

共同研究サービスにおけるIDaaSモデル (企業所属研究者との共同研究を可能とするしくみ)

2022年3月9日

エクスジェン・ネットワークス株式会社

江川 淳一

USE INNOVATIVE TECHNOLOGY.

1. 下位バージョン(私案)

下位バージョン

- ・ IAL 2 は現状運用でOK
- ・ AAL2は多要素認証の実装が必要
- ・ 規則縛り

大学にとっての大きな課題



フルバージョン

- ・ IAL2強化(プロトコル整備)
保証属性がIdPとSPでやりとりされる

共同研究サービスにとっての大きな課題

2. 企業所属研究者向けIDaaS設計のポイント

① 順番が大事

- ・ 共同研究サービスの整備が先行する。
 - ・ 現状は、共同研究サービスが、全研究者のIDを管理する認証基盤を保持しているケースが存在する。
←これもIDaaS (IDaaSにとってのお客様は共同研究サービス)
- ・ 新学認整備により、上記内容がどのように変化するかを計画する。

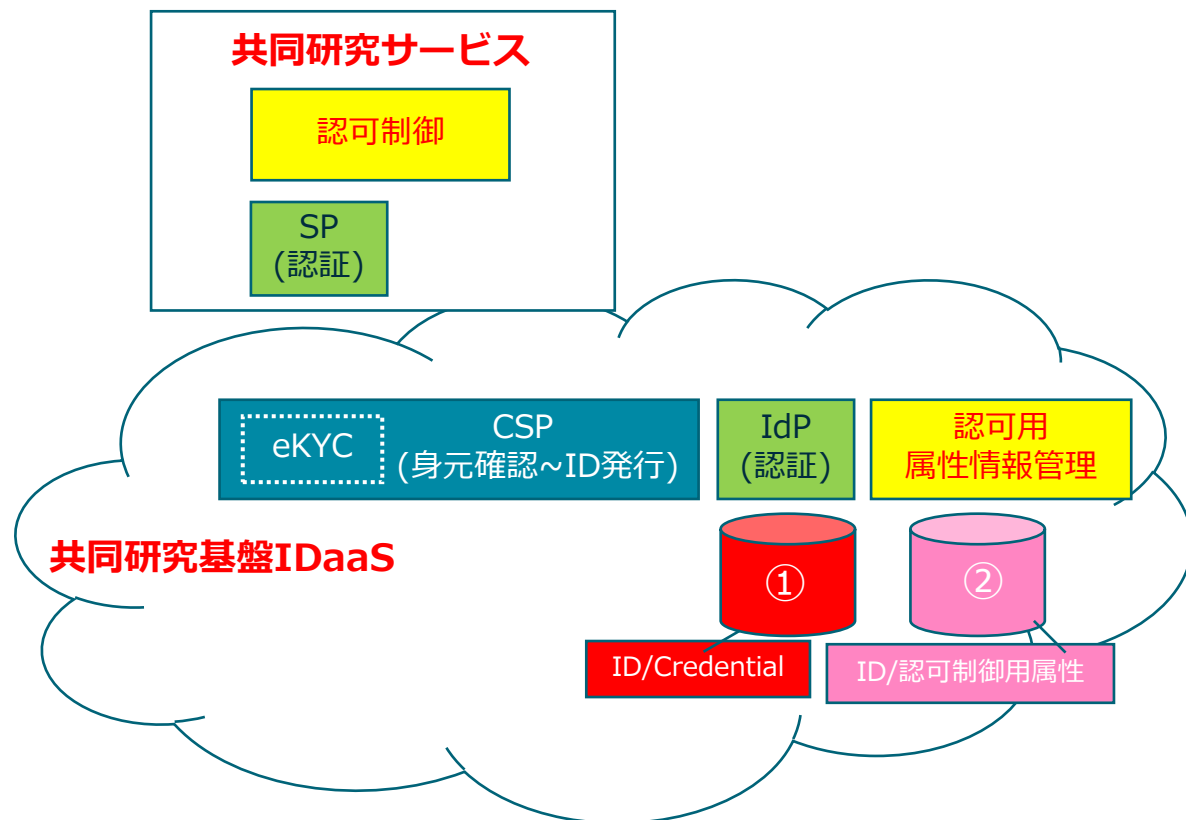
② 共同研究サービスに残るID管理機能は何か？

- ・ 共同研究サービスの認証基盤のゴールは何か？
- ・ 大学向けIDaaSと共同研究サービス向けIDaaSの違いは？

3. 共同研究サービス認証基盤の展開例

〔現在〕

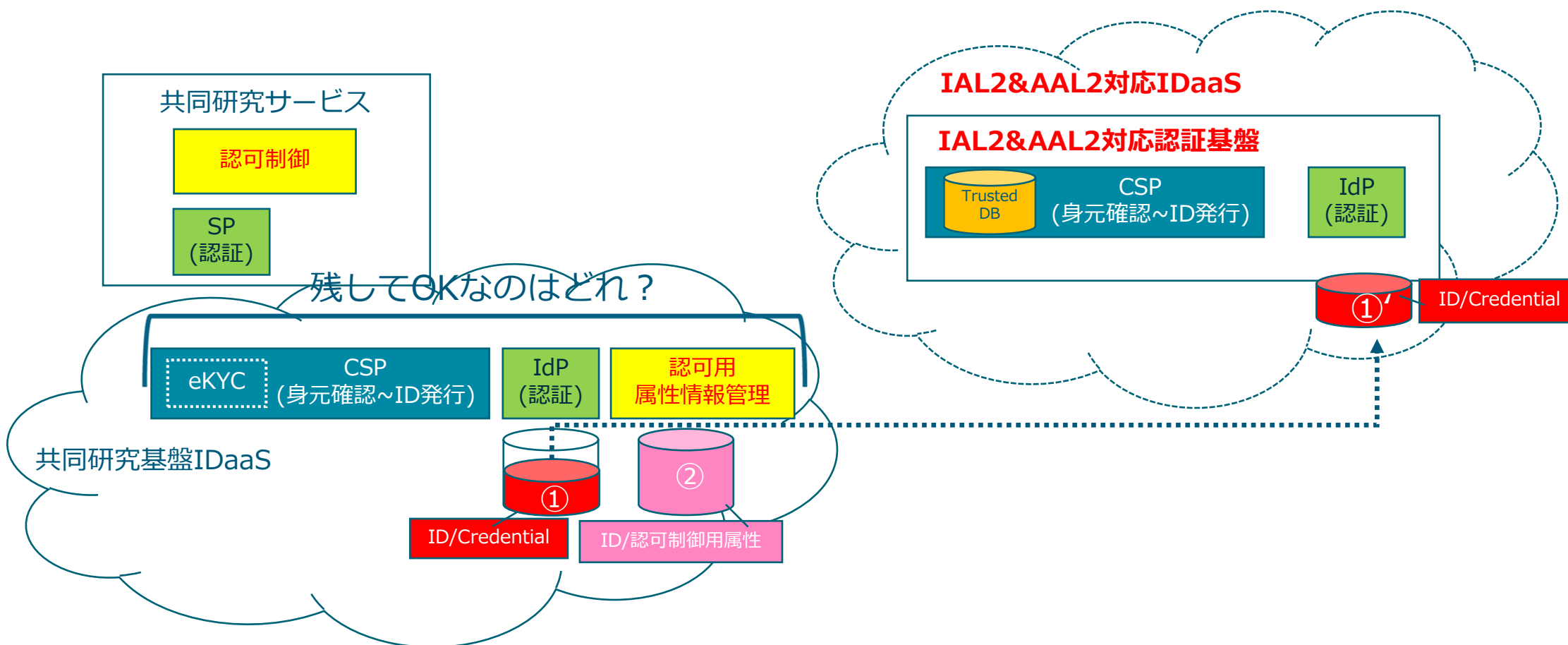
- ・ 共同研究サービスを利用するために共同研究基盤IDaaSでIDを発行、管理する。
- ・ 共同研究基盤IDaaSは、CSP、IdP、認可用の属性情報管理機能で構成される。
- ・ 共同研究基盤IDaaSで保有するID情報は、認証で利用するID情報 (①) と認可で利用するID情報 (②) の2種類。



3. 共同研究サービス認証基盤の展開例

〔STEP1〕

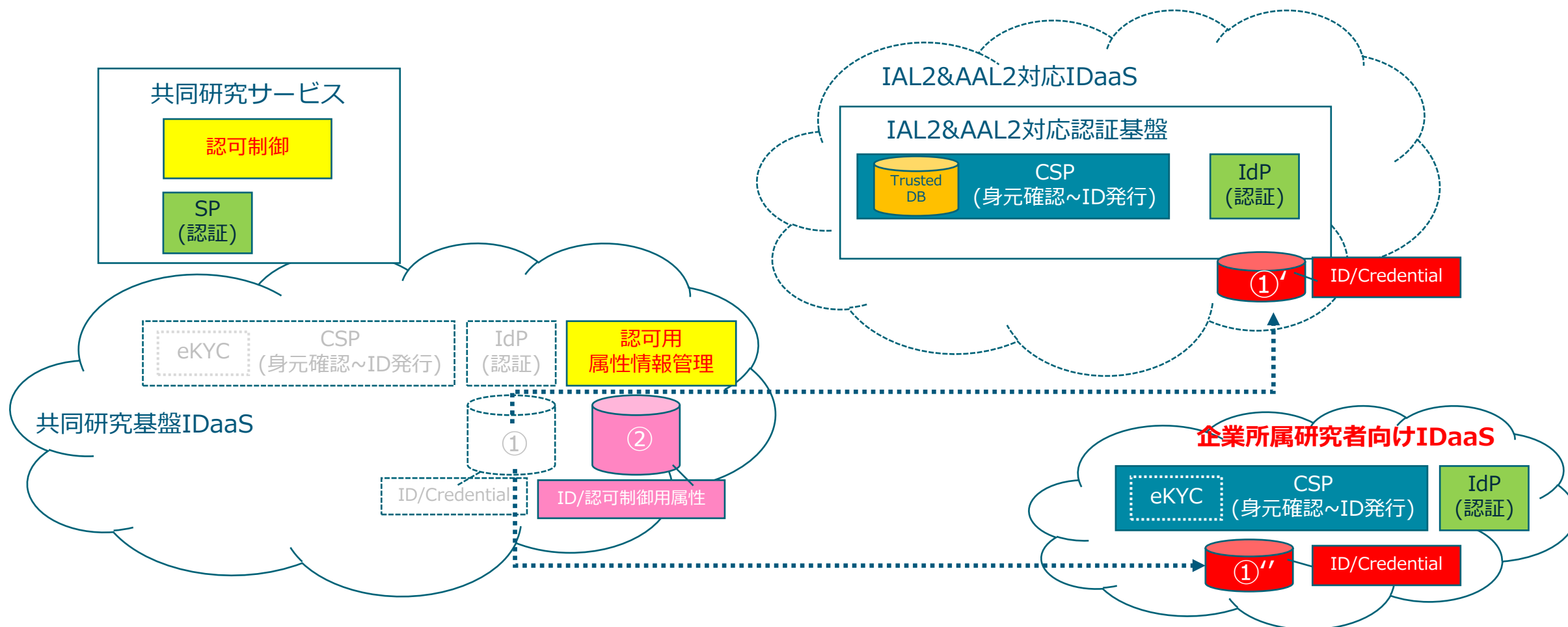
- ・ IAL2 & AAL2に対応した認証基盤を整備した組織は自組織で発行管理しているID (①') で共同研究サービスを利用できるようになる。
- ・ IAL2 & AAL2に対応したIDaaSであれば、大学はIDaaSの利用も可能。
- ・ 共同研究基盤IDaaSには、IAL2 & AAL2に未対応の組織(例：企業研究者)のID (①) が残る。



3. 共同研究サービス認証基盤の展開例

〔STEP2〕

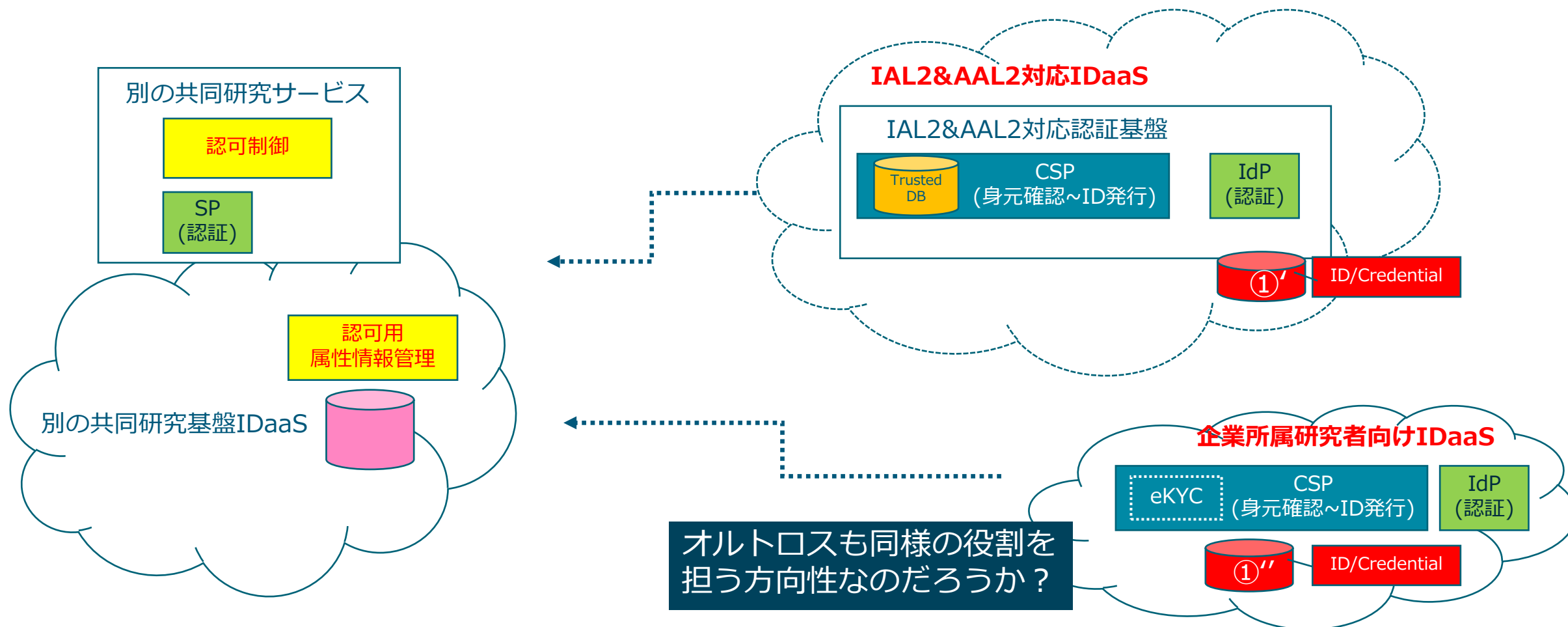
- ・ 企業所属研究者向けIDaaS (IAL2 & AAL2未対応組織用IDaaS)を作る。
共同研究基盤IDaaSには、認証で利用するID (①) はなくなる。 →①'と①''に。
IdPもCSPも不要になる。
- ・ 共同研究基盤IDaaSには、認可用属性情報管理を行うためのID (②) が残る。



3. 共同研究サービス認証基盤の展開例

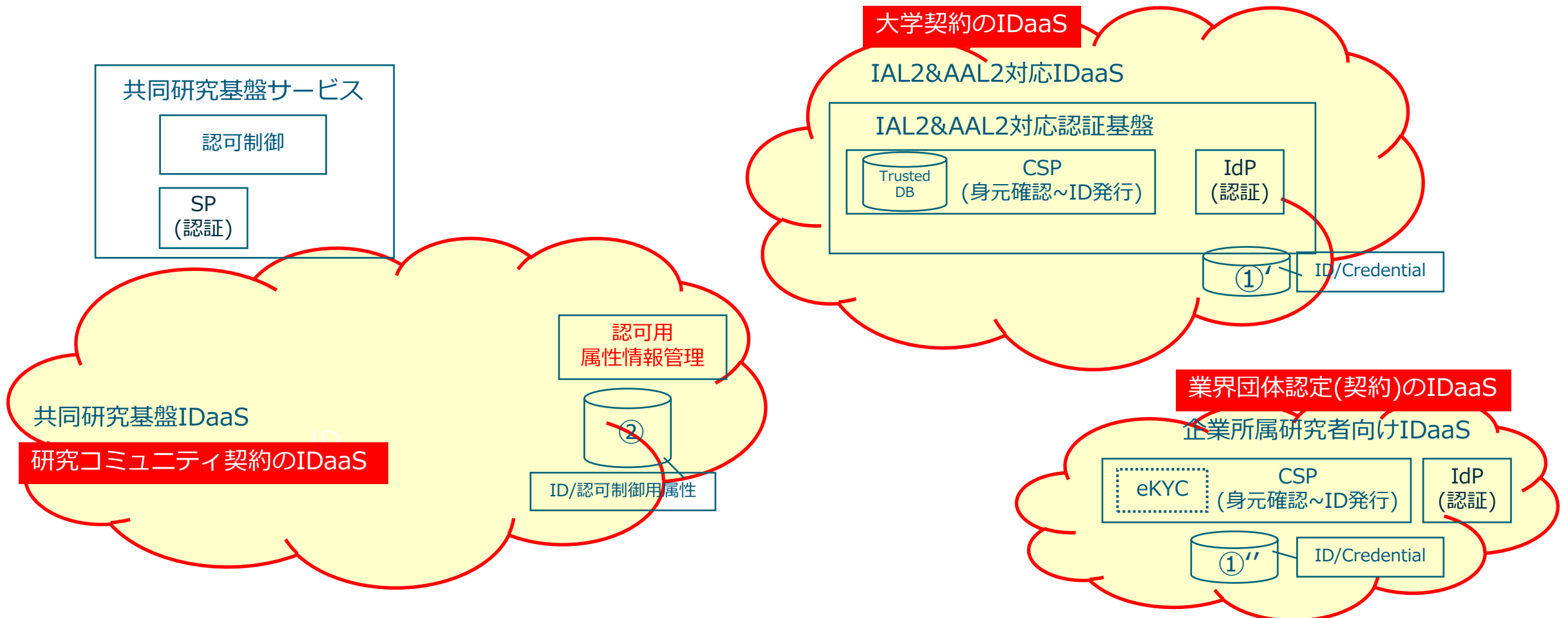
〔STEP3〕

- ・ IAL2 & AAL2対応認証基盤またはIAL2 & AAL2対応IDaaSを利用する組織(主に大学)や、企業所属研究者向けIDaaS (IAL2 & AAL2未対応組織用IDaaS)を利用する研究者(主に企業研究者)は、他の共同研究サービスも利用できるようになる。



4. 3種類のIDaaS

- ・ビジネス視点(契約先)で考えると、3つのIDaaSが存在する。
 1. 研究コミュニティ契約のIDaaS：認可用属性情報管理
 2. 大学契約のIDaaS：IAL2 & AAL2対応
 3. 業界団体認定(契約)のIDaaS：IAL2 & AAL2対応 + 業界団体のお墨付き



5. 大きな2つの課題

課題①

業界団体のお墨付き = 学認にAuthorityとしてデジタル署名してもらう。

- ・ IDaaSとしてIAL2 & AAL2の技術要素を実装しているだけではNG。
- ・ 企業研究者が所属する組織はこのIDaaSで発行、管理するIDに対して保証を付けることはできても、メタデータへの公開鍵の登録やIdPの送信情報において、デジタル署名付きAuthorityとはならない。
- ・ デジタル署名するAuthorityが必要。→学認
- ・ このIDaaSが誰と契約するかの観点から
 - ①企業所属研究者
IDaaSの課金、請求処理が煩雑となり、ビジネス観点からは、非常に実現性は困難。
 - ②共同研究サービス
これはあり得るか？
 - ③学認
これが一番良い。(マルチ共同研究サービス利用のためのインフラ)

課題②

所属確認/所属保証の方法を確立する必要がある。

- ・ 例) ホワイトリスト方式 + eKYC
 - ①所属組織が発行するメールアドレスのドメイン名をホワイトリストとしてチェックする。
 - ②NGの場合、eKYCサービスを利用し実在性の確認を行う。
- ・ 他に方式がないか。
- ・ IALのレベルとは別の規程が必要か？

6. 大きな流れ(私案)

新学認

フェーズ①
・IAL2は現状運用でOK
・AAL2は多要素認証の実装が必要
・規則縛り

フェーズ②
・IAL2強化(プロトコル整備)
保証属性がIdPとSPで
やりとりされる

フェーズ③
・企業所属研究者IDaaSと
契約

汎用
IDaaS

新学認(IAL2 & AAL2)に対応

新学認(IAL2強化)に対応

カスタム
IDaaS

共同研究基盤IDaaS

共同基盤IDaaSと
企業所属研究者IDaaSを分離

共同研究
サービス

学認RDM、NIMS、HPCI
機能拡充
共同研究サービス毎に
基盤IDaaSが整備される

1.SPとして新学認に対応
2.未対応

1.共同基盤IDaaSと
企業所属研究者IDaaSを分離
2.分離せず

大学

1.新学認に対応
2.新学認対応IDaaSと契約
3.未対応

1.新学認に対応
2.新学認対応IDaaSと契約
3.未対応

6. 大きな流れ(私案)

