資料1

トラストフレームワーク
利用者の利益を守る/サービス提供者を制御するために

学認/東京大学　　佐藤周行
学認/情報学研究所　山地一禎

学認のほうからきました(GAKUNIN.JP)

EXECUTIVE SUMMARY (1/3)

- 利用者の利便性を図るためのポータルを提供することがいろいろなレベルで行われています
- 利用者は、一つのアイデンティティ（ID）を使って、複数のサービスを利用できます（SSO）
- ひとつのSSOの枠内では、サービス提供者が互いを信頼し合って、プライバシーが含まれる属性情報等を流通させています。提供される属性に応じて、サービスのレベルを変えることができます
- この枠組では、アイデンティティを提供するサーバ、サービスを提供するサーバに利用者情報が蓄積されます
- 各サービス提供者のふるまいをコントロールすることが、利用者の（プライバシーに関する）利益に直結します

EXECUTIVE SUMMARY (2/3)

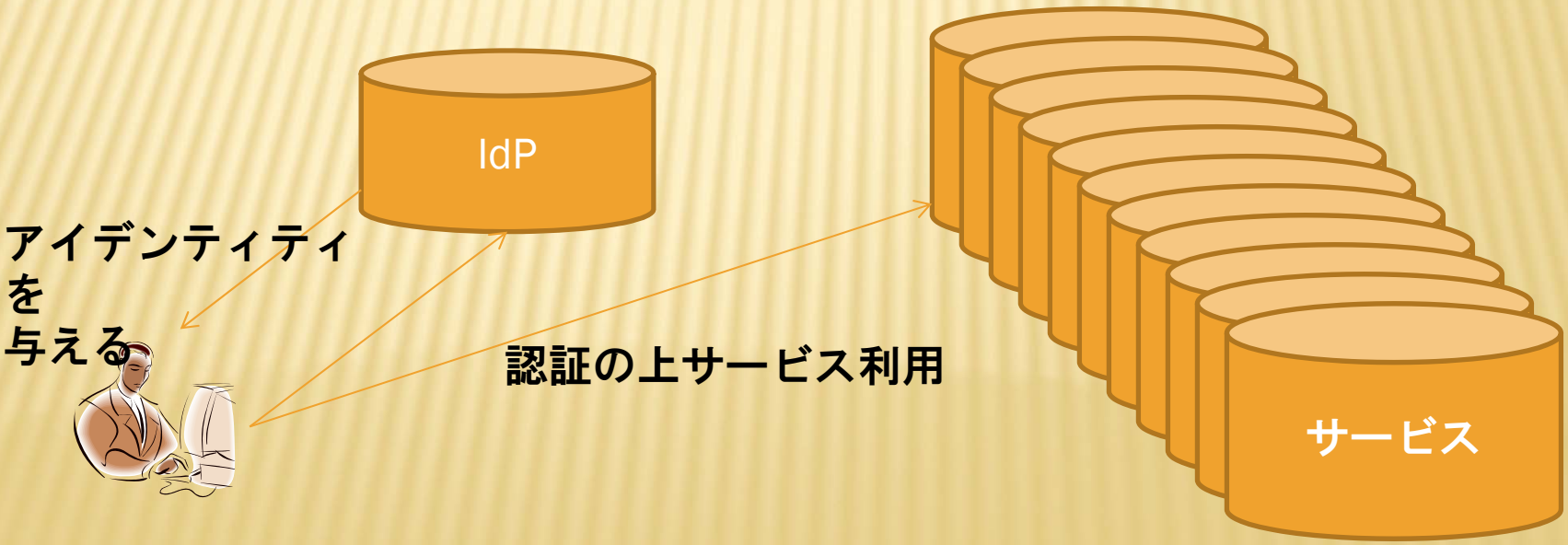
- アイデンティティを提供する側として、以下があります
  - 「インターネットに参加する個人」に対して
  - 「組織内で行動する組織人」に対して
- われわれ「学認」は、大学・研究機関に属する人間に与えられたアイデンティティを流通させて、学術サービスをSSOで利用するための組織です

EXECUTIVE SUMMARY (3/3)

- 学認はトラストフレームワークプロバイダ (TFP) です。
- TFPは、ポリシーを持ち、それを遵守することを参加機関 (IdP, SP) に求めることで運用をgovernします
- IdPの運用のレベルをLoAで認定します
- 学認TFPは、国際的な枠組の一部として機能しています
- 「トラスト」の構築が、インターネット（の一部）に秩序をもたらします

ネットサービスのARCHITECTURE

- 利用者は、ネット上で「アイデンティティ」を与えられる。ーー一つでも、複数でも。
- アイデンティティを確認する（認証）ことで、その利用者に応じたサービスが提供される



ネットサービスのARCHITECTURE (CONT'D)

- 認証を一度だけおこなうことで、ネット上のWebアプリケーションで提供されるサービスを自由に利用することが技術的に可能になりました
  - SAML，OpenID
- 「ネット上のポータル」が現実的になっています

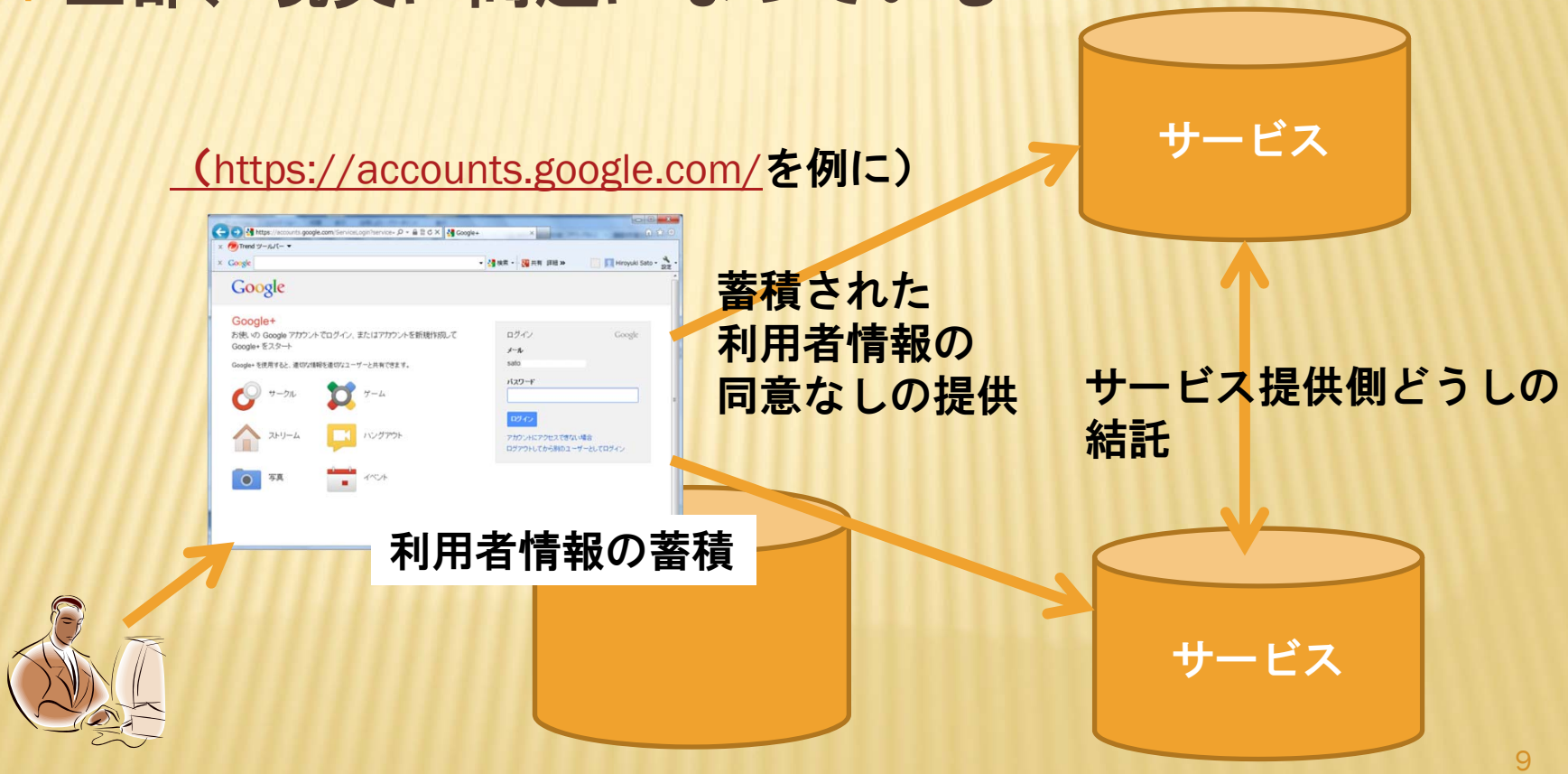
GOOGLE+の例

Google AccountがOpenIDアカウントとして他の場所で利用できることをアナウンス(2009年)

https://accounts.google.com/ より

SSOで安心してサービスを受けるには

- 指摘される様々な問題点
  - 全部、現実に問題になっている



サービス提供 VS 個人

- ポータル大手が（インターネット上の）巨人として、個人を飲み込む図式になっている
- 力関係として、個人は圧倒的に無力

「アイデンティティ」について

- 「アイデンティティ」の正体
  - 本人性
  - 本人の持っている属性全部
- どこにおけるアイデンティティ？
  - インターネットの中でのアイデンティティ
  - 組織の中でのアイデンティティ

ネット上の
アイデンティティ

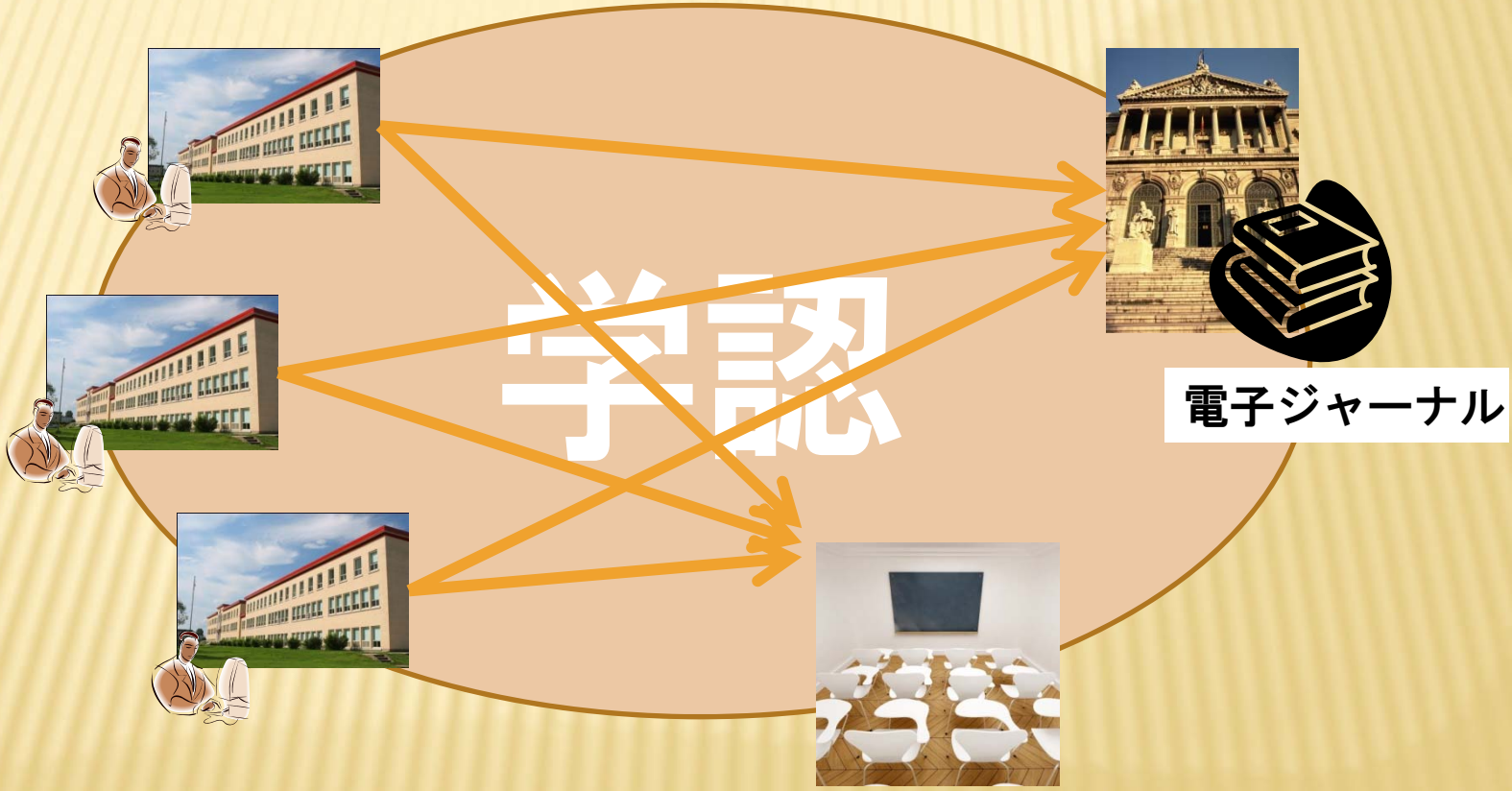
VS

教育・研究者としてのアイデンティティ

- さまざまなサービスの利用
  - 電子ジャーナルの閲覧
  - 学会への参加
  - （国際）学術団体での活動
  - …
  - 共同利用機関での利用（ファイル共有、無線LAN利用、…）
- 「大学が与えるアイデンティティ」での活動をSSOで利用する

学認フェデレーションの構築

- 大学が与えるアイデンティティで認証してサービスを利用



学認の現状

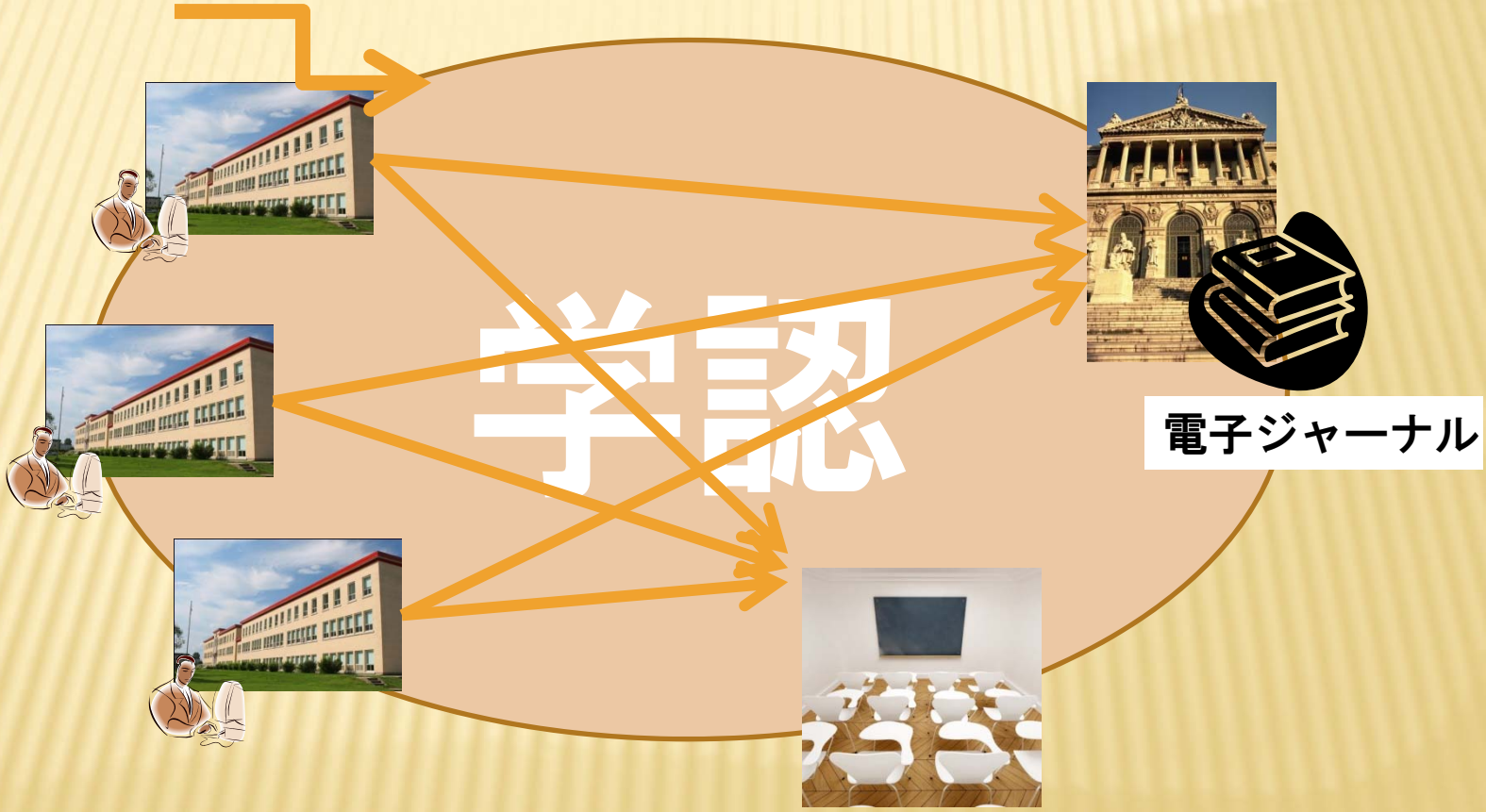
- 参加大学　ー約50大学
- サービスメニュー
  - 電子ジャーナル、ソフトウェアダウンロード、ファイル交換、無線LAN用ID発行、…
- 国際的な動き
  - 欧米での同種の動き（フェデレーション）との交流
  - 米InCommon、欧各国のフェデレーションが整備
  - ソフトウェアの整備が国際的に進められている

フェデレーション（各種トップページ）

http://www.incommonfederation.org/
http://www.switch.ch/
http://www.jisc.ac.uk/
http://www.csc.fi/
http://www.edugain.org/
(上から順に)

（オンライン）トラスト…

- これはなんだろうか？

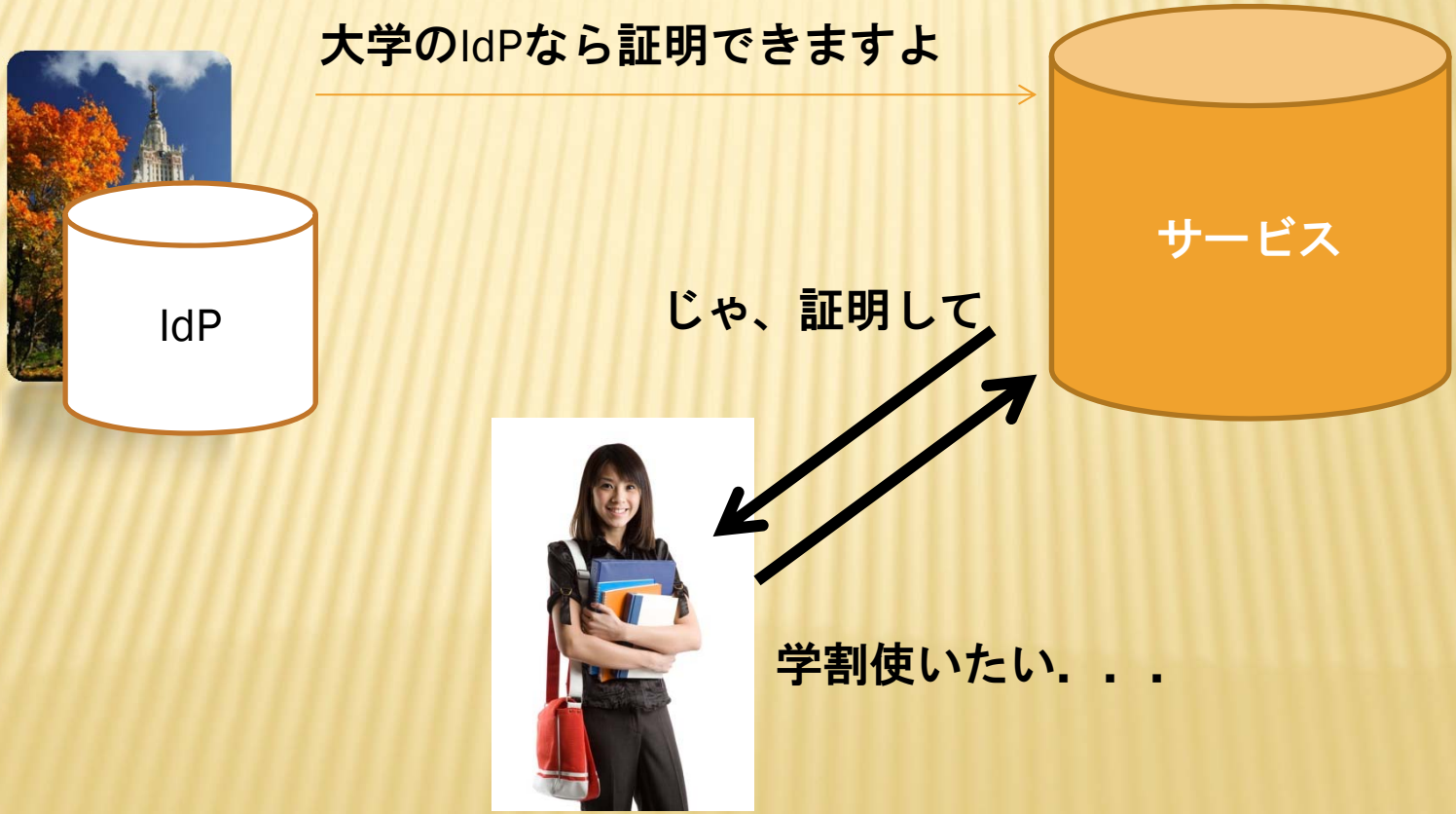


フェデレーションの問題

- IdP側の懸念
  - ふるまいのよろしくないSPが入ってきていないだろうか？
  - プライバシーを含む利用者情報を出す以上、その管理はきちんとしているべきだ
- SP側の懸念
  - IdPから渡ってくる情報は、正確なものだろうか？
  - 認証の正しさ、渡ってくる情報の正しさはどこまで担保されているのだろうか？
- 利用者の懸念
  - IdPやSPは、自分の行動履歴を使って何か変なことをしていないだろうか？
  - IdPはSPに、自分のデリケートな情報を勝手に渡していないだろうか？
- サービスメニューを学術以外に拡大すると必ず出てくる問題

学認と学生　（問題は顕在化している）

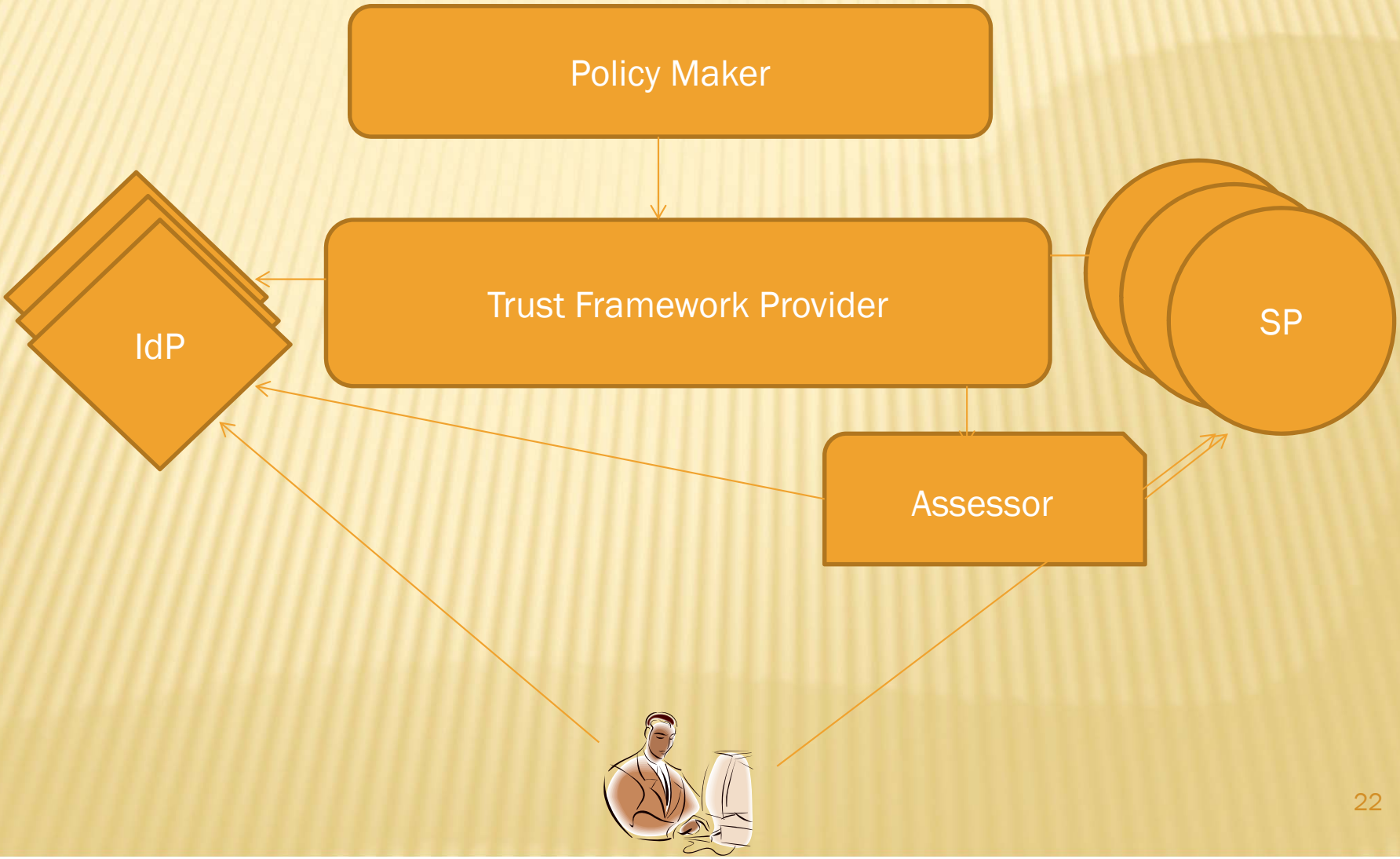
- インターネット上のサービスでの学割を考える　学術じゃないけど…



トラストによる解決

- トラスト
  - トラストの枠の中にいれば、その中で流通する情報について、「きちんと管理されること」「正確であること」などが保証される
  - デリケートな情報を交換する土台になる
  - 保証の度合いは、トラストを規定する「ポリシー」が決める

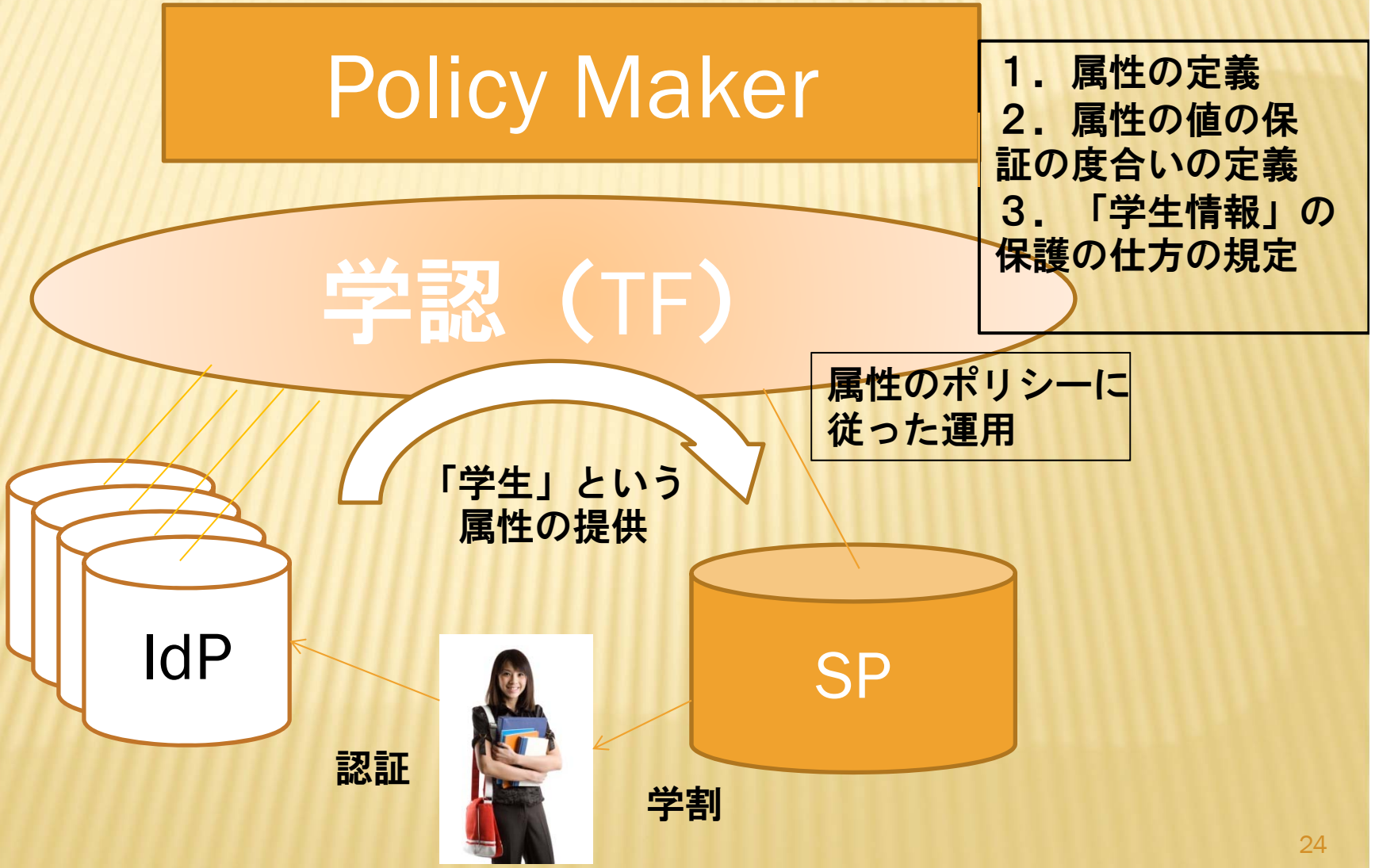
OIXによるトラストのモデル



TFPがGOVERNするもの

- IdPとSPのふるまいをGovernすることで、利用者に安心を与える
- Policymakerの作るポリシーで規定する
- 現状で問題になっているのは「認証の正確さ」
  - IdPのLevel of Assurance (LoA)
- 将来問題になりそうなのは
  - 「本人属性」のクオリティ (LoAA)
  - IdP，SPの持つ情報の守り方 (LoP, CoC)

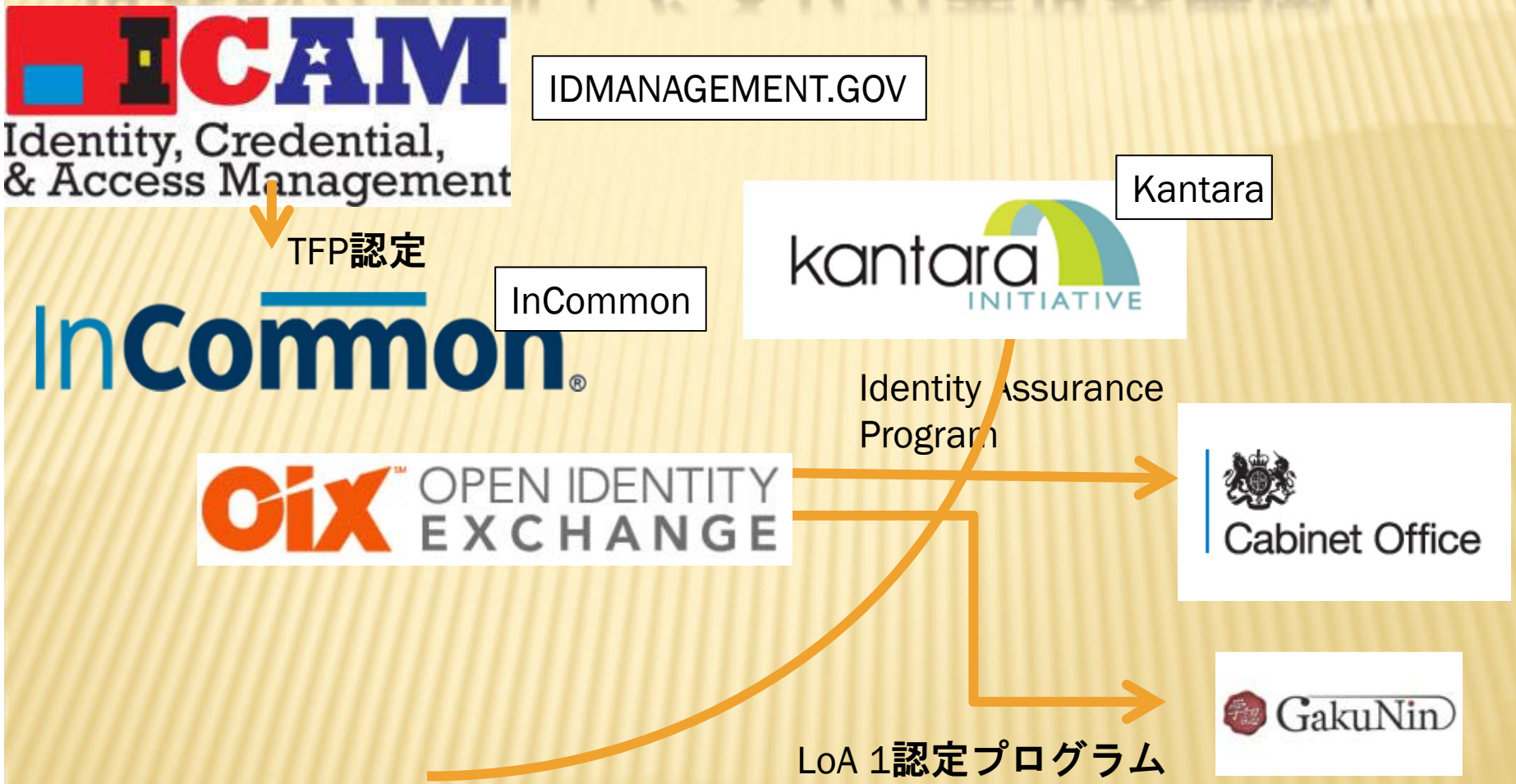
TRUST FRAMEWORK的な解



アセスメント

- TFPが参加機関を評価するポイント
  - Governance
    - 参加機関は、TFPの要求するレベルで、組織として成熟した形でサーバを運用しているか？
  - Privacy
    - 参加機関は、TFPの要求するレベルで、利用者のプライバシーを守っているか？
  - Technical
    - 参加機関は、TFPの要求する技術レベルで、セキュリティやアイデンティティ管理を運用しているか？
- アセスメントの基準
  - アメリカNIST800-63をベースにしている
  - TFPの採用プログラムを定め、共通の基準で動く
    - アメリカ連邦ICAMの基準
    - ISO化
- 監査
  - 認定し、品質保証は監査で行う→アメリカ的な考え方

世界的な動向（アメリカ発世界展開）



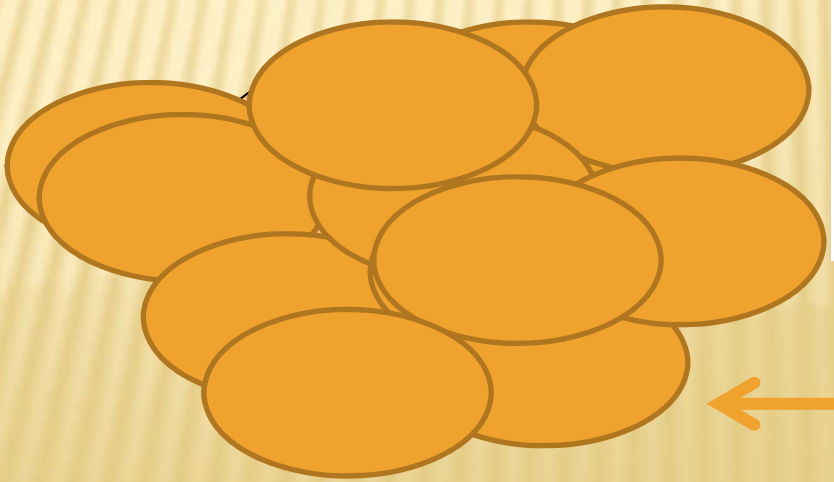
ここに掲載されているロゴ等はそれぞれの法人・団体のものです。

学認 AS A TFP

- 国際的な基準に則り運用
- 「学術機関」向けトラストの（テスト的な運用ではなく）本格的な運用をしている
  - Governance
  - Assessment（FICAM LoA1を認定できる）
    - Assessorの登録
    - 定期アンケートを通じての評価プロセスの確立
- 他の商業フェデレーション、欧米の学術フェデレーションと協調し、各種レベルの開発を進めている
  - LoA, LoP, LoAA
- 学割等、具体的なシナリオで展開を予定

トラスト AS 利用者の安心のアンカー

- IdPやSPをプライバシー等の面から安心、安全に運用させるには、上位のポリシーメーカーとTFPによるGovernanceが必要
- トラストは、プライバシー等、デリケートな情報の積極的な流通を可能にする



Bigにしないで、ローカルに守る。LoP (CoC)などで行動を制御できるようにする…のならば、プライバシー情報の流通・利用を促進

おわりに

- フェデレーションと、それを利用したSSOにより、利用者の利便性を高めることができます
- フェデレーション内で、デリケートな情報の積極的な流通を可能にするためには、トラストの構築が非常に効果的です
- 「学認」は、学術フェデレーションとして、国際標準のトラスト構築を進めています
- トラストでネットを覆うことができれば、情報流通はより活発になるでしょう