

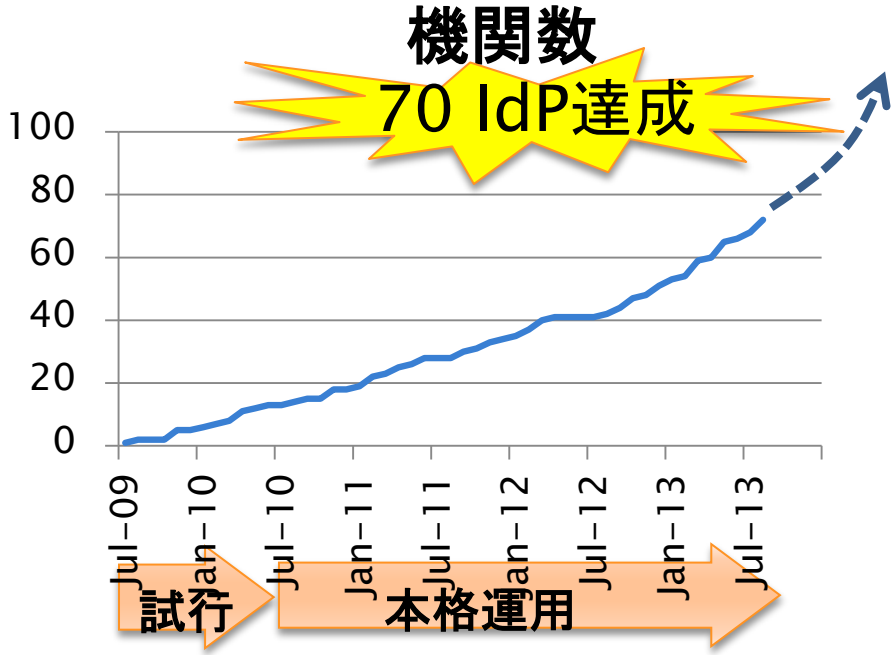
中村素典／国立情報学研究所
2013/9/11

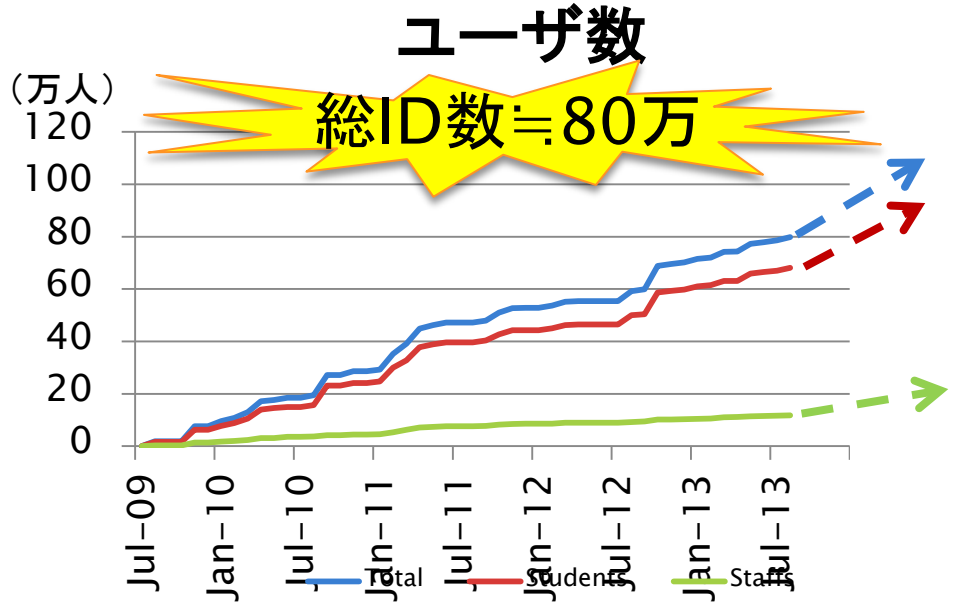
学術認証フェデレーション「学認」(2009～)

1. 大学におけるオンライン認証機構のデファクトスタンダード
   - 国際標準のSSO機構によるスムーズなアクセスが大学に急速に波及中
2. 大学ICTインフラのクラウド活用のカギ
   - 利便性の高いサービスを低コストで導入
3. 信頼性の高いID情報をセキュアに提供
   - インターネット学割にも利用できる仕組みとして企業も注目
4. 全世界の学術インフラが繋がる標準認証機構
   - 日本からの積極的な伝道によりアジア各国も準備中
5. 米国政府系サービスにも接続可能な学認の高信頼性



学認参加IdPの推移(2013/9/1現在)





高等教育人口は350万人(文部科学省)

学生の割合は、80%強

学認参加機関一覧（71機関）

- 国立情報学研究所
- 名古屋大学
- 山形大学
- 千葉大学
- 京都大学
- 広島大学
- 北海道大学
- 筑波大学
- 佐賀大学
- 成城大学
- 東邦大学
- 三重大学
- 日本大学
- 旭川医科大学
- 岡山大学
- 九州工業大学
- 京都産業大学
- 立教大学
- 九州大学
- 東京大学
- 明治大学
- 神戸大学
- 信州大学
- 自治医科大学
- 名古屋工業大学
- 山梨大学
- 広島市立大学
- 大阪大学
- 宮崎大学
- 横浜国立大学
- 放射線医学総合研究所
- 釧路工業高等専門学校
- 北見工業大学
- 広島工業大学
- 金沢大学
- 愛媛大学
- 鈴鹿工業高等専門学校
- 奈良先端科学技術大学院大学
- 奈良教育大学
- 立命館大学
- 東京医科歯科大学
- 札幌医科大学
- 国立高等専門学校機構
- 関西大学
- 大阪教育大学
- 京都教育大学
- 京都府立大学
- 豊橋技術科学大学
- 福井工業高等専門学校
- 静岡大学
- 宮城教育大学
- 帝塚山大学
- 東京歯科大学
- 昭和大学
- NTT東日本関東病院
- 東京海洋大学
- 創価大学
- 東京都医学総合研究所
- CCC-TIES
- 中部大学
- 国立女性教育会館
- 琉球大学
- 東京農工大学
- 芝浦工業大学
- 東京学芸大学
- 福井大学
- 苫小牧工業高等専門学校
- 大阪体育大学
- 北九州工業高等専門学校
- 福岡工業大学
- 武蔵学園

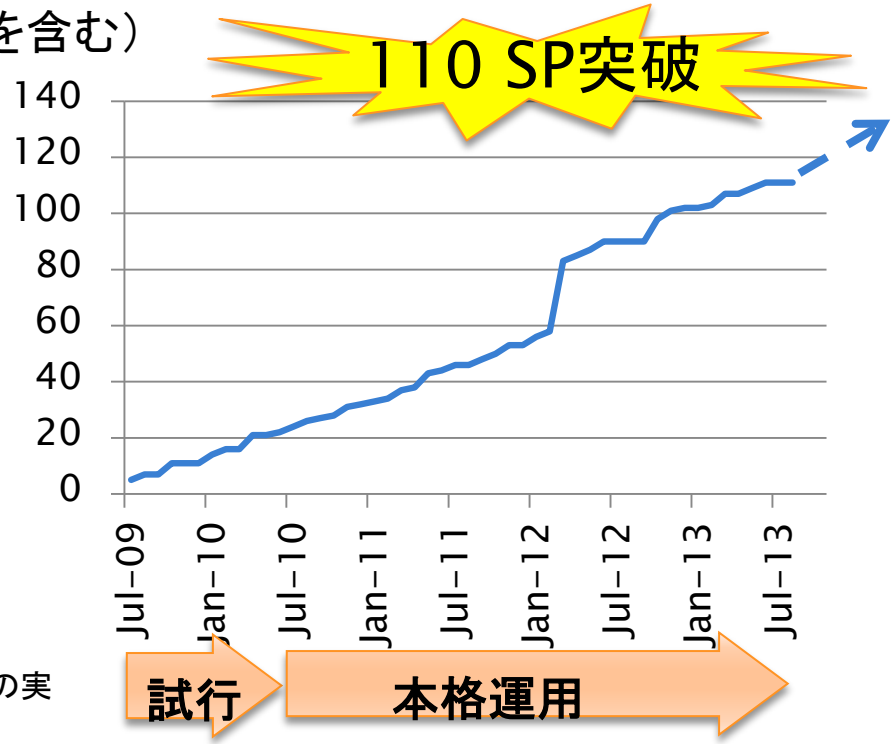
2013年9月1日現在

参加機関一覧：https://www.gakunin.jp/participants/

学認参加SPの推移（2013/9/1現在）

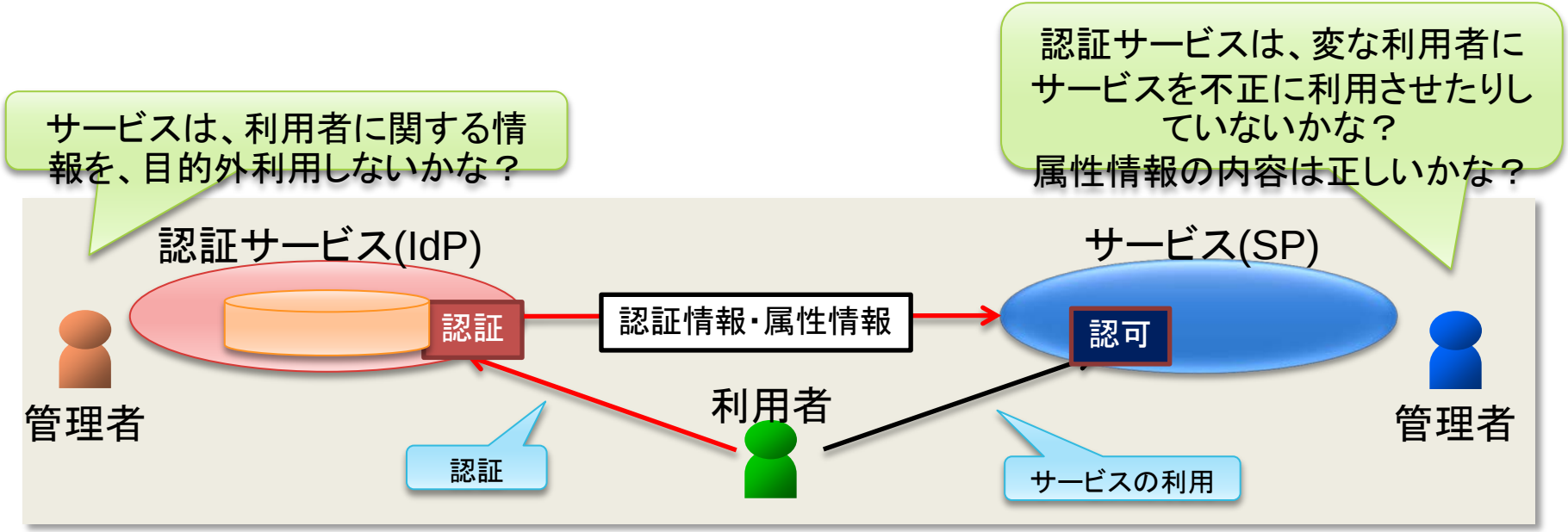
メタデータ登録数（公開準備中を含む）

- 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
  - クラウド環境
- SITF (Student Identity Trust Framework)による学割サービスの実現を検討中



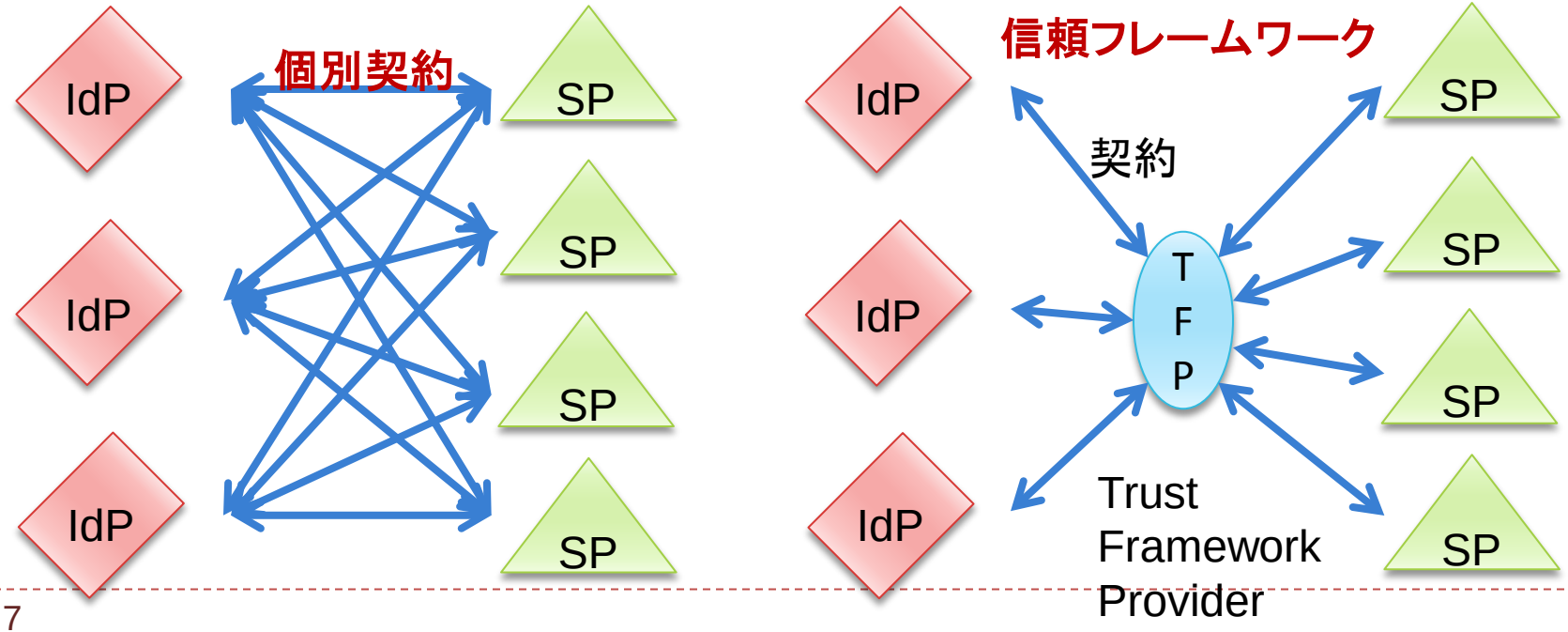
SSO技術の組織間利用での信頼

- 認証と認可の分離
- 異なる組織が個別に管理するため、相互の信頼が重要



信頼フレームワークの効果

- 一律のポリシーに基づく信頼フレームワークの導入により、個別契約でのN×Mの関係が、N＋Mの関係に削減



学認で定めるIdPの要件（システム運用基準）

- 組織の構成員であることの保証
  - 卒業、退職などによる異動の適切な反映
  - 名誉教授、OB、図書館の地域内利用者、その他ゲスト等の扱い
- 識別子再利用についての考慮
  - 同一識別子を利用する場合は、一定期間あける
- ユーザの同一性の保証
  - パスワード配布時の本人確認
  - 適切に管理された役職アカウント
- 個人情報保護への対応
  - 国公立大学ではオプトインが原則
- ログの保存
  - インシデント対応のための、eduPersonTargetdIDやtransient-idの記録

機関として責任を持った IDおよび属性の保証

⇒定期アンケート（毎年）によるチェックとフィードバックで維持

- IdP of The Year 2012 を大阪大学が受賞

LoA: Level of Assurance

OMB 04-04 / NIST SP800-63 / ISO 29115 / ITU-T X.1254

- OMB M-04-04 E-Authentication Guidance for Federal Agencies (2003)
- NIST SP800-63 Electronic Authentication Guideline (2006発行, 2011改訂)
- ITU-T X.1254 Entity Authentication Assurance Framework (2012-09承認)
- ISO/IEC 29115:2013 Entity authentication assurance framework
  - 2013-04-01日付で標準化

Level	Description
1 – Low	Little or no confidence in the asserted identity 身元確認不要、匿名 例：whitehouse.govのWebサイトでのオンラインディスカッションに参加
2 – Medium	Some confidence in the asserted identity 身元識別（身分証明書）、単一要素認証可、失効処理 例：社会保障Webサイトを通じて自身の住所記録を変更
3 – High	High confidence in the asserted identity 多要素認証 例：特許弁理士が特許商標局に対し、機密の特許情報を電子的に提出
4 – Very high	Very high confidence in the asserted identity 対面による発行、ハードウェアトークン 例：法執行官が、犯罪歴が格納されている法執行データベースにアクセス

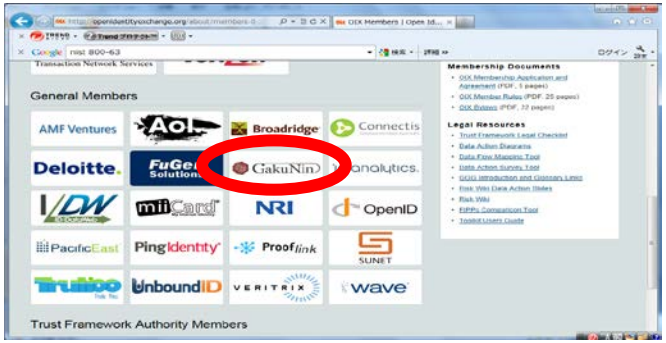
OpenID 2.0はLoA-2まで、SAML/OpenID ConnectはLoA-4まで対応

Level of Assurance (LoA)

- 米国連邦政府内のサービス(SP)を、外部の認証システム(IdP)に接続する場合には、SP側がIdPに適切な保証レベル(LoA)を要求

- PubMed(日本を含む世界約80カ国で発行される生物医学系文献の検索サイト)など、米国国立衛生研究所（NIH）が提供する95のサービスの要求はLevel 1（最低）
  - 利用するためには学認のIdPが米国の基準に則ったLevel 1を取得する必要あり。

- 学認は、学認のIdPにLevel 1を発行できる Trust Framework Providerに
  - 米OIX (Open Identity eXchange、非営利組織)のメンバー

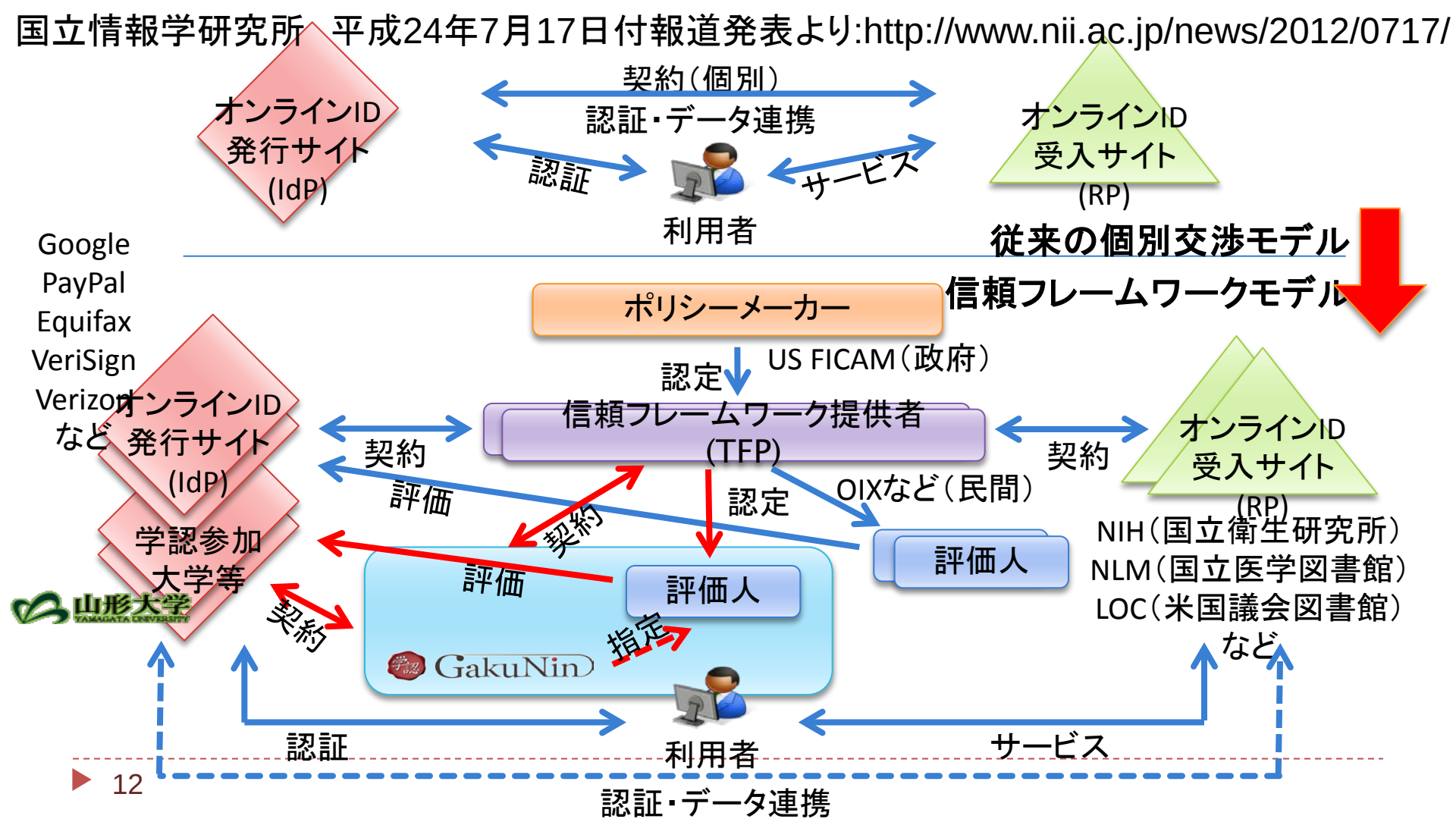


学認によるLoA1認定

- 米国FICAM信頼フレームワークにおけるLoA 1に準拠したIdP評価
  - 2012年7月4日より学認にて評価開始
    - 申請ベース（無償）
    - 毎年更新
  - OIX認定評価人：佐藤周行准教授（東京大学、NII客員）

- 認定の流れ
  1. 大学等から学認に申請
  2. 学認にて保証レベルを評価
     - 学認定期アンケート、公開情報、規定類の提出、面接など
  3. 学認よりOIXへ申請

国立情報学研究所　平成24年7月17日付報道発表より:http://www.nii.ac.jp/news/2012/0717/



山形大学をFICAM LoA 1認定

- 2013/8/1付


河北新報　東北のニュース／ＩＤ認証　世界水準　山形大を米機関が認定 - Mozilla Firefox

ファイル(F)　編集(E)　表示(V)　履歴(S)　ブックマーク(B)　ツール(T)　ヘルプ(H)

河北新報　東北のニュース／ＩＤ認証...

www.kahoku.co.jp/news/2013/09/20130906t55015.htm?sl

河北新報のニュースサイト・コルネット

山形のニュース

ID認証　世界水準　山形大を米機関が認定

ID認証が世界水準と認められたと発表する伊藤准教授(左)ら

山形大は5日、学生や教職員がインターネットサイトに接続する際に同大が発行するオンラインIDと認証システムが、米国の審査機関OIXの「第1保証レベル（LoA1）」に認定されたと発表した。OIXの認定を受けたID発行機関は国内に例がなく、アジアで第1号になるという。

山形大のIDを取得した学生や教職員は、米政府関連機関の国立衛生研究所、国立医学図書館、米国議会図書館のサイトなどに接続できるようになり、研究の幅が広がると期待される。

認定は8月1日付。国立情報学研究所（東京）が申請に基づき、ID認証の信頼性を評価。結果を踏まえ、OIXが山形大をLoA1認定機関のリストに載せた。保証レベルは4段階で、LoA1は最も基本的な段階という。

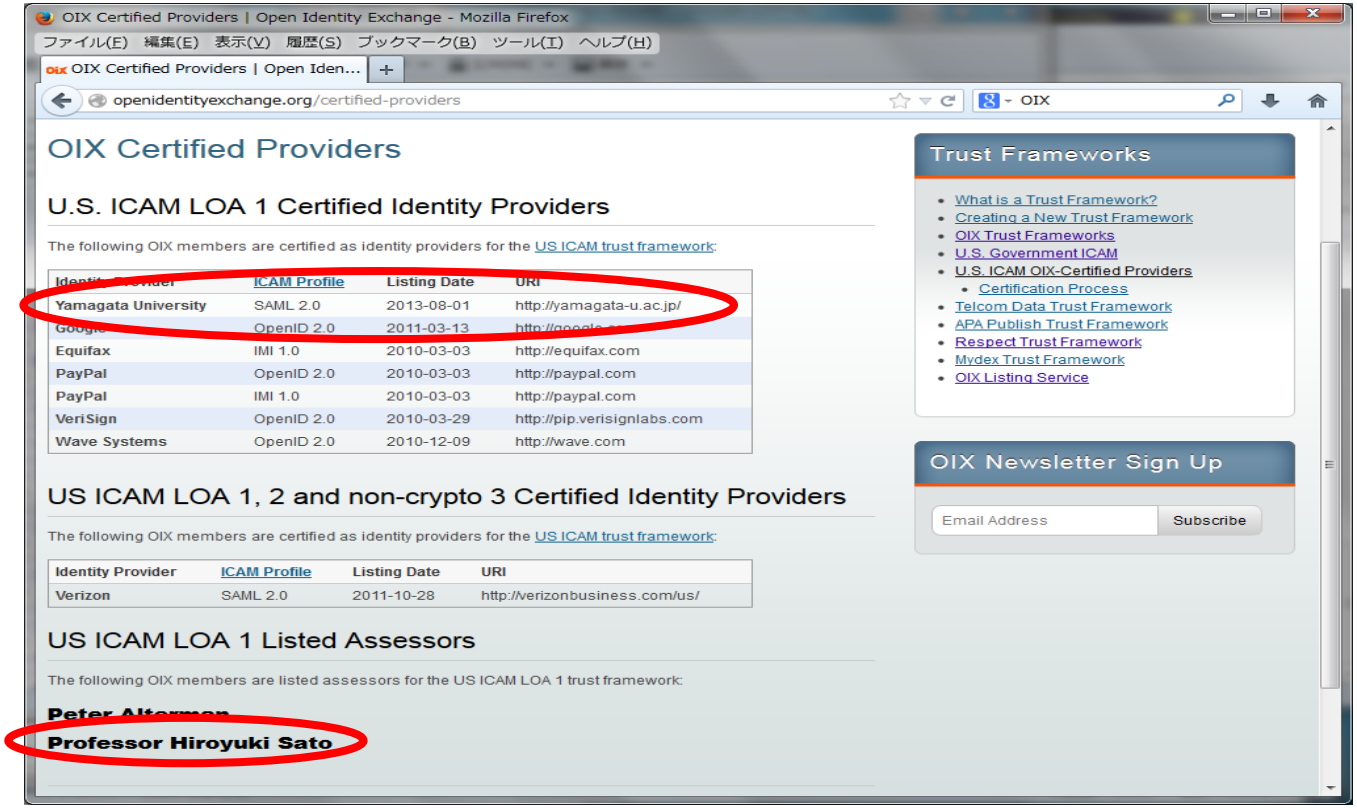
LoA1認定の機関は、他にインターネット検索最大手の米グーグルなどが名を連ねている。

山形大大学院理工学研究科の伊藤智博准教授は記者会見で「山形大のIDで購入した電子書籍には学割を設けるなど、認証の信頼性の高さを武器にして、商用サービスサイトとの新たな連携も模索したい」と話した。

2013年09月06日金曜日

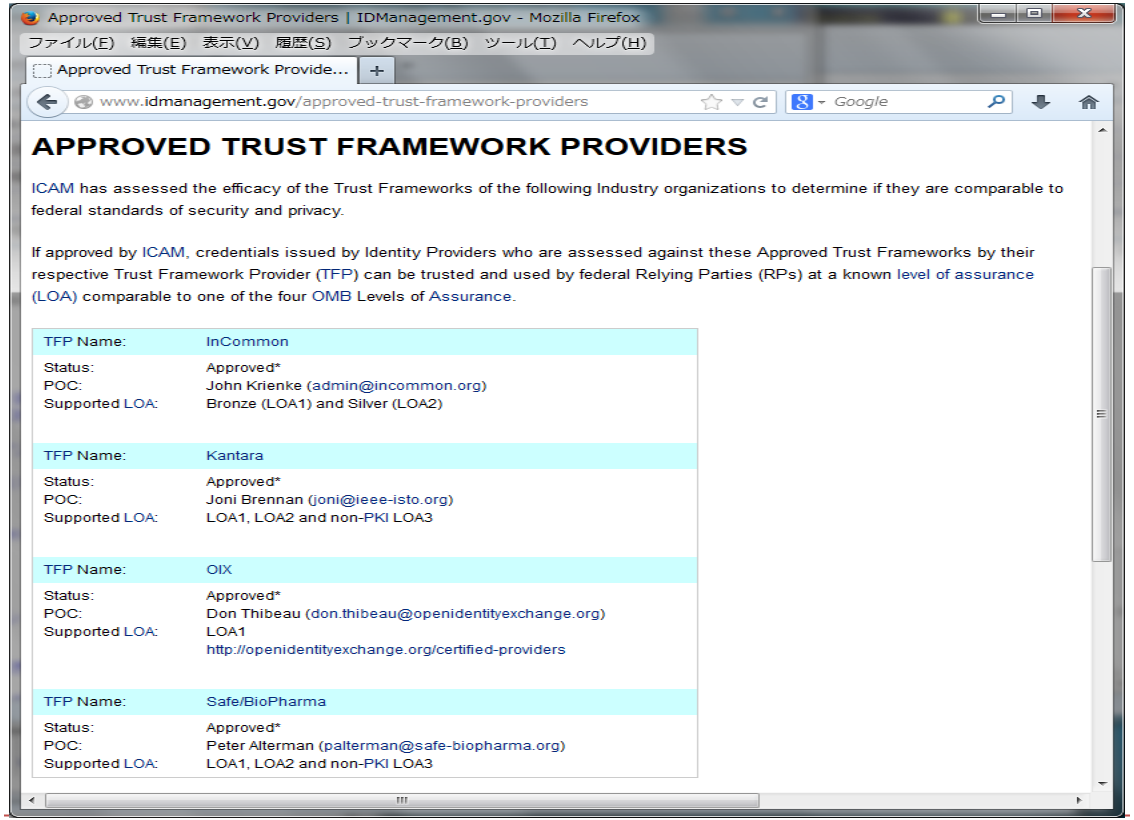
OIXのLoA 1リスティング

- 山形大学
  - 7番目

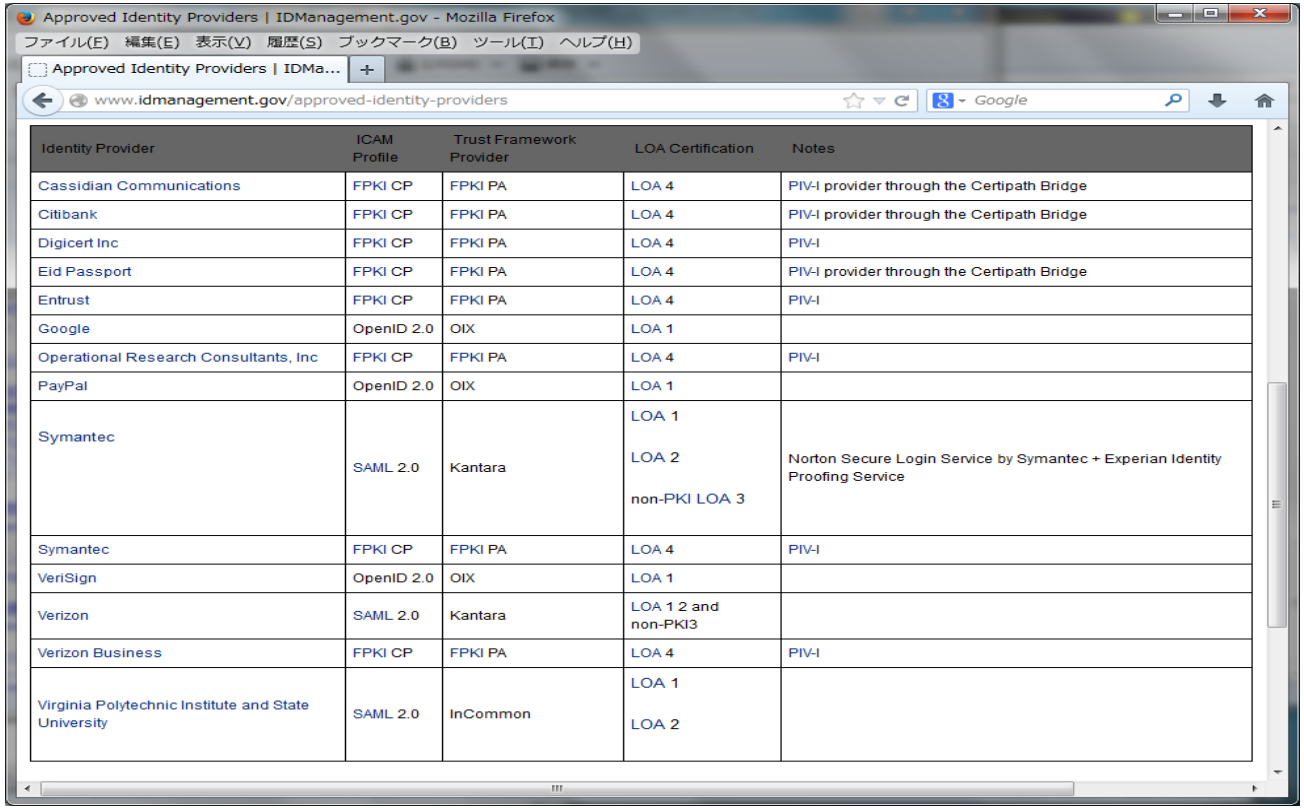


FICAMのTFPリスト

- InCommon
  - 1,2
- Kantara
  - 1,2,non-PKI 3
- OIX
  - 1
- Safe/BioPharma
  - 1,2,non-PKI 3
- FPKI PA
  - 4

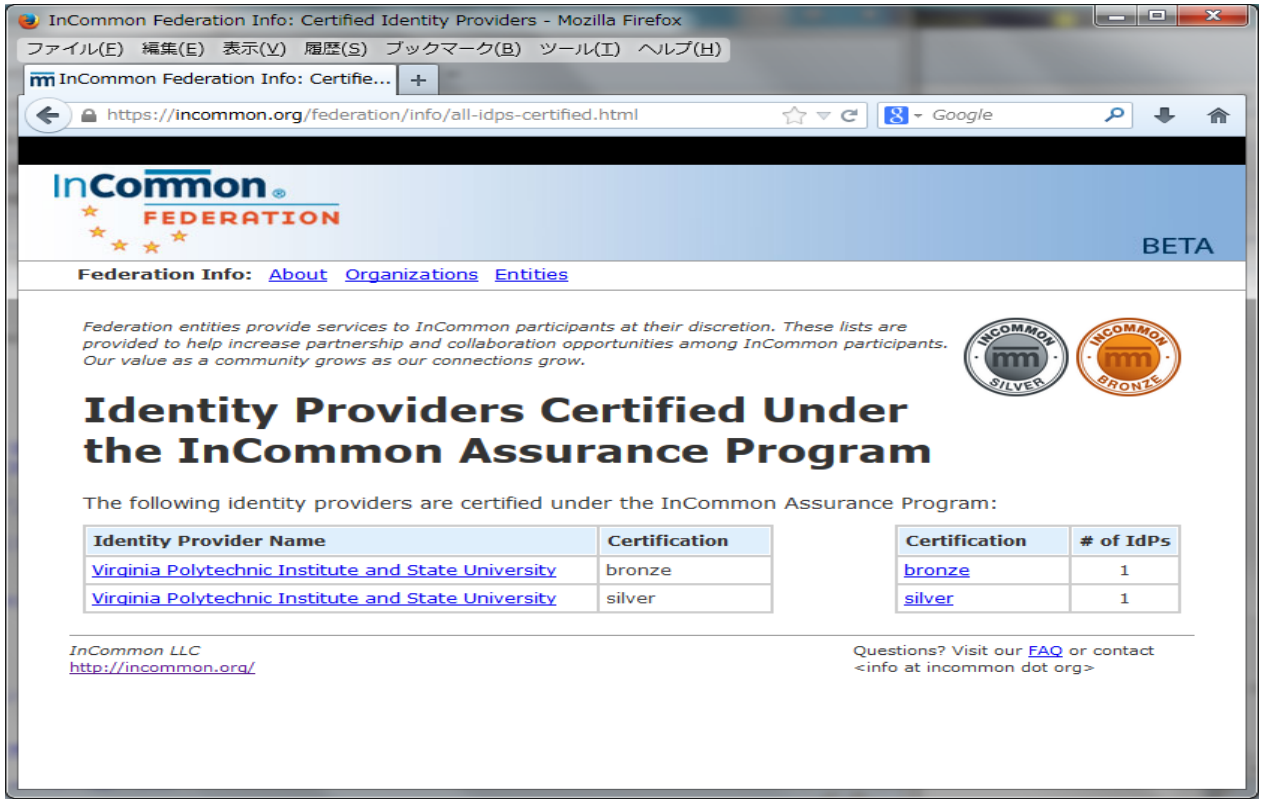


FICAMの認定IdPリスティング

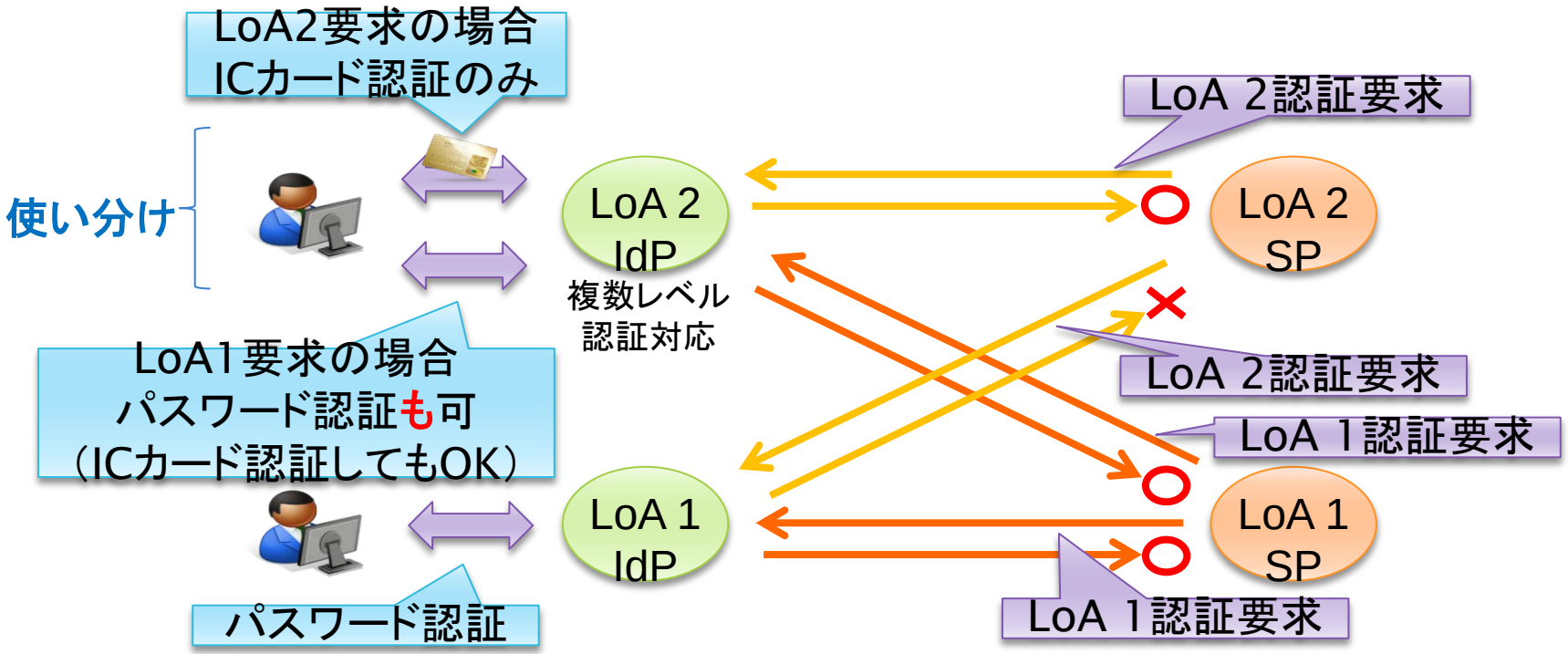


Identity Provider	ICAM Profile	Trust Framework Provider	LOA Certification	Notes
Cassidian Communications	FPKI CP	FPKI PA	LOA 4	PIV-I provider through the Certipath Bridge
Citibank	FPKI CP	FPKI PA	LOA 4	PIV-I provider through the Certipath Bridge
Digicert Inc	FPKI CP	FPKI PA	LOA 4	PIV-I
Eid Passport	FPKI CP	FPKI PA	LOA 4	PIV-I provider through the Certipath Bridge
Entrust	FPKI CP	FPKI PA	LOA 4	PIV-I
Google	OpenID 2.0	OIX	LOA 1	
Operational Research Consultants, Inc	FPKI CP	FPKI PA	LOA 4	PIV-I
PayPal	OpenID 2.0	OIX	LOA 1	
Symantec	SAML 2.0	Kantara	LOA 1 LOA 2 non-PKI LOA 3	Norton Secure Login Service by Symantec + Experian Identity Proofing Service
Symantec	FPKI CP	FPKI PA	LOA 4	PIV-I
VeriSign	OpenID 2.0	OIX	LOA 1	
Verizon	SAML 2.0	Kantara	LOA 1 2 and non-PKI3	
Verizon Business	FPKI CP	FPKI PA	LOA 4	PIV-I
Virginia Polytechnic Institute and State University	SAML 2.0	InCommon	LOA 1 LOA 2	

米国InCommonの認定IdPの状況



複数のLoAレベルによる認証



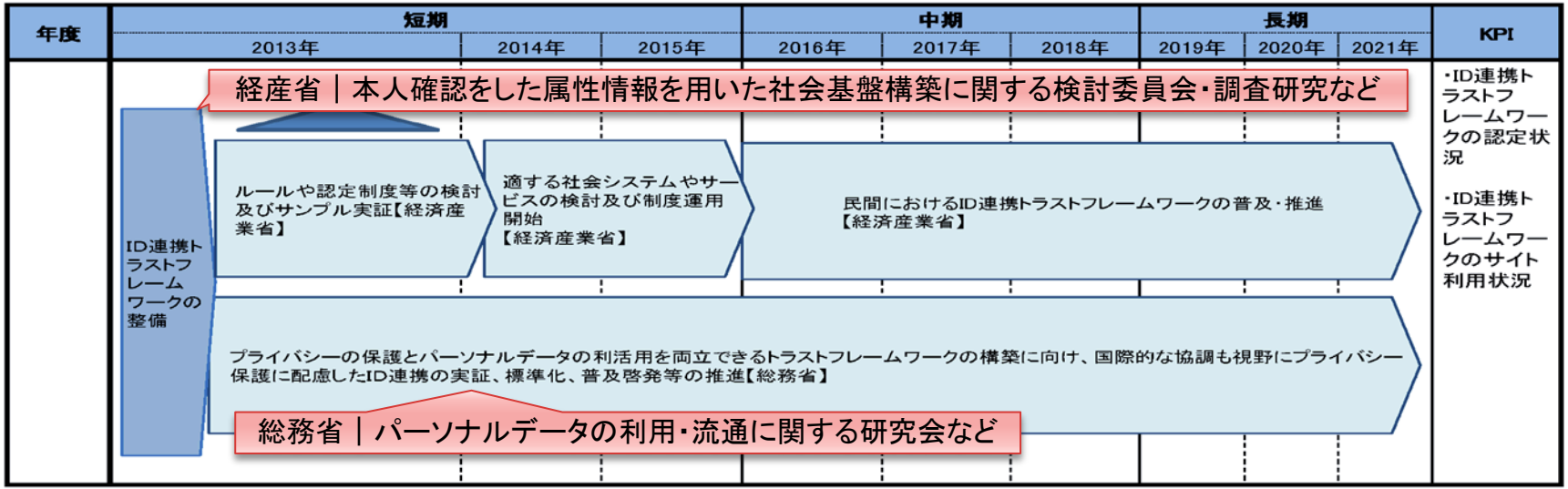
複数LoAに対応した認証の利用イメージ

- 例えば、ICカード認証とパスワード認証の両方をサポートすることで、ユーザの利用スタイルに柔軟に対応可能
  - LoA 1サービスの利用時は、どちらの認証方式を選択してもOK
    - どんな端末からでも使いやすく
  - パスワード認証後に、LoA 2サービスにアクセスすると、ICカード認証が要求される（昇格）
  - ICカードを抜くと、LoA 2サービスからログアウト（降格）
    - LoA 1サービスは引き続き利用可能
      - SSOの利便性を保つ
  - その他
    - 学内からであればパスワードでもOK、等

日本国内におけるID連携の活用に向けて

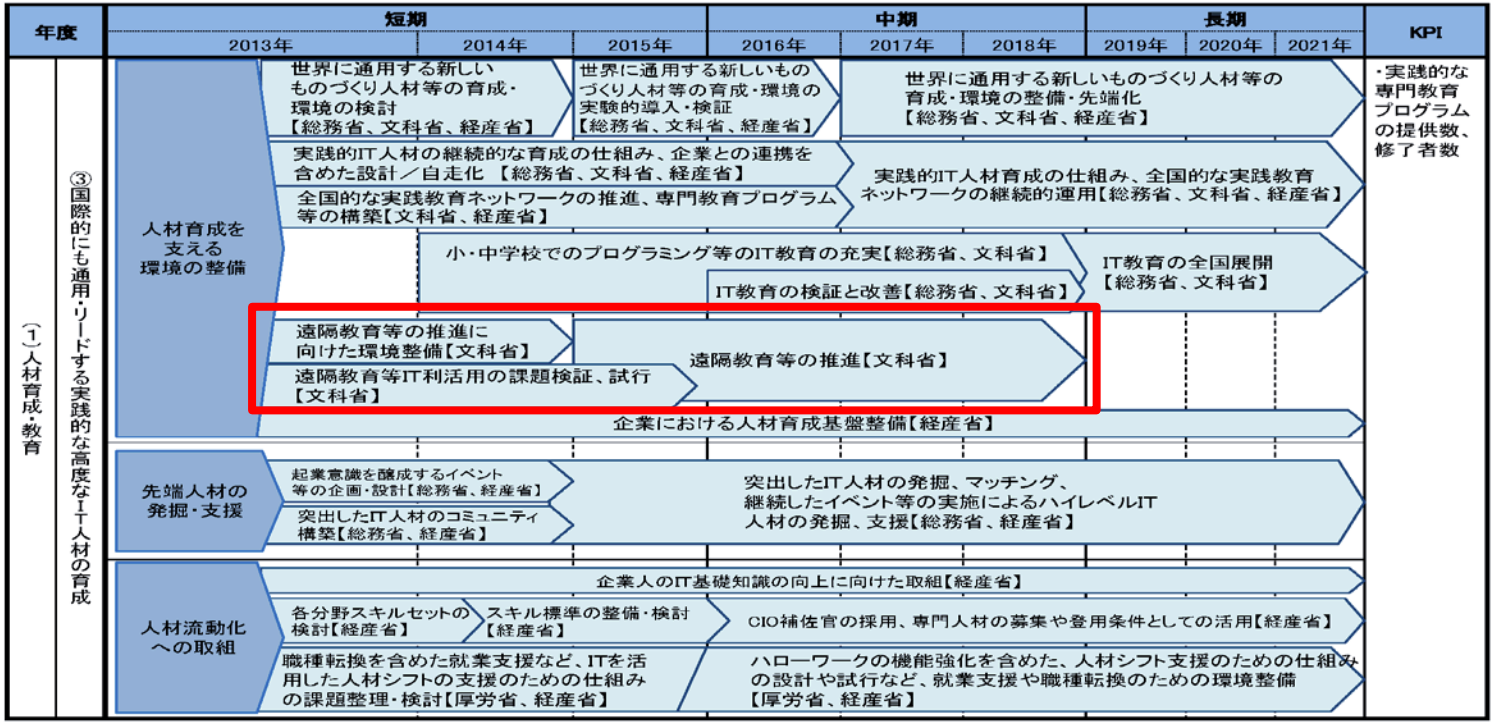
- 世界最先端 IT 国家創造宣言「工程表 」
  - 平成25年6月
  - 高度情報通信ネットワーク社会推進戦略本部（IT総合戦略本部）

実施スケジュール （5. 規制改革と環境整備）



（参考）

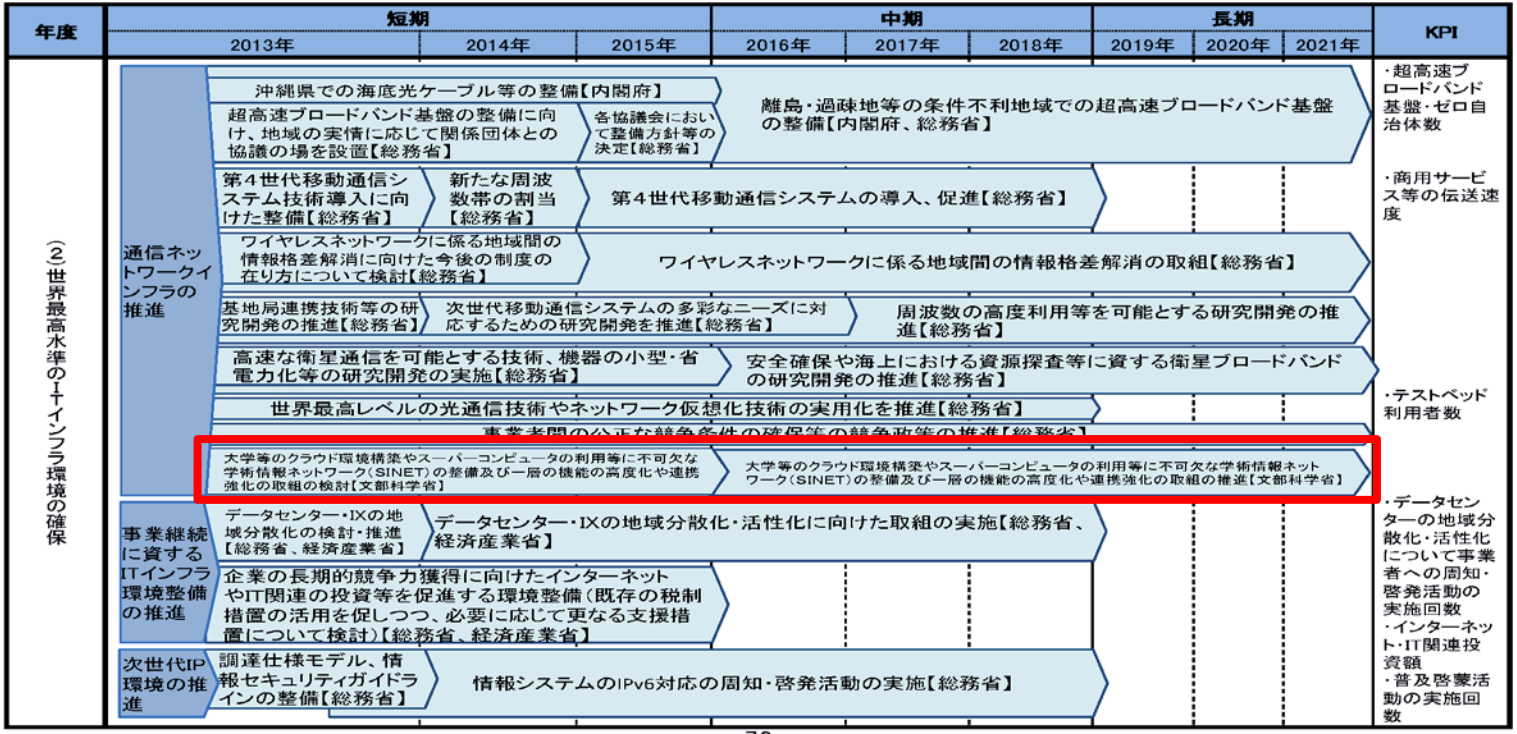
実施スケジュール （4. 利活用の裾野拡大を推進するための基盤の強化）



69

（参考）

実施スケジュール （4. 利活用の裾野拡大を推進するための基盤の強化）



76

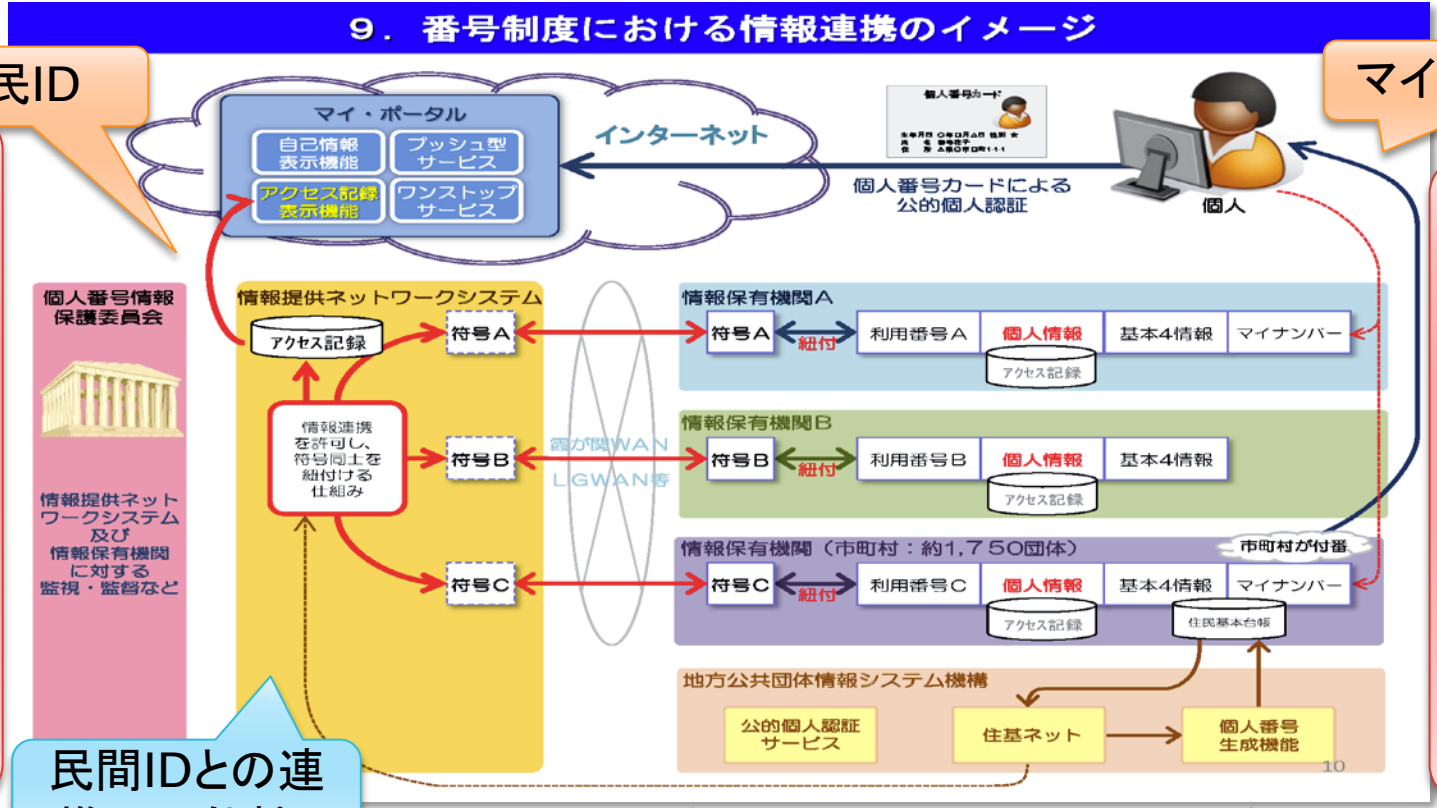
国民IDとマイナンバー

国民ID

行政サービスの利便性を向上させるための、紐付け等のために用いる「符号」と仕組み

マイナンバー

一人に一つの共通番号
盗用・漏洩のないように厳密に管理



民間IDとの連携の可能性?

出典：マイナンバー法案の概要とシステムについて（社会情報流通基盤研究センター）
Source: http://asist.ssr.titech.ac.jp/wp-content/uploads/2abe.pdf

まとめ

- トラストフレームワークプロバイダー (TFP)として
  大学にとってメリットを提供
  - まずはLoA 1から
  - LoA 2も視野に
- 民間におけるID連携の先行事例
- 属性プロバイダとしての大学の役割に向けて（島岡）
- NIIのプロジェクトから事業へ
  - 認証作業部会→学認運営委員会