学認に関する意見交換会
～IDaaS屋の意見～

2021年4月23日

エクスジェン・ネットワークス株式会社　江川

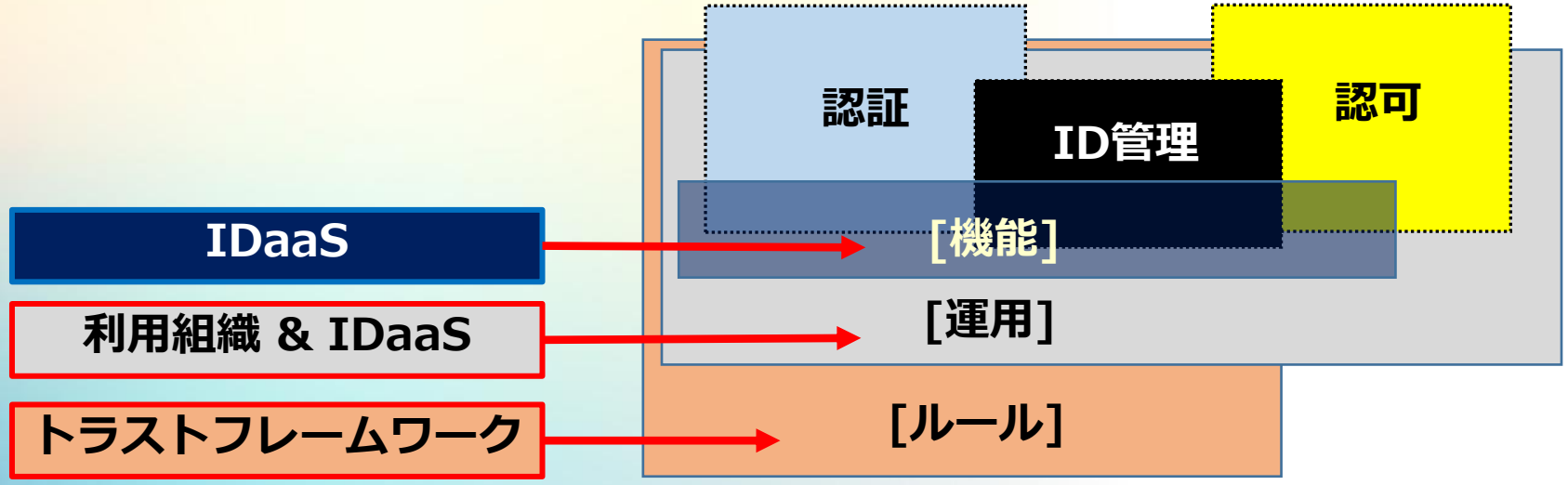
USE INNOVATIVE TECHNOLOGY.

1. 認証基盤構成 & トラストフレームワーク

1.1 認証基盤の機能構成

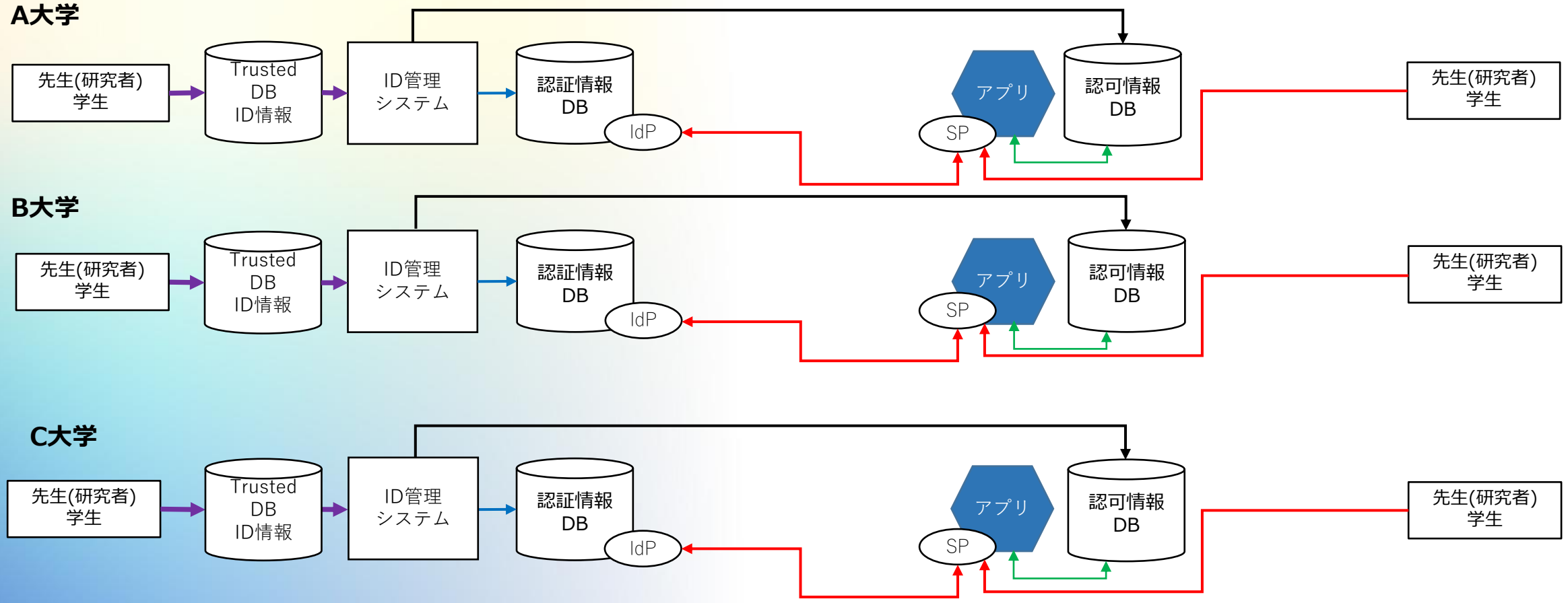
1. 認証基盤構成 & トラストフレームワーク

1.2 機能構成 & トラストフレームワーク



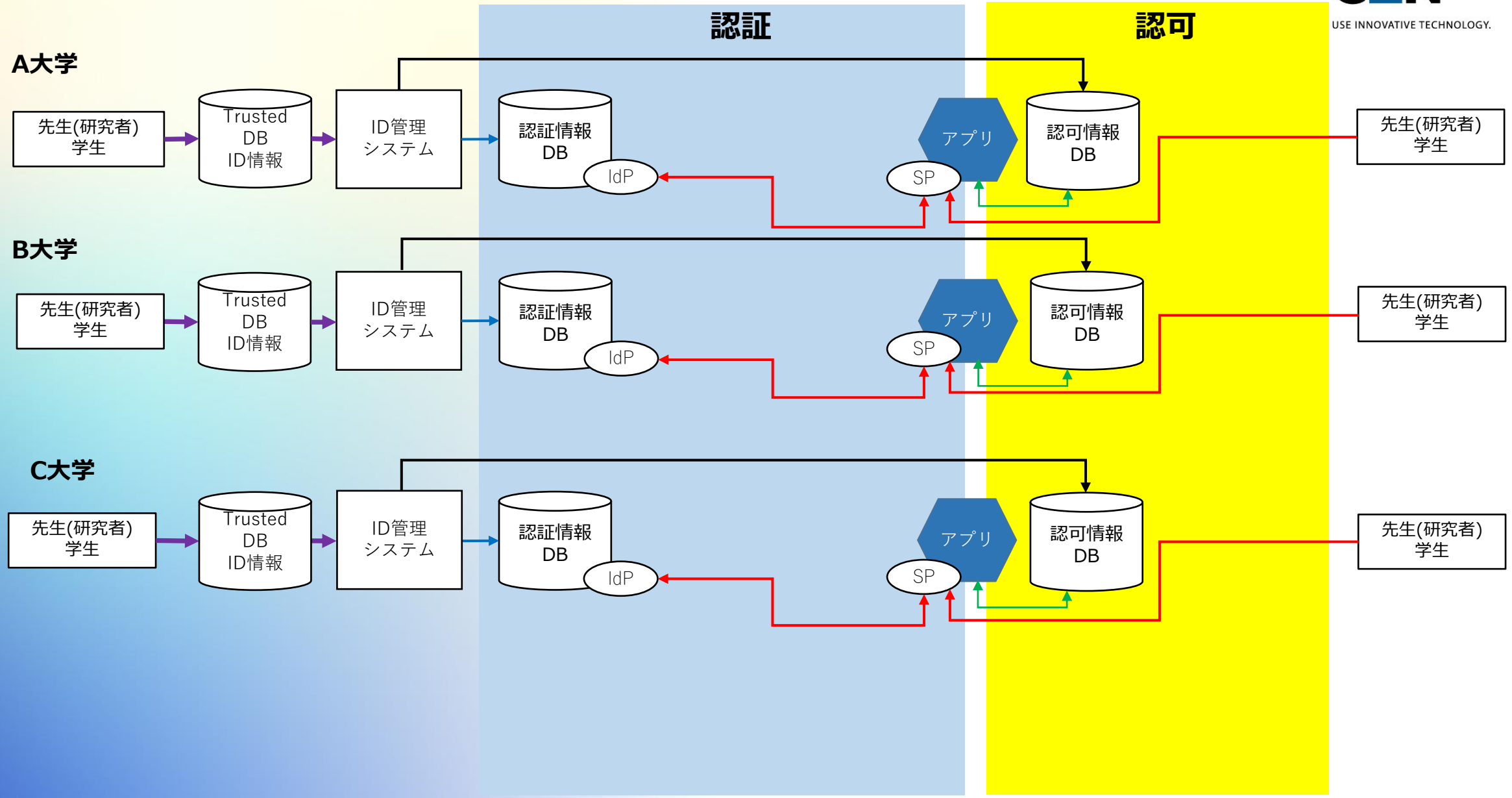
1. 認証基盤構成 & トラストフレームワーク

1.3 機能詳細図



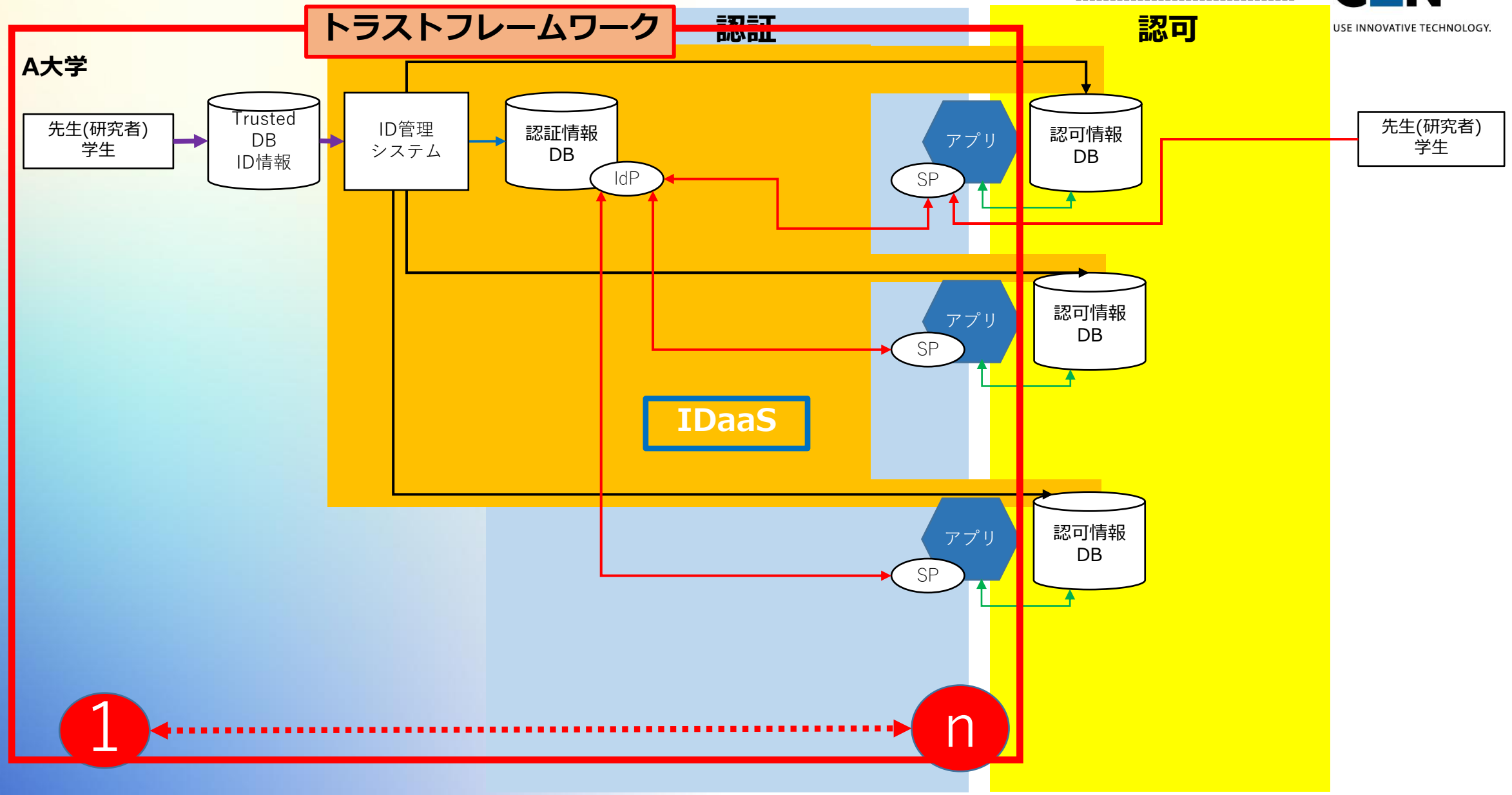
1. 認証基盤構成 & トラストフレームワーク

1.4 機能分類図



1. 認証基盤構成 & トラストフレームワーク

1.5 IDaaS & トラストフレームワークのマッピング



2. 新型認証基盤要件＆トラストフレームワーク

2.1 共同研究要件

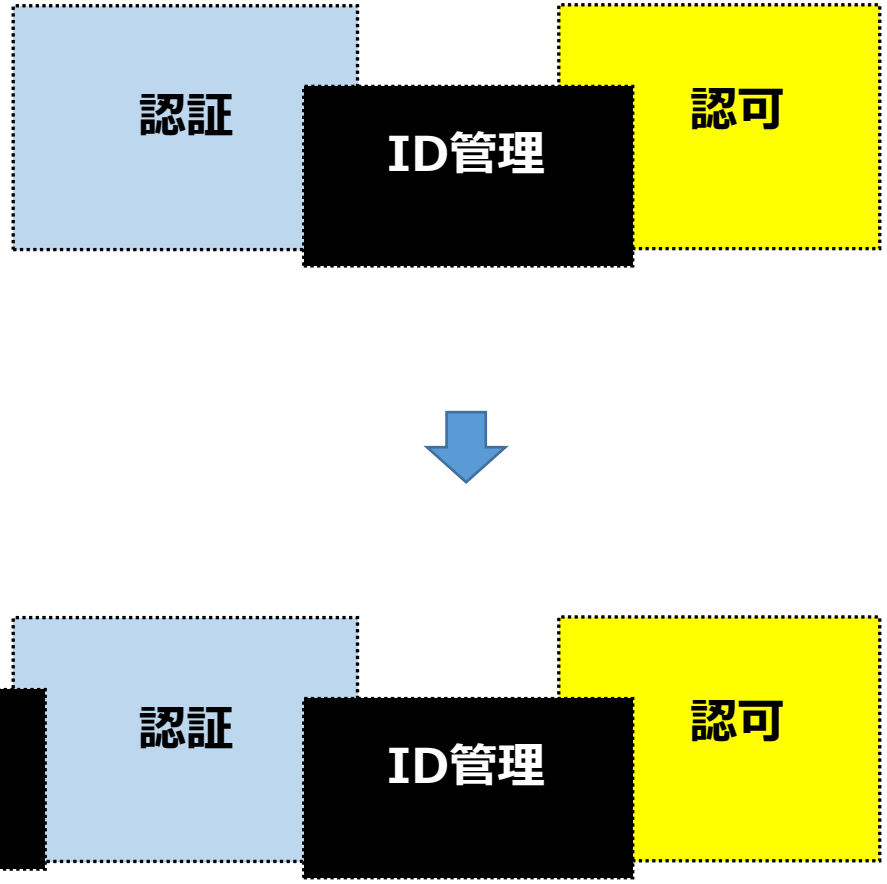
・HPCI、NIMS、学認RDM等の共同研究基盤が整備され、
この基盤をセキュアかつ効率的に利用するため、
研究コミュニティを対象とした認証基盤が求められ始めた。

2. 新型認証基盤要件＆トラストフレームワーク

2.1 共同研究要件

・HPCI、NIMS、学認RDM等の共同研究基盤が整備され、
この基盤をセキュアかつ効率的に利用するため、
研究コミュニティを対象とした認証基盤が求められ始めた。

・必要な機能構成は、
＋ 本人確認 属性保証



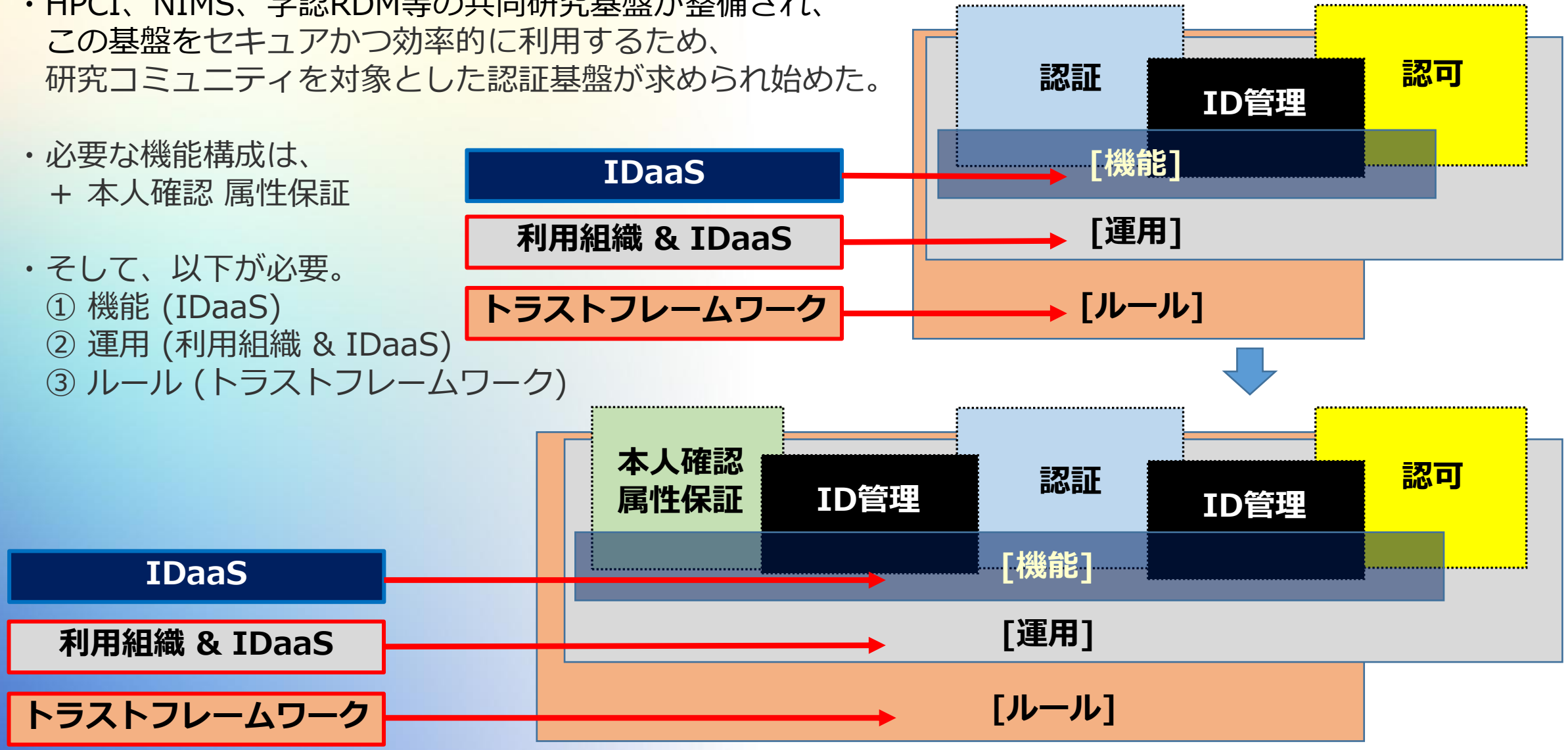
2. 新型認証基盤要件＆トラストフレームワーク

2.1 共同研究要件

・HPCI、NIMS、学認RDM等の共同研究基盤が整備され、
この基盤をセキュアかつ効率的に利用するため、
研究コミュニティを対象とした認証基盤が求められ始めた。

・必要な機能構成は、
＋ 本人確認 属性保証

・そして、以下が必要。
① 機能 (IDaaS)
② 運用 (利用組織 & IDaaS)
③ ルール (トラストフレームワーク)



2. 新型認証基盤要件＆トラストフレームワーク

2.2 本人確認/属性保証の構成要素と課題

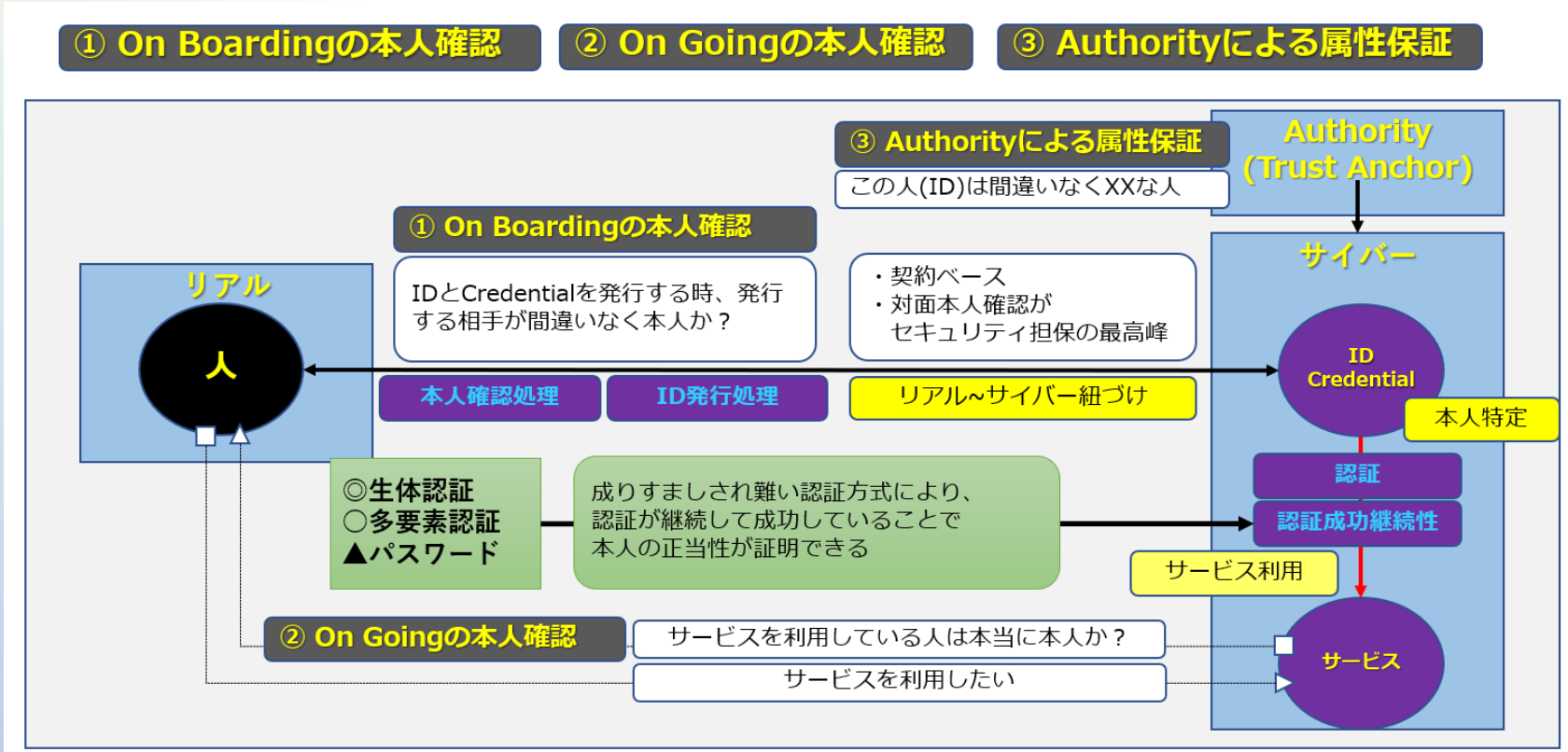
・本人確認には以下の３つの要素がある
① On Boardingの本人確認：ID発行時の実在性確認
② On Goingの本人確認：ID利用時の実在性確認
③ Authorityによる属性保証：ID利用時の所属とIDの確かな紐づけ

[課題]

・利用者が所属する組織で本人確認処理が適切に行われているか？
[ルール] [運用] [機能]

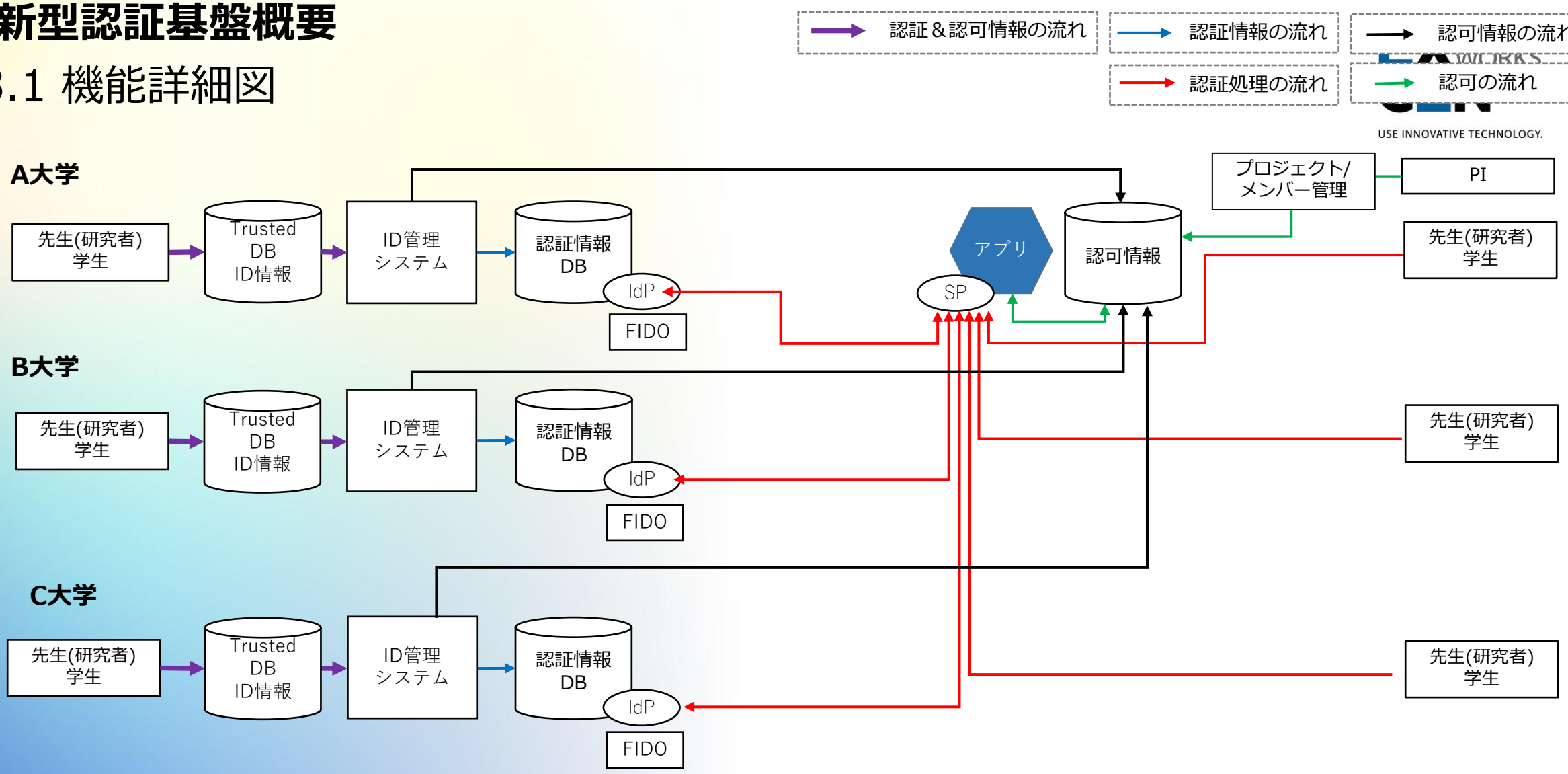
・本人確認処理を行う工数が利用者が所属する組織にあるか？
[運用]

・本人確認処理のレベルが利用者が所属する組織間で同レベルにあるか？
[ルール] [運用] [機能]



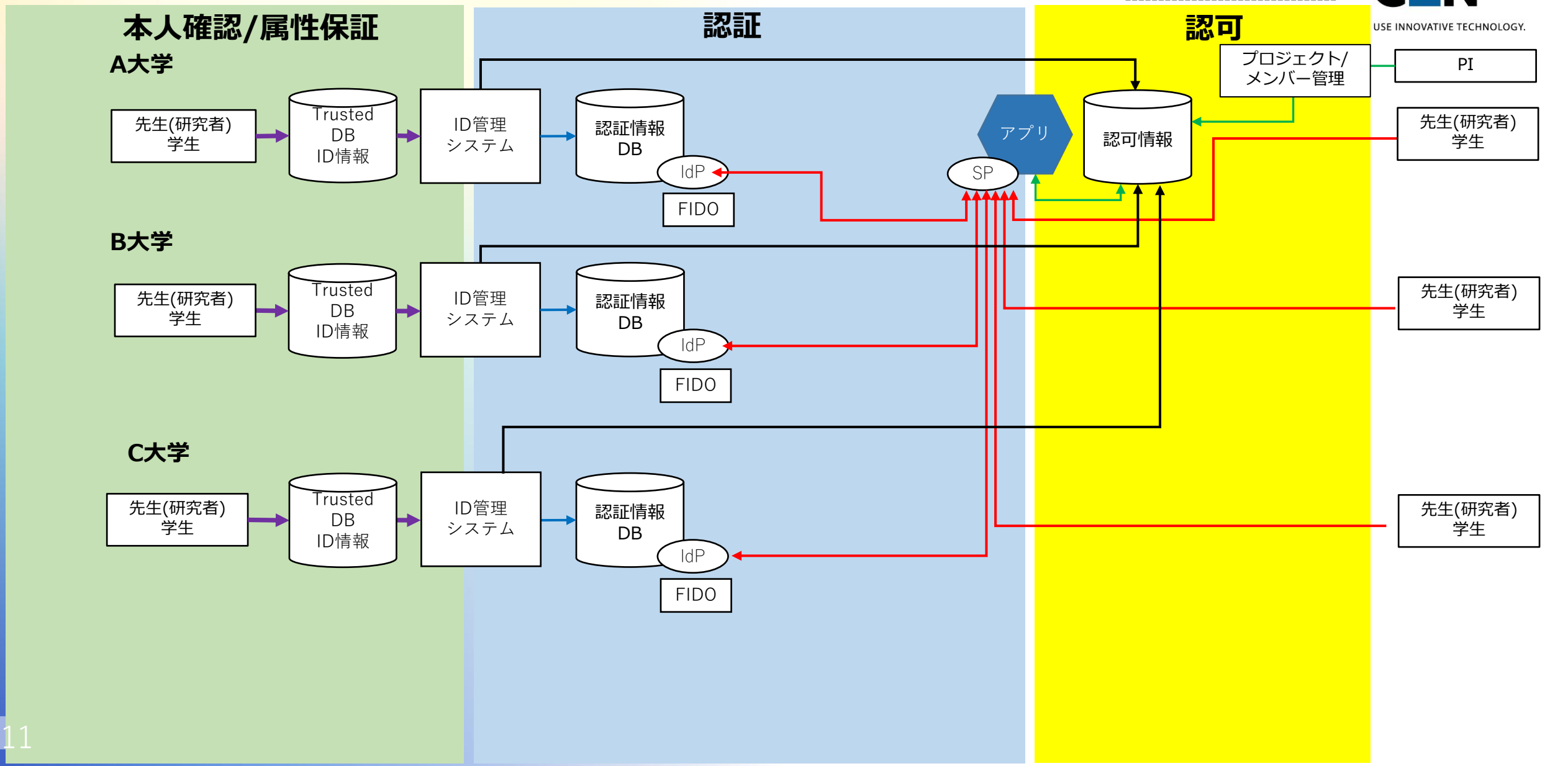
3. 新型認証基盤概要

3.1 機能詳細図



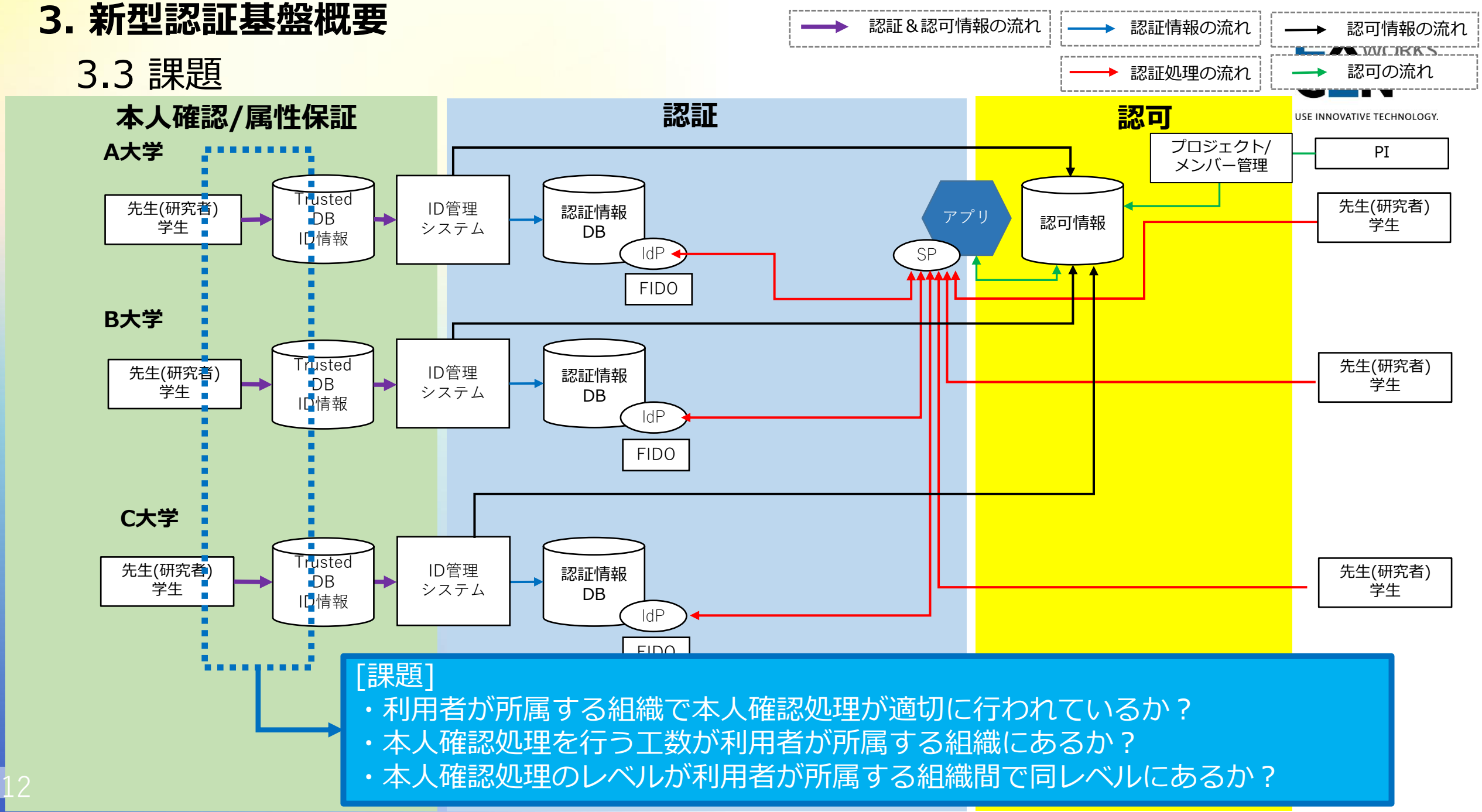
3. 新型認証基盤概要

3.2 機能分類図



3. 新型認証基盤概要

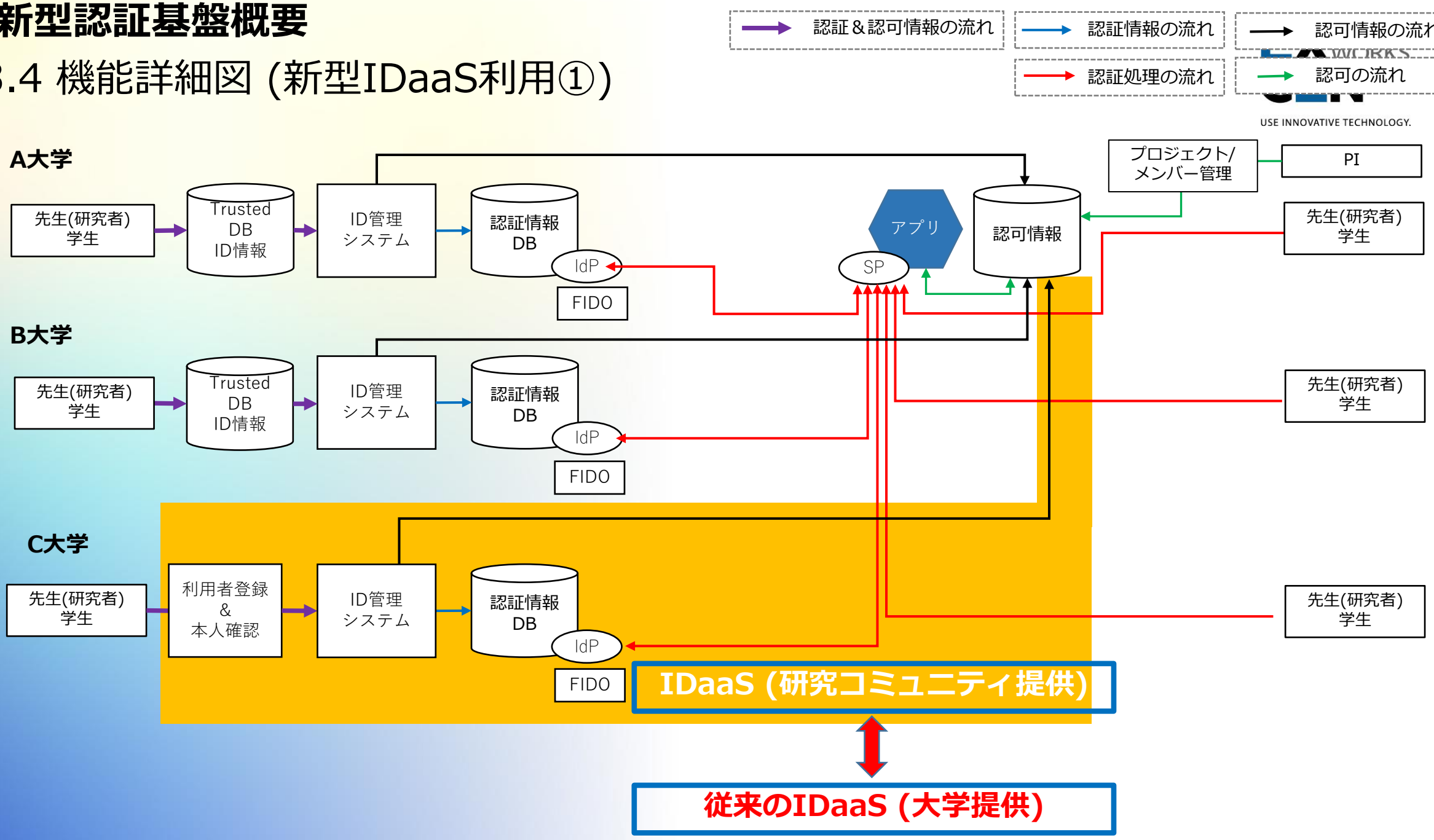
3.3 課題



[課題]
- 利用者が所属する組織で本人確認処理が適切に行われているか？
- 本人確認処理を行う工数が利用者が所属する組織にあるか？
- 本人確認処理のレベルが利用者が所属する組織間で同レベルにあるか？

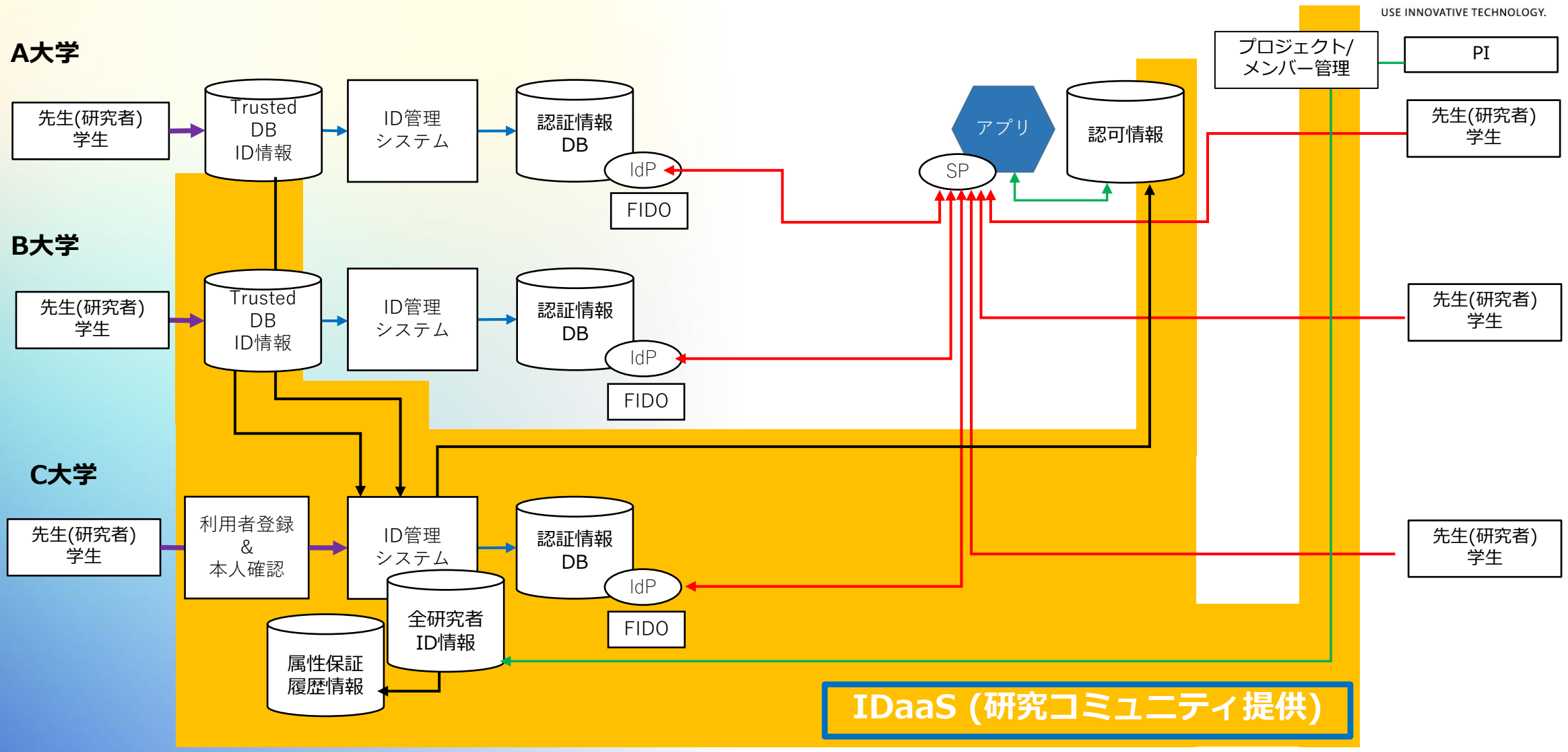
3. 新型認証基盤概要

3.4 機能詳細図 (新型IDaaS利用①)



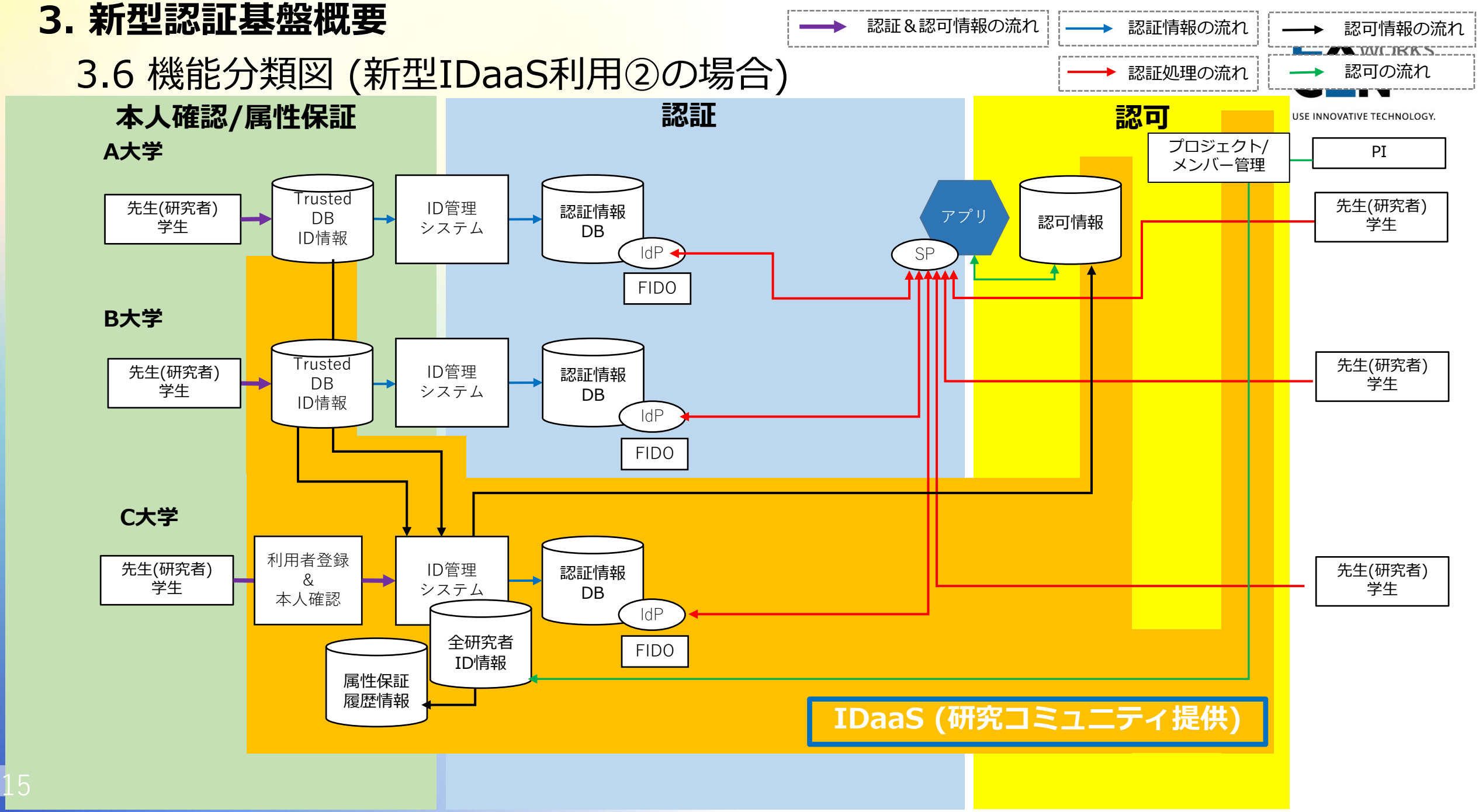
3. 新型認証基盤概要

3.5 機能詳細図 (新型IDaaS利用②)



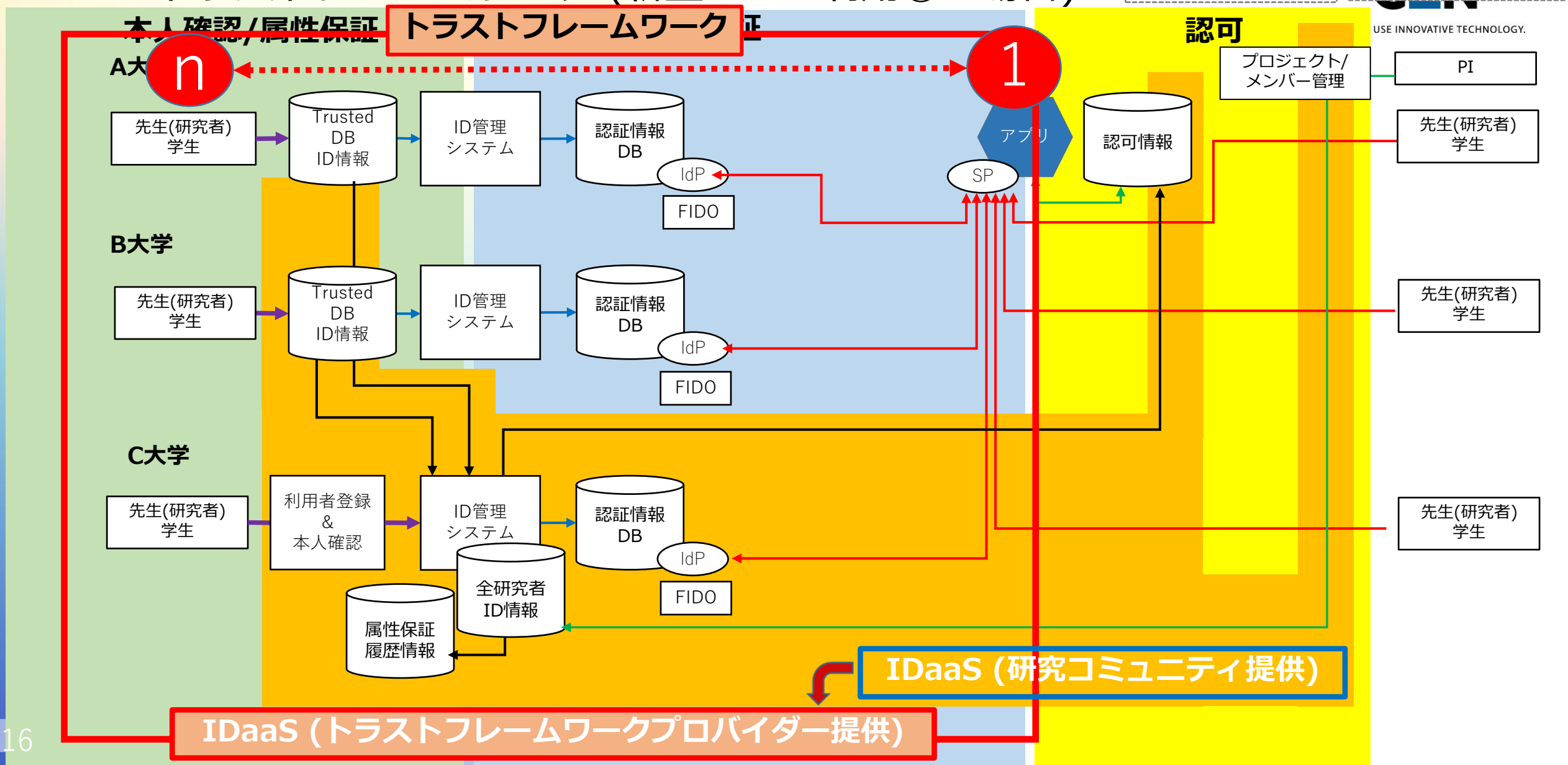
3. 新型認証基盤概要

3.6 機能分類図 (新型IDaaS利用②の場合)



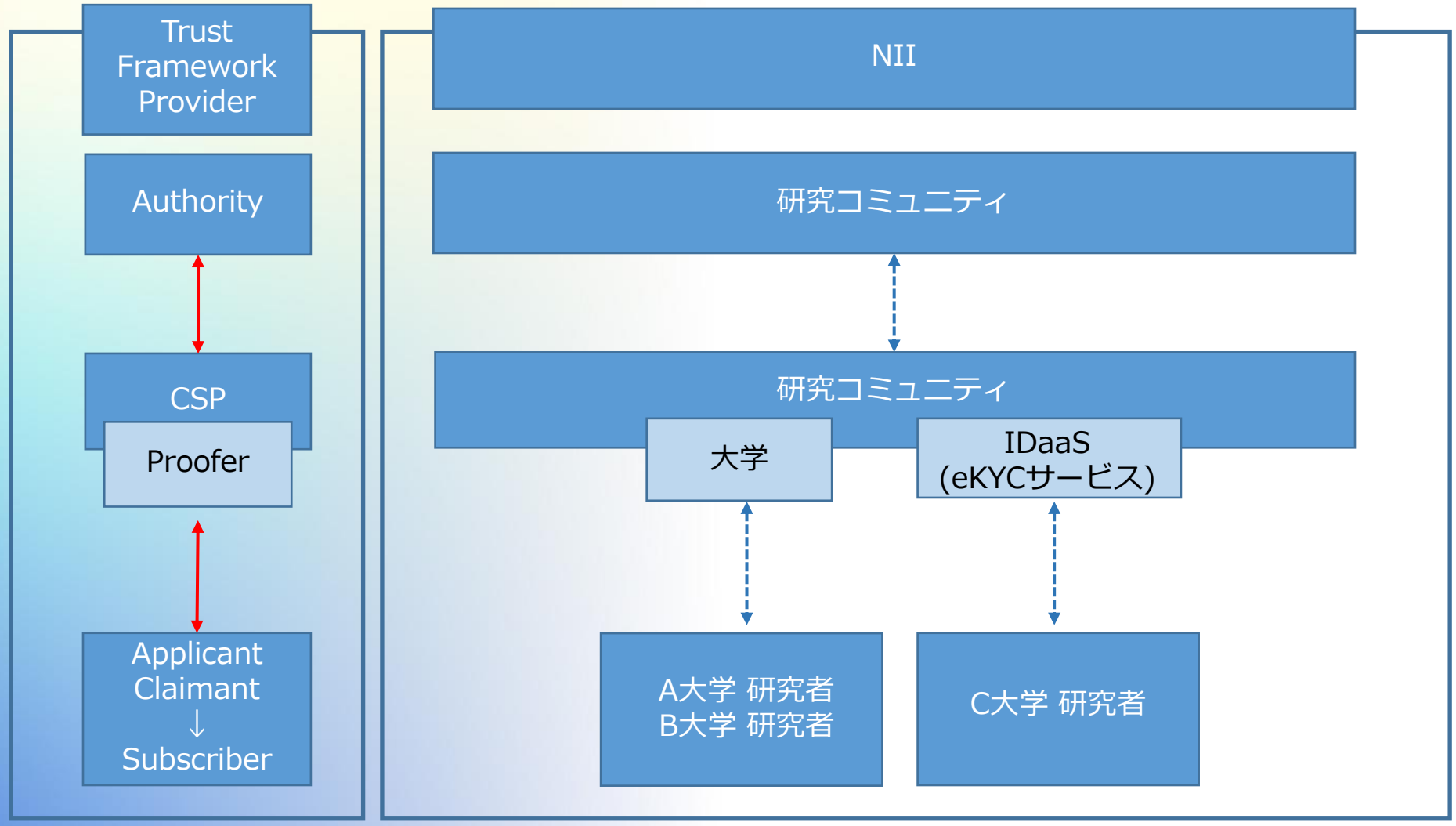
3. 新型認証基盤概要

3.7 トラストフレームワーク (新型IDaaS利用②の場合)



4. 新トラストフレームワーク

4.1 ステークホルダー



4. 新トラストフレームワーク

4.2 要件

・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。
・現在の学認ではTrusted DBと認証DBが直結されていることでセキュリティ保たれるとしている。
・Trusted DBに対する本人確認処理の規定はない。
　→本人確認処理の規定が必要。
　　・本人確認(実在性確認)に関しては、NIST SP800-63AのIAL 2 レベルを参考とする。
　　・属性保証では、所属と本人の紐づけ(どこに所属する誰）の保証が必要。
　　・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のID情報の本人確認/属性保証については本人確認処理サービス(eKYCサービス)を利用する。
　　→IDaaSがTrusted DBを保管、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。

・ログインIDとして利用ニーズがある、ORCIDやe-RAD研究者番号の利用についても規定が必要。

4. 新トラストフレームワーク

4.3 属性保証の方法

・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、本人確認処理において、利用者の所属する組織の学認IdPに対して、認証を行う。