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～

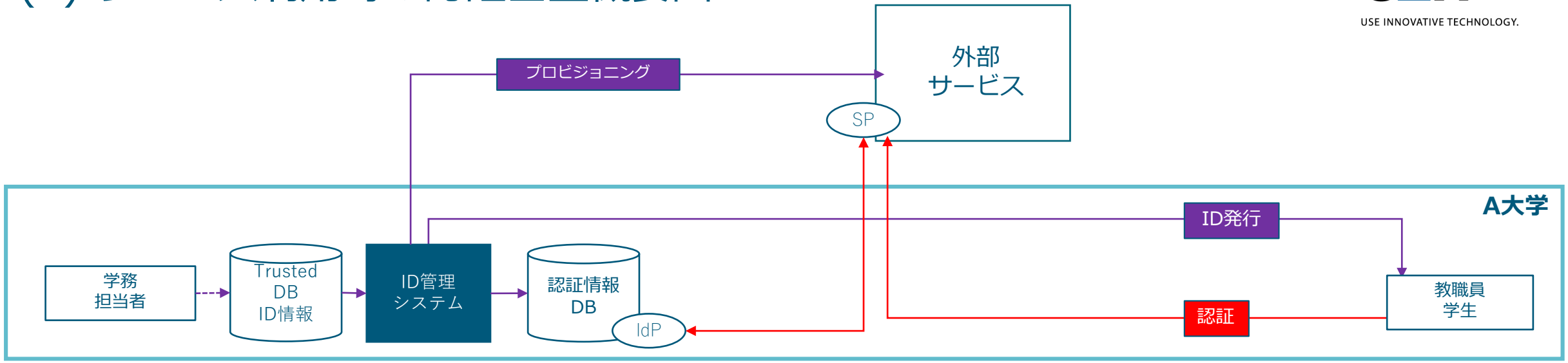
2021年10月8日

エクスジェン・ネットワークス株式会社
江川 淳一

USE INNOVATIVE TECHNOLOGY.

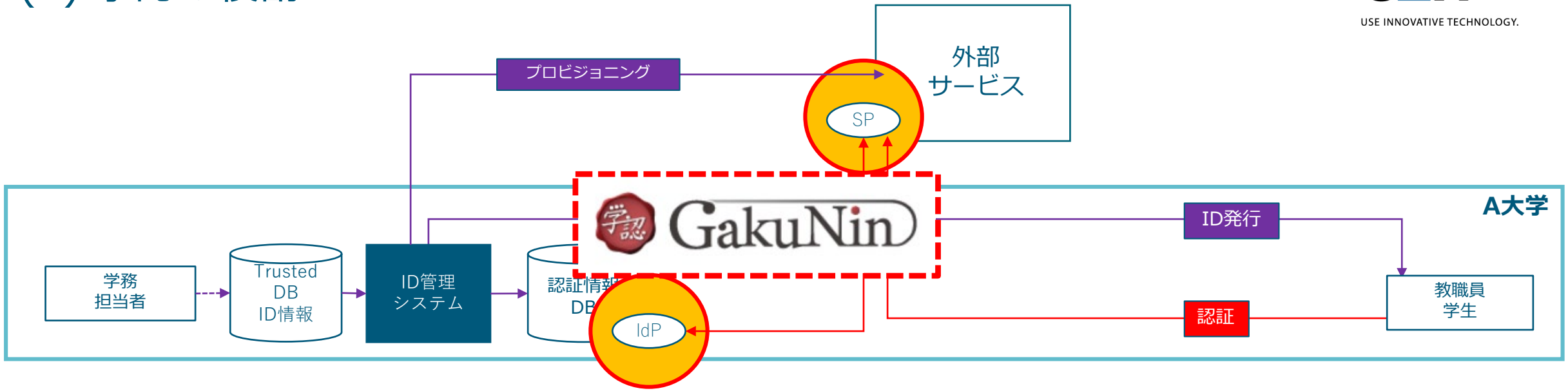
1. 学認とは

(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



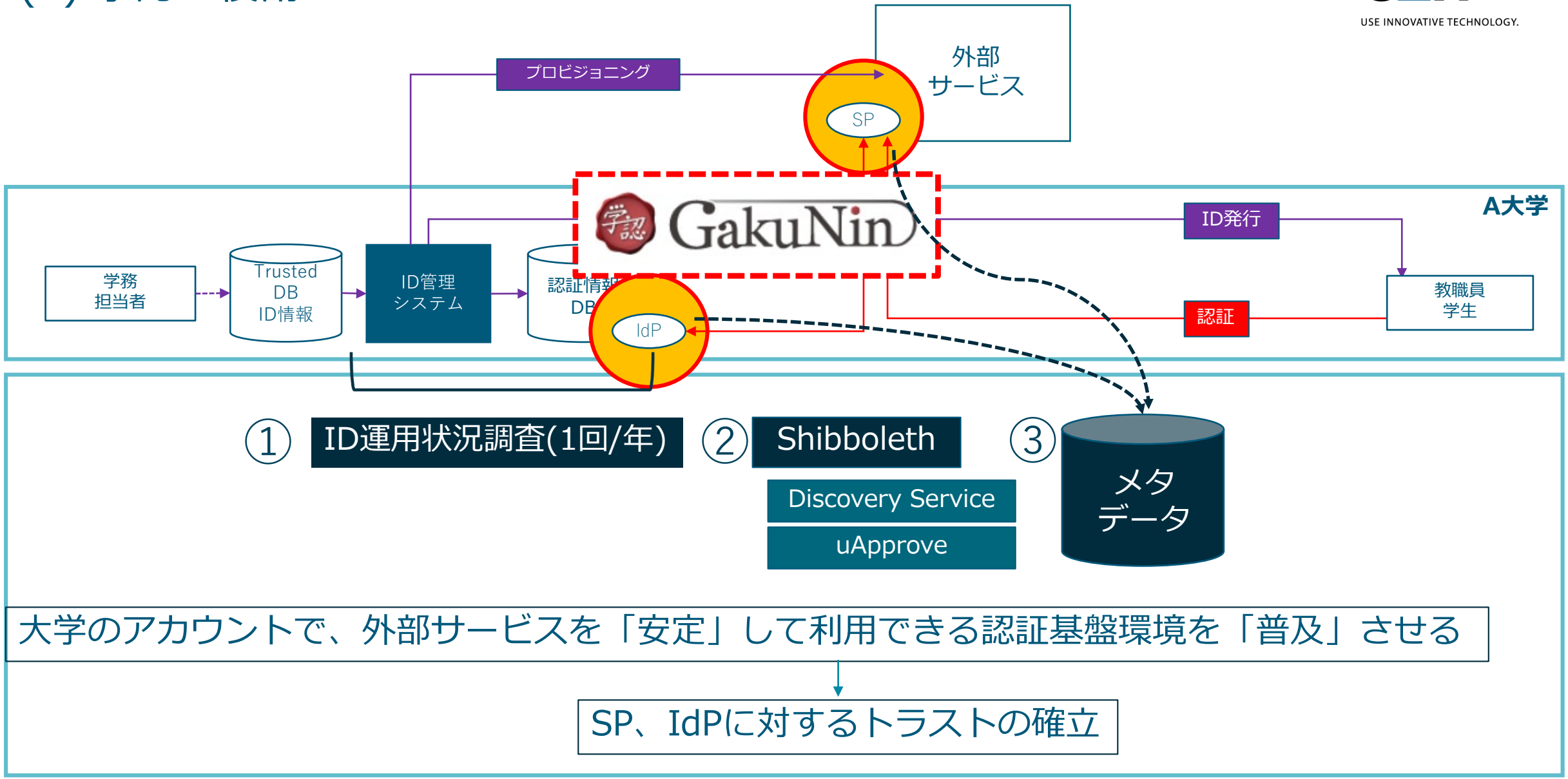
大学のアカウントで、外部サービスを「安定」して利用できる認証基盤環境を「普及」させる

↓

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。

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

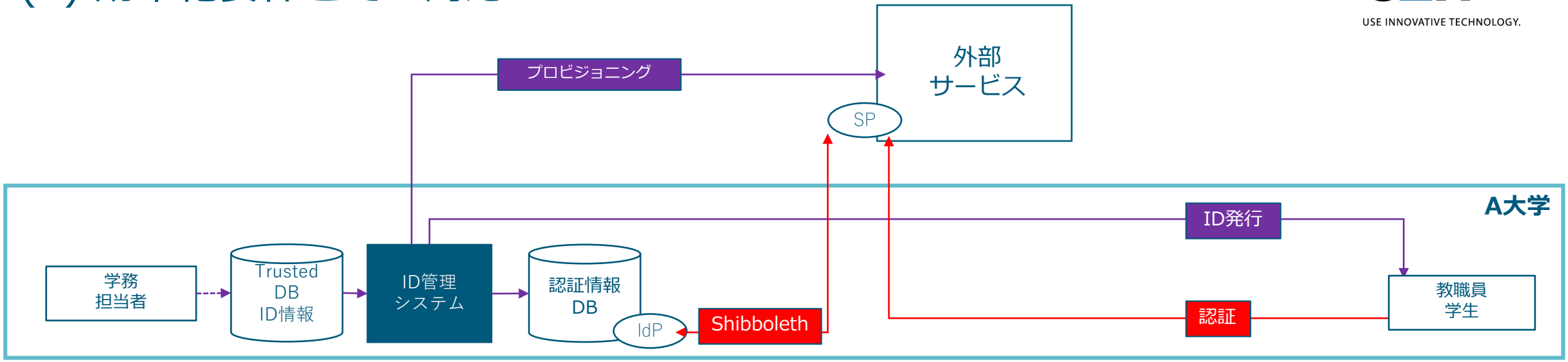
2. 教育・研究業界の新たな要件

(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。

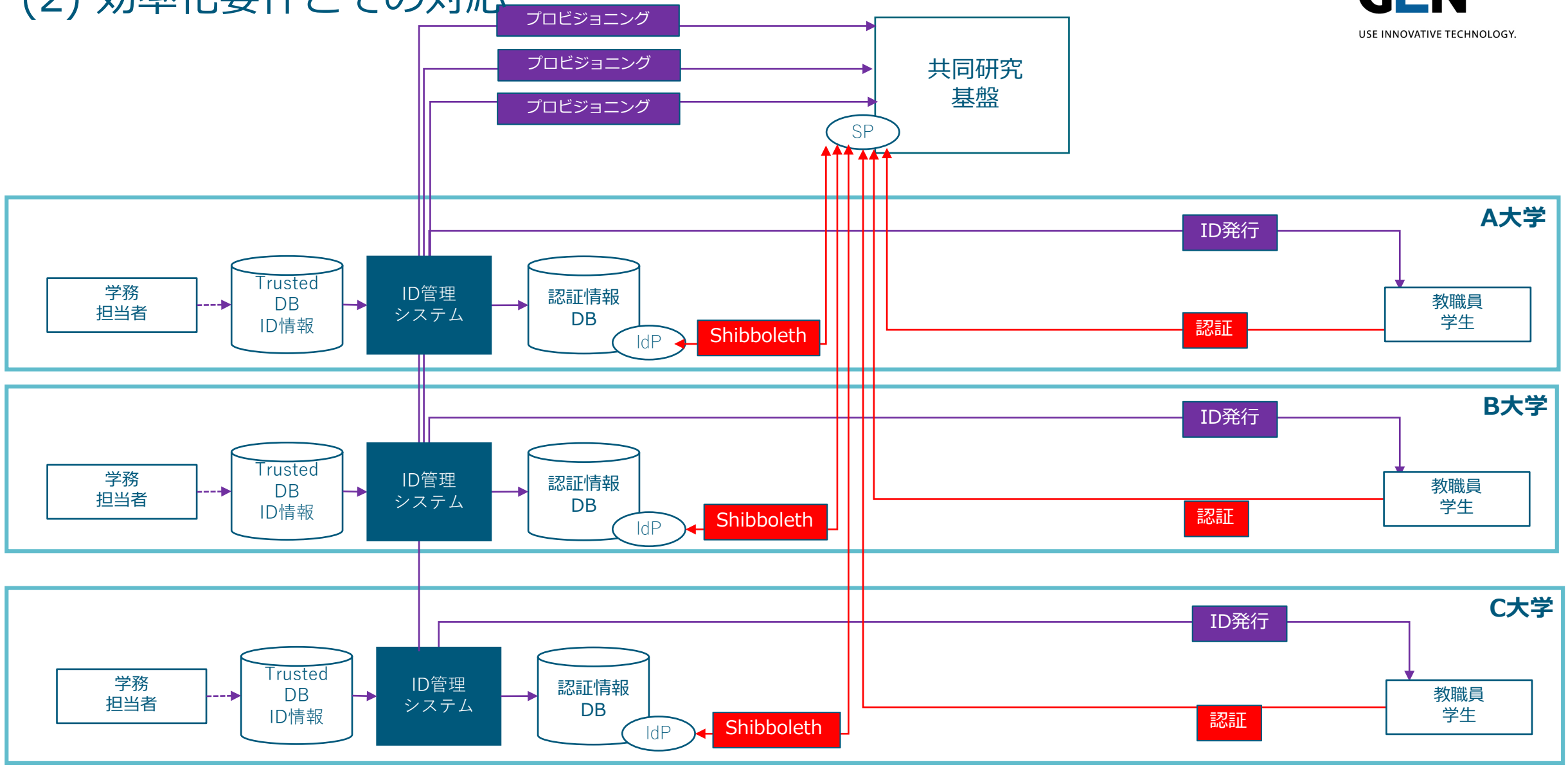
2. 教育・研究業界の新たな要件

(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

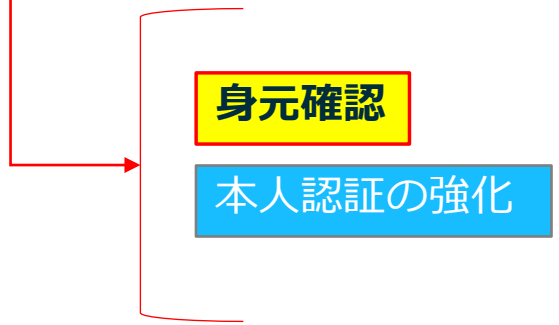


2. 教育・研究業界の新たな要件

(3) セキュリティ要件とその対応

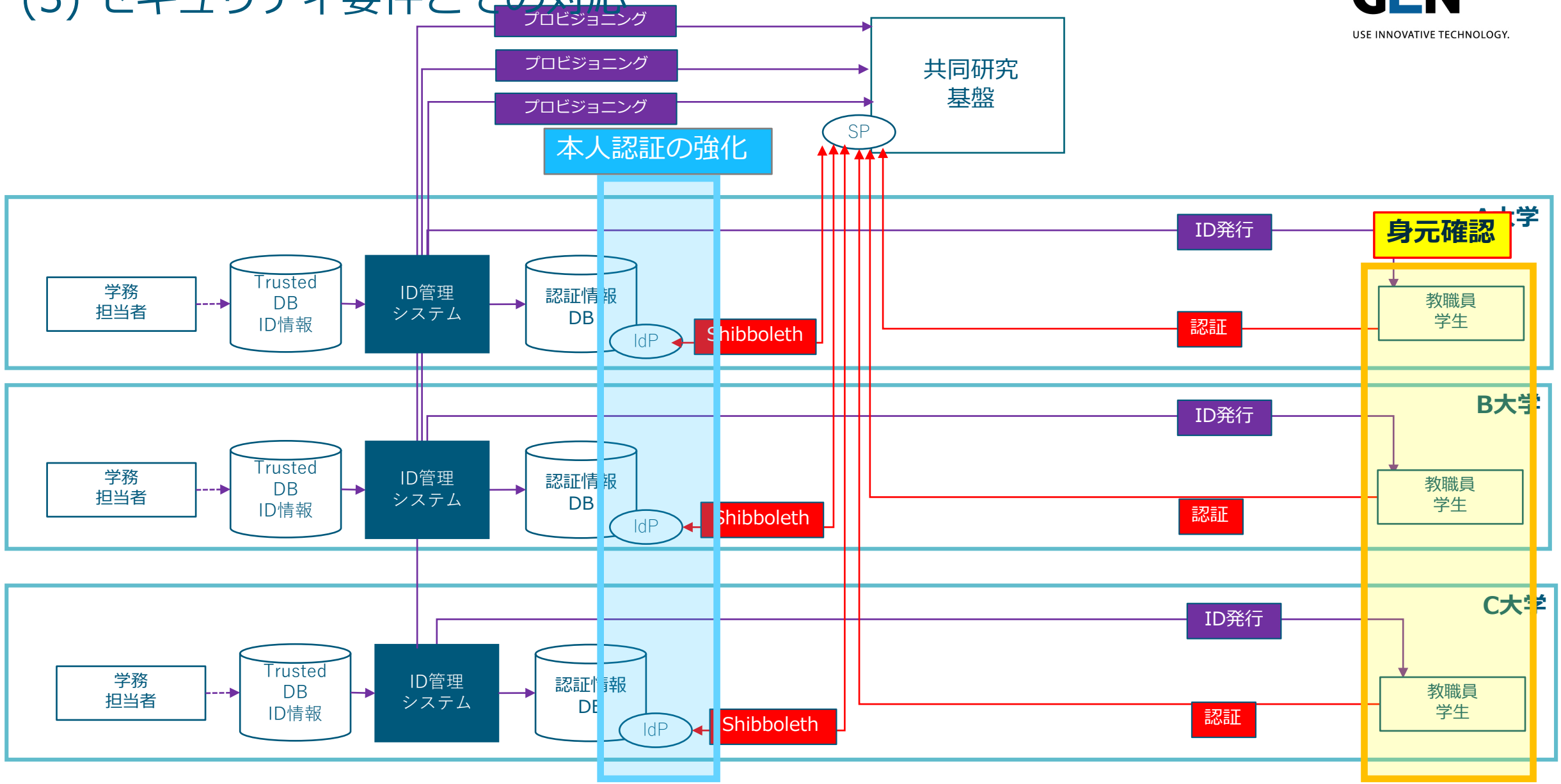
・高度なサービス、リソースを共同利用(情報共有)するためには、組織内利用時よりも
セキュアな本人確認が必要

・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



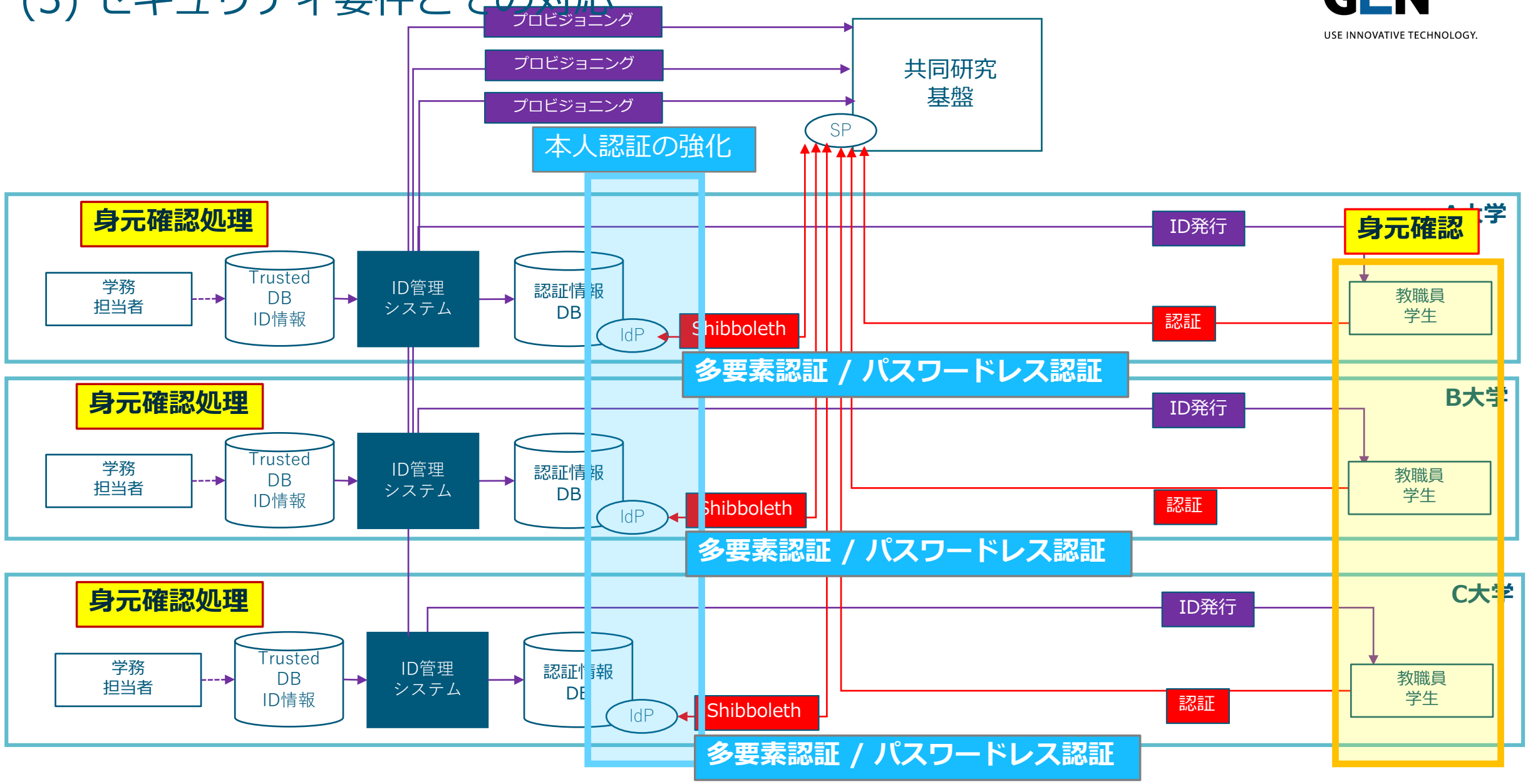
2. 教育・研究業界の新たな要件

(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。

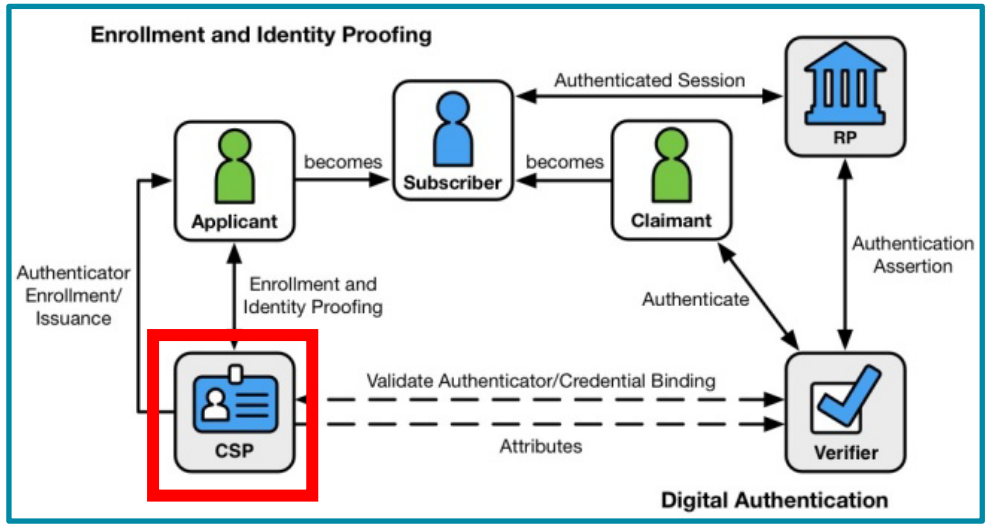
[新たな役割]

・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。

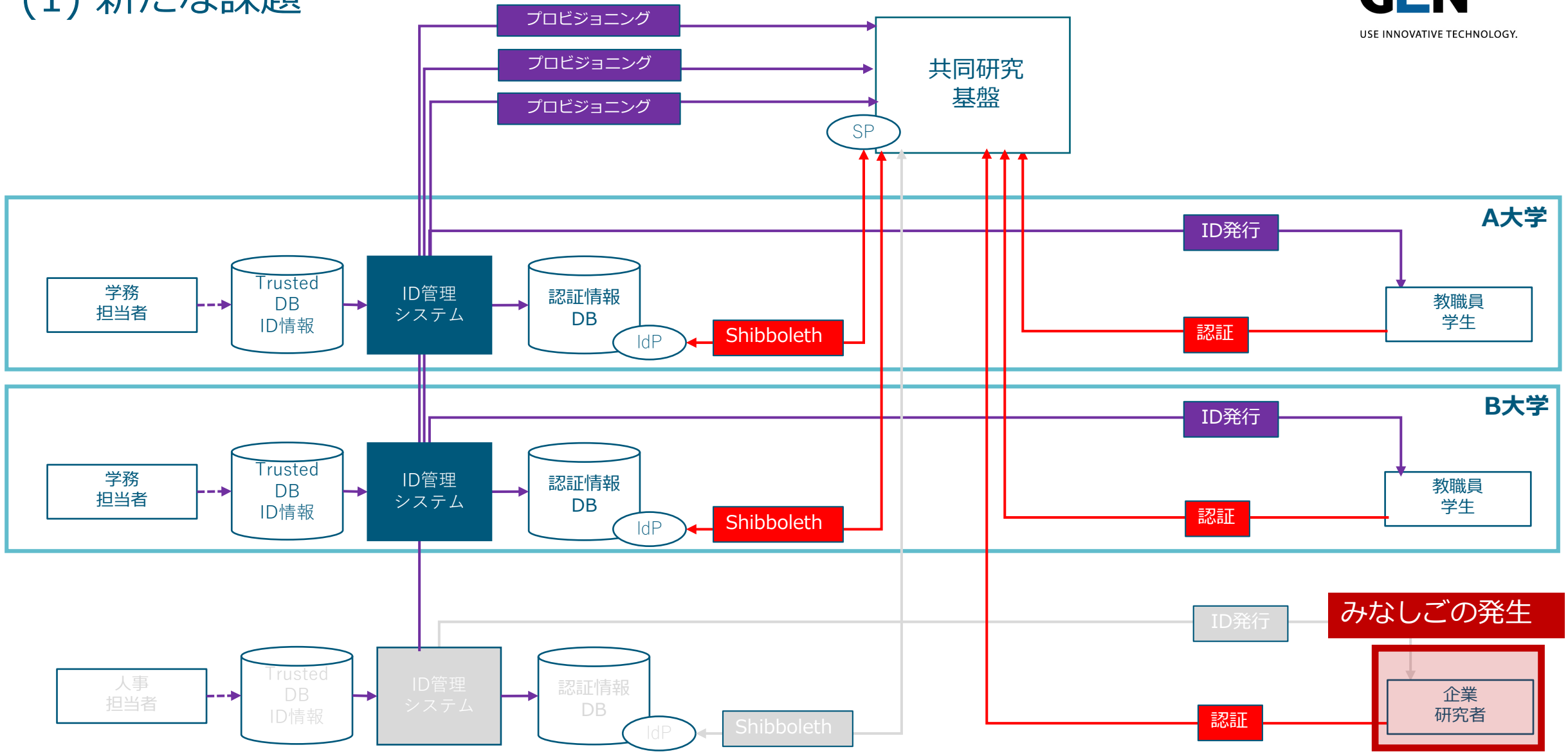
・大学等組織に対して

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、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とエンプラ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とエンプラ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

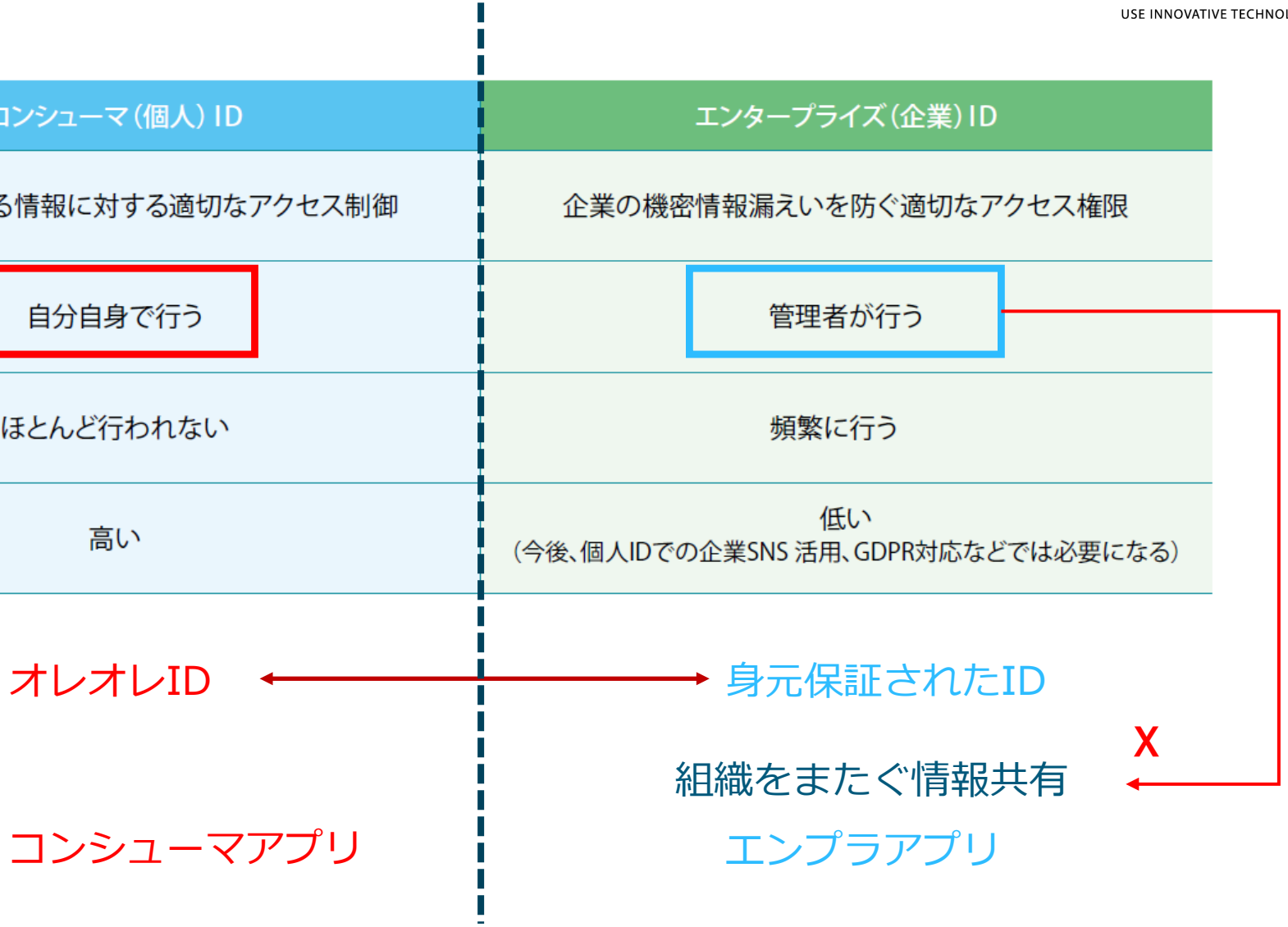
組織内での情報共有

コンシューマアプリ　　エンプラアプリ

3. IDaaSやOpenIdPの必要性

(2) コンシューマIDとエンプラ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）



3. IDaaSやOpenIdPの必要性

(2) コンシューマIDとエンプラ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）

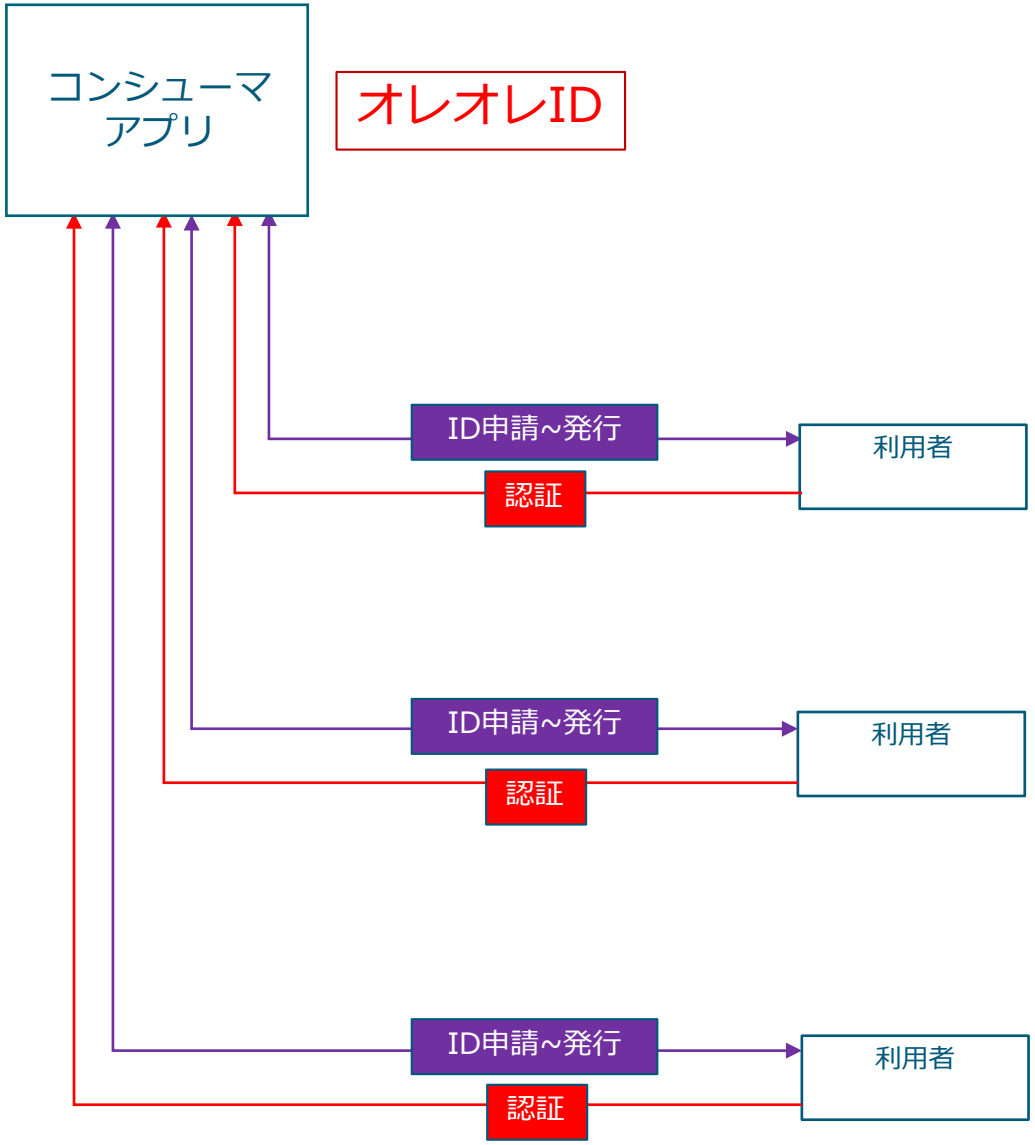
身元保証されたID

組織をまたぐ情報共有

エンプラアプリ

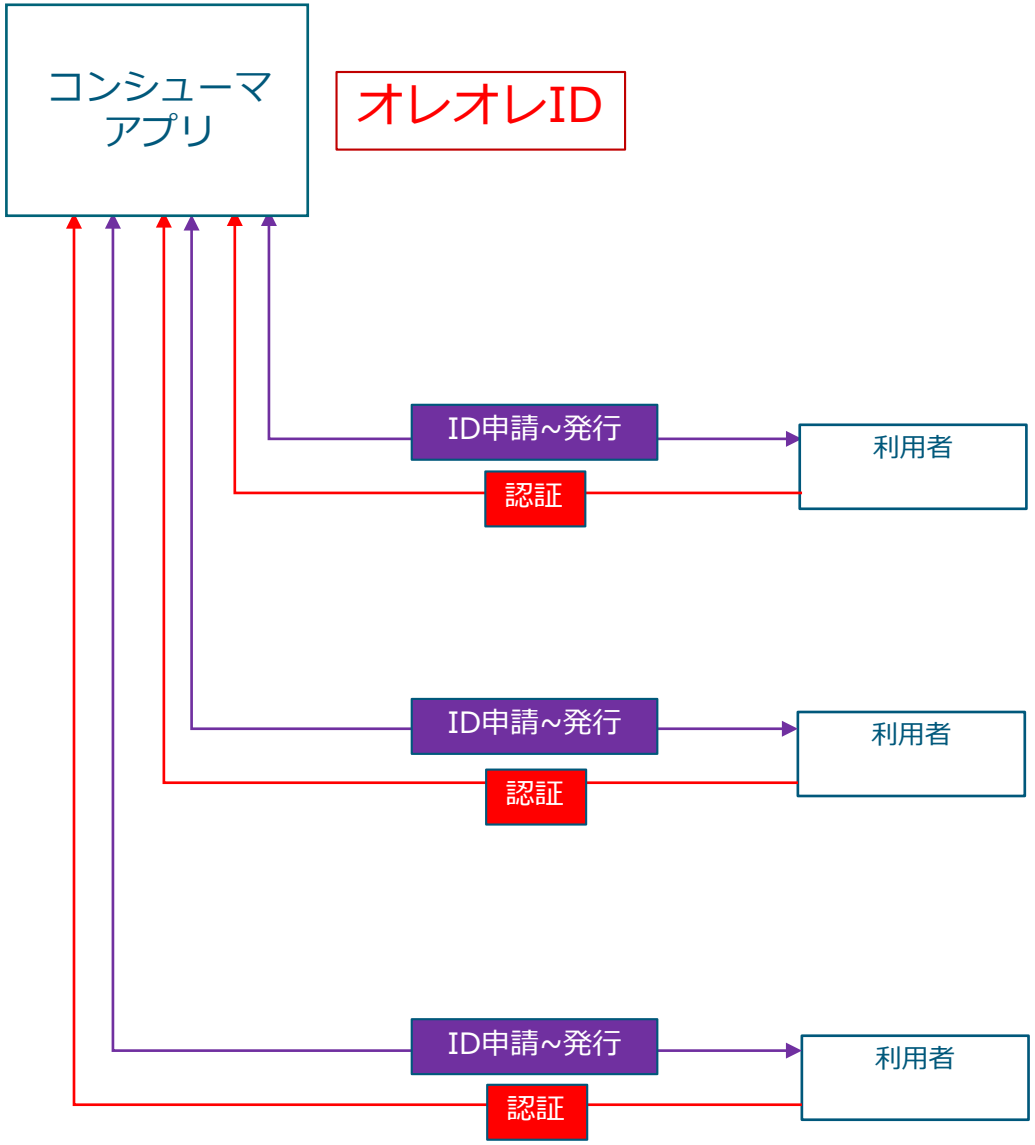
3. IDaaSやOpenIdPの必要性

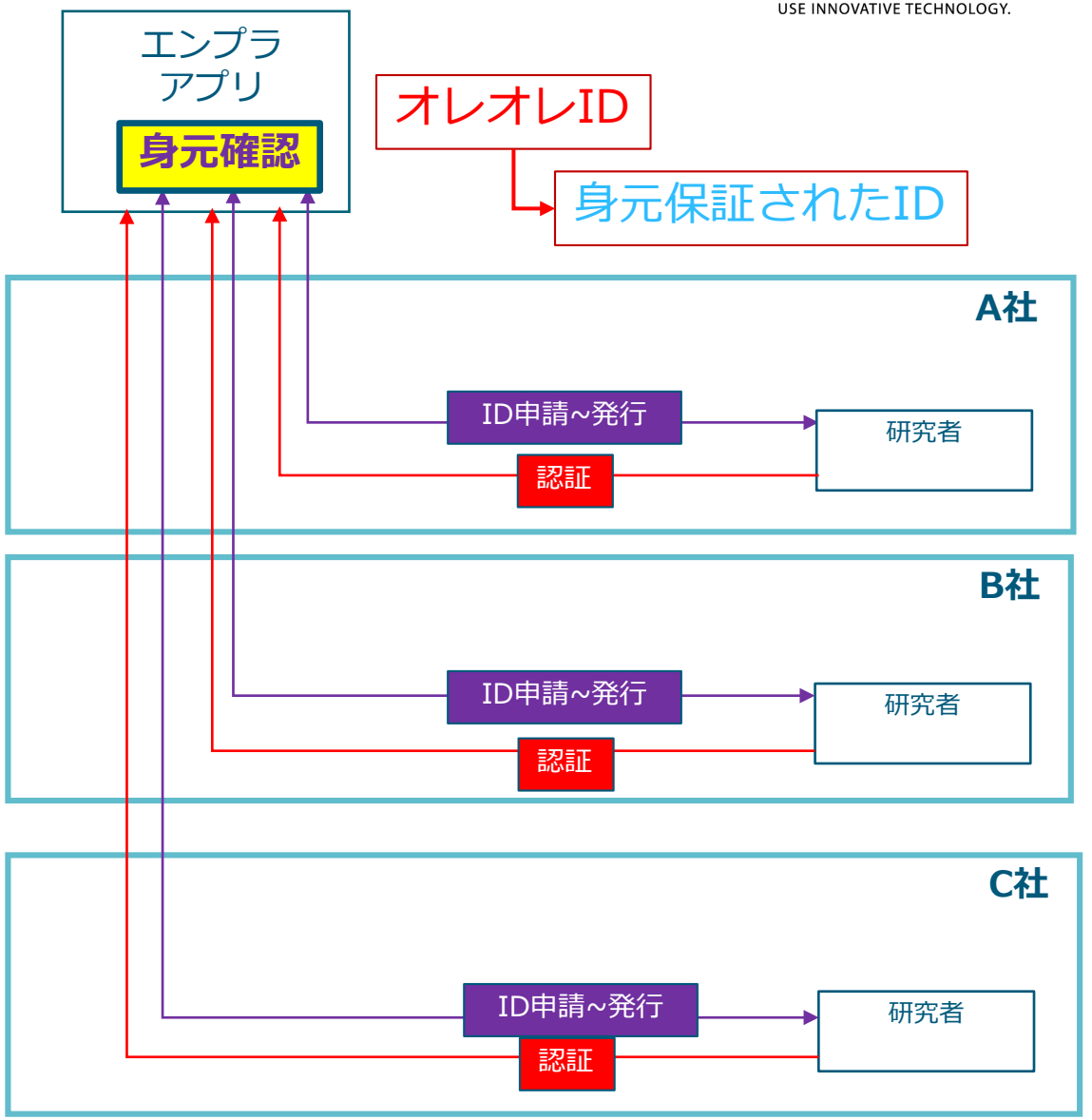
(3) コンシューマアプリとエンプラアプリ



3. IDaaSやOpenIdPの必要性

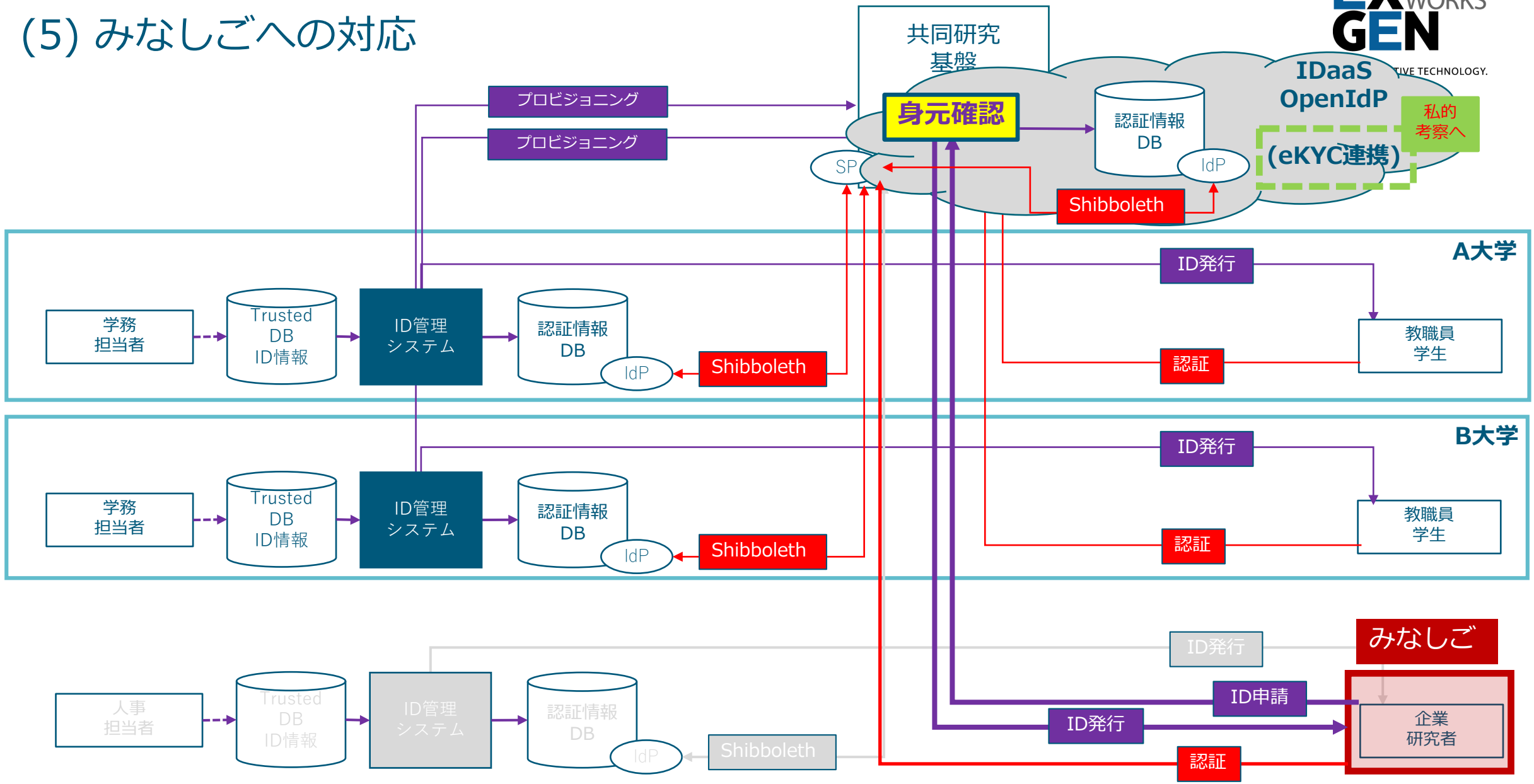
(4) コンシューマアプリとエンプラアプリ





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。