NII 学術情報基盤オープンフォーラム 2023
認証トラック３

# 学認が目指す次世代認証連携

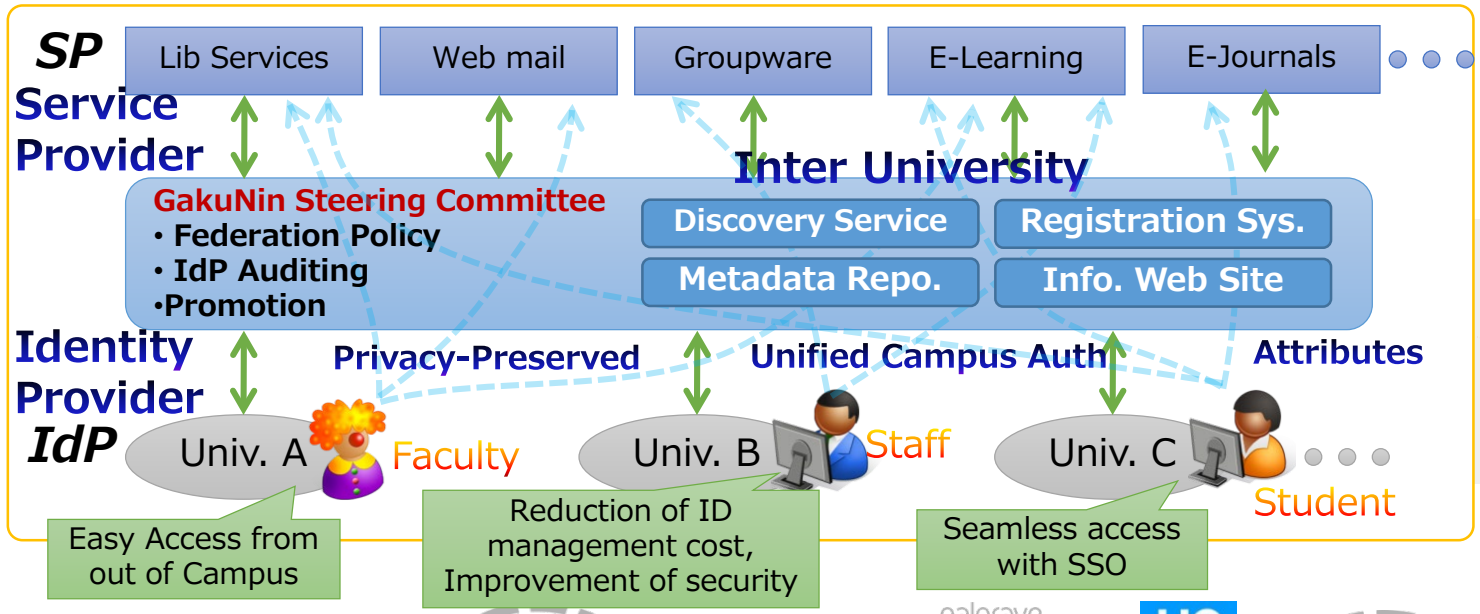
坂根 栄作

国立情報学研究所
アーキテクチャ科学研究系／学術認証推進室

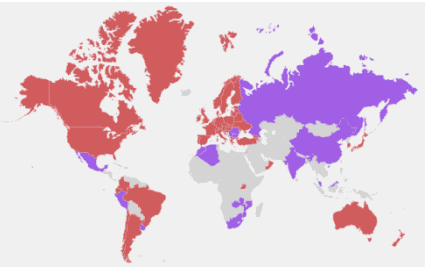
2023/05/30

# 学術認証フェデレーション

- 学認は、サイバー空間における円滑な学術活動を支援すべくトラストフレームワーク（ポリシ、技術、評価）を提供
  - 全学的なサービスに対してうまく機能



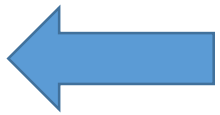

Academic Federations have been established per country basis



# 研究・教育DXを推進するために

- 研究・教育データ流通の加速が必須
  - 融合領域研究におけるコミュニティ間
  - 産学連携
  - 国際連携
- データ流通の加速には、全学的なサービスだけでなく、多種多様なサービスの円滑な利活用が必要

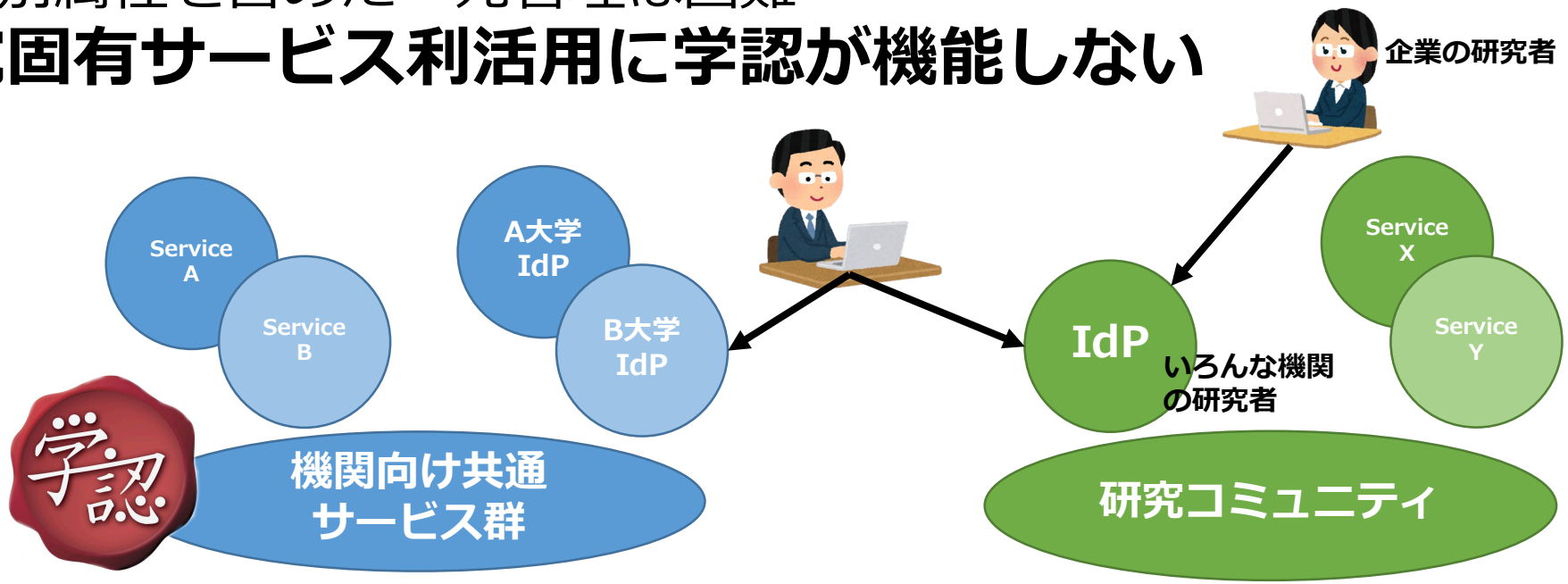
- データ流通において、認証認可は極めて重要
  - データを、誰が提供するのか
  - データに、誰が参照するのか



**複雑化**

# 多様なサービスの円滑な利活用

- 課題：機関(全学)共通サービスからより多様なサービスへ
  - 研究者は、機関共通サービスだけではなく、研究固有のサービスを利用
  - 研究固有サービスの認証認可における要件も多種多様：
    - 利用者と ID データとの紐付け度合い
    - 利用属性
  - 大学(ID管理者)は、多種多様な研究者が存在するため、共通属性以外の個別属性を含めた一元管理は困難
- **研究固有サービス利活用に学認が機能しない**



# 研究・教育DXを推進するために（続き）

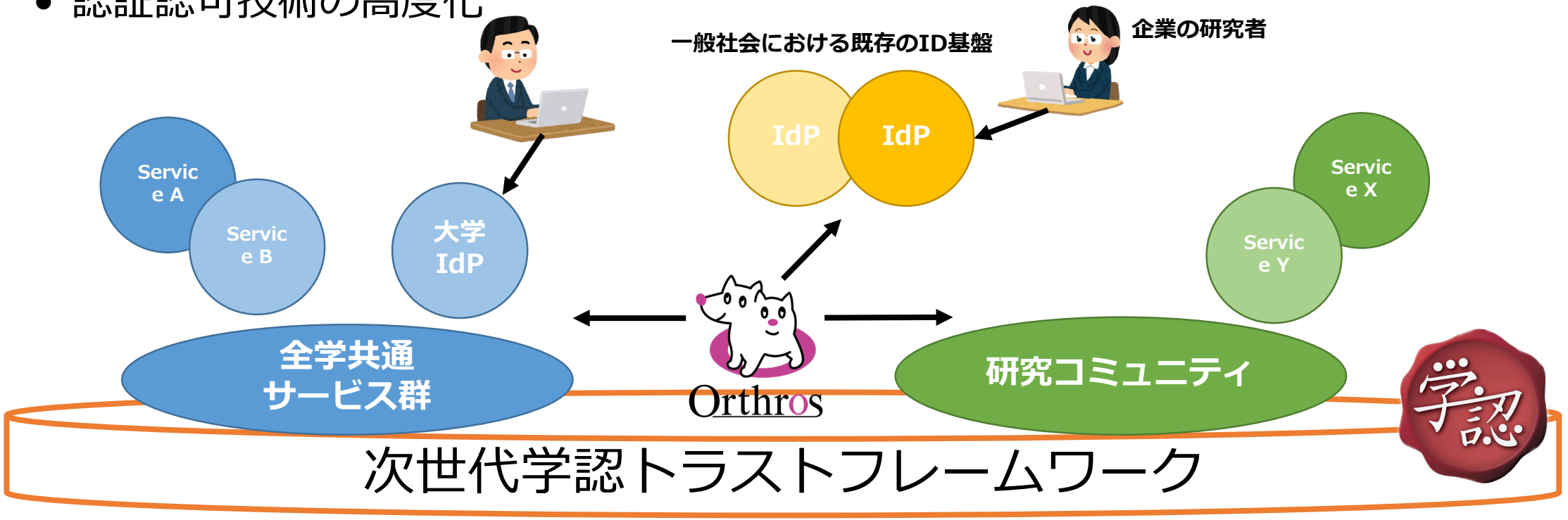
- 研究・教育データ流通の加速が必須
- データ流通において、認証認可は極めて重要
  - データを、誰が提供するのか
  - データに、誰が参照するのか

- コミュニティ単体で対応することの限界
  - 独自のトラストフレームワークに基づいた基盤運用は持続可能か？
  - コミュニティ間でデータ流通を加速させるには？

- 研究・教育DXを推進する新しいトラストフレームワーク
  - 認証ポリシの相互運用性
    - Identity Assurance Level (IAL), Authenticator Assurance Level (AAL)
  - 認証認可技術の高度化

# 次世代認証基盤研究開発の必要性

- 学術の研究・教育DX推進には、研究・教育データ流通の加速が必須
- データ流通の加速には、多種多様なサービスの円滑な利活用が鍵
  - 異種サービス間、異種コミュニティ間でのデータ共有
- **研究・教育DXを推進する新しいトラストフレームワークの確立**
  - 認証ポリシの相互運用性 (IAL, AAL, FAL)
  - 認証認可技術の高度化



# 新しいトラストフレームワーク

参加IdP数の更なる拡大

認可機能の高度化
・グループ機能

IdPs

IdP-SP 仲介
・IAL/AAL マッチング
・既存ID基盤連携

SPs

認証器の利活用

本人確認の保証度、認証強度の明確化
・どの程度の本人確認が実施されているのか
・どの程度の認証強度なのか

# 次世代認証連携における主要構成要素

## 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

## 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

## 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

## IdPホスティングサービス

- 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

## 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

# 作業部会およびサブWGにおける活動

- 学術認証運営委員会にて、以下の作業部会を設置
  - 次世代認証連携検討作業部会
    - 短期取組検討サブワーキンググループ

- 次世代認証連携検討作業部会
  - IAL/AAL 評価基準および認定手続きの検討
  - AAL 技術支援の検討
  - persistent ID の検討

- 短期取組検討サブWG
  - IAL2/AAL2 の認証試行開始に向けて
    - まずは試験的 IdP/SP で実証実験を実施
    - 各大学の実運用 IdP への展開に向けた課題整理
    - 中規模実証実験参加機関を募集

# 規準策定の取り組み

- 身元確認：IAL2 規準の策定
  - “IAL2の新学認での運用に当たって（案） Version 2”
  - 多くの大学等で達成が可能 -- Trusted DBの運用を前提
  - 組織外の研究者を受け入れる研究機関でも対応可能
    - eKYC 対応
- 当人確認：AAL2 規準の策定
  - “AAL2の新学認での運用に当たって（案）”
- お知らせ：次世代認証連携検討作業部会に係る資料の公開について
  - https://www.gakunin.jp/news/20221115
- 国際連携
  - IGTF, REFEDS, FIM4R, APAN, InCommon, …

# 連携強化

- FIDO Alliance との連携
  - NII（学認）が、FIDO Alliance の Liaison Partner として協同することについて MoU を締結（2023年5月24日付）
  - https://fidoalliance.org/members/liaison/

# 次世代認証連携における主要構成要素（再掲）

## 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

## 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

## 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

## IdPホスティングサービス

- 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

## 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 タイムライン