NII オープンフォーラム2022

AXIES認証基盤部会・学認合同企画セッション

日本の教育研究業界認証基盤の今
～IDaaSに対する要件の多様化と対応～

2022年6月2日

エクスジェン・ネットワークス株式会社

代表取締役　江川淳一

USE INNOVATIVE TECHNOLOGY.

1. 最近の認証基盤導入事例

1.1 福島大学様の事例

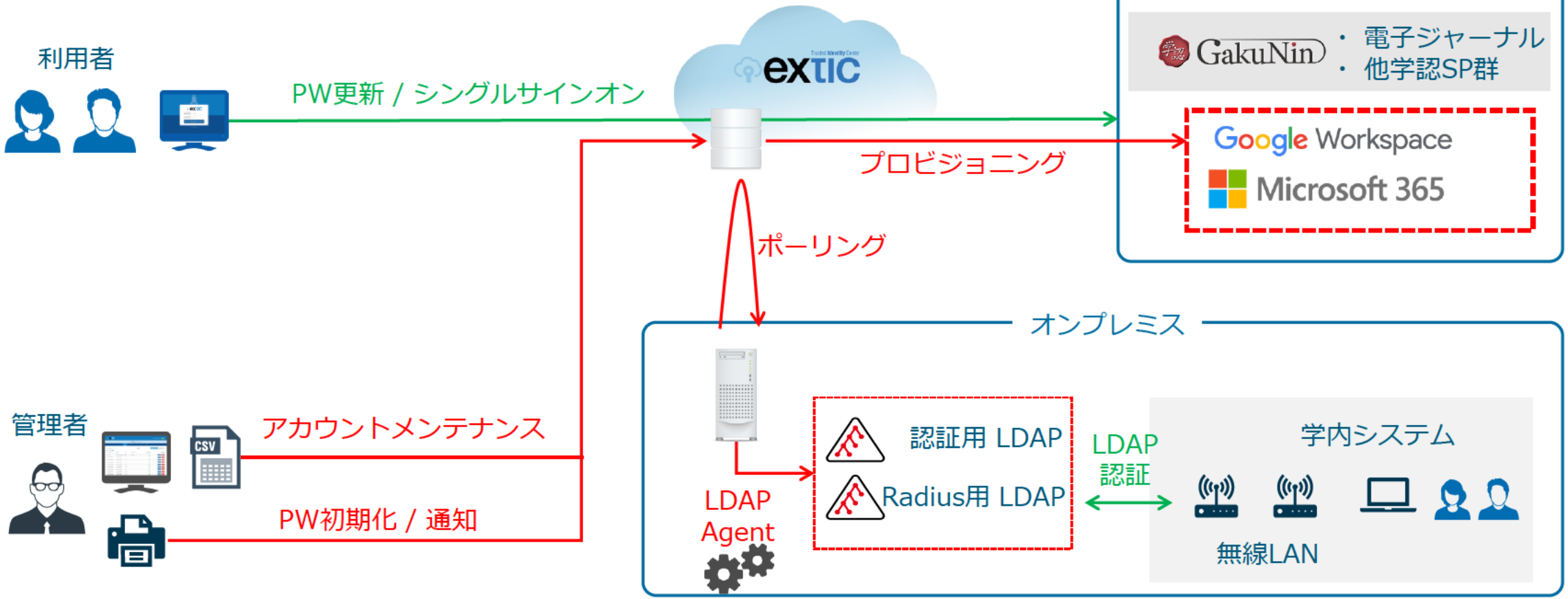
導入サービス	Extic
ユーザー数	5,500ユーザー
プロビジョニング対象	Open LDAP / Microsoft 365 / Google Workspace
シングルサインオン対象	Microsoft 365 / Google Workspace / 学認

要件

- 学認を速やかに利用開始したい
- クラウドサービスの認証を統合したい
- オンプレミスID管理システムをクラウド化したい
- オンプレミス環境へのプロビジョニングが必要
- パスワードセルフリセット機能などの充実した運用管理機能が必要
- 短納期でサービス利用したい

1. 最近の認証基盤導入事例

1.1 福島大学様の事例



1. 最近の認証基盤導入事例

1.2 東京農工大学様の事例

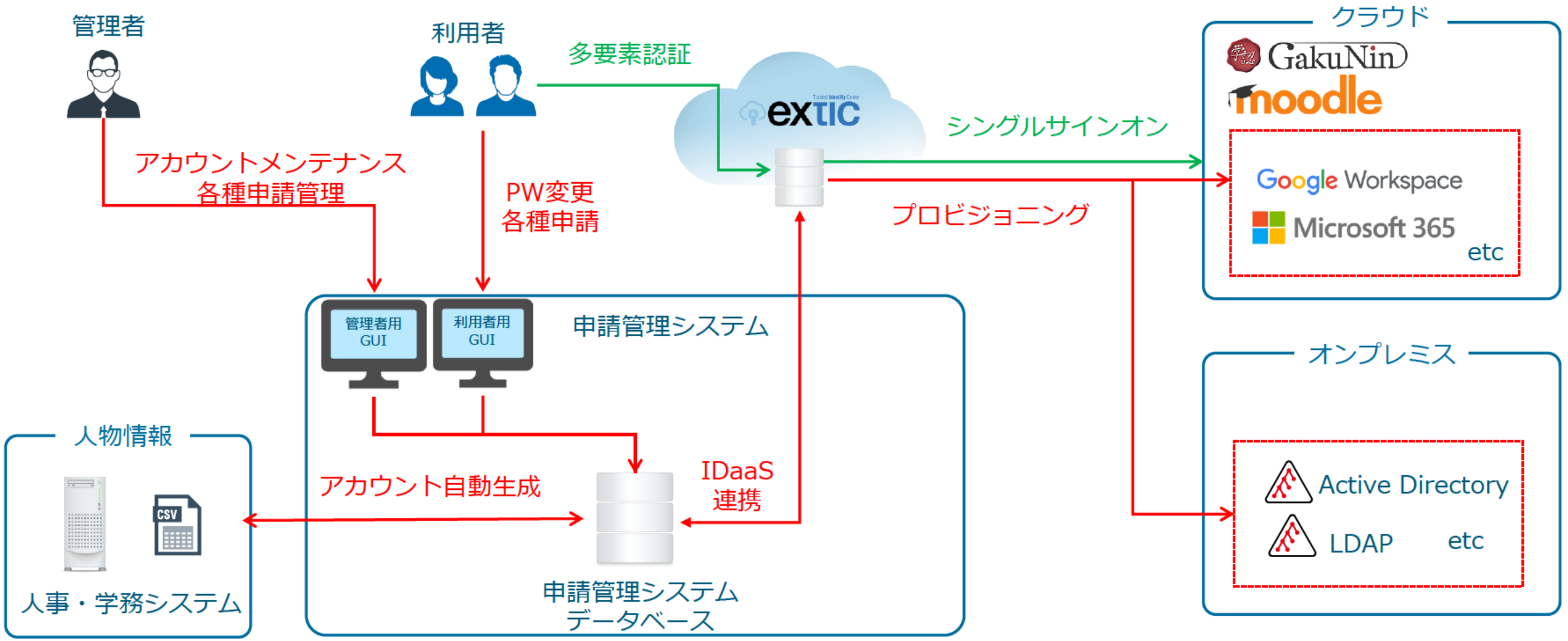
導入サービス	Extic / 申請管理システム（SRA東北社提供）
ユーザー数	6,700ユーザー
プロビジョニング対象	Active Directory / Open LDAP / Microsoft 365 / Google Workspace
シングルサインオン対象	Microsoft 365 / Google Workspace / 学認 / Moodle / Zoom 、他

要件

- 多要素認証導入でセキュリティを向上したい
- シングルサインオン導入で認証利便性を向上したい
- オンプレミスID管理と決別し、IDaaSを利用したい
- Shibboleth運用管理から解放されたい
- 基本的にフルクラウドの方針
- クラウドへのプロビジョニングを網羅してほしい
- 一部残るオンプレミス環境へのプロビジョニングが必要
- ID管理には、属性情報整備機能(ID申請管理機能や権限情報管理機能等)が必要

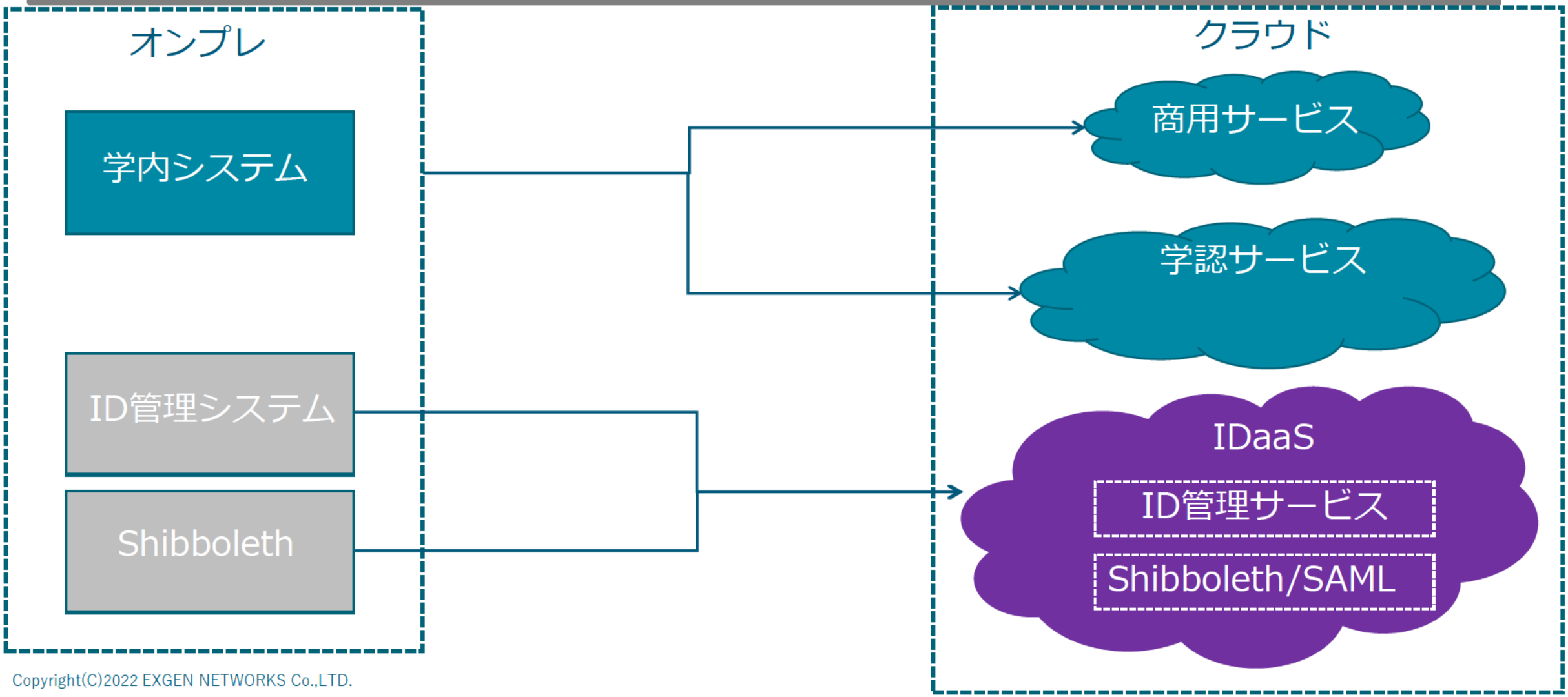
1. 最近の認証基盤導入事例

1.2 東京農工大学様の事例

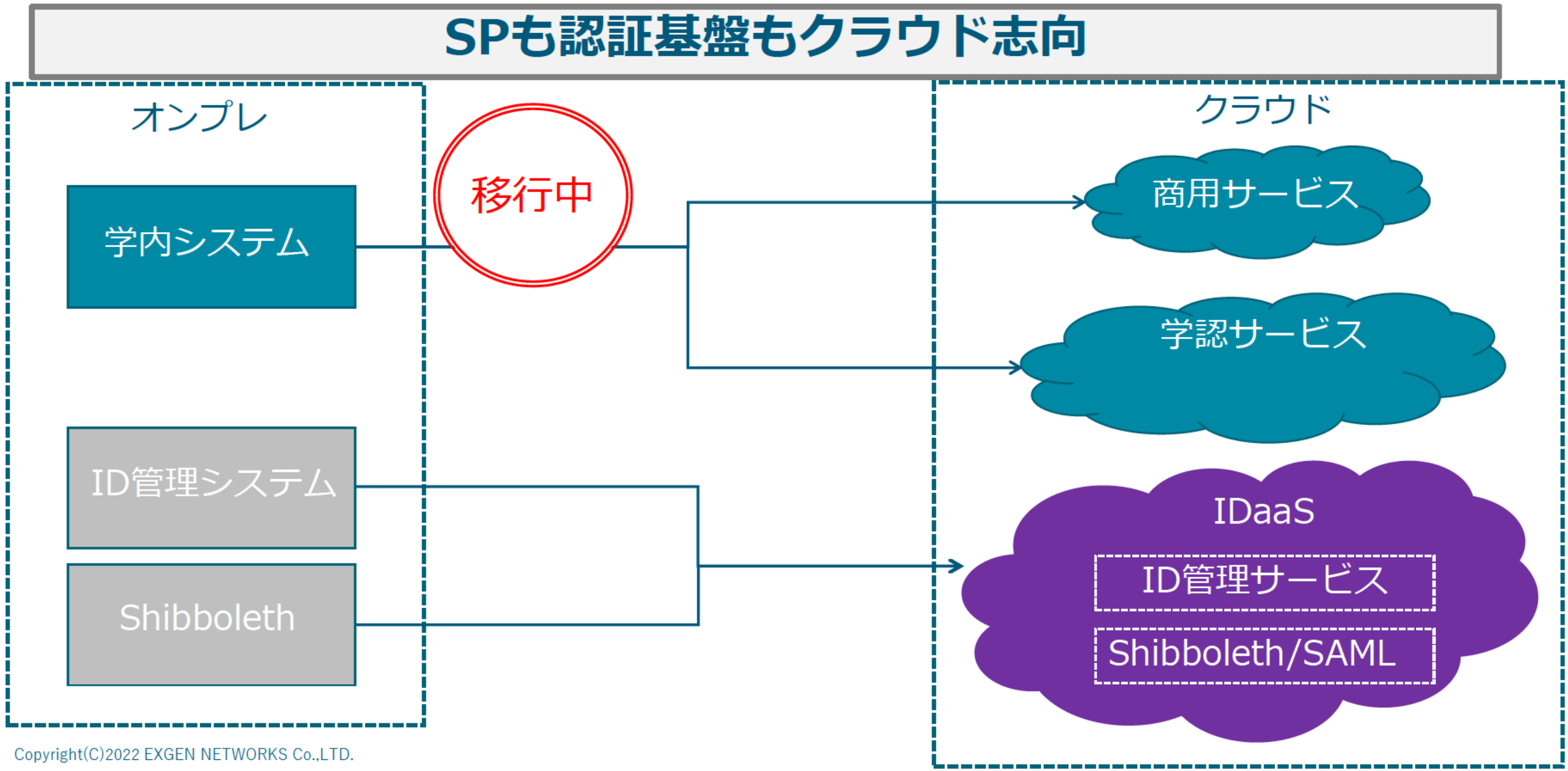


2. 要件分析

福島大学様、東京農工大学様事例に見る、認証基盤要件

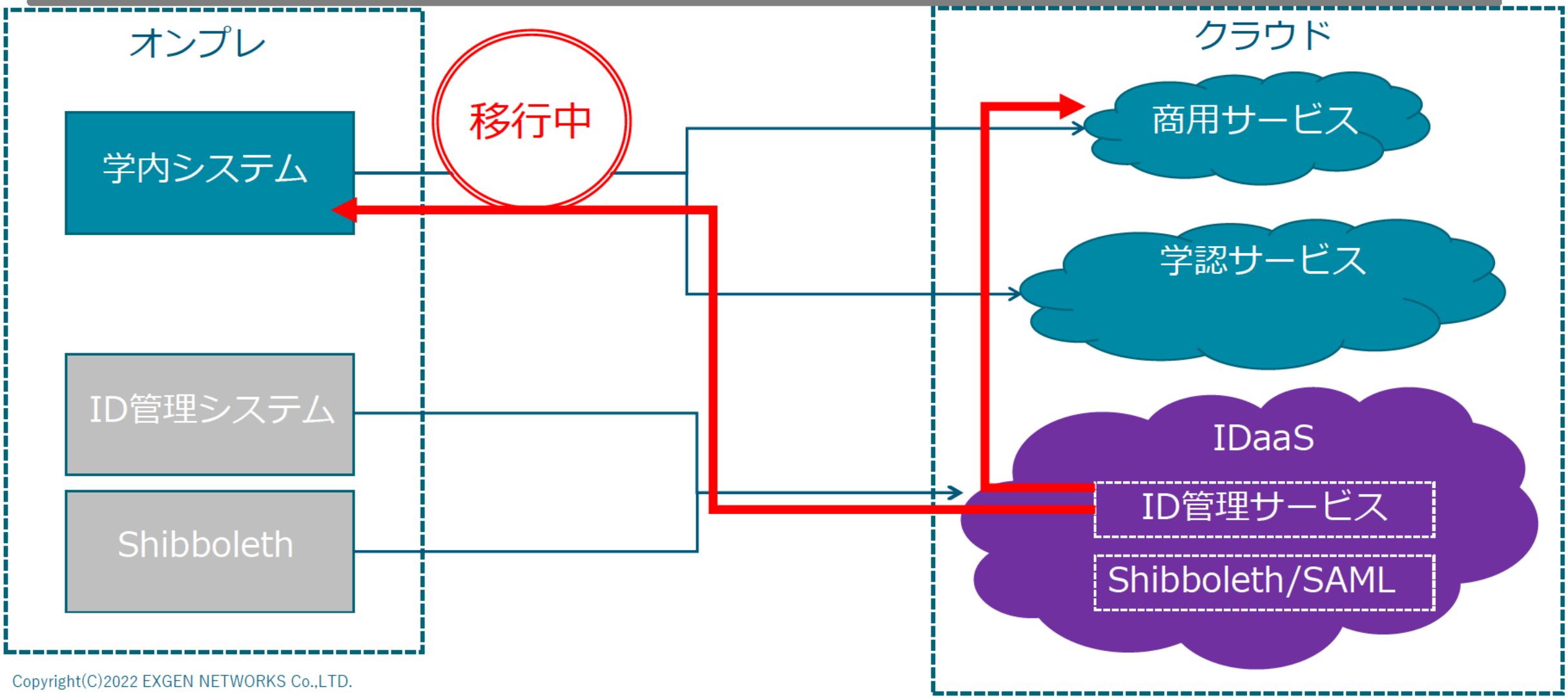


2. 要件分析



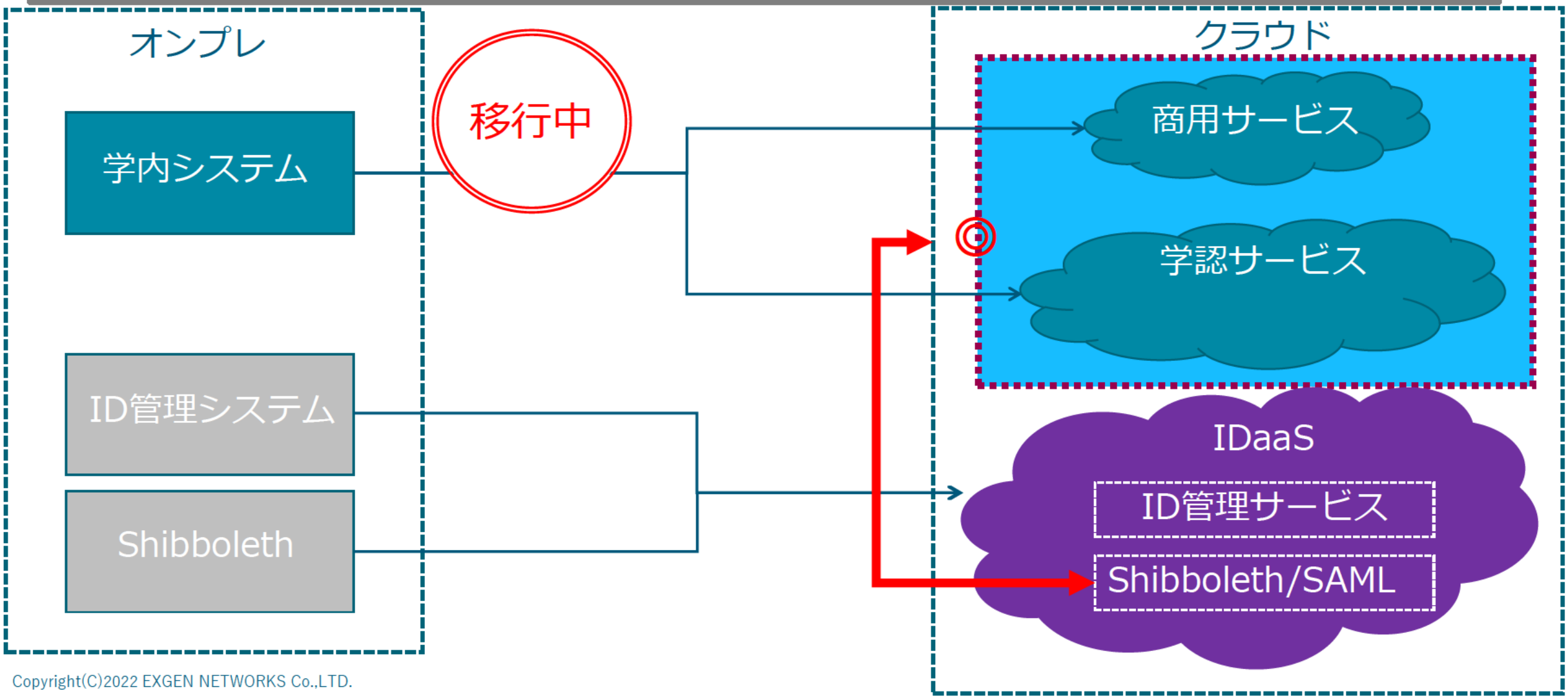
2. 要件分析

プロビジョンニング先はクラウドとオンプレの両方



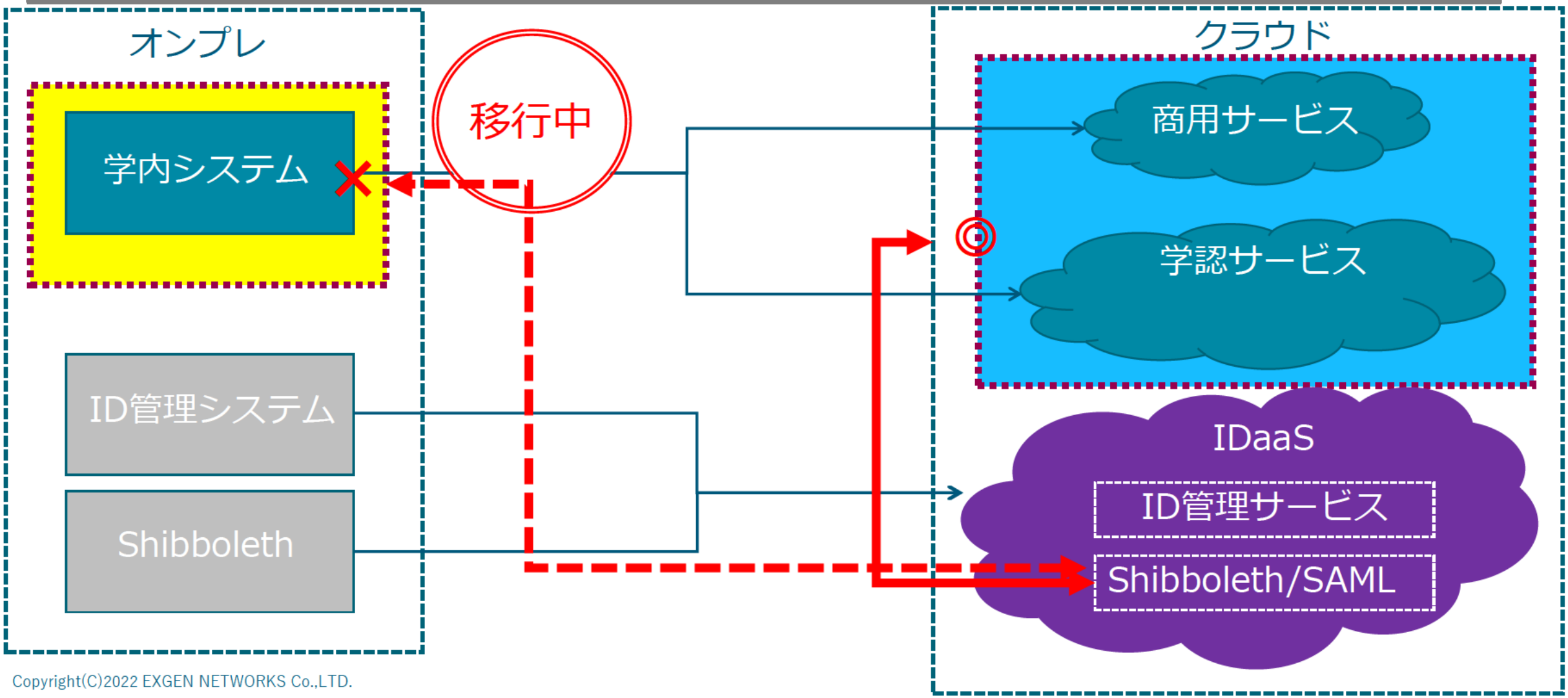
2. 要件分析

フェデレーション対応クラウドサービスの認証統合

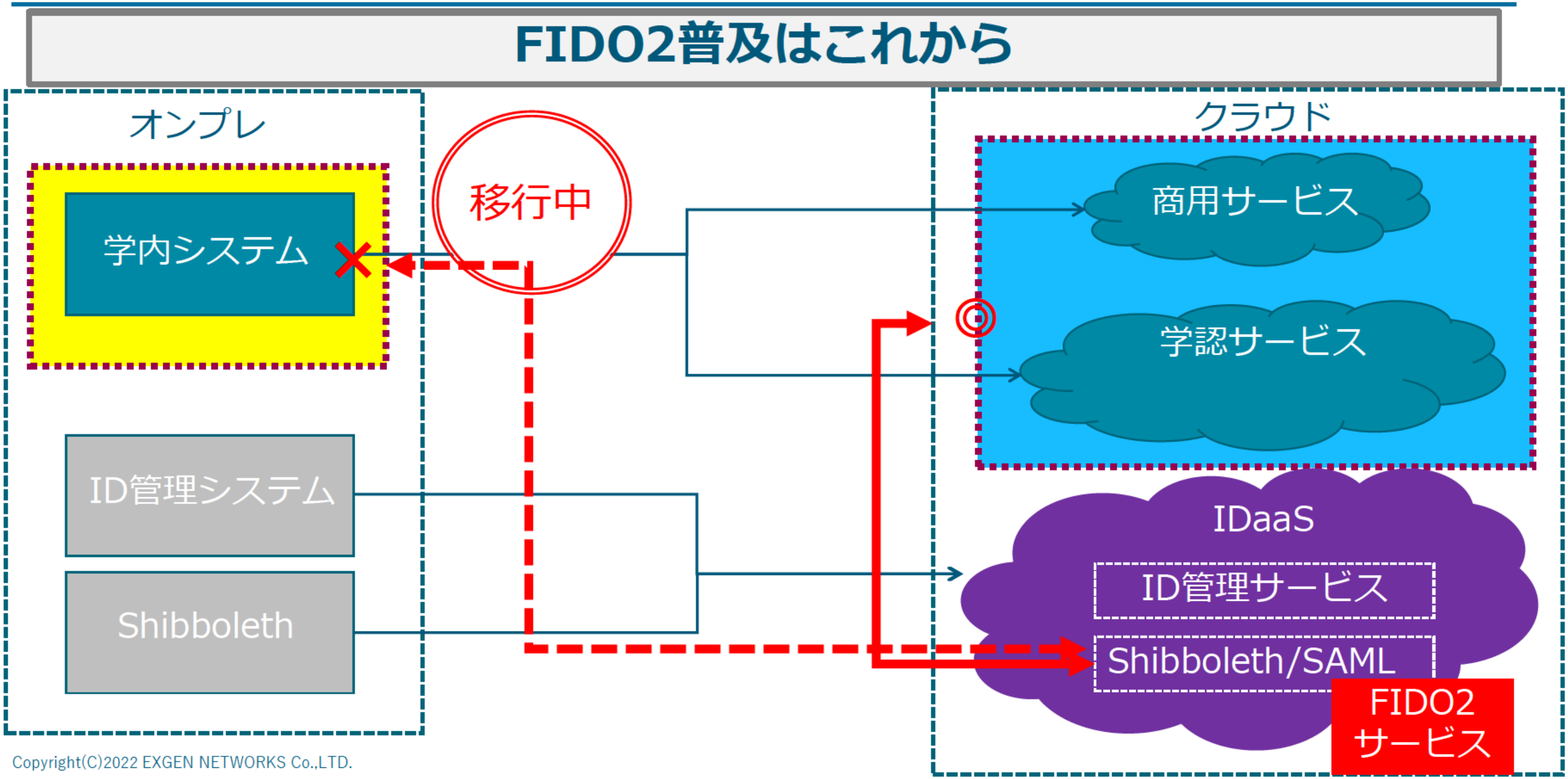


2. 要件分析

ID管理統合済み、認証完全統合はまだの状態が多い

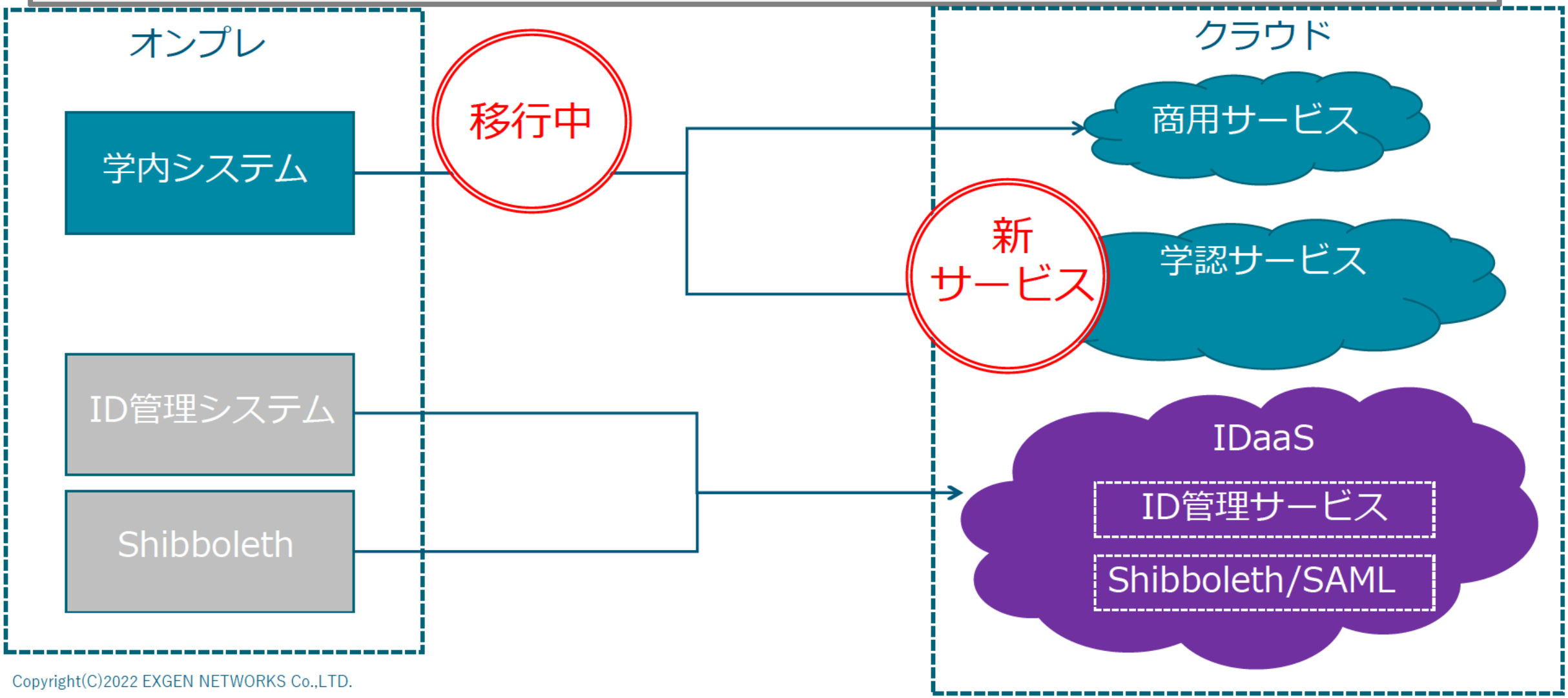


2. 要件分析



2. 要件分析

最近増えてきた要件



2. 要件分析

・新サービス
　　・HPCI、NIMS、学認RDM等、共同研究基盤サービスの整備
　　・オープンサイエンス対応

2. 要件分析

最近の大学IT環境

・オンプレ学内システムのクラウドサービス化が進む

① 2種類のクラウドサービスを利用したい

- 商用クラウドサービス：MS365やGoogle Workplace等
- 学認サービス

② クラウド移行過渡期で、オンプレ学内システムはまだ存在する。

③ 今後整備される、共同研究基盤サービスやオープンサイエンスに対応したい

最近の大学認証基盤要件

・上記要件を満たす、クラウドの認証基盤 (IDaaS) が必要

2. 要件分析

最近の大学IT環境

・オンプレ学内システムのクラウドサービス化が進む

① 2種類のクラウドサービスを利用したい

弊社の対応

・ 学認サービス

ビス：MS365やGoogle Workplace等

弊社の対応予定(2)

③ 今後整備される、共同研究基盤サービスやオープンサイエンスに対応したい

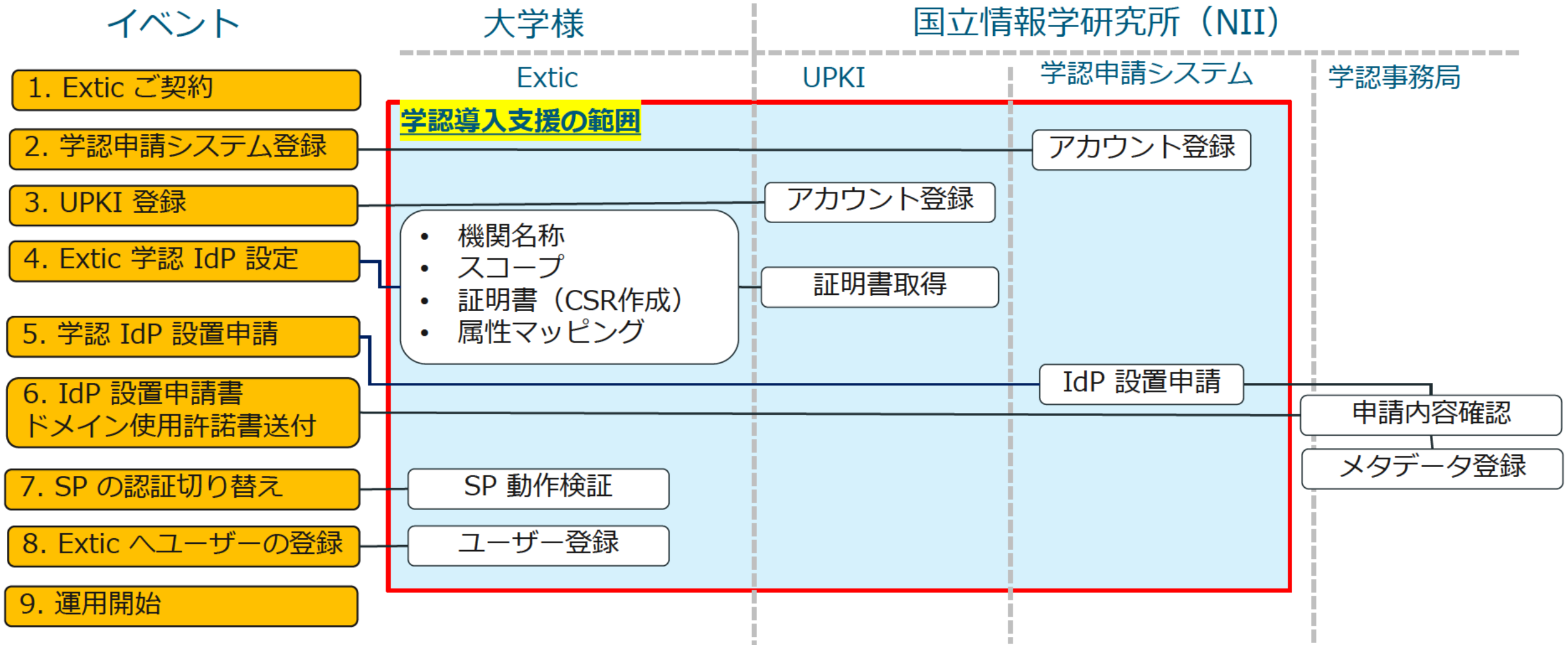
最近の大学認証基盤要件

弊社の対応予定 (1)

・上記要件を満たす、クラウドの認証基盤 (IDaaS) が必要

3. 弊社の対応 ～ 学認サービス

・学認導入支援サービスの提供



3. 弊社の対応 ～ 学認サービス

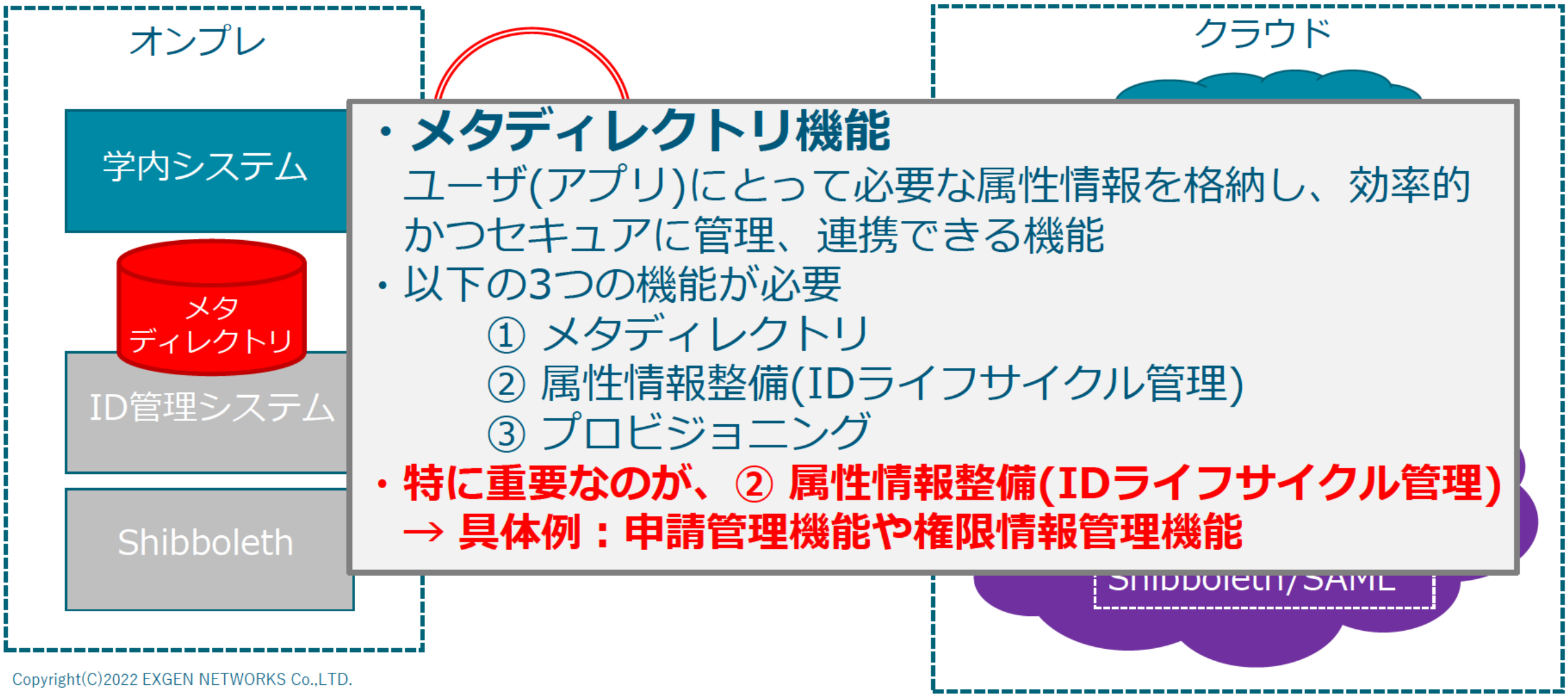
・学認導入支援サービスの提供

福島大学様が、連携したSP

・JapanKnowledge Lib
・KinoDen
・Maruzen eBook Library
・Nii-REO 電子ジャーナルアーカイブ
・Nii-REO 人文社会科学系電子コレクション
・ProQuest Central
・ScienceDirect
・Scopus
・CiNiiResearch

4. 弊社の対応予定 (1) ～ クラウドの認証基盤

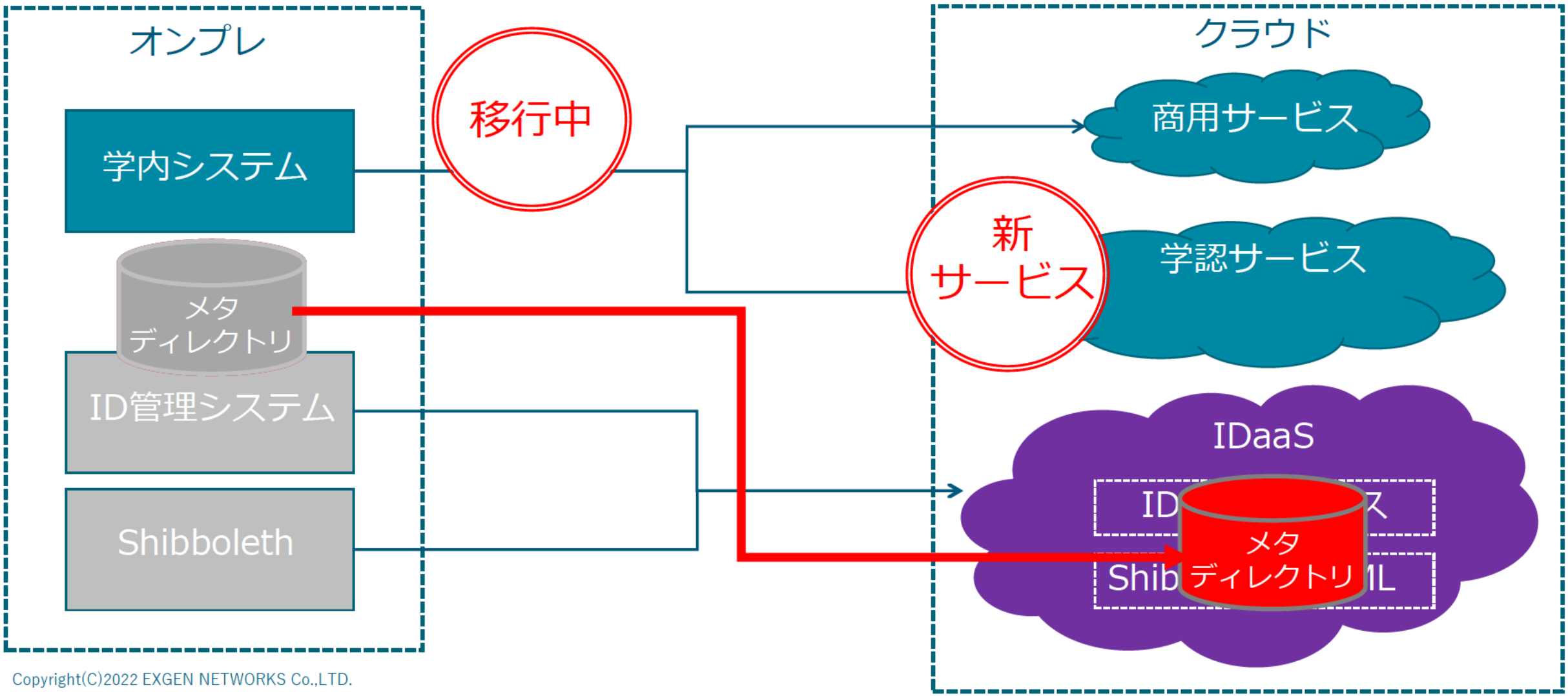
4.1 オンプレ認証基盤の要諦



- **メタディレクトリ機能**
  ユーザ(アプリ)にとって必要な属性情報を格納し、効率的かつセキュアに管理、連携できる機能
- 以下の3つの機能が必要
  - ① メタディレクトリ
  - ② 属性情報整備(IDライフサイクル管理)
  - ③ プロビジョニング
- **特に重要なのが、② 属性情報整備(IDライフサイクル管理)**
  → 具体例：申請管理機能や権限情報管理機能

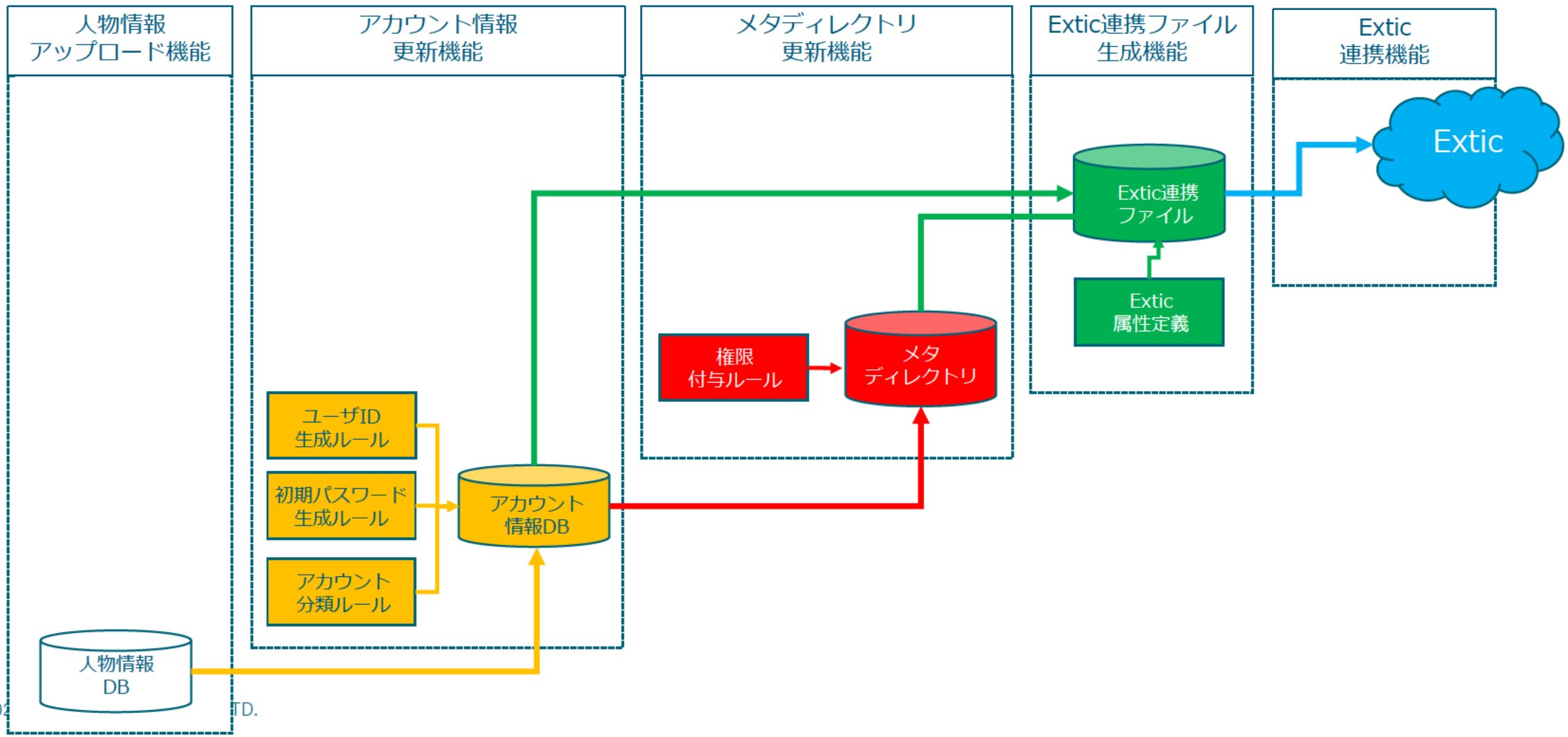
4. 弊社の対応予定 (1) ～ クラウドの認証基盤

4.1 オンプレ認証基盤の要諦



4. 弊社の対応予定 (1) ～ クラウドの認証基盤

4.2 メタディレクトリ機能のSaaS化



4. 弊社の対応予定 (1) ～ クラウドの認証基盤

4.2 メタディレクトリ機能のSaaS化

1. 人物情報アップロード機能
   - 大学内の源泉情報である人事・学務システムから最新の人物情報(全件データ)をアップロード
   - 人事情報DBに対して差分抽出処理を介し、人物情報の更新(追加、削除、変更)が行なわれる。
2. アカウント情報更新機能
   - 人物情報DBから、以下の生成ルールに従い、アカウント情報の更新が行なわれる。
     ① ユーザID作成ルール、② 初期パスワード生成ルール、③ アカウント分類ルール
3. メタディレクトリ更新機能
   - アカウント情報DBから、権限付与ルールに従い、メタディレクトリ情報の更新が行なわれる。
4. Extic連携ファイル生成機能
   - Extic連携対象アカウントを抽出し、Extic属性定義と合致する項目を出力し、Extic連携ファイルを生成する。
5. Extic連携機能
   - Extic連携ファイルをExticへ連携する。

5. 弊社の対応予定 (2) ～ 共同研究基盤サービスとオープンサイエンス

5.1 共同研究基盤サービスの整備とIDaaS要件

異なる組織の方々が、情報共有を行う事を可能にする認証基盤の要件

セキュリティレベルの異なる組織で情報共有を行う場合
→ **セキュリティ基準**が必要

NIST準拠でいいの？

IDaaS要件：セキュリティ基準への対応(準拠)

NIST SP800-171/63
サプライチェーンでの情報共有に関するセキュリティ規程
- IAL： 身元確認プロセス (Identity Proofing Process) に関する規程
- AAL： 認証プロセス (Authentication Process) に関する規程
- FAL： Federation に用いる Assertion Protocol の強度に関する規程

オンラインで実施
eKYC

CSP (Credential Service Provider)
- 認証基盤の中で、パスワードや証明書などのクレデンシャルを利用者に発行するサービスを行う箇所。ここでeKYC等を用いて、身元確認を行う。

5. 弊社の対応予定 (2) ～ 共同研究基盤サービスとオープンサイエンス

5.2 NIST準拠でいいの？

① 業界向けガイドライン

・**NIST SP800-171**：連邦政府機関と以外の組織を対象とした、CUI(Controlled Unclassified Information)を保護するためのガイドライン。

・**NIST SP800-63**：SP800-171の具体的要件であり、連邦政府機関の情報システムに対しての電子認証ガイドライン。

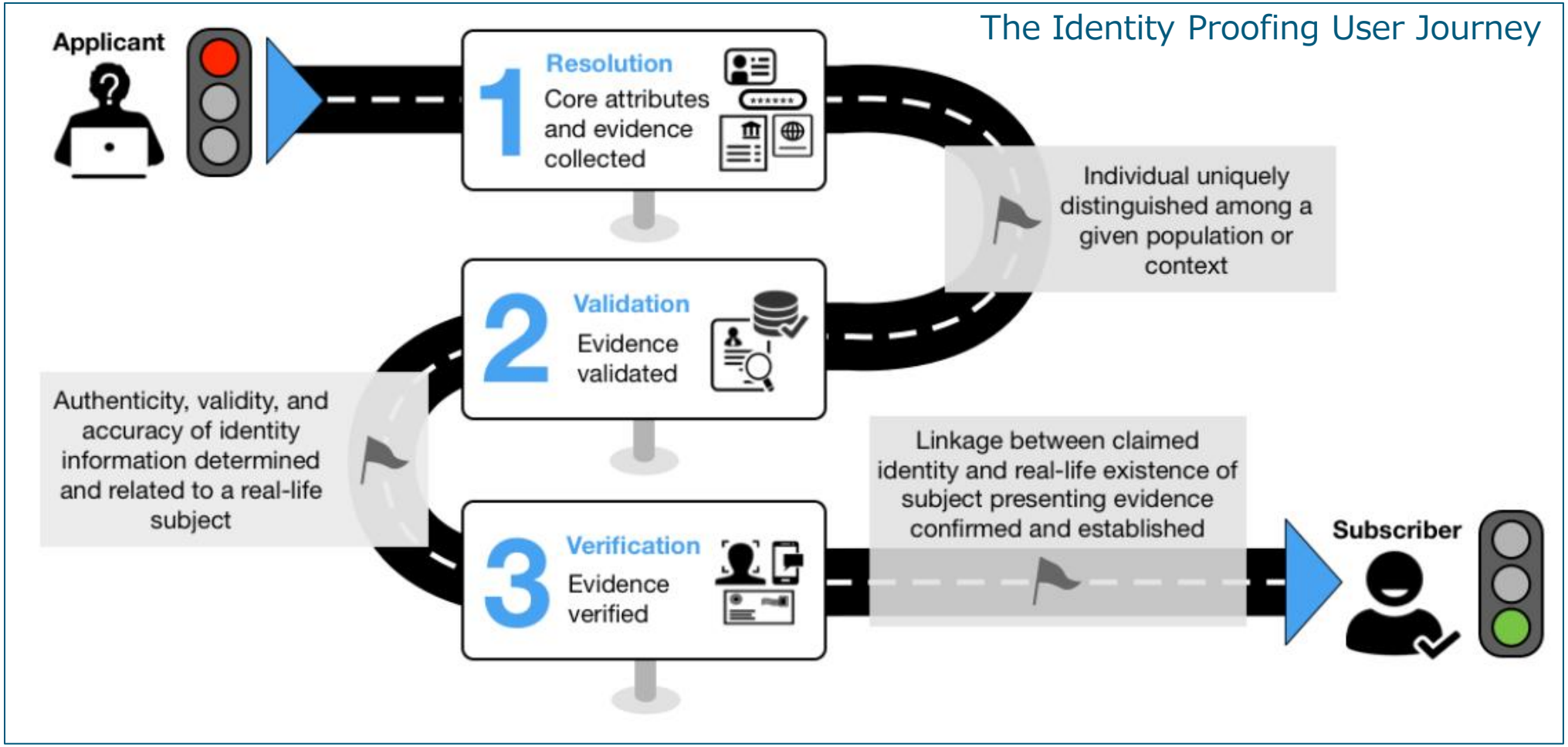
② 法律

・**犯罪収益移転防止法**：平成28年10月施行。マネーロンダリング(犯罪による収益の出所や帰属を隠そうとする行為)防止が目的。身元確認処理については、**eKYC「ホ」**として、サービス利用者の身分証と顔写真を提出してもらい、サービス利用申請内容と突合し、本人かどうかを確認する。金融業界や古物業界で利用されている。

日本の共同研究基盤サービスの認証基盤でのセキュリティ基準は、
次世代認証連携検討作業部会が、 **IALとAALについて、研究教育業界向けガイドラインとして、NISTSP800-63等を参考にして、国際間相互利用を考慮し**検討中。

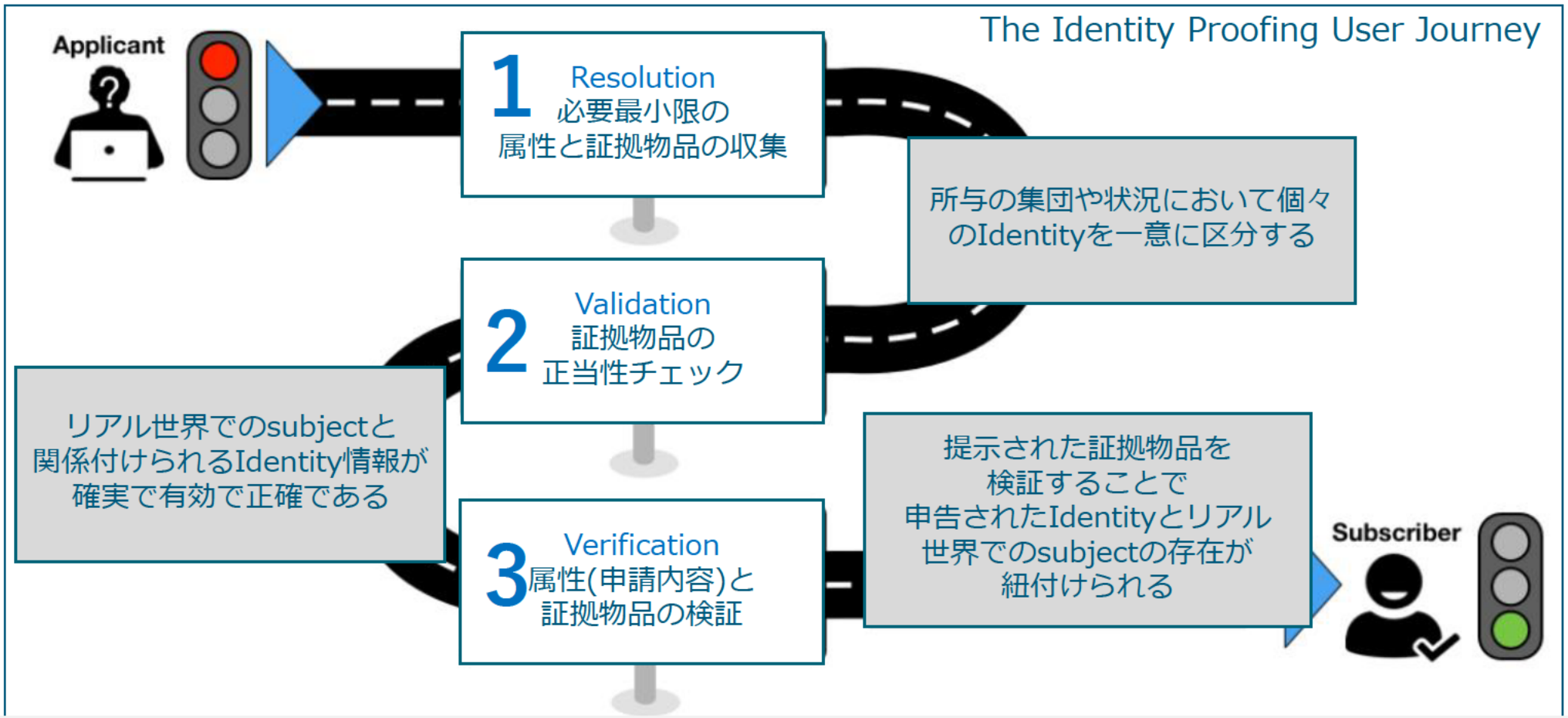
5. 弊社の対応予定 (2) ～ 共同研究基盤サービスとオープンサイエンス

5.3 身元確認プロセス概要 ～ NIST SP800-63A



5. 弊社の対応予定 (2) ～ 共同研究基盤サービスとオープンサイエンス

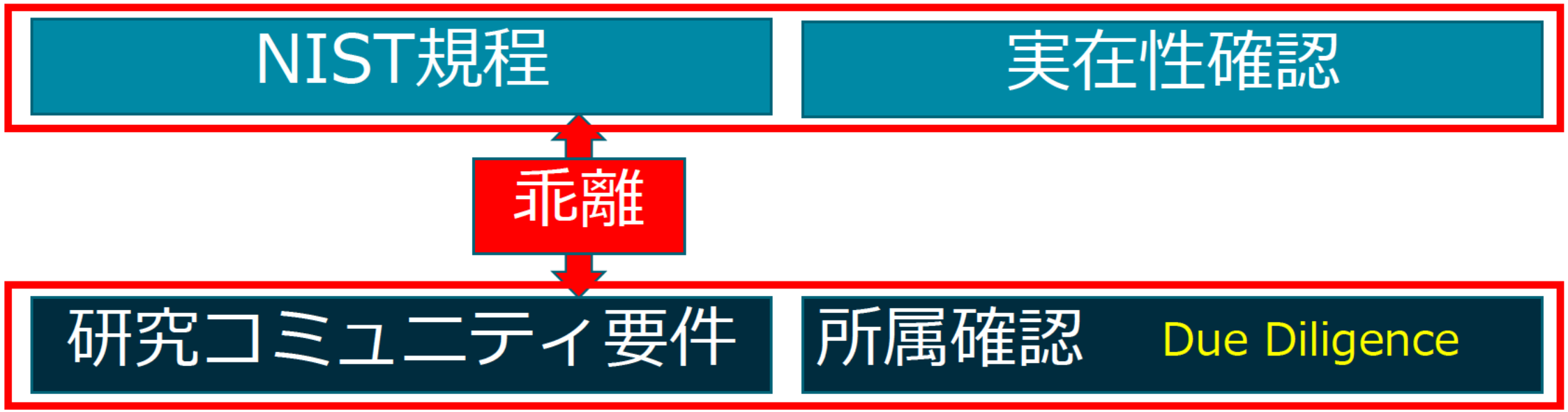
5.3 身元確認プロセス概要 ～ NIST SP800-63A



- 確かな証拠 (stated level of certitude)により、 Applicant が間違いなく、本人であること (Applicant is who they claim to be)を証明することである。

5. 弊社の対応予定 (2) ～ 共同研究基盤サービスとオープンサイエンス

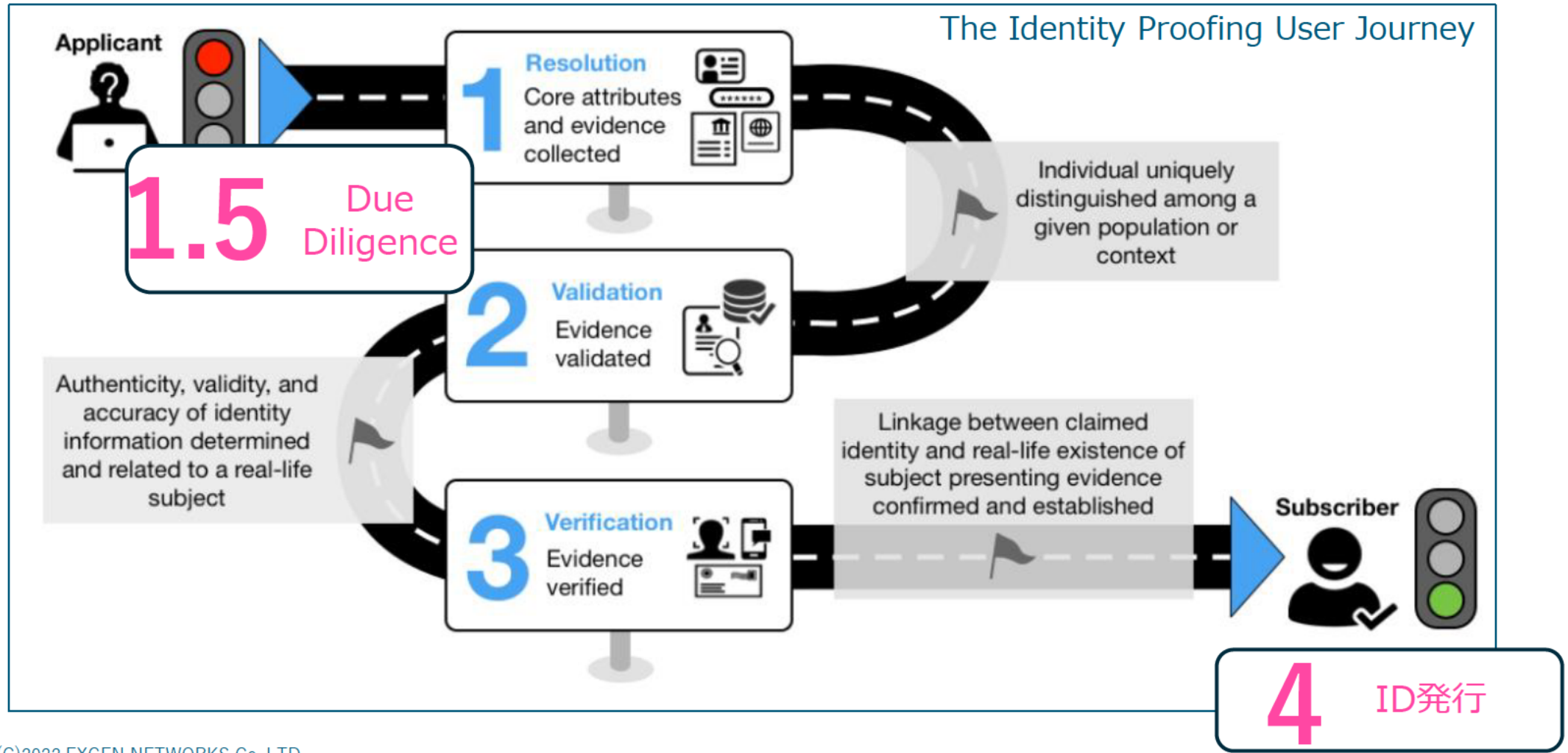
5.4 NISTと日本の研究コミュニティ要件との乖離



課題	eKYCサービスでは、社員証、教職員証、学生証等の証拠物の種類が多岐にわたるためValidation、Verification工程における真正性の確保が困難
対策	eKYCサービスとは別に、CSPの機能として、所属組織ドメインのメアドによるホワイトリストチェック等で、所属確認を行うしくみを実装する必要がある

5. 弊社の対応予定 (2) ～ 共同研究基盤サービスとオープンサイエンス

5.5 日本の研究コミュニティ要件に対応した身元確認処理



5. 弊社の対応予定 (2) ～ 共同研究基盤サービスとオープンサイエンス

5.5 日本の研究コミュニティ要件に対応した身元確認処理

CSP

Trusted Identity Center exTIC

実装中

1 Resolution

- 申請書の記載/提出
  - 氏名、生年月日、性別、住所等
- 本人確認書類の提出
  - パスポート、免許証等の写真付き公的身分証
- セルフィの提出

1.5 Due Diligence

- ホワイトリスト等による所属検証
  - 所属ドメインのメールアドレス名の検証
- メールアドレスの到達性確認
  - 確認コード送信

eKYC

TRUSTDOCK

2 Validation

- 本人確認書類の真正性検証

3 Verification

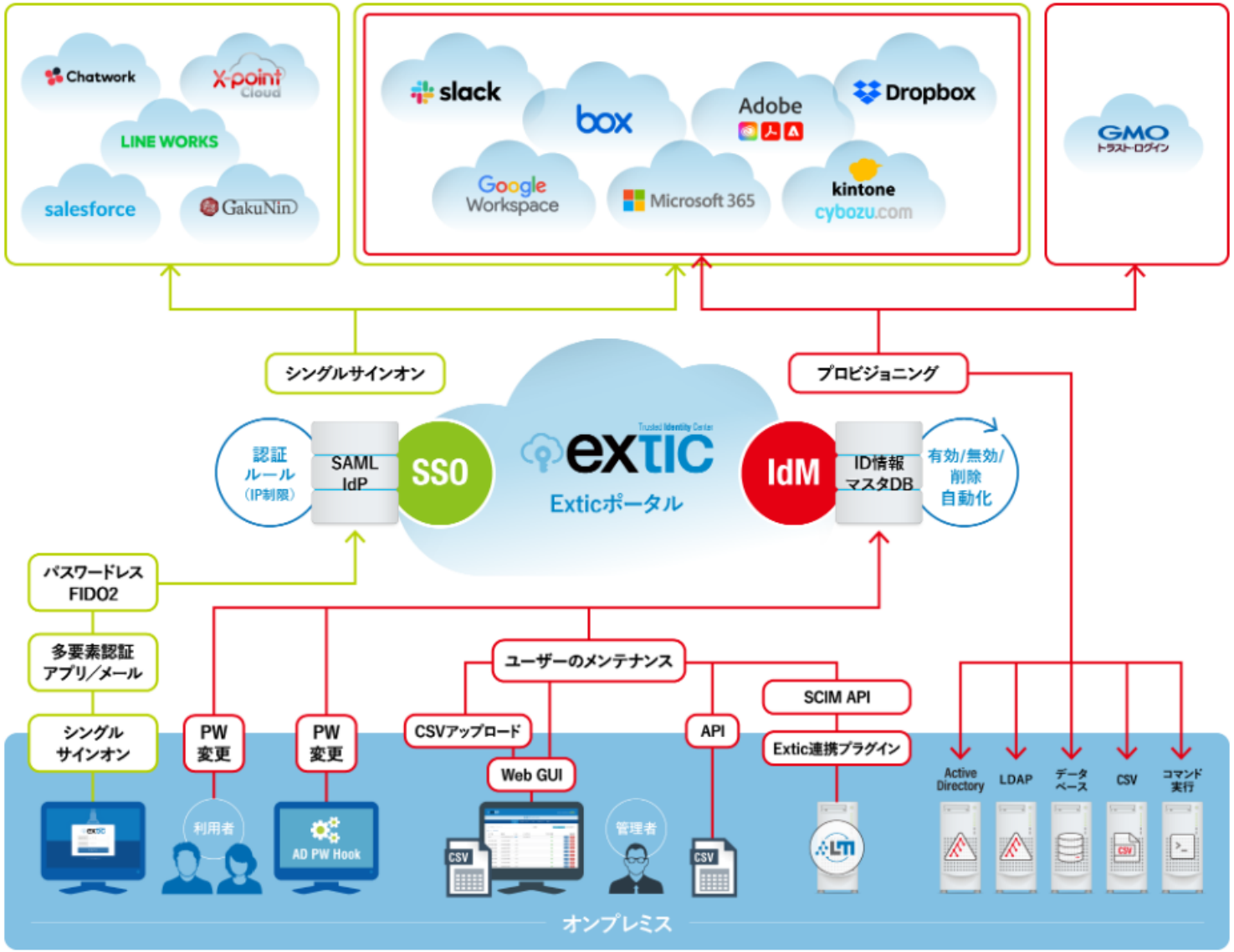
- 申請書とセルフィーと、本人確認書類の突合

ID発行

- 申請者に対するID発行

5. 弊社の対応予定 (2) ～ 共同研究基盤サービスとオープンサイエンス

5.6 CSP開発中



5. 弊社の対応予定 (2) ～ 共同研究基盤サービ

どのようなケースで
CSP (eKYC) が必要かは、
次のセッションを
ご参照ください

5.6 CSP開発中