ネットワーク越しの
アナタは誰？
-- サイバー空間における認証 --

坂根 栄作

国立情報学研究所
アーキテクチャ科学研究系

お品書き

- 認証とは…その勘どころ
- 認証と認可…認証連携
- 次世代認証連携実現に向けた NII の取り組み

認証の必要性

- インターネット上では様々なやり取りが行われています
  - 例えば、インターネット通販を利用することを考えてみましょう

  - アナタは、何かを買おうとしています
  - 販売しているのは誰か、どうでもよくはないですよね？

  - アナタは、何かを売ろうとしています
  - 注文しているのは誰か、どうでもよくはないですよね？

認証の必要性（続き）

- インターネット上では様々なやり取りが行われています
  - 誰かが、何かをします
  - 「誰かが、何かをする」のを別の誰かが把握します
  - 「誰か」に焦点をあてると、誰なのかが重要な場合と、そうでない場合があります
  - 程度の差はあれど、今や「誰」なのかが重要な場合が増えています

認証とは…

- モニタ越しに居る誰かをどのように認識するか、考えてみましょう

認証方法：IDとパスワード

- インターネットのサービスを利用する際に、しばしば ID とパスワードによる認証が求められます
  - ID：そのヒトを識別するもの
  - パスワード：その ID と紐づく、そのヒトしか知らない合言葉

- 認証される側
  - ID とパスワードを入力することにより、ID に紐づくヒトであることを証明する

- 認証する側
  - 入力された ID とパスワードを、**事前に作成した帳票**と照合し、確認する

認証方法：IDとパスワード（続き）

- インターネットのサービスを利用する際に、しばしば ID とパスワードによる認証が求められます

- 認証する側
  - ヒトと ID とを紐づける
  - パスワードを、認証される側と共有する
- 認証される側
  - 自分の ID を把握する
  - パスワードを設定（し認証する側と共有）する

- 認証される側
  - ID とパスワードを入力することにより、ID に紐づくヒトであることを提示する
- 認証する側
  - 入力された ID とパスワードを、事前に作成した帳票と照合し、確認する

ネットワーク越しのアナタは…

- ID とパスワードが正しく照合できれば

サービス利用手続き

- とあるオンラインサービスの利用登録を思い浮かべてみましょう

- 利用者側
  - 名前、生年月日、年齢、性別、住所、電話番号、電子メールアドレスなどを入力する
  - ID を把握し、パスワードを設定する

- 提供者側
  - 利用者、利用者情報のセット、ID とパスワードとを紐付ける

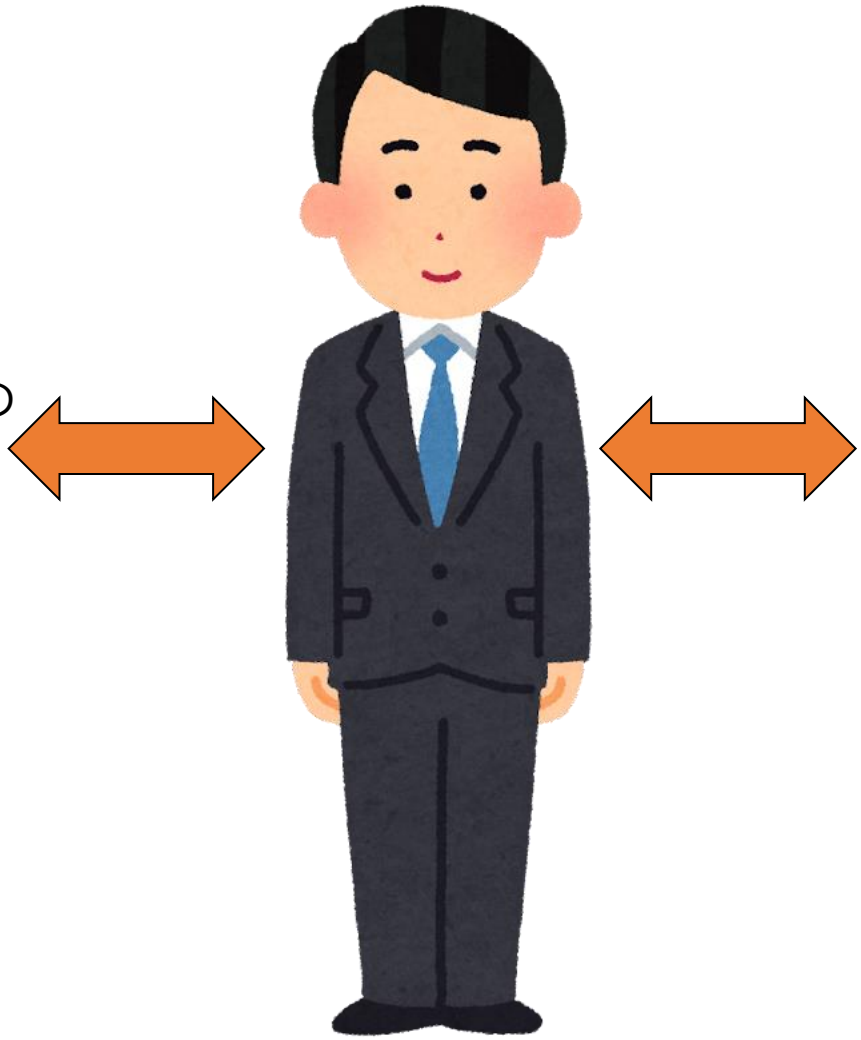
- サービス利用時の認証
  - ID・パスワードによる認証

ネットワーク越しのアナタは…

- ID とパスワードが正しく照合できれば

利用者自身、利用者情報、合言葉

ID とパスワードの提示



- 氏名
- 生年月日
- 年齢
- 性別
- 住所
- 電話番号
- メールアドレス

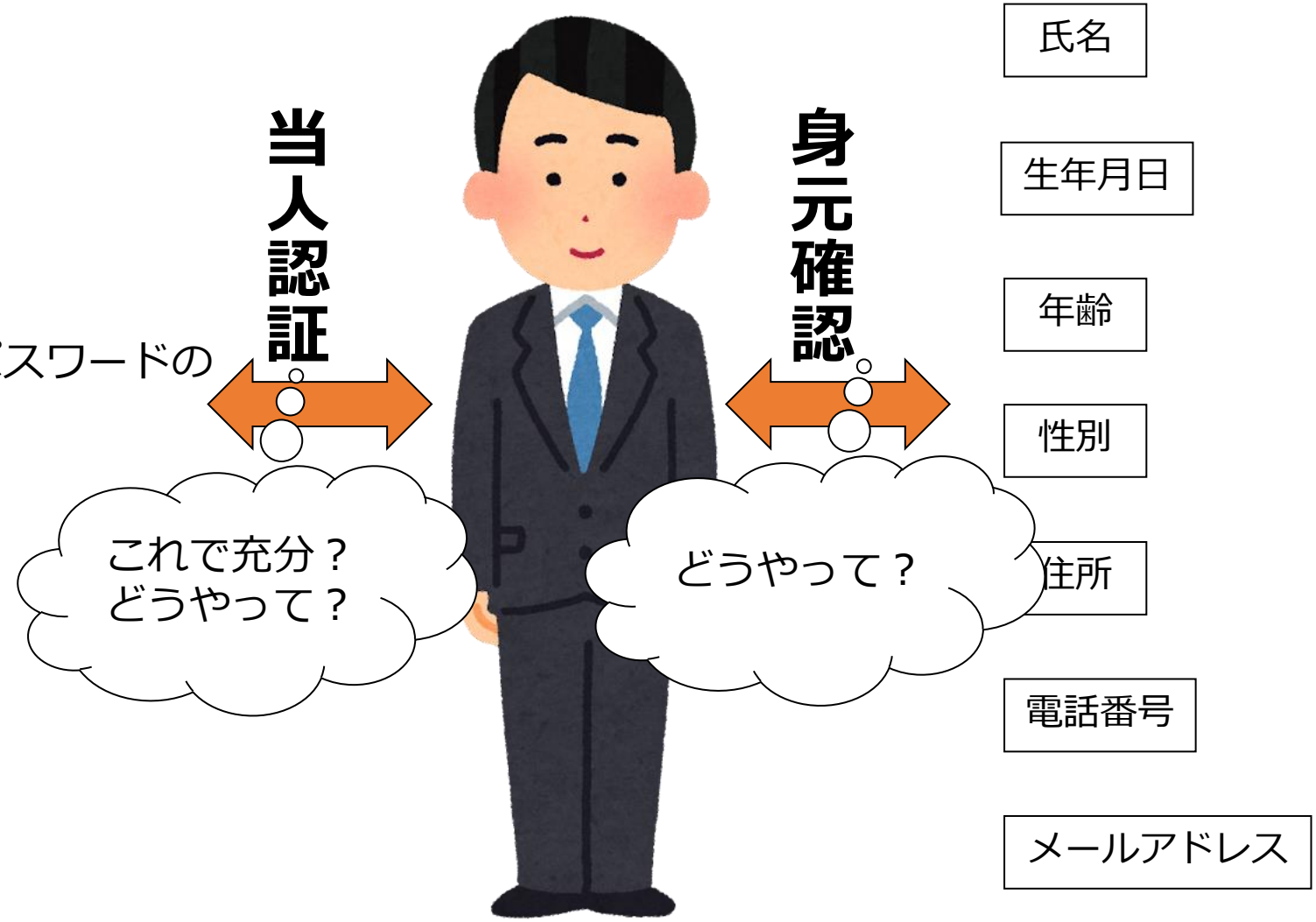
身元確認と当人認証

- 身元確認とは、利用者当人の実在性を確認すること
  - 登録するデータ（氏名・住所・生年月日等）が正しいことを証明／確認すること
- 当人認証とは、利用者の行為を確認すること
  - 例：IDとパスワードの提示

- 本人確認とは、両方の組み合わせを通じて行うもののこと

経済産業省, NEDO, PwC「オンラインサービスにおける身元確認手法の整理に関する検討報告書（概要版）」（https://www.meti.go.jp/press/2020/04/20200417002/20200417002-1.pdf）（検索日：2023年10月1日）

本人確認：身元確認、当人認証



本人確認の保証度

- 身元確認や当人認証は、それらのやり方次第で保証度に違いがある
- 身元確認：**Identity Assurance Level (IAL)**
  - 例：氏名と住所と生年月日を確認する方法は…
  - 自己申告のみ（何も確認しない）
  - 公的身分証（の写し）を活用して確認する
  - 対面で、かつ、公的身分証を活用して確認する
  - IAL1(低) → IAL2 → IAL3(高)

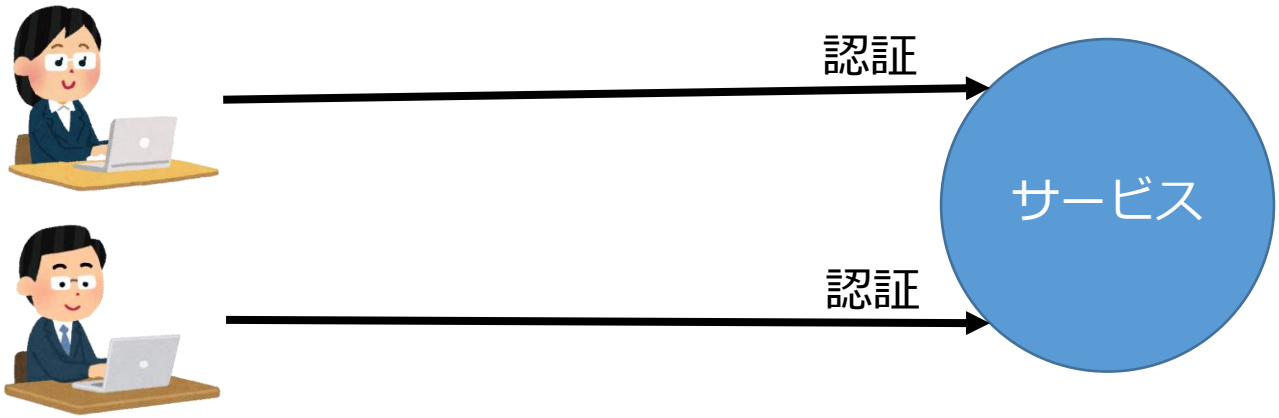
- 当人認証：**Authenticator Assurance Level (AAL)**
  - ID・パスワードの提示以外の別の手段はあるのか？

  - 認証要素（知識、所持、生体）の整理から多要素認証へ
  - AAL1(低) → AAL2 → AAL3(高)
  - 単要素 → 多要素

認証認可の分離、
認証連携へ…

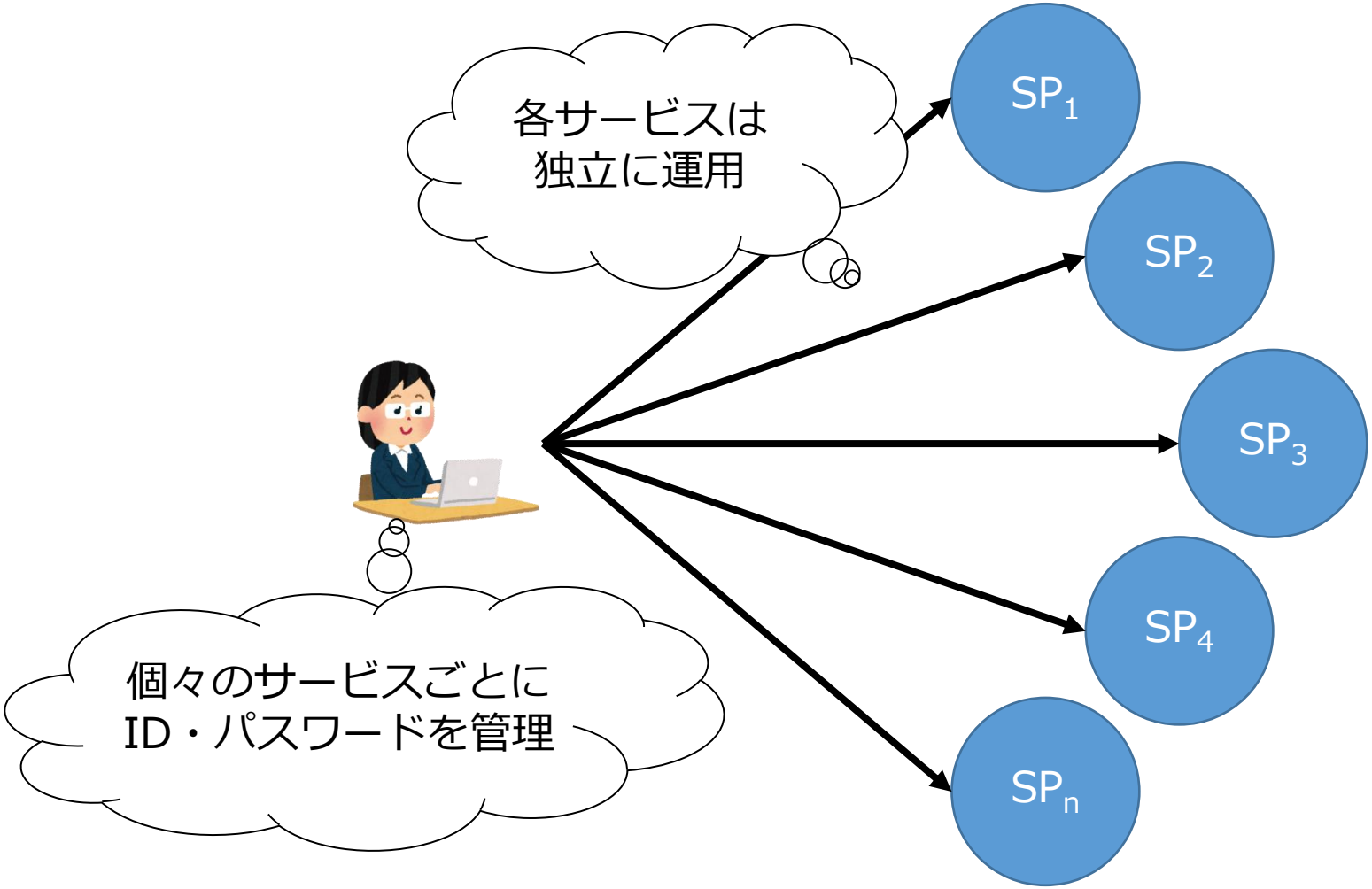
認証認可分離以前

- とあるオンラインサービスの利用を思い浮かべてみましょう
  - サービスは、利用者登録をした利用者に対してのみ提供されるものとします
  - サービスは、そのサービスを利用しようとするヒトに対して認証を行います
  - 認証が成功すれば、そのヒトは正規の利用者であることが確認され、サービスを利用できます



認証認可分離以前：利用者視点

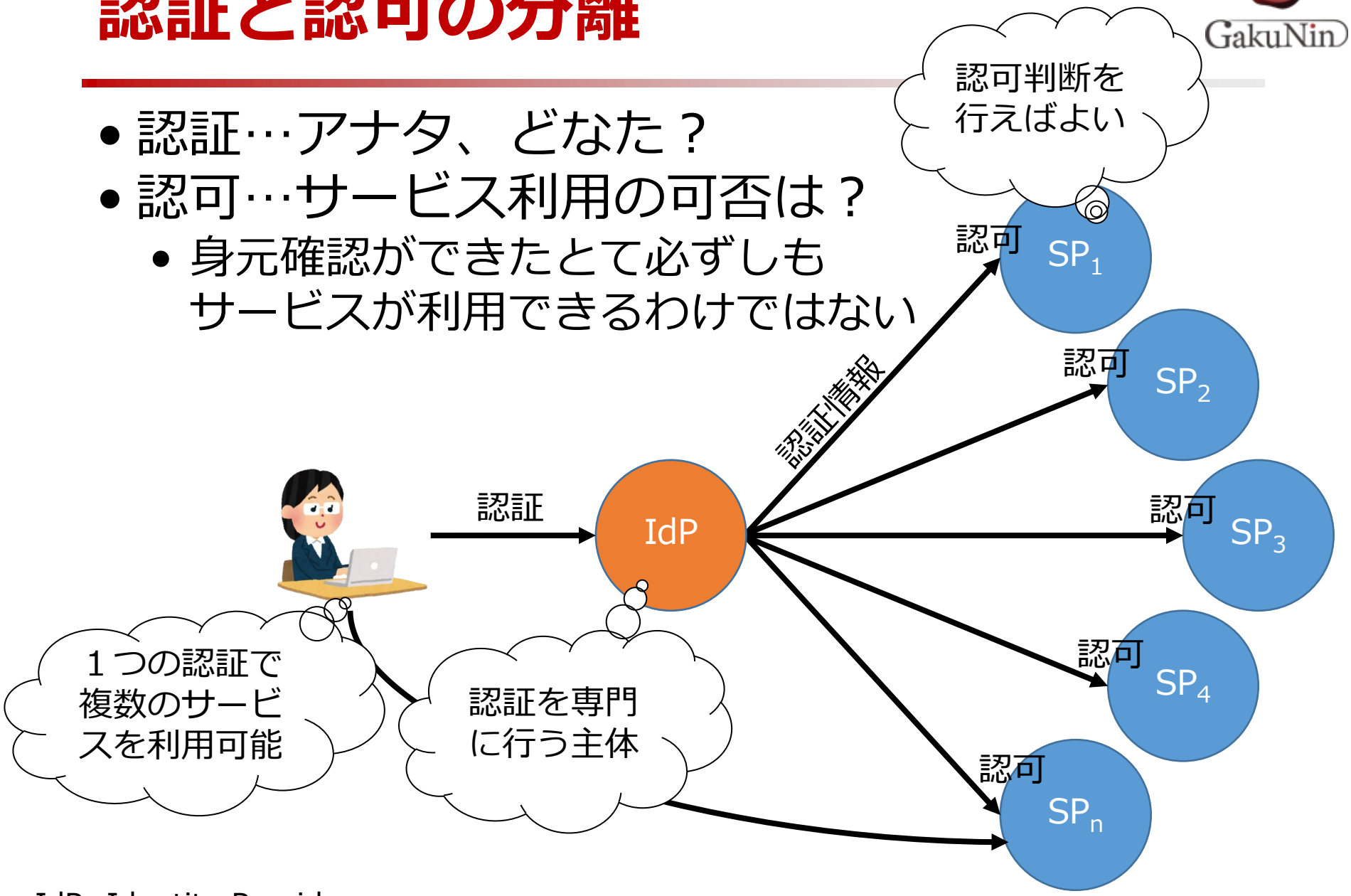
- 利用者は様々なサービスを利用する



SP: Service Provider

認証と認可の分離

- 認証…アナタ、どなた？
- 認可…サービス利用の可否は？
  - 身元確認ができたとて必ずしも
    サービスが利用できるわけではない



IdP: Identity Provider

認証認可分離後

- 利用者視点
  - サービスごとのID・パスワード管理からの解放
- SP 視点
  - 利用者を認証するための照合データ管理からの解放
  - 認可判断だけを行えばよい
    - 判断基準によって、認可条件を簡素化

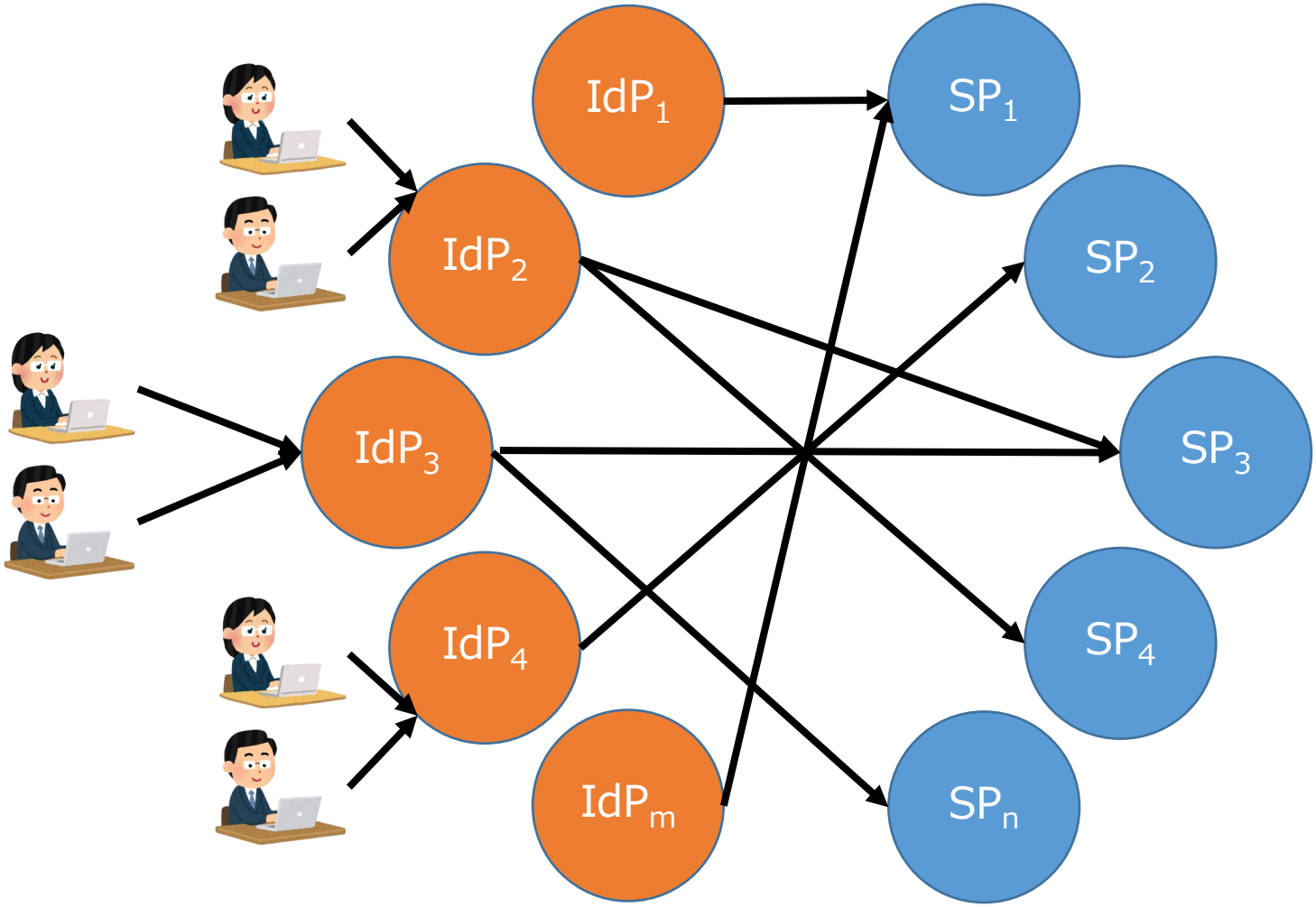
- IdPでの認証結果を複数のSPに対してうまく連携することにより、１回の認証で複数のサービスを利用可能（シングル・サインオン）

学術サイバー空間では

- 利用者：研究者、学生
- IdPを担う主体：大学や研究機関
  - 構成員（学生、教職員）の認証を行い、
  - その結果をSPに送る
- SPの例
  - 電子ジャーナル
    - 認可判断：大学に所属していること（が保証されていればよい）
  - 学生割引サービス
    - 認可判断：学生であること

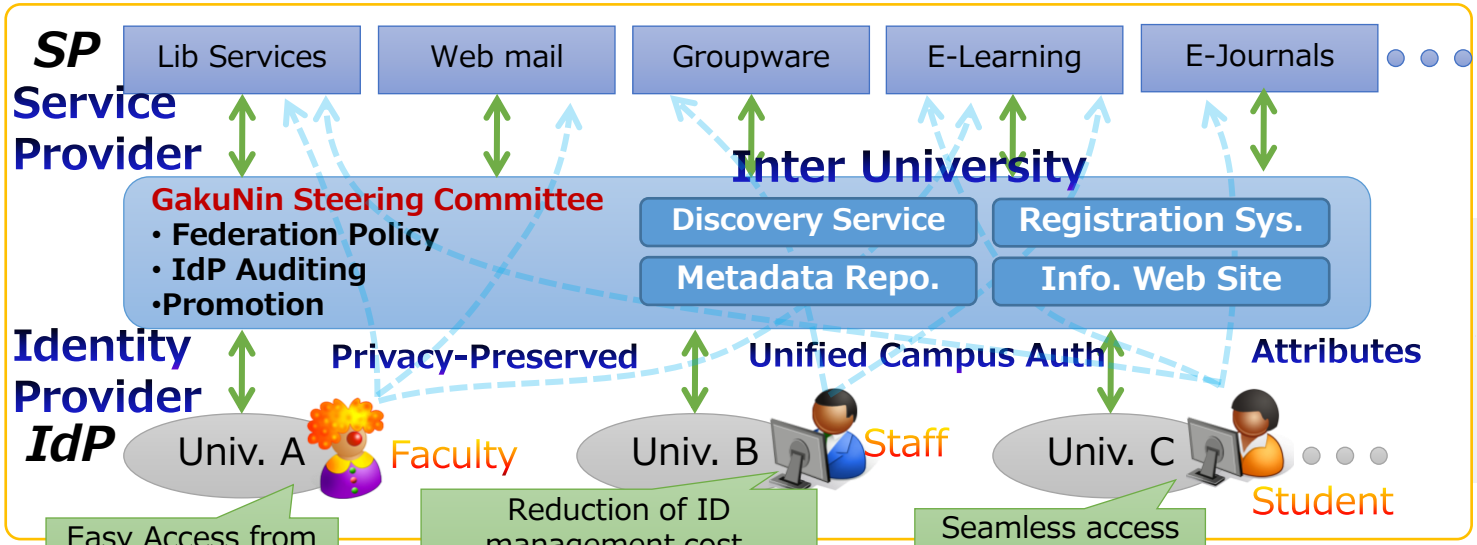
フェデレーションの必要性

- 認証情報のやり取りの標準化が必要
  - 認証フェデレーションが標準化を提供

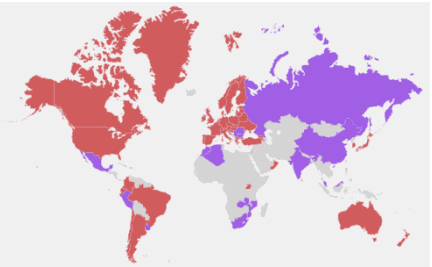


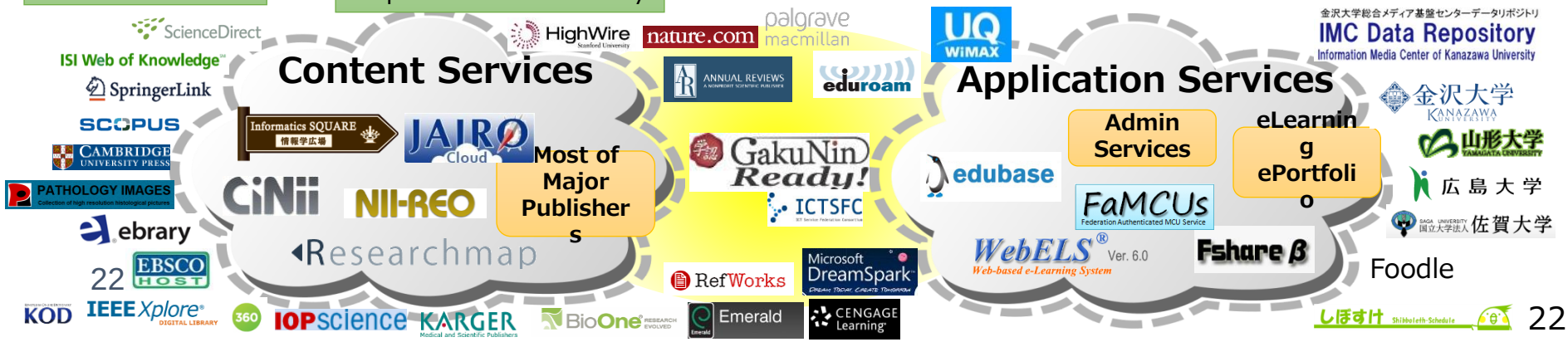
学術認証フェデレーション

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



Academic Federations have been established per country basis

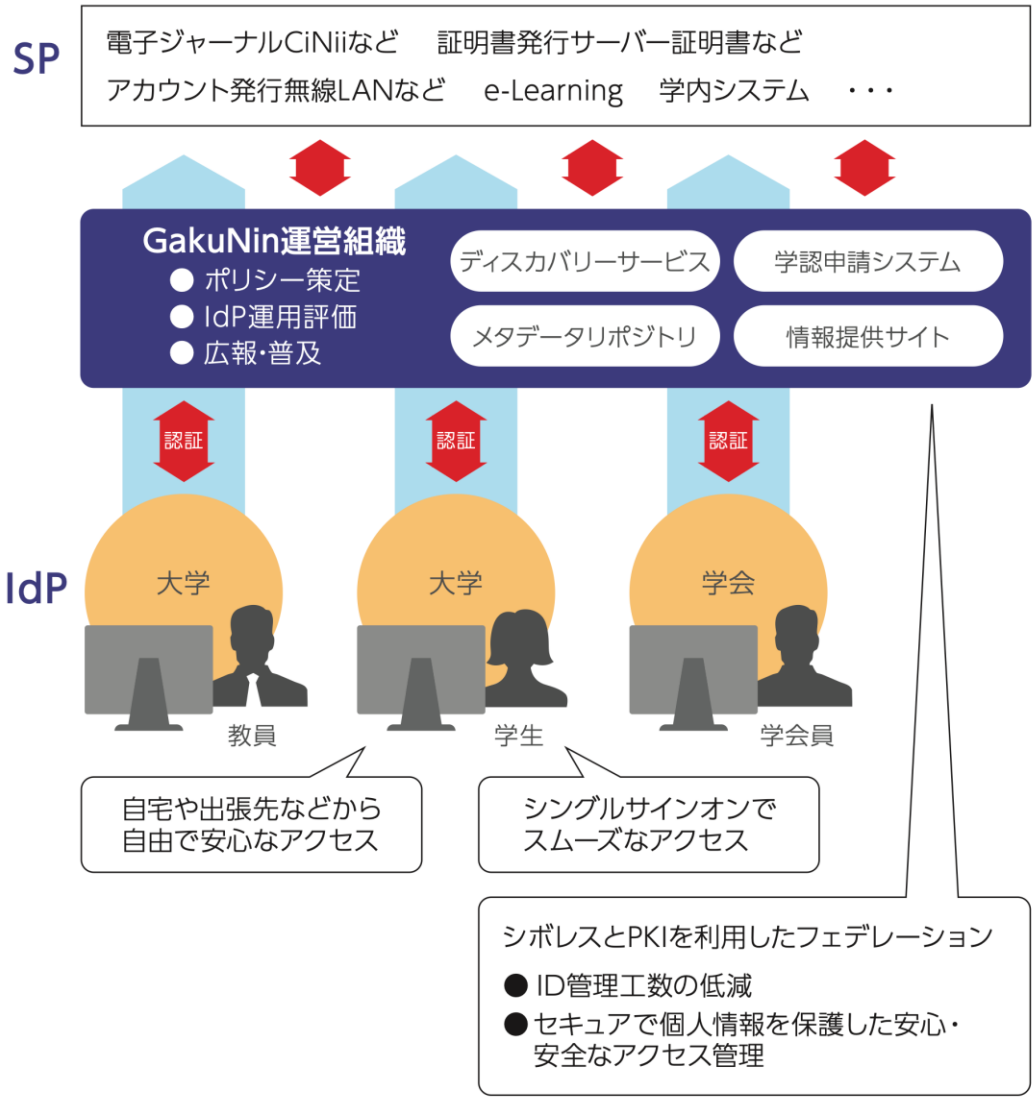




学認の概要

- 学認：日本における、学術e-リソースを利用する大学(IdP)、学術e-リソースを提供する機関・出版社等(SP)から構成された連合体（フェデレーション）
- 各参加機関は学認が定めた規程（ポリシー）を信頼しあうことで、相互に認証連携を実現することが可能となる
- 特長
  - 利用者の記憶するIDは1種類（統合認証）
  - パスワード入力は1回のみ（シングルサインオン）
  - 学内外からのアクセスが可能（リモートアクセス）
  - 必要なのはウェブブラウザのみ（別ソフト不要）
  - 多要素認証につなげる拡張性（セキュリティレベルの一元管理）

- 参加状況（2023年8月末現在）
  - 利用機関数：299
  - サービス数：207

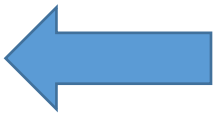


次世代認証連携に向けて

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、機関向け共通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

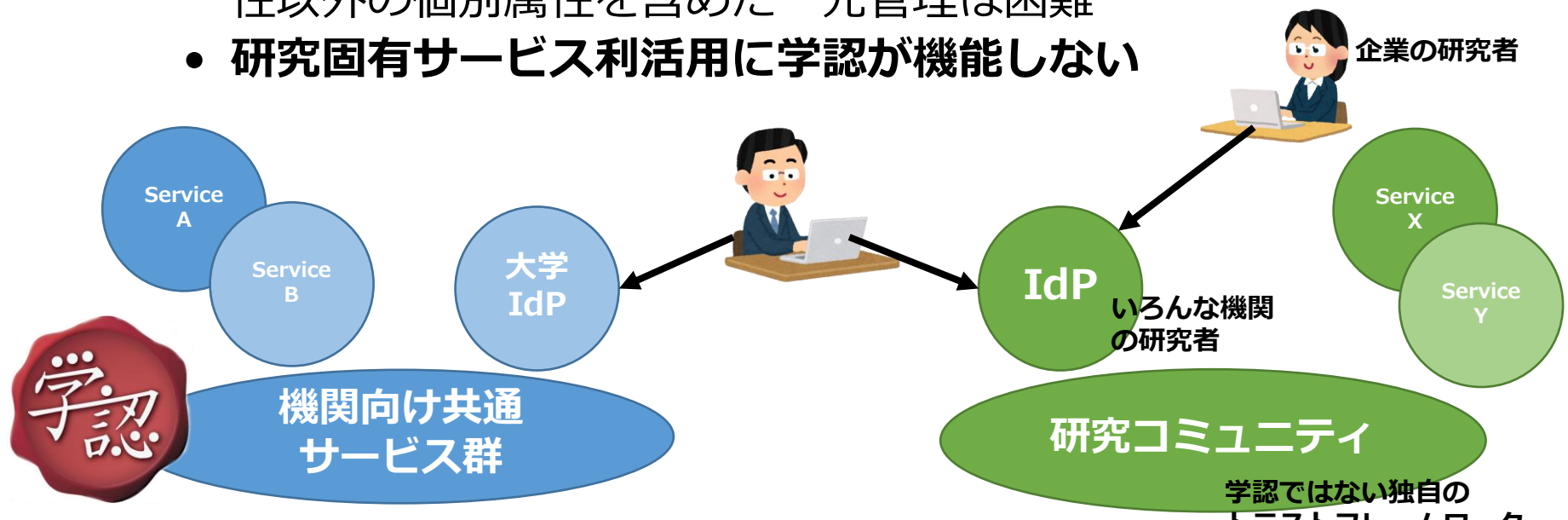
- データ流通において、認証認可は極めて重要
  - データを、誰が提供するのか
  - データに、誰が参照するのか



複雑化

学認の課題

- 共通サービスからより多様なサービスへ
  - 研究者は、機関向け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は多種多様：
    - 利用者と ID データとの紐付け度合い（本人確認の保証度、認証強度）
    - 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をどのように流通させるのか？

研究コミュニティからの要望（SP視点）

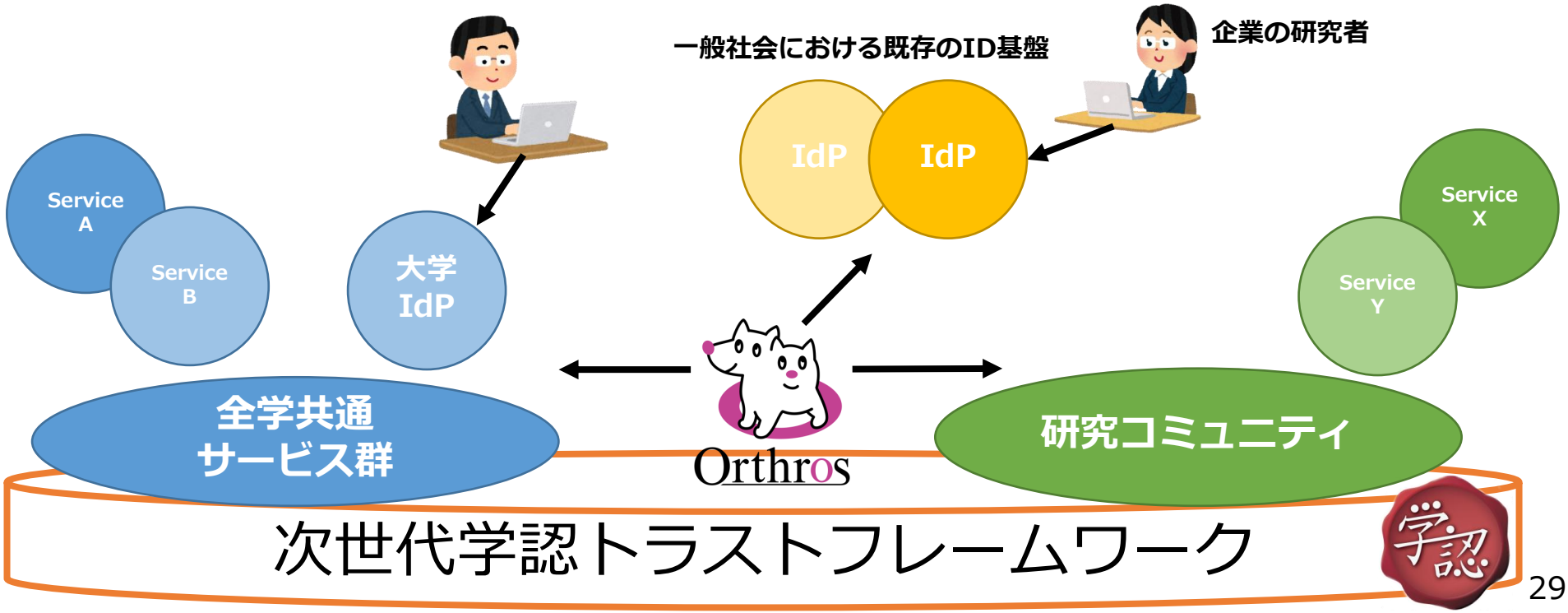
- IdP を持たない利用者の認証
  - 利用者は、必ずしも学認に参加するIdPのアカウントを所有しているわけではない
  - 信頼に足る本人確認を行っている IdP に依拠したい
- 認証レベルの把握
  - ID・パスワードか多要素か
  - 多要素認証を経た利用者のみにサービスを提供する、のようなフィルタリング

- 複数組織に所属する利用者の同定
  - 組織異動における利用者の同一性の担保
  - 組織間異動があっても情報資産利活用の継続性を担保したい
  - 例：GakuNin RDM 上の資産を継続的に利用したい

- 用途に応じた属性の提供
  - 例：居住者か非居住者かを把握したい（輸出管理）

次世代認証連携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の鍵
  - 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
  - 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

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

- 本人確認の保証度、認証強度について規定

認証器レジストリ

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

- 学認AALに基づく認証器の評価

認証プロキシサービス "Orthros"

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

- IAL/AAL matching, Credential bridging, Attribute coordination

学認対応IdPホスティングサービス

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

- 大学、研究機関のIdP構築運用の課題を解決

グループ機能の高度化

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

- より高度な認可要求に対応

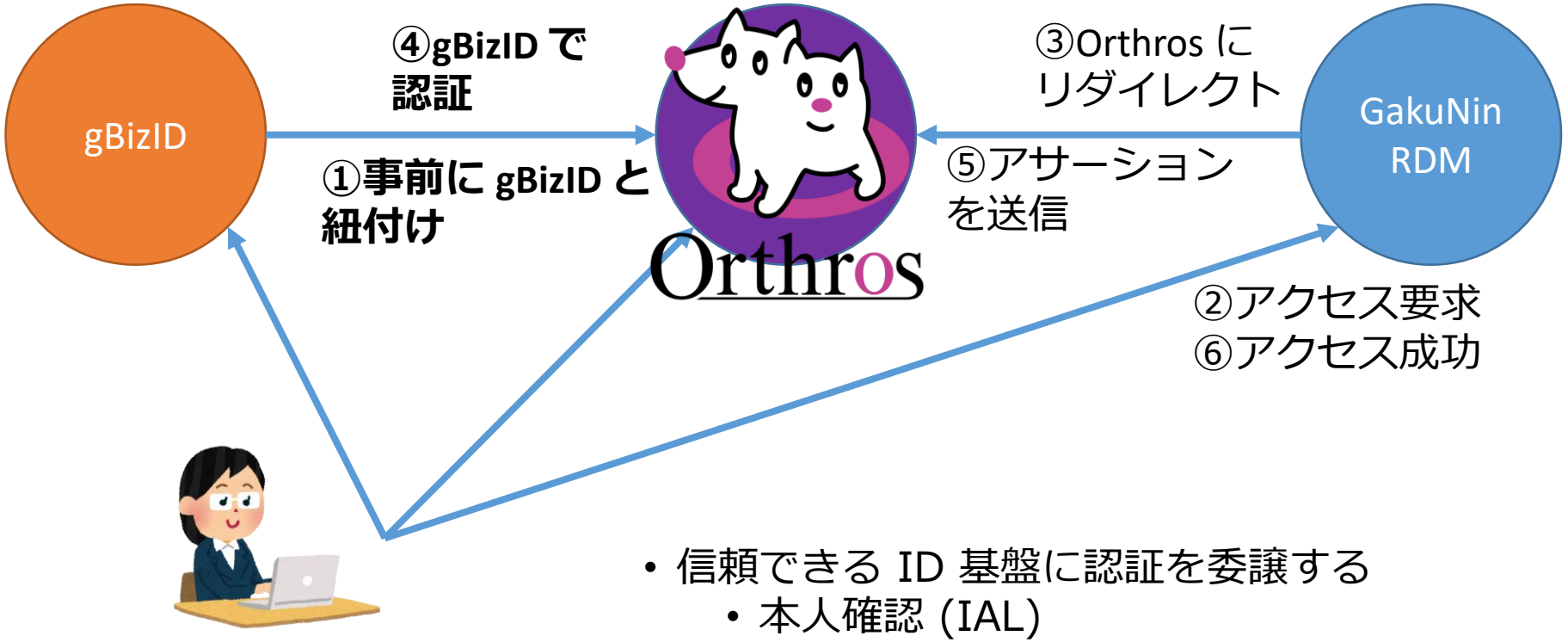
認証プロキシサービスの研究開発

- 産学連携を念頭においた SP へのアクセスにおいて、必要なID保証の担保やID連携、属性保証などに柔軟に対応する
  - IAL, AAL matching, AL enhancement
  - credential bridging (e.g., OAuth access token -> SAML assertion)

- 認証プロキシサービス “Orthros”

ユースケース１：認証情報の橋渡し

- 企業の研究者が、既存IDの認証により GakuNin RDM を利用する

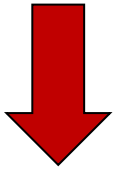


- 信頼できる ID 基盤に認証を委譲する
  - 本人確認 (IAL)
  - 認証クレデンシャル (AAL)

このようなID連携の実現を目指す

学認の目指す未来像

- 認証技術の観点から、研究･教育DXの推進に資する



- 全国の大学・研究機関の**すべて**が学認に参加している
  - 研究者・学生の基本的な ID 基盤
- 認証ポリシの相互運用性が確立されている
  - 国内のみならず海外とも
- 高度な認証認可が実現されている

まとめ

- 認証とは
  - 身元確認と当人認証
  - 保証度
- 認証認可分離から認証フェデレーション
  - 認証連携
- 次世代認証連携実現に向けたNIIの取り組み