NII 学術情報基盤オープンフォーラム 2024
認証トラック２

認証プロキシサービス Orthros について

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

次世代認証連携における問題と課題

- 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
- 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

IAL：Identity Assurance Level
AAL：Authenticator Assurance Level
IdP：Identity Provider
SP：Service Provider

Orthros - 何を解決するのか？

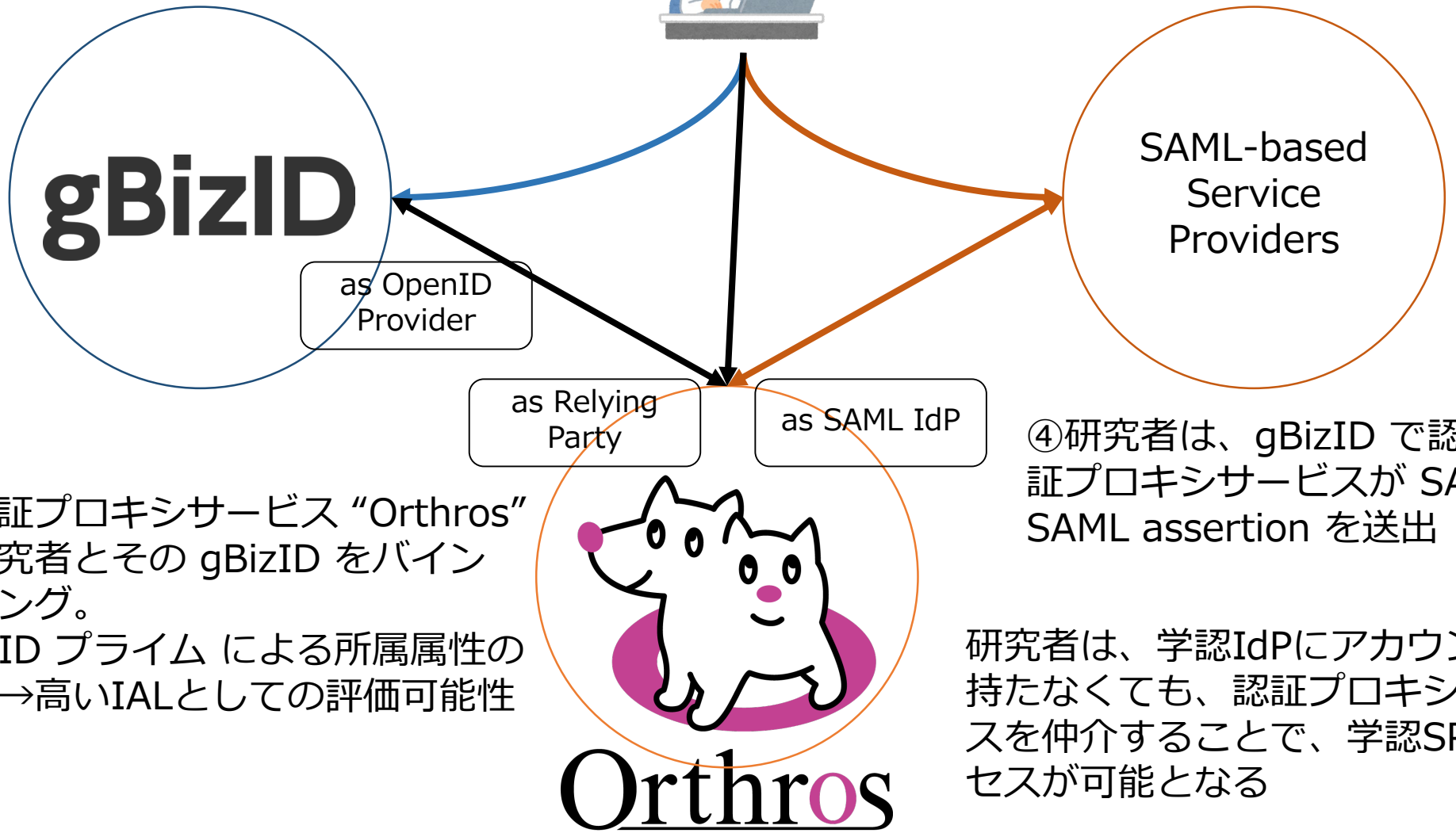
- IdP 拡大
  - 学認への参加を促進
    - 学認 IdP 構築運用支援 - 学認対応 IdP ホスティング
  - **学認への参加が難しい機関（の研究者）を支援**
    - 企業の研究者
    - 自治体等に在籍し研究活動に資する方
    - その他

- 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



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

Orthros 基本設計

- 目的
  - 利用者の身元保証、認証強度を、連携する SP に対し担保する
  - enhancement of AL
  - binding / aggregating
- 利用者の属性
  - 基本4情報（住所、氏名、生年月日、性別）
  - 所属機関（大学、研究所、会社、…）
  - その他（所属属性に関連のある、IdP/所属機関 から送出/担保可能なもの）
- 保証度が依存する何か
  - Orthros で閉じる確認手続き
  - 外部ID基盤（個人による紐付け）
  - 「機関」管理（「機関」管理者）
    - 「機関」~=部局ないしそれに準ずる部分集合、研究プロジェクトなど
- 認可・アクセス制御に利用する属性
  - 上述の利用者属性以外は扱わない
  - 認可・アクセス制御に利用する属性管理機構を別途議論する
    - Role-based, Attribute-based (except Identity-based)

令和6年度計画

- 外部ID基盤接続（本運用環境）
  - 企業の研究者のIDとして
- 新しい学認 IAL/AAL 対応
  - 外部ID基盤認証から SP アクセスまでのユースケースを検討・試行
    - 認可・アクセス制御のための要件も考慮
    - SP: GakuNin RDM, …
- 運用ポリシ・運用規程との整合性をとりつつ試行評価
  - Credential Policy / Credential Practices Statement

- 他の外部ID基盤接続（随時）