自己主権型IDと分散型ID

一般社団法人 OpenID ファウンデーション・ジャパン
理事／KYC ワーキンググループ・リーダー
米国OpenID Foundation
eKYC and Identity Assurance Working Group – Co-Chairman

富士榮　尚寛

OpenID Japan

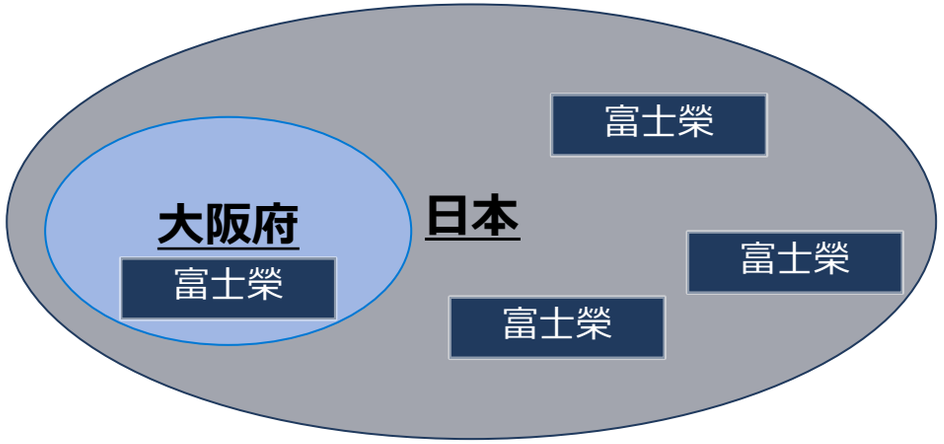
自己紹介

- デジタル・アイデンティティ歴、約17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
  - MVP for Enterprise Mobility 2010～
  - LINE API Expert for LINE Login 2018～
  - Auth0 Ambassador 2018～
- SIerでビジネス開発を担当
- Blog : IdM実験室（https://idmlab.eidentity.jp）

本日の内容・テーマ

- 言葉の定義に少しこだわってみる
  - アイデンティティ（Identity）
  - 識別子（Identifier）
- 自己主権型アイデンティティと分散台帳の関係性
- 普及向けて必要なこと

識別子（Identifier）とアイデンティティ（Identity）



- **識別子：Identifier**
  - 特定の集合の中で実体を一意に識別するための属性情報（一つとは限らない）
  - 日本の中に「富士榮」は複数いるので苗字は識別子にならないが、大阪府の中なら苗字で識別できる
- **アイデンティティ：Identity**
  - 実体を構成する属性の集合（ISO/IEC 24760-1より）
  - 識別子もアイデンティティを構成する要素の一つ

要素	解説	例
属性	後天的に取得された主体に関わる情報（後から変化する）	名前、電話番号、メールアドレス等
好み	主体の嗜好に関わる情報	甘いものが好き
形質	主体の先天的な特有の性質（後から変化しにくい）	生年月日、性別
関係性	他の主体との関係に関わる情報（一部属性と重複）	XX大学卒業、YY部所属

自己主権型アイデンティティ (Self Sovereign Identity/SSI)

CURRENT MODEL OF IDENTITY

SELF-SOVEREIGN IDENTITY

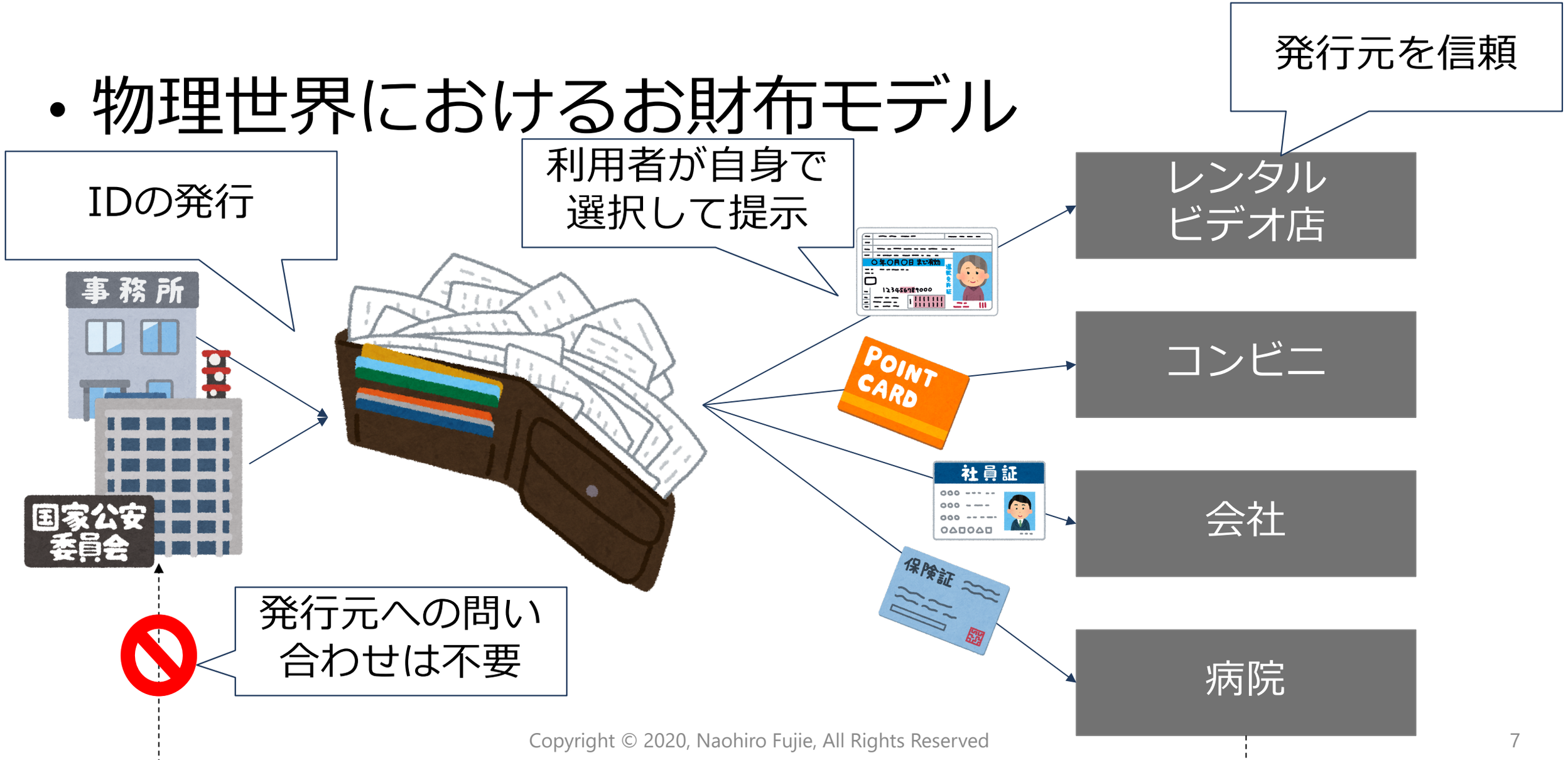
出典,
https://blog.goodaudience.com/how-blockchain-could-become-the-onramp-towards-self-sovereign-identity-dd234a0ea2a3

自己主権型**アイデンティティ** (Self Sovereign Identity/SSI)

- Sovrin foundationの定義
  - 自己主権型アイデンティティ（SSI）とは「**個人は、管理主体が介在することなく、自身のアイデンティティを所有しコントロールできるべきである**」、と考えるデジタル・ムーブメントを表す言葉である。SSIを使うと、人々は現実世界で彼らが行っているのと同じ自由度と信頼性をもってデジタル世界でも活動することが出来る。（https://sovrin.org/faq/what-is-self-sovereign-identity/）
- インテンション・エコノミー（Doc Searls / 2012）
  - 顧客の意思に基づく経済（VRM）の実現
  - 企業が顧客の関心（アテンション）を中心に行う経済活動（CRM）と対局
  - 顧客が企業に**自分自身の意思を持って属性を提供**することで、
    - 企業がBig Dataをもとに推測したリコメンド・広告表示による気持ち悪さからの脱却
    - 企業が大量データを収集・分析を行うためのコストの削減

SSIで実現したい世界観

- 物理世界におけるお財布モデル



自己主権型アイデンティティの考え自体は
ブロックチェーンと何の関係もない
→思想とテクノロジの分離が必要

The Laws of Identity in SSI / Kim Cameron

1. User Control and Consent
   - 利用者による管理と同意に基づくこと
2. Minimal disclosure for a constrained use
   - 制限された利用のための最低限の開示
3. Justifiable parties
   - 不必要なエンティティが関与しないこと
4. Directed identity
   - 名寄せ可能な（双方向）識別子、不可能な（単一方向）識別子
5. Standardized identity hub
   - 利用者が一貫性を持ち、かつコンテキストによってアイデンティティを使い分けられること
6. Standardized DID for long-terms identity stability
   - 事業者に依存せずにサービスを利用できる標準化された分散型ID
7. Human integration
   - ユーザが使いやすいこと（テクノロジ論ではない）

自己主権型アイデンティティ実現のための要件

視点	SSI実現のための要件		従来モデルにおける課題
利用者	特定のIDプロバイダに依存しないこと	事業継続性、可用性	IDプロバイダが停止すると連携サービスが使えない
		アカウント管理	IDプロバイダ側のポリシーによるアカウント管理。BANされると連携サービスが使えない
	プライバシ保護のための考慮を行うこと	IDプロバイダによる行動把握	サービスとID連携を行う＝IDプロバイダが利用するサービスを把握できてしまう
		サービスへ渡す属性の管理	どの属性を提供するかはIDプロバイダがサービスとの間で決める
		サービス同士の結託による行動把握	提供属性がIDプロバイダに依存、場合によってサービス同士で結託すると行動把握が可能となってしまう
サービス事業者	利用者から提示された属性情報を信頼できること	属性自体の信頼性	IDプロバイダによる検証に依存（KYCをIDプロバイダに依拠）
		属性発行主体の信頼性	基本的に事前信頼でスケールしない

自己主権型アイデンティティ実現のための要件

視点	SSI実現のための要件		従来モデルにおける課題
利用者	特定のIDプロバイダに依存しないこと	事業継続性、可用性	IDプロバイダが停止すると連携サービスが使えない
		アカウント管理	IDプロバイダ側のポリシーによるアカウント管理。BANされると連携サービスが使えない
	プライバシ保護のための考慮を行うこと	IDプロバイダによる行動把握	サービスとID連携を行う＝IDプロバイダが利用するサービスを把握できてしまう
		サービスへ渡す属性の管理	どの属性を提供するかはIDプロバイダがサービスとの間で決める
		サービス同士の結託による行動把握	提供属性がIDプロバイダに依存、場合によってサービス同士で結託すると行動把握が可能となってしまう
サービス事業者	利用者から提示された属性情報を信頼できること	属性自体の信頼性	IDプロバイダによる検証に依存（KYCをIDプロバイダに依拠）
		属性発行主体の信頼性	基本的に事前信頼でスケールしない

1 2 3 4 5 6

The Laws Of Identity in SSIの項目をマッピング

分散型**識別子**（Decentralized Identifiers/DID）

- The Laws of Identity in SSIの6番目
  - 事業者に依存せずにサービスを利用できる標準化された分散型ID
- 特定の事業者に依存しない識別子（Identifier）
  - 発行主体の事業継続性、発行主体によるアカウントBANへの対応
  - 標準化が最も大切な領域（W3Cによる標準化対象）
- 分散台帳（≒ブロックチェーン）の出番の一つ
  - 特定の主体に依存しない　：　**パブリックチェーン　＞　コンソーシアム**
  - プライベートチェーンで発行するDIDに意味はない
    - コンソーシアムを含め運用主体のライフサイクルに依存するDIDに永続性はない
  - W3Cのメソッドレポジトリを見ていると微妙なものも
    - https://w3c.github.io/did-spec-registries/#did-methods

利用者のDIDの発行は
分散台帳（≒ブロックチェーン）
を適用できる分野の一つ
効果を出すにはパブリックチェーンが適している

サービス事業者から見たSSI適用時の課題

利用者が表明したアイデンティティをどう信頼するか

- **発行されたアイデンティティ**をどうやって信頼するか
  - 発行されたアイデンティティは確かに利用者に対して発行されたものか
  - 改竄されていないか
- **発行者**をどうやって信頼するか
  - 従来モデルと異なり、都度発行主体への問い合わせは行わない
  - その発行主体は（過去を含め）実在し、現実世界の発行主体と等しいか

自己主権型アイデンティティ実現のための要件

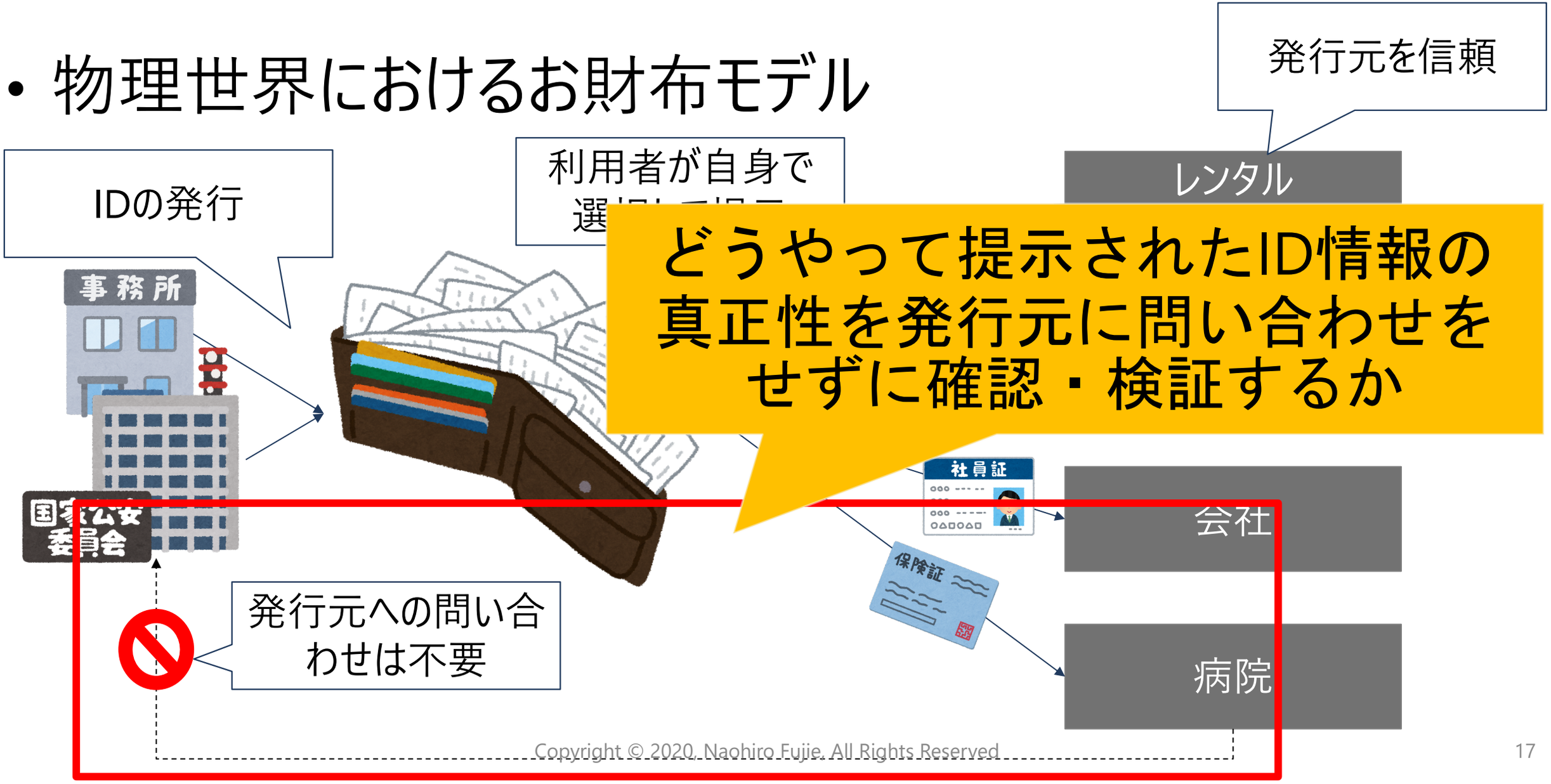
視点	SSI実現のための要件		従来モデルにおける課題
利用者	特定のIDプロバイダに依存しないこと	事業継続性、可用性	IDプロバイダが停止すると連携サービスが使えない
		アカウント管理	IDプロバイダ側のポリシーによるアカウント管理。BANされると連携サービスが使えない
	プライバシ保護のための考慮を行うこと	IDプロバイダによる行動把握	サービスとID連携を行う＝IDプロバイダが利用するサービスを把握できてしまう
		サービスへ渡す属性の管理	どの属性を提供するかはIDプロバイダがサービスとの間で決める
		サービス同士の結託による行動把握	提供属性がIDプロバイダに依存、場合によってサービス同士で結託すると行動把握が可能となってしまう
サービス事業者	利用者から提示された属性情報を信頼できること	属性自体の信頼性	IDプロバイダによる検証に依存（KYCをIDプロバイダに依拠）
		属性発行主体の信頼性	基本的に事前信頼でスケールしない

発行されたアイデンティティ自体の信頼

- Verifiable Credentials（VC）
  - 検証可能なアイデンティティ情報の表現
  - 発行者が行った身元確認情報（方法など）を含むことができる
  - 発行者によりデジタル署名される
  - 発行者のDID Documentに含まれる公開鍵を使って検証可能
  - https://www.w3.org/TR/vc-data-model/

提示されたID情報の信頼性の担保

- 物理世界におけるお財布モデル



公開鍵基盤の利用

- 物理世界におけるお財布モデル

課題①：誰が公開鍵基盤を運営するか？

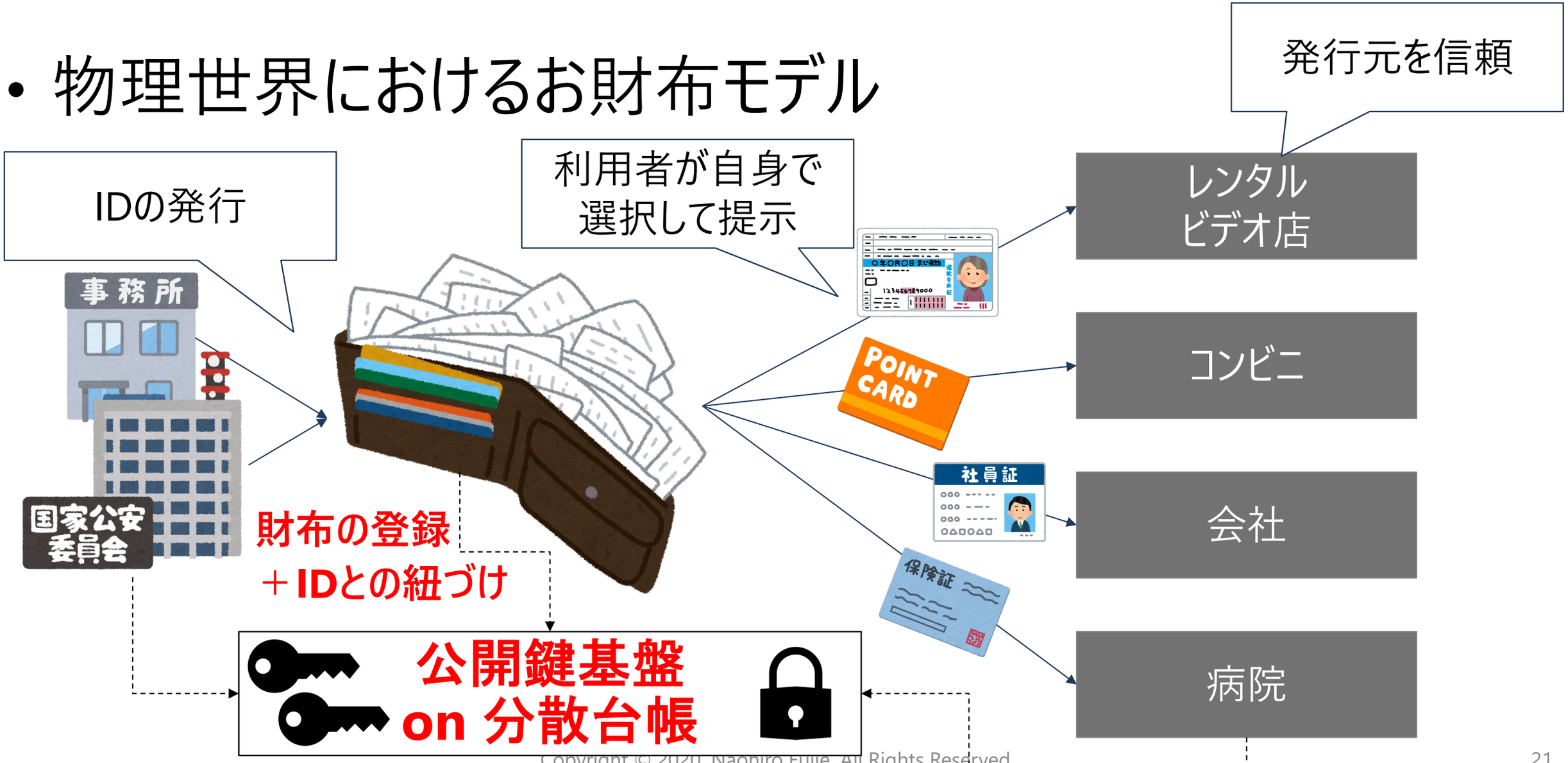
- 物理世界におけるお財布モデル

課題②：そこに悪意はないのか？

- 物理世界におけるお財布モデル

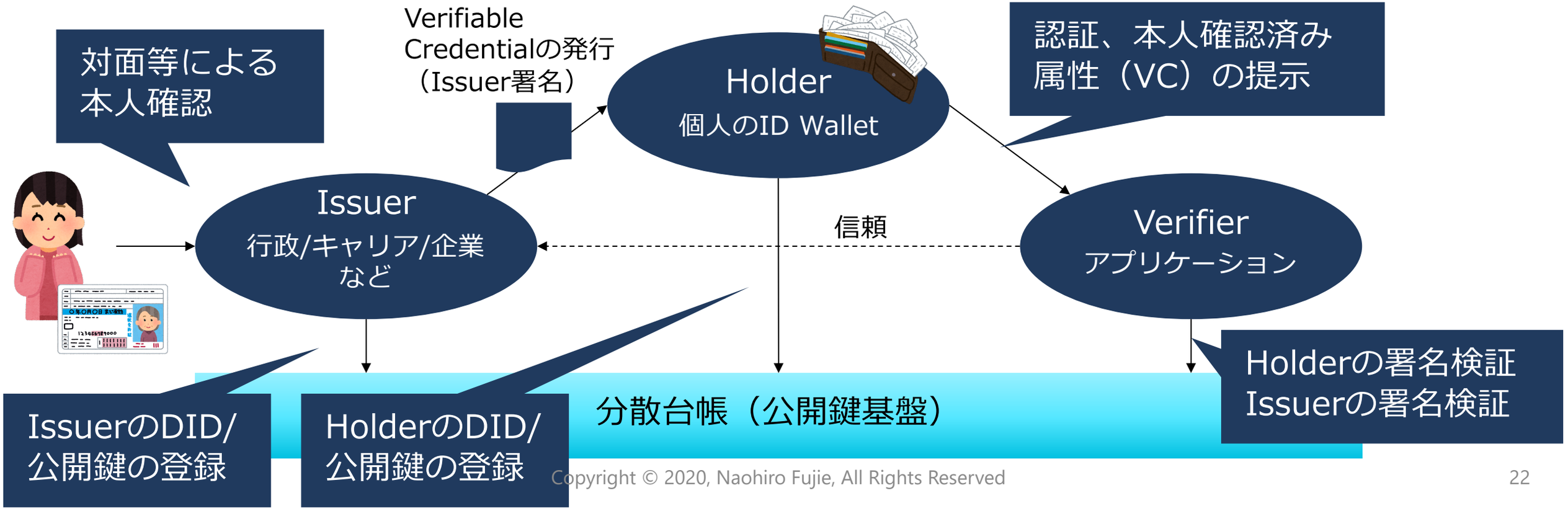
公開鍵基盤 on 分散台帳

- 物理世界におけるお財布モデル



Verifiable Credentialsの利用モデル

- IssuerからHolderに対して発行
- HolderがVerifierに対して提示
- Verifierは分散台帳上の公開鍵（DID Document）で真正性を検証



DID Document（上の公開鍵）の保管は
分散台帳（≒ブロックチェーン）
を適用できる分野の一つ
効果を出すにはパブリックチェーンが適している

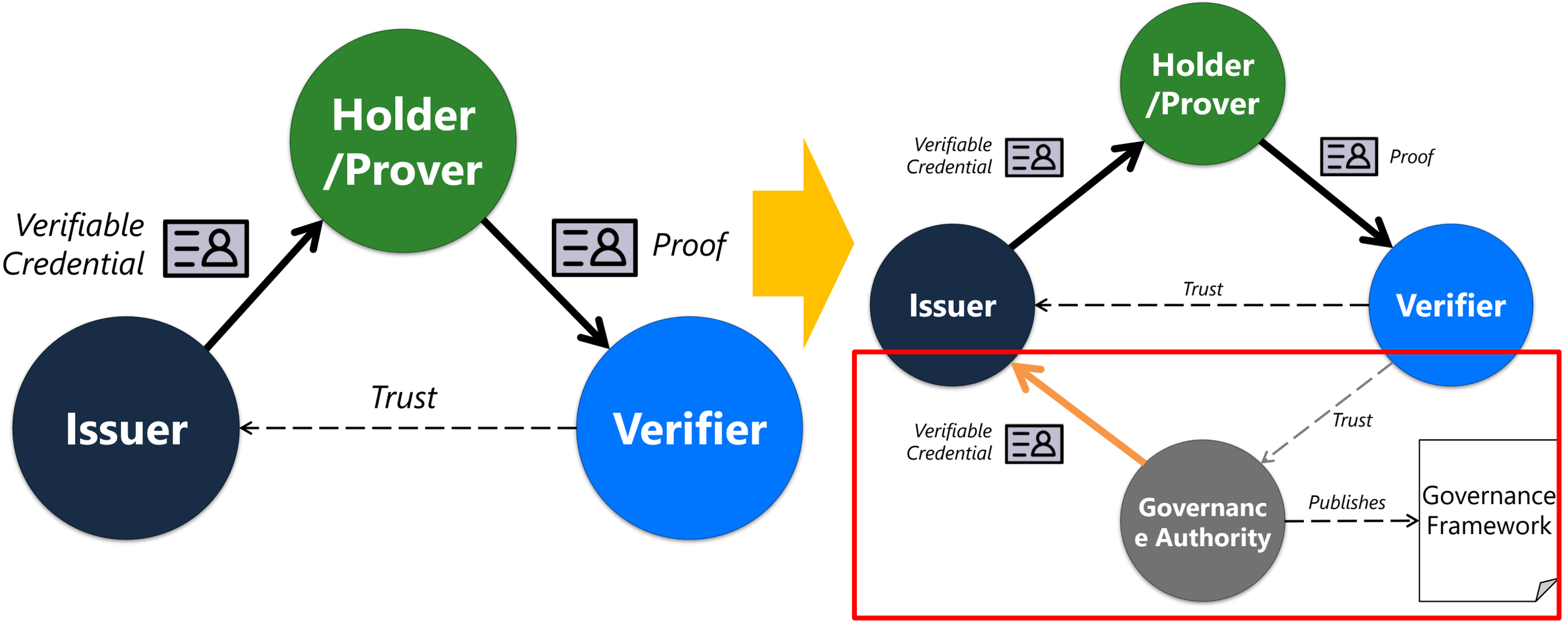
発行者の信頼

発行者（Issuer）のDIDの信頼性担保の方法

1. コンソーシアム型チェーンで発行されたDIDを使う
   - コンソーシアムに参加している組織しか発行できないDIDメソッドを利用
   - 前提：コンソーシアム参加には一定のガバナンスが効いていること
2. 既存ガバナンスの枠組みと紐づける
   - DNSとの紐付けが検討されている
   - DIF*のドラフト：Well Known DID Configuration
     - https://identity.foundation/.well-known/resources/did-configuration/
   - ドメイン取得のプロセスにおけるガバナンスに依拠

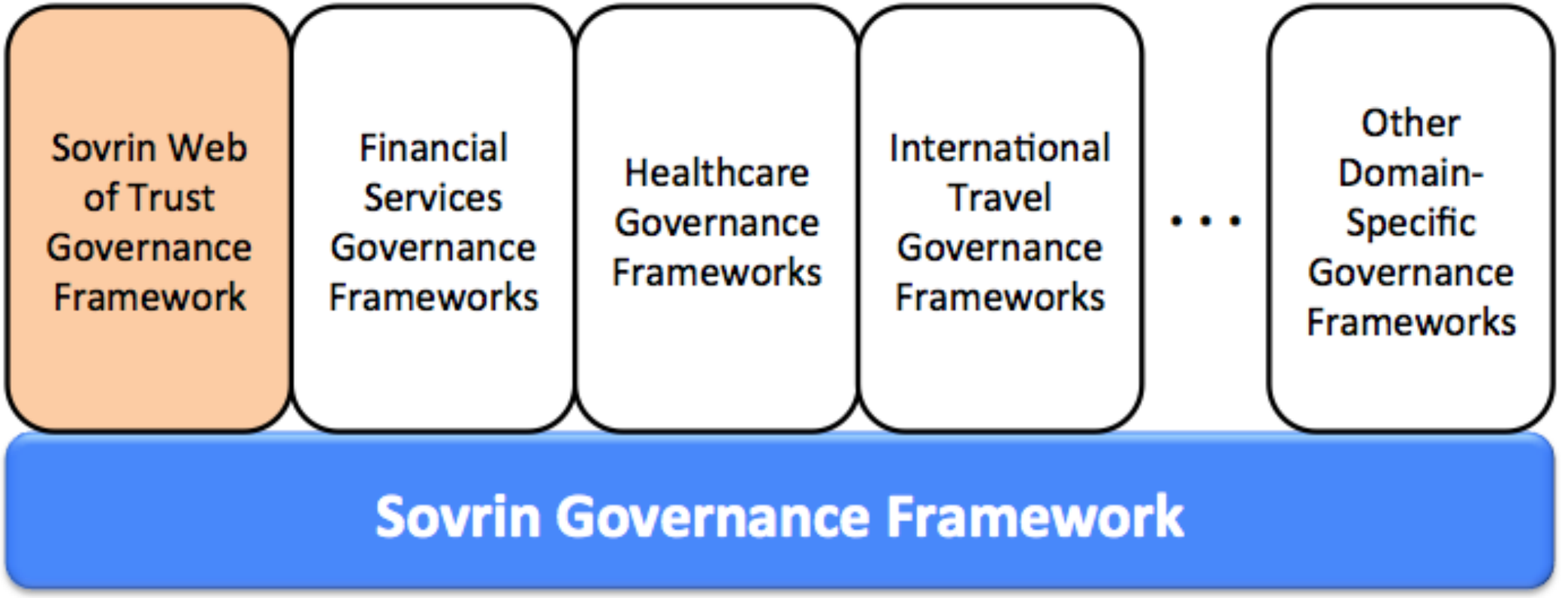
*DIF: Decentralized Identity Foundation

Sovrin Foundationのガバナンスモデル



Sovrin Governance Framework

業界毎のトラストフレームワーク運用を想定したモデル



出典）https://docs.google.com/document/d/1WqUOqdTBc3JACIlRviJoWJRcJHTNTNzk9_As9v-jwrY

発行者のDIDの発行に関するガバナンスは
分散台帳（≒ブロックチェーン）
を適用できる分野の一つ
効果を出すにはコンソーシアム型が適している
（もしくは別のガバナンスへの依拠が必要）

自己主権型アイデンティティモデルの普及のために

- 既存システムとの連携・相互運用
  - DID SIOP
  - OpenID Connect for Identity Assurance + VC
- 他の証明形式との相互運用
  - Blockcerts、OpenBadgeなど

DID SIOP

- SIOP（Self Issued OpenID Provider）
  - OpenID Connectで定義されている自己発行型のOpenID Provider
- DID SIOP
  - 従来OpenID Connectが達成してきたID連携と、DIDが持つ事業者からの独立性といった特徴を組み合わせる取り組み
  - OpenID Connectとの後方互換性を持つことで、アプリケーションへのID連携（サインアップ・サインイン）をスムーズに実行する
  - https://identity.foundation/did-siop/

OpenID Connect for Identity Assurance / VC

- OpenID Connect for Identity Assurance（OIDC4IDA）
  - OpenID Connectプロトコルに載せて検証済み属性情報をアプリケーションへ提供するための仕様
- VCとの共通点が多く連携できる可能性あり（と個人的に考えている）

	OIDC4IDA	VC
基本思想	発行者（IdP）中心	利用者中心
焦点	IdPにおけるアイデンティティ検証	RPにおけるアイデンティティ検証
提供するもの	検証済みのアイデンティティ情報	検証可能なアイデンティティ情報
信頼の根底	アプリケーションとIdPの間の事前信頼	分散台帳の改竄耐性

DIF/Presentation ExchangeとOpenID Connect

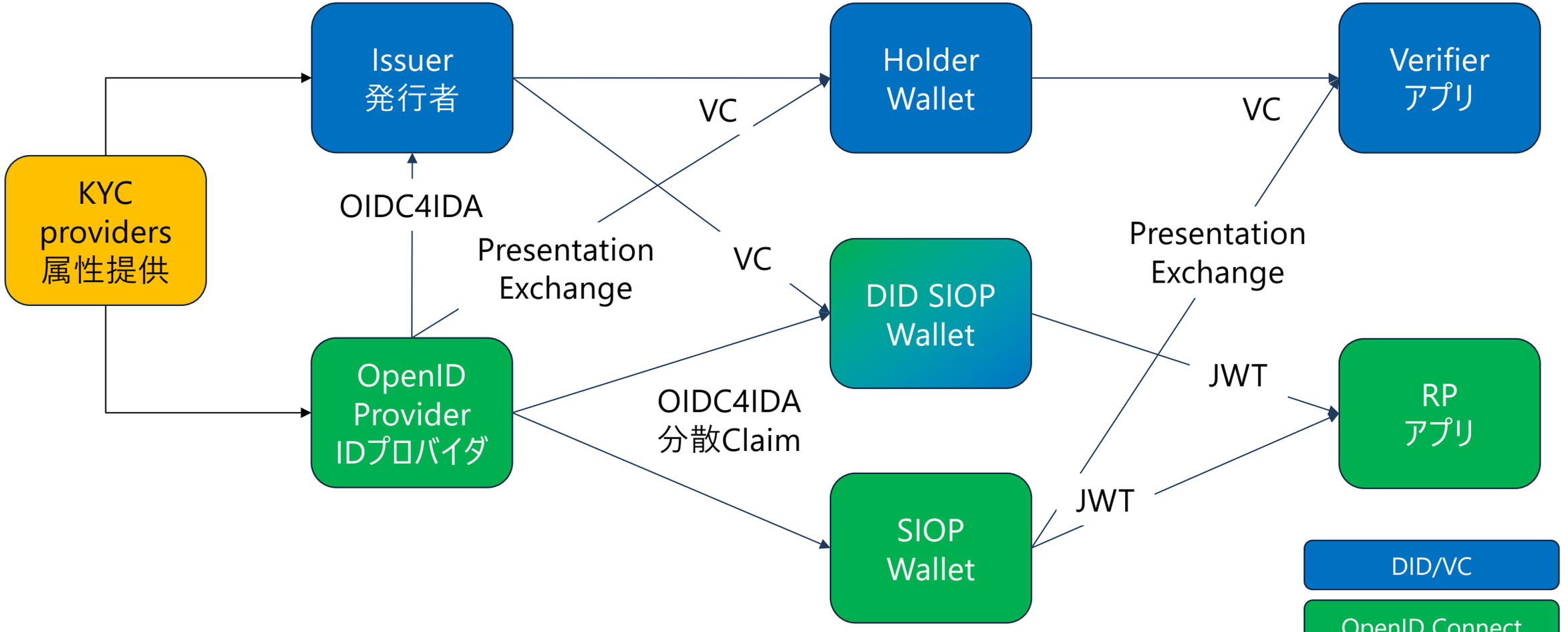
- VC発行のための仕様
  - Presentation Definition
  - Presentation Submission
- 以下とは切り離して策定
  - クレデンシャルフォーマット：JWT、VC、JWT-VCなど
  - トランスポート：OpenID Connect、DIDComm、CHAPIなど
- https://identity.foundation/presentation-exchange/

データフォーマットの互換性の議論

- 証明データを表現する取り組みは過去にも
  - 学位等：Blockcerts、OpenBadge
- Schema.org
  - JSON-LDのcontextにセットして、属性の読み替え・意味の統一を行う

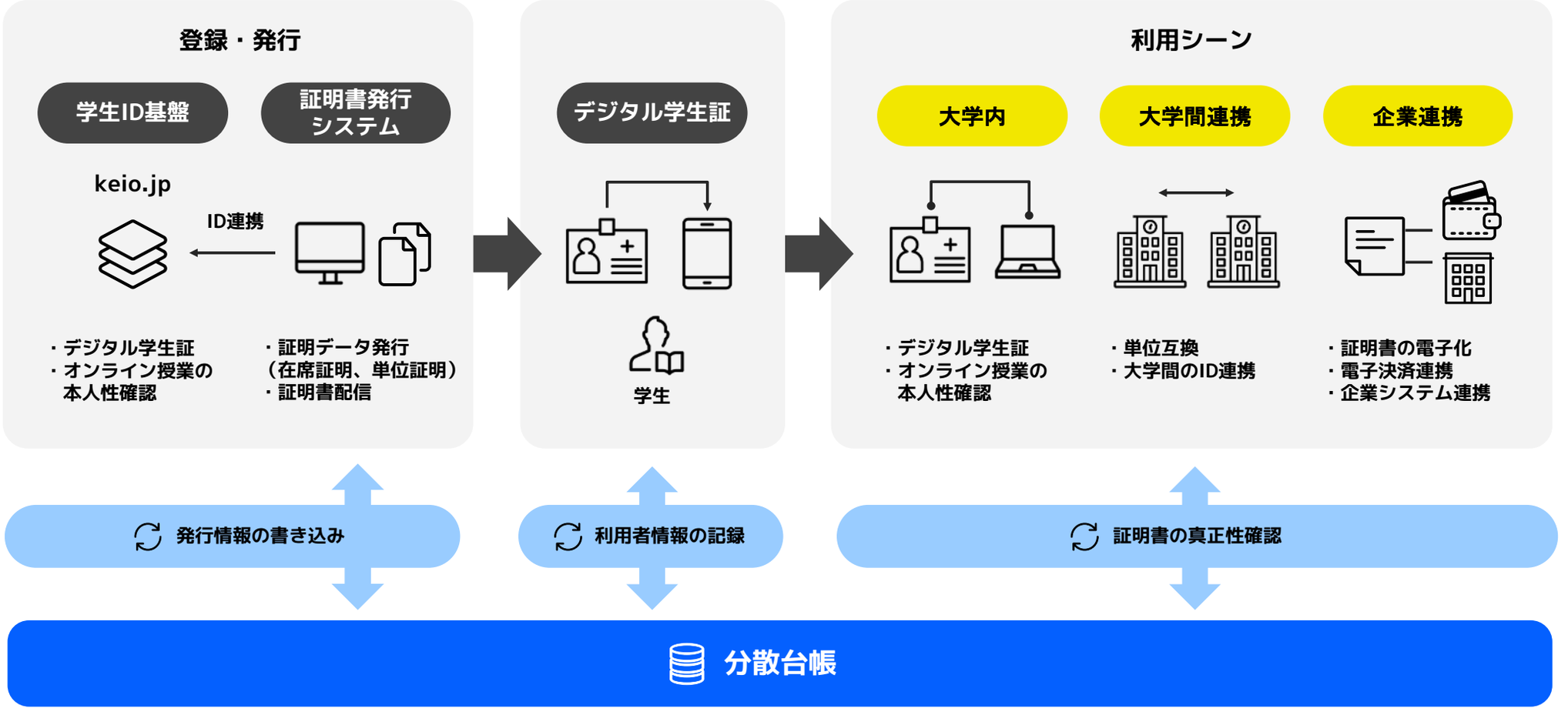
既存システムとの連携・相互運用

様々なケースを想定しつつ仕様策定が進んでいる状況



相互運用性とVCに関する実証実験（慶應義塾）

- 大学における各種証明をVCとして発行、大学内外のVerifierが検証を行う
- 各コンポーネント、証明書フォーマットの相互運用性を担保する取り組みを行う



まとめ

- アイデンティティ（Identity）≠識別子（Identifier）
- 自己主権型アイデンティティと分散台帳の関係性
  - 概念としては分散台帳（≒ブロックチェーンは関係ない）
  - 部分的に分散台帳が有効な部分も存在する
- 分散台帳の使い所
  - 利用者のDID：特定の組織に依存しないという意味でパブリックチェーンが有効
  - 発行者のDID：ガバナンスを効かせる意味でコンソーシアムチェーンが有効
  - VC：検証を継続的に行うためにパブリックチェーンが有効
- 既存技術やデータ形式を含めた相互運用性が普及の要