次世代 KYC と自己主権型アイデンティティの動向

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
富士榮　尚寛
@phr_eidentity

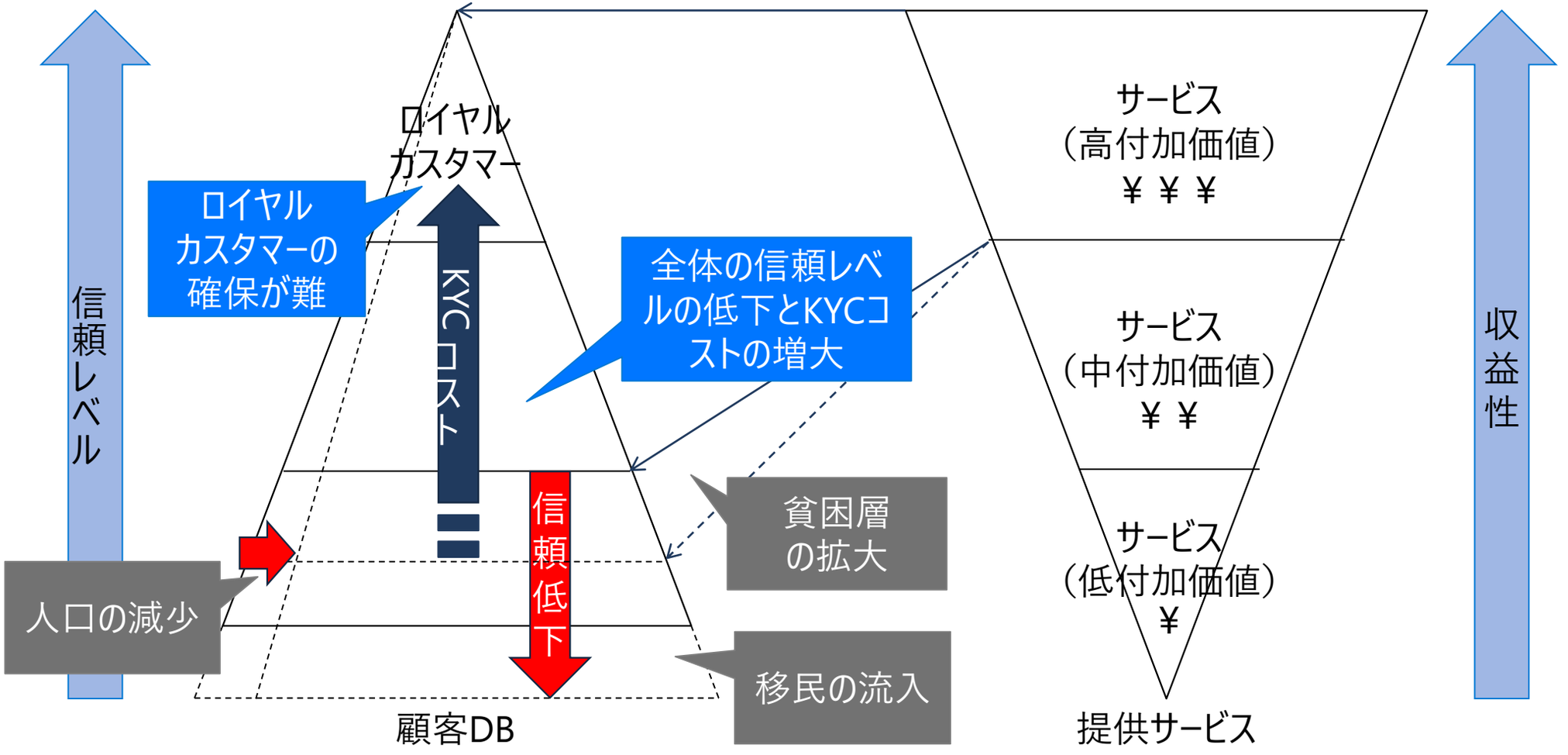
OpenID Japan

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
  - 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）

次世代KYCが求められる背景

人口減少、貧困層の増加、移民の流入など　⇒　顧客DBの維持が困難、KYCコストの増大



KYCとリスク・マネージメント

KYC：Know Your Customer

- **相手のことを調べる** → 回避
  - 返済能力の有無
  - もしもの時に連絡が取れるかどうか

- **担保を取る** → 転嫁
  - 抵当権、連帯保証人
- **利子を上げる** → 軽減
  - 逃げられても被害を減らす
- **保険に入る** → 軽減

色々なKYCの目的（例）

目的	金融	キャリア	ECサイト
金銭的被害の低減	融資の回収不能	契約後1か月間のタダでの利用 端末代金の回収不能	代金未収 配達不能（配送料・回収料）
犯罪利用の回避	マネーロンダリング テロ資金供与	飛ばし携帯としての利用	他人名義での商品横取り、転売
離脱リスクの回避	非活発ユーザの離脱兆候発見	非活発ユーザの離脱兆候発見	非活発ユーザの離脱兆候発見
顧客により良いサービスを提供する	他の商品の提案	割引プランの提案	商品のリコメンド

リスク・コンバージョン・プライバシーのジレンマ

- リスク回避を行うにはより**詳細・確実な情報収集**が必要

- 利用者は調べられすぎると逃げてしまい、コンバージョン率が下がってしまう
  - サービスを使い始めるまでのハードルが高すぎる
- 他の用途でも使えるのでついつい情報を集めすぎてしまう
  - リスク回避のはずが、マーケティングにも・・・

KYCは何しろ大変

- 事業者
  - 何しろ面倒
  - お金がかかる
- 利用者
  - なにしろ面倒
  - 離脱してしまう

金融機関では平均1.5億円/年、平均307名のKYC専門人材を採用

出典）https://www.thomsonreuters.com/en/press-releases/2017/october/thomson-reuters-2017-global-kyc-surveys-attest-to-even-greater-compliance-pain-points.html?teal_wdm=016ad5e0d248004dcbdaf508000003073003806b0086e

KYCの簡素化は事業者にとって死活問題となる

KYCの構成要素

- 本人確認
  - 取引相手が本人であることの確認
- デューデリジェンス
  - 取引相手と取引ができる相手かどうかの確認（与信、反社チェックなど）

KYCの過去～今～これから

構成要素	過去	今	これから
本人確認	事業者が個別に確認 例）免許証を各事業者に提示	かんたん本人確認（eKYC） 各事業者が電子的に書類を取り込むことでプロセスを短縮	他事業者の本人確認結果の利用（依拠、共有）
デューデリジェンス	各事業者が持つデータベースと個別にマッチング	同左	信用スコアの利用？

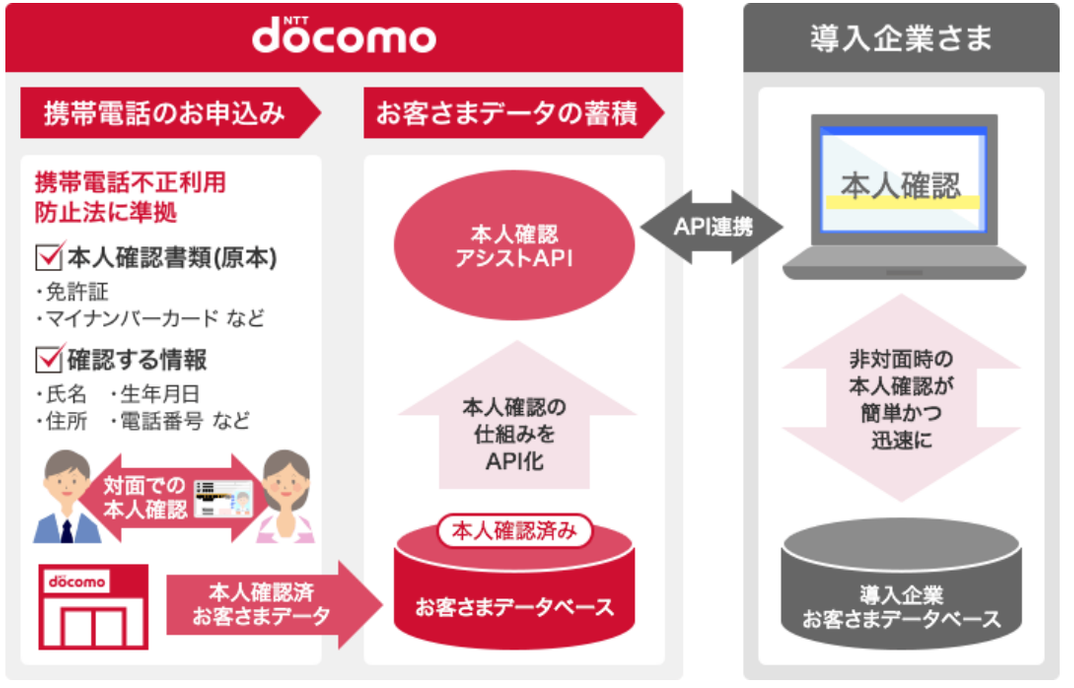
かんたん本人確認

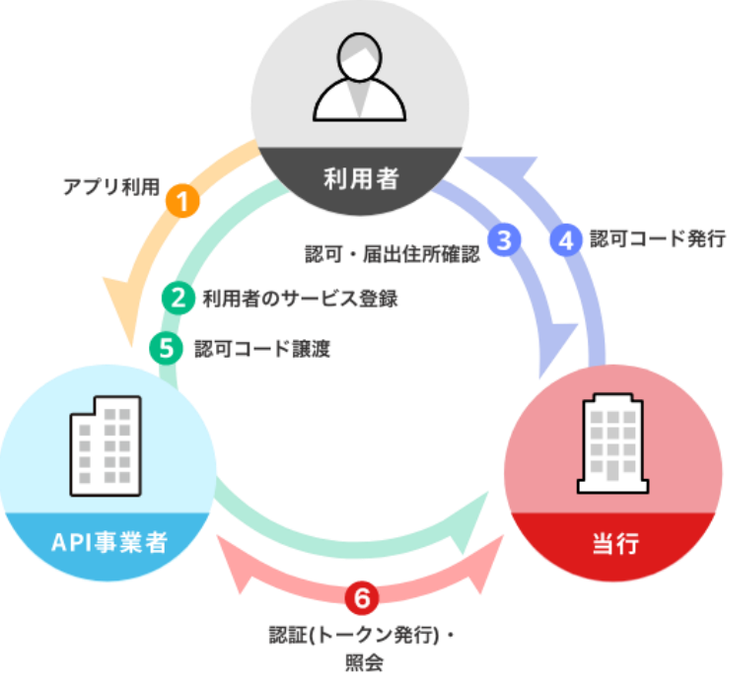
- LINE Pay、メルペイ

LINE Pay かんたん本人確認

本人確認済み情報の提供

- NTTドコモ／本人確認アシストAPI
- 三菱UFJ銀行／本人確認サポート(個人)APIサービス





信用スコア

- J.Score、Yahoo!スコア、LINEスコア

J.Score

YAHOO! JAPAN スコア

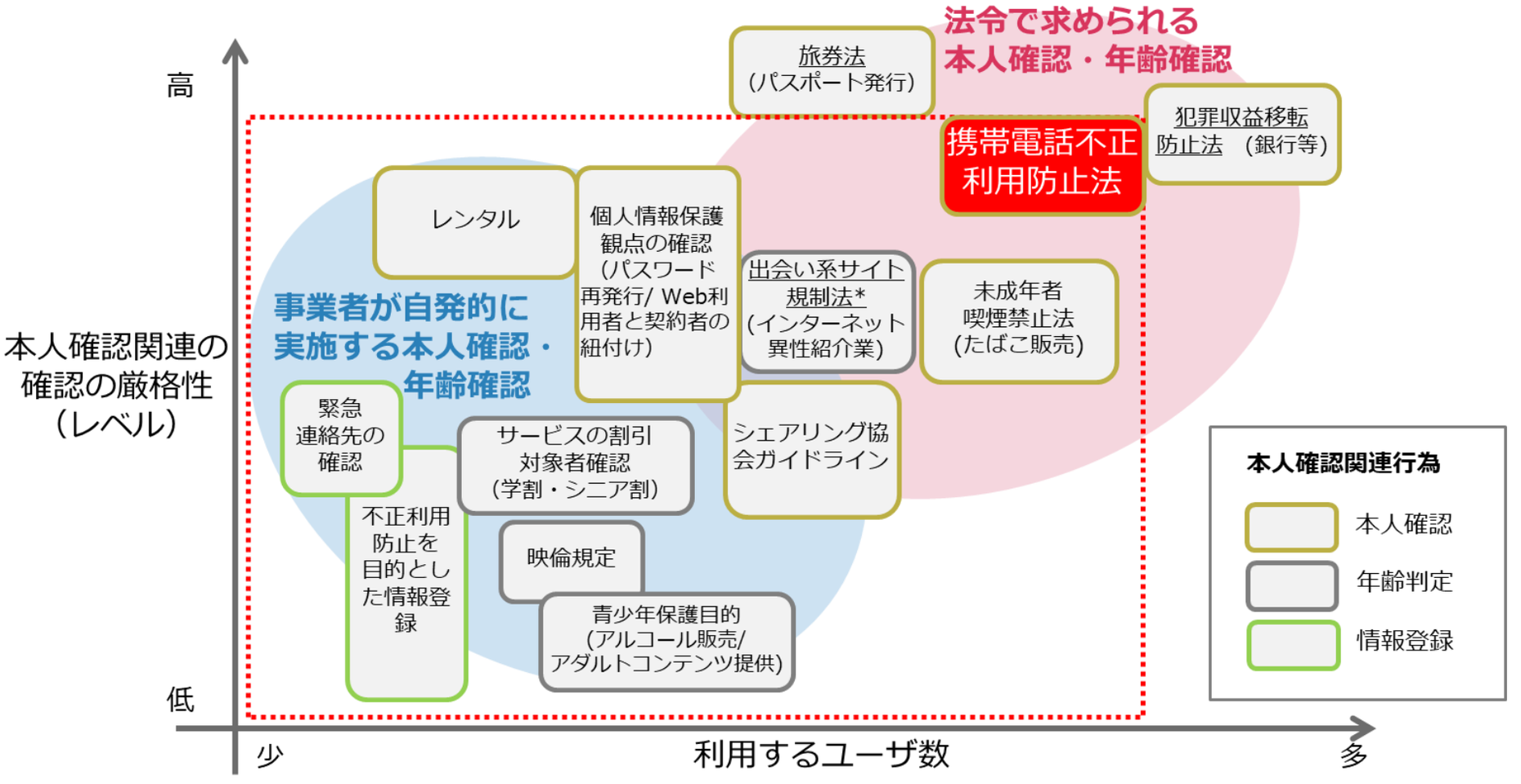
LINE Score

次世代のKYCを考える上での観点

- ポリシー、レギュレーション
  - 何を持って本人確認済み、デューデリジェンス済みとみなすか
  - 各法令の互換性
- テクノロジー
  - どうやって安全かつ確実に情報を伝達するか
- ビジネス
  - 依拠する側とされる側でのコスト構造の変化への対応

ポリシー、レギュレーション）法令の互換性

- 例）携帯電話不正利用防止法のカバー範囲



*本人確認支援API導入検討にあたっては両社で法的要件を確認する必要があります
*出会い系サイト規制法の正式名称は「インターネット異性紹介事業を利用して児童を誘引する行為の規制等に関する法律」です

出典）NTTドコモ様資料

テクノロジー）ID関連技術の応用による依拠

- みんなが毎回KYCを行うのは不毛
- 誰か信頼できる機関から確認済みの属性をもらいたい

KYC済み属性を持っているIdentity Provider（IdP）から情報をもらえないか？

アプローチ❶	フェデレーション、API連携による情報連携
アプローチ❷	自己主権型アイデンティティによる利用者による持ち運び

フェデレーション、API連携による依拠に向けた動き

- キャリア／銀行による本人確認済情報の提供
  - NTTドコモ：本人確認アシストAPI
  - 三菱UFJ銀行：本人確認サポート（個人）APIサービス

- KYC済み情報のID連携に向けた仕様策定
  - OpenID Foundation / OpenID Connect for Identity Assurance 1.0

フェデレーションの課題

- プライバシ（IdPによる行動把握。Facebook問題）
- IdPの信頼性/可用性

どうすればプライバシを保護と確実性を両立できるのか？

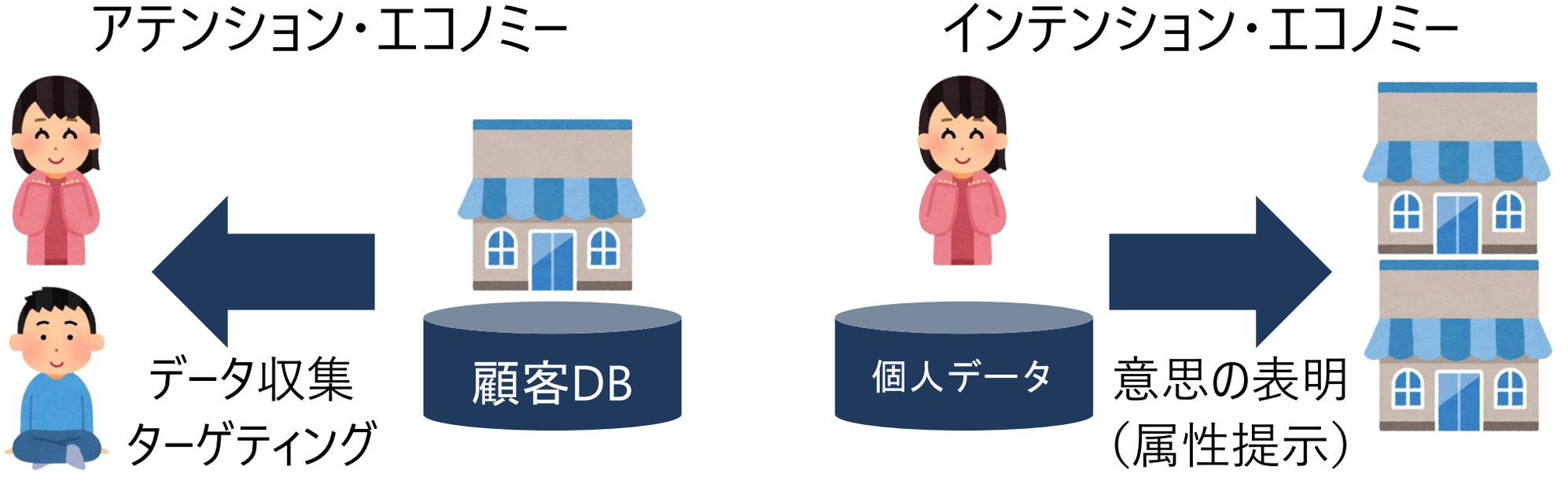
自己主権型アイデンティティ

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

- 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/
  - 抄訳：ふじえ

アテンション・エコノミーからインテンション・エコノミー

- アテンション・エコノミー：顧客の関心が中心の経済
- インテンション・エコノミー：顧客の意思が中心の経済

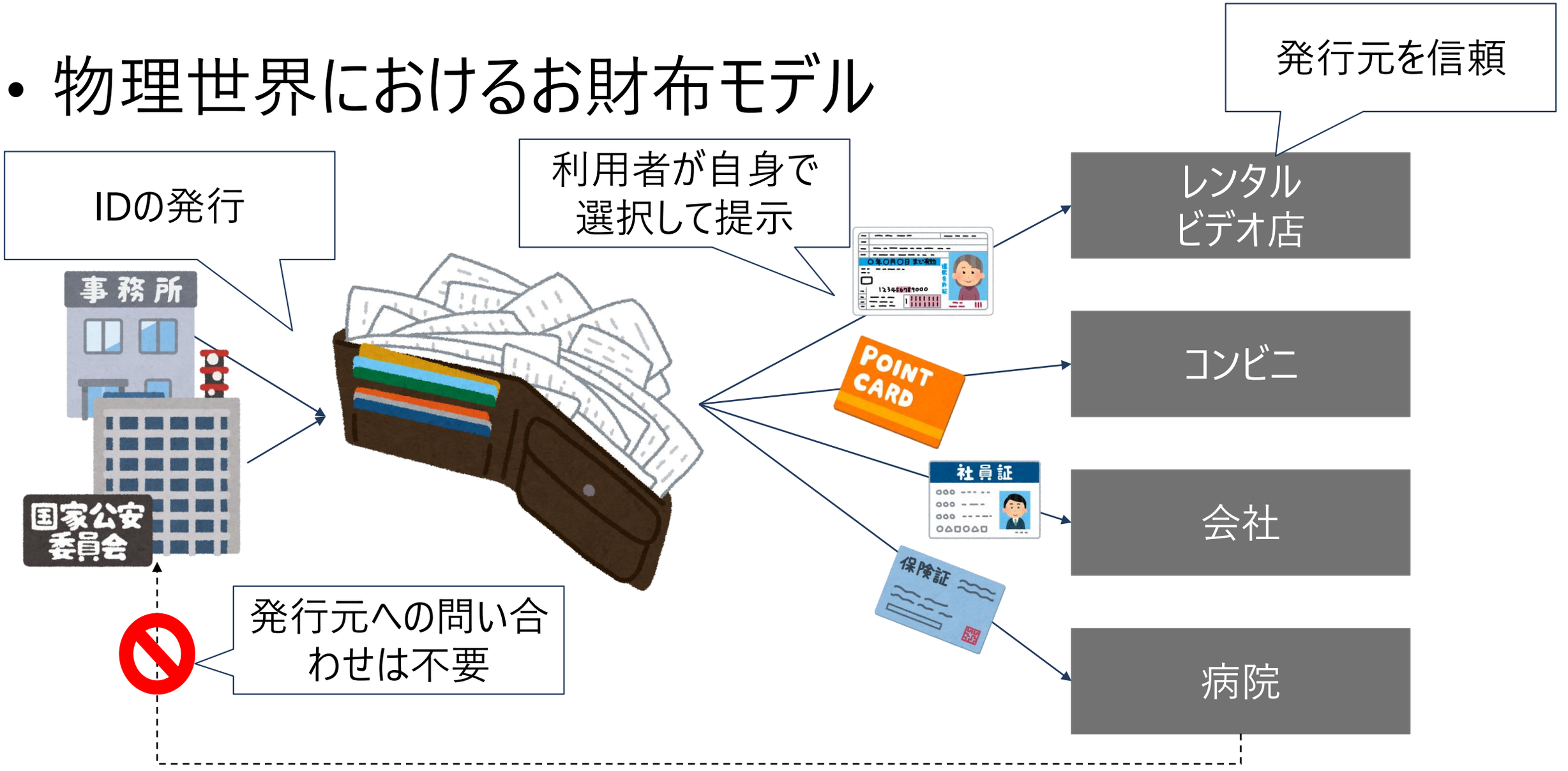


自身の意思に基づく属性情報の提示

参考）インテンション・エコノミー～顧客が支配する経済／Doc Seals

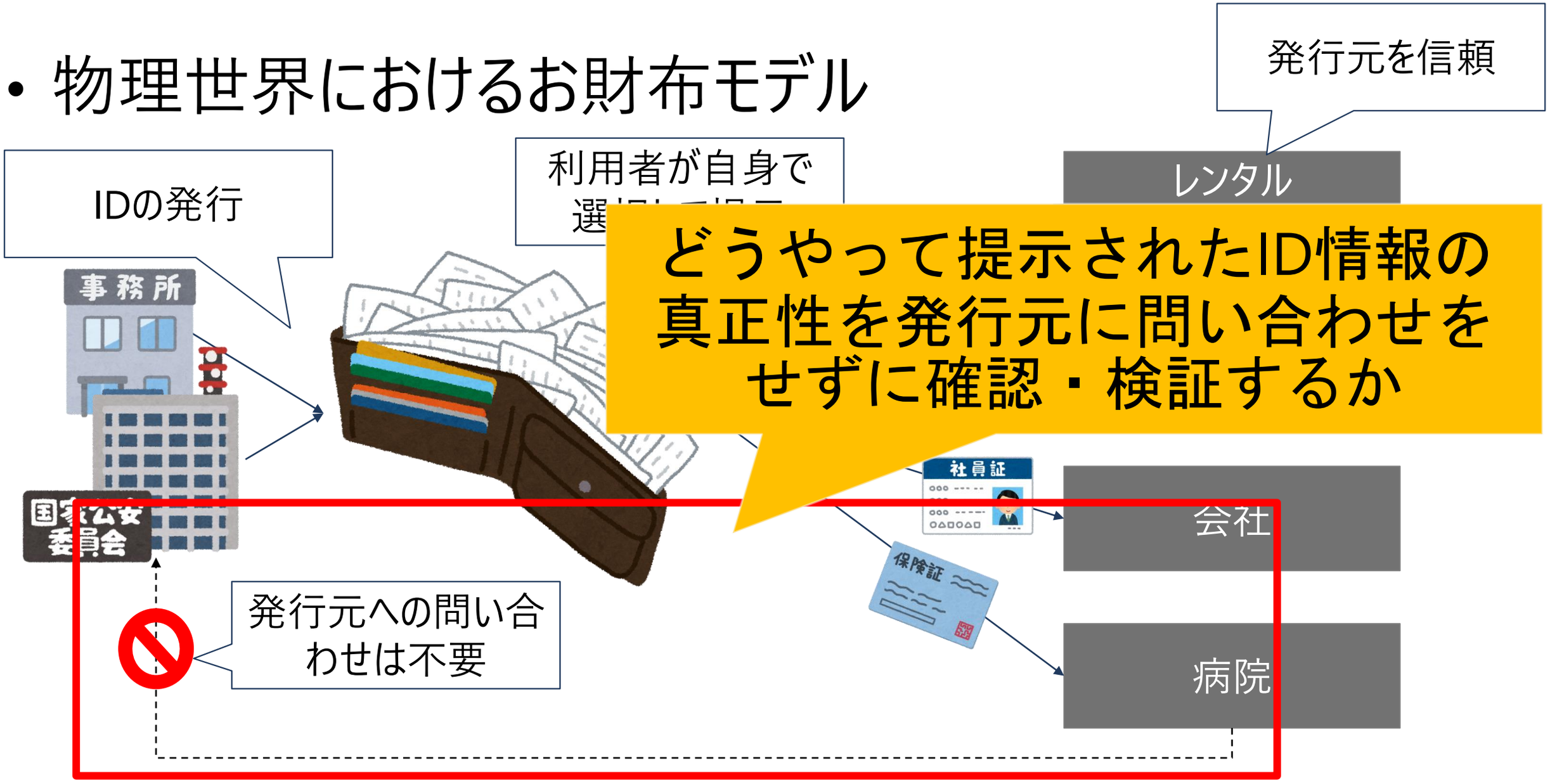
実現したいこと

- 物理世界におけるお財布モデル



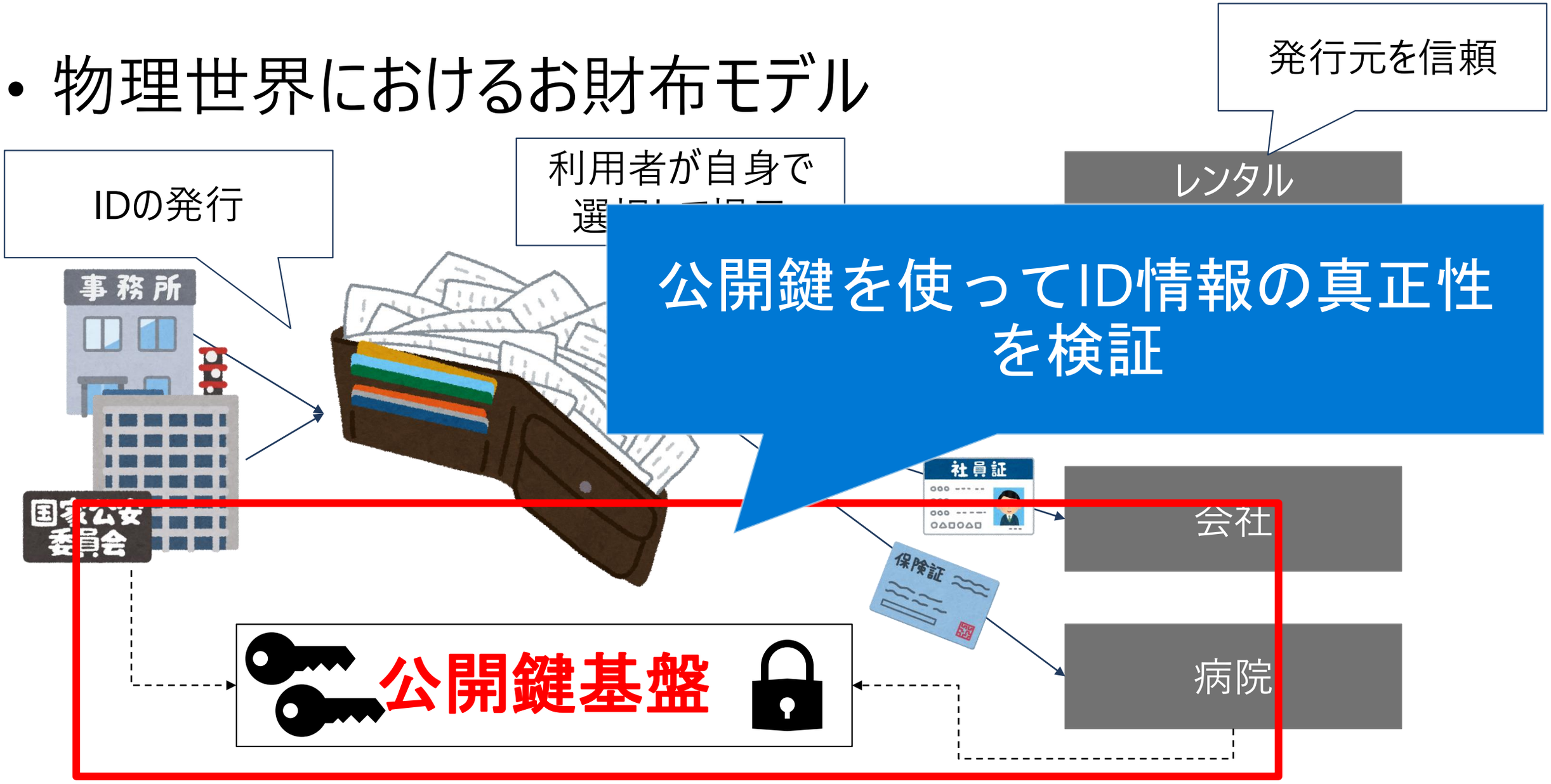
提示されたID情報の信頼性の担保

- 物理世界におけるお財布モデル



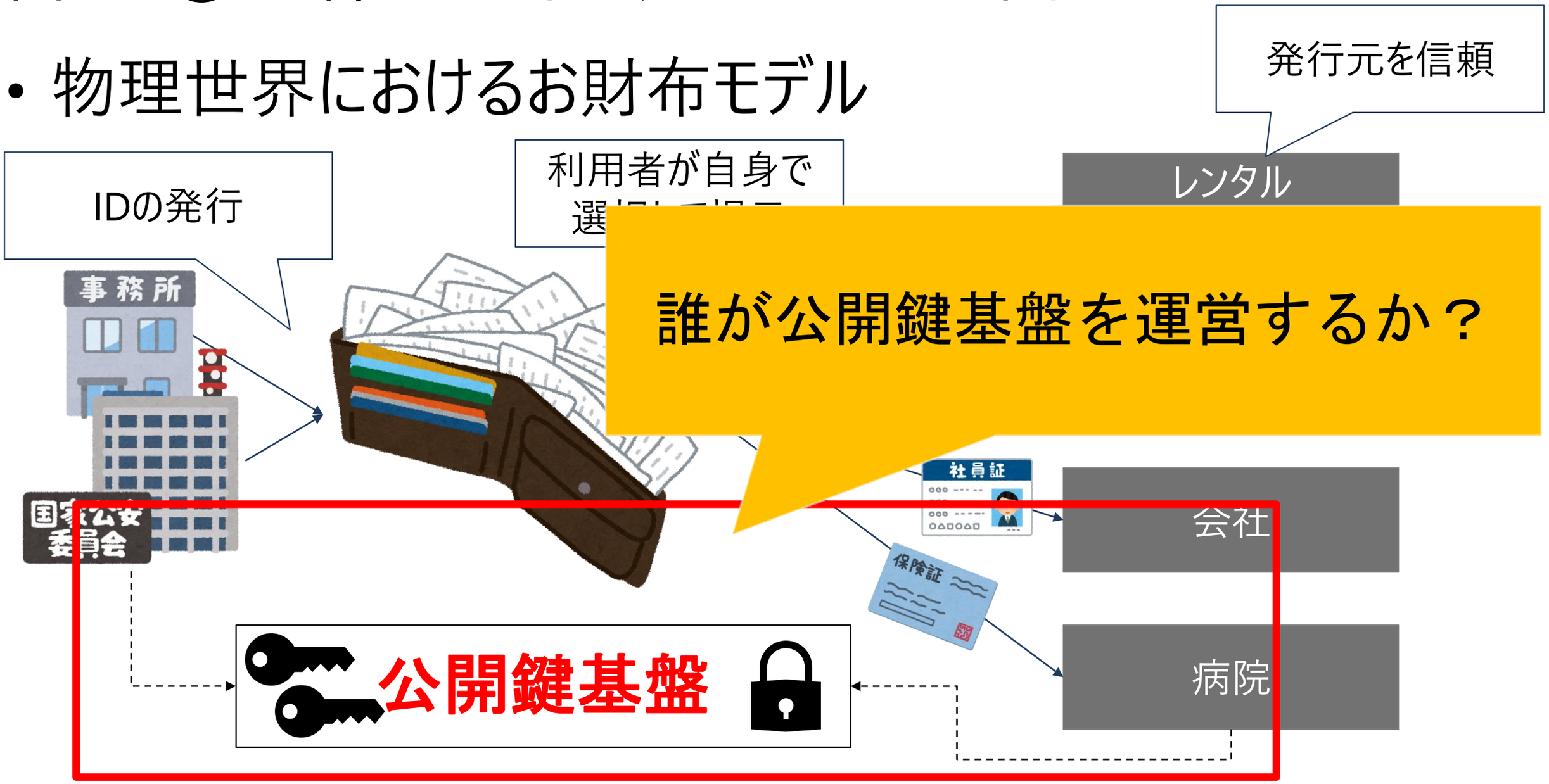
公開鍵基盤の利用

- 物理世界におけるお財布モデル



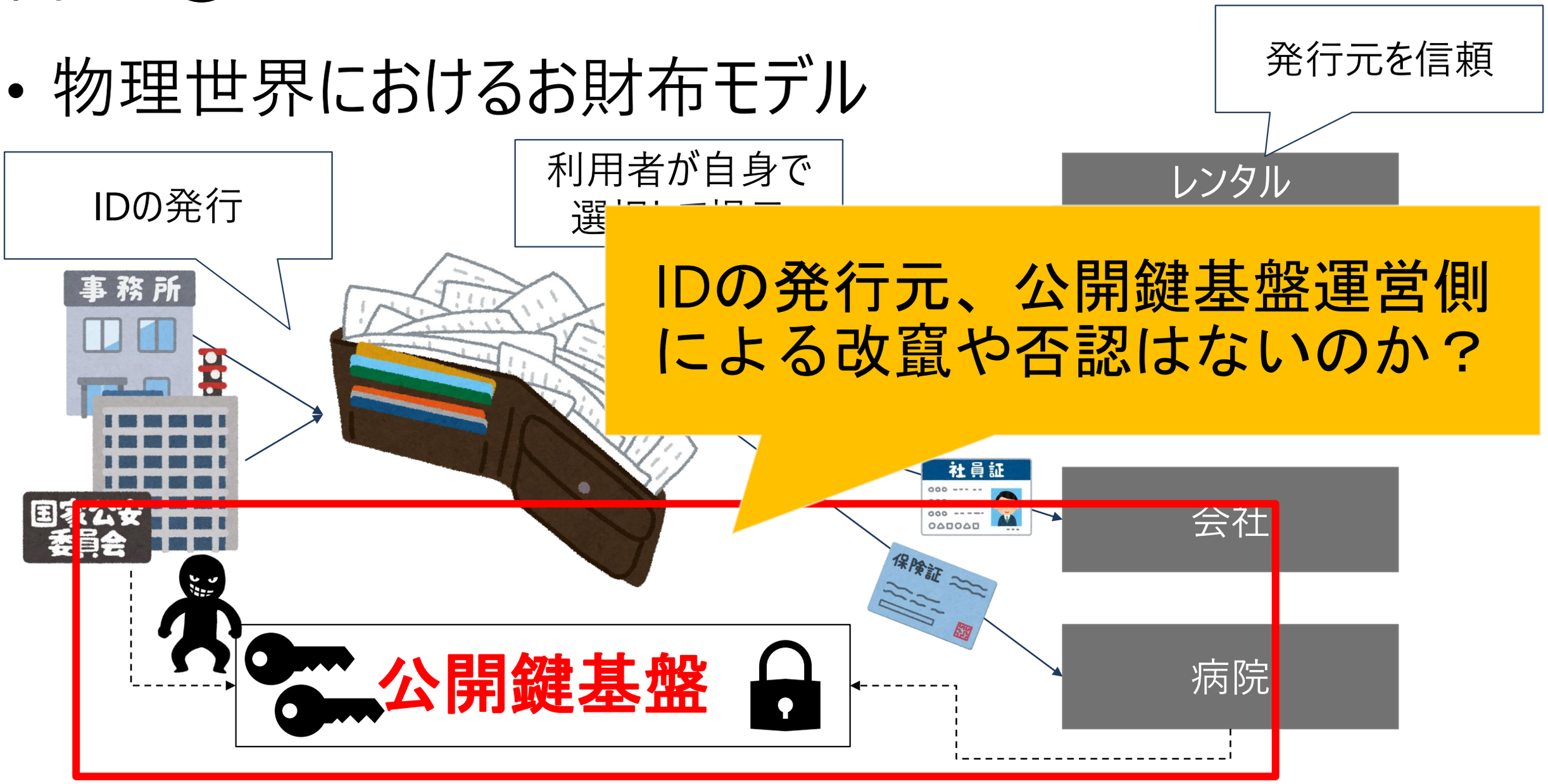
課題①：誰が公開鍵基盤を運営するか？

- 物理世界におけるお財布モデル



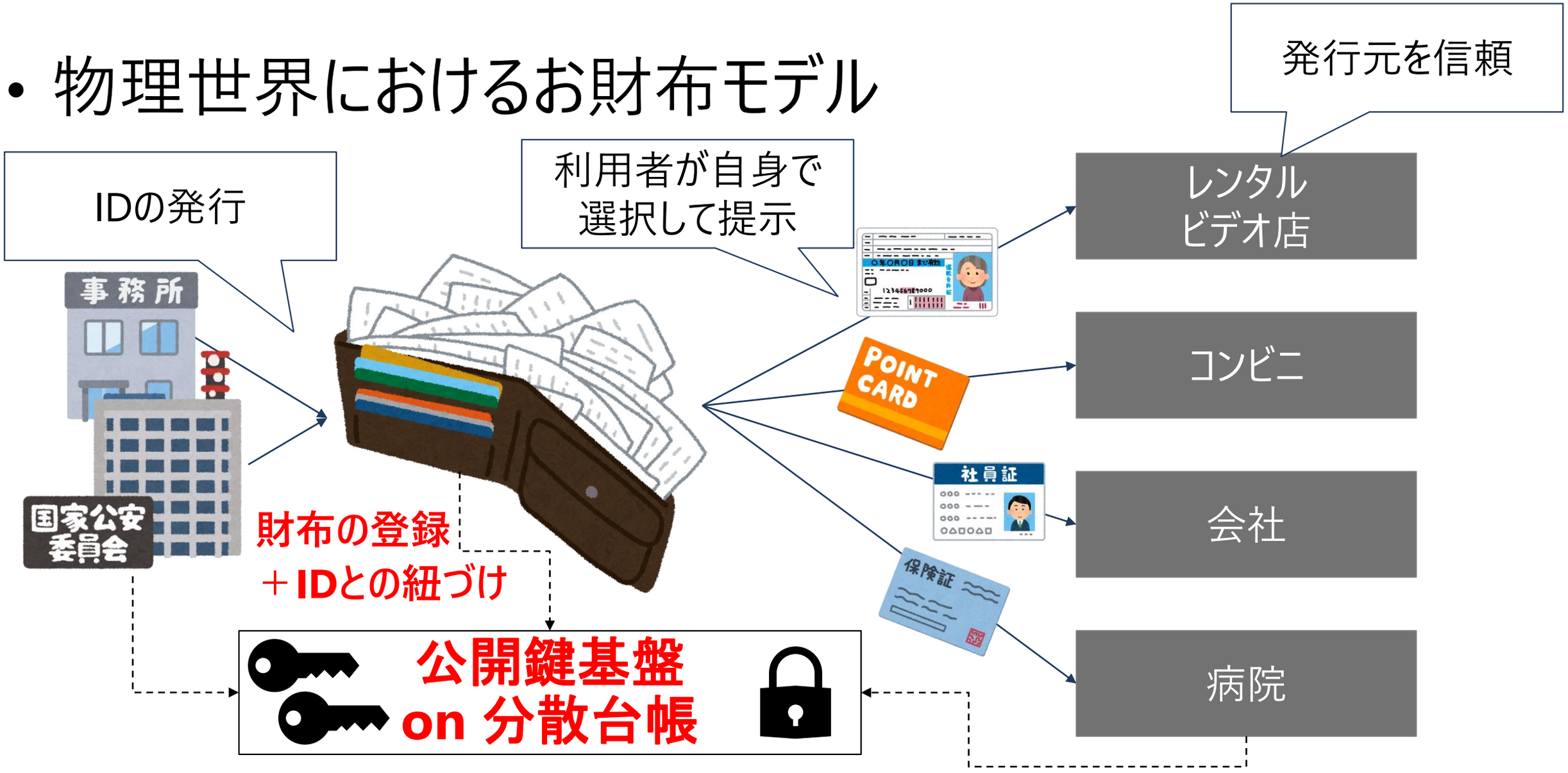
課題②：そこに悪意はないのか？

- 物理世界におけるお財布モデル



分散台帳の利用

- 物理世界におけるお財布モデル



分散台帳

- 特徴：「共有かつ不変」
  - 利害の一致するとは限らない複数の主体により運営される
  - 一度書き込むと改変が困難

- ブロックチェーンが必須とは言っていないが有力な選択肢

ブロックチェーンが活きるシーンとは？

If you need a blockchain, it is for a very specific need. **That need is to share a database of records with people you do not trust.** The records need access and updating by everyone, and yet you do not trust any of them and so the network manages that trust. Sweet and simple. If you do not need to share a database or if you trust the people accessing the database, you do not need a blockchain. We've known this for a long time.

https://thefinanser.com/2019/03/blockchain-dead-long-live-blockchain-2.html

「信頼できない人とデータを共有しないといけない場合の記録場所」

嘘つきがいない所で使っても仕方がない

IDにおける“嘘つき”

- 個人による詐称　⇒　個人的な利益
  - 経歴詐称
  - 身元詐称
  - 年齢詐称
- 組織による不正や否認　⇒　制度の不備や紛争等
  - 難民等、存在の否認（存在しなかったことにされる）
  - 無国籍（出生届が受け付けられない）

こうしてみると相性は悪くなさそう

公開鍵基盤における課題への対応

- 誰が公開鍵基盤を運営するのか
  - グローバル、インターネット・スケールでの可用性
- 改竄や否認への対応は？
  - ID発行元の消失、関連主体による改竄、否認

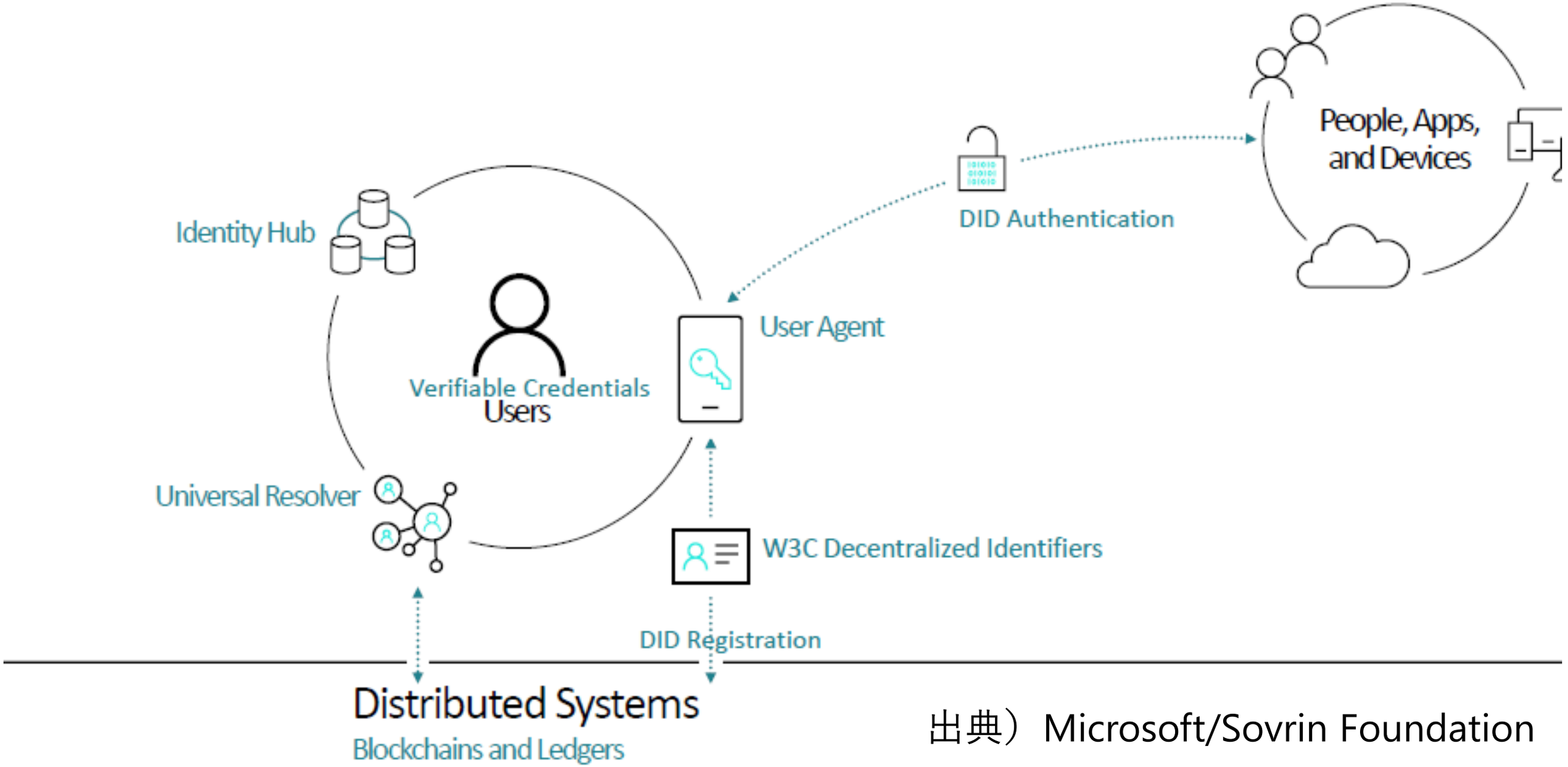
⇒分散台帳（≒ブロックチェーン）の活用

「Decentralized Identity」（非中央集権型アイデンティティ）

分散ノードによる可用性、耐改竄性の担保

利用者の財布とID情報との紐づけ自体を台帳上への記録

Decentralized Identity Building Blocks

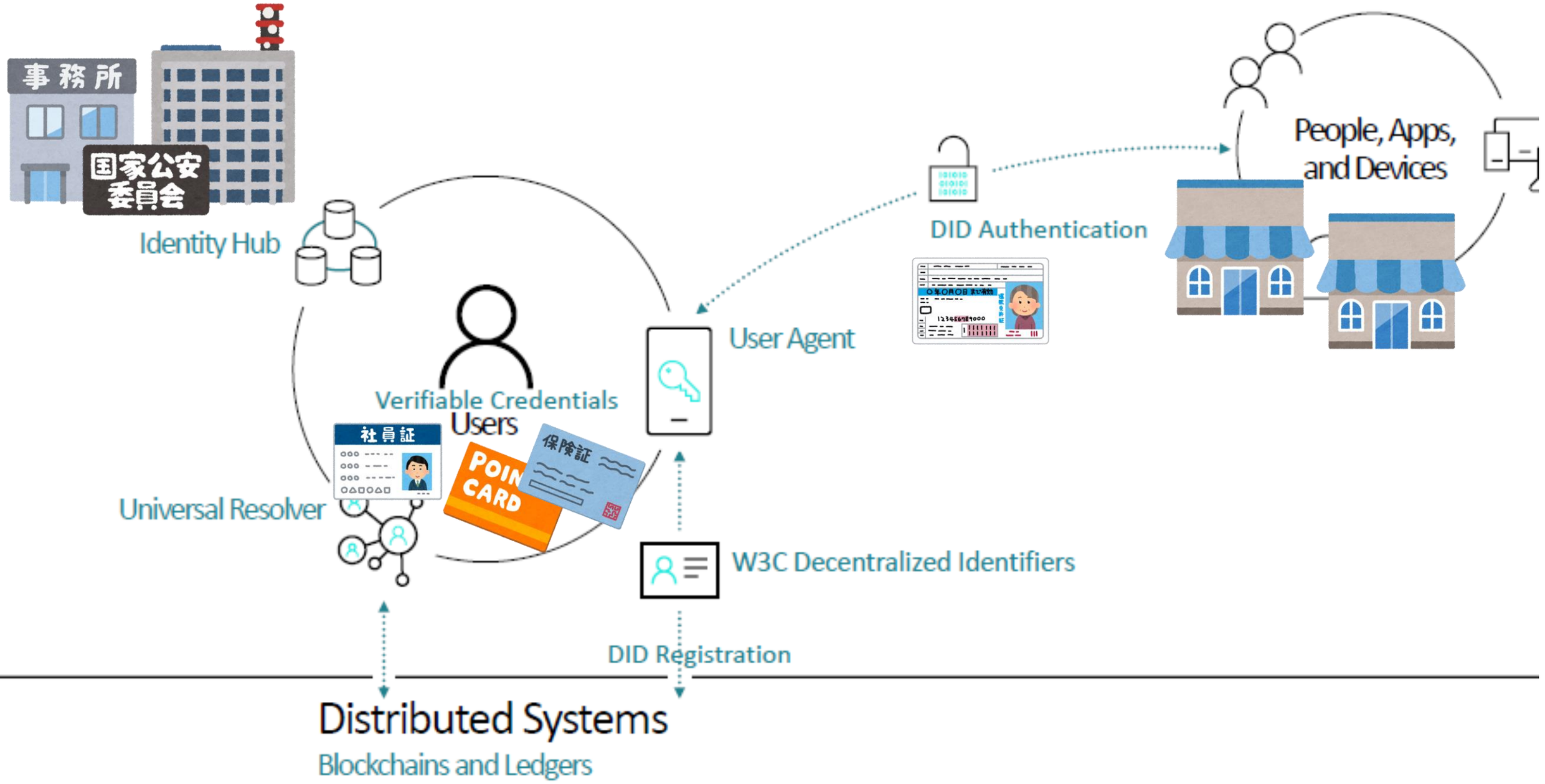


出典）Microsoft/Sovrin Foundation

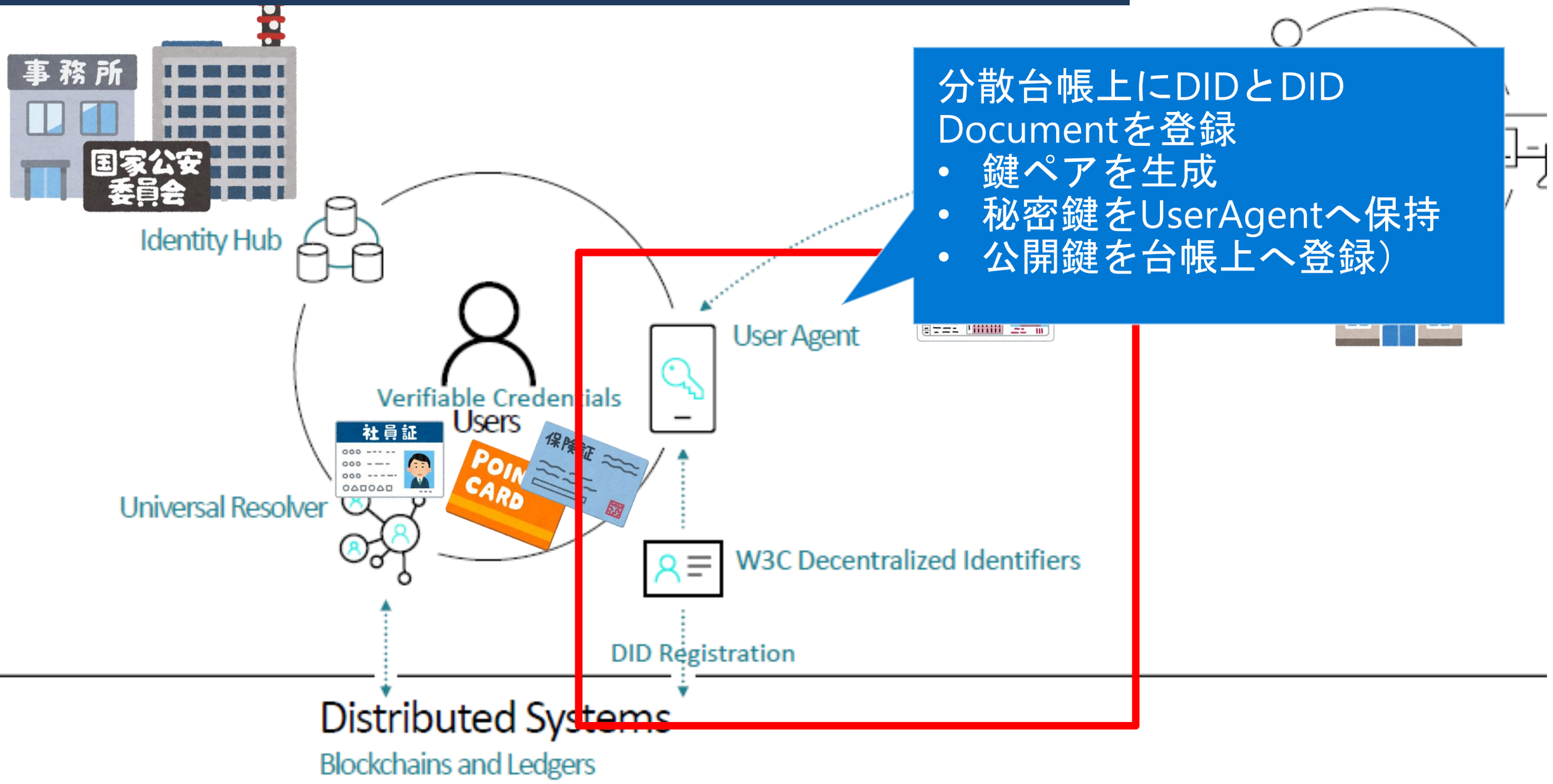
構成要素

コンポーネント	概要
User Agent	いわゆるIdentity Wallet。スマホアプリやブラウザExtensionとして実装される。鍵ペアの生成とDID（Decentralized Identifier／識別子）の登録、DID Authにおける認証器の役割を果たす
Identity Hub	DIDに関連するIdentity情報を保存する
Distributed Ledger	DIDとDID Documentを記録する分散台帳（ブロックチェーンなど。ブロックチェーンが必須なわけではない）
Universal Resolver	他の台帳上にあるDID Documentを解決する（複数の系の分散台帳で運営される前提）
Verifiable Credentials	第3者から発行された検証可能なアイデンティティ情報（を表すデータ構造の標準）

Decentralized Identity Building Blocks



Step1 : DID Registration



分散台帳上にDIDとDID Documentを登録
- 鍵ペアを生成
- 秘密鍵をUserAgentへ保持
- 公開鍵を台帳上へ登録）

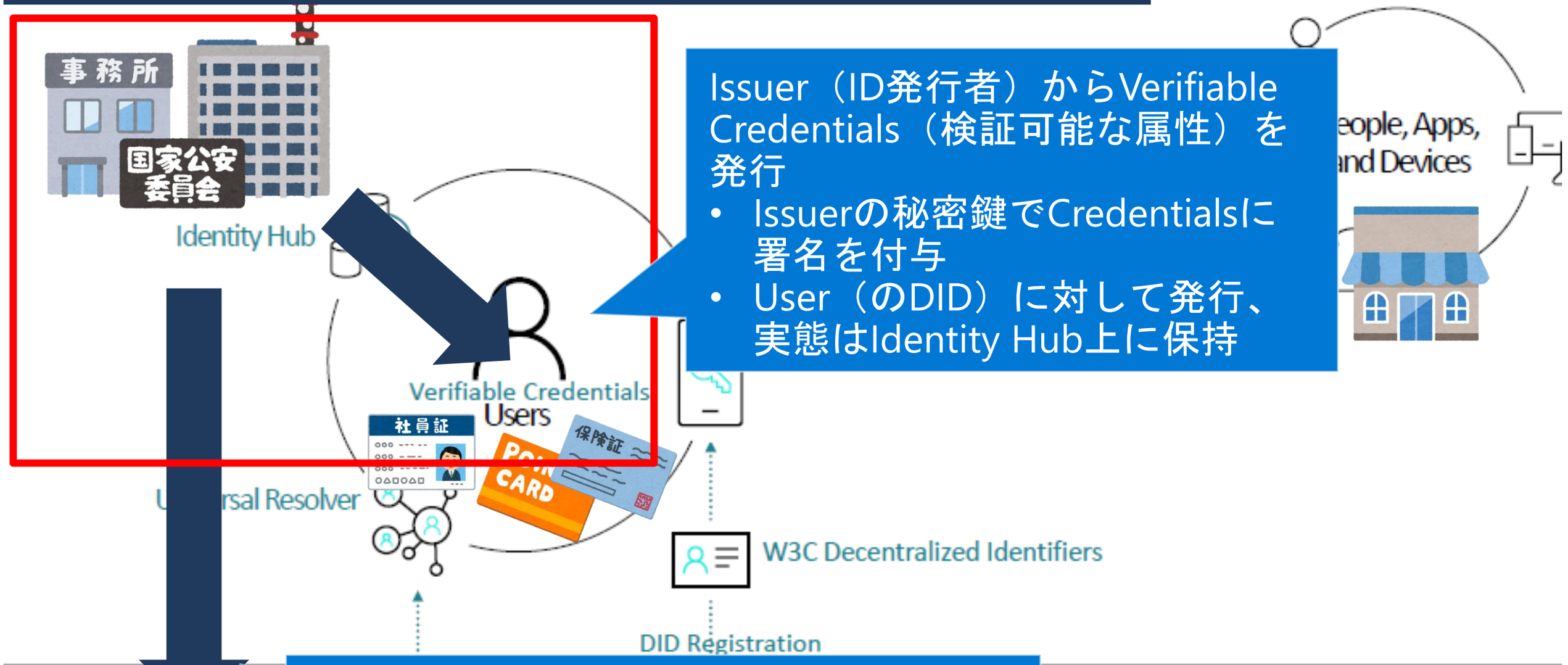
DID Documentのサンプル

```
{ "@context": "https://w3id.org/did/v1",
  "id": "did:example:123456789abcdefghi",
  "publicKey": [{
    "id": "did:example:123456789abcdefghi#keys-1",
    "type": "RsaVerificationKey2018",
    "controller": "did:example:123456789abcdefghi",
    "publicKeyPem": "-----BEGIN PUBLIC KEY...
                    END PUBLIC KEY-----¥r¥n"}],
  "authentication": [
    "did:example:123456789abcdefghi#keys-1"],
  "service": [{
    "type": "OpenIdConnectVersion1.0Service",
    "serviceEndpoint":"https://hoge.example.jp/"}]}
```

識別子
Decentralized Identifier

公開鍵に関する情報

Step2：Verifiable Credentialsの発行



Issuer（ID発行者）からVerifiable Credentials（検証可能な属性）を発行

- Issuerの秘密鍵でCredentialsに署名を付与
- User（のDID）に対して発行、実態はIdentity Hub上に保持

Issuer自体もDIDを持ち、DID Document（公開鍵等）を台帳上に公開

Verifiable Credentialsのサンプル

```
{ "@context": ["https://www.w3.org/2018/credentials/v1"],
  "id": "http://example.edu/credentials/1872",
  "type": ["VerifiableCredential", "AlumniC                ],
  "issuer": "https://example.edu/issuers/565049",
  "issuanceDate": "2019-05-30T14:50:00Z",
  "credentialSubject": {
    "id": "did:example:ebfeb1f712ebc6f1c276e12ec21",
    "alumniOf":"<span lang='en'>Example University</span>"},
  "proof": {
    "type": "RsaSignature2018",
    "created": "2019-05-30T14:50:00Z“,
    …}
}
```

Credentialsの識別子

発行者の識別子

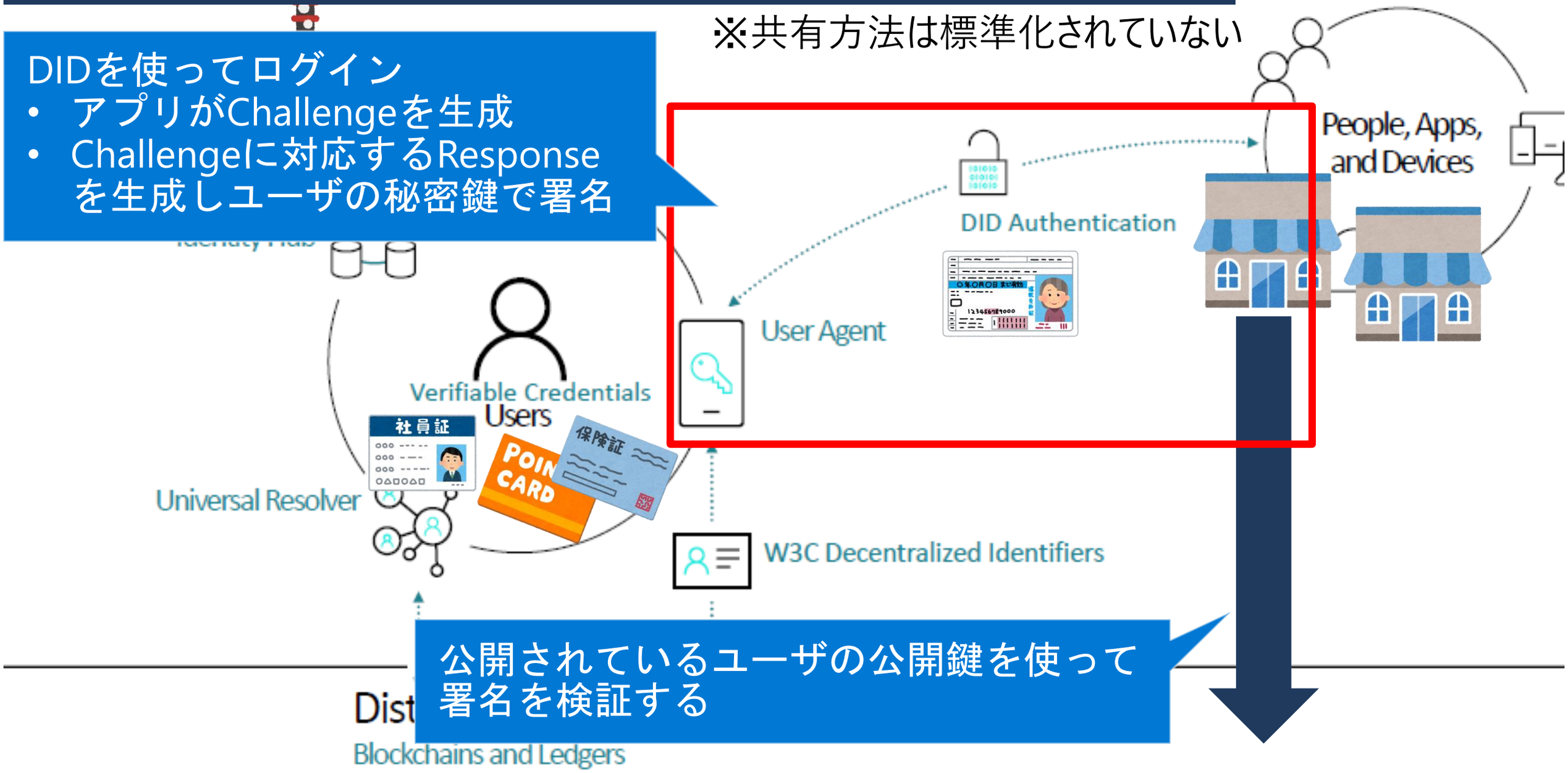
発行先の識別子（DID）

Credentialsの内容

Step3：DID Auth（ユーザ認証）～Credentials共有

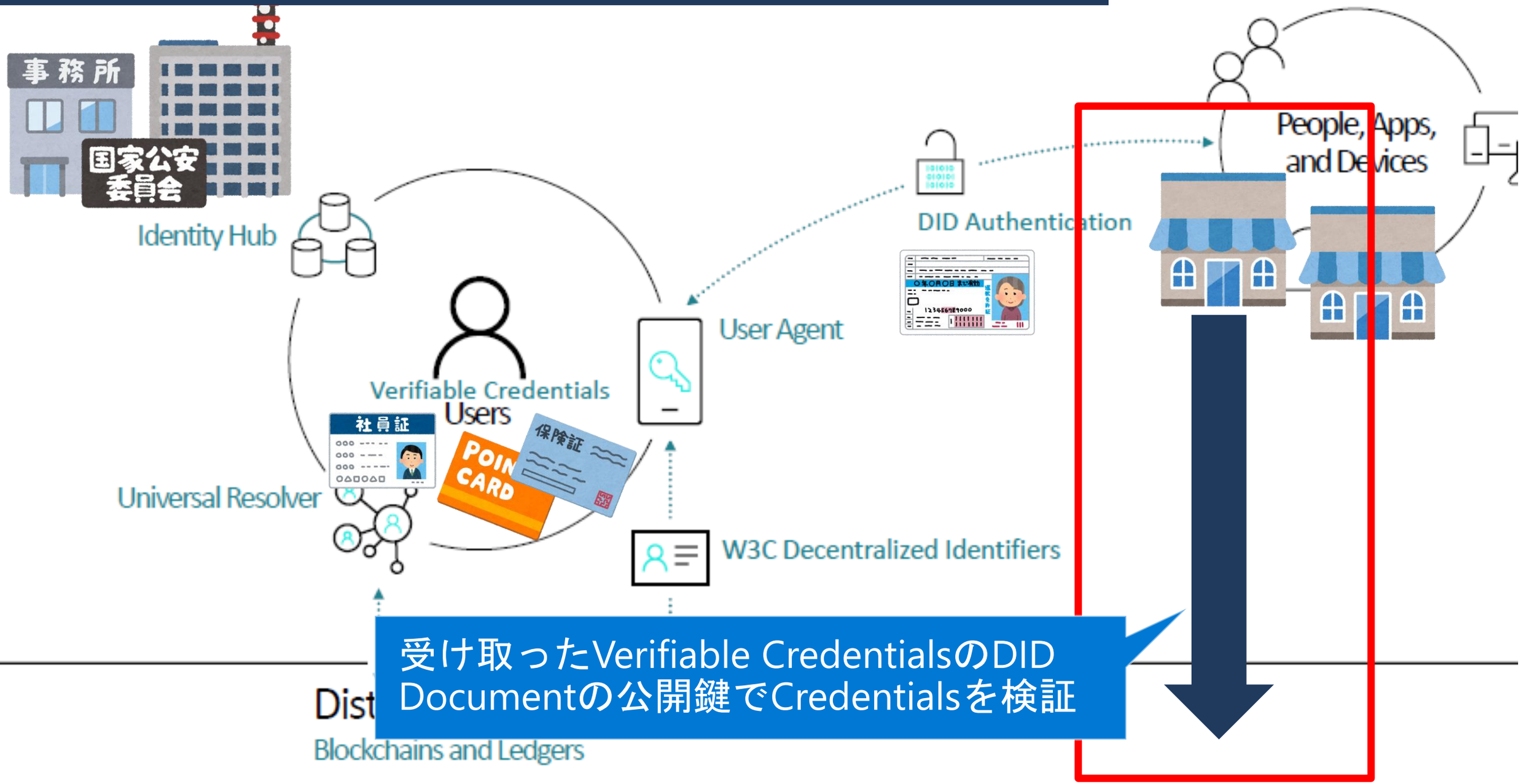
※共有方法は標準化されていない

DIDを使ってログイン
- アプリがChallengeを生成
- Challengeに対応するResponseを生成しユーザの秘密鍵で署名

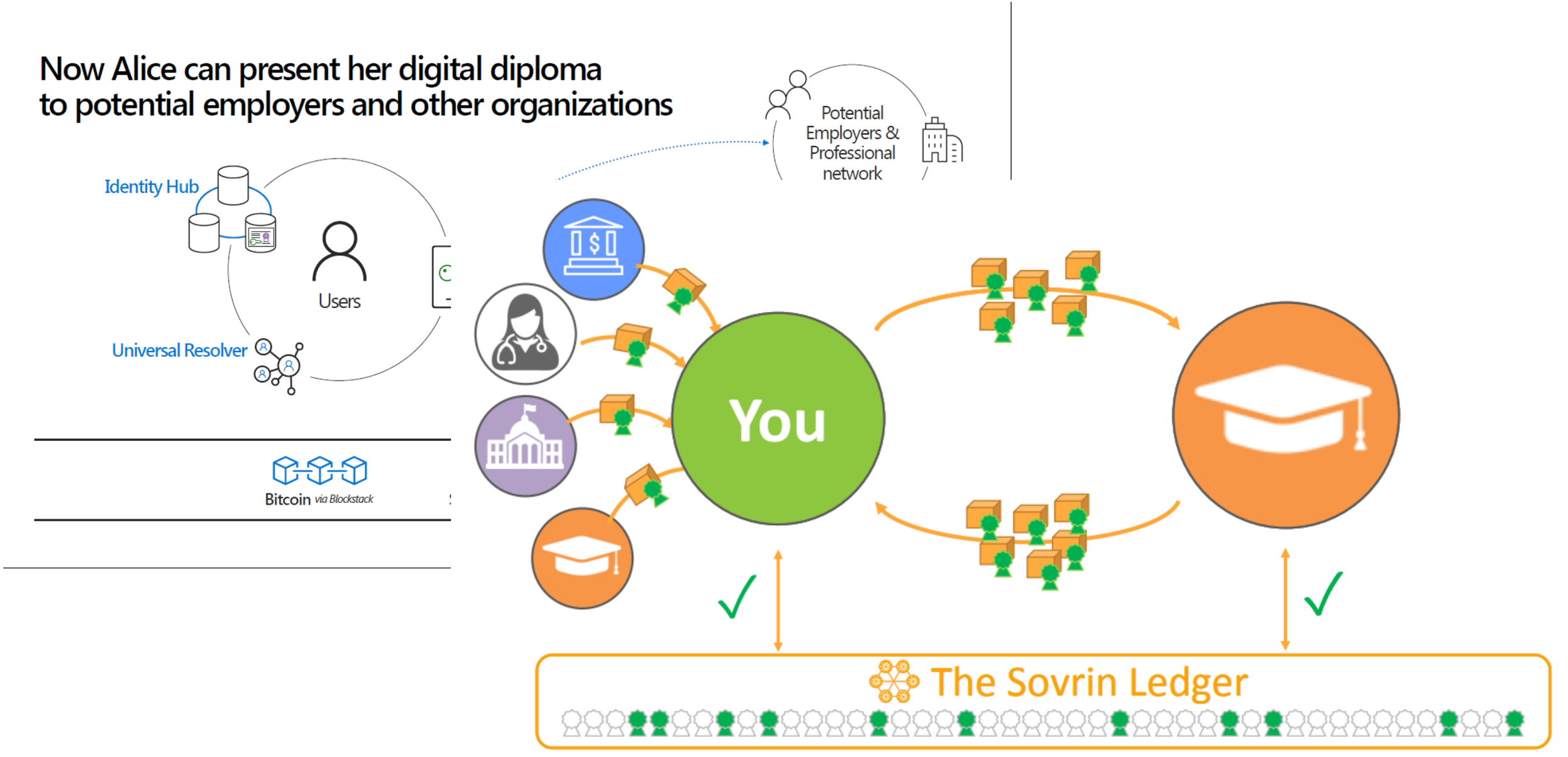


公開されているユーザの公開鍵を使って署名を検証する

Step4：属性の検証

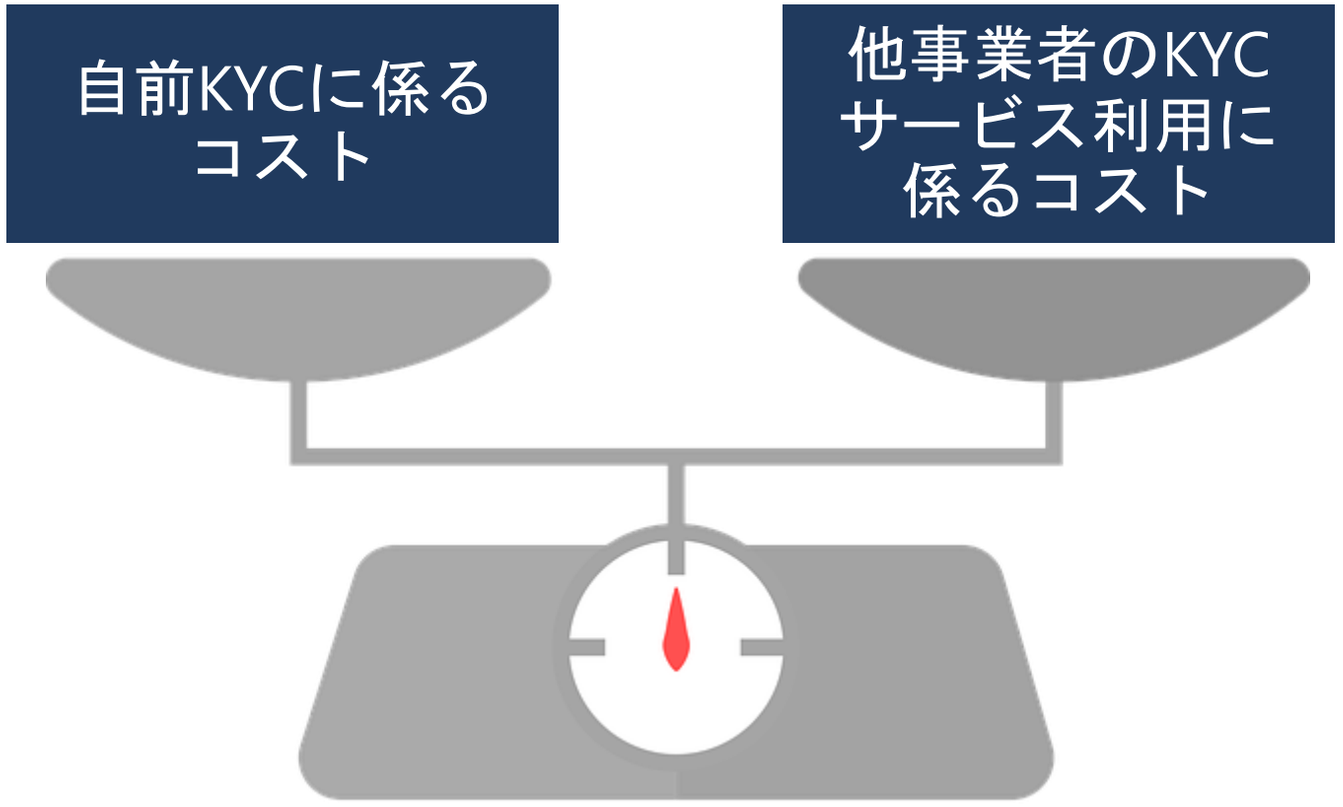

事務所
国家公安委員会
Identity Hub
DID Authentication
People, Apps, and Devices
User Agent
Verifiable Credentials
Users
社員証
保険証
POINT CARD
Universal Resolver
W3C Decentralized Identifiers
受け取ったVerifiable CredentialsのDID Documentの公開鍵でCredentialsを検証
Dist
Blockchains and Ledgers

PoCの例：学位証明、医師資格の証明



ビジネス）APIビジネスは成立するか？

- 本当に他社のKYC結果を「買う」のか？



今後の課題①：技術・ポリシー・ビジネスのバランス

- 本人確認済み属性の伝搬は技術的には簡単
  - 伝搬された情報を（精度・鮮度を含め）信じてOKかどうかは別問題
- デューデリジェンスの結果は更に難しい
  - 銀行APIで個人の情報が取得できれば反社チェックをOKとするのか？
  - 信販会社の決済履歴をAPI公開するのか？
  - 信用スコアを信用・利用するのか？（ロジックは公開されていないことが多い）
- 本人確認済み情報やスコア提供を提供する側と利用する側のビジネスモデル（コスト構造）は難しい

今後の課題②：利用者は管理主体となれるのか

結局のところ、自己主権型アイデンティティでは、

- 主権はユーザに！
- 責任もユーザに！

⇒自身のアイデンティティ情報を渡す先の信頼性の確認や事故が起きた時の責任もユーザ自身が取る必要がある

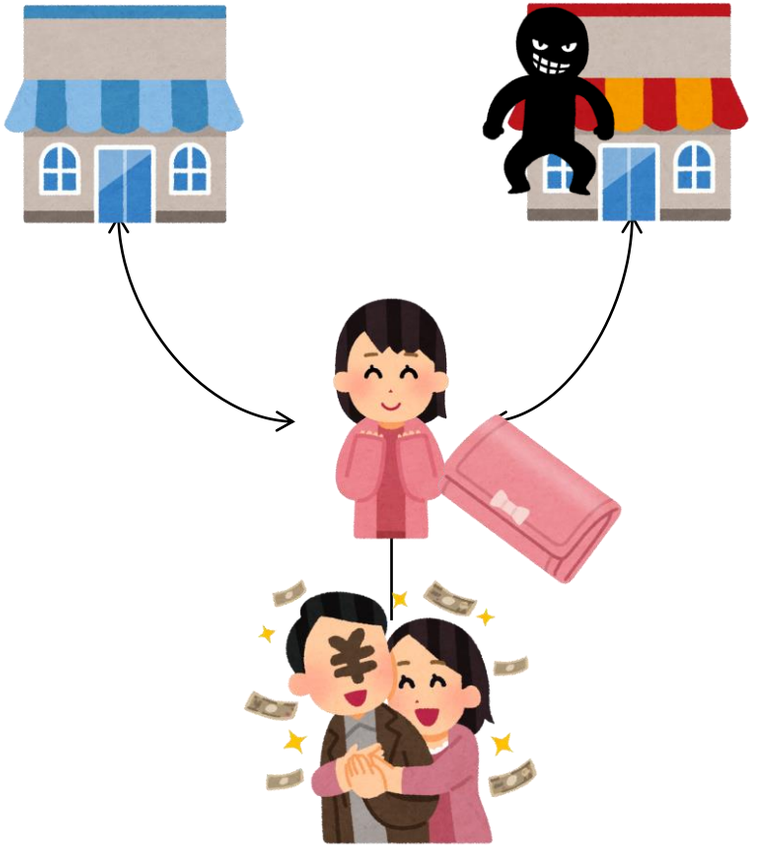
⇒利用者に代わって信頼を担保する枠組みの必要性

- 情報銀行
- Identity Custodian

フェデレーション
買ってもらう

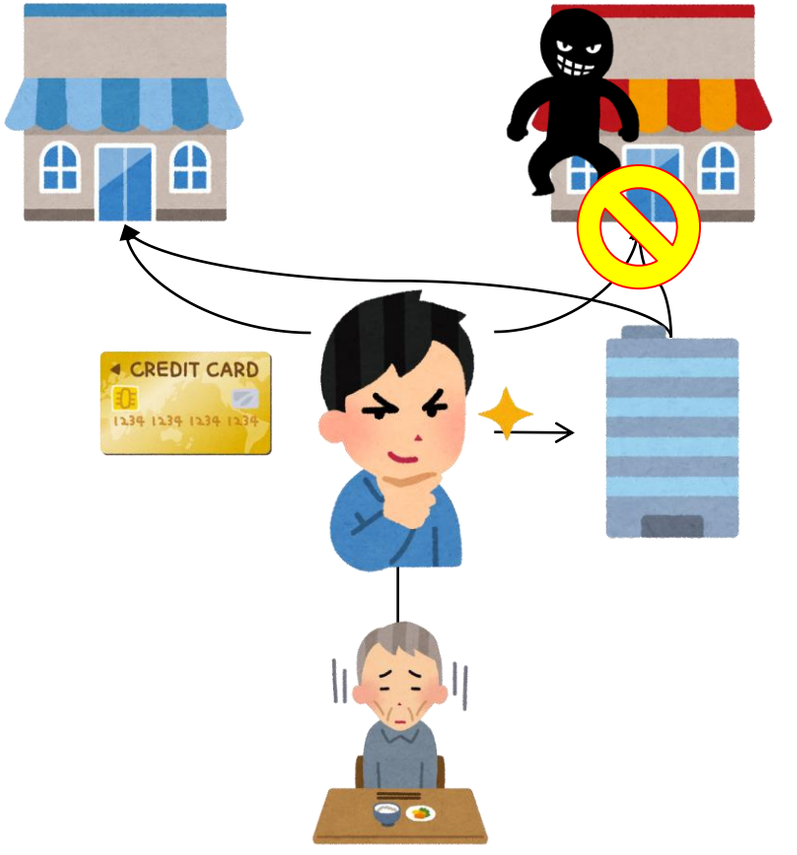
親が信頼する店で買い物
事故があったら親が保証
どこで買い物をするか把握

自己主権型Identity
お小遣いをもらう



自分が信頼する店で買い物
事故があったら自己責任
親は子の行動を把握しない

情報銀行
クレジットカード



カード会社が信頼する店で買い物
事故があったらカード会社が保証
親は子の行動を把握しない

OpenIDファウンデーション・ジャパンでの取り組み

- KYCワーキング・グループでの活動
  - ポリシー
    - 業界毎のKYCの要件の洗い出し
    - 共有化を行うための法令面の互換性の確認など
  - 技術
    - DIDなど新技術の調査
    - OpenID Connectへの影響調査
    - その他課題（KYC済みデータの共有化時のスキーマ共通化など）の検討

まとめ

- 人口構造の変化やフリクションレスのサービスへの要求により KYCの新しい姿が求められている
- 各種APIや信用スコア提供サービスが出てきているが、ポリシー・レギュレーション、テクノロジー、ビジネスの観点で整理が必要
- テクノロジーの面ではブロックチェーンの利活用の一つとして自己主権型アイデンティティの考え方が活発に議論されている
- 今後の課題として技術とポリシーのバランス、利用者が本当に自己主権を求めているのか？について深堀・議論が必要