次世代デジタルアイデンティティ基盤の実証実験について

2021年1月

伊藤忠テクノソリューションズ株式会社

富士榮　尚寛

自己紹介

デジタル・アイデンティティ歴、約18年

- OpenIDファウンデーション・ジャパン/理事、KYC WGリーダ
- 米国OpenID Foundation/eKYC and Identity Assurance WG Co-chair
- 日本ネットワークセキュリティ協会デジタル・アイデンティティWG
- 大学ICT推進協議会（AXIES）/認証基盤部会 運営委員
- SIerでビジネス開発を担当

次世代デジタルアイデンティティ基盤@慶應義塾

参画組織

・慶應義塾大学

・伊藤忠テクノソリューションズ株式会社

・Japan Digital Design株式会社

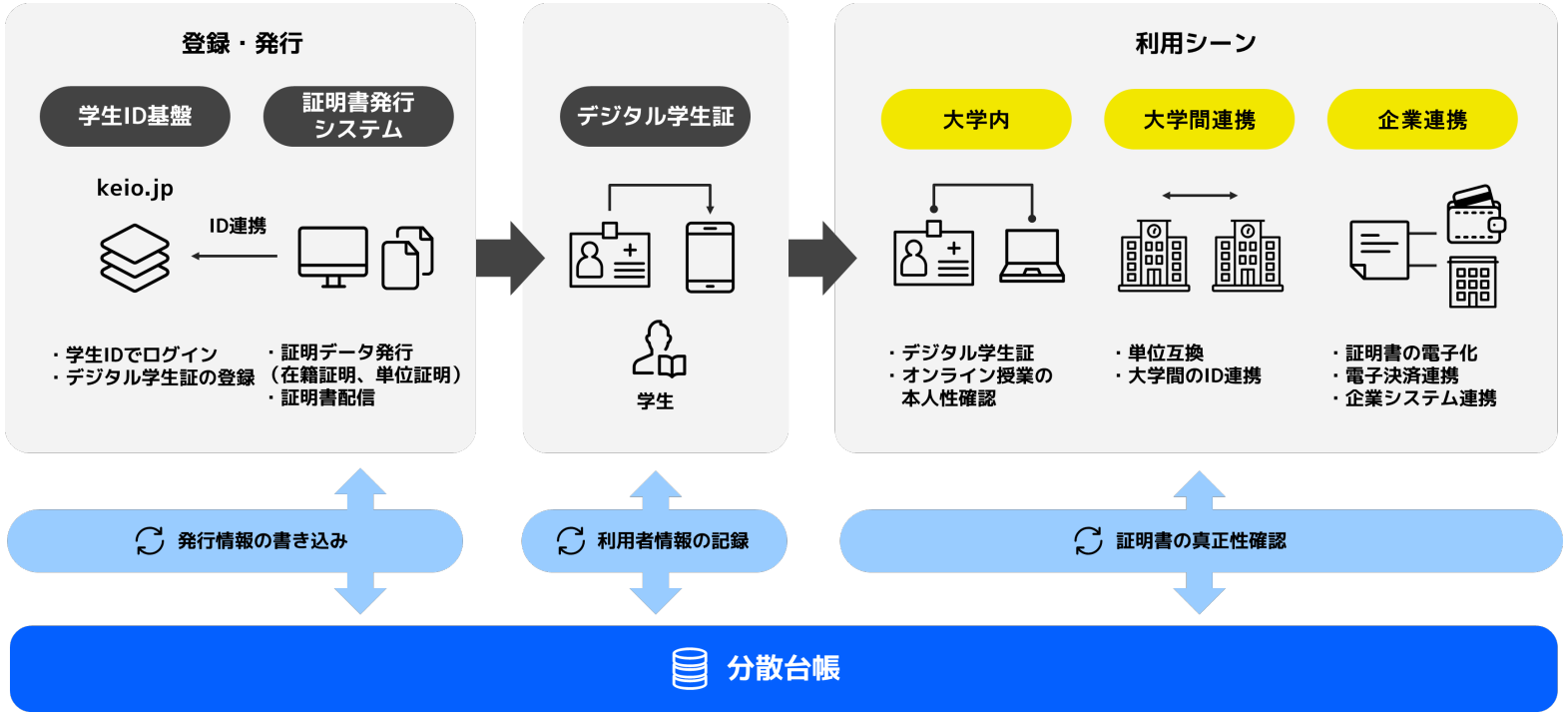
・株式会社ジェーシービー

・西日本電信電話株式会社

・BlockBase株式会社

<u>各種個人証明（在学証明、卒業証明等）をスマホアプリに格納、ポータビリティの実現と、確実な検証を可能とする</u>

- オンライン・オフラインの両方で利用可能な身分証明書
- 塾内だけでなく大学間・企業との連携など広く展開を目指す
- 大学発行の証明書以外に民間の発行する証明書も格納
- 分散型IDの標準技術利用により永続性、相互運用性を実現



背景とこれまでの取り組み

背景①：資格証明の課題

ブロックチェーンの利活用先として注目
- アイデンティティ
- 資格証明（学位等）

課題はある！

背景②：標準化等の動き

分権型アイデンティティに関する標準化
- W3C
- Sovrin Foundation
- Decentralized Identity Foundation

そろそろ行けそう

背景③：実用化への壁

適用シナリオの検討不足
PoCばかりで実用化に至らない

先に進めたい！

これまでの取り組み

① プロトタイプシステムの開発
- 既存実装（uPort）をベース
- ID基盤連携
- 証明書発行システム連携

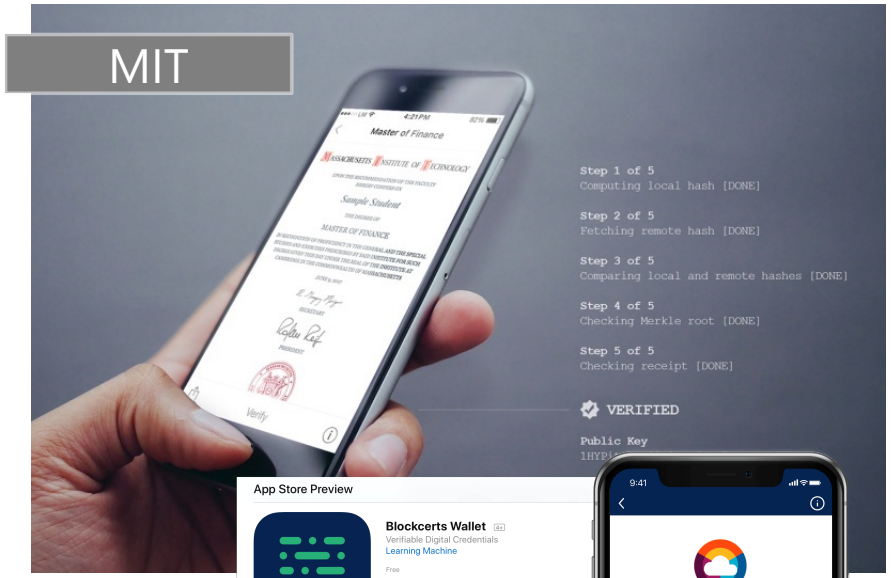
② 利活用シナリオの検討
- AXIES年次大会でのサーベイ
- その他大学における利用シナリオ検討

③ 他の取り組みの情報収集・共有
- キャッシュレス決済
- 他の属性証明の取り組み（古物など）

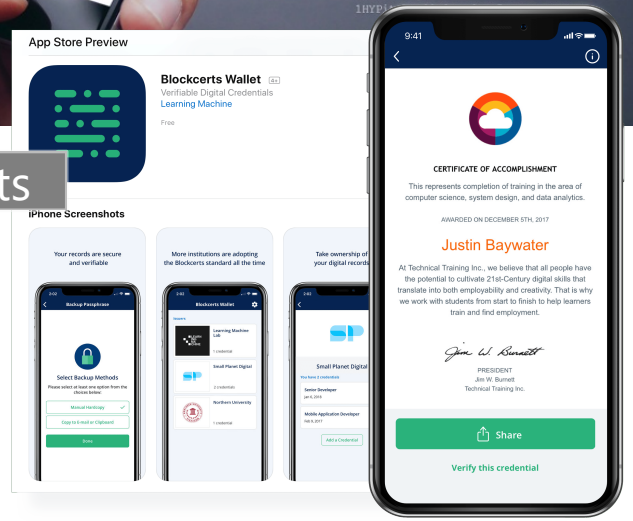
背景①：資格証明の課題

- 資格証明・学位証明へのBlockchainを適用

MIT



Blockcerts



経済産業省
Ministry of Economy, Trade and Industry

申請・お問合せ | English | サイトマップ | 本文へ | 文字サイズ変更 小 中 大

ニュースリリース | 会見・談話 | 審議会・研究会 | 統計 | 政策について

ホーム ▶ ニュースリリース ▶ ニュースリリースアーカイブ ▶ 2018年度2月一覧 ▶ ブロックチェーンハッカソン2019を開催しました

ブロックチェーンハッカソン2019を開催しました

～学位・履修・職歴証明や研究データ管理の真正性が担保される社会基盤構築を目指して～

2019年2月28日

▶ 経済産業

の領域においてブロックチェーン技術による社会実装を進める端緒とし（事務局：株式会社リクルートR&D）を下記のとおり開催し、最優しました。

経産省

本取り組み関係者も関与

- 審査委員長：JDD楠さん
- 審査委員/WS：富士榮
- 優勝チーム：BlockBase

背景②：標準化等の動き

- DID（Decentralized Identifiers）
- VC（Verifiable Credentials）

- Discovery
- Presentation Exchange

etc

- Governance Model

etc

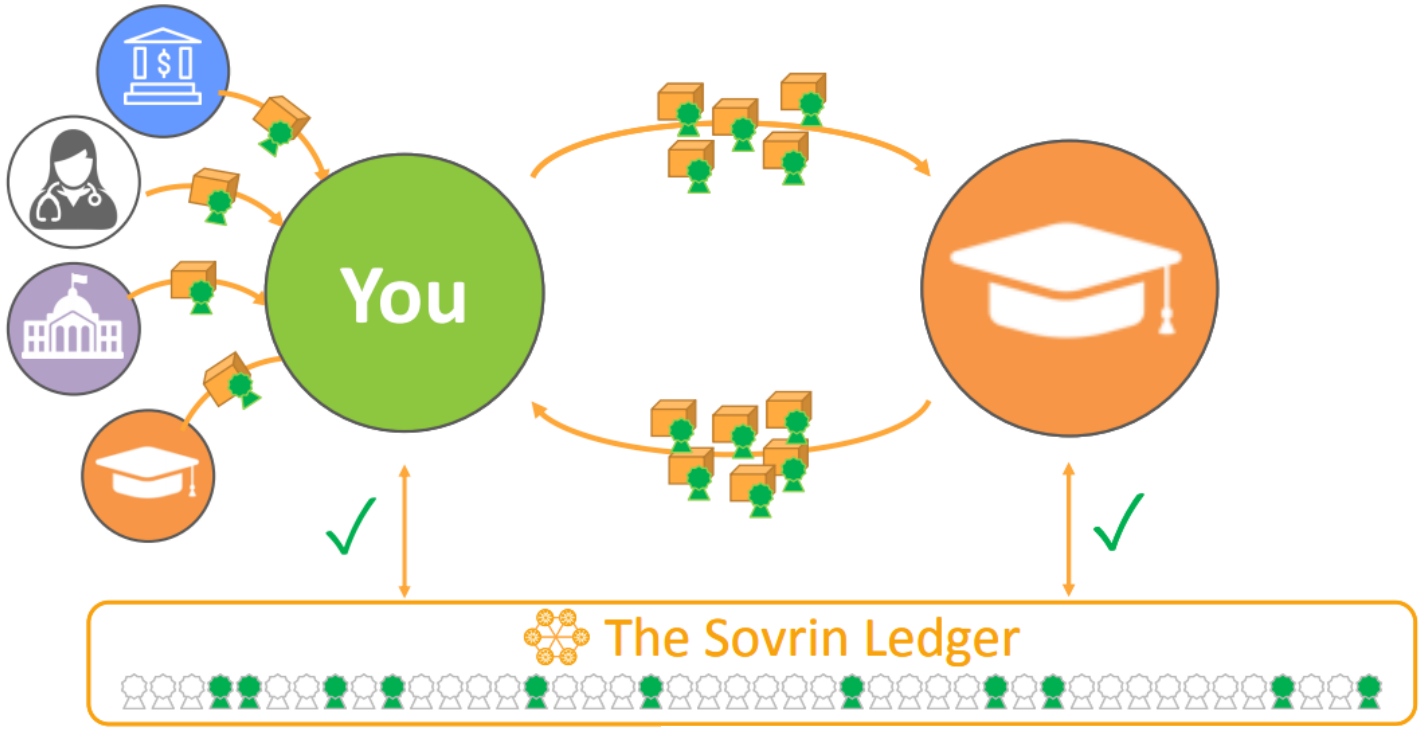
背景③：実用化への壁

控えめに見積もってもドクターは年間25,000人日かけて55,000人の研修医の身元確認を行っている。

PoCばかりで実用化に至っていない

- ビジネスモデルが描けない
- 従来の方法でそれほど困らない

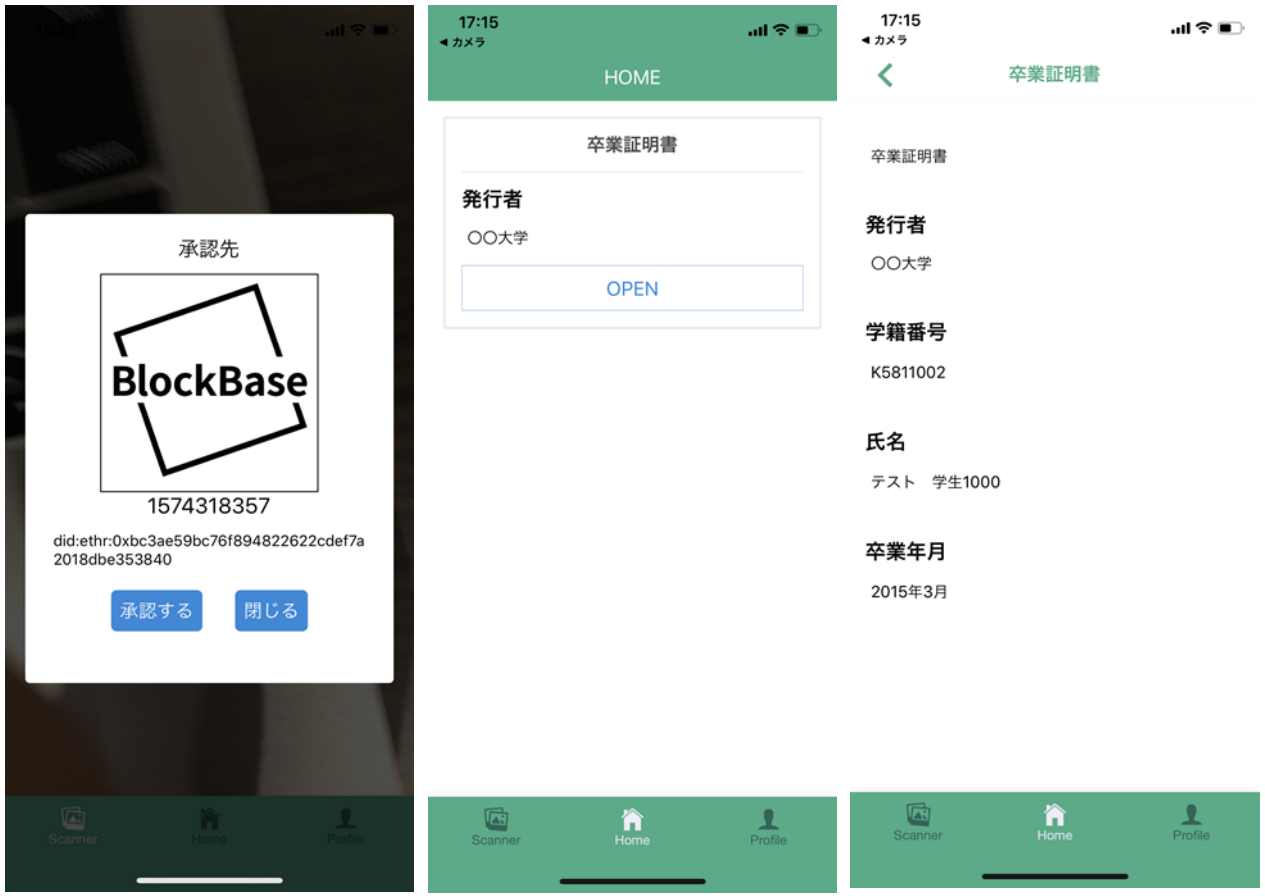
COVID-19によるリモート推進は起爆剤？



出典）The world's first digital self sovereign identity for Doctors: Where trust meets trust / Dr Manreet Nijjar, EIC2018

これまでの取り組み

MVP開発



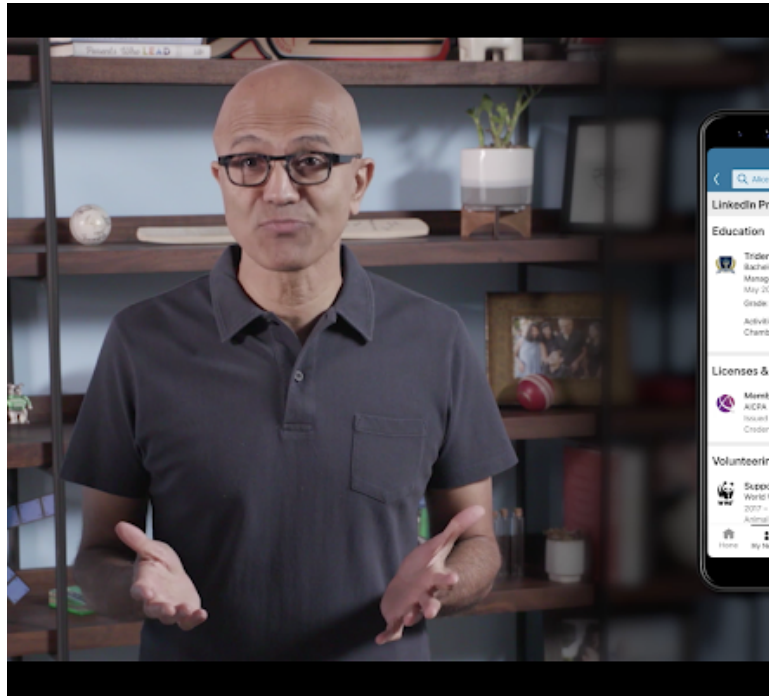
AXIES2019でのヒアリング

一方でMicrosoftの動き

- 2017 : uPort/Consensysとの協業@Consensus 2017
- 2019 : ION（アイオン）の発表
- 2019 : DID Preview update, private preview開始
- 2020 : 米国の退役軍人の

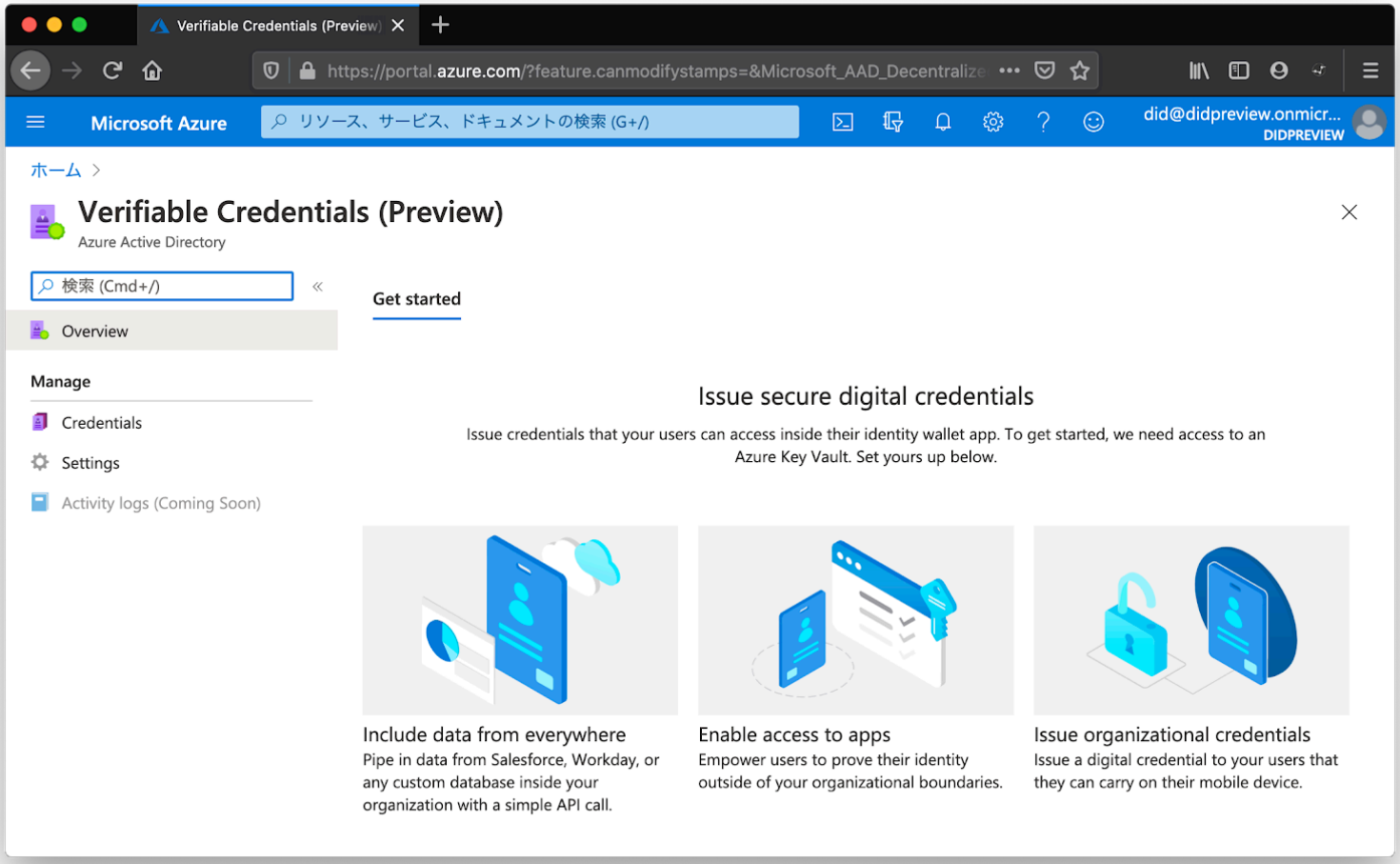
シナリオで実証実験発表@Ignite

良いタイミング！検証開始



通称PICS: Portable Identity Card Service

- Azure Active Directoryのコンポーネントの一部として提供
（要Azure AD Premium P1）
- MSがホストするIssuerサービス＋α
- ＋αの部分は
  - Discovery（Universal ResolverのFork）
  - Presentation Exchange
- IssuerのフロントはSDK提供
- HolderはMS Authenticator
- VerifierはSDK提供



デジタル学生証に関するご協力の依頼

慶應義塾様への打診

目的

「**学生の身元確認、学位取得確認**」を効率化する

目標

オンラインで利用できる
「**学生の身元証明、学位取得証明**」に関する「**グローバル標準**」を作成する

そのために、2020年度に下記2点を実施する

1. 学位等の証明データの**スキーマ標準化**
2. **Blockchain**を使った証明データの発行～真正性確認技術の確立（PoC実施）

慶應義塾様への依頼事項

本年度施策２：**PoC実施のためのフィールドをご提供いただきたい**

※想定シナリオ：デジタル学生証への在学証明の発行～利用

- 各種申請等のオンラインシステムの利用（ログイン～身元確認）
- JCB殿のプリペイドカード（JCB PREMO）との連携（アプリ間連携から試行）

取り組みの背景と目指す方向性

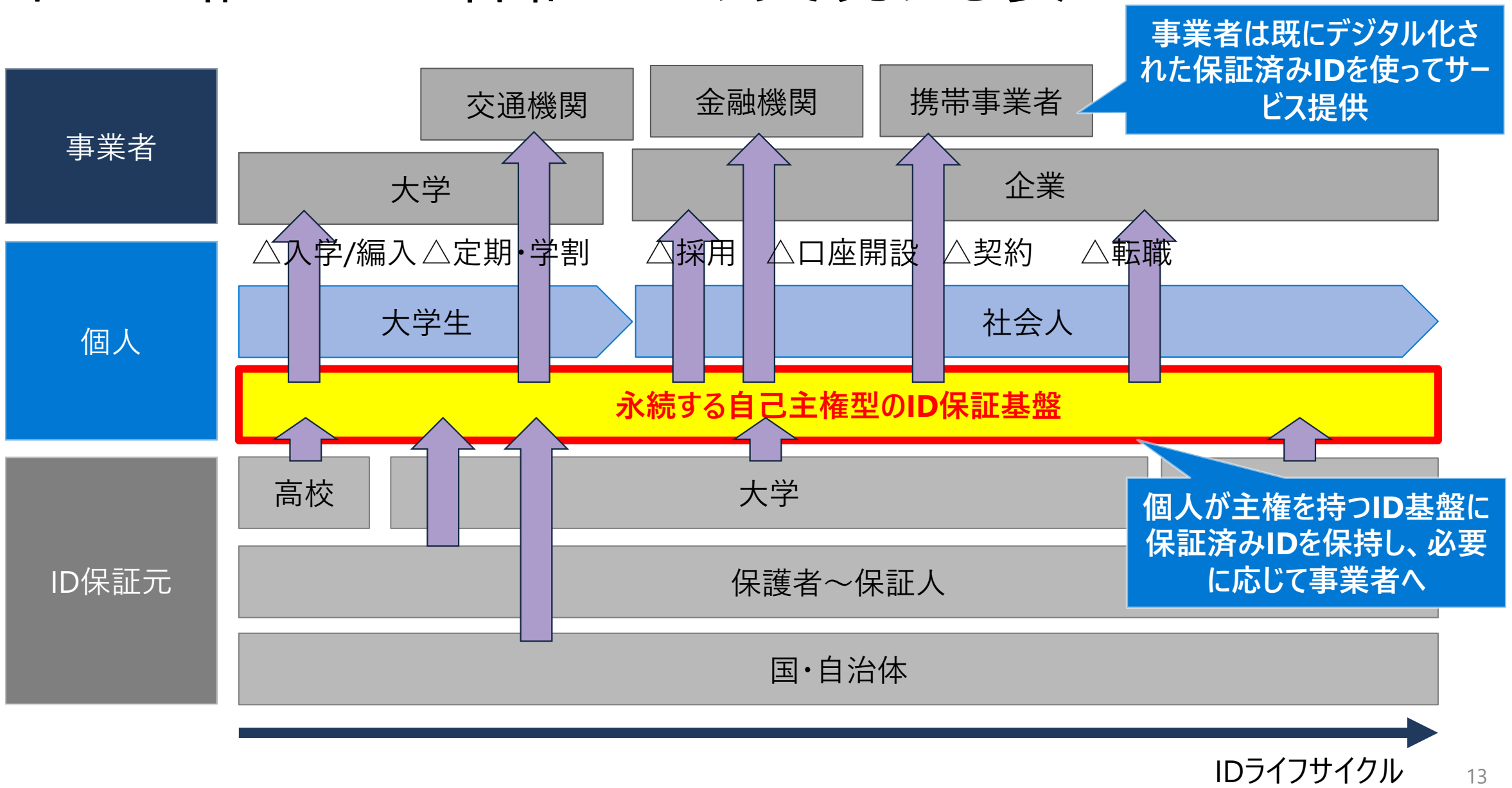
慶應義塾様への打診

	課　　題	背　　景	取り組みの方向性
信頼・保証	• KYCコストの増大（時間、手間、コスト） • セキュリティ対策コストの増大	• 対面を前提とした信頼フレームワーク • 信頼できる共通の属性提供基盤が存在しない（公的個人認証の低普及率）	• 永続的に検証可能な属性提供基盤の構築 • 入口（属性付与）の段階でのデジタル保証
プライバシ・非対称性	• 力のある事業者による過度な個人情報の収集（GAFAなど） • コンテキストを超えた情報の共有によるプライバシ侵害	• 個人情報に基づくサービス提供（CRM）構造の過度な発達 • データを中心としたビジネスモデル	• 利用者自身により選択的に属性を提供することの出来る基盤の構築（自己主権型ID）

デジタル世界における個人証明によるDXの実現

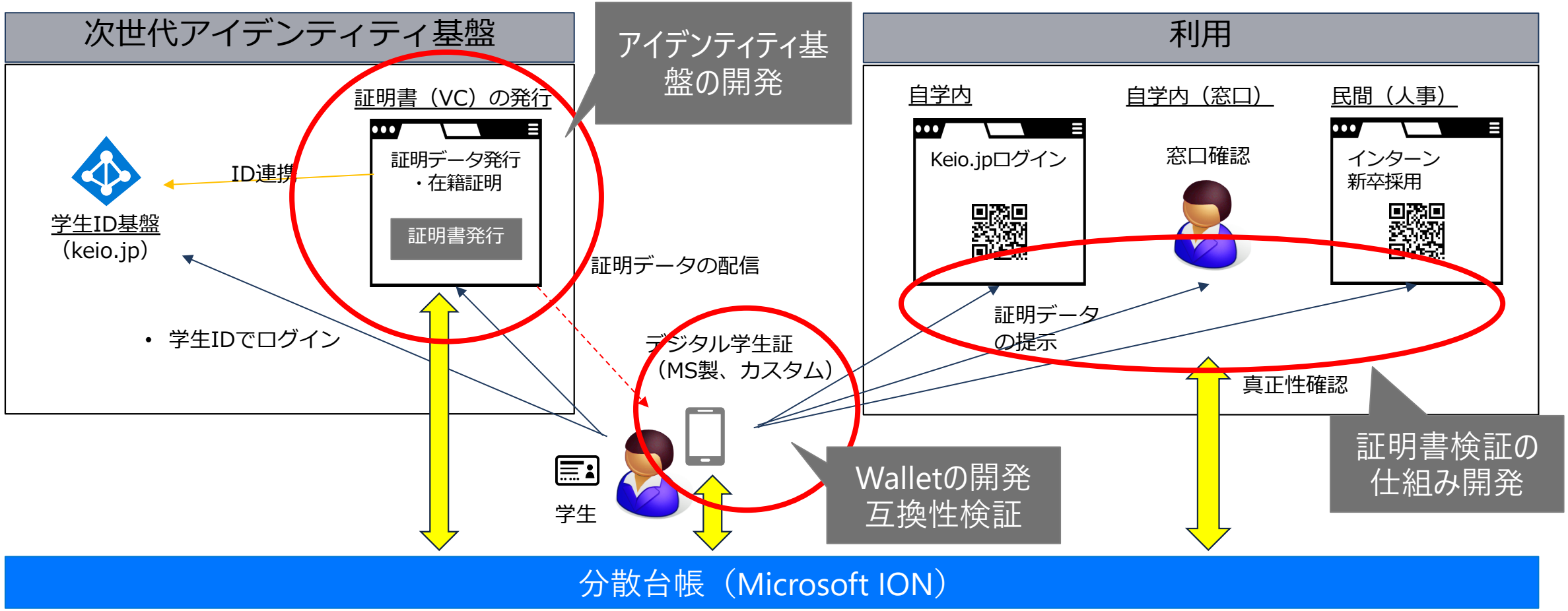
自己主権型のID保証により実現する姿

慶應義塾様への打診



PoCシステム構成と開発内容

標準仕様に則り、アイデンティティ基盤、デジタル学生証（スマホWalletアプリ）、証明書検証の仕組みの開発を実施
（基盤としてMicrosoft社の提供するSDK、Serviceの利用して開発）



PoCシナリオの例

最終的には永続的に検証できることが大切だが、普及に向けて目に見えるシナリオから入る必要あり

- 既存認証基盤との連携
  - Webシステムへのログイン
    - QRコードをスマホアプリで読み込むことでログイン
  - 従来窓口で本人確認をしてパスワードリセットをしていたが、スマホでQRコードを読み込むことで学生証提示をし、オンラインでリセット
- 各種オンライン受付
  - QRコードをスマホアプリで読み込むことで受付完了
  - デジタル学生証を提示することで別の証明書を発行
    - 卒業証明書、学割チケットなど

学生証を提示して学割チケットを入手する例

スマホアプリに
デジタル学生証を発行

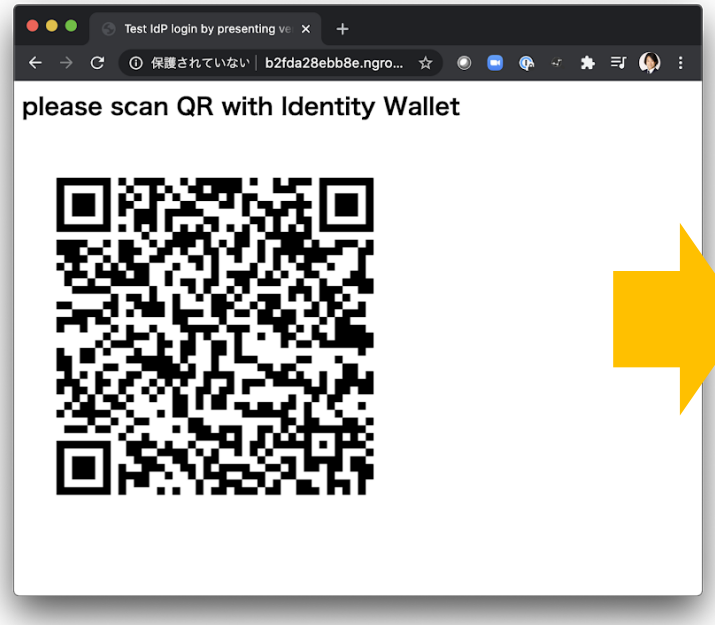
デジタル学生証の提示
学割チケットを取得

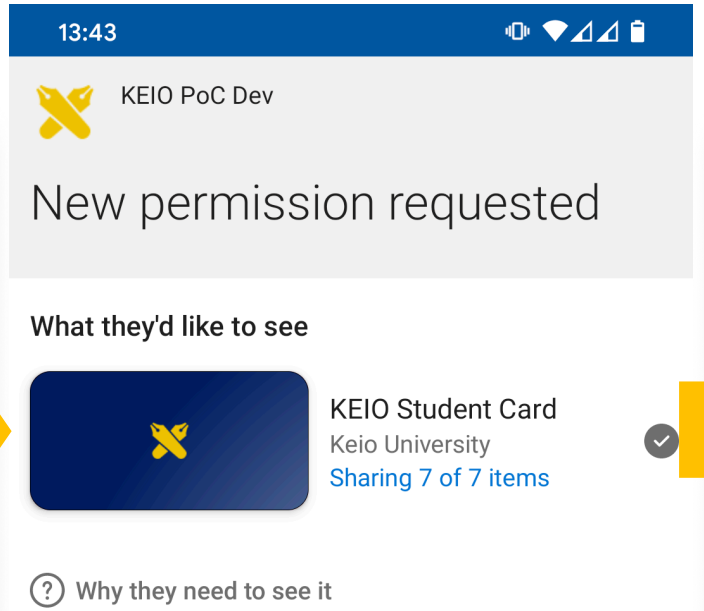
スマホアプリに
学割チケットが発行

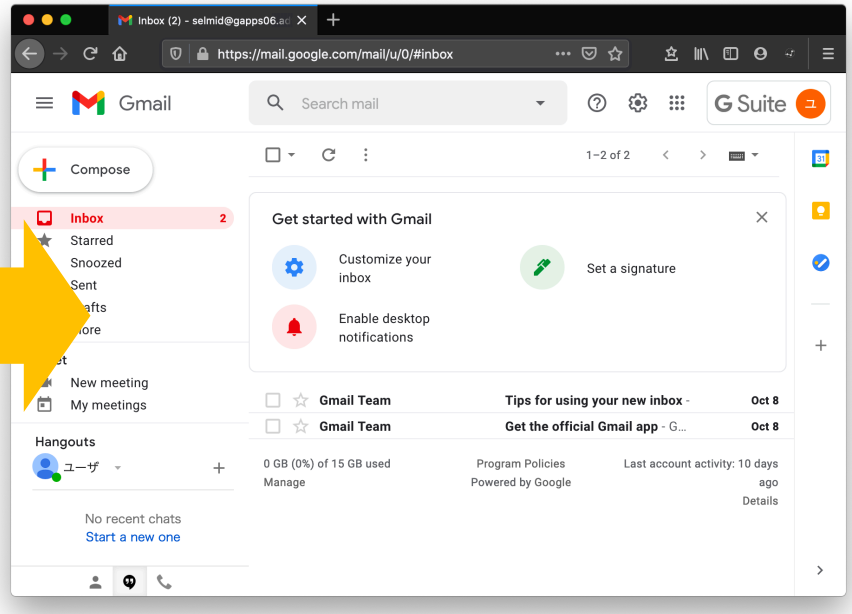
※技術標準に対応した複数種類のスマートフォンアプリを使い相互運用性を検証

デジタル学生証でWebサイトへログインする例

- Webサイトを開き、QRを表示
- スマホアプリ（デジタル学生証）でQRを読み込み
- ログイン完了







なぜデジタル学生証に分散台帳を使うのか

証明書発行のシナリオ

証明書で一番重要な点は「確実に検証できること」

要件	考慮事項
発行者の状況に依存しない	大学の統廃合、大学以外も考えると発行者がなくなる可能性
改竄、捏造の検知ができる	改竄だけでなく、発行者がなくなった状態でも捏造できない
誰もが検証できる	全ての利用者が発行者と直接連携する必要がないこと

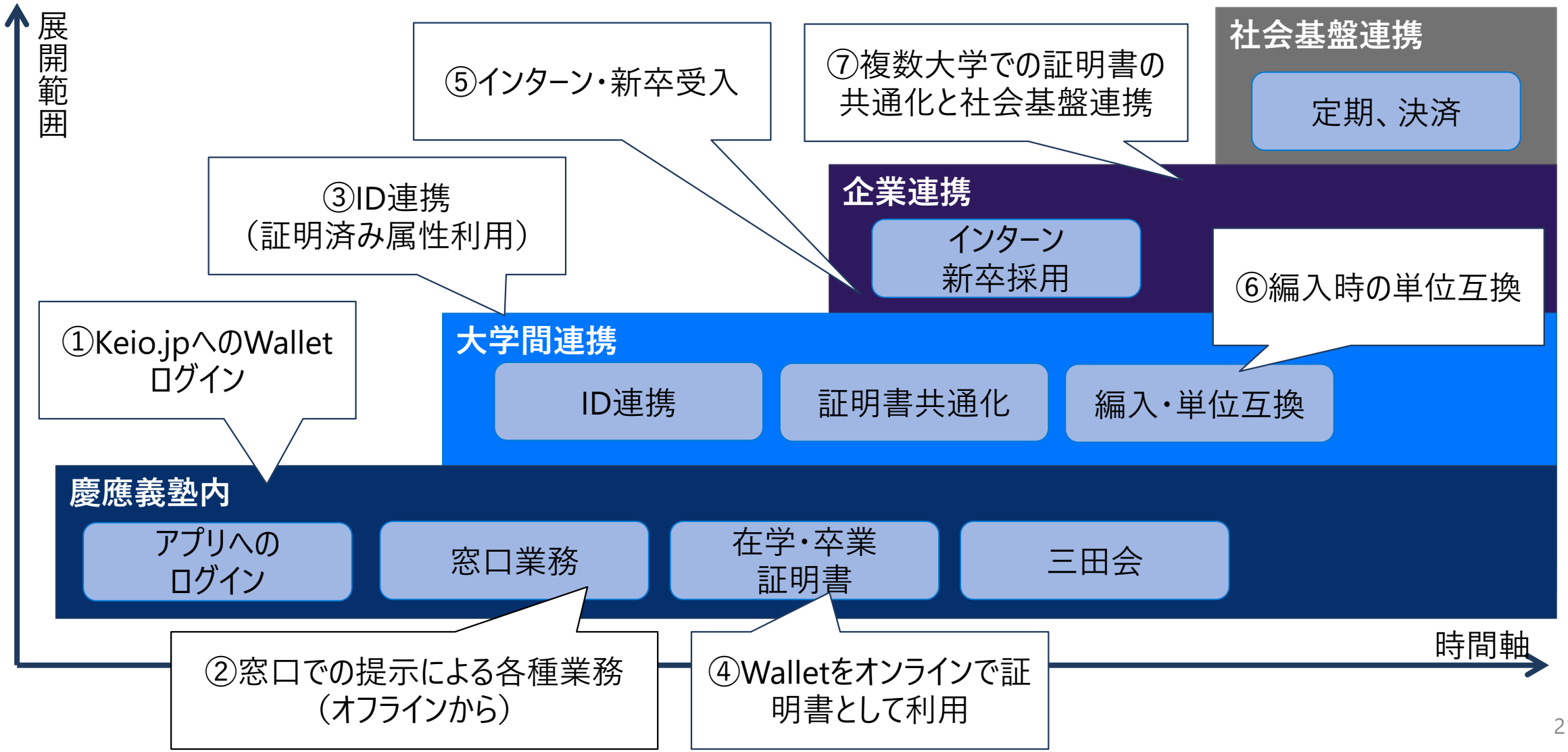
単純にPDFへの電子署名＋αが必要となる可能性がある

分散台帳を使う理由

- まず、分散台帳（≠ブロックチェーン）ありきではない
  - 決して**ブロックチェーンありきではない**
- やりたいことは**確実な検証**
  - 検証自体は鍵とデジタル署名で行う
  - ここまでなら分散台帳は不要
- **永続性**を担保できる仕組みが必要
  - 発行者がいなくなってもユーザが永続する
  - 発行者がいなくなっても発行済み証明書を継続的に検証できる
  - 署名検証用の基盤が永続する

少なくとも卒業生は使えるようにしないと・・・

今後の展開


展開範囲
⑤インターン・新卒受入
⑦複数大学での証明書の共通化と社会基盤連携
社会基盤連携
定期、決済
③ID連携
（証明済み属性利用）
企業連携
インターン
新卒採用
⑥編入時の単位互換
①Keio.jpへのWallet
ログイン
大学間連携
ID連携
証明書共通化
編入・単位互換
慶應義塾内
アプリへの
ログイン
窓口業務
在学・卒業
証明書
三田会
②窓口での提示による各種業務
（オフラインから）
④Walletをオンラインで証
明書として利用
時間軸

今後の展開において鍵となるポイント

- 標準への準拠
  - グローバルで広く・永続的に利用するためには標準が対応
    - 技術レイヤ：W3C/DID、VC、DIF/PE、OpenID Foundation/DID-SIOP、eKYC&IDA
    - データレイヤ：MIT/OpenBadge、Blockcerts

- 出口戦略の練り込み
  - シナリオの検討：金融、保険、教育、人材、運輸など
  - 現行の法規制との調整：犯罪収益移転防止法、携帯電話不正利用防止法など

最後に

- 証明書のシナリオは典型的な卵と鶏
  - 発行者（Issuer）が増えないと利用者（Verifier）が増えない
- 今後はデータ層の標準と相互運用性がポイント
  - 技術層（DID/VCなど）はある程度標準が固まってきた

多くの機関に参加していただき、社会基盤へ広げていくことが肝心
是非一緒に取り組んでいきましょう