NII 学術情報基盤オープンフォーラム 2024
NII RDCトラック

次世代認証連携と研究データ管理

坂根 栄作

国立情報学研究所
アーキテクチャ科学研究系
トラスト・デジタルID研究開発センター／学術認証推進室

今後の展望：次世代認証基盤との連携

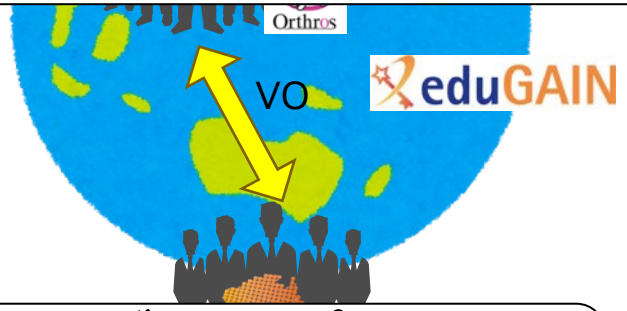
1. 次世代認証基盤を通じた産官学の共同研究で利用できる認証システムへの対応
2. 海外の大学に所属する研究者との国際共同研究の実現
3. 組織を越えたグループ管理への対応
4. 認証保証レベルへ対応

産官学の共同研究での利用における障壁は何か？

ループの参加

民間企業の参加

国際共同研究での利用における障壁は何か？



組織を越えたグループ管理の要件は何か？

認証保証レベルとは何か？

IAL2/AAL2

出典：込山悠介, ”管理基盤 GakuNin RDM の役割と今後の展望”, 2024/06/11

研究データ管理における認証・認可／アクセス制御の課題

- 産官学の共同研究における障壁
  - 産官の研究者であることをどのように認証するか；産官の研究者の ID は何（が適切）か
- 国際共同研究における障壁
  - 海外の大学に所属する研究者をどのように認証するか
- 組織を越えたグループ管理の要件
  - グループはどのように構成されるのか？
  - 認可／アクセス制御をどのように行うのか？
    - Identity-based, Role-based, Attribute-based
- 認証保証レベル
  - サービスに送られる認証情報；身元確認＋当人認証＋α
  - 身元確認の保証度 (IAL: Identity Assurance Level)
  - 当人認証の保証度 (AAL: Authenticator Assurance Level)
    - 例：写真付きIDで身元確認をし、オンラインでの認証ではパスワード認証に加えワンタイムパスワードに基づく２要素めの認証を課す
  - このような保証度の違う認証をどのように利活用できるか？

次世代認証連携における問題と課題

- 研究DX促進；多種多様なサービスへの適用
  - 機関の全構成員共通のサービス：認可・アクセス制御が比較的単純
  - 研究者が利用するサービスは多種多様：認可・アクセス制御の条件は単純ではなく、加えて身元保証度 (IAL) や認証強度 (AAL) への要件もいろいろ
- SP 視点での運用理想像：認可・アクセス制御に専念
  - 認証を完全に分離して、信頼できる IdP（利用者の所属機関）に委譲

- 問題
  - 利用者の所属機関が（連携可能な）IdP を運用していない
  - それぞれの顧客の IdP が、IAL/AAL 要件を満たすかどうかが明確ではない
  - より高度なグループ管理要件（柔軟、高効率など）に応えていない？

IdP：Identity Provider
SP：Service Provider

- 課題
  - IdP の拡大 – 適切な IdP をもたない利用者をどのように認証するか
  - IdP の強化 – より信頼性の高い認証に向けて
  - 認可・アクセス制御の要件整理；SP に送るクレデンシャルに、誰が、何を、どのように含めるべきか

次世代認証連携における主要構成要素

6/12 認証トラック2

学認IAL/AAL

- 本人確認の保証度、認証強度について規定

IdPとSPが参照することにより統一的かつ効率的な議論が可能となり、また、各機関が遵守することにより学認全体のトラストを担保できる

6/12 認証トラック2

認証器レジストリ

- 学認AALに基づく認証器の評価

認証器を評価、結果を公開し、大学・研究機関のIdPの多要素認証対応を促進する

6/12 認証トラック2

認証プロキシサービス "Orthros"

- IAL/AAL matching, Credential bridging, Attribute coordination

SPからの要求を仲介しIdPと連動することで、IAL, AALの担保が可能となる

6/12 認証トラック3

IdPホスティングサービス実証実験

- 大学、研究機関のIdP構築運用の課題を議論

大学・研究機関のIdP構築運用の負荷を軽減、様々な運用形態のなかから機関に適したものを選択し、すべての機関がIdPを運用できるようになる

6/12 認証トラック2

グループ管理機能の高度化

- より高度な認可要求に対応

所属などの基本属性に加えて一般的なIdPが扱わない属性に基づいたグループ管理を実現し、SPの認可管理が効率化できる

次世代認証連携の取り組み (1/2)

- 学認 IAL/AAL
  - 何を解決するのか；学認はどの程度信頼できるのか、に応える
  - 学認から得られる認証情報（クレデンシャル／アサーション）の保証度について、サービスが求めるより高い保証度を規定する文書を提供し、高信頼な基盤運用の基準となる

- 認証器レジストリ
  - 何を解決するのか；流通する認証器の個別評価の負担を軽減
  - 流通する認証器を評価し、学認 AAL 準拠性や導入運用の勘所を公開
  - https://level2.gakunin.jp/

学認 IAL/AAL の広がり

新しい学認 IAL/AALが、外部ID基盤/IdP との連携や研究プロジェクトにおける利活用の議論を可能とする

学認 IAL/AAL の広がり - 国際認証連携・相互運用

REFEDS Assurance Framework, IGTF Profiles of Authentication Assurance との相互運用性の議論を新しい学認 IAL/AAL 文書に基づいて行うことが可能

次世代認証連携の取り組み (2/2)

- 認証プロキシサービス Orthros
  - 何を解決するのか；
    - ・適切な IdP をもたない利用者をどのように認証するか
    - ・より信頼性の高い認証をどのように提供するか
- IdP 拡大
  - 学認への参加を促進
    - 学認 IdP 構築運用支援 - 学認対応 IdP ホスティング
  - **学認への参加が難しい機関（の研究者）を支援**
    - 企業の研究者
    - 自治体等に在籍し研究活動に資する方
    - その他
- IdP 強化 - **認証情報の強化**
  - 単独の IdP では対応できない保証度要求や属性要求に応えられるようにする

産学連携イメージ

①gBizID を持つ

②学認参加IdPにアカウントを持たない

gBizID

as OpenID Provider

GakuNin RDM

as Relying Party

as SAML IdP

Orthros

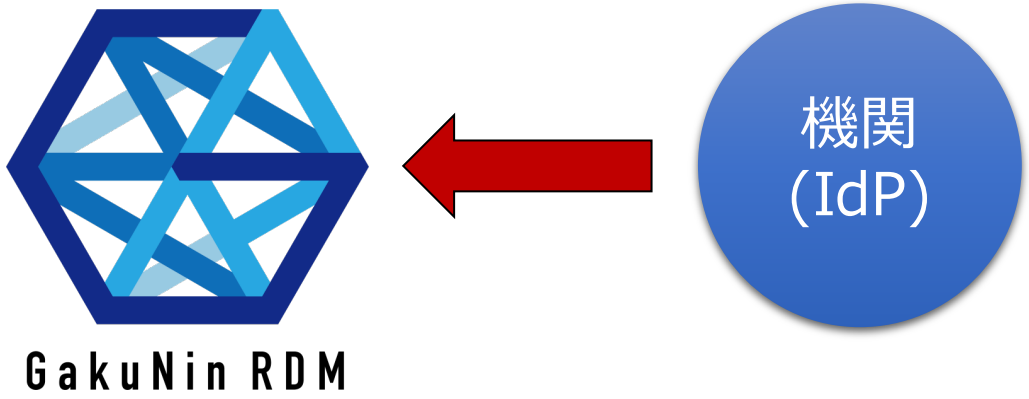
③認証プロキシサービス “Orthros” で研究者とその gBizID をバインディング。
gBizID プライム による所属属性の担保→高いIALとしての評価可能性あり

④研究者は、gBizID で認証し、認証プロキシサービスが SAML SP に SAML assertion を送出

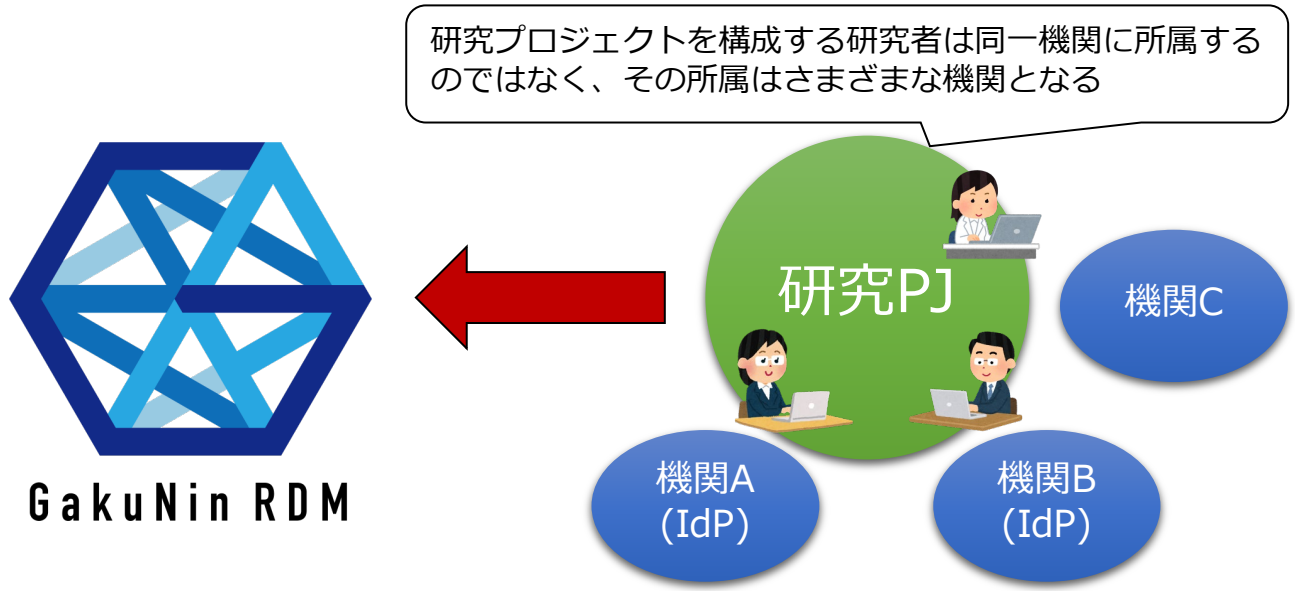
研究者は、学認IdPにアカウントを持たなくても、認証プロキシサービスを仲介することで、学認SPにアクセスが可能となる

複数の組織を跨ぐ研究プロジェクト

機関単位の利用申請を拡張



利用責任は機関が負う
機関を識別する＝IdPを識別する



利用責任はプロジェクトが負う？
プロジェクトを識別するには
→ 対応するIdPを立ち上げるか
→ または**識別子を定義**

サービスはプロジェクト識別子を扱えるようにする必要

研究データ管理における認証・認可／アクセス制御の課題

再掲

- 産官学の共同研究における障壁
  - 産官の研究者であることをどのように認証するか；**産官の研究者の ID は何（が適切）か**
- 国際共同研究における障壁
  - **海外の大学に所属する研究者をどのように認証するか**
- 組織を越えたグループ管理の要件
  - **グループはどのように構成されるのか？**
  - 認可／アクセス制御をどのように行うのか？
    - Identity-based, Role-based, Attribute-based
- 認証保証レベル
  - サービスに送られる認証情報；身元確認＋当人認証＋α
  - 身元確認の保証度 (IAL: Identity Assurance Level)
  - 当人認証の保証度 (AAL: Authenticator Assurance Level)
    - 例：写真付きIDで身元確認をし、オンラインでの認証ではパスワード認証に加えワンタイムパスワードに基づく２要素めの認証を課す
  - **このような保証度の違う認証をどのように利活用できるか？**

まとめ

- 研究データ管理における認証・認可に係る課題を、次世代認証連携における取り組み、特に認証に関する取り組みがどのように解決しようとしているのか
  - 新しい学認 IAL/AAL
  - 認証器レジストリ
  - 認証プロキシサービス Orthros
  - 学認対応 IdP ホスティング

- 触れられなかった話題
  - 異動に伴うサービス利用の継続性を担保する