

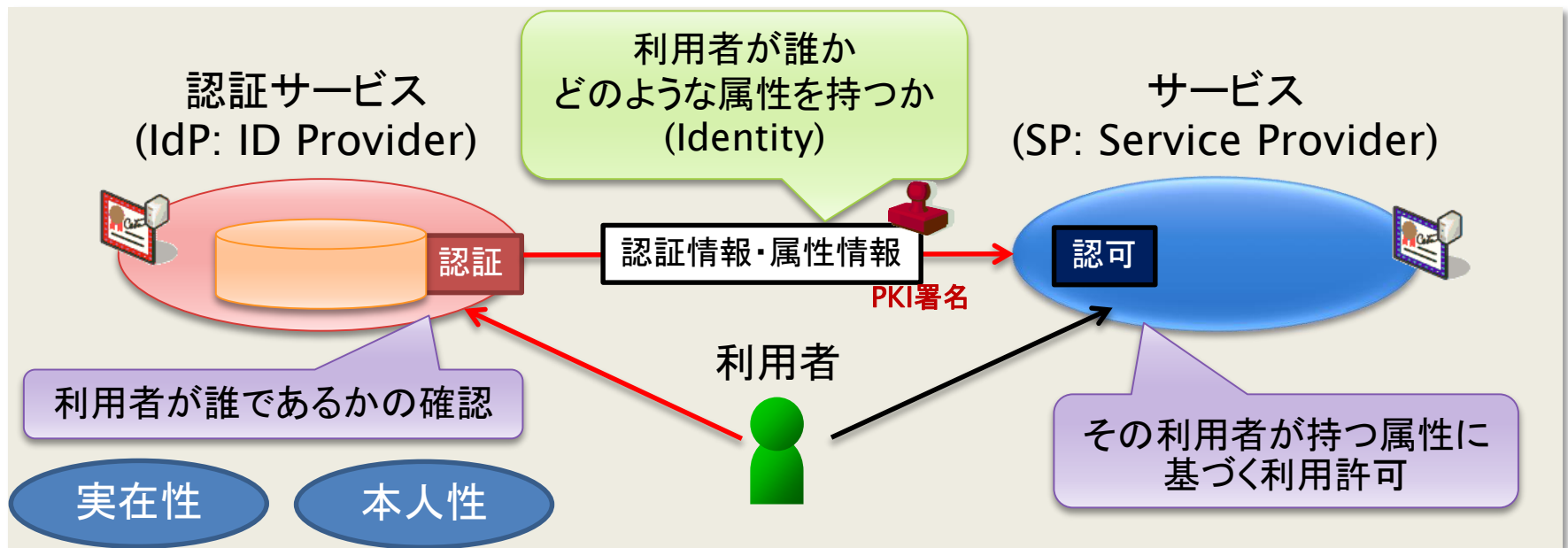


LoA 1 認定プログラム

中村素典 / 国立情報学研究所

ID連携の基礎となる認証と認可の分離

- ▶ 認証
 - ▶ 利用者が誰であるかの確認
- ▶ 認可
 - ▶ その利用者が持つ権限に対応した利用許可

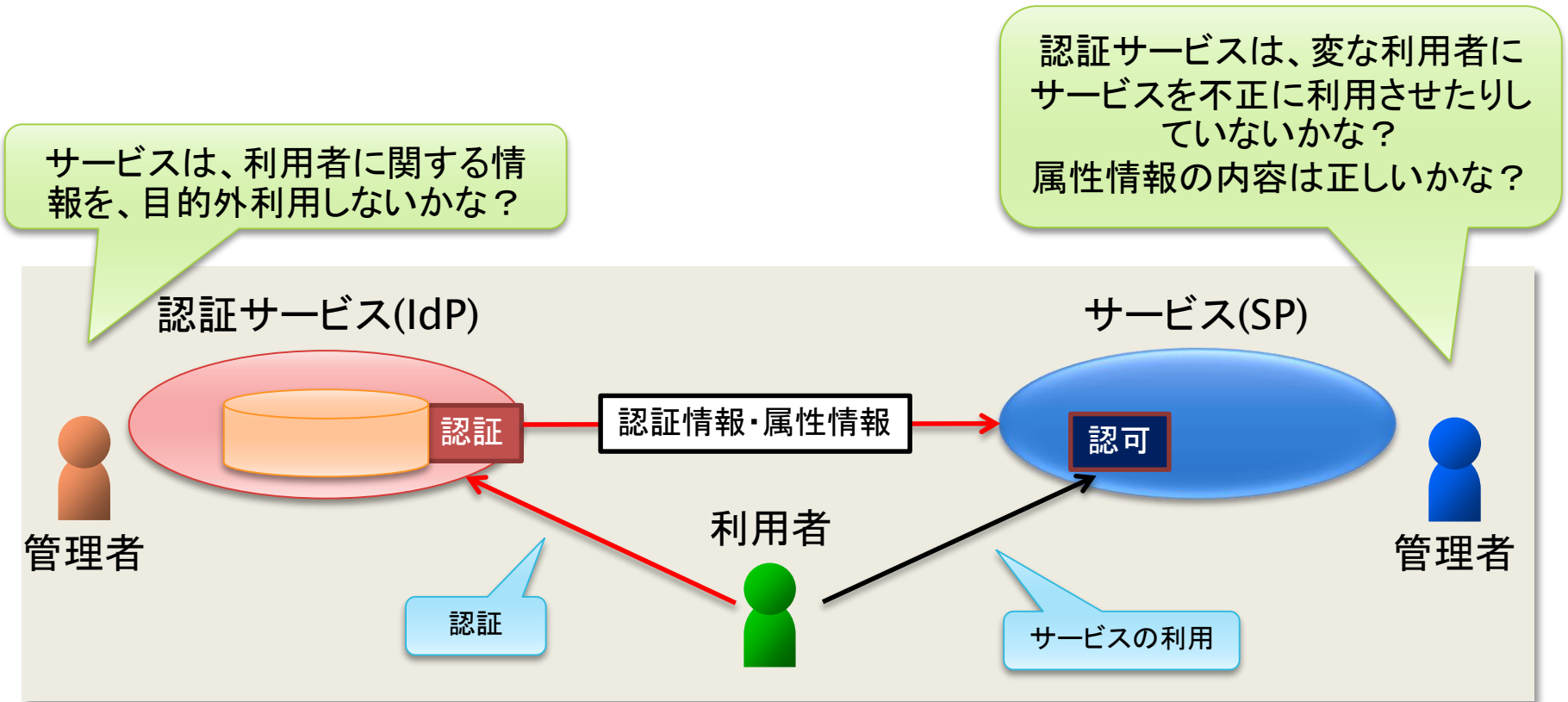


「認証」「認可」分離のメリット

- ▶ クレデンシャルの一元(集中)管理
 - ▶ セキュリティレベルの統一が容易
- ▶ クレデンシャルの入力先の一元化
 - ▶ 高度な認証技術の導入が容易
- ▶ シングルサインオンへの応用
 - ▶ SSOは主目的ではない(再認証を求める運用も可能)
- ▶ 「ID」(識別子)と「属性」の分離
 - ▶ 仮名認証が可能
 - ▶ 学生のみ、教員のみがアクセス可能なサービス
 - ▶ グループアクセスのための認証
 - ▶ グループ情報の提供により共有パスワードが不要

SSO技術の組織間利用での信頼

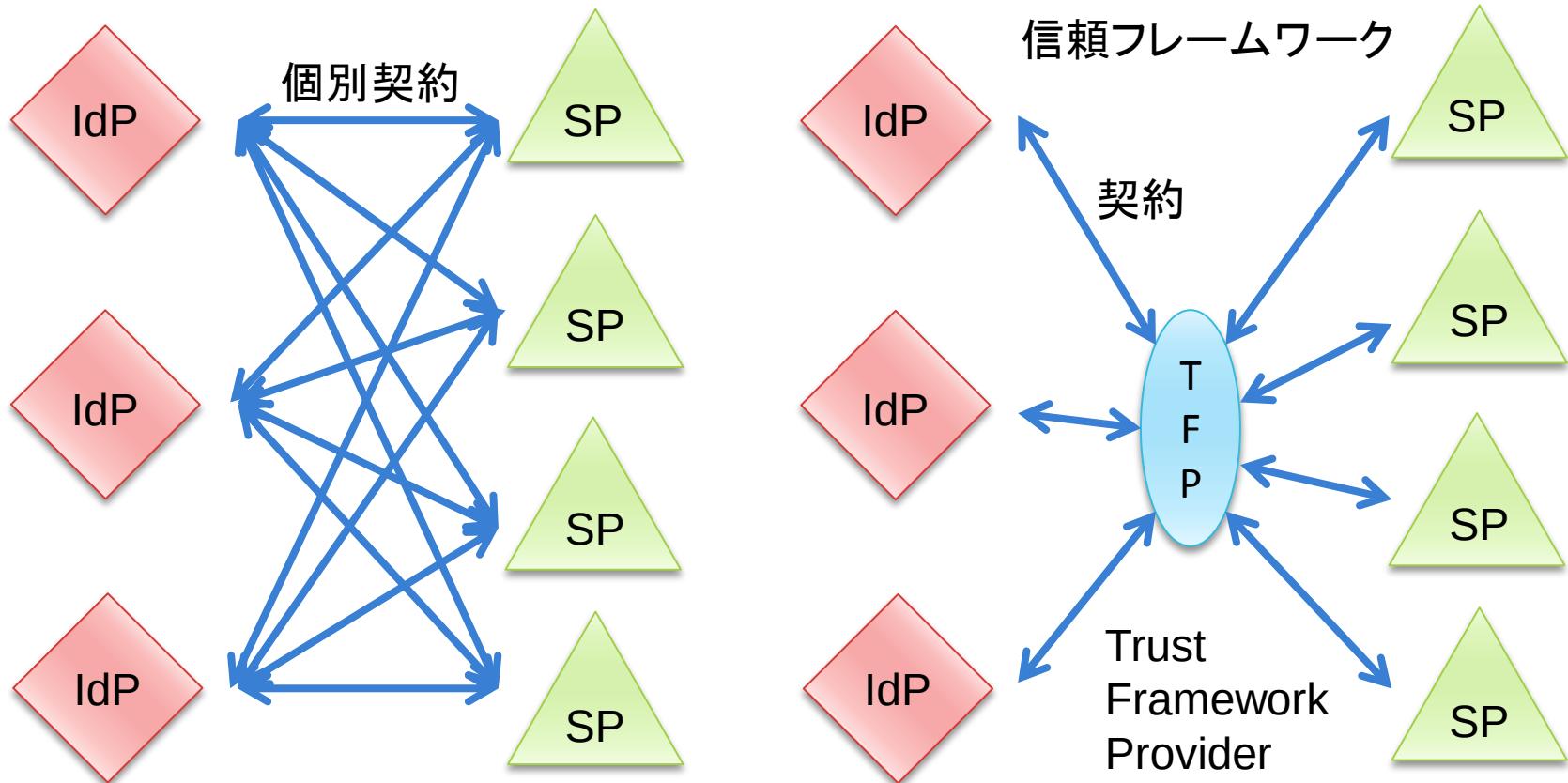
- ▶ 異なる組織が個別に管理するため、相互の信頼が重要



- ▶ 信頼のための共通の枠組み(トラストフレームワーク)が必要
 - ▶ 運用レベルの統一

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



学認で扱う属性情報 (IdPからSPへ送出)

属性	内容
OrganizationName (o)	組織名
jaOrganizationName (jao)	組織名 (日本語)
OrganizationalUnit (ou)	組織内所属名称
jaOrganizationalUnit (jaou)	組織内所属名称 (日本語)
eduPersonPrincipalName (eppn)	フェデレーション内の共通識別子
eduPersonTargetedID	フェデレーション内の 仮名 識別子
eduPersonAffiliation	職種
eduPersonScopedAffiliation	職種 (@scopeつき)
eduPersonEntitlement	資格
SurName (sn)	氏名 (姓)
jaSurName (jasn)	氏名 (姓) (日本語)
GivenName	氏名 (名)
jaGivenName	氏名 (名) (日本語)
displayName	氏名 (表示名)
jaDisplayName	氏名 (表示名) (日本語)
mail	メールアドレス
gakuninScopedPersonalUniqueCode	学生・職員番号 (@scopeつき)

実際に使われる属性情報の例

サービスA (1項目必須)

eduPersonPrincipalName(必須)

サービスB (1項目必須)

eduPersonAffiliation (必須)
eduPersonTargetedID

サービスC (必須項目なし)

eduPersonEntitlement
eduPersonAffiliation

必要最低限のみを送出

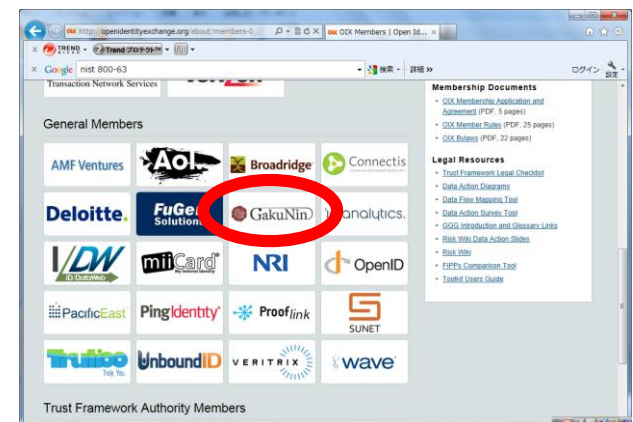
(参考) <https://meatwiki.nii.ac.jp/confluence/x/1oS5>

PubMedへのアクセスと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
 - ▶ かつ、要求された属性のみを送出することの保証を要求
(Privacy Impact Assessment (PIA), E-Government Act of 2002)
- ▶ 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)



- ▶ 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





GakuNin

LoA: Level of Assurance (4つのレベル)

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, 2013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



世界標準へ

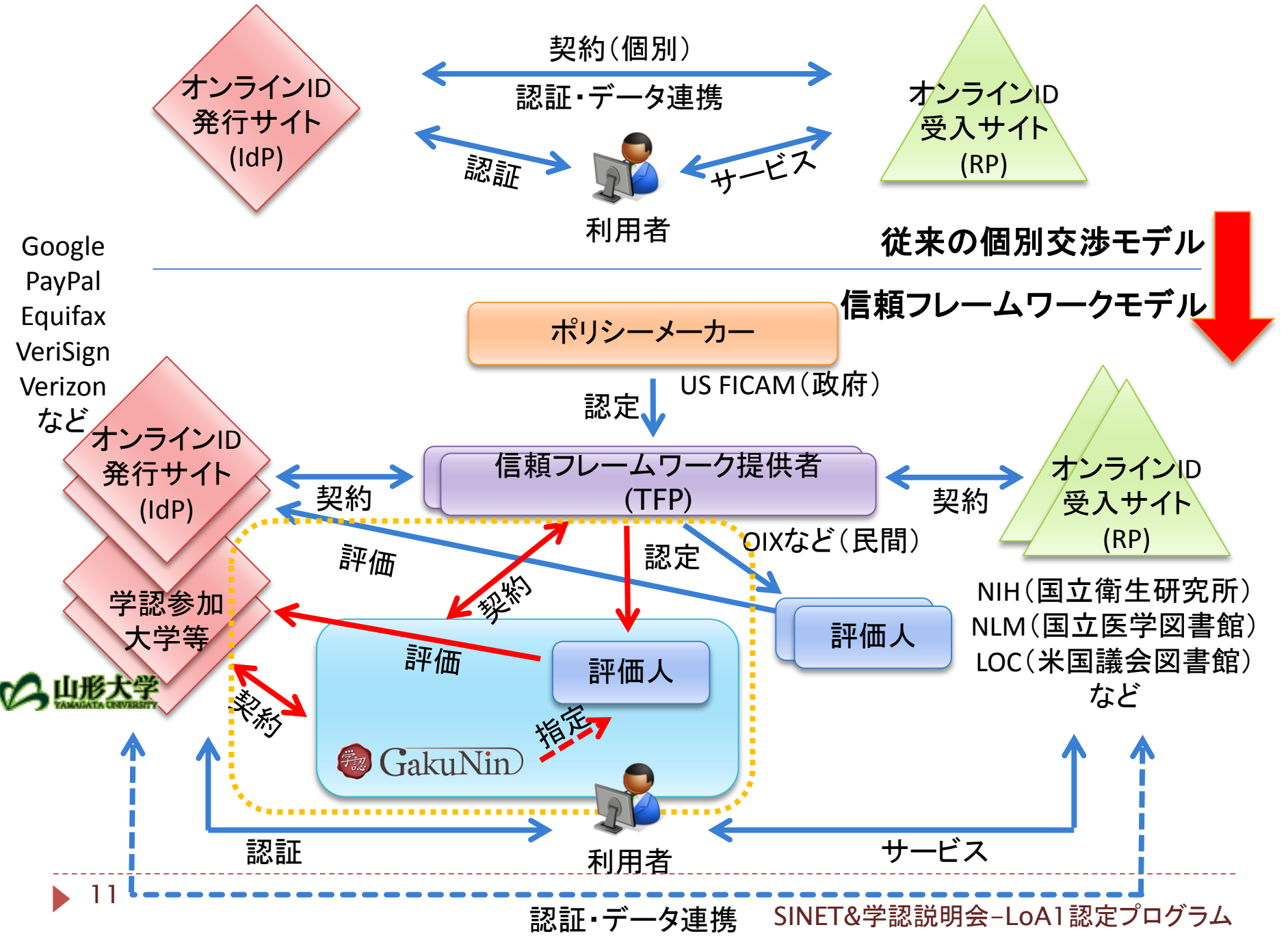
Level	Description
1 – Low	Little or no confidence in the asserted identity 身元確認不要、仮名(ユーザの同一性保証)、有効期限なし 例: whitehouse.govのWebサイトでのオンラインディスカッションに参加
2 – Medium	Some confidence in the asserted identity 身元識別(身分証明書)、単一要素認証、失効処理、平文PW保持 × 例: 社会保障Webサイトを通じて自身の住所記録を変更
3 – High	High confidence in the asserted identity 多要素認証 (ソフトトークン可) 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、認証後の暗号化の強化 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

認証におけるリスクに基づく指標

- ▶ 利用者の同一性、身元確認の確からしさ
 - ▶ ID/パスワード等を確実に本人に渡しているか
- ▶ 属性情報の確からしさ
 - ▶ 身分の変更や退職・卒業などへの対応
- ▶ 認証メカニズムの強度
 - ▶ 盗聴、リプレイ、辞書攻撃などに対する耐性
- ▶ アサーションメカニズムの強度
 - ▶ IdPの成りすまし等に対する耐性

学認によるLoA-1 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
 - ▶ LoA-1なので、アカウント発行プロセスがポイント
- ▶ 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)



山形大学をFICAM LoA 1 認定

▶ 2013/8/1付

2012/10頃: 申請の相談

⇒ **プレ審査**をやることに

2012/11頃: 学内文書の開示

2012/12頃: ヒアリング

2013/1頃: 不足文書の作成

工数: 計30時間・人

2013/1末: 正式に申請(英語)

最初の事例として、申請の進め方を

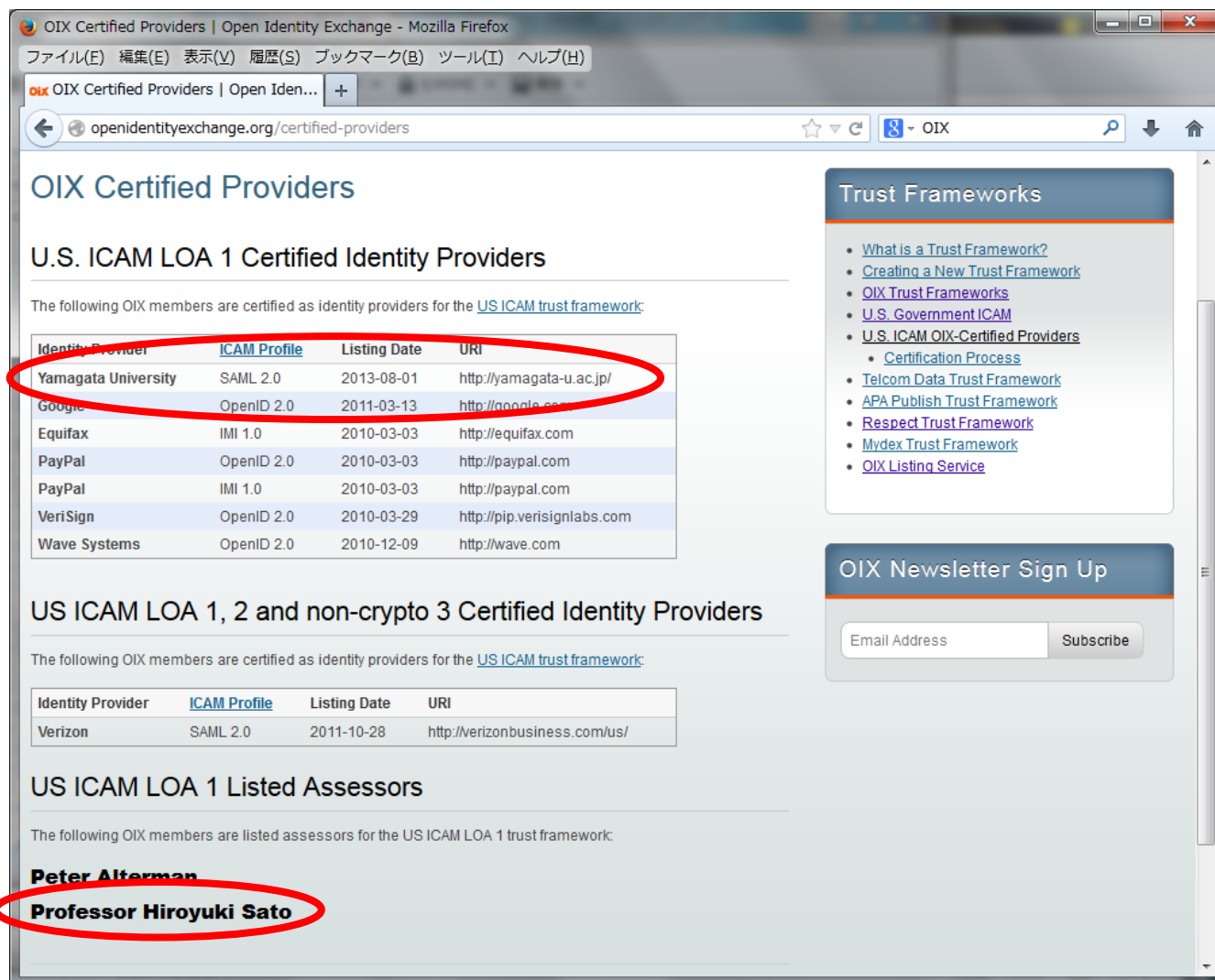
OIXと協議

2013/7頃: OIXに最終評価レポート提出



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

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)

OIX OIX Certified Providers | Open Iden... +

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 Alterman

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](#)
- [Mydex 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

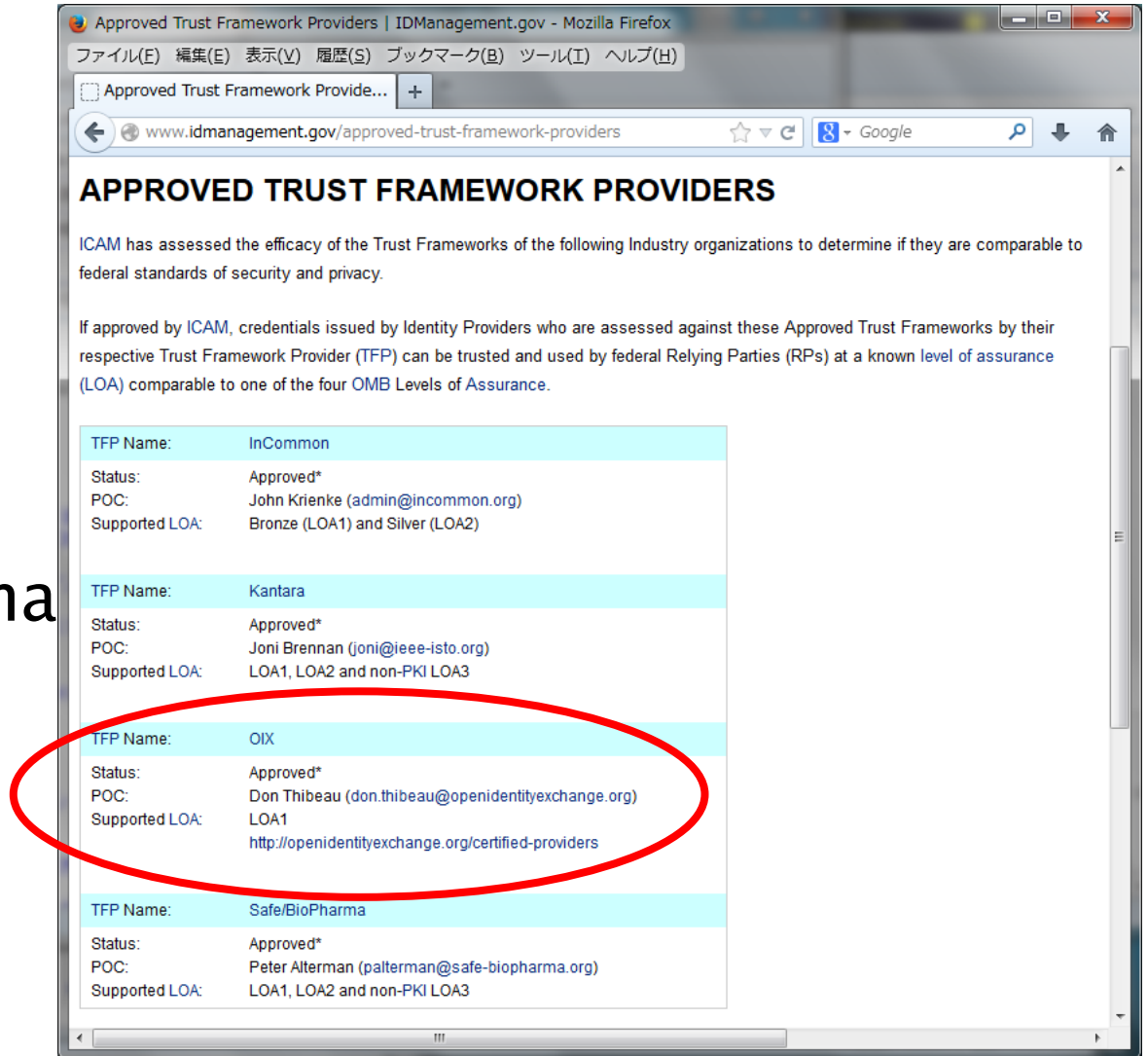
▶ 1

▶ Safe/BioPharma

▶ 1,2,non-PKI 3

▶ FPKI PA

▶ 4



APPROVED TRUST FRAMEWORK PROVIDERS	
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 Thibeaudeau (don.thibeaudeau@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

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)

Approved Identity Providers | IDMa... +

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	Norton Secure Login Service by Symantec + Experian Identity Proofing Service
			LOA 2	
			non-PKI LOA 3	
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	InCommonによる認定
			LOA 2	

LoA 1 取得の事務的な流れ

- ▶ 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
- ▶ 申請先
 - ▶ oix-loa1@nii.ac.jp
 - ▶ 最初のコンタクト時は、書類の提出等は不要
 - ▶ 相談窓口もここ
- ▶ 学認の「トラスト作業部会」が作業をします
- ▶ 作業の結果は「学認指定OIX LoA1 指定Assessor」がOIXに報告します
- ▶ OIXは理事会の決定としてLoA1を認定します

申請 / 審査に入る前に

- ▶ 以下のことが満たされているか事前チェックしてください
 - ▶ 学認の運用フェデレーションに参加し、「安定」してIdPを運用していること
 - ▶ 学認の各種規程を遵守している
 - ▶ ある程度の規模で、ある程度以上の期間、問題なく運用が継続している
 - ▶ 毎年行われる「学認アンケート」に誠実に回答していること
 - ▶ アンケートの回答もチェック対象です
 - ▶ 回答例の丸写し、運用レベルが判断できないような短すぎる回答等は審査の時にチェックされるでしょう



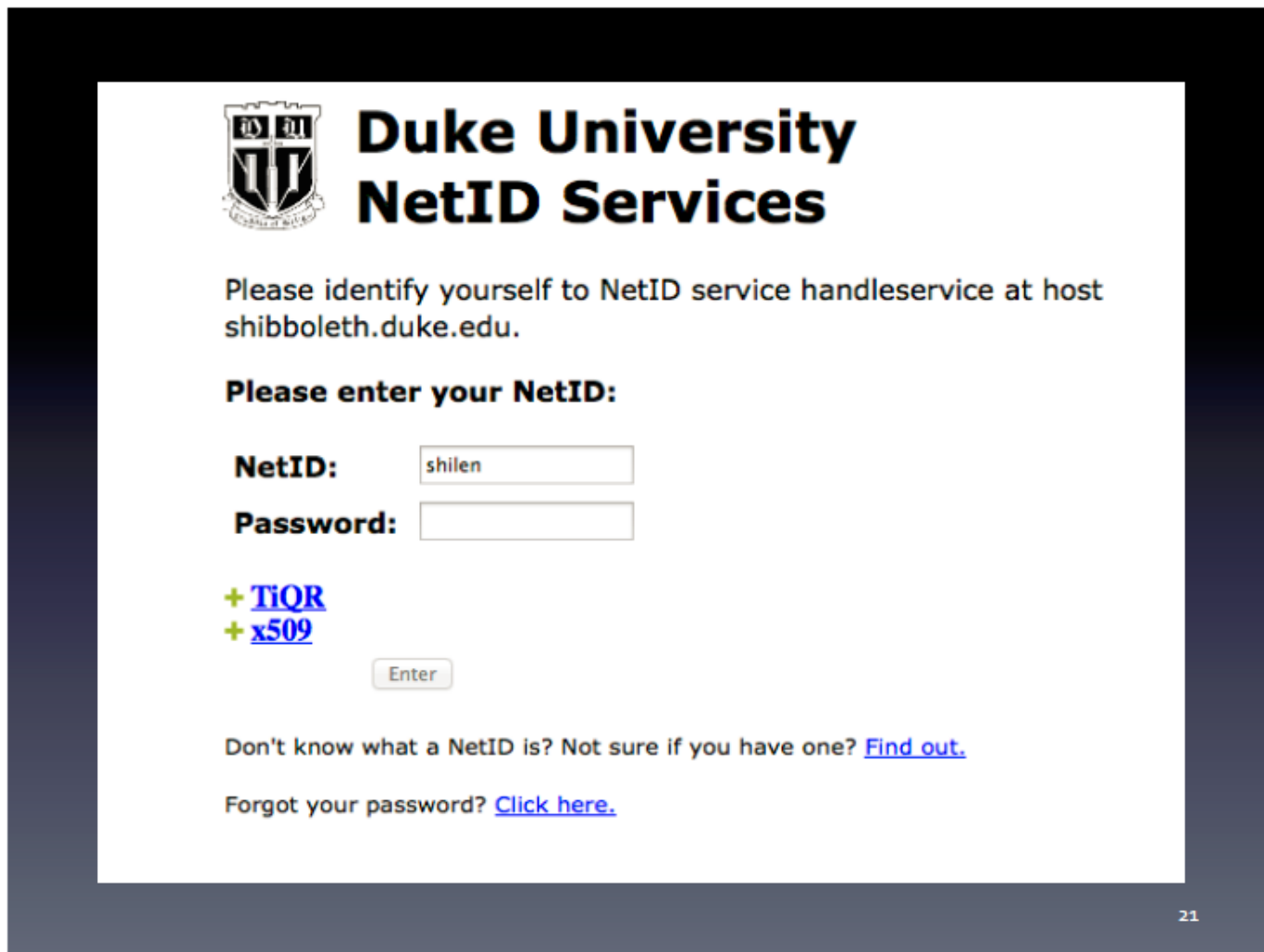
注意点

- ▶ Governanceにおいて、
 - ▶ 規程類が死蔵されていないか？
 - ▶ 現場権力を抑える規程がeffectiveか？
- ▶ Privacyにおいて、
 - ▶ 独立行政法人等の場合は法によってOpt-Inが強制されているが、それ以外の場合は学内での規程の整備等が必要
 - ▶ uApprove等を導入しましょう
- ▶ Technicalにおいて、
 - ▶ NIST SP800-63には一度目を通しておくべき
 - ▶ 2006年版はIPAの和訳がある。2011年版、2013年版の和訳はまだ。
 - ▶ 基本は上記文書のこの文章に集約される
 - ▶ the authentication mechanism provides some assurance that the **same** claimant is accessing the protected transaction or data

LoA-1 認定を越えて

- ▶ 大学のIdP運用はLoA-1を十分満たしているはず
 - ▶ 学認システム運用基準では、アカウント廃止等も規定
- ▶ 米国認証フェデレーションInCommonにおける認定
 - ▶ ブロンズ: LoA-1相当
 - ▶ シルバー: LoA-2相当
 - ▶ National Student Clearinghouse for financial aid
 - ▶ CILogon access to CI services such as Open Science Grid.
 - ▶ Research Virtual Organizations such as LIGO.
 - ▶ Federal grant submission programs.
 - ▶ Department of Education.
- ▶ 国内でより高度な保証レベルを要求するサービス例
 - ▶ e-Rad?
 - ▶ HPCI?
 - ▶ 学割サービス?
- ▶ 今後のサービス拡大には、LoA-1では不足、かといってLoA-2は少し過大
 - ▶ LoA-1.5? LoA-1.9?

Duke Universityでの多要素認証事例



The screenshot shows the Duke University NetID Services login interface. It includes the Duke University crest and logo, a request to identify oneself to the NetID service at shibboleth.duke.edu, and a form for entering the NetID and password. The NetID field contains the text 'shilen'. Below the password field, there are two links: '+ TiQR' and '+ x509'. An 'Enter' button is located below these links. At the bottom, there are two links: 'Find out.' and 'Click here.'.

 **Duke University
NetID Services**

Please identify yourself to NetID service handleservice at host shibboleth.duke.edu.

Please enter your NetID:

NetID:

Password:

+ [TiQR](#)
+ [x509](#)

Don't know what a NetID is? Not sure if you have one? [Find out.](#)

Forgot your password? [Click here.](#)

21

http://www.incommon.org/docs/iamonline/20111206_IAM_Online.pdf

リスクに基づくサービスの分類(例)

	比較的低リスクのもの	リスクの高いもの
学生サービス	履修登録 証明書交付 施設利用予約	
教育研究	出席確認 単位互換 研究者総覧	成績管理
教職員業務	時間管理 掲示板 施設利用予約 電子申請	財務会計 人事給与 決裁・稟議 DBアクセス
福利厚生	健康診断 ポイントサービス	検診履歴 電子マネー
図書館サービス	図書館入館 図書貸出 電子ジャーナル	



複数LoAを活用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
 - ▶ LoA 1 (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
 - ▶ LoA 2サービスでも、学内からであればLoA 1 (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	
ID連携トラストフレームワークの整備	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									・ID連携トラストフレームワークの認定状況 ・ID連携トラストフレームワークのサイト利用状況
	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】		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】		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】					
	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】									
	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									

国民IDとマイナンバー

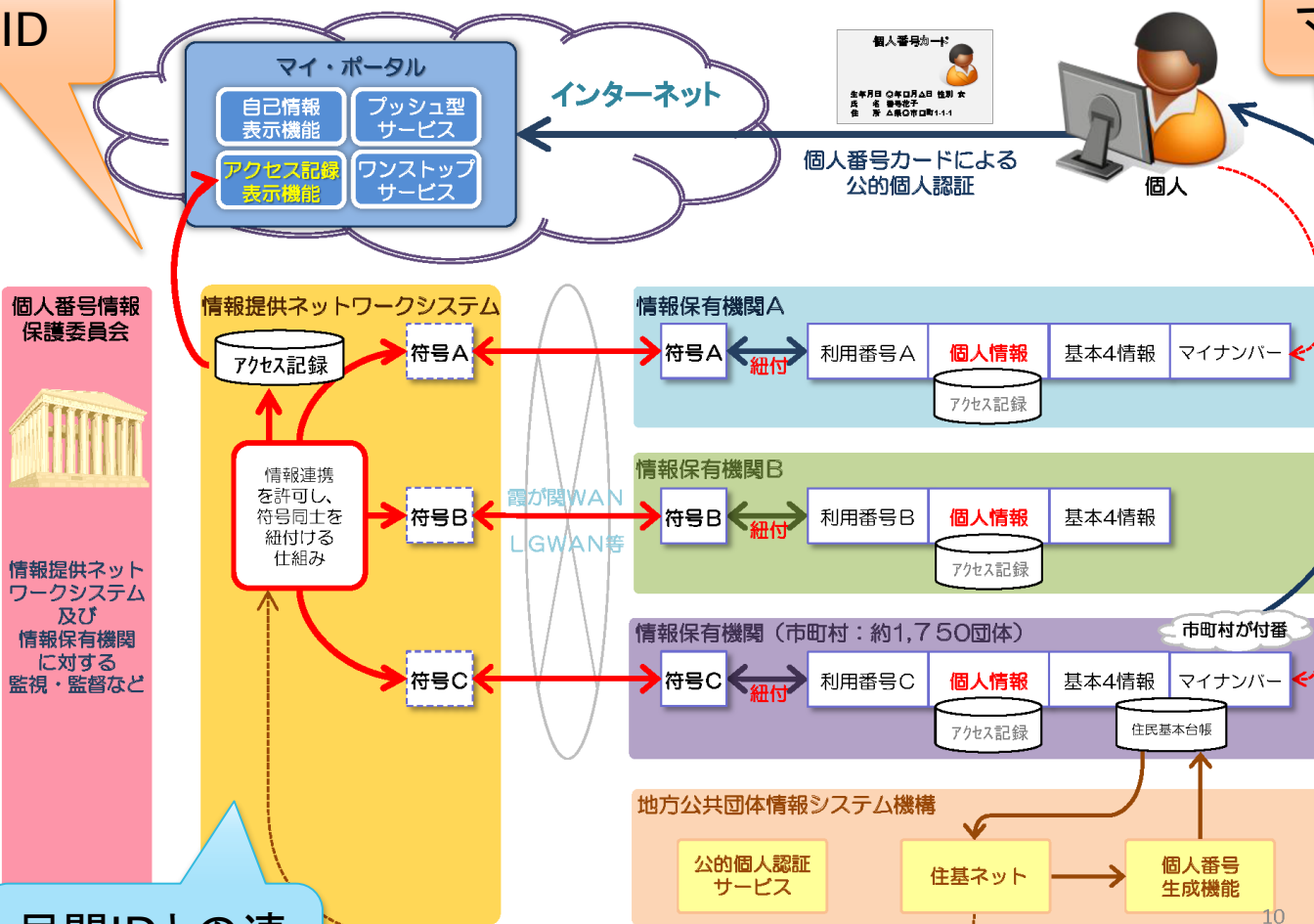
9. 番号制度における情報連携のイメージ

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?

さらなる信頼性向上とサービス拡大に向けて

- ▶ IdPのLoA認定の普及
 - ▶ LoA 1はベースラインなので、難しい資格ではない(というか簡単)
 - ▶ しっかり運用されていれば、基本的に新たな投資は不要
 - ▶ 組織として正式に安定して運用されていることを示すことが重要
 - ▶ 組織の中でIdP管理者や基盤センターがきっちりやっているという意味も
 - ▶ LoA 2も大学にとってそんなに難しい話ではない
 - ▶ LoA 1 + (LoA 1.5?)でも十分かもしれない
- ▶ LoA 2 (LoA 1+)に準拠したサービスの展開
 - ▶ 日本国内における実用的なID連携の先行事例として
- ▶ 高度な認証技術への柔軟な対応のために
 - ▶ 様々な認証方式の任意の組み合わせに対応可能な、汎用認証インタフェースの実現

参考：国立国会図書館 カレントアウェアネス



E1482 - 山形大学の事例からはじまる学認の次世代認証基盤構想 | カレントアウェアネス・ポータル - 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)

E1482 - 山形大学の事例からはじまる... +

current.ndl.go.jp/e1482

CA Current Awareness Portal
図書館に関する情報ポータル

CA-R	CA-E	CA	調査研究
ホーム » カレントアウェアネス-E » 2013年 (通号No.230- : E1384-) » No.245 (E1478-E1483) 2013.09.26			
E1482 - 山形大学の事例からはじまる学認の次世代認証基盤構想			
カレントアウェアネス-E No.245 2013.09.26			
E1482 山形大学の事例からはじまる学認の次世代認証基盤構想			
現在、大学ではユーザのIDを集中管理することで、一つのIDとパスワードで全ての学内サービスにログインでき、さらに、認証を一度行えば他のサービスに再認証なしにログインできるシングルサインオン(Single Sign-On: SSO)という環境の整備が進められている。SSOでは、これまでサービス毎に独自に行っていた認証処理をサービスから分離し、サービス間で共有する一つの認証サーバを用意して共用する。パスワード情報はサービス間で共用せず、			