アカデミックIDaaSのオモテとウラ

オ モ テ
(理想像編)

2017年3月10日

エクスジェン・ネットワークス(株)

USE INNOVATIVE TECHNOLOGY.

1. 今後のIT基盤＆認証基盤に求められる要件

目的 より良い教育に資するIT基盤構築

戦略 デジタルトランスフォーメーションの流れに乗る
(クラウドの有効活用など)

そのための 手段 認証基盤整備 → IDaaS

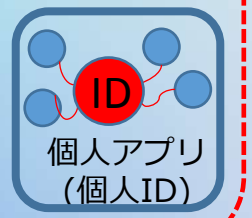
Copyright© 2017 EXGEN NETWORKS Co.,LTD. All Rights Reserved.

1. 今後のIT基盤＆認証基盤に求められる要件

大学内だけではなく、
様々な場所から

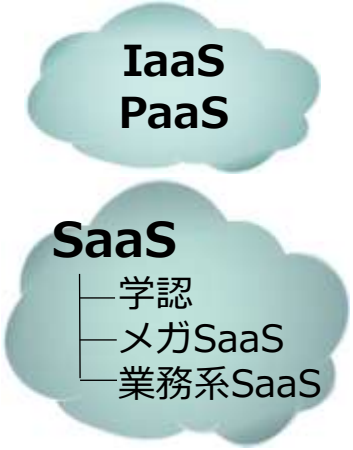
教職員、学生だけではなく
様々な人が

さらに、Lineや
Facebook等
個人のアプリや
IDを利用する
場合もある。



大学内のPCだけではなく、
様々なデバイスを介して
利用する、

大学内だけではなく、
様々な場所にある
システムやデータを



様々なハイブリッド環境に対応できるアカデミックIT基盤

Copyright© 2017 EXGEN NET

1. 今後のIT基盤＆認証基盤に求められる要件

大学内だけではなく、
様々な場所から

教職員、学生だけではなく
様々な人が

大学内だけではなく、
様々な場所にある
システムやデータを

IaaS
PaaS

aS
学認
メガSaaS
業務系SaaS

さらに
Face
個人の
IDを
場合も

認証基盤

様々な人が
様々な場所から
ハイブリッドクラウドを
ハイブリッドデバイスとハイブリッドIDで
セキュアに効率良く利用するための

様々なハイブリッド環境に対応できるアカデミックIT基盤

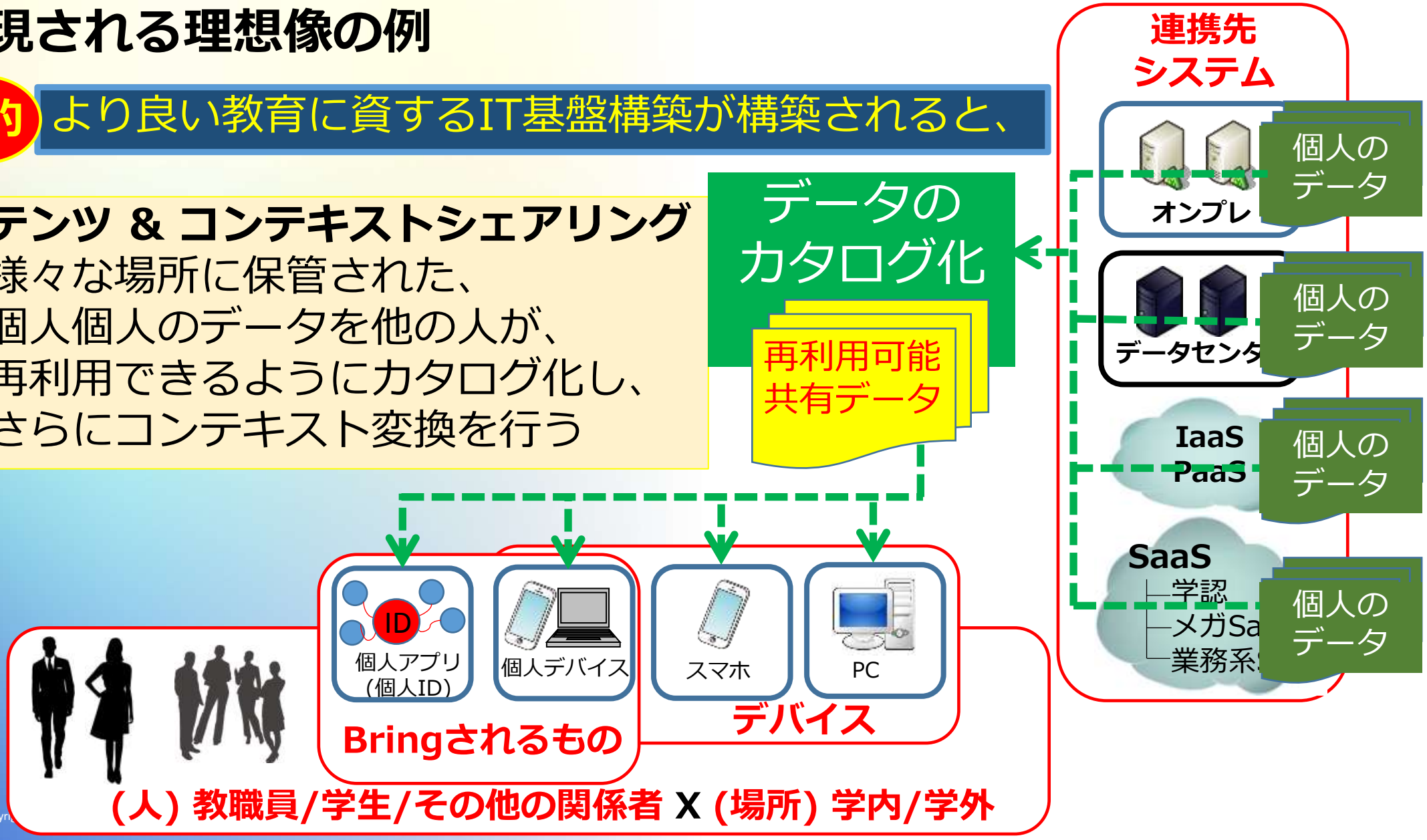
Copyright© 2017 EXGEN NET

1. 今後のIT基盤＆認証基盤に求められる要件
実現される理想像の例

目的 より良い教育に資するIT基盤構築が構築されると、

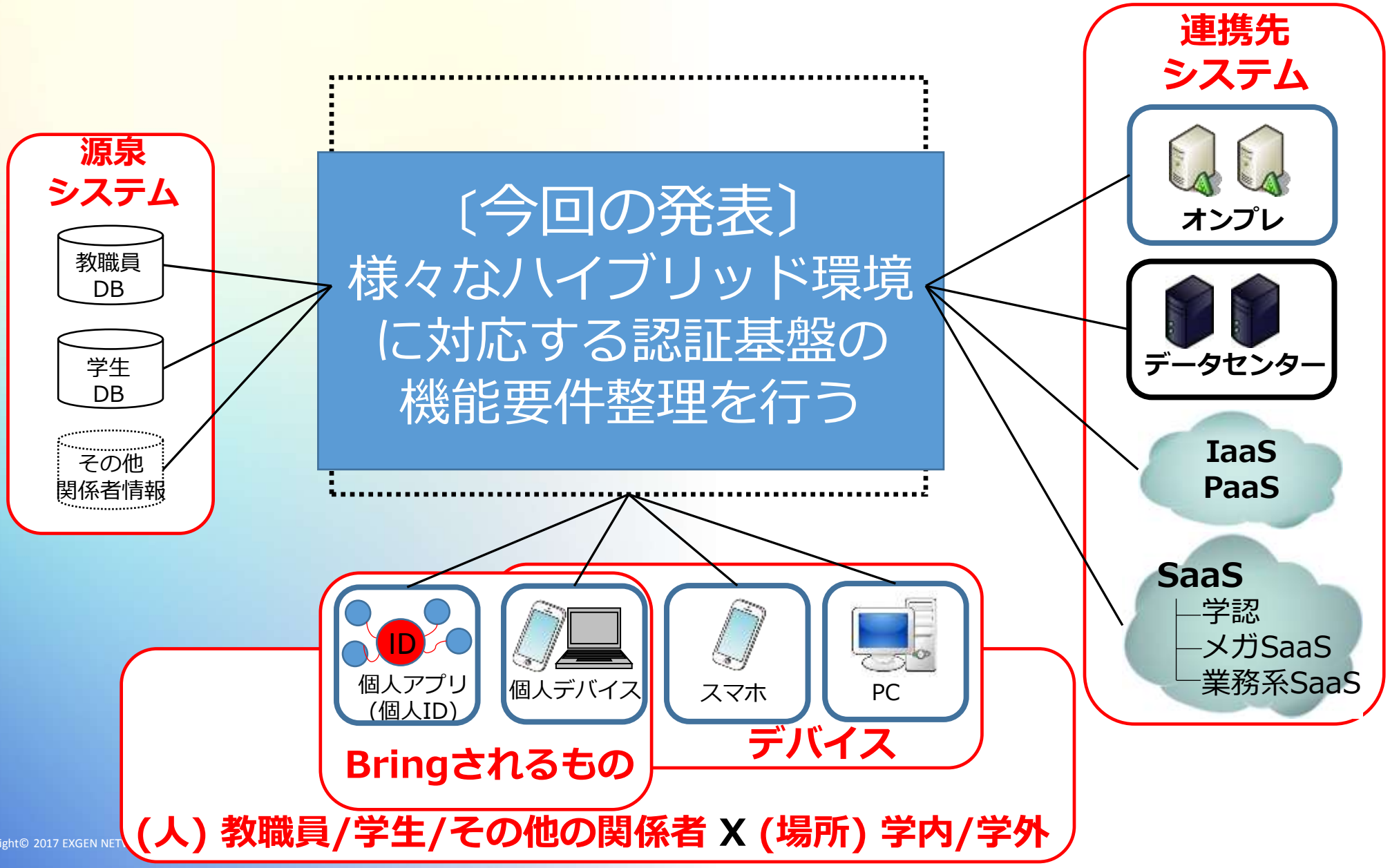
コンテンツ ＆ コンテキストシェアリング

・様々な場所に保管された、
個人個人のデータを他の人が、
再利用できるようにカタログ化し、
さらにコンテキスト変換を行う



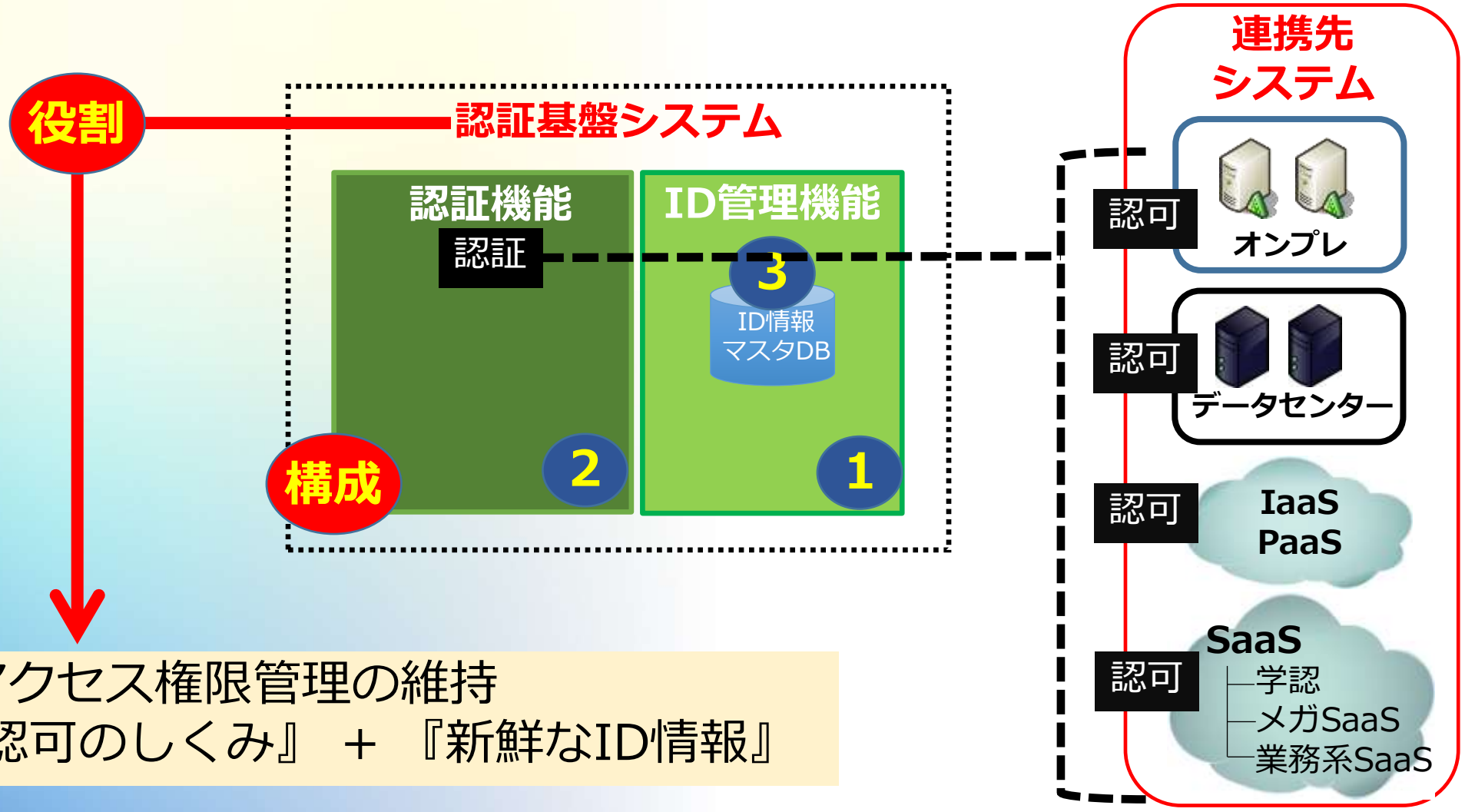
Copyri

2. 認証基盤システム概要



Copyright© 2017 EXGEN NET

2. 認証基盤システム概要

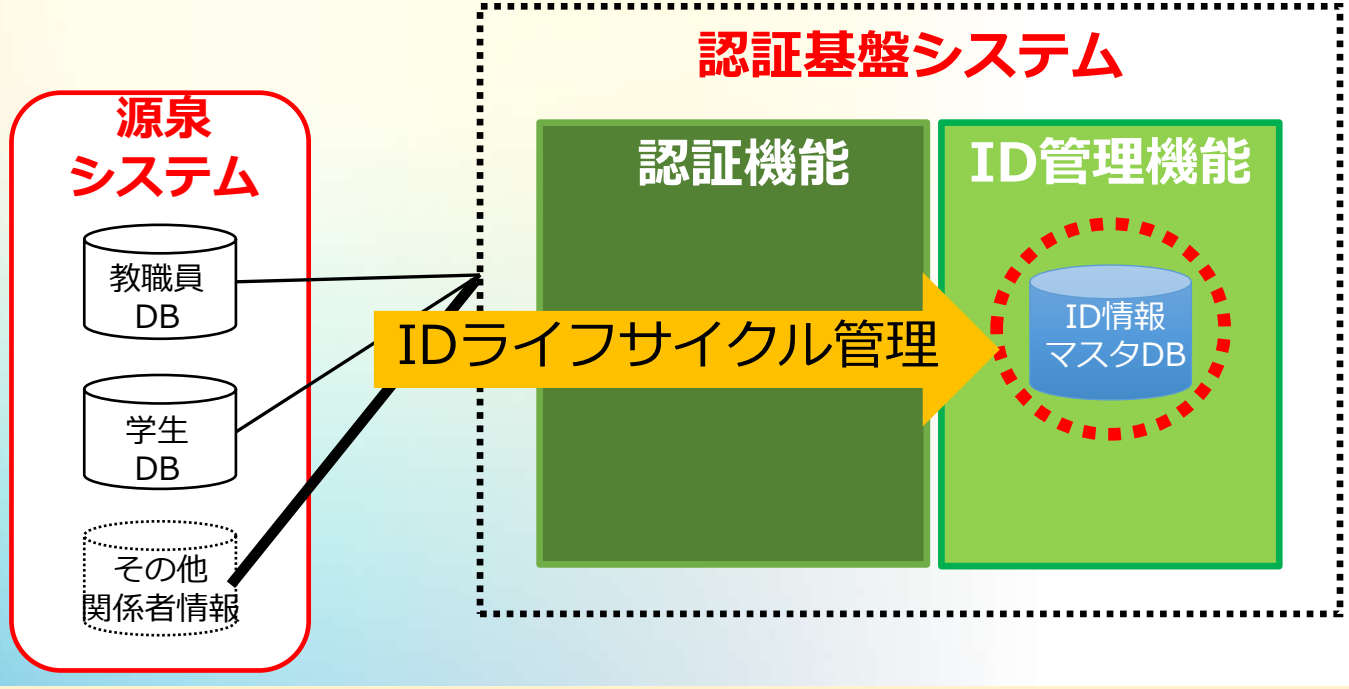


適切なアクセス権限管理の維持
『認証/認可のしくみ』 ＋ 『新鮮なID情報』

Copyright© 2017 EXGEN NETWORKS Co.,LTD. All Rights Reserved.

3. 認証基盤システムの詳細要件

3.1 源泉システム関連

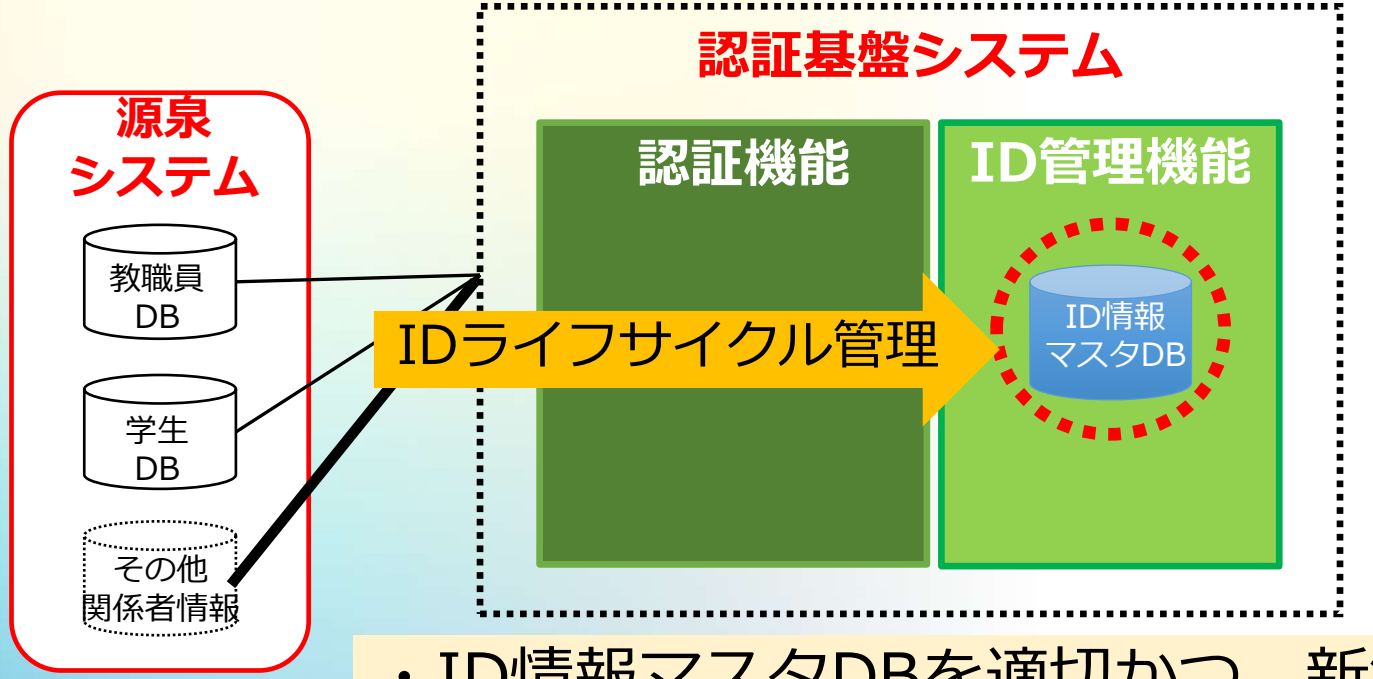


- 教職員DB、学生DBだけではなく、その他関係者の情報を含めた**ID情報マスタDB**を構築し管理する。
- その他関係者情報は源泉DBが整備されていない場合が多いので、**IDライフサイクル管理**には、**GUIメンテ、 CSV連携、API連携**以外に**ワークフロー機能**等も必要。

Copyright© 2017 EXGEN NETWORKS Co.,LTD. All Rights Reserved.

3. 認証基盤システムの詳細要件

3.1 源泉システム関連

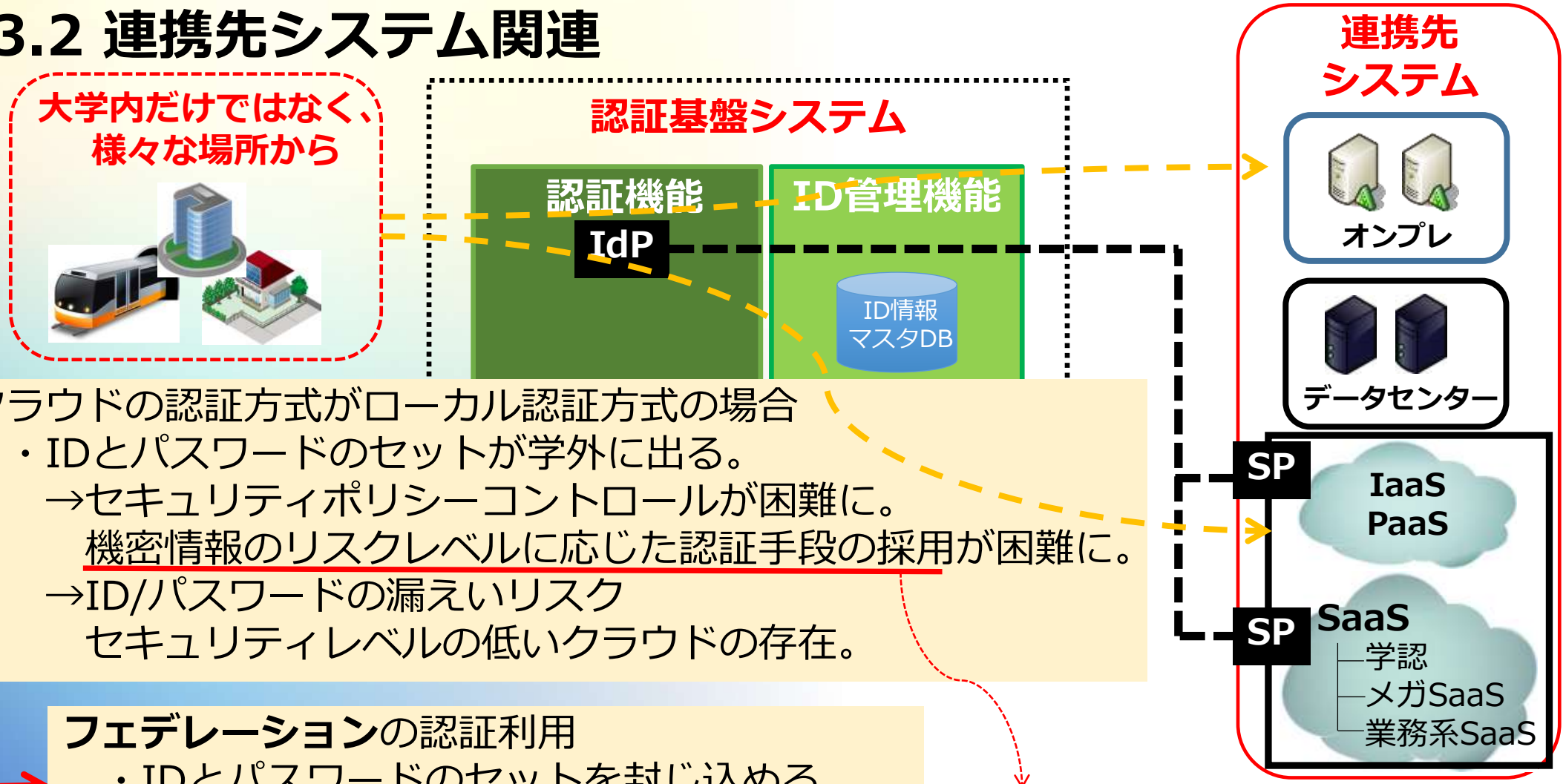


・ID情報マスタDBを適切かつ、新鮮な状態に保つためには
(構築/再構築時)
　・**棚卸し(クリーニング)**後、ID情報の投入。 最初が肝心！
(ID運用管理開始後)
　・ID管理機能を利用し、ID情報の鮮度を保つ**運用の徹底**。

Copyright© 2017 EXGEN NETWORKS Co.,LTD. All Rights Reserved.

3. 認証基盤システムの詳細要件

3.2 連携先システム関連



クラウドの認証方式がローカル認証方式の場合
- IDとパスワードのセットが学外に出る。
  - →セキュリティポリシーコントロールが困難に。
    機密情報のリスクレベルに応じた認証手段の採用が困難に。
  - →ID/パスワードの漏えいリスク
    セキュリティレベルの低いクラウドの存在。

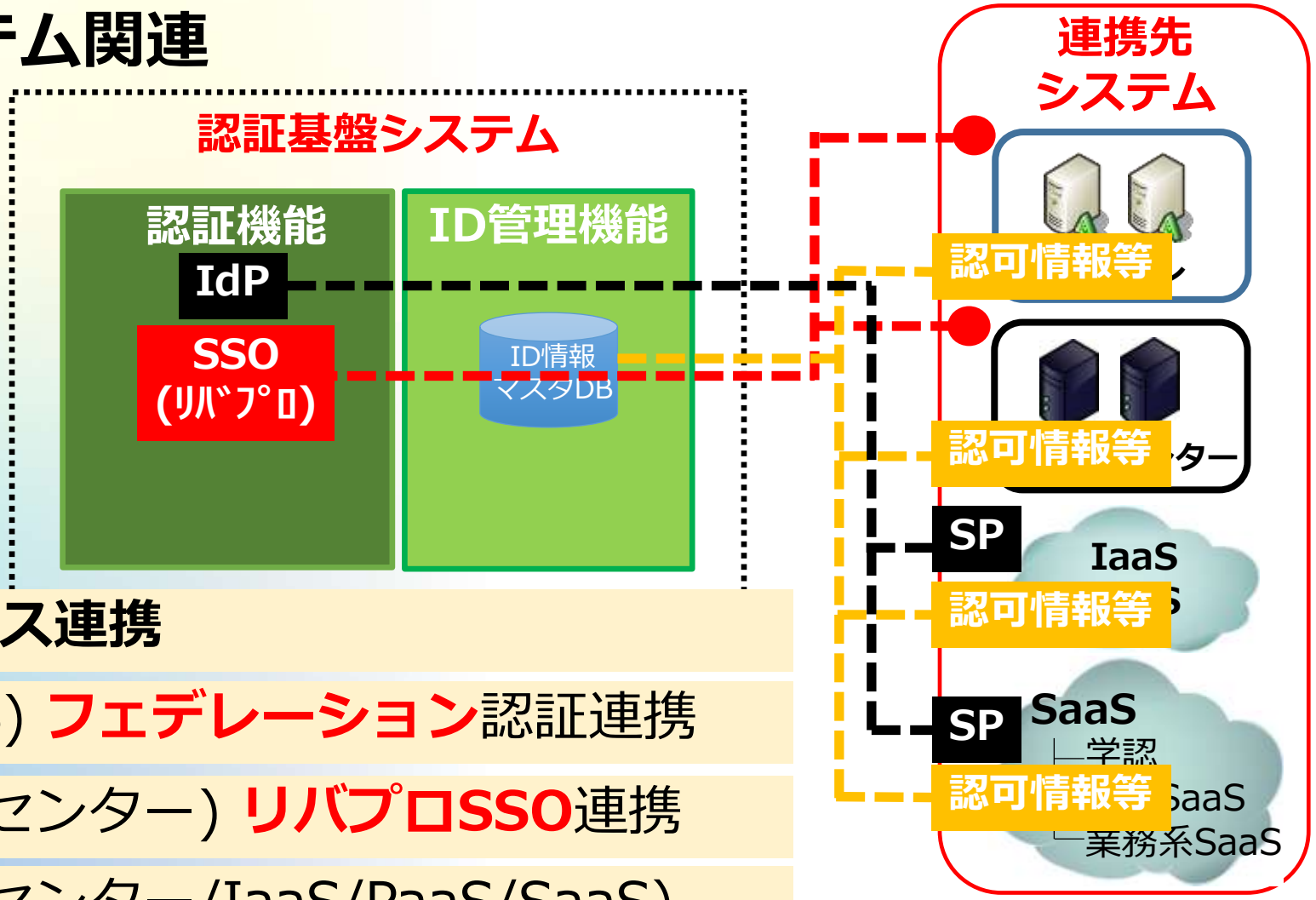
フェデレーションの認証利用
- IDとパスワードのセットを封じ込める。
- フェデレーションプロトコルの認証利用。

IdP側での
多要素認証の実装

Copyright© 2017 EXGEN NETWORKS Co.,LTD. All Rights Reserved.

3. 認証基盤システムの詳細要件

3.2 連携先システム関連



利用システム/サービス連携

① (IaaS/PaaS/SaaS) **フェデレーション**認証連携

② (オンプレ/データセンター) **リバプロSSO**連携

③ (オンプレ/データセンター/IaaS/PaaS/SaaS)
認可情報等の**プロビジョニング**連携

Copyright© 2017 EXGEN NETWORKS Co.,LTD. All Rights Reserved.

3. 認証基盤システムの詳細要件

3.2 連携先システム関連

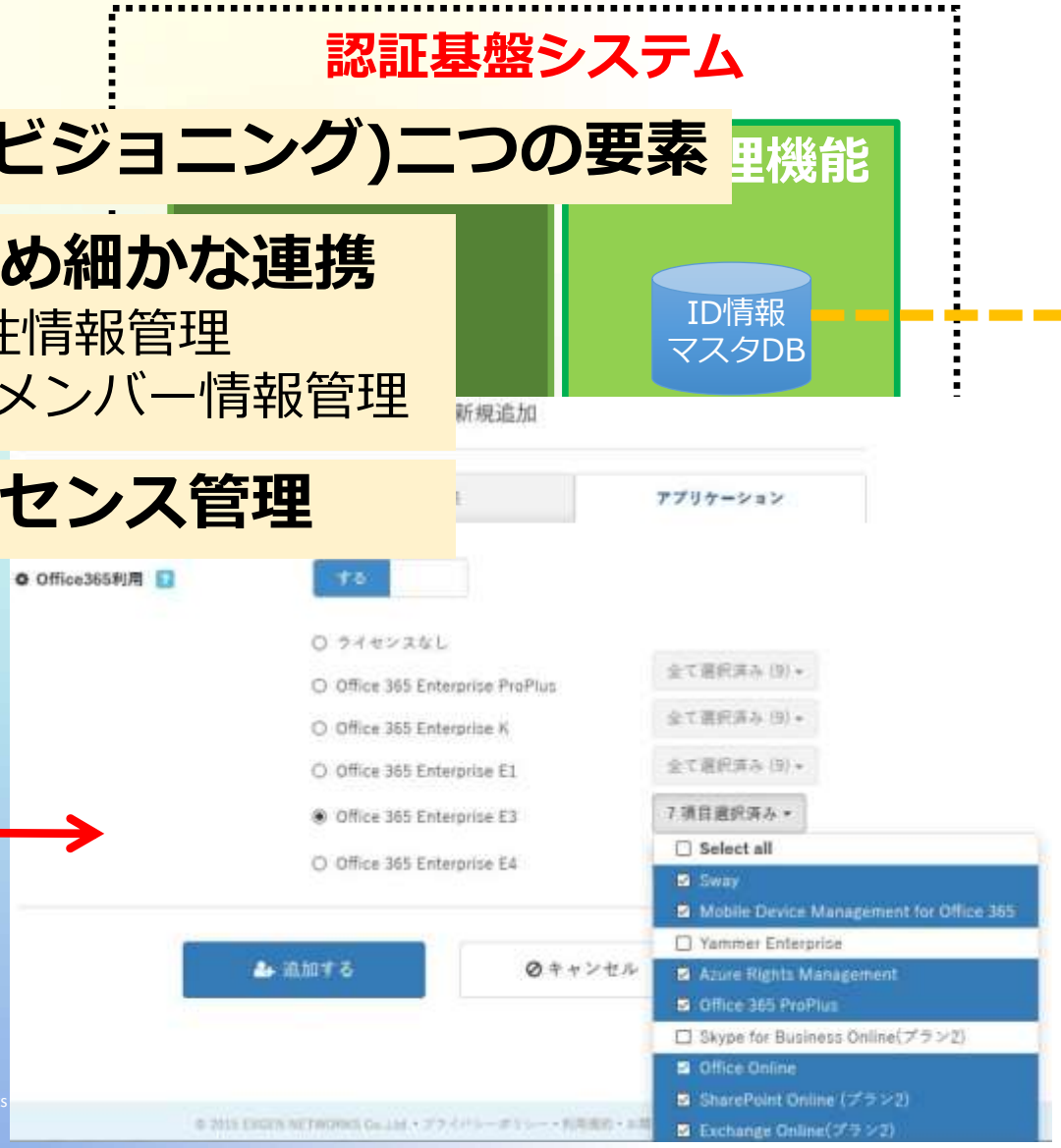
ID管理機能(プロビジョニング)二つの要素

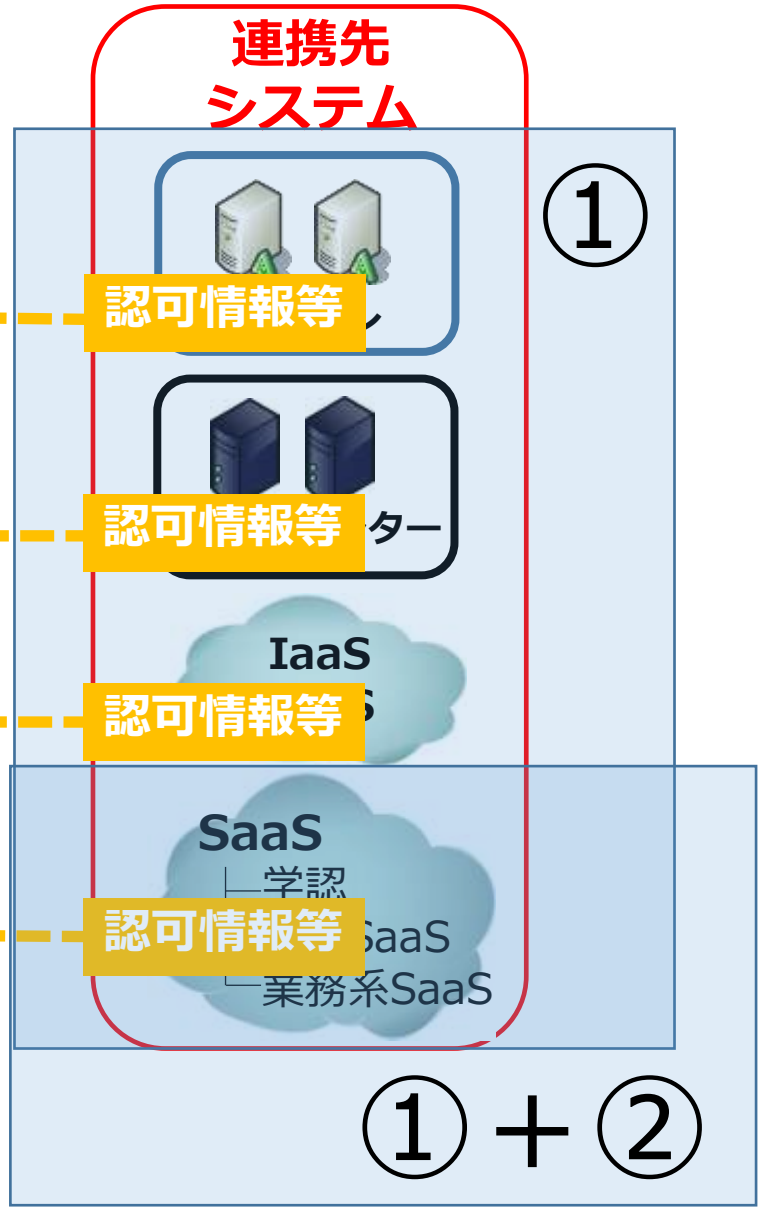
①認可情報等のきめ細かな連携

- ユーザ情報の属性情報管理
- グループ情報 & メンバー情報管理

②わかり易いライセンス管理

Exticで可能な
ライセンス管理

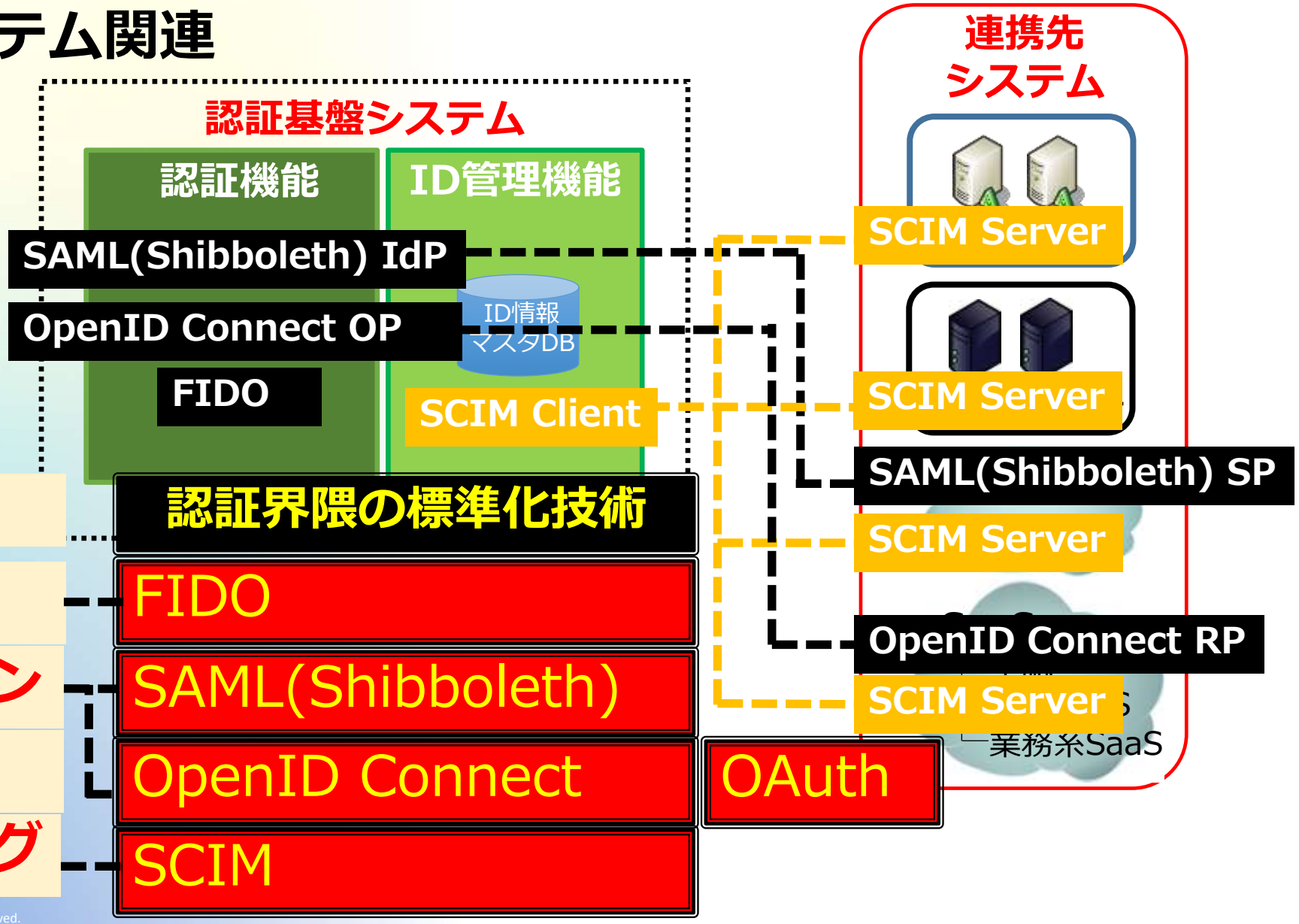




Copyright© 2017 EXGEN NETWORKS Co.,LTD. All Rights

3. 認証基盤システムの詳細要件

3.2 連携先システム関連



標準化技術の採用

多要素認証

フェデレーション

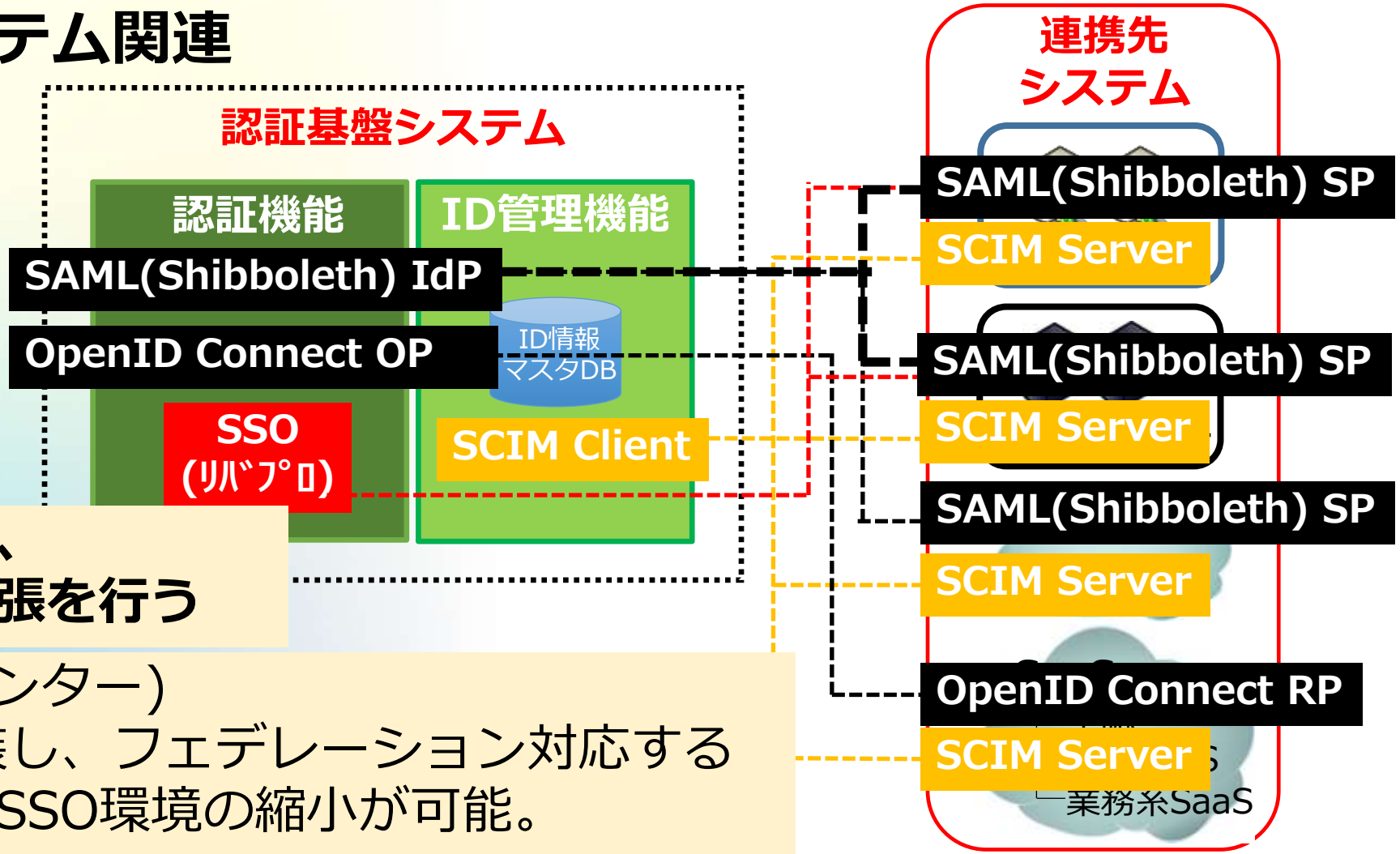
リバプロSSO

プロビジョニング

Copyright© 2017 EXGEN NETWORKS Co.,LTD. All Rights Reserved.

3. 認証基盤システムの詳細要件

3.2 連携先システム関連



標準化技術を活用し、
効率的なシステム拡張を行う

(オンプレ/データセンター)

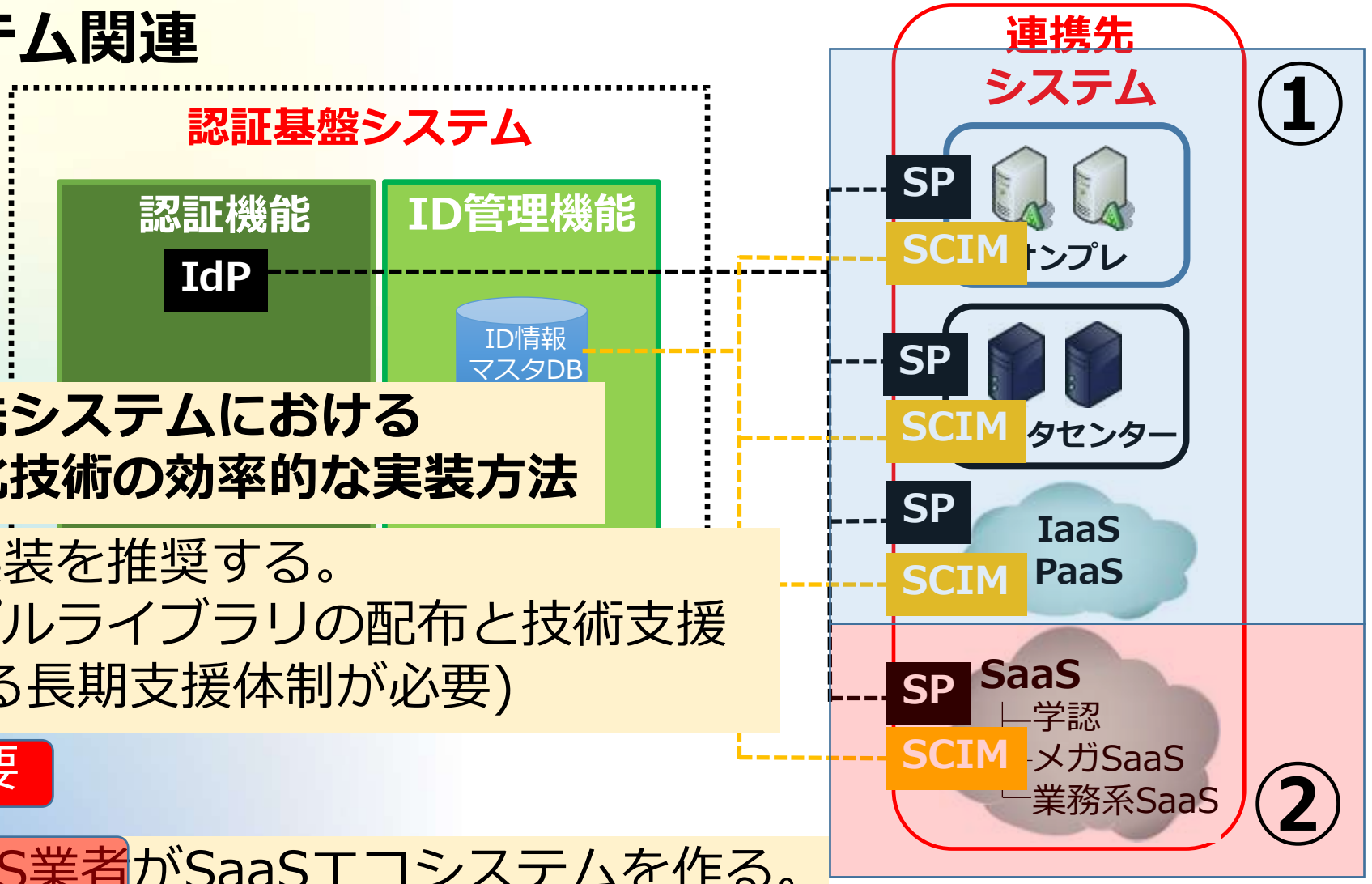
・SAML SPを実装し、フェデレーション対応することでリバプロSSO環境の縮小が可能。

連携先システムにおける、標準化技術の実装
SAML SP (OpenID Connect RP)& SCIM Server

Copyright© 2017 EXGEN NETWORKS Co

3. 認証基盤システムの詳細要件

3.2 連携先システム関連



IdP ---- SP
IDM → SCIM

連携先システムにおける
標準化技術の効率的な実装方法

① 大学が標準APIを実装を推奨する。
・SIerによるサンプルライブラリの配布と技術支援
→(SIerによる長期支援体制が必要)

戦略的協業体制が必要

② IDベンダー、IDaaS業者がSaaSエコシステムを作る。
→(SaaS企業のモチベーションが必要)

ツールのカタログ化

Copyright© 2017 EXGEN NETWORKS Co.,LTD. All Rights Reserved.

3. 認証基盤システムの詳細要件

3.3 デバイス/Bringされるもの関連

認証基盤システム

(人) x (場所) ⇔ 情報 に応じた認証方式の採用

- **多要素認証デバイス**としてのBYOD利用
- 教職員 x 学外(他大学キャンパス)：**eduroam連携**

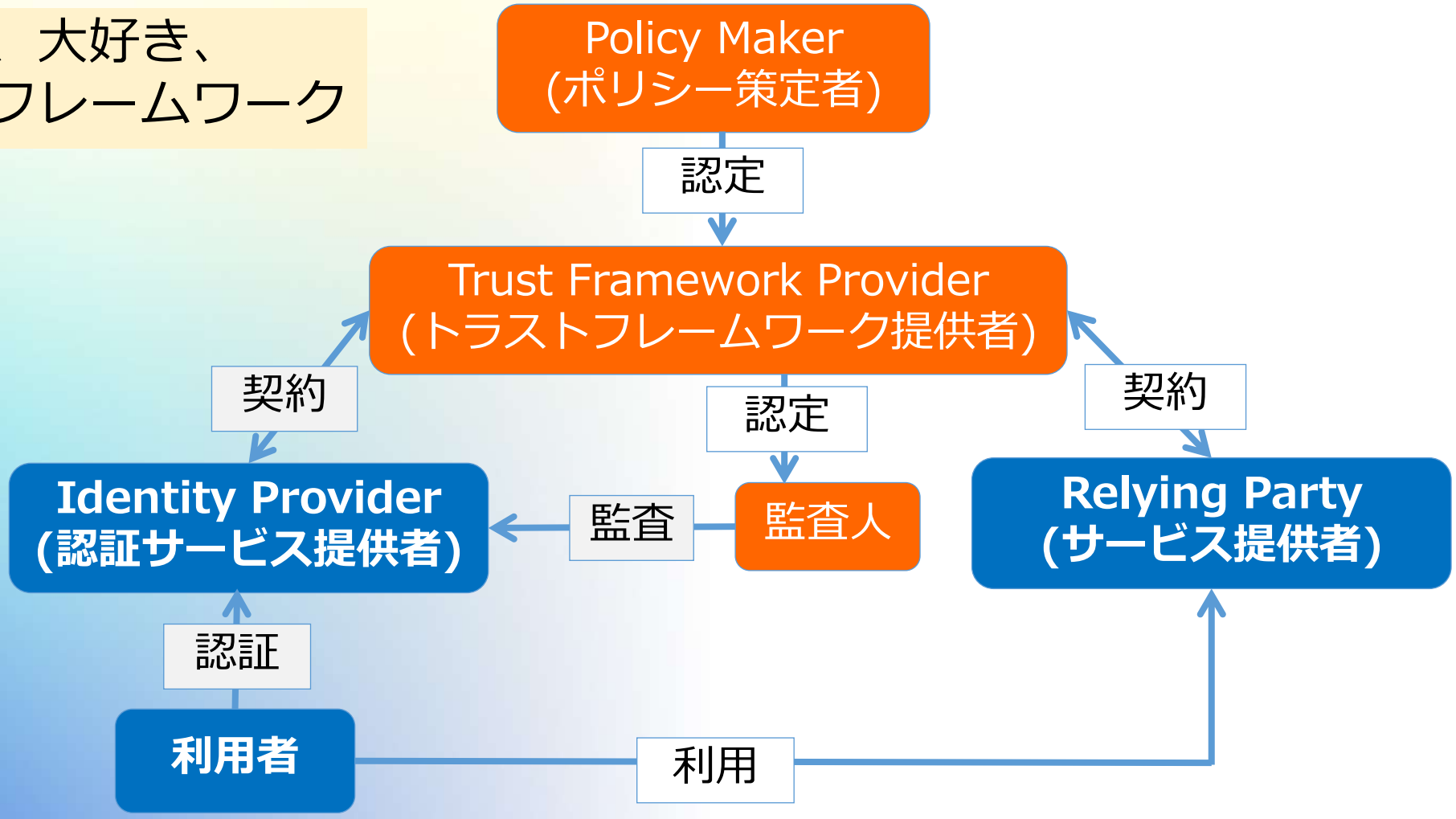
個人アプリ(個人ID)への対応

- トラストフレームワークの考えを適用すると、、、、(？)

Copyright© 2017 EXGEN NET

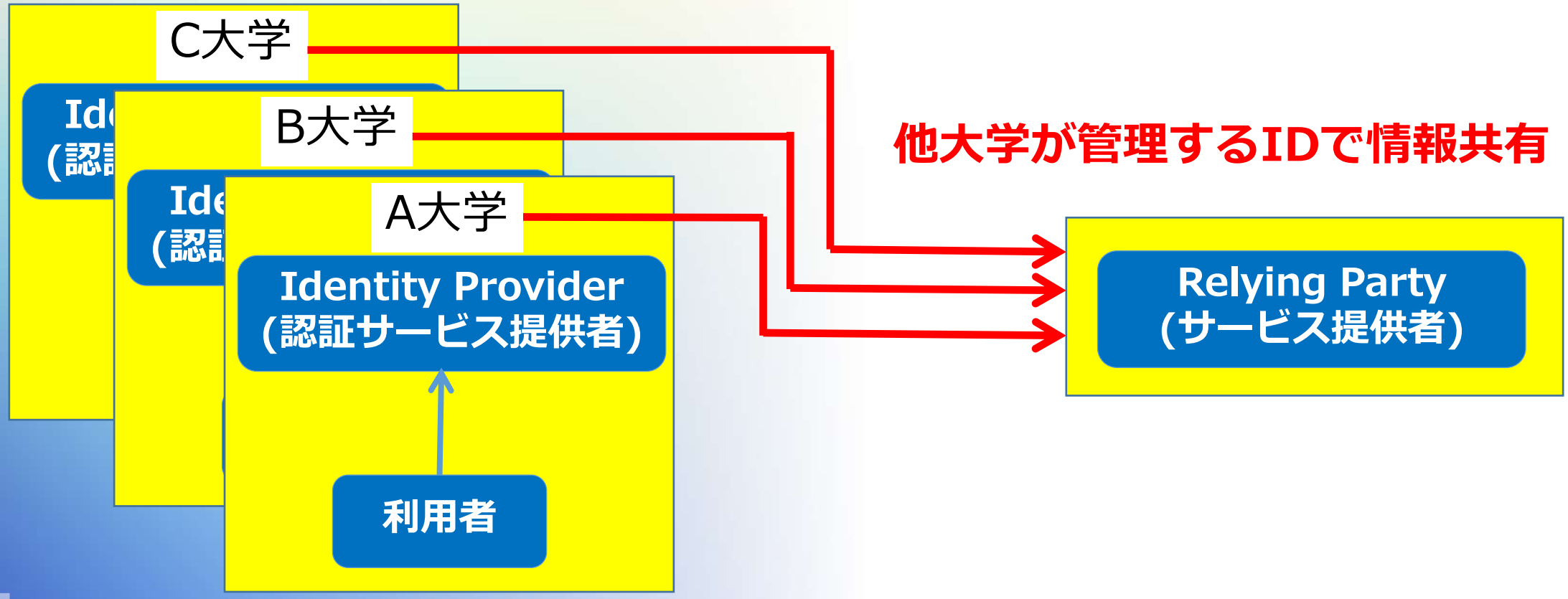
3. 認証基盤システムの詳細要件
3.3 デバイス/Bringされるもの関連

みなさん、大好き、
トラストフレームワーク



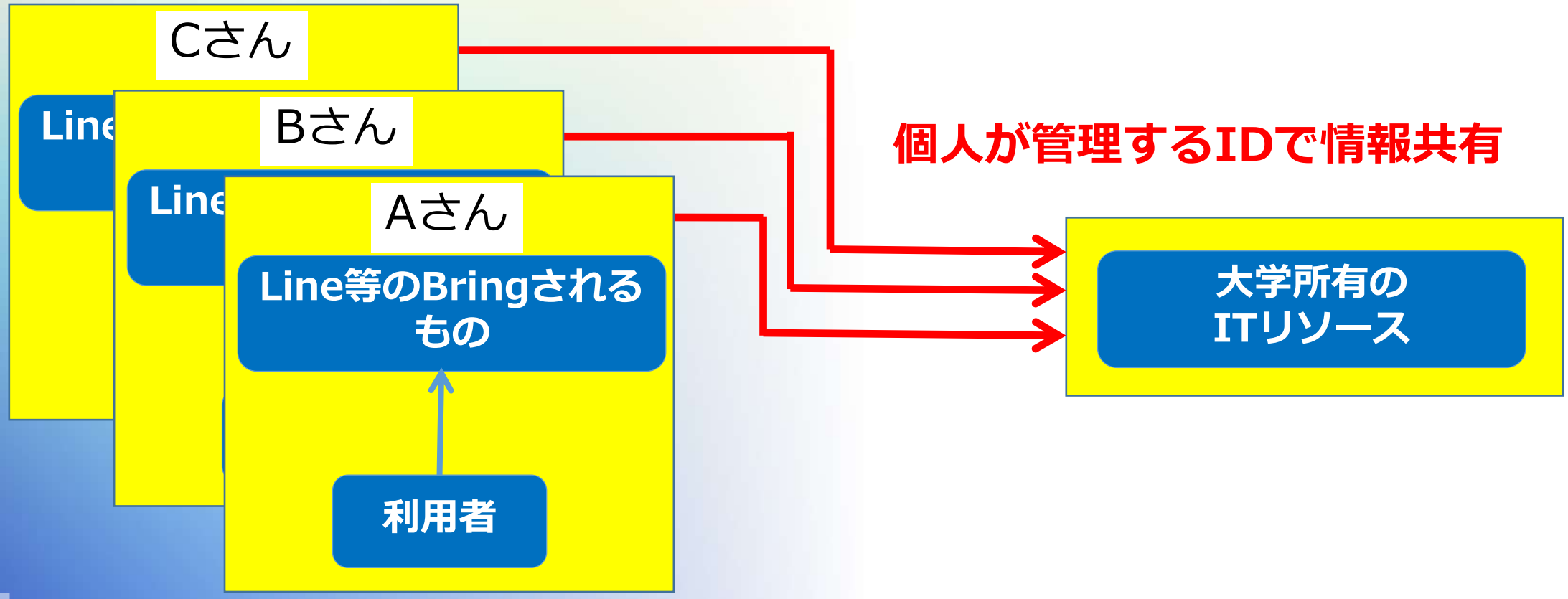
Copyright© 2017 EXGEN NETWORKS Co.,LTD. All Rights Reserved.

3. 認証基盤システムの詳細要件
3.3 デバイス/Bringされるもの関連



Copyright© 2017 EXGEN NETWORKS Co.,LTD. All Rights Reserved.

3. 認証基盤システムの詳細要件
3.3 デバイス/Bringされるもの関連

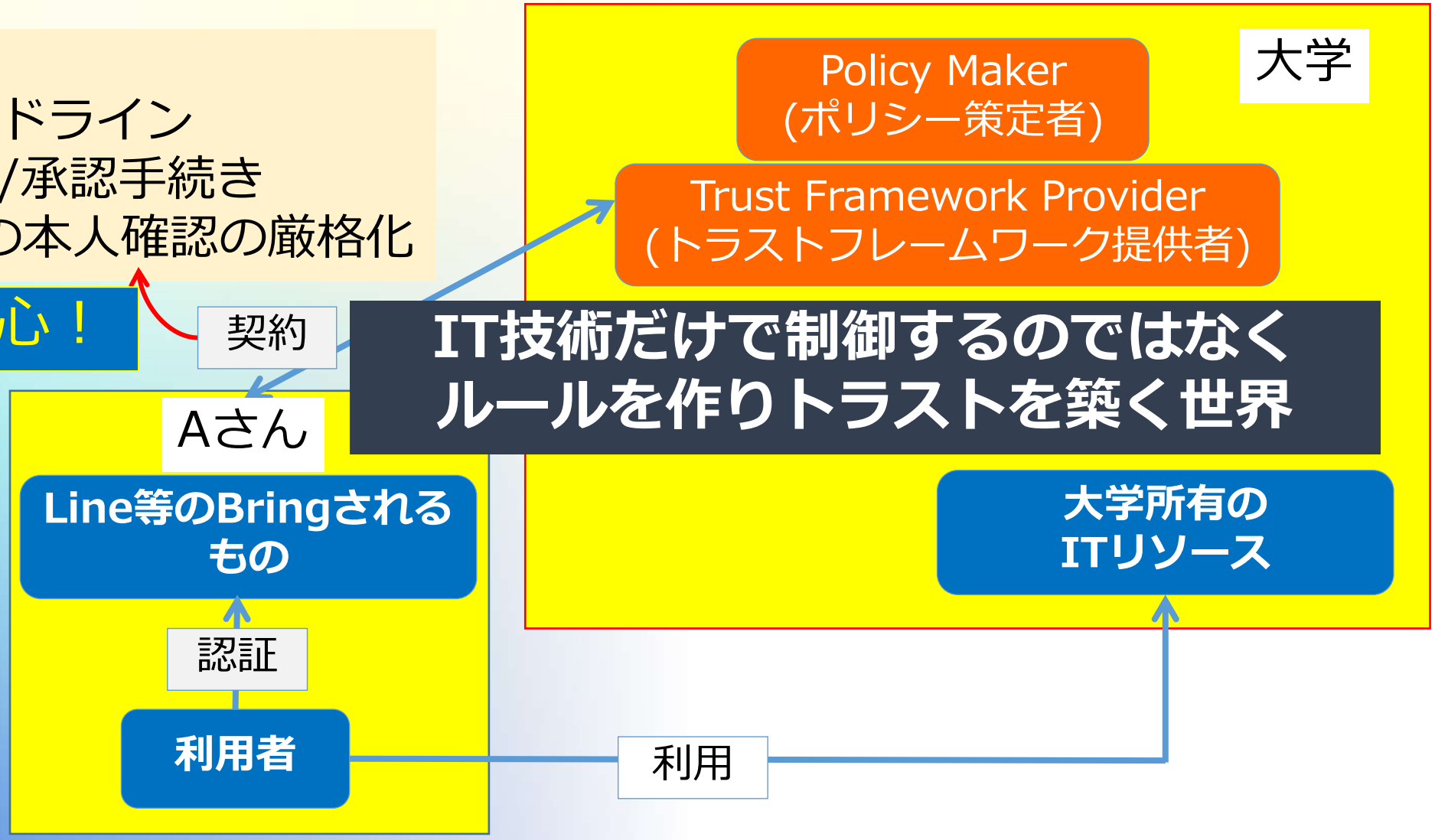


Copyright© 2017 EXGEN NETWORKS Co.,LTD. All Rights Reserved.

3. 認証基盤システムの詳細要件
3.3 デバイス/Bringされるもの関連

- 契約
- 利用ガイドライン
- 利用申請/承認手続き
- Line IDの本人確認の厳格化

最初が肝心！



IT技術だけで制御するのではなく ルールを作りトラストを築く世界

Copyright© 2017 EXGEN NETWORKS Co.,LTD. All Rights Reserved.

3. 認証基盤システムの詳細要件

3.4 まとめ

様々なハイブリッド環境に対応する認証基盤とは

1. 基本構成

①ID管理機能
②認証機能
③ID情報マスタDB

2. ID管理機能

①IDライフサイクル管理
　源泉システムからのGUIメンテ、CSV連携、API連携、ワークフロー連携
②様々な連携システムへのプロビジョニング
　・認可情報等のきめ細かな連携
　・SaaSライセンス管理
　・プロビジョニング(SCIM対応)
③eduroam連携

Copyright© 2017 EXGEN NETWORKS Co.,LTD. All Rights Reserved.

3. 認証基盤システムの詳細要件

3.4 まとめ

様々なハイブリッド環境に対応する認証基盤とは

3. 認証機能

①フェデレーション(SAML/Shibboleth & OpenID Connect対応)
②リバプロSSO
③多要素認証(FIDO対応と多様素認証デバイスとしてのBYOD利用)

4. ID情報マスタDB

①稼働前のID情報の棚卸し(クリーニング)
②運用ルールの策定、遵守

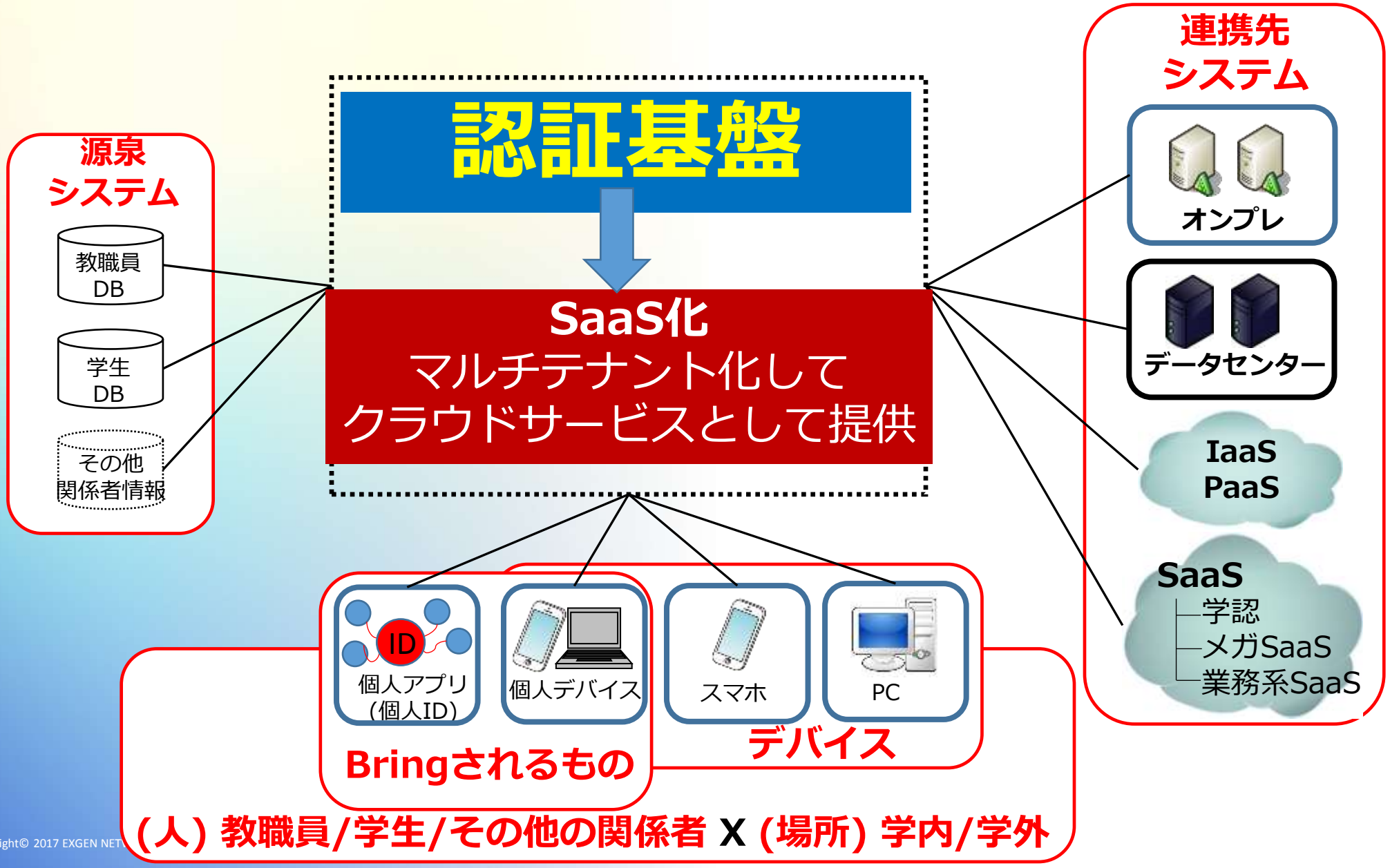
5. 標準化技術の効率的な実装

①オンプレの各システムに対する標準API実装体制の確立
②IDaaS業者に対するSaaSエコシステム作り要求

6. 教職員、学生とのトラスト作り

Copyright© 2017 EXGEN NETWORKS Co.,LTD. All Rights Reserved.

4. IDaaSとは



Copyright© 2017 EXGEN NET