

学術認証基盤における新トラストの創出 ～次世代認証連携作業検討部会の活動～

2021年10月8日

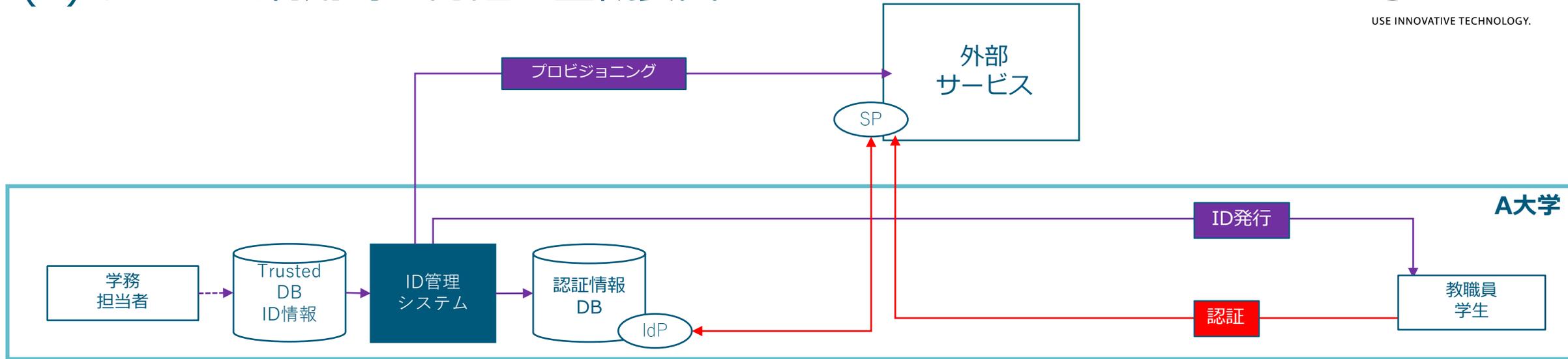
エクスジェン・ネットワークス株式会社

江川 淳一

USE INNOVATIVE TECHNOLOGY.

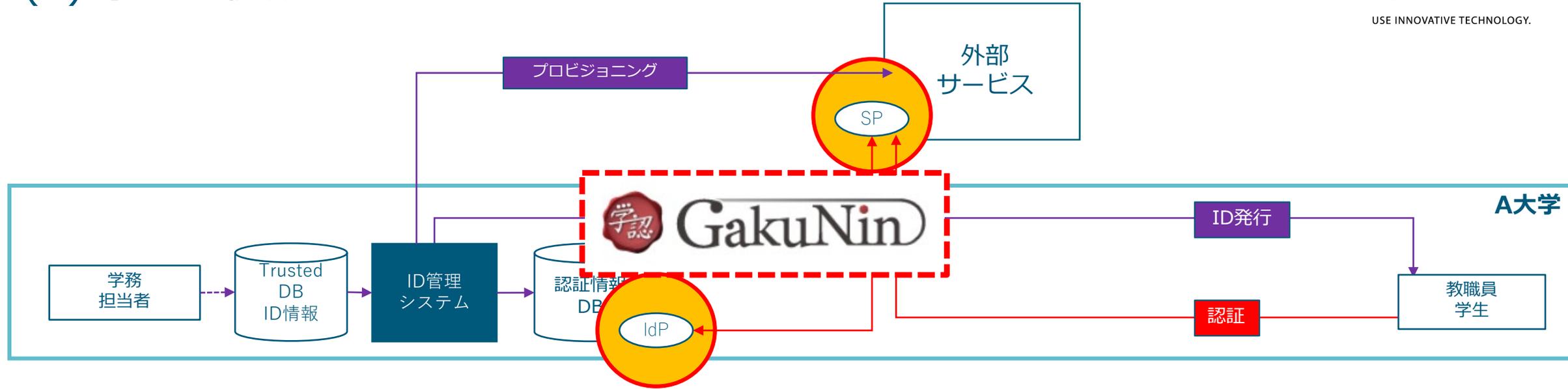
1. 学認とは

(1) サービス利用時の認証基盤概要図



1. 学認とは

(2) 学認の役割

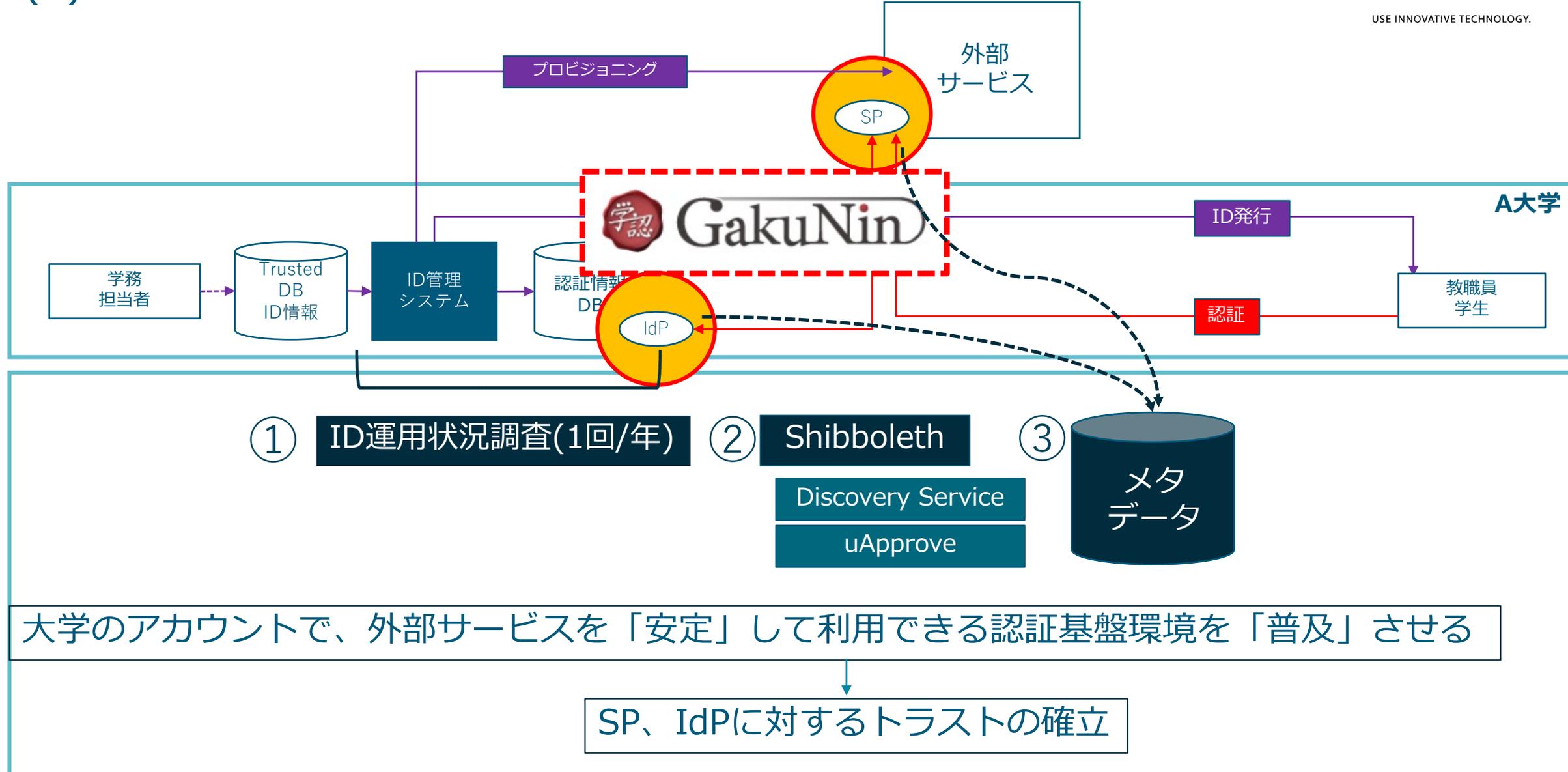


大学のアカウントで、外部サービスを「安定」して利用できる認証基盤環境を「普及」させる

SP、IdPに対するトラストの確立

1. 学認とは

(2) 学認の役割



2. 教育・研究業界の新たな要件

(1) 研究コミュニティサービスの整備と学認に対する新たな要件

- ・ HPCI、NIMS、学認RDM等の共同研究基盤の整備が進んでいる。



https://www.hpci-office.jp

HPCI High Performance Computing Infrastructure

English

サイト内検索

詳細検索

文字サイズ: A A A

HPCIについて 利用案内・申請 利用支援 HPCI研究成果 イベント・講習会 広報 利用者向け情報



Twitterで富岳を応援！
ハッシュタグでつぶやいてください

#富岳応援 #GoFugaku

いただいた応援ツイートは3月9日(土) HPCI フォーラム特設サイトに展示する予定です



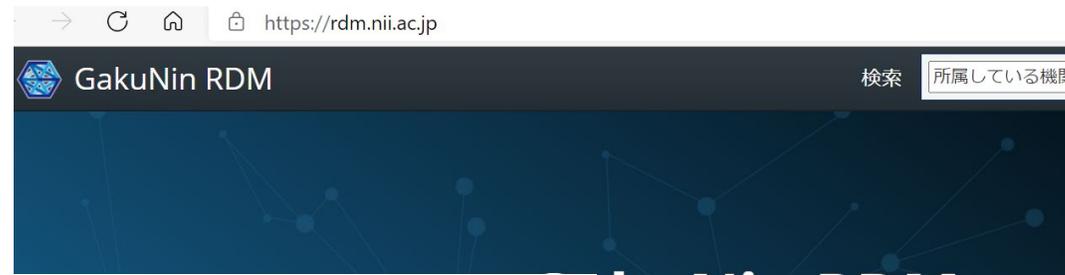
目的別ショートカット

計算機利用の流れを知りたい

使える計算機について知りたい

使えるソフトウェアを知りたい

令和3年度「富岳」を中核とするHPCIシステム [電子申請受付期間] 令和2年10月6日(火)~11月5日(木) 課題選定結果通知: 令和3年2月中旬



https://rdm.nii.ac.jp

GakuNin RDM

検索 所属している機関



https://mits.nims.go.jp

MatNavi

DICE

データサービス DICEとは 利用方法 お知らせ

NIMS 物質・材料データベース (MatNavi)

NIMS 物質・材料データベース(MatNavi)は、新材料の開発、材料の選択に貢献することを目的としています。MatNaviは、高分子データベース、NMRスペクトル・・・、無機材料データベース(結晶構造、状態図、物性・・・)、金属材料データベース(密度、弾性係数、クリスタル構造データベース(第一原理計算によるバンド構造・・・)など、十数種類の材料データベースで構成された統合データベースシステムのようなアプリケーションも提供しています。これらのデータベースはユーザ登録を行えば、無料で各種データベースを検索・閲覧することができます。

MatNaviユーザ登録・認証システム移行に関するお知らせ

NIMS物質・材料データベース(MatNavi)は更なるセキュリティ強化のため、2020年12月1日にMatNaviユーザ登録・認証システムを包含する新しいシステムに移行いたします。11/30以前にユーザ登録された方は、再度ユーザ登録が必要になります。旧システムにご登録いただいたユーザ情報につきましては、全て破棄され、ユーザ登録は無効となります。皆様には大変ご不便とお手数をおかけ致しますが、ご対応のほどお願い申し上げます。



GakuNin RDM

管理による研究推進と研究公正

所(NII)がサービスを提供しているものであり、利用にあたっては関係が定めた規程が適用されます。また、GakuNin RDMでは、関係が定めた規程が適用されます。また、GakuNin RDMをご利用されるお客様は、関係が定めた規程が適用されます。また、GakuNin RDMをご利用されるお客様は、関係が定めた規程が適用されます。

2. 教育・研究業界の新たな要件

(1) 研究コミュニティサービスの整備と学認に対する新たな要件

- ・ HPCI、NIMS、学認RDM等の共同研究基盤の整備が進んでいる。



学認に対する新たな要件

共同研究基盤を
効率的かつセキュアに利用できる
認証基盤環境を普及させるための
トラストの確立

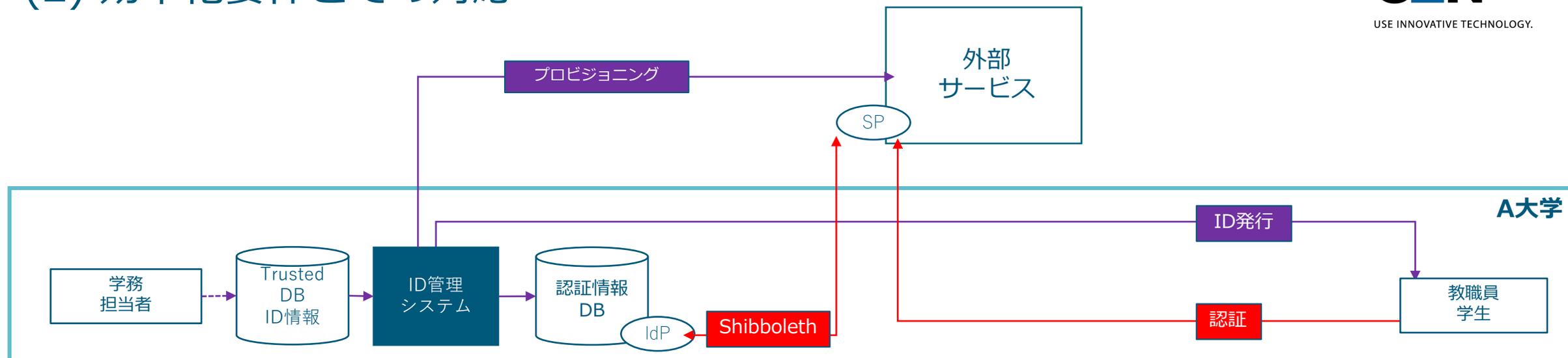
2. 教育・研究業界の新たな要件

(2) 効率化要件とその対応

- ・ 研究コミュニティ参加者の大きな部分は、学認参加組織のメンバーと被る。
- ・ 大学の学内システムのアカウントをそのまま、研究プラットフォームで使えないだろうか。
 - ・ DBへのアクセス。
 - ・ 各種システムへのログイン、またはシステム上のアカウント作成。
- ・ 研究コミュニティ側は、権限管理に集中できる。
 - ・ 本人のアカウント管理を大学や企業に受け持ってもらおう。
 - ・ 大学や企業は、アカウントの価値を高めることができるだろう。

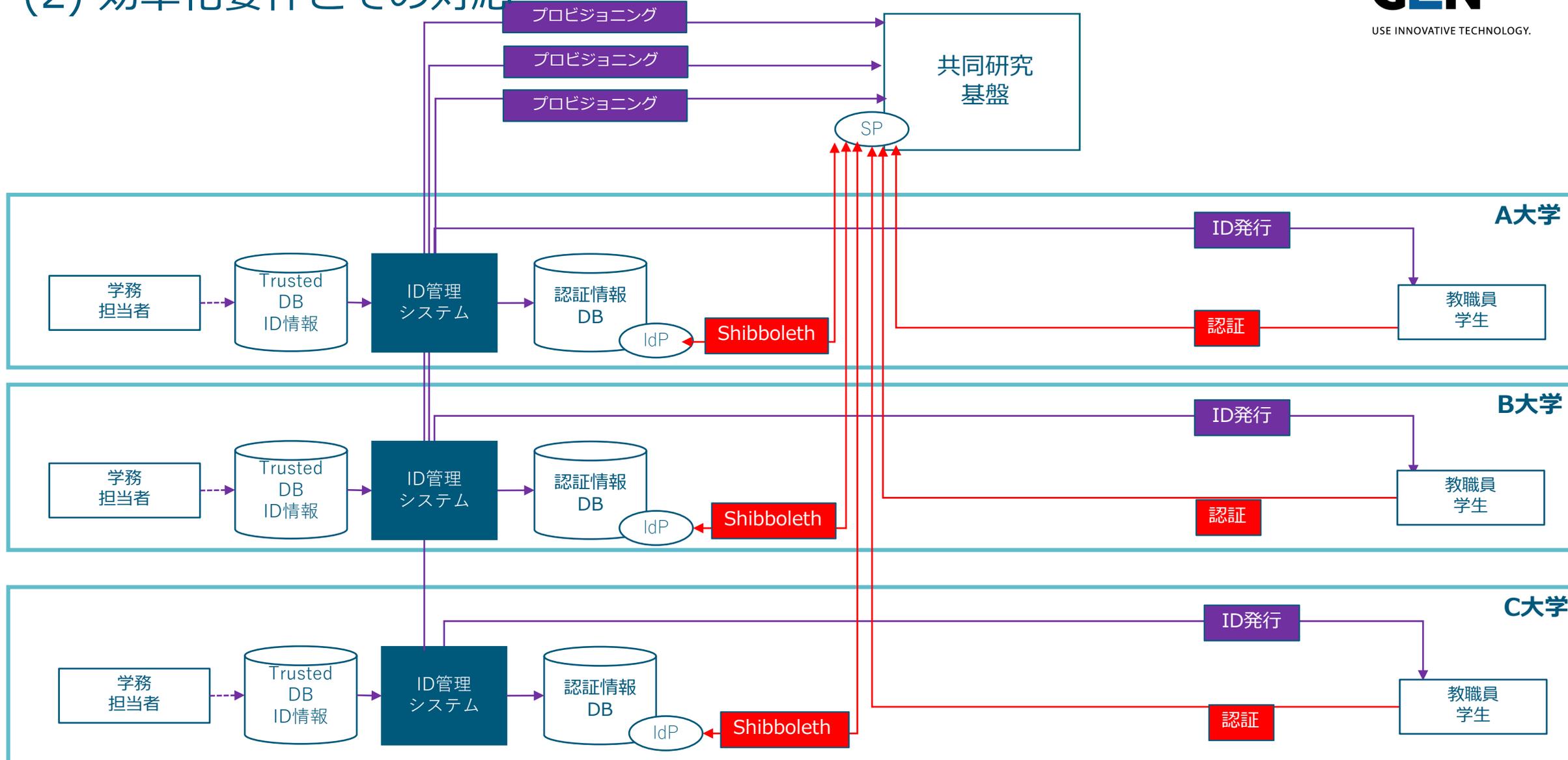
2. 教育・研究業界の新たな要件

(2) 効率化要件とその対応



2. 教育・研究業界の新たな要件

(2) 効率化要件とその対応



2. 教育・研究業界の新たな要件

(3) セキュリティ要件とその対応

- ・ 高度なサービス、リソースを共同利用(情報共有)するためには、組織内利用時よりもセキュアな本人確認が必要
- ・ 先行事例：Exostar～NIST SP800-63ベースのサプライチェーンセキュリティIDaaS

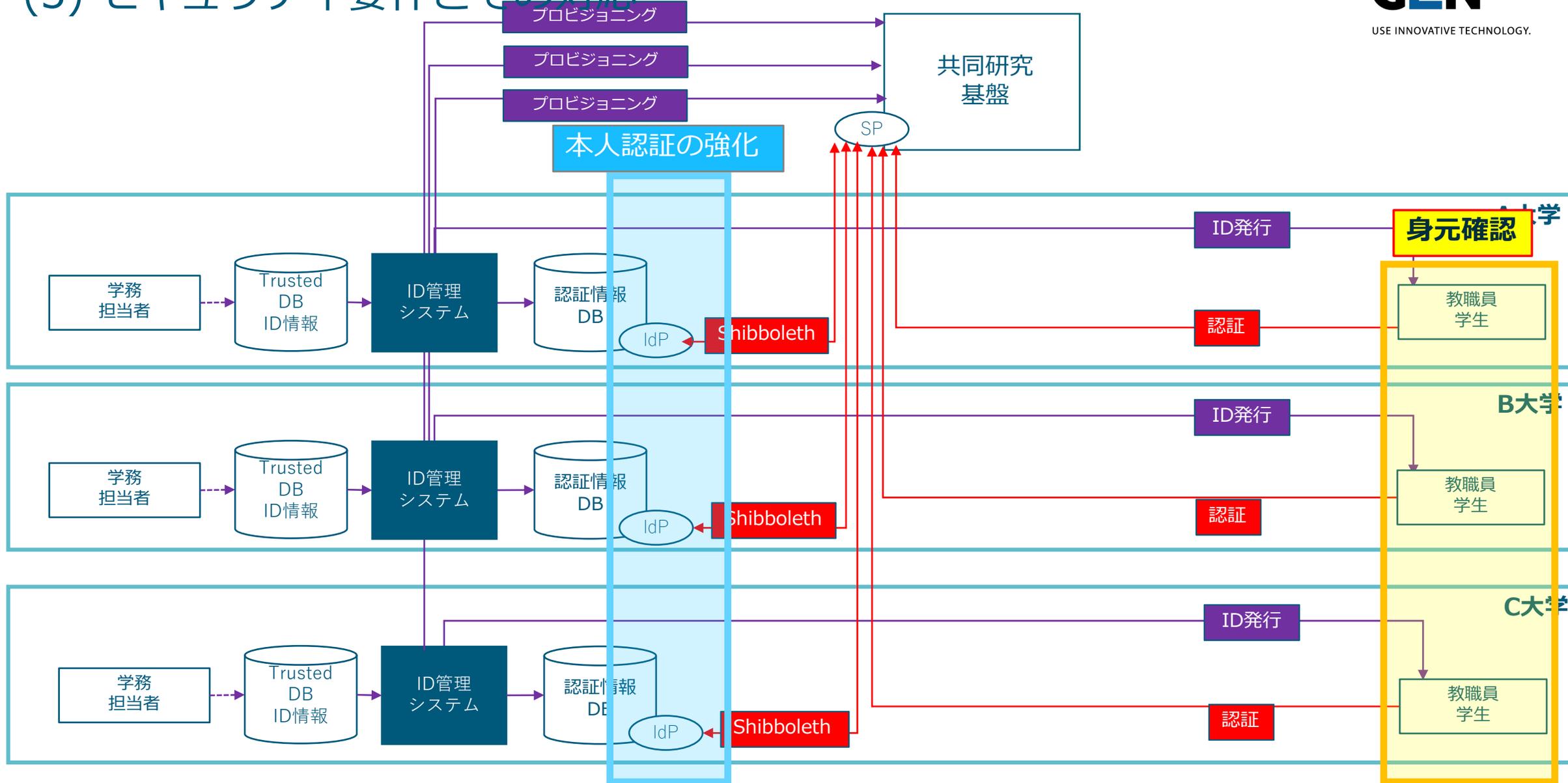


身元確認

本人認証の強化

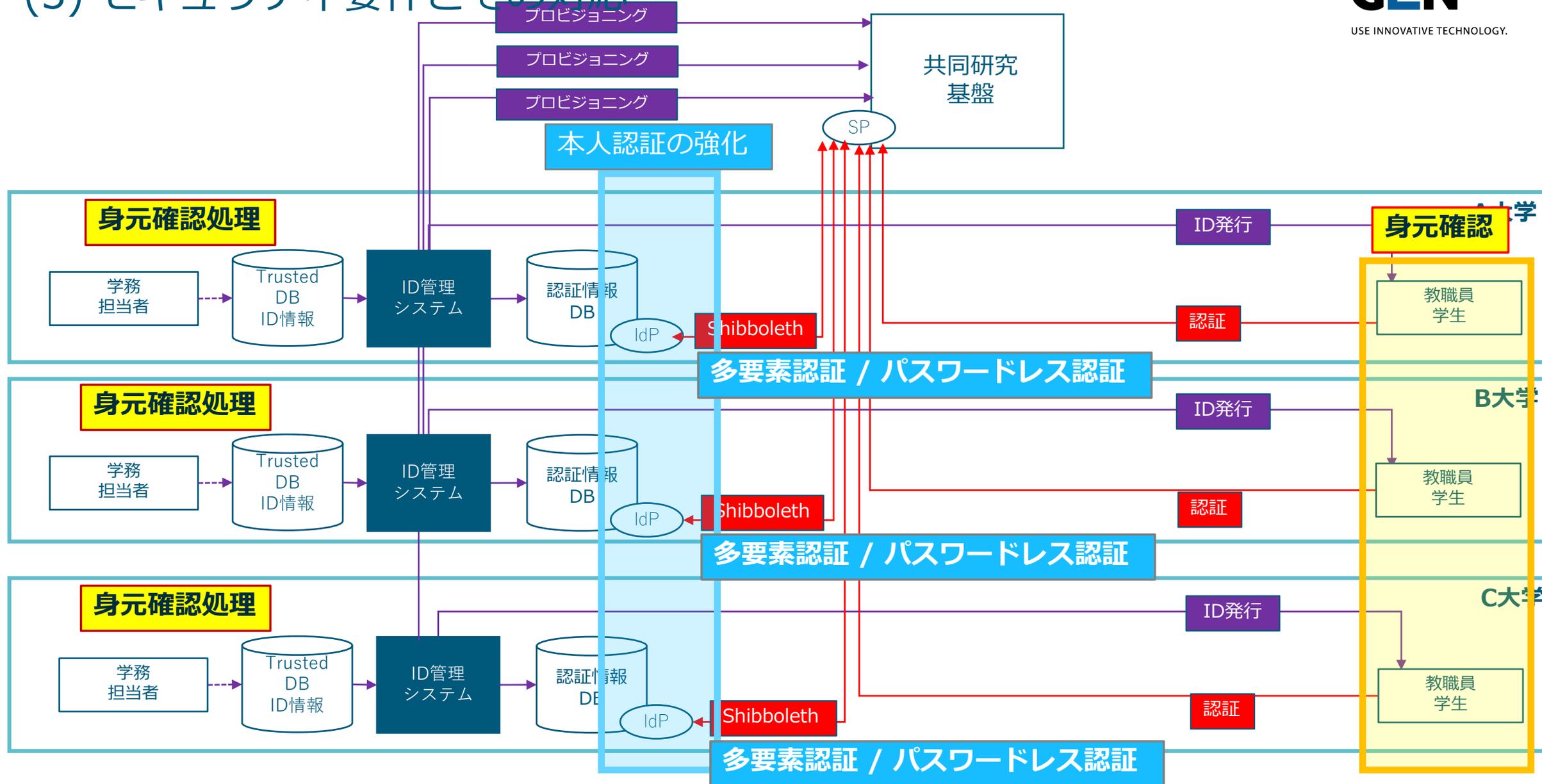
2. 教育・研究業界の新たな要件

(3) セキュリティ要件とその対応



2. 教育・研究業界の新たな要件

(3) セキュリティ要件とその対応



2. 教育・研究業界の新たな要件

(4) 学認が新たに提供するものと新たな役割

- ・ 現在、次世代認証連携作業検討部会で検討中

[新たに提供するもの]

- ① 身元確認を行う手続きについての基準の提示。
- ② 国際的な相互運用性（eduGain, IGTF, Kantara等）に配慮する。
- ③ パスワードを超えた強い認証システムを運用するための技術サポート。
- ④ 認証器（Authenticator）の運用の本人確認のレベルの作成。

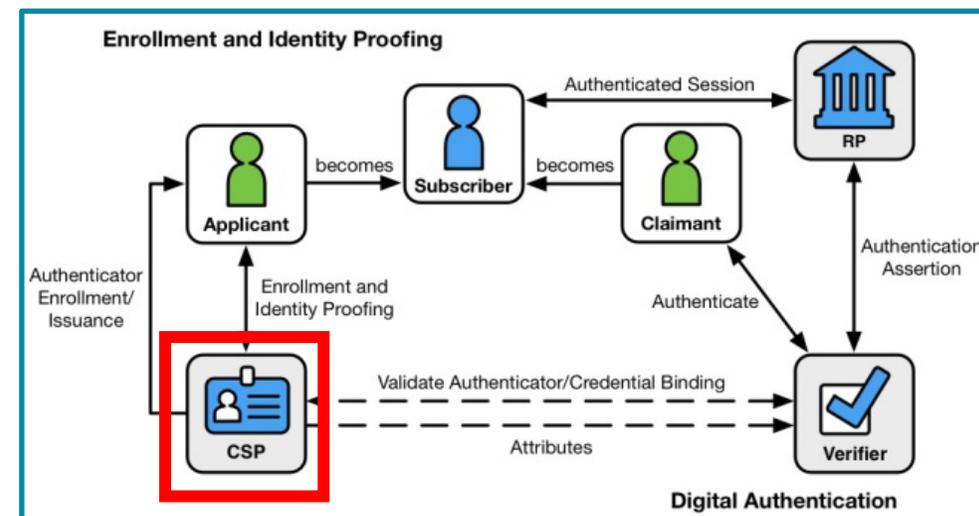
[新たな役割]

- ・ 研究コミュニティに対して

- ① 認定した組織、アカウントが十分な認証レベルを持っていることを保証する。
- ② 「十分な認証レベル」について、認定ポリシーを公開し、運用する。
- ③ IDaaSやOpenIdP等の認定を通して、広い範囲をカバーする。

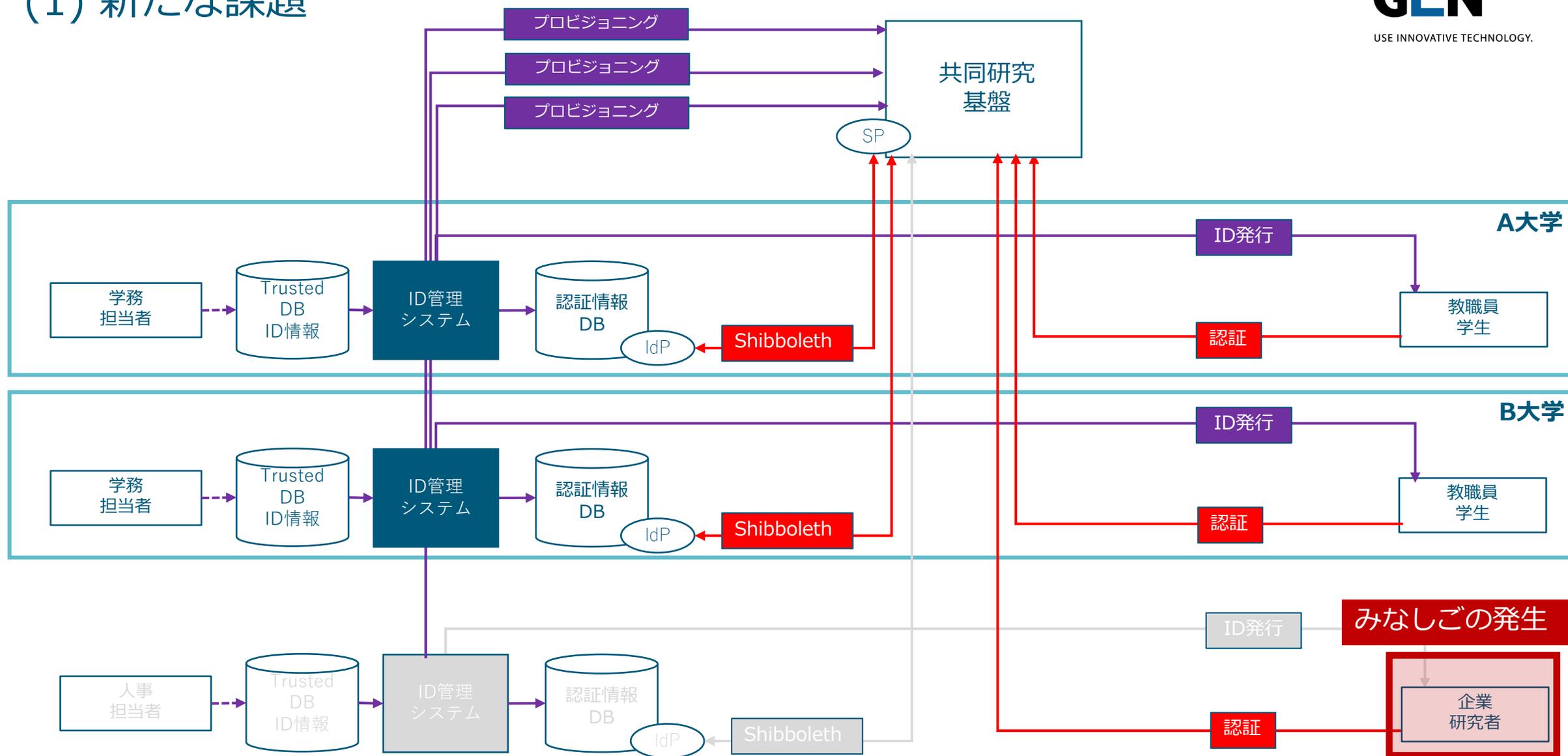
- ・ 大学等組織に対して

- ① 研究コミュニティのリソース利用を、
大学アカウントでできるように、認定システムをくみ上げる。
- ② 認定レベルを高く保つための技術的なサポートを行う。



3. IDaaSやOpenIdPの必要性

(1) 新たな課題



3. IDaaSやOpenIdPの必要性

(2) コンシューマIDとエンブラID

	コンシューマ(個人) ID	エンタープライズ(企業) ID
目的	個人が利用する情報に対する適切なアクセス制御	企業の機密情報漏えいを防ぐ適切なアクセス権限
登録・運用	自分自身で行う	管理者が行う
削除	ほとんど行われない	頻繁に行う
プライバシー性	高い	低い (今後、個人IDでの企業SNS 活用、GDPR対応などでは必要になる)

オレオレID



身元保証されたID

3. IDaaSやOpenIdPの必要性

(2) コンシューマIDとエンブラID

	コンシューマ(個人) ID	エンタープライズ(企業) ID
目的	個人が利用する情報に対する適切なアクセス制御	企業の機密情報漏えいを防ぐ適切なアクセス権限
登録・運用	自分自身で行う	管理者が行う
削除	ほとんど行われない	頻繁に行う
プライバシー性	高い	低い (今後、個人IDでの企業SNS 活用、GDPR対応などでは必要になる)

オレオレID

身元保証されたID

コンシューマアプリ

組織内での情報共有
エンブラアプリ



3. IDaaSやOpenIdPの必要性

(2) コンシューマIDとエンブラID

	コンシューマ(個人) ID	エンタープライズ(企業) ID
目的	個人が利用する情報に対する適切なアクセス制御	企業の機密情報漏えいを防ぐ適切なアクセス権限
登録・運用	自分自身で行う	管理者が行う
削除	ほとんど行われない	頻繁に行う
プライバシー性	高い	低い (今後、個人IDでの企業SNS 活用、GDPR対応などでは必要になる)

オレオレID

身元保証されたID

コンシューマアプリ

組織をまたぐ情報共有
エンブラアプリ

X

3. IDaaSやOpenIdPの必要性

(2) コンシューマIDとエンブラID

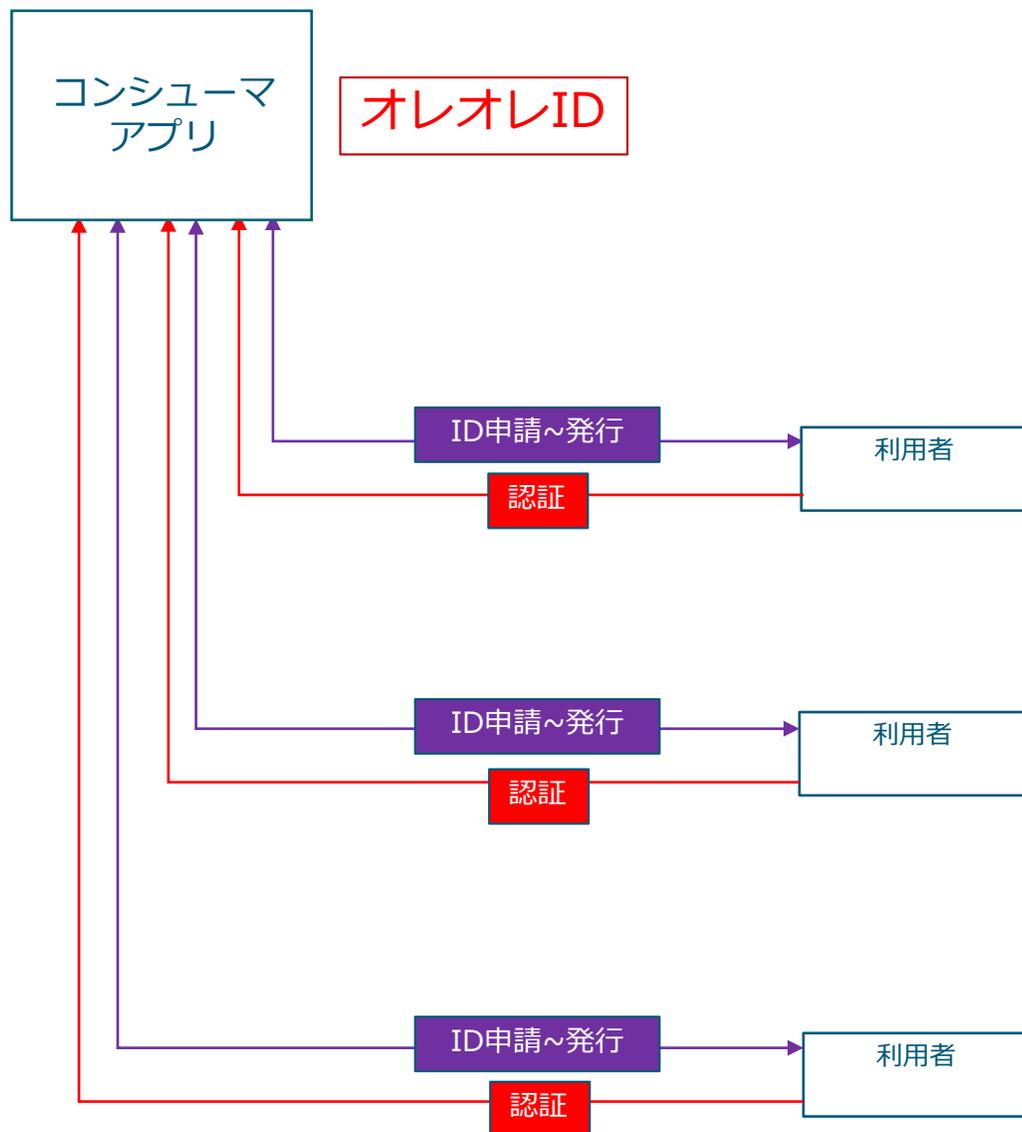
	コンシューマ(個人) ID	エンタープライズ(企業) ID
目的	個人が利用する情報に対する適切なアクセス制御	企業の機密情報漏えいを防ぐ適切なアクセス権限
登録・運用	自分自身で行う	管理者が行う
削除	ほとんど行われない	頻繁に行う
プライバシー性	高い	低い (今後、個人IDでの企業SNS 活用、GDPR対応などでは必要になる)

身元保証されたID

組織をまたぐ情報共有
エンブラアプリ

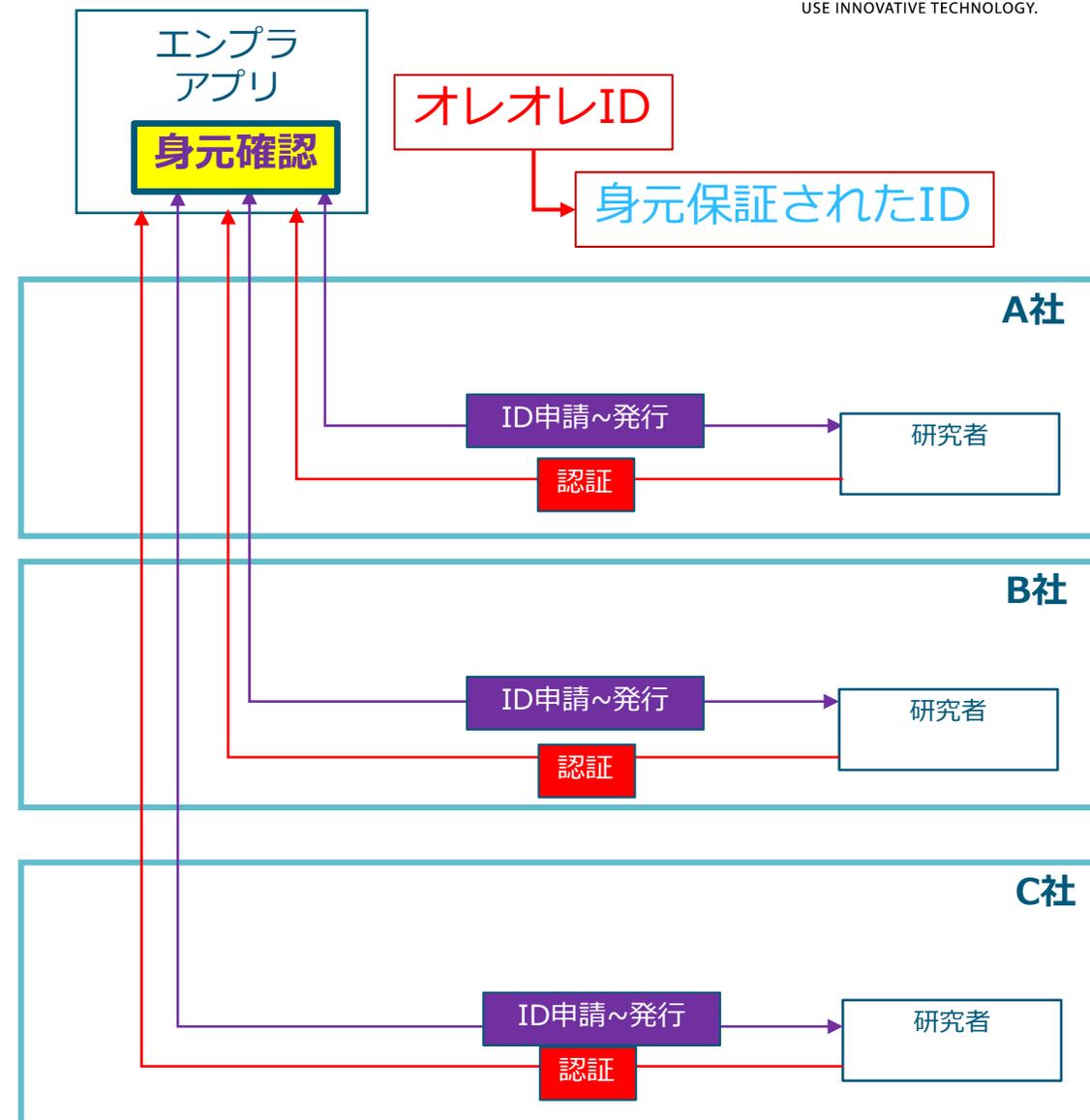
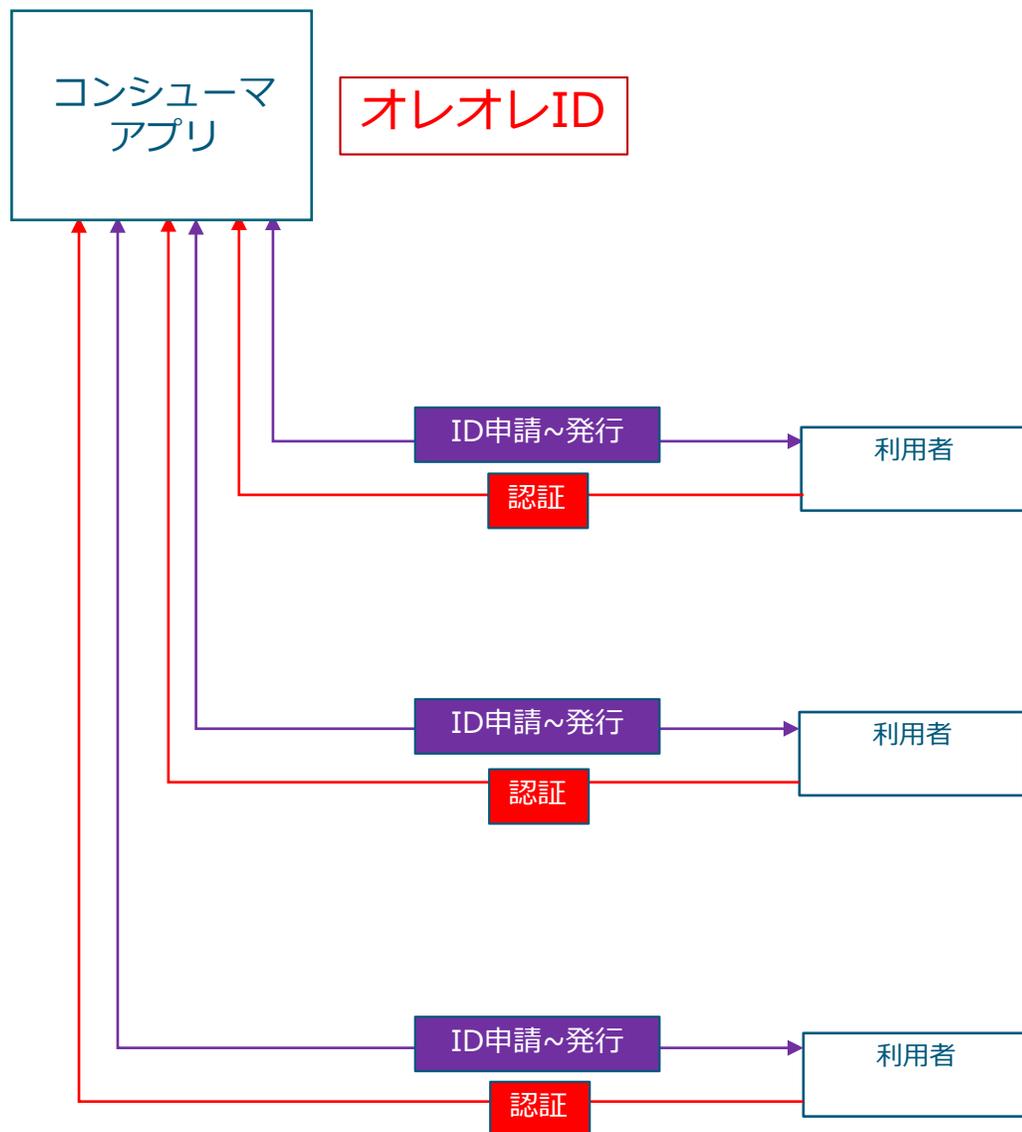
3. IDaaSやOpenIdPの必要性

(3) コンシューマアプリとエンブラアプリ



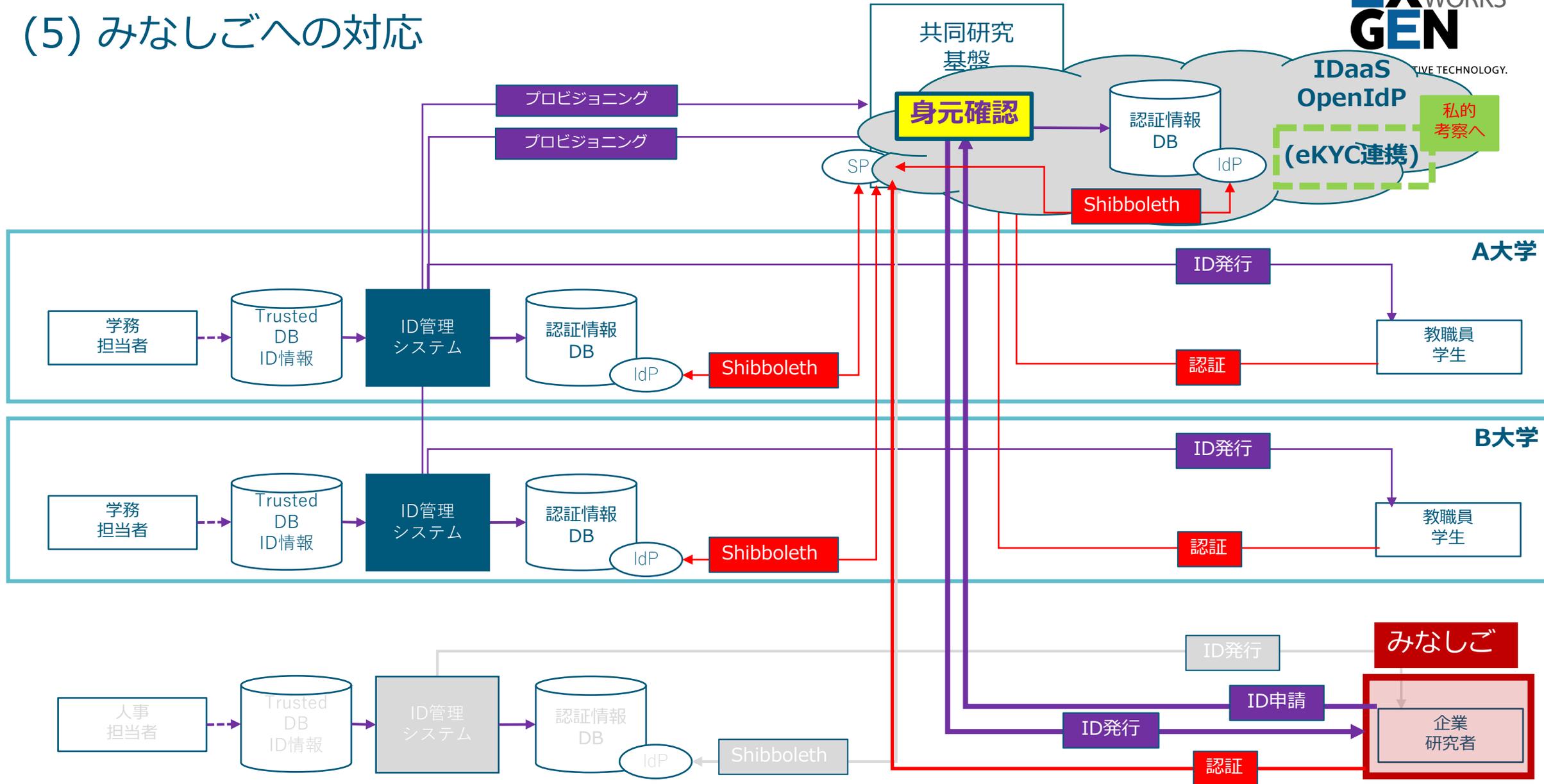
3. IDaaSやOpenIdPの必要性

(4) コンシューマアプリとエンプラアプリ



3. IDaaSやOpenIdPの必要性

(5) みなしごへの対応



3. IDaaSやOpenIdPの必要性

(6) 私的考察

[教育産業におけるeKYCビジネス]

- 学生証や社員証はそれ自体がeKYCのevidenceとして利用される可能性のあるもの。
この発行機関である大学や企業がID発行時にeKYCを利用するケースは少なく、前ページのように研究コミュニティが、企業研究者のようなみなしごに、IDを発行する場合にeKYCを利用するケースが多いのではないか。

[研究コミュニティが要求するeKYCの中身と課題]

- 「実在性の確認」に関しては、ID発行以外の分野での事例も多く、validationを含めて、研究コミュニティでも利用可能と考えられる。
- 但し、共同研究基盤では本人確認として利用者の「在籍の確認」を必要としている。
ある研究コミュニティでは、現在、IDを発行する時、対面での本人確認を実施し、身分証として、学生証、社員証、職員証等の提示を求め、その中で、申請者の氏名と所属機関名が記載されており、その所属機関が申請者の身分を認める旨の記述があることの確認を行っている。
- eKYCで「在籍の確認」が、十分な保証レベルで実施できるか。特に学生証、社員証のvalidationをどうするか。
これは学生証、社員証を発行する所属機関の協力が必要となるはず。