# 学認トラストフレームワーク

2012/09/12
学認CAMP@香川大

東京大学 / 学認　佐藤周行

# いきなり結論

- 学認のIdPとSPの間で、安心して情報交換を行う枠組（Trust Framework）が構築されつつあります
- 「トラスト」は学認の外にあるサービスを呼び込むためのキーになっています
- 学認は一部国際的な枠組とトラストを共有しています（Open Identity Exchange）
- 学認アンケートへの回答を用意することで、ふだんの運用を見直していきましょう

# IDPの信頼を高めるために –学認アンケートの傾向と対策–

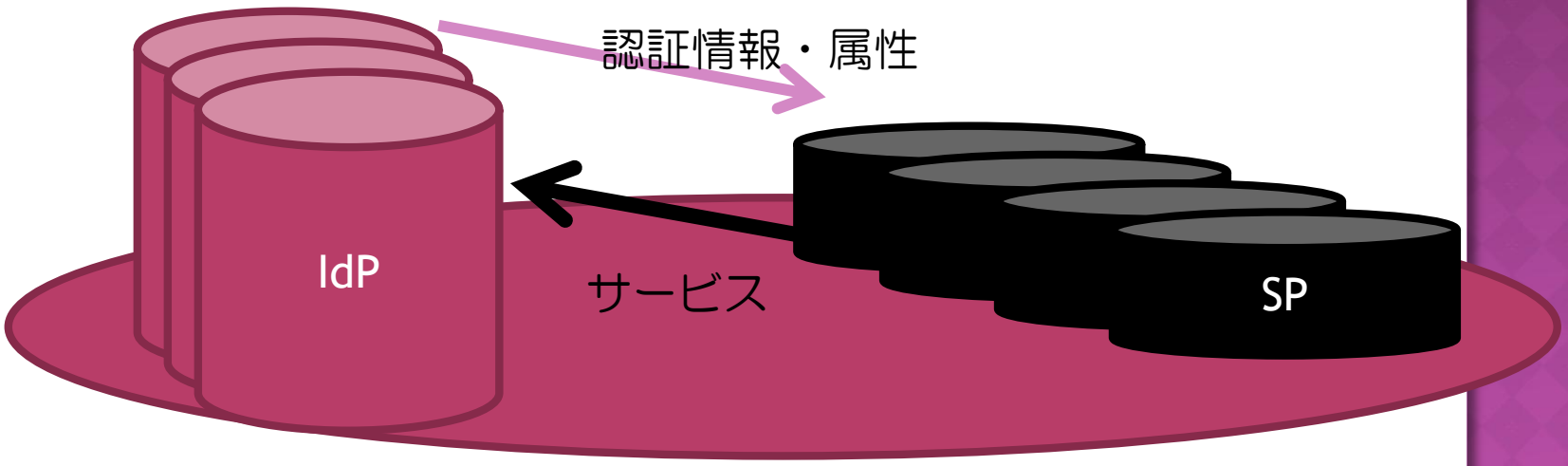
東京大学 / 学認
佐藤周行

# 安心できるデータ交換のために

- オンラインでのデータ交換
  - フェデレーションでは本質的
- この認証情報は信用できるか？（SPサイド）
  - 本人が確実にサインオンしている保証
  - 信用できれば、サービスが提供できる
- このサービスは信用できるか？（IdPサイド）
  - 提供した属性が「正当に」使われる保証
  - 信用できれば、認証情報を提供できる

# 保証の枠組としての学認

- IdPの質とSPの質に保証を与えるのが「学認」
  - 実施要領
  - システム運用基準



# サービスの多様化と要求レベル

- サービスの多様化、高度化に対応して、要求されるIdPのレベルも多様化しています
  - 高機密情報（Healthcare等）
  - 予算申請等、お金に関係するもの
- フェデレーションは、要求されるレベルに応じてIdPの運用レベルを審査することができます
  - IdP側の対応の仕方は？（この手の話はこのセッションの後のほうで触れられるでしょう）

# TRUST FRAMEWORK

- 学認（フェデレーション）が、IdP（とSP）に対して、運用レベルの保証を求める
  - 運用レベルは複数存在する場合がある
  - SP（とIdP）は、保証された運用レベルに応じて提供できるサービスを決定する
- フェデレーションは、参加機関に対して「運用レベル」の認定を行う
  - LoA認定
- レベルの基準決定と認定を通して、「安心できるデータ交換」の枠組を提供する
  ＝　Policy Making
- このポリシーを実装する
  ＝　Trust Framework

# TRUST FRAMEWORKのご利益

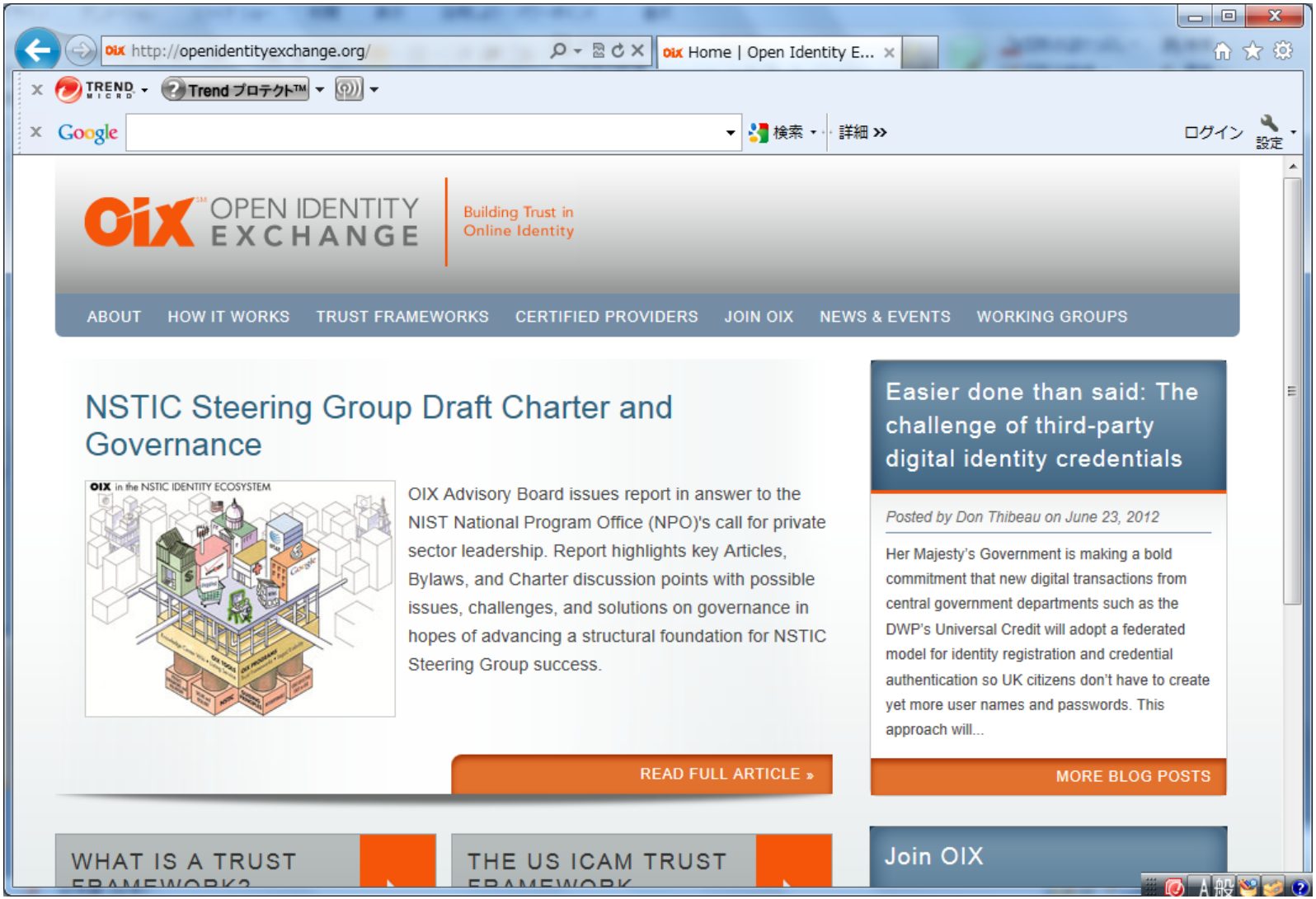
- 外部のサービスを呼び込む
- なまぐさい例１：
  - 学割を提供したいのだが、学認参加のIdPから提供される「eduPersonAffiliation=student」はどのくらい信用できるのか？
- なまぐさい例２：
  - アメリカの連邦系サービスを利用したいのだが、先方はFICAM LoA 1で運用していないと接続を認めないと言っている

- SPとIdPが運用レベルを相互評価することから Trust Frameworkと、それを律するポリシーの評価へ

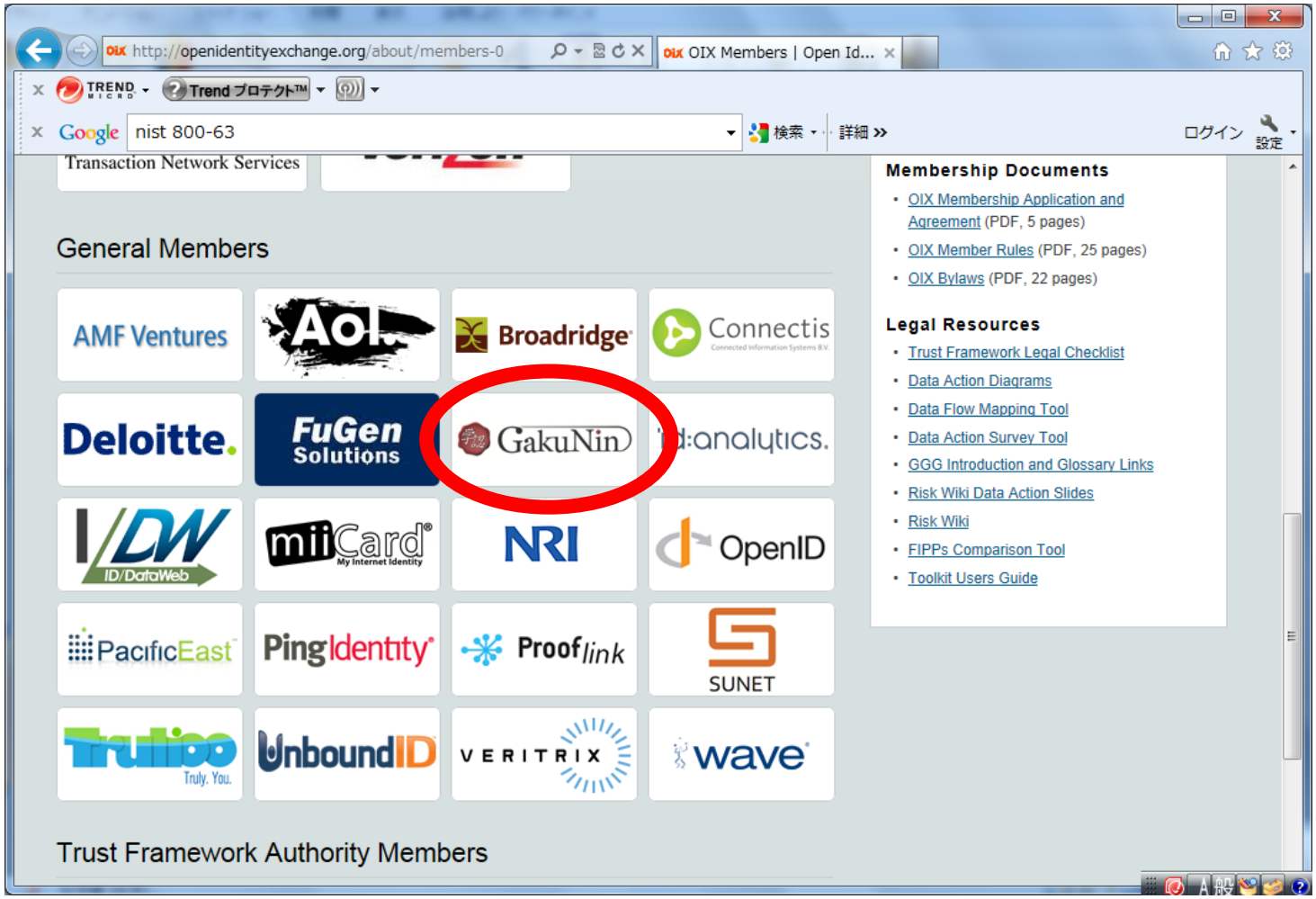
# 学認 AS A TRUST FRAMEWORK

- 学認はTrust Framework　Providerとして機能しはじめています
  - 学認トラストチームの発足
  - トラストに関係するポリシーの検討
  - 国際的に通用するレベル (LoA) の運用
    - Open Identity Exchangeへの参加
    - OIX　LoA 1認定を内部で行うことが可能に

# OPEN IDENTITY EXCHANGE



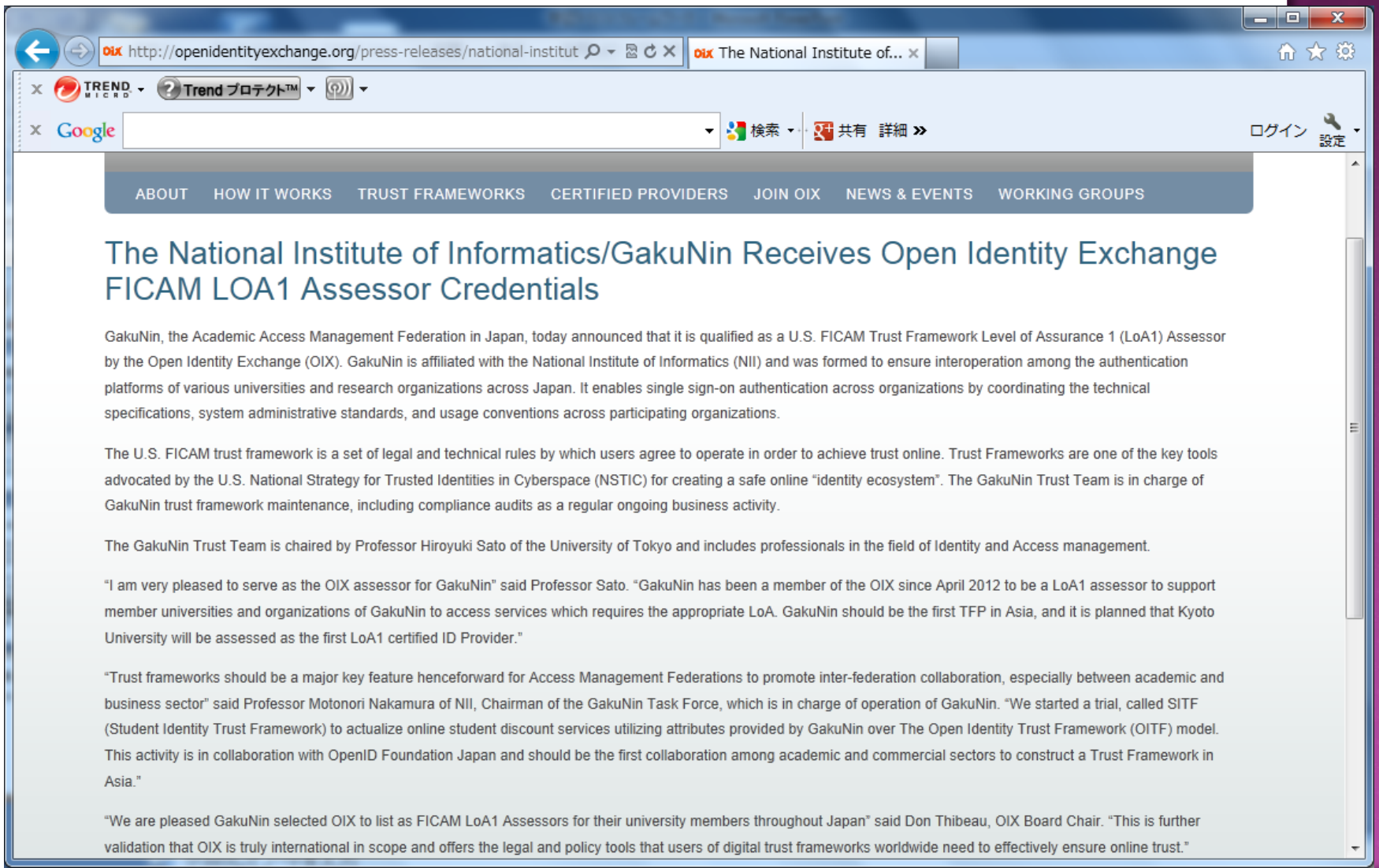
# 学認はOIXのメンバー



# OPEN IDENTITY EXCHANGEの正体

- アメリカのFICAM (Federal Identity, Credentials, and Access Management) の運用するTFPAP (Trust Framework Provider Adoption Program) のひとつとして認定されている
  - LoA 1については独自の評価基準を持つ
  - Google, PaypalなどにLoA 1認定を行っている
- アメリカとはいいながら、日本（学認）とヨーロッパでも活動を開始
  - LoAの評価基準はISO標準化が進行（世界共通化）
- 認定基準は…

# 学認 AS OIX LOA 1 認定者



http://openidentityexchange.org/press-releases/national-institut

The National Institute of...

ABOUT HOW IT WORKS TRUST FRAMEWORKS CERTIFIED PROVIDERS JOIN OIX NEWS & EVENTS WORKING GROUPS

## The National Institute of Informatics/GakuNin Receives Open Identity Exchange FICAM LOA1 Assessor Credentials

GakuNin, the Academic Access Management Federation in Japan, today announced that it is qualified as a U.S. FICAM Trust Framework Level of Assurance 1 (LoA1) Assessor by the Open Identity Exchange (OIX). GakuNin is affiliated with the National Institute of Informatics (NII) and was formed to ensure interoperation among the authentication platforms of various universities and research organizations across Japan. It enables single sign-on authentication across organizations by coordinating the technical specifications, system administrative standards, and usage conventions across participating organizations.

The U.S. FICAM trust framework is a set of legal and technical rules by which users agree to operate in order to achieve trust online. Trust Frameworks are one of the key tools advocated by the U.S. National Strategy for Trusted Identities in Cyberspace (NSTIC) for creating a safe online “identity ecosystem”. The GakuNin Trust Team is in charge of GakuNin trust framework maintenance, including compliance audits as a regular ongoing business activity.

The GakuNin Trust Team is chaired by Professor Hiroyuki Sato of the University of Tokyo and includes professionals in the field of Identity and Access management.

“I am very pleased to serve as the OIX assessor for GakuNin” said Professor Sato. “GakuNin has been a member of the OIX since April 2012 to be a LoA1 assessor to support member universities and organizations of GakuNin to access services which requires the appropriate LoA. GakuNin should be the first TFP in Asia, and it is planned that Kyoto University will be assessed as the first LoA1 certified ID Provider.”

“Trust frameworks should be a major key feature henceforward for Access Management Federations to promote inter-federation collaboration, especially between academic and business sector” said Professor Motonori Nakamura of NII, Chairman of the GakuNin Task Force, which is in charge of operation of GakuNin. “We started a trial, called SITF (Student Identity Trust Framework) to actualize online student discount services utilizing attributes provided by GakuNin over The Open Identity Trust Framework (OITF) model. This activity is in collaboration with OpenID Foundation Japan and should be the first collaboration among academic and commercial sectors to construct a Trust Framework in Asia.”

“We are pleased GakuNin selected OIX to list as FICAM LoA1 Assessors for their university members throughout Japan” said Don Thibeau, OIX Board Chair. “This is further validation that OIX is truly international in scope and offers the legal and policy tools that users of digital trust frameworks worldwide need to effectively ensure online trust.”

- 学認は、OIXの LoA 1を参加機関に対して認定することができます。
- アメリカ連邦系のサービスを利用するときにLoA 1は最低限の保証レベルになっています
- 自大学のIdPを国際連携に使う予定のあるところはご相談ください
  - oix-loa1@nii.ac.jp
  - https://www.gakunin.jp/docs/fed/loa/loa1program

# IDPの運用でのチェックポイント

- ポイントは４つ（NIST 800-63）
  - 本人確認の確かさ
    - LoA 1　あまり決めない（GoogleもLoA 1認定されている）
    - LoA 2--　政府発行の写真付きIDカード…（日本でも、携帯電話購入の際の基準になっている）
    - 電子証明書の世界では1と2の間に「きちんとした組織のTrusted DBにあるもの」という認定基準がある
  - クレデンシャル（パスワード）の強度
    - 本人（だけ）がそのパスワードを使ってログインできることを保証する
  - 認証方法の確かさ（特にリモート）
  - アサーション

# 保証レベルの認定

- ここではIdPがリリースする認証情報の確かさの保証レベルについて論じます
  - 他にも面白いトピックが…
- 学認の大方針
  - 実施要領、システム運用基準に沿った運用をしていれば、LoA 1は基本的にクリアできるように運用する
  - 運用レベルの保証は毎年行う監査（学認アンケート）によって行う、すなわち
    監査合格　＝　LoA 1のレベルクリア

# 厳密にいえば

- OIX LoA 1認定を受けるには、学認の基準を満たすことに加えて、以下のことが必要になります
  - 組織が成熟していること
    - セキュリティ/プライバシー保護の体制
    - 保険その他（アメリカの基準だからしょうがない）
  - IdPの運用が組織によりオーソライズされていること
    - 運用規則その他
  - プライバシーに関して、アメリカの基準を満たして運用していること
- 規則の有無については、一度確認することをお勧めします

# 学認アンケート

- 昨年秋に第一回目のアンケート
- 今年の春にトラストチームを発足させ、監査の体制を整備
  - 監査の資格を持っている人をそろえました
- 9/3付で今年度のアンケート開始のアナウンス
  - ご協力をよろしくお願いします
- 監査を基にした助言、フォローアップその他を希望する参加機関は遠慮なくご相談ください
- ふだんの運用を見直す機会としてもご利用ください

# 連絡先

- 今回の監査について
  - gakunin-audit@nii.ac.jp
- OIX　LoA 1について
  - oix-loa1@nii.ac.jp

# 学認アンケートのポイント(1/2)

- アイデンティティ（アカウント）のライフサイクル管理
  - Trusted DBから下りてきているか？
    - Trusted DBとは
      人事DBと学務DBが典型的
    - 大学の場合、心配ないはず（？）。LoA 2の場合「政府発行のIDカードを持って面接」などという、アメリカらしい基準があるが、大学では基本的に不要
  - 変更、廃棄も含む
    - 棚卸その他
  - 共有アカウントのコントロール

# 学認アンケートのポイント(2/2)

- パスワードの管理
  - 十分なエントロピーを持っているか
  - パスワードポリシーを持って運用されていれば問題なし
    - パスワード長、有効期間…
- （OIX的な）残りの基準については、Shibbolethを安定して運用していれば問題ありません

# 結論

- 学認のIdPとSPの間で、安心して情報交換を行う枠組（Trust Framework）が構築されつつあります
- 「トラスト」は学認の外にあるサービスを呼び込むためのキーになっています
- 学認は一部国際的な枠組とトラストを共有しています（Open Identity Exchange）
- 学認アンケートへの回答を用意することで、ふだんの運用を見直していきましょう

# TRUST FRAMEWORKの今後（実は「ご利益」のスライドの焼き直し）

- Trust Framework
  - ポリシー（基準）の公開
  - ポリシーに則った運用の保証（アセスメント）
- →　フェデレーションの拡張を容易に
  - 外部のSPの参加が容易に（公開されたポリシーを評価して参加決定できる）
  - 外部のフェデレーションとの連携が容易に（具体的にはアメリカ連邦系のサービス）
  - 自大学の研究環境、福利厚生の整備に積極的にお使いください
    - たとえば、学割などが可能になるかもしれません