DIDと関連技術、その標準化動向、応用事例

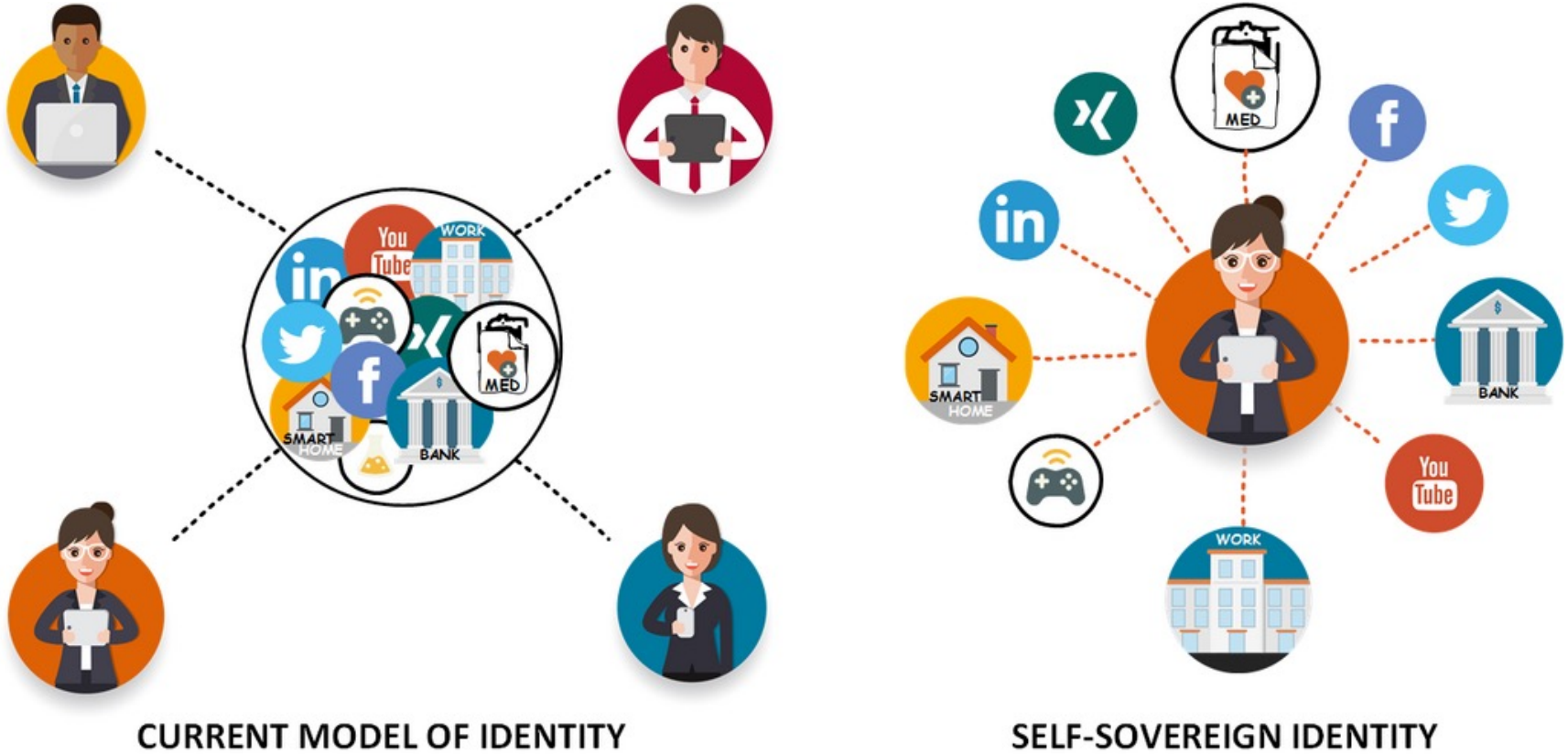
2021/09

一般社団法人OpenIDファウンデーションジャパン – 代表理事/KYC WGリーダー
OpenID Foundation – Co-chair, eKYC & Identity Assurance Working Group
伊藤忠テクノソリューションズ株式会社

目指すデジタル社会

ヒトを中心としたデジタル社会＝自己主権型アイデンティティが根ざした社会

- ✓ 事業者非依存：巨大な一部の事業者に個人情報を管理されない
- ✓ 個人の尊重　：自身の属性情報に主権を持ち、サービス提供者へ選択的に開示
- ✓ 高度な信頼　：サービス提供者は提供された属性情報を信頼し、無駄なく利活用



出典）https://blog.goodaudience.com/how-blockchain-could-become-the-onramp-towards-self-sovereign-identity-dd234a0ea2a3

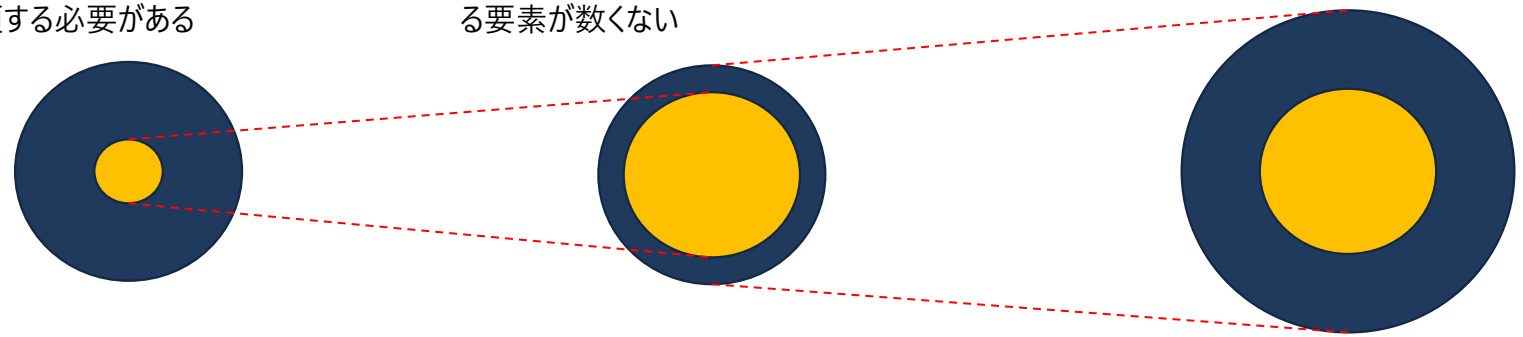
検証に基づく信頼と安全な社会へ

	デジタイゼーション	デジタライゼーション
デジタル社会	現在のインターネット • 容易に成りすませるID • 偽造コストの劇的な低下（スキャンした証明書等）	検証に基づく信頼 • 検証可能な仕組みの導入 • 検証可能な範囲の拡大が経済圏拡大の鍵
アナログ社会	信頼が成立する世界 • 知っている人だから信頼 • 提示された免許証が本物っぽいから信頼	–

アナログ社会～現在のインターネット：
検証できる部分が小さく、相手を大きく信頼する必要がある

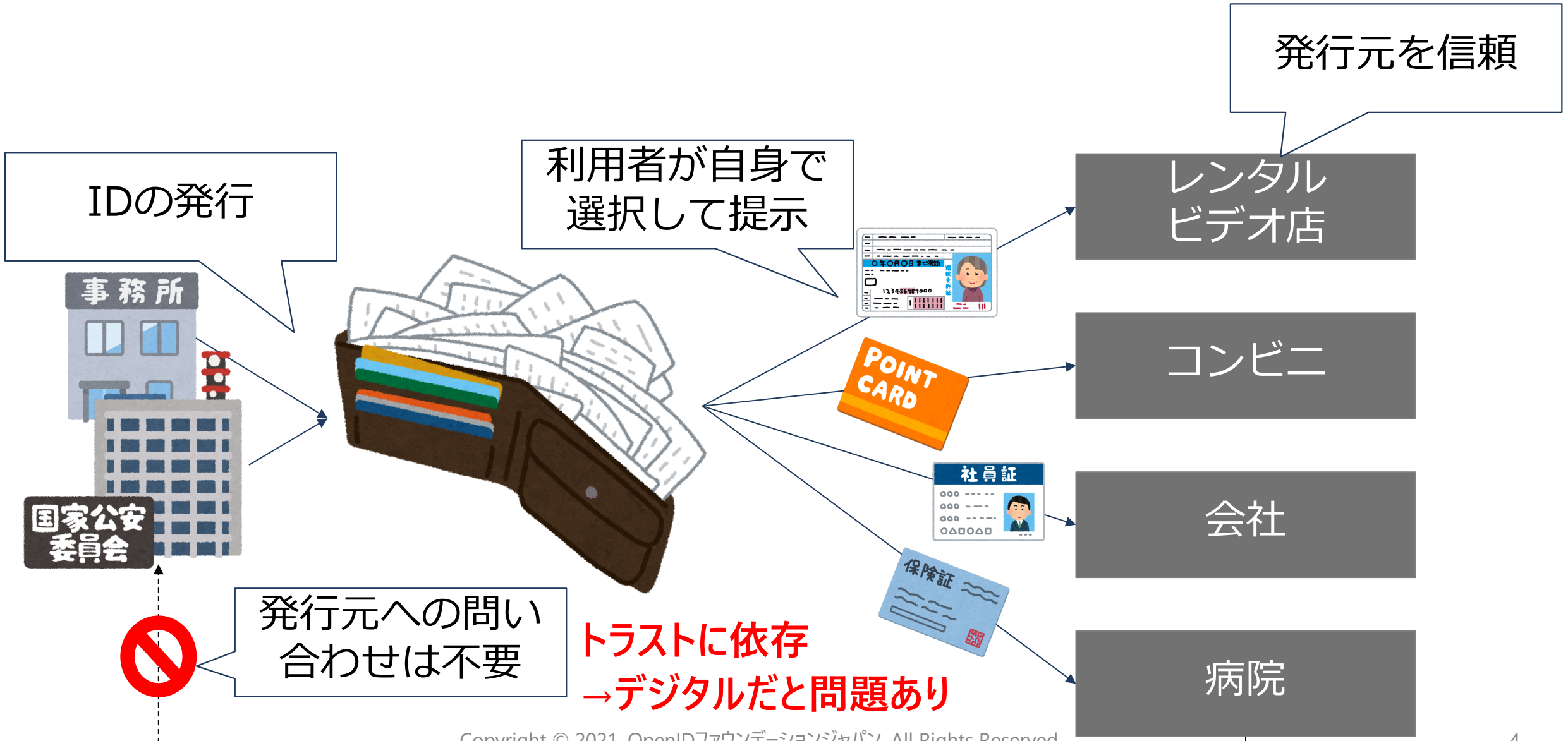
分散台帳等により検証可能な範囲の拡大：
検証できる部分が大きく、相手を信頼する要素が数くない

目指すところ：
検証できる部分の担保により信頼できる幅をより広げる



信頼（トラスト）の定義：
→事実の確認をしない状態で、相手先が期待したとおりに振る舞うと信じる度合い
※内閣官房/Trusted Web推進協議会より
※図はTrusted Web推進協議会の資料をもとに作成

現実世界のモデル＝ポータブルだが未検証



信頼のDXと分散型ID

	ポイント	物理世界のID	従来のデジタルID	分散型ID（DID/VC）
持ち運べる	**利用者の意思**で、 • いつでも使える • 使い分けができる	• 財布に入れて免許証、社員証などを持ち運ぶ • 使い分けができる	• IDシステム状態に**依存**する（システム停止、アカウント停止等） • 提示情報の使い分けは難しい（利用者の**意思は反映されにくい**）	• **スマホ、NFCチップ等**にIDを入れて持ち運ぶ • 提示属性の**選択・使い分け**ができる
検証可能である	受取った側が、 • **真贋判別が出来る**	• **対面で**表情などを含め総合的に判断 • **勘と経験で**免許証の真贋を判断	• IDシステムでユーザ認証して検証する（認証強度により**ID漏洩の危険性**） • IDシステム状態に**依存**する（システム停止等）	• 分散台帳上の公開鍵を使い、**ID発行元への問い合わせせずに**検証可能（永続性の担保、事業者依存からの脱却）
		対面前提、勘と経験	ID漏洩、プライバシ問題	**真のDXの要として注目**

中心となる技術要素
- 分散台帳上で管理される**分散型識別子**（Decentralized Identifiers / DID）
- 分散型識別子と関連付けされた公開鍵で**検証可能な属性情報**（Verifiable Credentials / VC）

DID/Decentralized Identifiers

- メソッドを構成する事業者やノードに依存しない**識別子**
- 自然人や組織など（Subject）とメタデータ（DID Document）に紐づくURI
- フォーマット
  - [スキーム]：[メソッド]：[メソッド固有の識別子]
  - 例）did:sov:123456789abcdefghi
  - メソッドは系毎に割り当てられる（sov, ion, btcrなど..現在約100種類）
- **鍵ペアの生成と署名・署名検証**
  - 公開鍵はDID Document上へ公開、秘密鍵で署名したVerifiable Credentialsを検証
- 仕様（現在CR）
  - https://www.w3.org/TR/did-core/

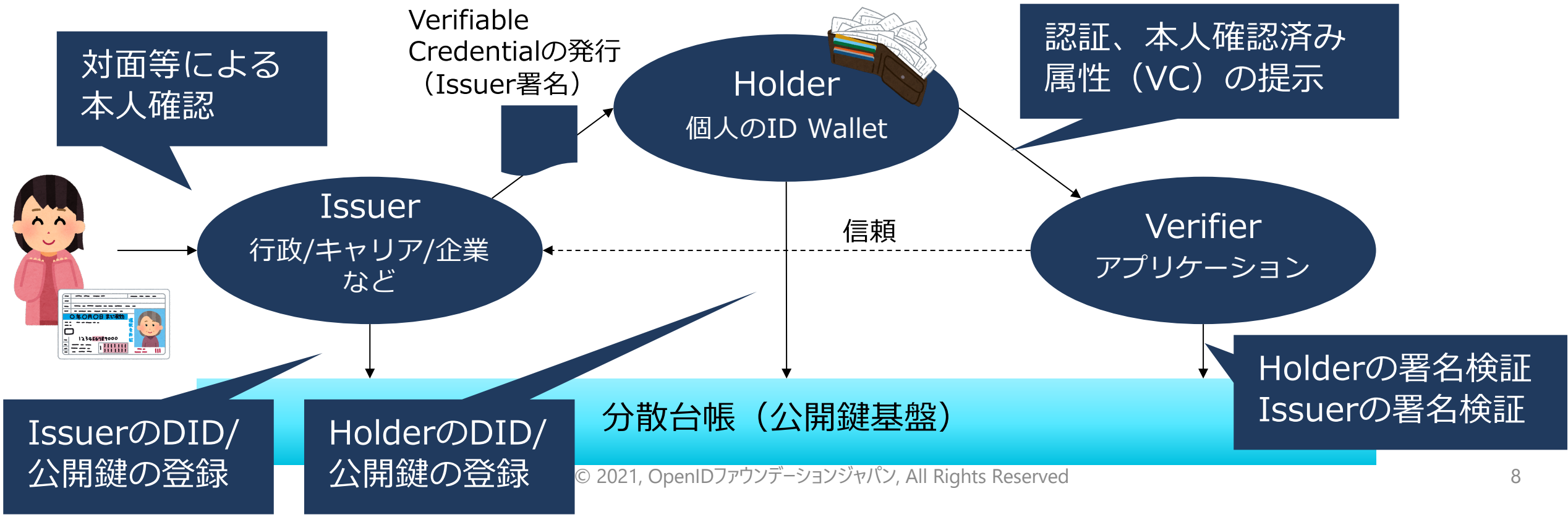
Mozilla foundationからの物言い（2021/9）

https://lists.w3.org/Archives/Public/public-new-work/2021Sep/0000.html

- No practical interoperability.
- Encourages divergence rather than convergence.
- Centralized methods allowed, in contradiction to WG & spec goals & name.
- Proof-of-work methods (e.g. blockchains) are harmful for sustainability (s12y).

Verifiable Credentialsの利用モデル

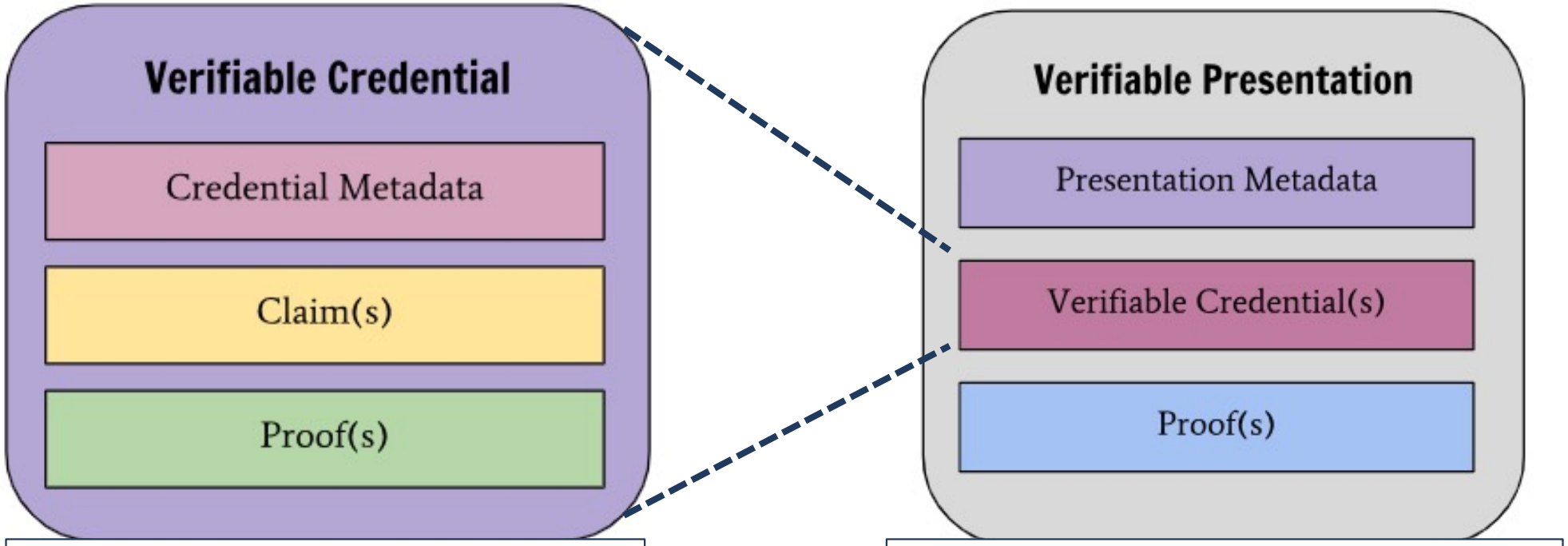
1. IssuerからHolderに対してVC発行（Issuer DIDで署名）
2. HolderがVerifierに対して提示（Holder DIDで署名）
3. Verifierは分散台帳上の公開鍵（DID Document）で真正性を検証



VC / Verifiable Credentials
VP / Verifiable Presentation

検証可能なデータモデル/表現（2019年11月 W3C勧告）

Issuerにより発行され、HolderがVerifiable PresentationとしてVerifierへ提示



Issuerが発行した検証可能な属性のセット

一つ以上のVerifiable Credentialsを含むHolder署名されたデータセット

Verifiable Credentialsの例

```
{ "@context": ["https://www.w3.org/2018/credentials/v1"],
  'type": ["VerifiableCredential",”https://vc.example.com/cred/Employee2020a”],
  'credentialSubject": {
        "firstName": "Duke",
        "lastName": "Harding",
        "employeeId": "3852985",
        "employeeType": "ft"
  },
  …
  "iss": "did:ion:EiCpKPqGVi_d…XRoIiwiZ2VuZXJhbCJdfV19fV19",
  "sub": "did:ion:EiBDu2M5GU…292ZXJ”
}
```

Schema

SubjectのIdentity情報

IssuerのDID

関連する標準化の動向

データモデルの標準化はほぼ完了（W3C DID、VC）

トランスポートについては議論が進行中

- DIDComm（DIF/Decentralized Identity Foundation）
  - https://identity.foundation/didcomm-messaging/spec/
- OpenID Connect拡張（OpenID Foundation）
  - SIOP v2（Self-Issued OpenID Provider）
    - https://openid.net/specs/openid-connect-self-issued-v2-1_0.html
  - OpenID Connect for Verifiable Presentation
    - https://openid.net/specs/openid-connect-4-verifiable-presentations-1_0.html
  - OpenID Connect Claims Aggregation 1.0
    - https://openid.net/specs/openid-connect-claims-aggregation-1_0.html

学位・成績証明への活用：OpenBadgeの動き

OpenBadgeとVCの互換に関する検討

W3C/CCG vc-eduで議論

- DCC（Digital Credential Consortium）
- IMS Global：OpenBadge自体の標準化はIMSで行うのが筋だが、ユースケース検討などはvc-eduで実施しているように見える
- ユースケース・相互運用性の観点からVC/OpenBadge連携について議論

v3でのHosted型→自己完結型への移行検討

- Hosted型：Badge検証を行う際に発行元へ問い合わせる
- 自己完結型：分散台帳等を使いBadge単体で検証できるようにする

VCとの互換性の方式の検討

VC Reference to OpenBadge Assertion

- VCの中に属性としてOpenBadgeを組み込む
- VC自体を検証後、OpenBadgeを取り出して改めて検証する

Prioritize OpenBadge as VC

- OpenBadgeのスキーマを優先しつつVCのスキーマにマッピングする

OpenBadge as VC – OpenBadge v3のProposal

- OpenBadgeとVCのスキーマの重複部分をVCに寄せる形で調整
- 現在、vc-eduではこの方式を推しており、ついでに理解度レベルなど新たなスキーマの追加も検討している状態

若干の宗教戦争？

JWT（JSON Web Token）or JSON-LD

- OpenBadgeの仕様としてはどちらでも良い、とはしているがv3はJSON-LDを前提とした書かれ方をしている
- VCとマッピングする上でJWT派、JSON-LD派が存在、実装系に依存する状態
- JWT派（MSなど）が提起している問題点
  - 署名の標準が存在しない
  - JWTだとJWSがあるが、JSON-LDにおけるLD-Proofについてはセキュリティ評価が済んでいない
  - 署名時にJSON-LDだとCanonicalizationが必要だが、これまでのSAMLの脆弱性の例のようにCanonicalizationで脆弱性が混入しやすい

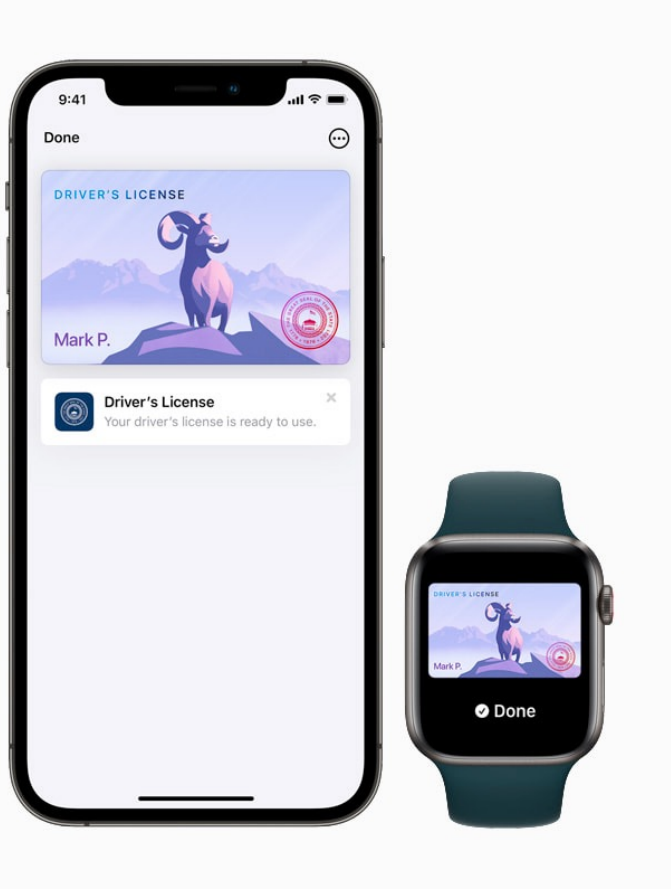
その他の動き：mDL（mobile drivers license）

ISO 18013-5

https://www.iso.org/standard/69084.html

Apple

https://www.apple.com/newsroom/2021/09/apple-announces-first-states-to-adopt-drivers-licenses-and-state-ids-in-wallet/



VCの応用事例

まだまだ試行錯誤の段階

特徴の整理

- 事業者がVCを発行する際は事業者のDIDに紐づく秘密鍵で署名を行う
- 公開鍵は分散台帳上に置かれるので、事業者は管理する必要がない
- 事業者が鍵をなくしても発行済みのVCの検証は継続的に可能

VC発行時点で発行者と関連があったことの証明（検証）が可能

- 多要素認証のキーとして
- 事業者所属である・だったことの証明として
- 各種アクティビティとの関係性の維持

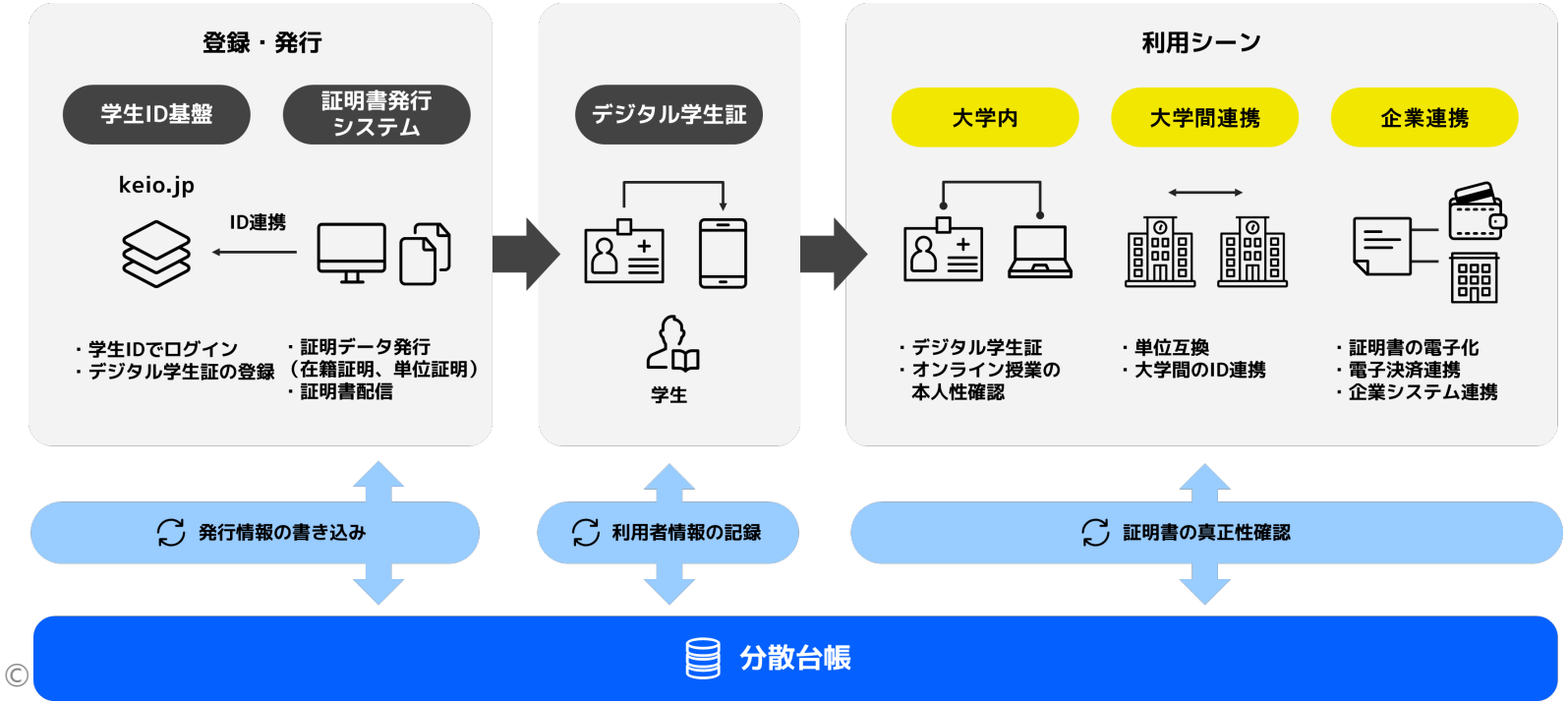
慶應義塾大学の事例（VCの利用）

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
・Microsoft Corporation（基盤提供）

<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>

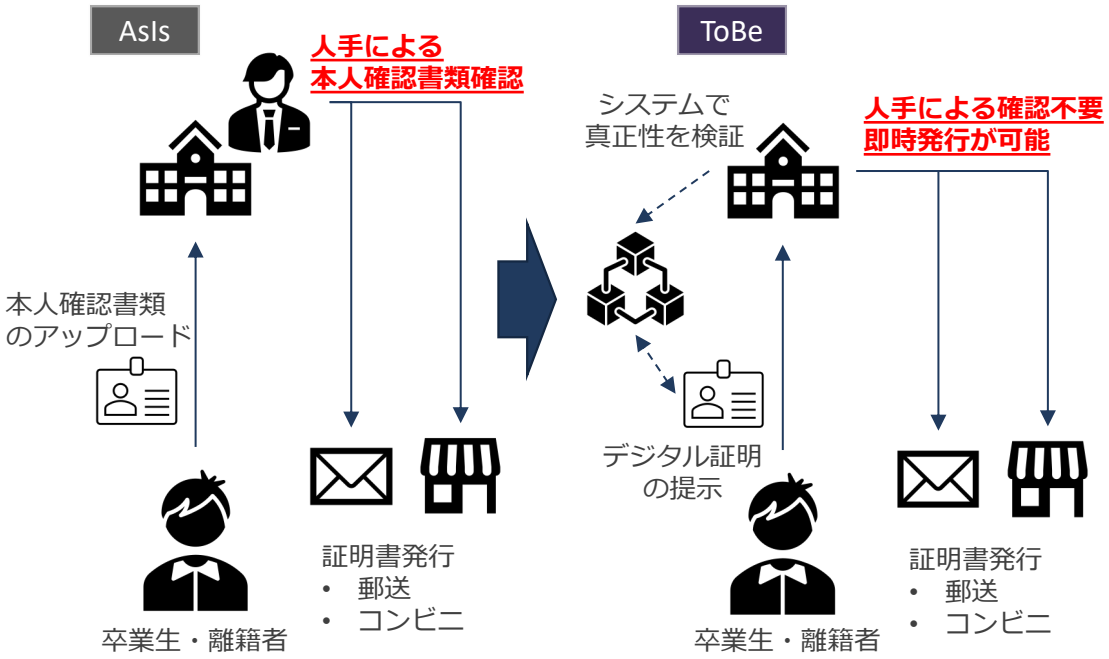
- オンライン・オフラインの両方で利用可能な身分証明書
- 塾内だけでなく大学間・企業との連携など広く展開を目指す
- 大学発行の証明書以外に民間の発行する証明書も格納
- 分散型IDの標準技術利用により永続性、相互運用性を実現



例）本人確認、成績証明など

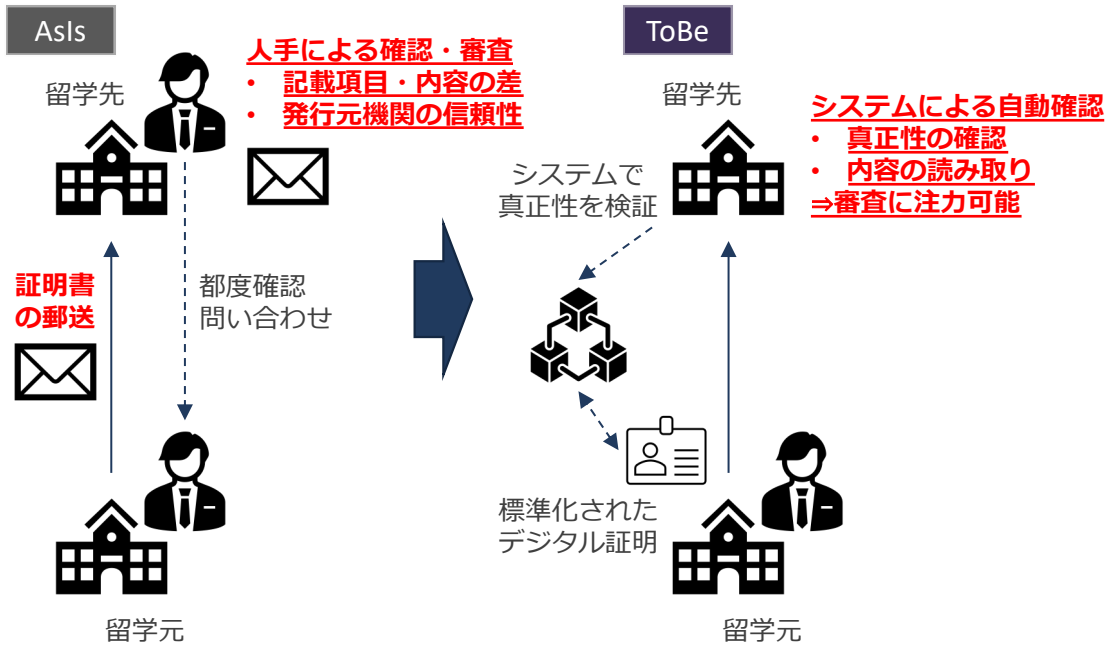
①本人確認の効率化

As Is：**本人確認書類の確認後**、アカウント払い出し～証明書発行
To Be：**確かに在籍していたことの電子的な証明**による証明書発行



②証明書確認の効率化

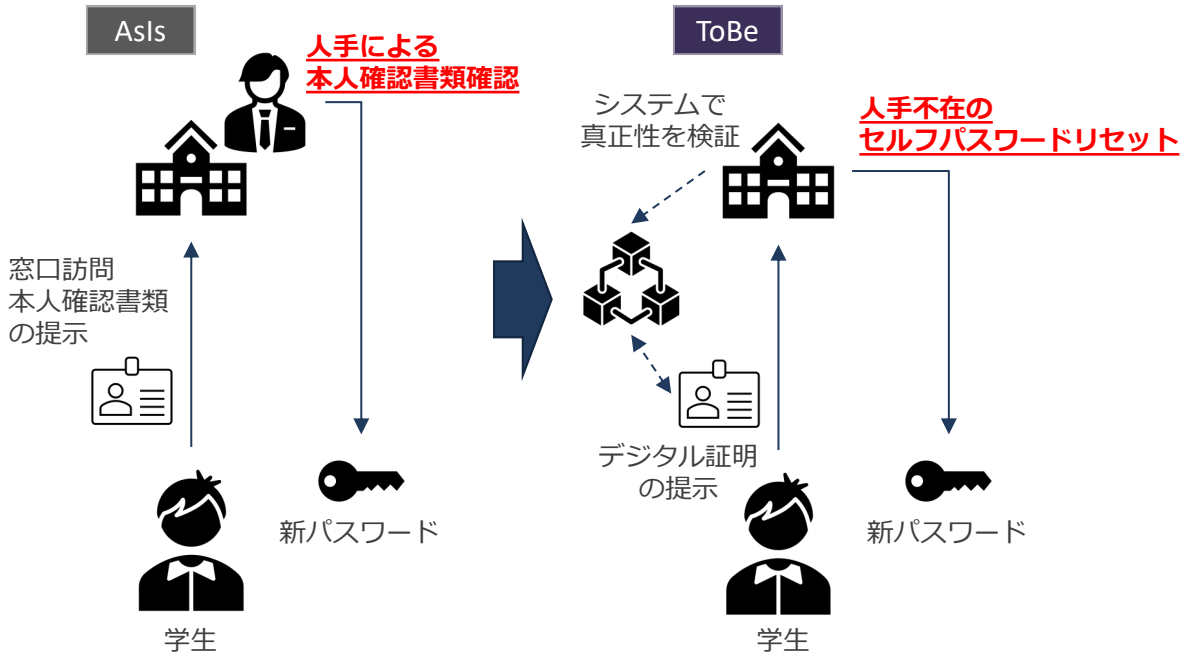
As Is：紙ベースの証明書の**郵送・確認、真贋確認が困難**
To Be：**標準化**されたデジタル証明書の**オンライン交換、真正性検証**



例）アカウントリカバリ、認証強化

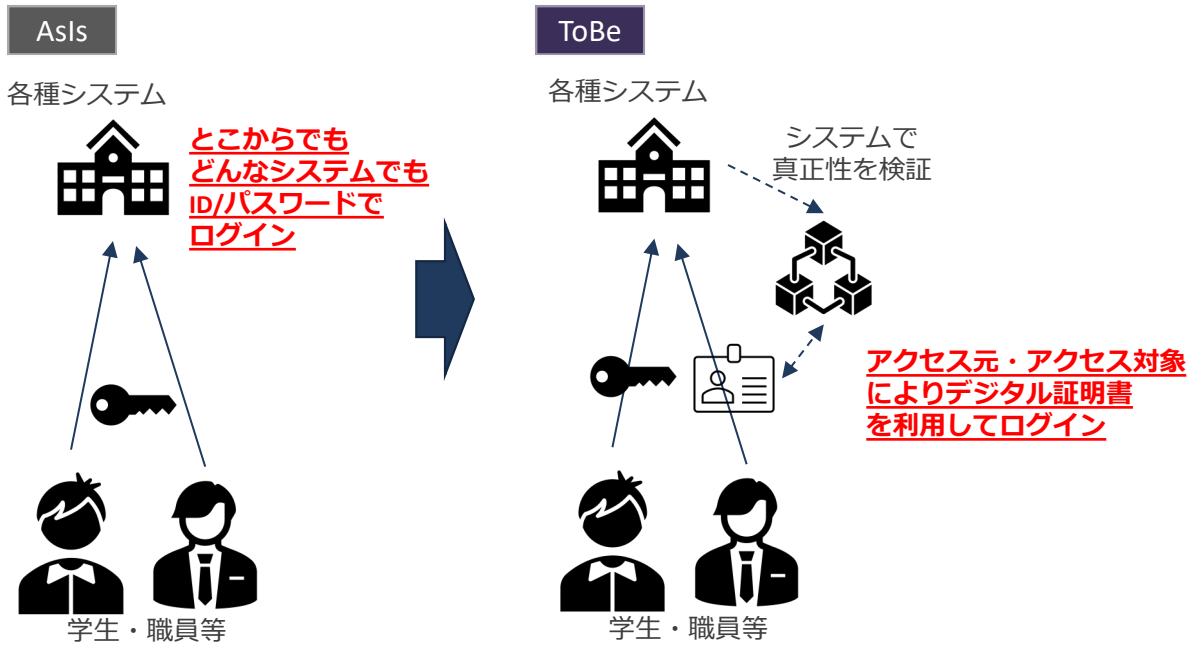
③パスワードリセットの効率化

As Is：**窓口での本人確認後**、パスワードリセット
To Be：電子的な本人確認による**セルフパスワードリセット**



④認証強化

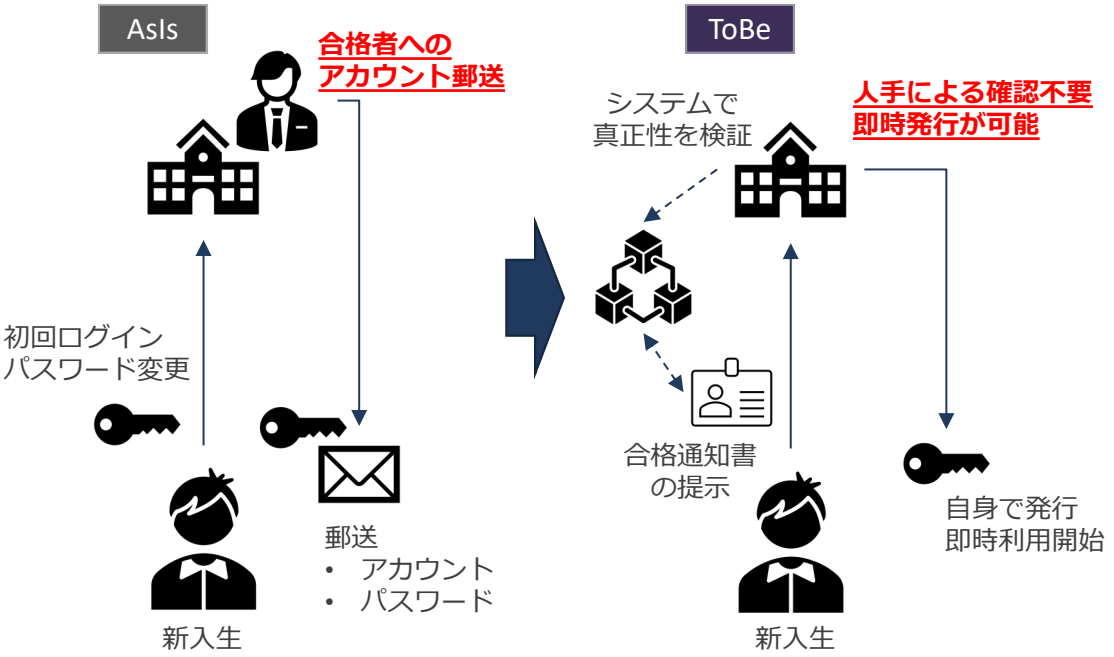
As Is：ID＋パスワードのみでログイン（**なりすましの危険性あり**）
To Be：利用シナリオに合わせて**デジタル証明書の提示を求め、認証強化**



例）リモートオンボーディング、卒業生ID

⑤アカウント払い出しの効率化

As Is：**郵送や対面でのアカウント払い出し**～システム利用開始
To Be：合格通知をデジタル証明書として発行、**自身でアカウント発行**



⑥卒業生IDの管理からの解放

As Is：卒業生・離籍者の**ID管理を行いたいが**人数規模・セキュリティ懸念から**断念**
To Be：デジタル証明書を発行、自身でIDを持ち運ぶため大学側で**ID管理は不要**