新認証基盤要件と
トラストフレームワークプロバイダー
に対する要望

2021年6月30日

エクスジェン・ネットワークス株式会社　江川

USE INNOVATIVE TECHNOLOGY.

1. 新認証基盤要件

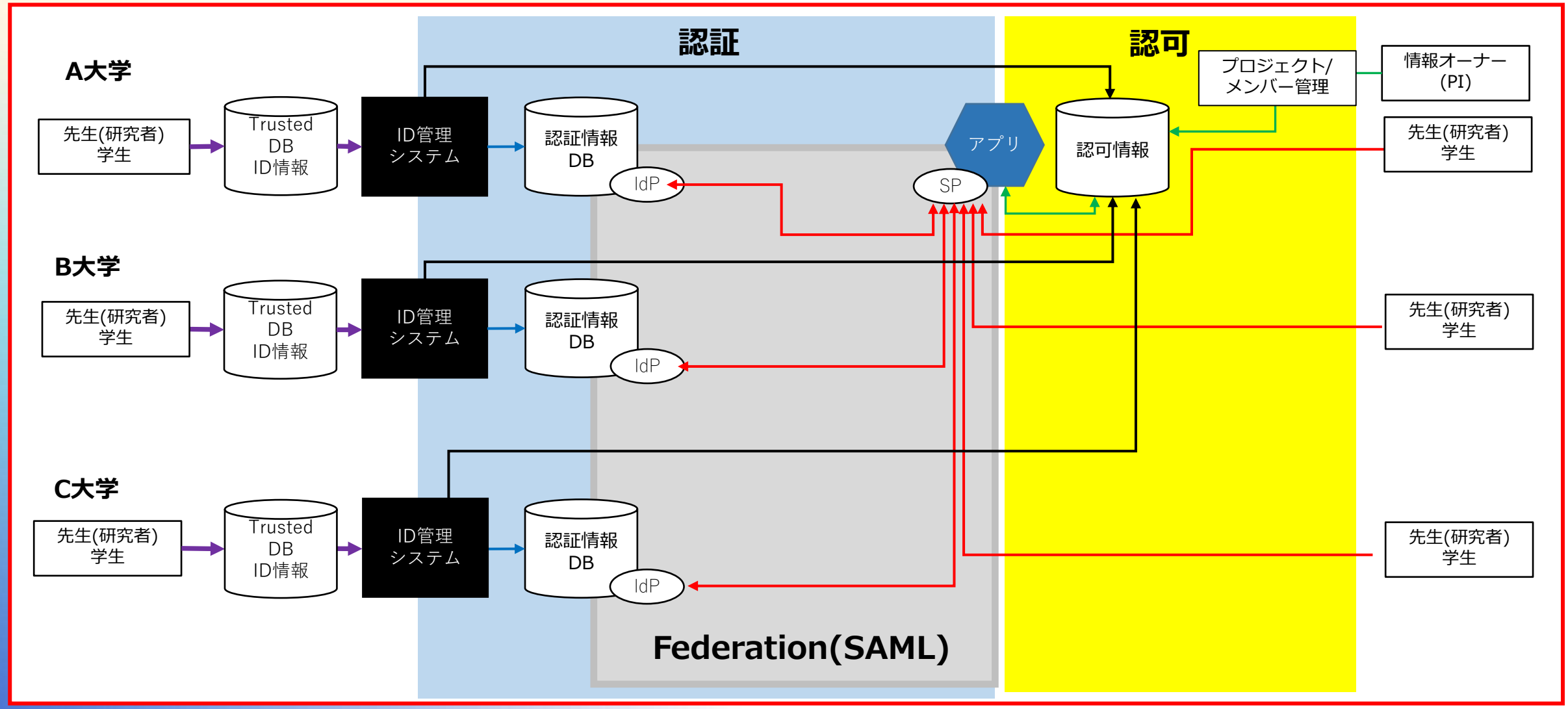
1.1 最近の認証基盤TOPICS

- **ZERO TRUST**
  - Identity is the new perimeter
  - IDを制御することでセキュリティが確保されるという考え方が主流に。
  - オンライン授業、テストをセキュアかつ本当の生徒に実施できるための認証基盤が必要。

- **情報共有ニーズの増加**
  - HPCI、NIMS、学認RDM等の共同研究基盤の整備が進んでいる。
    この共同研究基盤をセキュアかつ効率的に利用するための認証基盤が求められ始めた。
  - これにより、認証基盤の契約主体が、利用組織だけではなく、研究コミュニティの場合も出てくるだろう。

1. 新認証基盤要件

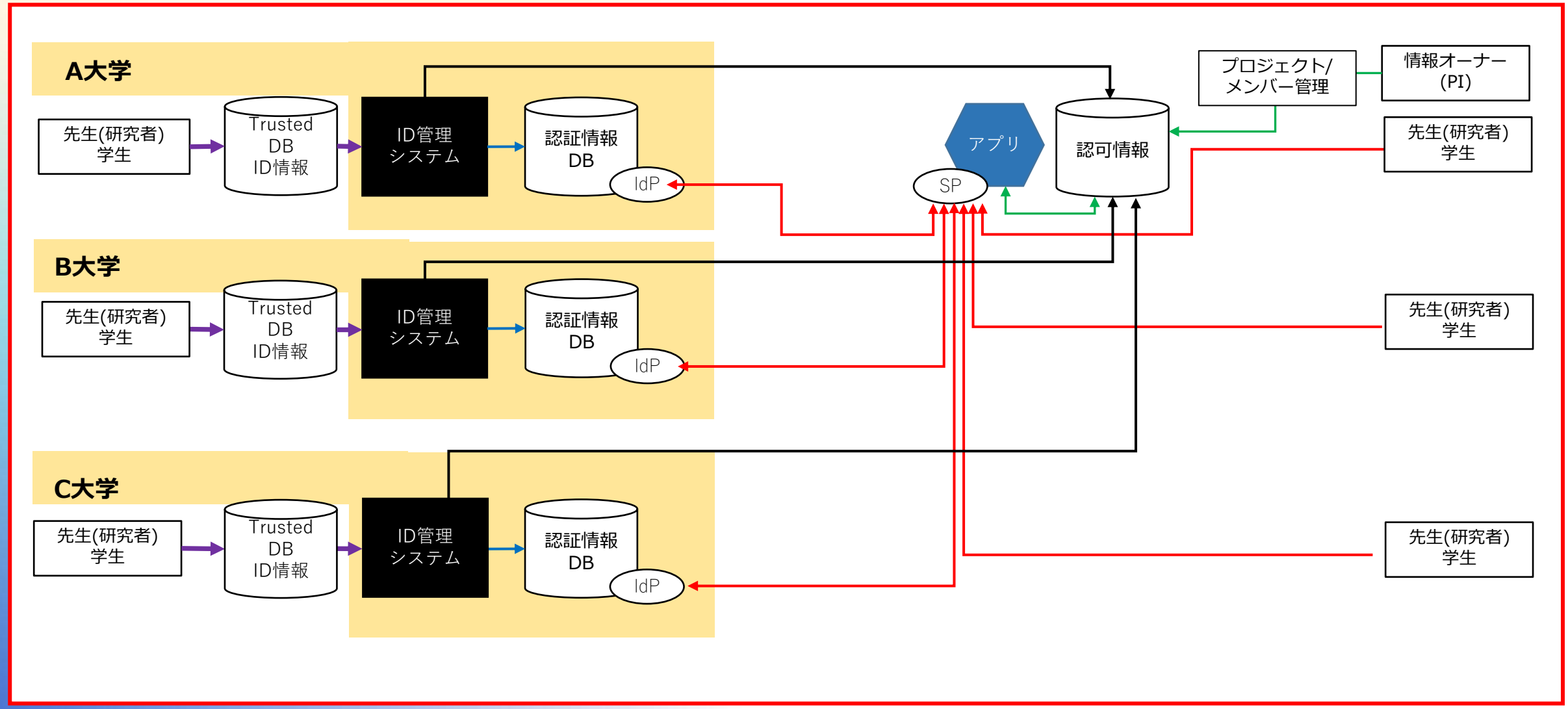
1.2 従来の認証基盤での情報共有



1. 新認証基盤要件

1.3 従来の認証基盤での情報共有~IDaaSの位置

IDaaS

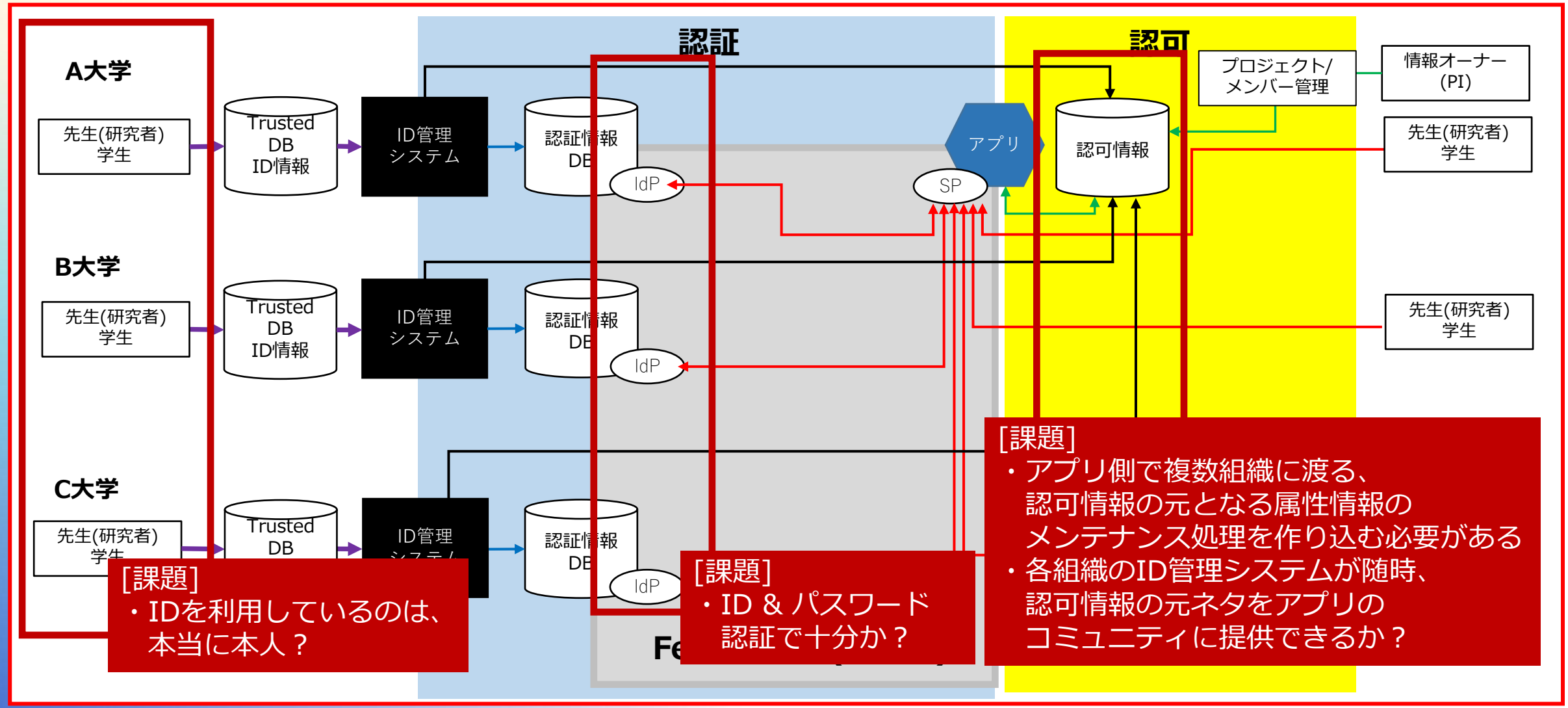


1. 新認証基盤要件

1.4 従来の認証基盤での情報共有~課題

ZERO TRUSTとして十分な認証基盤か？

情報共有に耐えうる認証基盤か？



1. 新認証基盤要件

1.5 認証基盤要件の変化

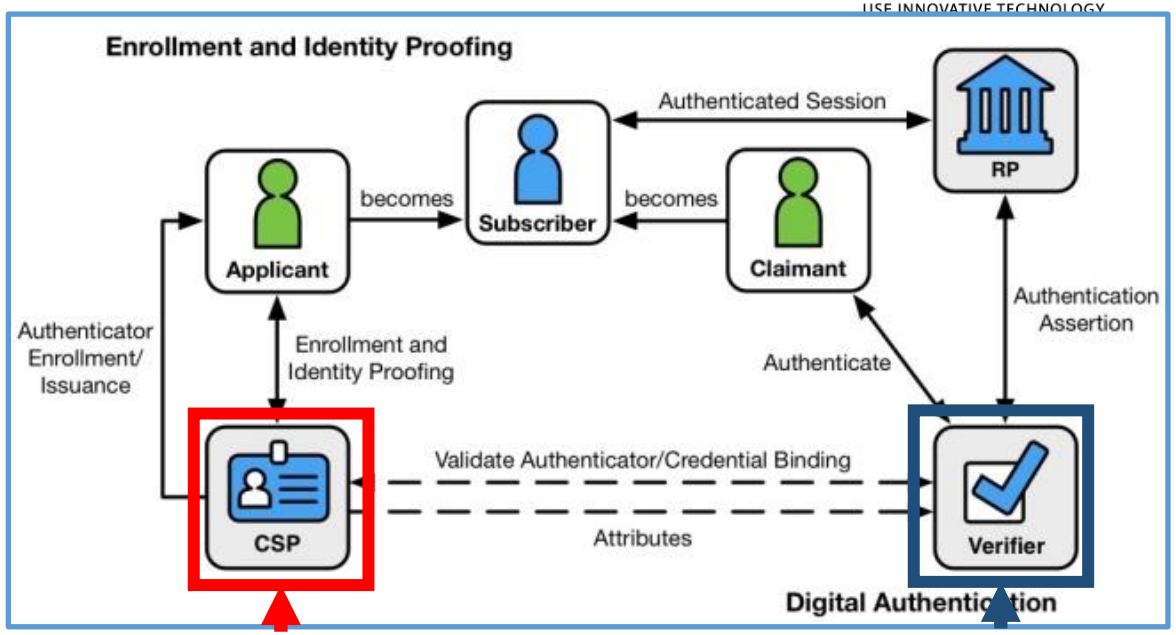
認証

ID管理

認可

ZERO TRUST対応の
認証基盤

セキュアな情報共有を
実現する認証基盤



1

本人確認
属性保証

ID管理

2

認証
機能強化

3

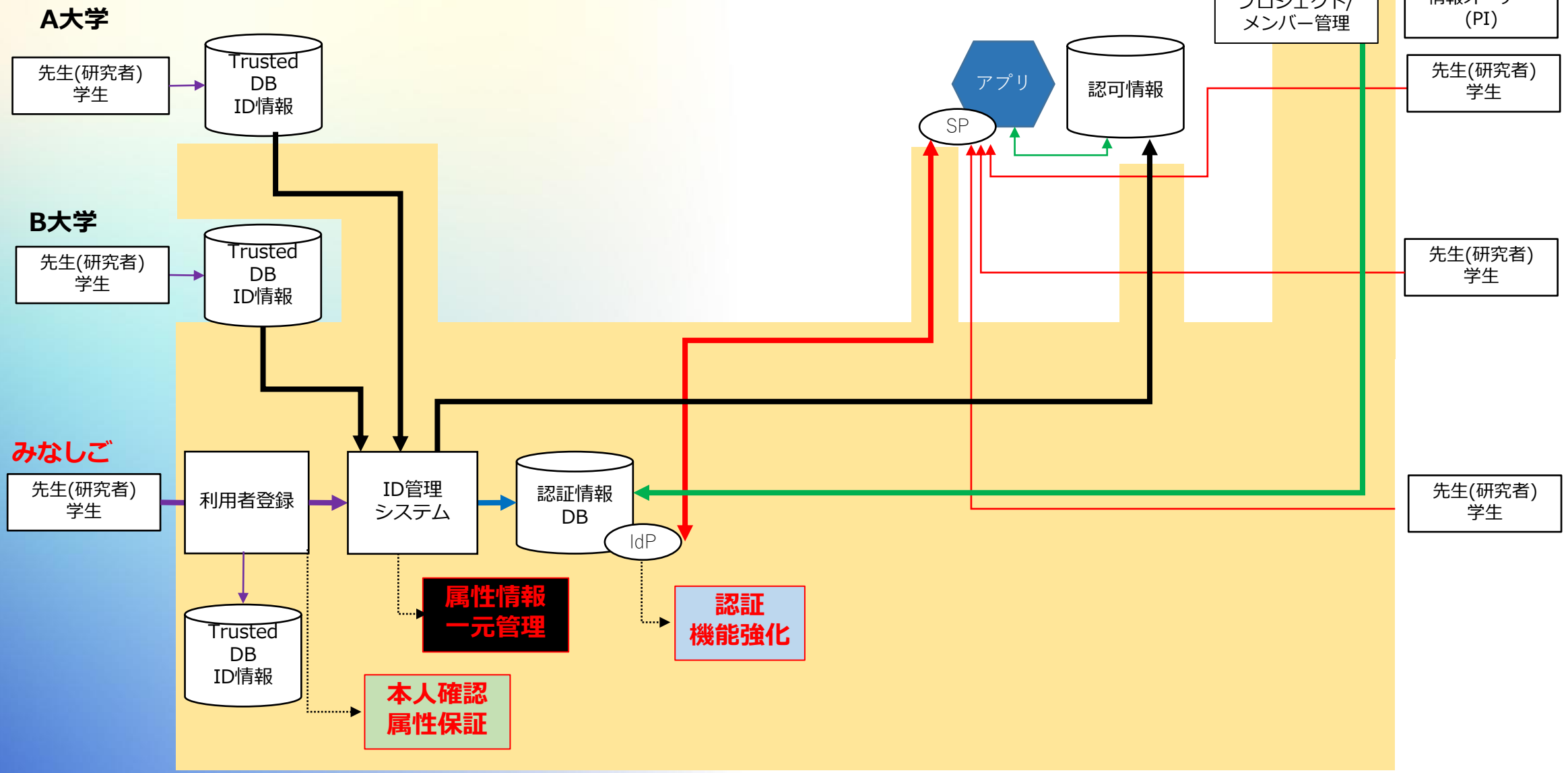
ID管理

属性情報
一元管理

認可

1. 新認証基盤要件

1.6 新認証基盤のシステム構成図



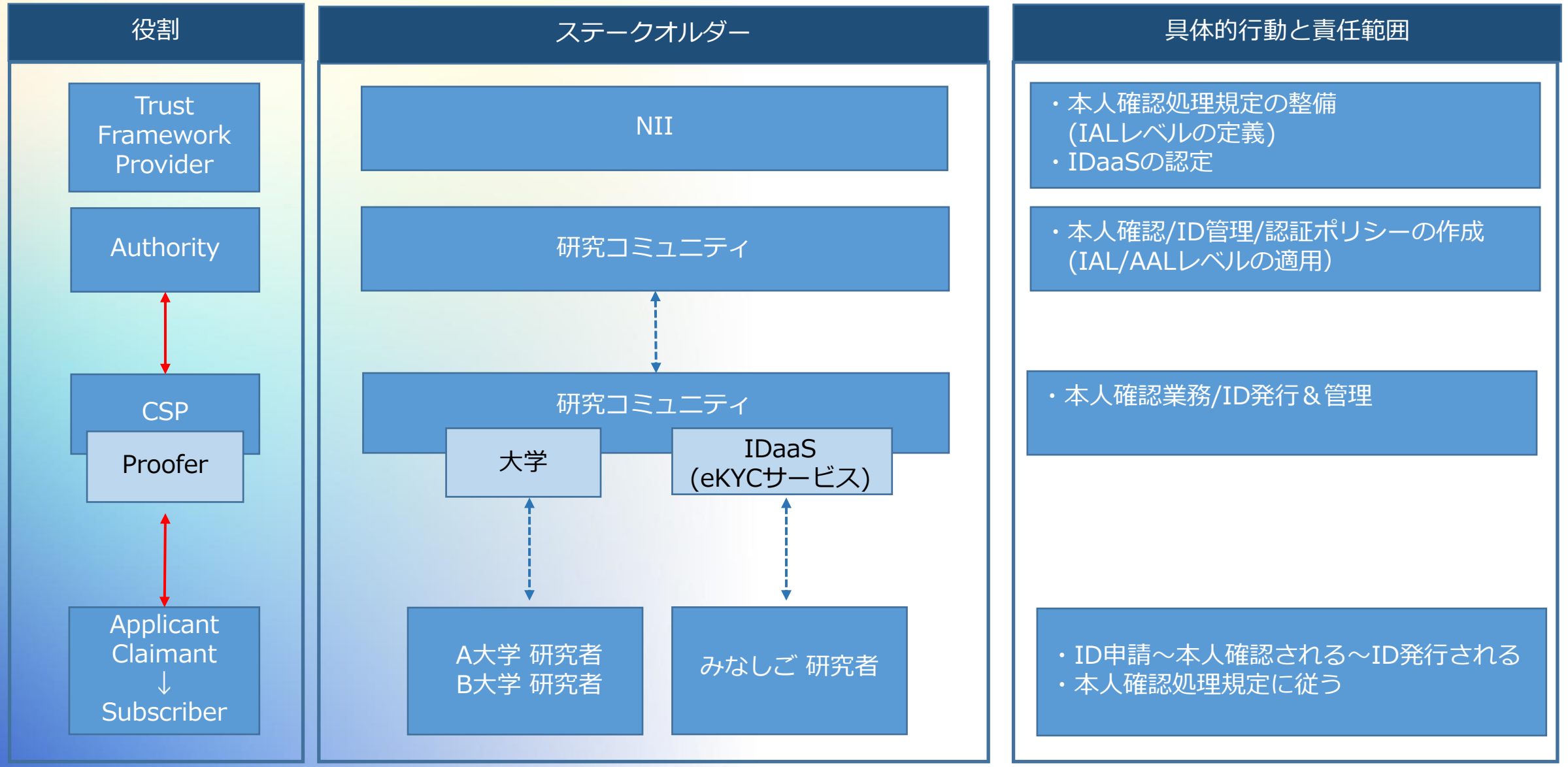
2. トラストフレームワークプロバイダーに対する要望

2.1 概要

① 本人確認における、ステークホルダーと役割の明確化
② 本人確認処理規定の定義
③ IDaaSの認定

2. トラストフレームワークプロバイダーに対する要望(私案)

2.2 本人確認における、ステークホルダーと役割の明確化



2. トラストフレームワークプロバイダーに対する要望(私案)

2.3 本人確認処理規定の整備

① 本人確認処理の内容について、定義する。
- 「実在性確認」共同研究サービスを利用するユーザーが実在する存在であることを確認する。
- 「属性確認」共同研究サービスを利用するユーザーが自己申告された組織に在籍している
  こと(所属と本人の紐づけ(どこに所属する誰）の保証)を確認する。

② レベル定義が必要。
- 「実在性確認」NIST SP800-63AのIAL２レベルを参考とする。
- 「属性確認」NIST SP800-63AのIALでは定義されていない。

③ AALレベルとの連携

2. トラストフレームワークプロバイダーに対する要望(私案)

2.3 本人確認処理規定の整備

④ 本人確認処理の具体的方法の明記

(1) Trusted DB

・Trusted DB=本人確認/属性保証処理が行われたID情報DBと捉える。
・Trusted DBに対する、本人確認処理の規定が必要。
・Trusted DBと認証DBの直結性の規定が必要。

(2) 属性確認の方法

(例1)
AuthorityよりCSP機関やProoferとして認めらた機関により作成された、利用者リストの提出(厳格なプロセスとして成立させるには、利用者リスト発行機関が本物であることの証明が必要)~運用が煩雑。

(例2)
アプリの利用契約を取り交わす時に、予め、利用者の所属する組織のドメイン名入りメールアドレス体系を登録しておく。本人確認処理(①Presenceの確認と②Credentialの配布処理)において、利用者の所属する組織のドメイン名入りメールアドレスの突合を行い、登録作業用のURLを送付する、またはID、Credentialダウンロード用のストレージURLを送信する。

(例3)
学認参加機関であれば、本人確認処理として、利用者の所属する組織の学認IdPに対して、認証を行う。
＊このような使い方の学認SPを認定していただく必要もある。

(例4)
ORCIDやe-RAD研究者番号を属性保証として利用。
＊そもそも、使えるかどうかの検討も必要。

2. トラストフレームワークプロバイダーに対する要望(私案)

2.4 IDaaSの認定

・組織内にTrusted DBはあるが、共同研究基盤を利用するための認証DBと連携できない組織の研究者(みなしご)のID情報の本人確認/属性保証については本人確認サービス(eKYCサービス)を利用する。

・IDaaSがみなしごIDを管理するため、Trusted DBを運用管理することになる。

＊このIDaaSに対して、Trusted Third Party(Trust Framework Provider?)である学認等の認定が必要。