



魅力的な学認

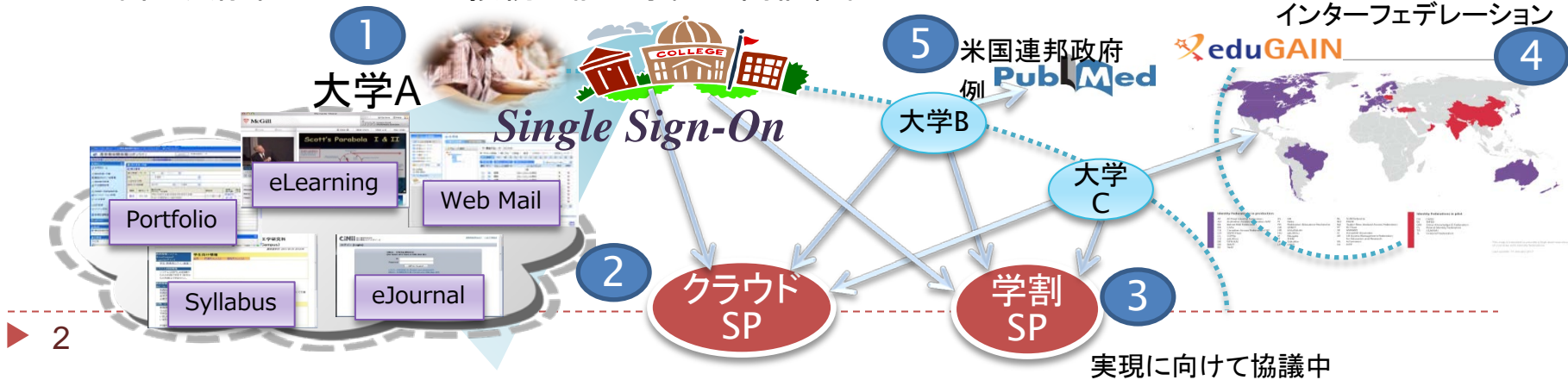
中村素典／国立情報学研究所

2013/9/11

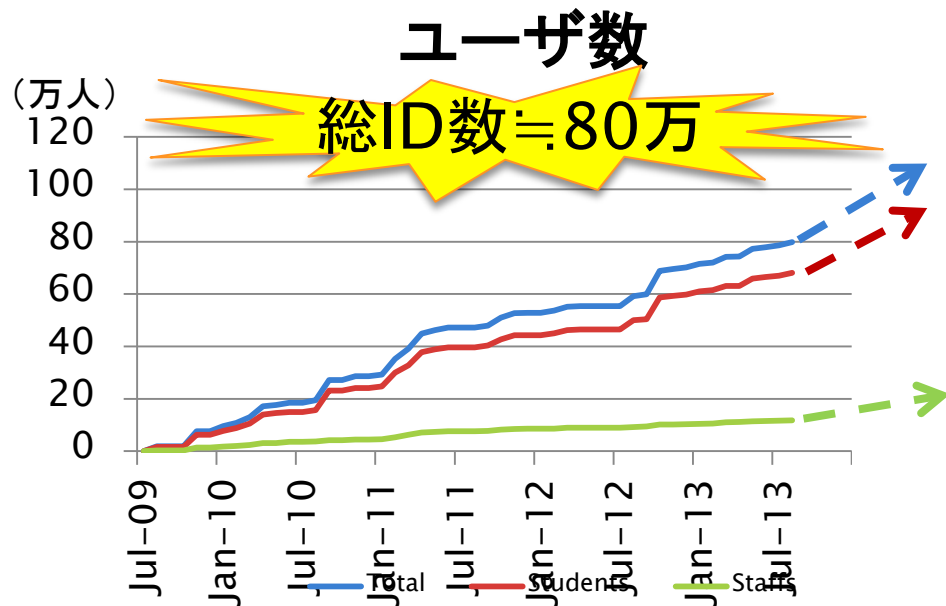
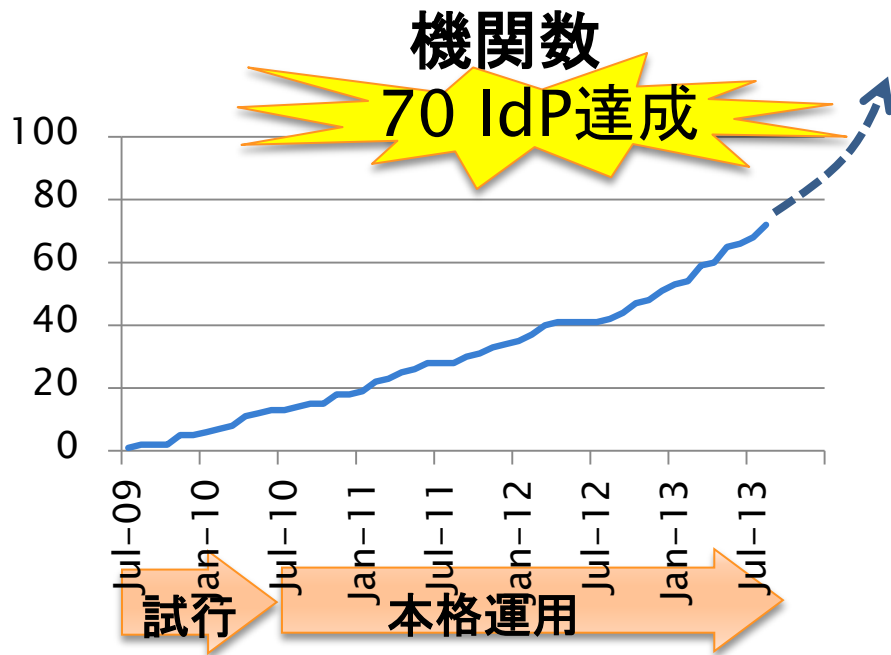


学術認証フェデレーション「学認」(2009～)

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

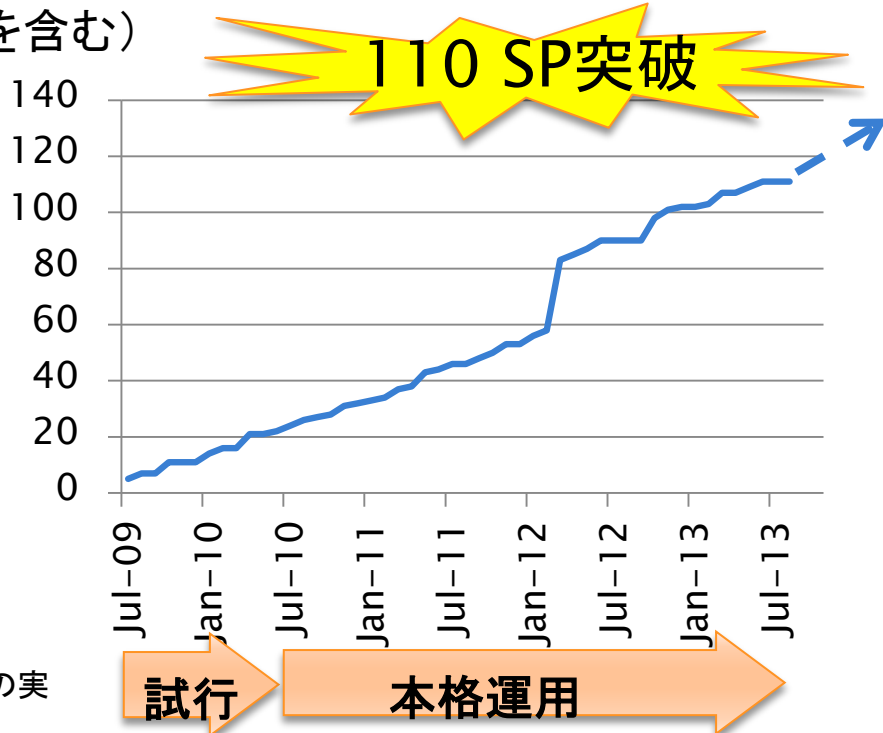
2013年9月1日現在

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

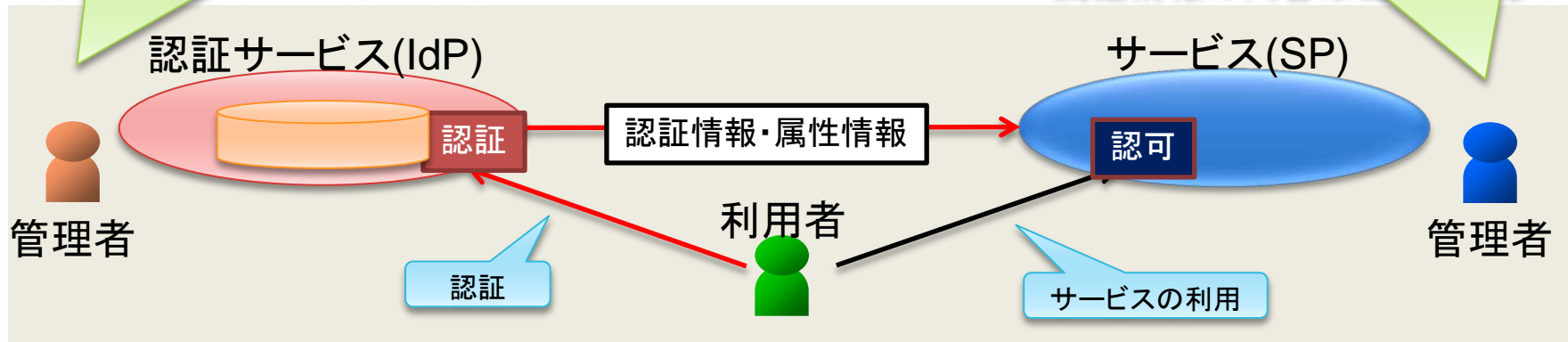


SSO技術の組織間利用での信頼

- ▶ 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

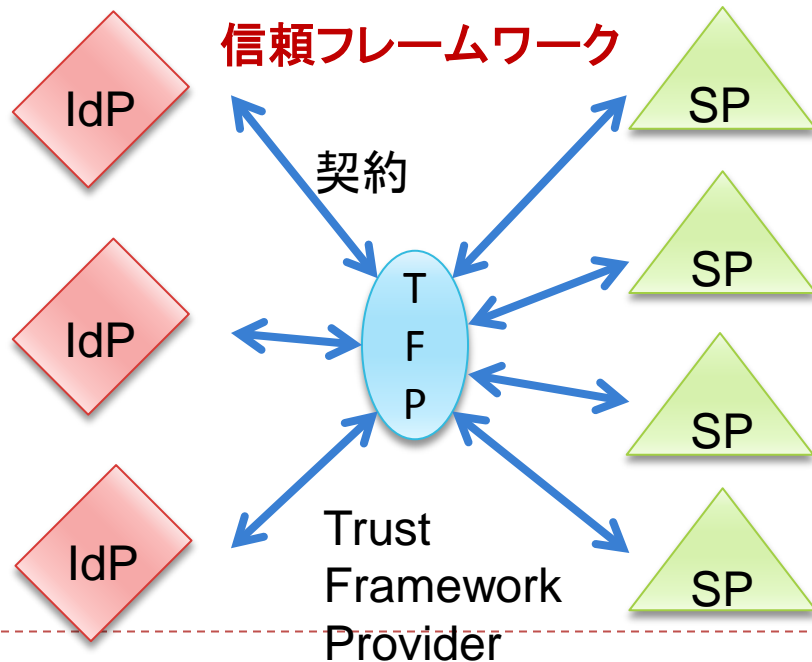
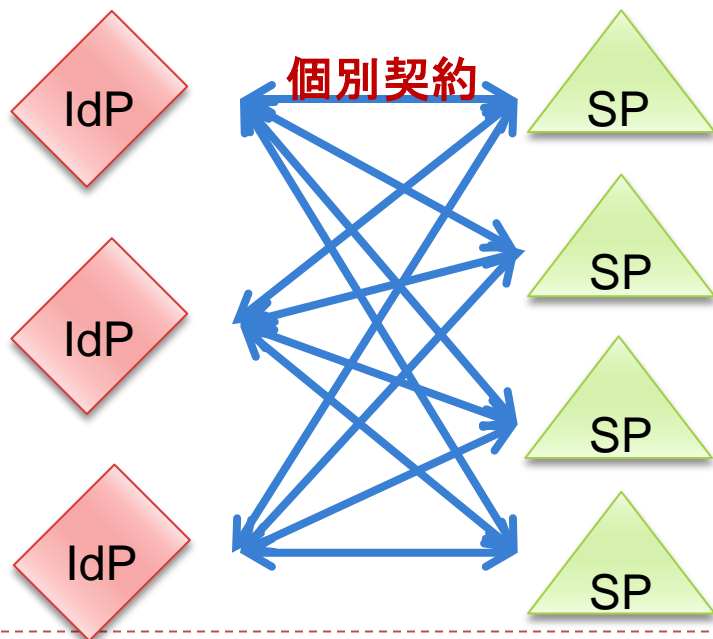
サービスは、利用者に関する情報を、目的外利用しないかな？

認証サービスは、変な利用者にサービスを不正に利用させたりしていないかな？
属性情報の内容は正しいかな？



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 $N \times M$ の関係が、 $N + M$ の関係に削減





GakuNin

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

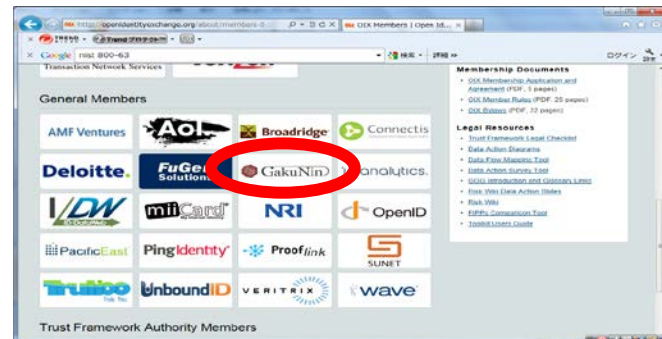


Level of Assurance (LoA)

- ▶ 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

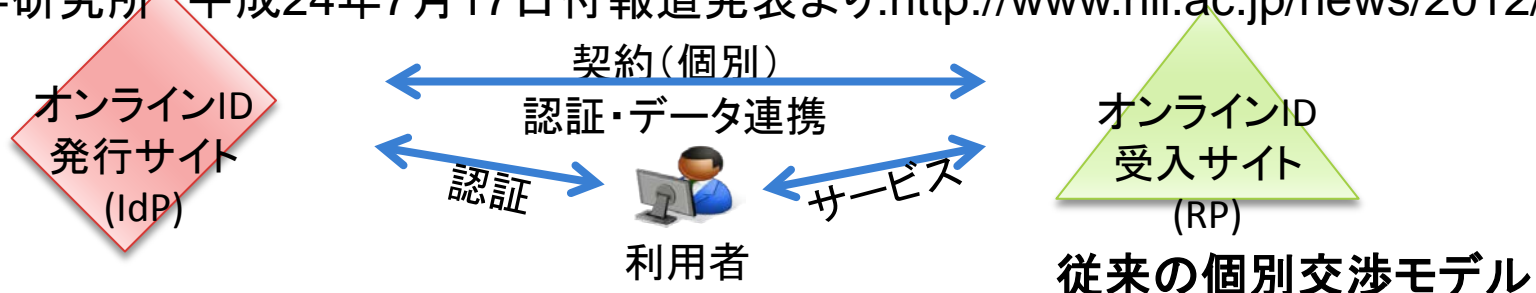




学認によるLoA1認定

- ▶ 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

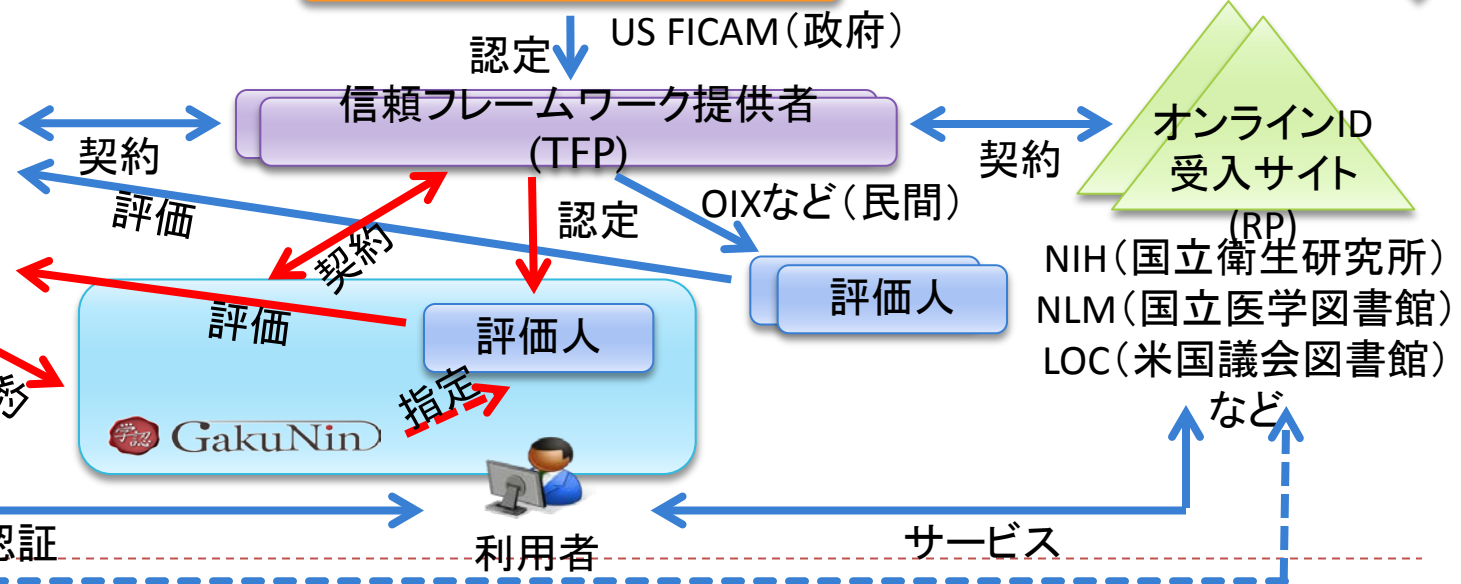


Google
PayPal
Equifax
VeriSign
Verizon



ポリシーメーカー

信頼フレームワークモデル



NIH (国立衛生研究所)
NLM (国立医学図書館)
LOC (米国議会図書館)
など

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(E) 編集(E) 表示(V) 履歴(S) ブックマーク(B) ツール(I) ヘルプ(H)

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

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

Copyright © KAHOKU SHIMPO PUBLISHING CO.



OIXのLoA 1リスティング

▶ 山形大学

▶ 7番目

OIX Certified Providers | Open Identity Exchange - Mozilla Firefox

openidentityexchange.org/certified-providers

OIX Certified Providers

U.S. ICAM LOA 1 Certified Identity Providers

The following OIX members are certified as identity providers for the [US ICAM trust framework](#):

Identity Provider	ICAM Profile	Listing Date	URI
Yamagata University	SAML 2.0	2013-08-01	http://yamagata-u.ac.jp/
Google	OpenID 2.0	2011-03-13	http://google.com
Equifax	IMI 1.0	2010-03-03	http://equifax.com
PayPal	OpenID 2.0	2010-03-03	http://paypal.com
PayPal	IMI 1.0	2010-03-03	http://paypal.com
VeriSign	OpenID 2.0	2010-03-29	http://pip.verisignlabs.com
Wave Systems	OpenID 2.0	2010-12-09	http://wave.com

US ICAM LOA 1, 2 and non-crypto 3 Certified Identity Providers

The following OIX members are certified as identity providers for the [US ICAM trust framework](#):

Identity Provider	ICAM Profile	Listing Date	URI
Verizon	SAML 2.0	2011-10-28	http://verizonbusiness.com/us/

US ICAM LOA 1 Listed Assessors

The following OIX members are listed assessors for the US ICAM LOA 1 trust framework:

- Peter Altman
- Professor Hiroyuki Sato**

Trust Frameworks

- [What is a Trust Framework?](#)
- [Creating a New Trust Framework](#)
- [OIX Trust Frameworks](#)
- [U.S. Government ICAM](#)
- [U.S. ICAM OIX-Certified Providers](#)
 - [Certification Process](#)
- [Telcom Data Trust Framework](#)
- [APA Publish Trust Framework](#)
- [Respect Trust Framework](#)
- [Mvdx Trust Framework](#)
- [OIX Listing Service](#)

OIX Newsletter Sign Up

Email Address



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

Approved Trust Framework Providers | IDManagement.gov - Mozilla Firefox

www.idmanagement.gov/approved-trust-framework-providers

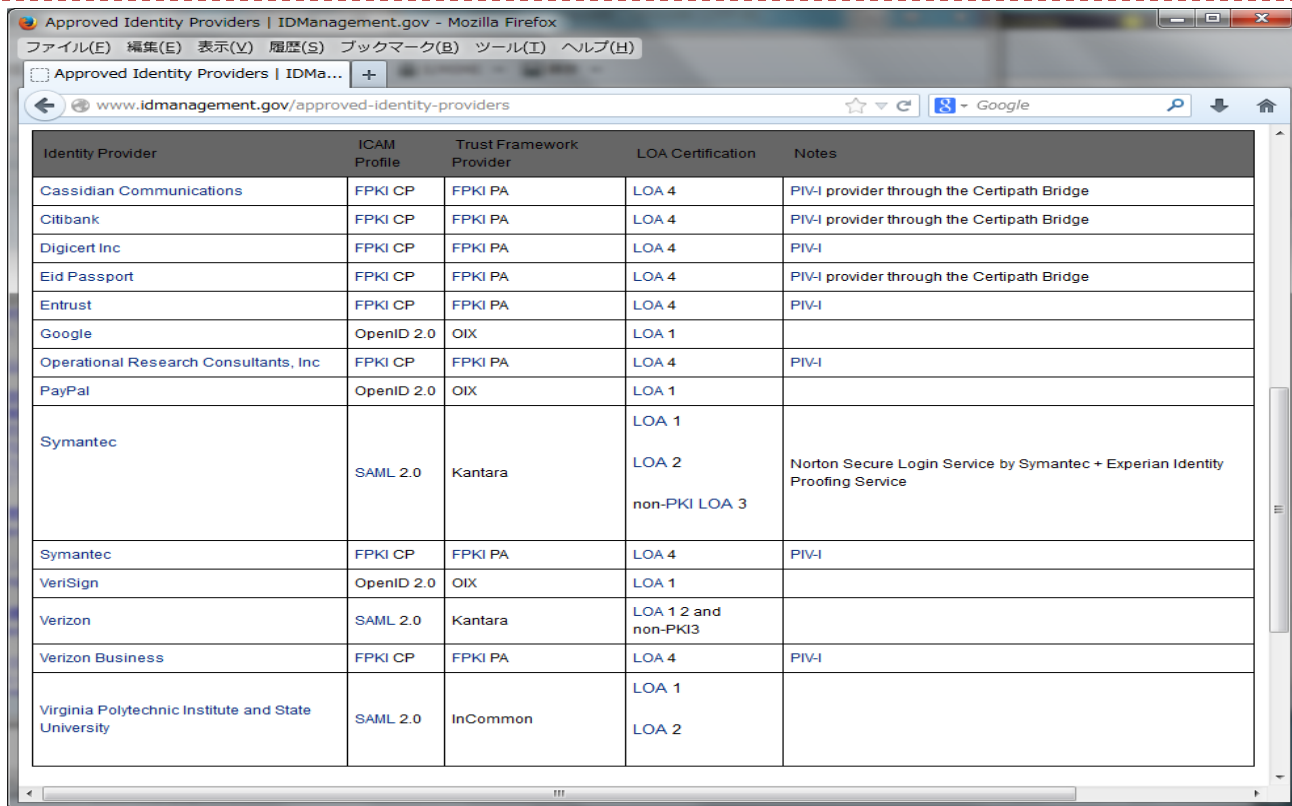
APPROVED TRUST FRAMEWORK PROVIDERS

ICAM has assessed the efficacy of the Trust Frameworks of the following Industry organizations to determine if they are comparable to federal standards of security and privacy.

If approved by ICAM, credentials issued by Identity Providers who are assessed against these Approved Trust Frameworks by their respective Trust Framework Provider (TFP) can be trusted and used by federal Relying Parties (RPs) at a known level of assurance (LOA) comparable to one of the four OMB Levels of Assurance.

TFP Name:	InCommon
Status:	Approved*
POC:	John Krienke (admin@incommon.org)
Supported LOA:	Bronze (LOA1) and Silver (LOA2)
TFP Name:	Kantara
Status:	Approved*
POC:	Joni Brennan (joni@ieee-isto.org)
Supported LOA:	LOA1, LOA2 and non-PKI LOA3
TFP Name:	OIX
Status:	Approved*
POC:	Don Thibeau (don.thibeau@openidentityexchange.org)
Supported LOA:	LOA1 http://openidentityexchange.org/certified-providers
TFP Name:	Safe/BioPharma
Status:	Approved*
POC:	Peter Alterman (palterman@safe-biopharma.org)
Supported LOA:	LOA1, LOA2 and non-PKI LOA3

FICAMの認定IdPリスティング

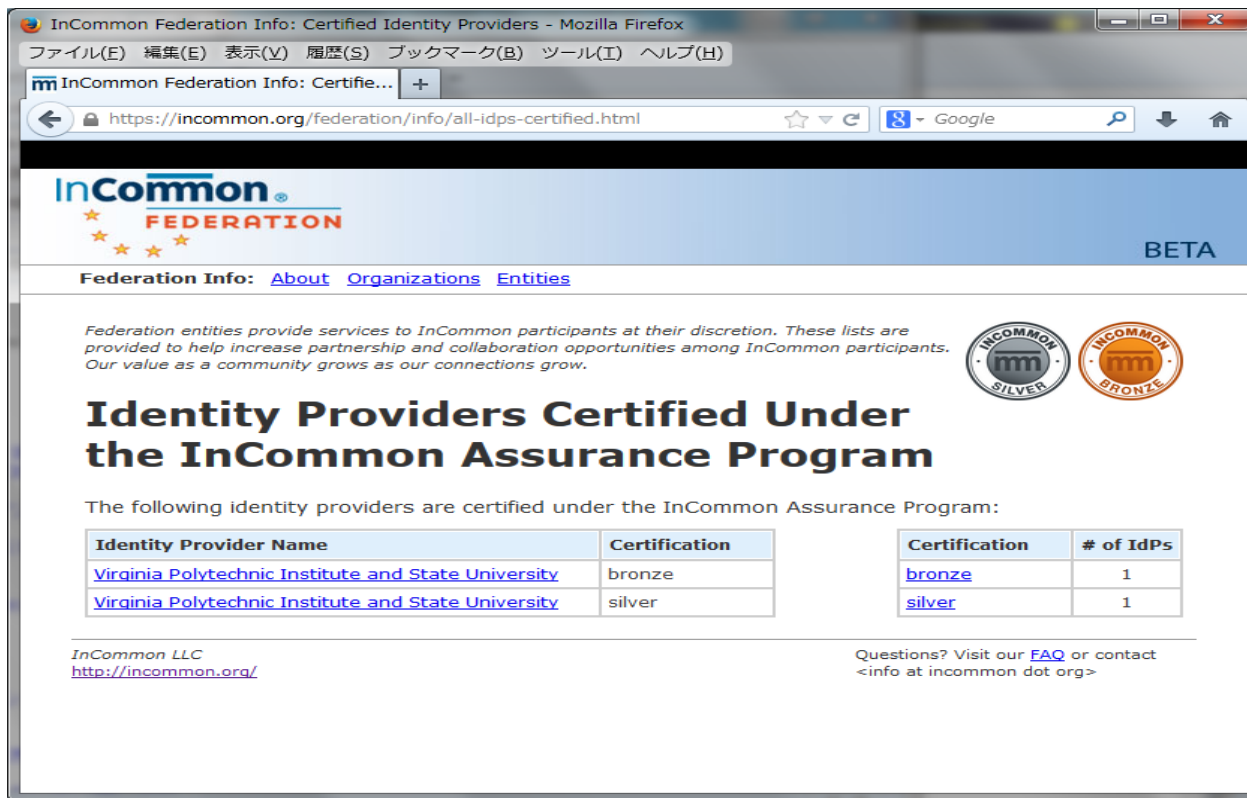


Approved Identity Providers | IDManagement.gov - Mozilla Firefox

www.idmanagement.gov/approved-identity-providers

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



InCommon Federation Info: Certified Identity Providers - Mozilla Firefox
 ファイル(E) 編集(E) 表示(V) 履歴(S) ブックマーク(B) ツール(I) ヘルプ(H)

InCommon Federation Info: Certifie... +

https://incommon.org/federation/info/all-idps-certified.html

InCommon
 FEDERATION

BETA

Federation Info: [About](#) [Organizations](#) [Entities](#)

Federation entities provide services to InCommon participants at their discretion. These lists are provided to help increase partnership and collaboration opportunities among InCommon participants. Our value as a community grows as our connections grow.

Identity Providers Certified Under the InCommon Assurance Program

The following identity providers are certified under the InCommon Assurance Program:

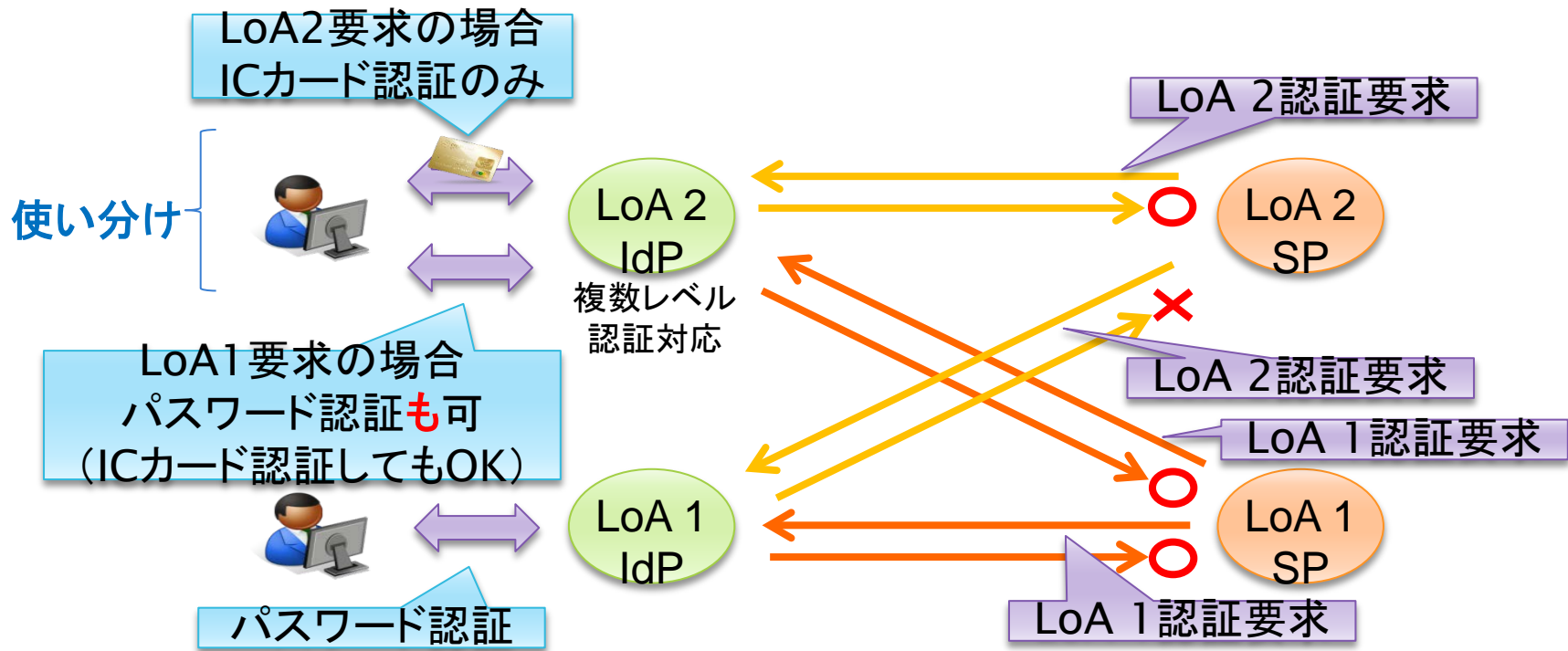
Identity Provider Name	Certification
Virginia Polytechnic Institute and State University	bronze
Virginia Polytechnic Institute and State University	silver

Certification	# of IdPs
bronze	1
silver	1

InCommon LLC
<http://incommon.org/>

Questions? Visit our [FAQ](#) or contact <info at incommon dot org>

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)

年度	短期			中期			長期			KPI
	2013年	2014年	2015年	2016年	2017年	2018年	2019年	2020年	2021年	
	<p>経産省 本人確認をした属性情報を用いた社会基盤構築に関する検討委員会・調査研究など</p>									<p>・ID連携トラストフレームワークの認定状況</p> <p>・ID連携トラストフレームワークのサイト利用状況</p>
	<p>ID連携トラストフレームワークの整備</p> <p>ルールや認定制度等の検討及びサンプル実証【経済産業省】</p>			<p>適する社会システムやサービスの検討及び制度運用開始【経済産業省】</p>			<p>民間におけるID連携トラストフレームワークの普及・推進【経済産業省】</p>			
	<p>総務省 パーソナルデータの利用・流通に関する研究会など</p>									
	<p>プライバシーの保護とパーソナルデータの利活用を両立できるトラストフレームワークの構築に向け、国際的な協調も視野にプライバシー保護に配慮したID連携の実証、標準化、普及啓発等の推進【総務省】</p>									

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)

年度	短期			中期		長期			KPI	
	2013年	2014年	2015年	2016年	2017年	2018年	2019年	2020年		2021年
③ 国際的にも通用リードする実践的な高度なIT人材の育成 (1) 人材育成教育	世界に通用する新しいものづくり人材等の育成・環境の検討【総務省、文科省、経産省】		世界に通用する新しいものづくり人材等の育成・環境の実験的導入・検証【総務省、文科省、経産省】		世界に通用する新しいものづくり人材等の育成・環境の整備・先端化【総務省、文科省、経産省】					・実践的な専門教育プログラムの提供数、修了者数
	実践的IT人材の継続的な育成の仕組み、企業との連携を含めた設計／自走化【総務省、文科省、経産省】			実践的IT人材育成の仕組み、全国的な実践教育ネットワークの継続的運用【総務省、文科省、経産省】						
	全国的な実践教育ネットワークの推進、専門教育プログラム等の構築【文科省、経産省】			小・中学校でのプログラミング等のIT教育の充実【総務省、文科省】			IT教育の全国展開【総務省、文科省】			
	IT教育の検証と改善【総務省、文科省】									
	遠隔教育等の推進に向けた環境整備【文科省】			遠隔教育等の推進【文科省】						
	遠隔教育等IT利活用の課題検証、試行【文科省】									
	企業における人材育成基盤整備【経産省】									
	起業意識を醸成するイベント等の企画・設計【総務省、経産省】			突出したIT人材の発掘、マッチング、継続したイベント等の実施によるハイレベルIT人材の発掘、支援【総務省、経産省】						
	突出したIT人材のコミュニティ構築【総務省、経産省】									
	企業人のIT基礎知識の向上に向けた取組【経産省】									
各分野スキルセットの検討【経産省】			スキル標準の整備・検討【経産省】			CIO補佐官の採用、専門人材の募集や登用条件としての活用【経産省】				
職種転換を含めた就業支援など、ITを活用した人材シフトの支援のための仕組みの課題整理・検討【厚労省、経産省】			ハローワークの機能強化を含めた、人材シフト支援のための仕組みの設計や試行など、就業支援や職種転換のための環境整備【厚労省、経産省】							

(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)

年度	短期			中期			長期			KPI
	2013年	2014年	2015年	2016年	2017年	2018年	2019年	2020年	2021年	
(2) 世界最高水準のITインフラ環境の確保	沖縄県での海底光ケーブル等の整備【内閣府】			離島・過疎地等の条件不利地域での超高速ブロードバンド基盤の整備【内閣府、総務省】						・超高速ブロードバンド基盤・ゼロ自治体数
	超高速ブロードバンド基盤の整備に向け、地域の実情に応じて関係団体との協議の場を設置【総務省】			各協議会において整備方針等の決定【総務省】						
	第4世代移動通信システム技術導入に向けた整備【総務省】			新たな周波数帯の割当【総務省】			第4世代移動通信システムの導入、促進【総務省】			・商用サービス等の伝送速度
	ワイヤレスネットワークに係る地域間の情報格差解消に向けた今後の制度の在り方について検討【総務省】			ワイヤレスネットワークに係る地域間の情報格差解消の取組【総務省】						
	基地局連携技術等の研究開発の推進【総務省】			次世代移動通信システムの多彩なニーズに対応するための研究開発を推進【総務省】			周波数の高度利用等を可能とする研究開発の推進【総務省】			
	高速な衛星通信を可能とする技術、機器の小型・省電力化等の研究開発の実施【総務省】			安全確保や海上における資源探査等に資する衛星ブロードバンドの研究開発の推進【総務省】						
	世界最高レベルの光通信技術やネットワーク仮想化技術の実用化を推進【総務省】			事業者間の公正な競争条件の確保等の競争政策の推進【総務省】						・テストベッド利用者数
	大学等のクラウド環境構築やスーパーコンピュータの利用等に不可欠な学術情報ネットワーク(SINET)の整備及び一層の機能の高度化や連携強化の取組の検討【文部科学省】			大学等のクラウド環境構築やスーパーコンピュータの利用等に不可欠な学術情報ネットワーク(SINET)の整備及び一層の機能の高度化や連携強化の取組の推進【文部科学省】						
	データセンター・IXの地域分散化の検討・推進【総務省、経済産業省】			データセンター・IXの地域分散化・活性化に向けた取組の実施【総務省、経済産業省】						・データセンターの地域分散化・活性化について事業者への周知・啓発活動の実施回数
	企業の長期的競争力獲得に向けたインターネットやIT関連の投資等を促進する環境整備(既存の税制措置の活用を促しつつ、必要に応じて更なる支援措置について検討)【総務省、経済産業省】									・インターネット・IT関連投資額
次世代IP環境の推進			調達仕様モデル、情報セキュリティガイドラインの整備【総務省】			情報システムのIPv6対応の周知・啓発活動の実施【総務省】			・普及啓発活動の実施回数	

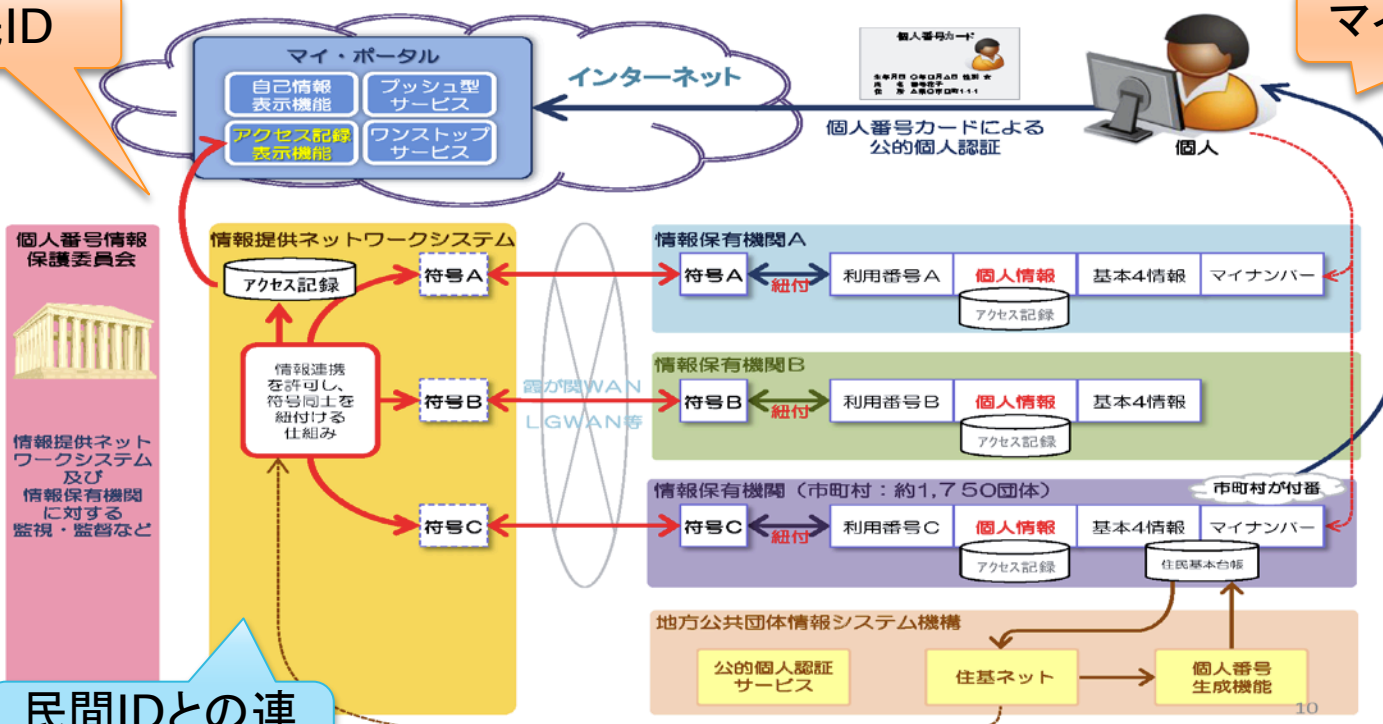
国民IDとマイナンバー

9. 番号制度における情報連携のイメージ

国民ID

マイナンバー

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



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?



まとめ

GakuNin

- ▶ 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