

DID/VCをビジネスで 活用する上での可能性と課題

Yoichi Maejima

Identity Tech Lead

City Platform

yoichi.maejima@woven.toyota

自己紹介



ウーブン・バイ・トヨタ株式会社
Woven City Management, City Platform,
Identity Tech lead
前嶋 陽一

- 監査法人トーマツにてブロックチェーンに関連したビジネス開発や暗号資産関連のセキュリティ支援・監査業務を実施
- トヨタファイナンシャルサービスへ移り、トヨタブロックチェーンラボに参画
- ウーブンバイトヨタへ出向し、CityPlatformチームメンバーとして、初期設計から関わる
- 現在、City PlatformのIdentity Tech LeadとしてID基盤の設計・開発を推進
- 筑波大学非常勤講師「ブロックチェーン技術と地域未来創生」担当

トヨタにはグループ横断でブロックチェーンを推進するラボがあります

Organization



TOYOTA
BLOCKCHAIN
LAB

代表幹事会社

TOYOTA



参加会社



TOYOTA SYSTEMS

DENSO



TOYOTA CENTRAL R&D LABS

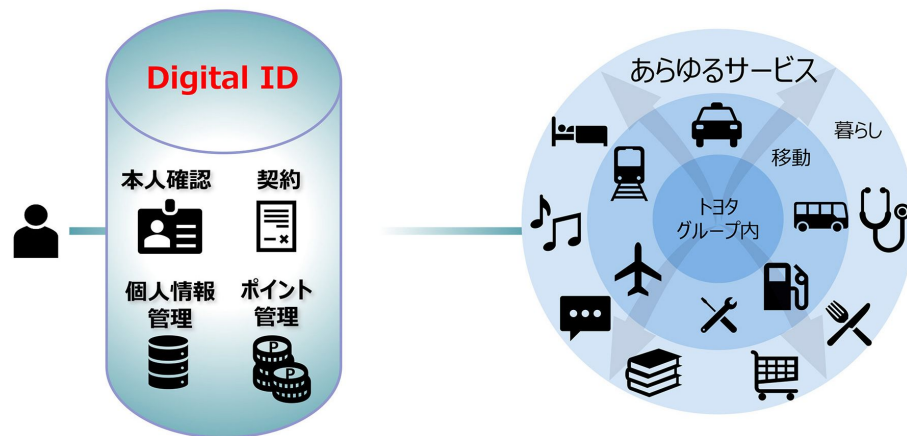


DAIHATSU

注力領域の 1つ: デジタルアイデンティティ

グループ内外の様々なサービスを「安全・安心」のもと、
「より便利に」「カスタマイズされた形で」利用できる世界を目指す

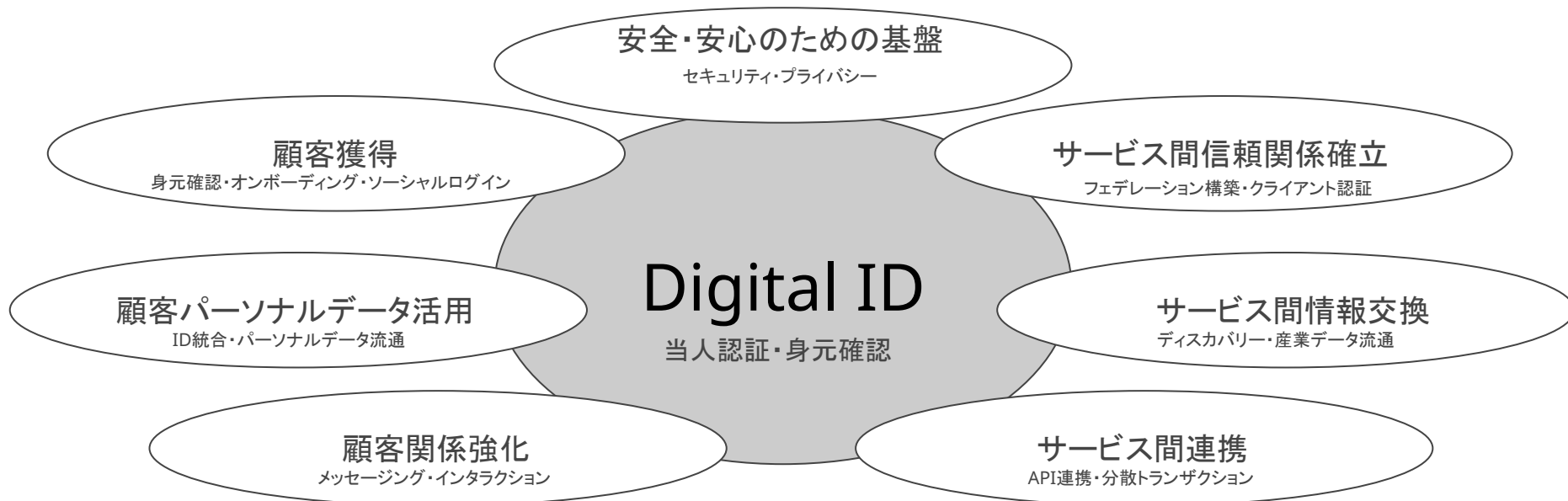
目指す世界



出所: トヨタプレスリリース, 2020/3/16, 「トヨタ・ブロックチェーン・ラボ」、ブロックチェーン技術の活用検討と外部連携を加速化 ,
<https://global.toyota/jp/newsroom/corporate/31827409.html>

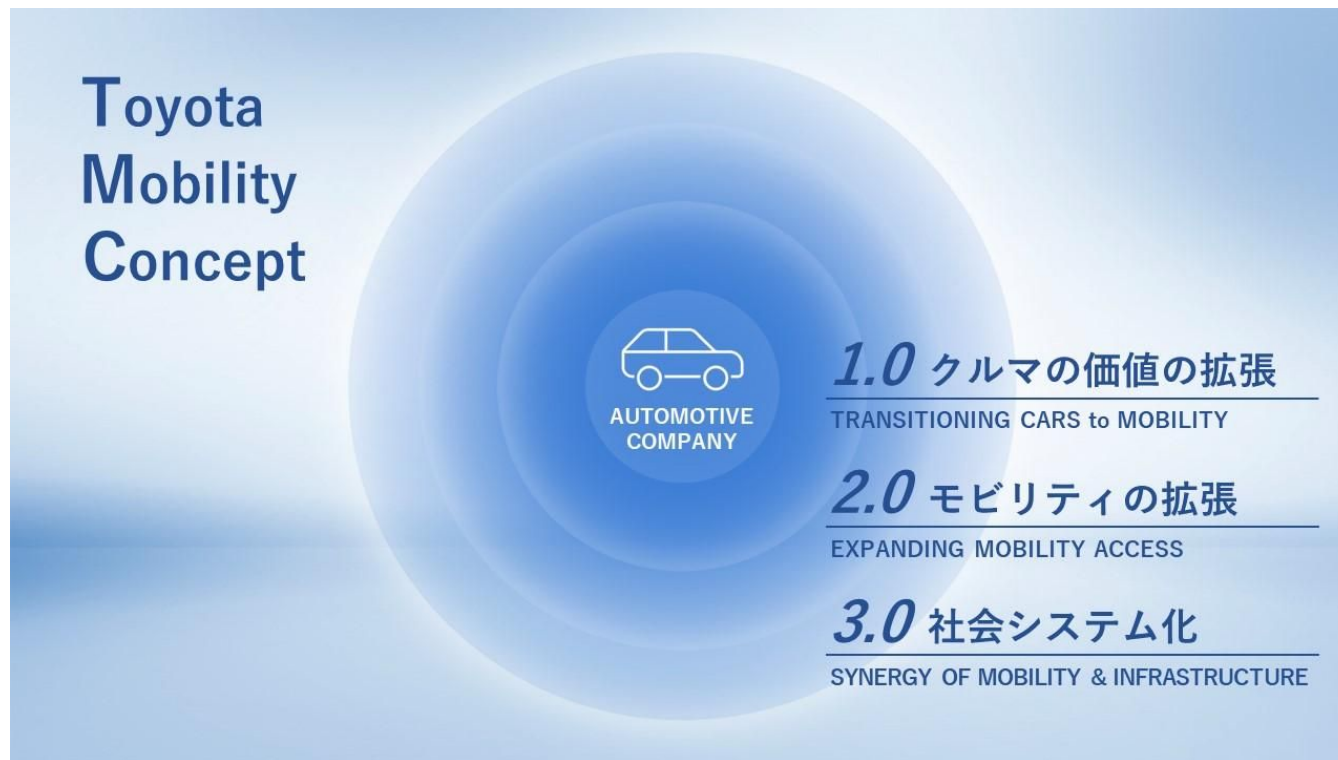
分散型ID/VCの可能性

企業の中で「アイデンティティ」には様々な期待が寄せられます



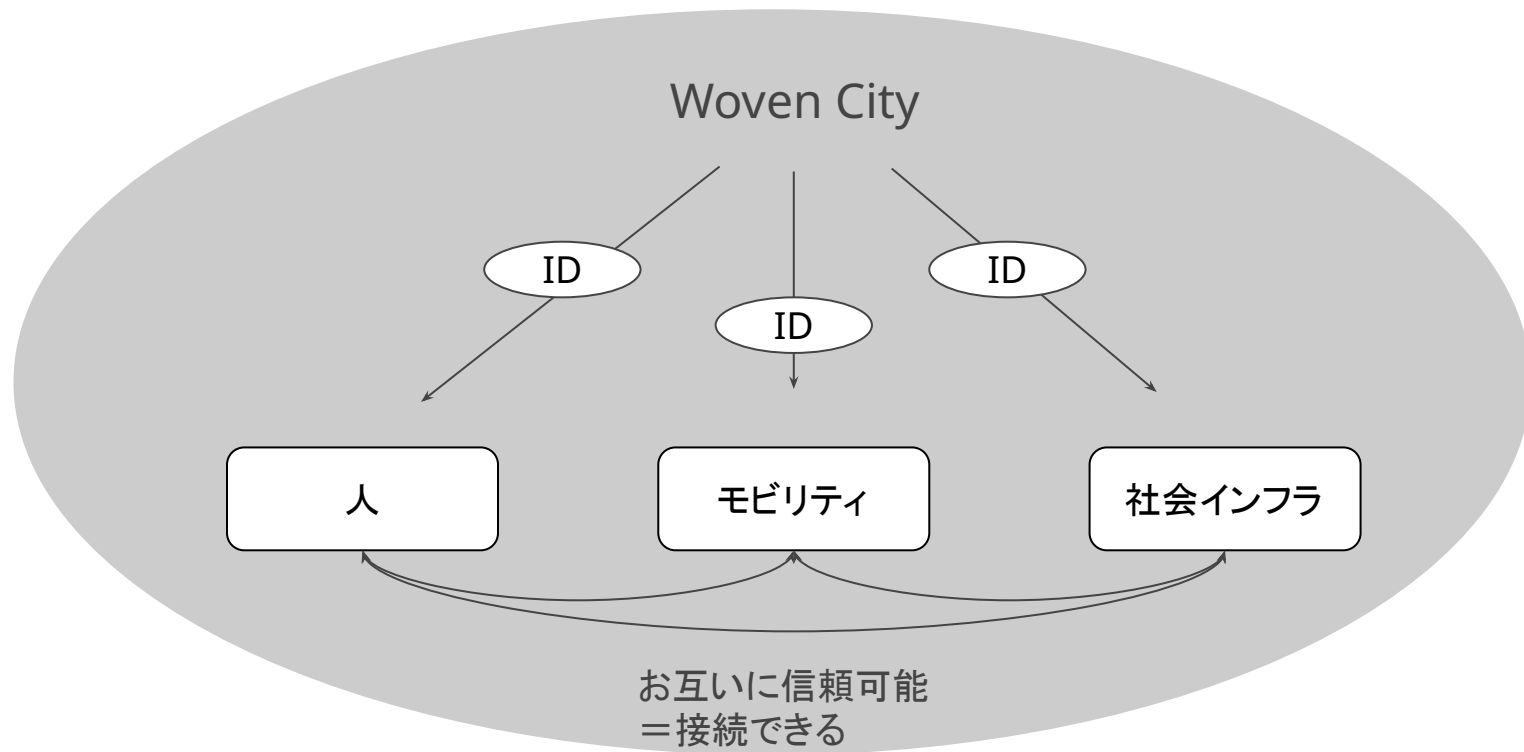
アイデンティティは、さまざまなものを「つなげる」ための基盤技術としてビジネスの中での重要性が高まっている

トヨタはモビリティカンパニーへと変革し、社会システム化を目指しています



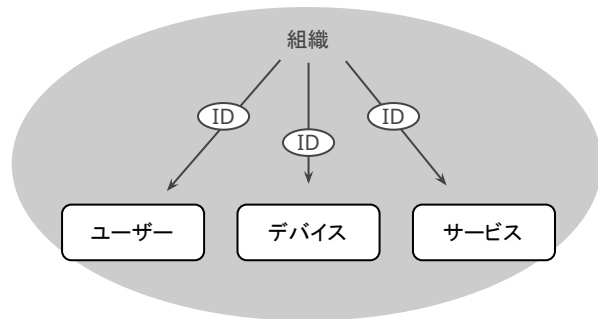
出所: トヨタタイムス, 2023/4/11, モビリティ・カンパニーへの変革加速 佐藤社長が語るトヨタの未来 , https://toyotatimes.jp/toyota_news/new_management_policy/001_1.html

Woven Cityでは私たちが信頼を担保するため、サービス同士でつながれます



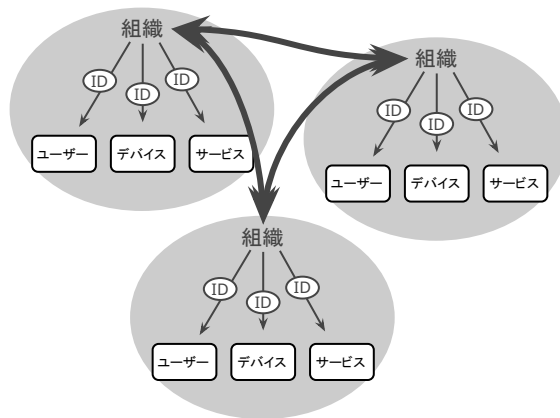
分散型IDは分散エコシステムへの拡大の道筋を示すと期待しています

1. シングルオーソリティモデル



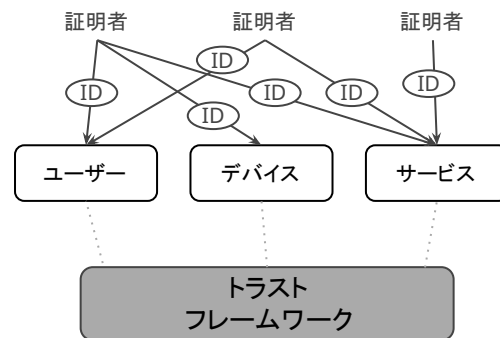
全ての参加者が信頼できる組織からアイデンティティを発行してもらい、それを相互に提示する

2. フェデレーションモデル



組織間でも信頼関係を構築し、いずれかの組織からのIDがあれば信頼する

3. オープンワールドモデル



様々な証明者が発行する検証可能な情報を集め、利用者（エージェント）がトラストフレームワークに則り自律的に判断する。

分散型ID/VCユースケース

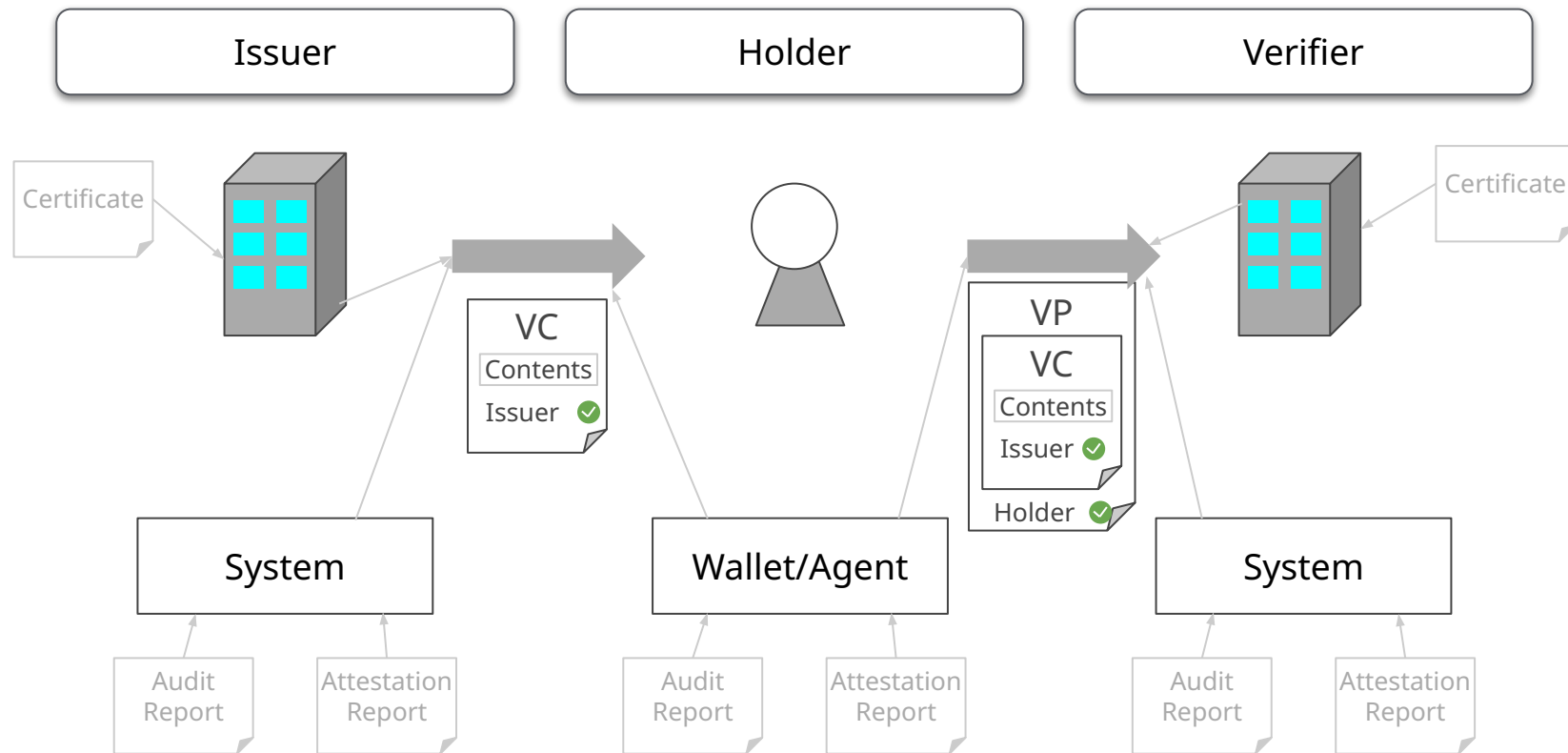
数多くのDID/VCのユースケースが提案され、実証されています

表 3. 2023 年度実証事業における顧客の課題と提供価値

事業者名	ユースケース名	対象顧客	課題・懸念 (ペイン)	本ユースケースで実現する顧客への提供価値
DataSign	ウォレットにおけるアイデンティティ管理とオンラインコミュニケーション	情報のやりとりを行いたいビジネスパーソン	・通信相手が本当に意図した人物かわからない ・特定の事業者によくの情報を渡すに不安	・自らアイデンティティを管理でき、サービス事業者や他の生活者を検証しつつ、必要最小限の情報を選択的に開示し、特定の事業者へ依存せずに安全なコミュニケーションを実現
DNP	共助アプリにおけるプラットフォームを超えたユーザー間の共有	共助アプリベンダー	・アプリユーザーの信頼性を担保するためにコストがかかる、アプリユーザーの継続的利用・活性化に課題 ・マネタイズの方法が広告・利用料などパターンに限られる、自社エコシステムでは規模的に収益が不十分	・他共助アプリの共助実績をユーザー間の検証として利用化可能 ・共助実績を、共助以外のサービスとも連携可能
IGS	国際間の教育拡充と労働市場の流動性を高める信頼ネットワーク構築～お金の問題なく学び自らの可能性を広げられる世界へ～	国内に拠点を置く日本企業	・デジタル領域の人材不足であり、海外から人材を採用する必要があるが、海外人材は能力の把握が難しく、採用にかかるデータ管理が複雑	・標準化された能力データを活用し、海外人材が自身でデータを管理可能な採用マッチングサービス活用による効率的な管理のもと海外人材の採用
富士通 Japan	大学技術職員の活躍に向けたスキルの見える化：スキルの質保証と主体的情報開示の試行	地域のニーズに応える人材育成・研究の推進を重点施策とするS55の国立大学等	・研究促進や地域貢献に繋げる機会を増やしたいが、技術職員がどのようなスキルや経験を持っているか分からない ・プロジェクトへのアサインがコネクションや主観的な判断になっており、非効率・機会損失となっている	・スキルの標準化/可視化を行い、マッチング基盤を整備することで、大学とマッチングしやすい一般企業・大学間の研究推進および地域貢献（産業活性化や課題解決など）の支援
PitPa	海外人材選流におけるクロスボーダー型個人情報流通システム	海外人材を採用したい/雇っている日本国内企業	・海外出身従業員の採用数・満足度を向上したいが、企業認知度の不足が生じている	・証明書発行による企業努力によってコストを下げずに海外採用PRの実現 ・海外出身従業員のモチベーション向上、生活支援にも繋がる福利厚生ツールの獲得
みずほR&T	もてぶりのサプライチェーンにおける製品含有化学物質情報等の確実な伝達を可能とする Chemical Management Platform (CMP)	自動車・電機電子機器等の組立製品サプライチェーンに関わる企業における製品含有化学物質管理の担当部署・担当者	・製品含有物質にかかる情報の授受の対応や、正確性・信頼性を確認するのに時間・負荷がある ・企業機密情報が保護されないリスクがある	・機密情報を保護しつつ、法規制や顧客要求への対応に必要な製品含有化学物質情報の効率的な授受手段の提供
SBI HD	事業所 I D とそのデジタル認証基盤	製品のサプライヤー	・業界・業種横断で事業者・製品の信頼性の担保をしたいが、実態は模造品が流通している。第三者からの真正性が担保できていない状態	・事業所の実在性を確認でき、第三者が検証可能なデジタル証明書を付与することで取引相手の信頼度を向上すること・出荷検査時に製品ロットに対して製造者の保証を追加すること
シミック	臨床試験及び医療現場における信頼性及び応用可能性の高い情報流通システム	製薬会社、CRO・SMO・ARO等の知見に関する機関の臨床事業部門	・臨床試験、臨床研究のコスト削減と速度向上を図りたいが、関連システム・デバイスに多様なものがあり、ベンダー・プロダクトごとに技術基盤や操作方法がそれぞれ異なることから自社で包括的に整備することが困難	・多様なウェアラブルデバイスに適用可能かつ、eConsentからウェアラブルデバイスデータの抽出までをシームレスに行うためのAPI提供やコンサルティング提供により円滑な治験推進を支援
ORPHE	下肢運動器疾患患者と医師、研究者間の信用できる歩行データ認証・流通システム	変形性膝関節症の患者/病院・研究機関	・下肢運動器疾患の改善を図りたいが、患者日常生活利用の時間や、データ共有に不安があり進んでいない状態	・インセンティブのあるエコシステムの中で、歩行データを主とした患者データを安心/安全/簡単に共有できる仕組み
電通総研	「KYC/KYBに基づいたトラストのある取引」を促進する新しい仕組み	法人確認業務を行う金融機関	・取引開始や途上や信用の、相手先情報の取得と確認に時間と手間がかかる ・デジタルでの信頼性確認に限界があり、窓口での対面対応が必要 ・デジタル化が遅れており、ユーザリテラシーや環境整備が進んでいない	・KYC/KYBに基づいたトラストのある取引に必要な真正性が担保されたKYC-KYB VC発行サービス
JISA	補助金事業を題材とした法人向け行政手続DX社会基盤化のプレ検証	補助金事業の所管省庁の設計担当 補助金事業の事務局や事業管理機関等の運営責任者	・事務局等の確認業務運用において、取得可能な情報の不足により、確認レベルの向上と対応負担の軽減の両立が困難 ・機械可読性のあるデータとして取得および提出可能な対象書類が限定的であり、自動照合等含む業務効率化に支障	・「民間事業者同士のビジネス活動や行政手続き等の様々なコネクスト」から生成されたデータの利活用の拡大により、「行政手続き、特に補助金事業等の不適切利用の抑止、関連書類等のデジタル化促進」および「民間ビジネス環境へ寄与する可能性も意識した事業KYC/KYBのDX」が継続的に進展し続ける姿の実現
OP CIP	Trusted web advertising system with Originator Profileを活用したWeb広告取引における信頼性付与	インターネット利用者 インターネット広告利用企業	・インターネット広告の信用度が低くアクセスしにくい、アクセスすると被害に遭う ・アドフランドやフェイクニュースによるブランドリスクの顕現	・インターネット広告の健全性を向上させることで、生活者、広告主の双方に安心をもたらす

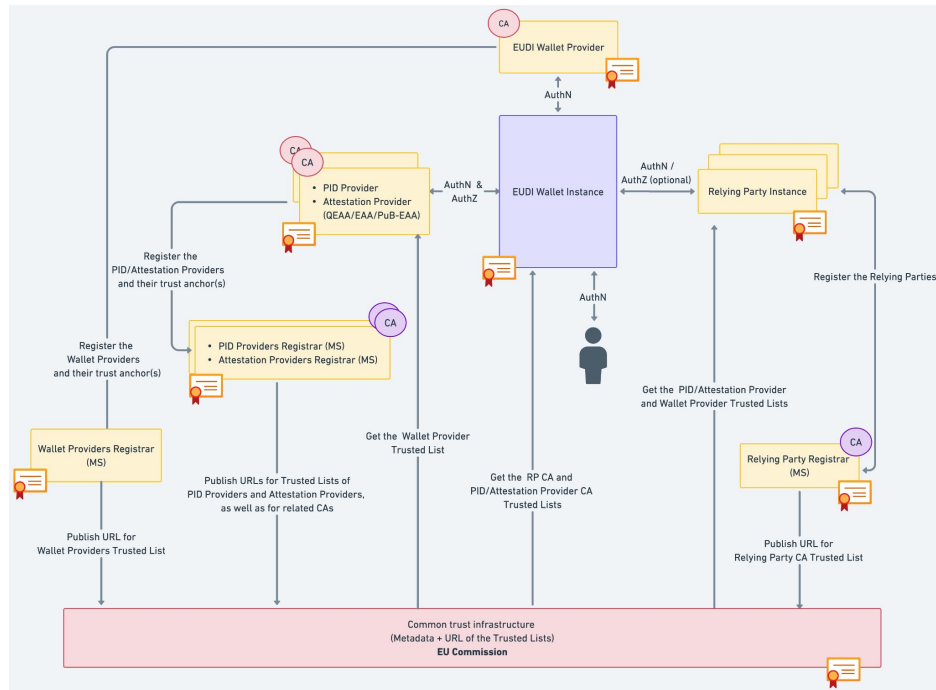
出所:Trusted Web推進協議会, 2024/6/28, DX 実現に向けたデータ活用におけるトラスト向上のためのアクション・リスト(α版) https://www.kantei.go.jp/jp/singi/digitalmarket/trusted_web/pdf/actionlist.pdf

シンプルなユースケースでも、芋づる式に検証すべきことが増えてしまいます



実用的なユースケースでは検証すべきことが非常に多くなります

事例1: EU Identity Wallet Reference Architecture



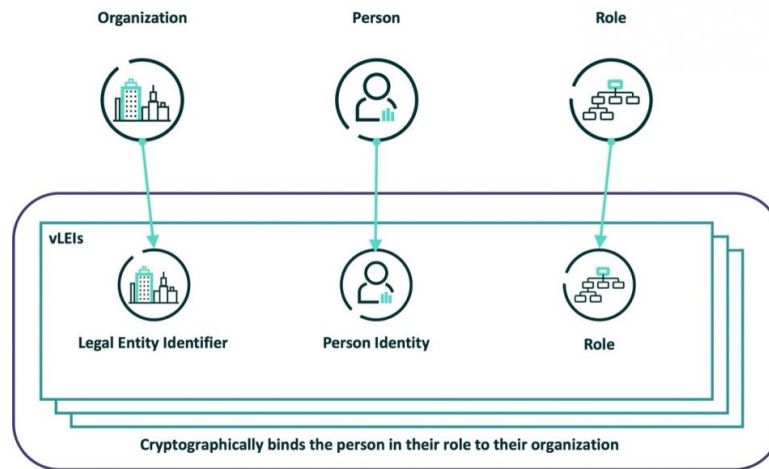
Issuer = PID Provider
Holder = Wallet
Verifier = Relying Party

それぞれの主体がEUに認定されたRegistrarに登録されなければ、データのやり取りに接続できない

出所: European Commission, 2024/8/30, European Digital Identity Wallet Architecture and Reference Framework(v3),
<https://github.com/eu-digital-identity-wallet/eudi-doc-architecture-and-reference-framework/blob/main/docs/arf.md>

組織のアイデンティティを証明するvLEIは実際に稼働しています

事例2: GLEIF vLEI

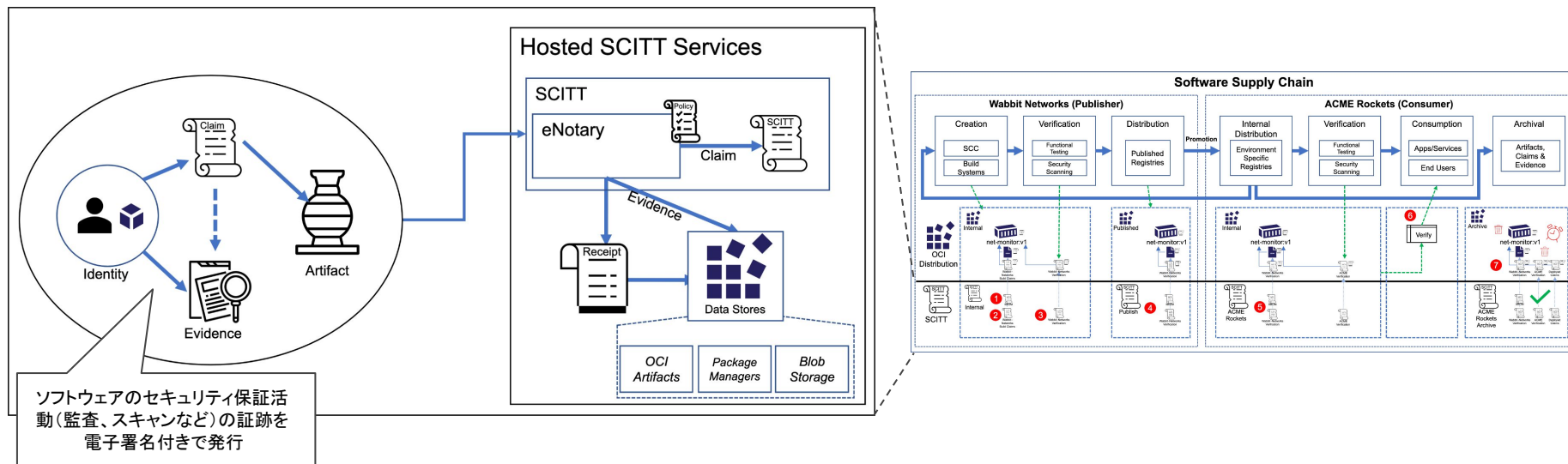


- 「法人の実在性」と「組織の中での代表権」を証明するためのフレームワーク
- グローバルに発行・運用されている法人識別子「LEI」に基づき発行され、そのLEIは金融規制やサプライチェーンのポリシーで必須とされている
- 組織のVC発行はGLEIFから承認を受けたQualified vLEI Issuer(QVI)が発行し、組織の代表者を示す個人に対するVCはその組織に発行が委譲される
- それぞれの発行者はGLEIFが定めるポリシーに準拠し、契約した上で定期的にレビューを受ける

出所:GLEIF, Introducing the verifiable LEI (vLEI), <https://www.gleif.org/en/vlei/introducing-the-verifiable-lei-vlei>

ソフトウェアのサプライチェーンでトラストを確立するSCITTが策定されています

事例3: SCITT(Supply Chain Integrity, Transparency and Trust)



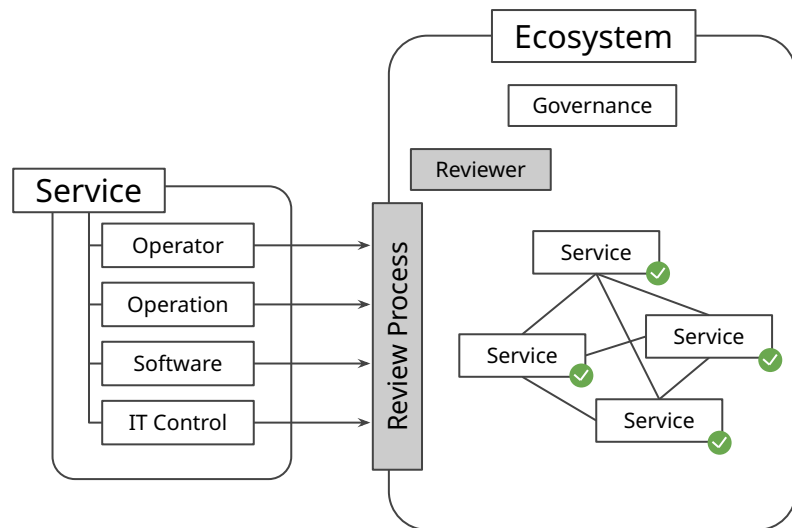
- ソフトウェアのセキュリティ保証活動の証跡を、組織を跨いで流通できるようにするための仕様
- 最終的な製品から個別の製品へ遡り必要なセキュリティ保証活動が実施されていることを自動的に検証可能
- Reference APIではDID/VCを意識した設計になっている

出所: SCITT introduction, <https://scitt.io/>

IETF, An Architecture for Trustworthy and Transparent Digital Supply Chains, <https://datatracker.ietf.org/doc/draft-ietf-scitt-architecture/>

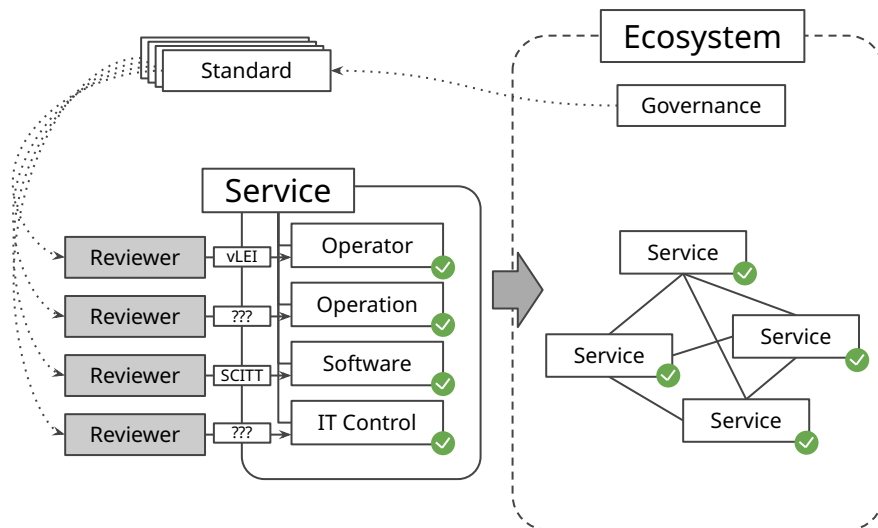
多数の証明を組み合わせて、重厚な人手によるレビューを自動化できるのでは

現在



エコシステムへの参加時に人手による重厚長大なレビューが必要なため、加入に時間や大きなコストがかかる

将来



サービスの構成要素へのレビュープロセスを分解し、それぞれ証明することで加入にかかる時間・コストを分割できる

エコシステムへの参加時のレビュープロセスを、
別のトラストフレームワークの証明を組み合わせて自動化できないか

Gaia-XはDID/VCによりTrustを自動確立しデータ流通できる世界を目指しています

事例4: Gaia-X

Advanced Smart Services

(Cross-) Sector Innovations /
Market places / Applications

Data Spaces

Interoperable & portable (Cross-) Sector data-sets
and services

Gaia-X Federation Services

Federated & distributed for interoperability Trust &
Sovereignty services

Compliance

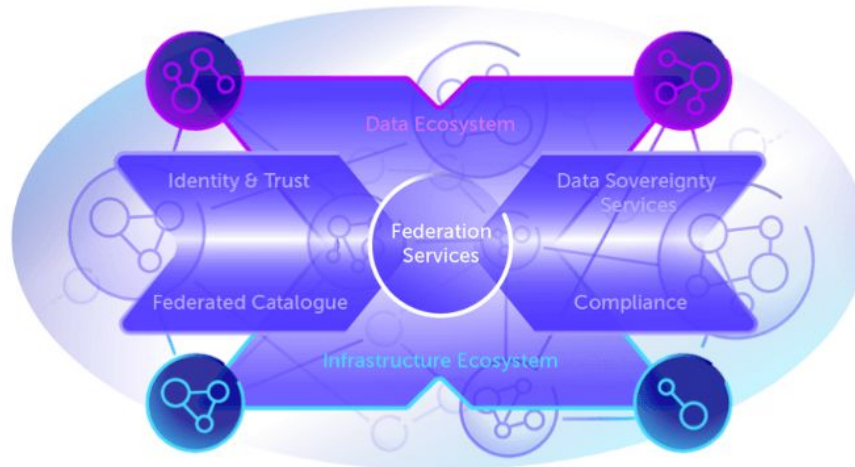
Legal: Regulation & Policies

Portability, Interoperability & Interconnectivity

Technical: Architecture of Standards
Commercial: Policies

Infrastructure Provider

Cloud, Edge, HPC, Interconnection, On Premise



産業ごとに構成されるData Ecosystem(Data Space)の参加者が、Ecosystemを跨いでデータ交換できるようにするため、DID/VCベースのIdentity & Trustサービスや契約状況を集中管理するComplianceサービスなどを含むFederation ServiceをGaia-X全体で運用している。

出所: Gaia-X Federation Service, About Gaia-X, <https://www.gxfs.eu/connection-to-gaia-x/>

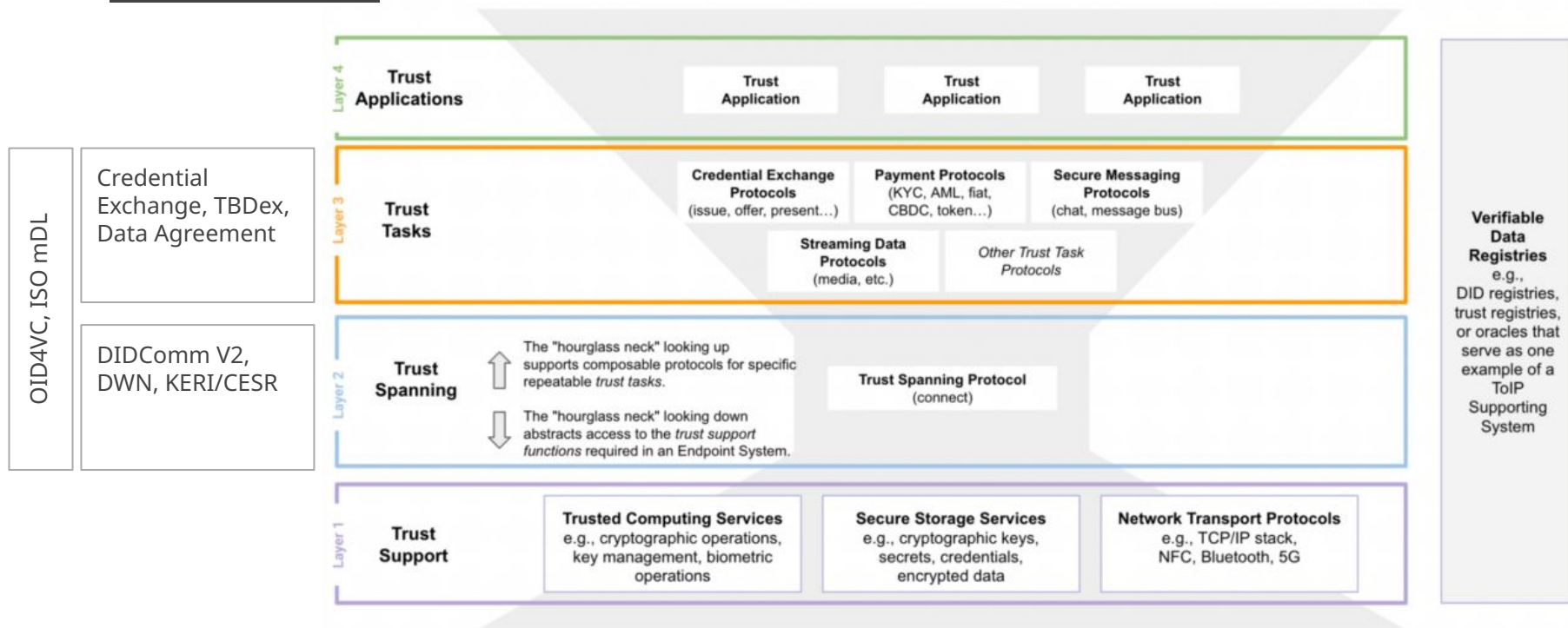
ビジネスではトラストの確立だけでなく、その活用までつなげる必要があります

- アイデンティティには様々な期待が寄せられており、認証・認可のみならずビジネスユースケースへの直接の繋がりをアピールできないと意思決定者を説得することができない
- 基礎となるトラストの確立のためだけでも非常に大きな労力が必要とされるのに、その先のトラストの確立されたアイデンティティを使ったアプリケーションを作るためには、さらに労力が必要になってしまう

確立されたアイデンティティの上で、トラストなアプリケーションを迅速に構築できるようになる必要がある

プロトコルをパーツに分け再利用性を高めるフレームワークが提案されています

Trust over IP model

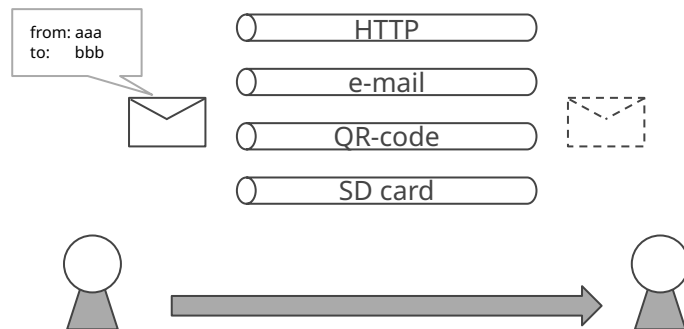


出所: Trust over IP foundation, 2023/1/5, The ToIP Trust Spanning Protocol, <https://www.trustoverip.org/blog/2023/01/05/the-toip-trust-spanning-protocol/>

スパンングレイヤーでは同期通信と非同期通信をカバーしています

DID Comm

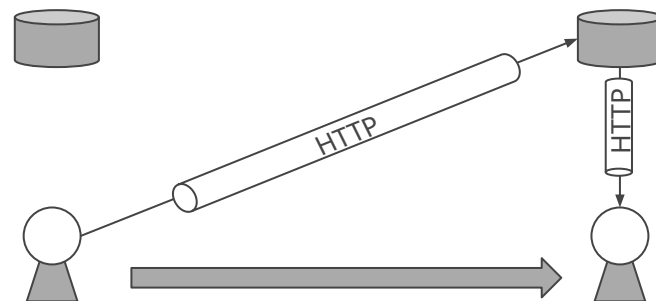
通信手段にかかわらず、相手にセキュアに情報を送るプロトコル



- 相手が原則オンラインのときに同期的にメッセージを送信
- RelayやRoutingにより複雑な通信方式も可能

Decentralized Web Node

相手のサーバーにデータをPushもしくはQueryできるHTTPベースのプロトコル



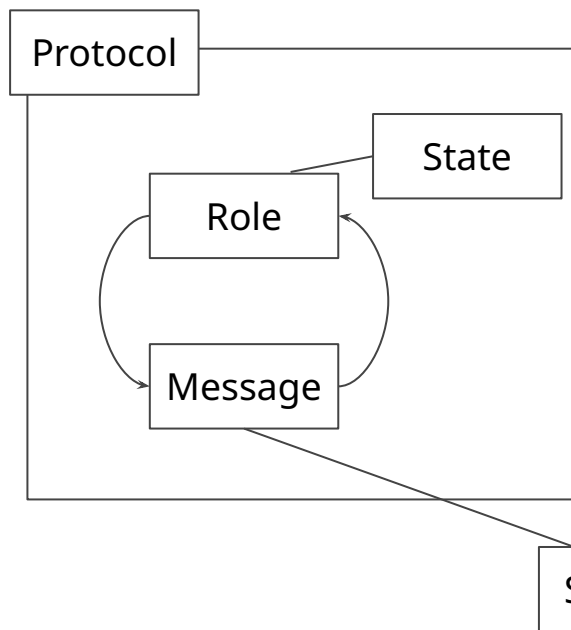
- サーバーに送るので非同期にメッセージを送れる
- DIDに紐づくデータを蓄積できるのでパーソナルデータストアのように利用できる

出所: Decentralized Identity Foundation, DIDComm Messaging v2.1 Editor's Draft, <https://identity.foundation/didcomm-messaging/spec/v2.1/>
Decentralized Identity Foundation, Decentralized Web Node, <https://identity.foundation/decentralized-web-node/spec/>

DIDCommやDWNではプロトコルの上でプロトコルを定義できます

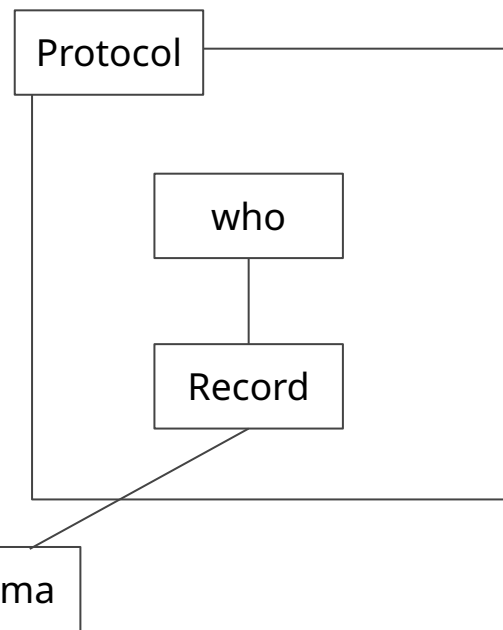
DID Comm messaging:

9. Protocols



Decentralized Web Node:

9.2 Protocols



Example of protocol definition

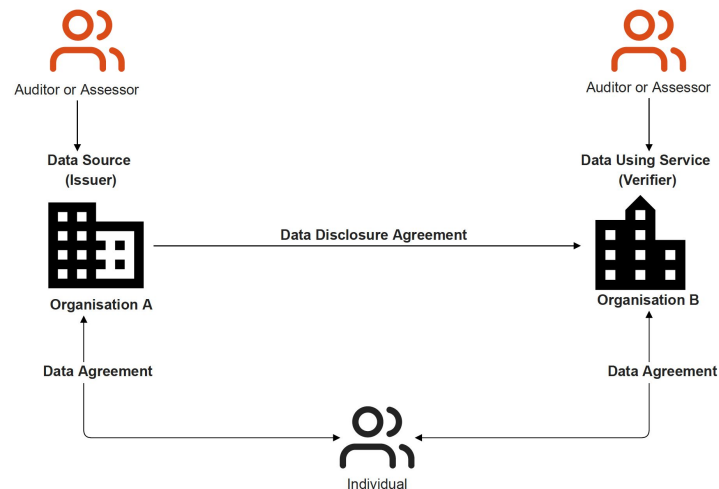
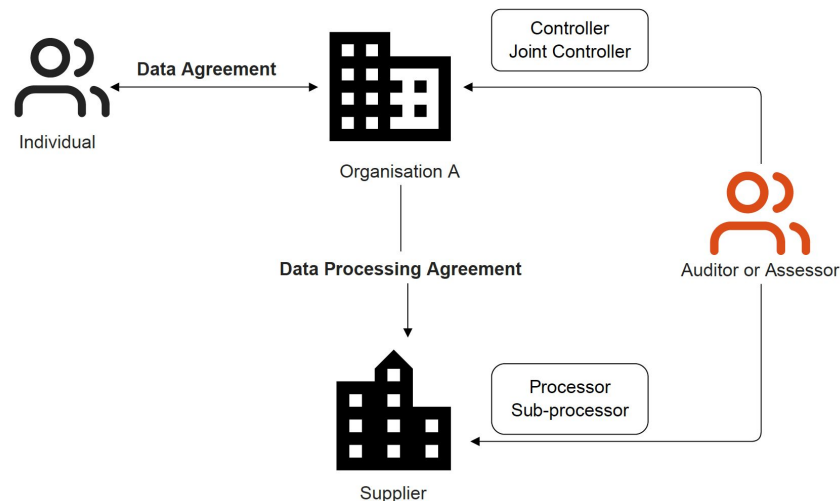
```
{
  "interface": "Protocols",
  "method": "Configure",
  "definition": {
    "protocol": "https://decentralized-social-example.org/protocol/",
    "published": true,
    "types": {
      "post": {
        "schema": "https://decentralized-social-example.org/schemas/post",
        "dataFormat": ["application/json"],
      },
      "reply": {
        "schema": "https://decentralized-social-example.org/schemas/reply",
        "dataFormat": ["application/json"],
      }
    },
    "structure": {
      "post": {
        "$actions": [
          {
            "who": "anyone",
            "can": "read",
          }
        ],
        "reply": {
          "$actions": [
            {
              "who": "anyone",
              "can": "write",
            }
          ]
        }
      }
    }
  }
}
```

Data Schema

Role-based Access Control

DID/VCを利用してGDPR上の「同意」を管理するプロトコルも提案されています

事例5: Data Agreement

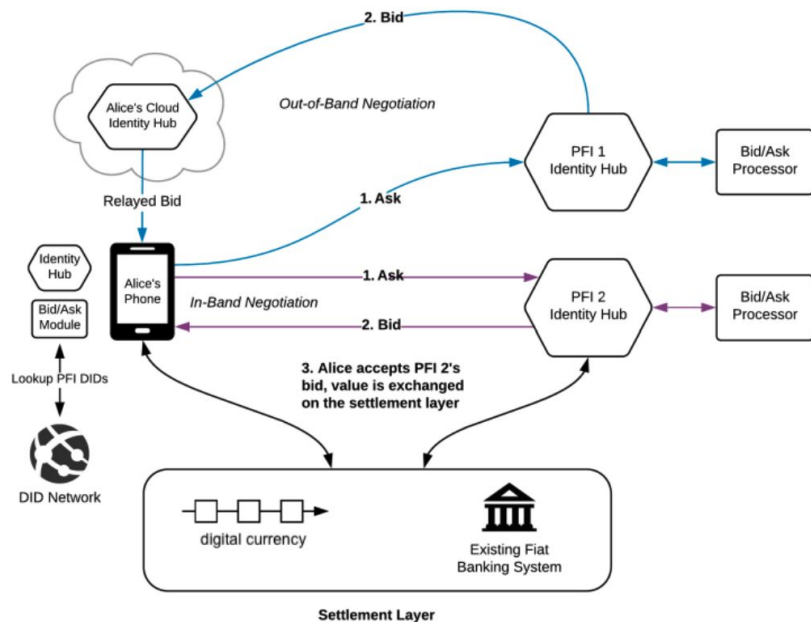


- GDPR上求められる「同意」を、DIDに紐づいた電子署名付きで授受するプロトコルを定義。
- HTTPとDIDCommを使いData Agreement Negotiation, Data Agreement Proofs, Data Agreement Termination, Data Disclosure Agreement, Data Agreement Context Decoratorの5つが定義されている。

出所: iGrunt.io, Data Agreement (DA) Specification, <https://da.igrunt.io/>

DID/VCを利用してPayment Coordinationを行うTBDexが提案されています

事例6: TBDex



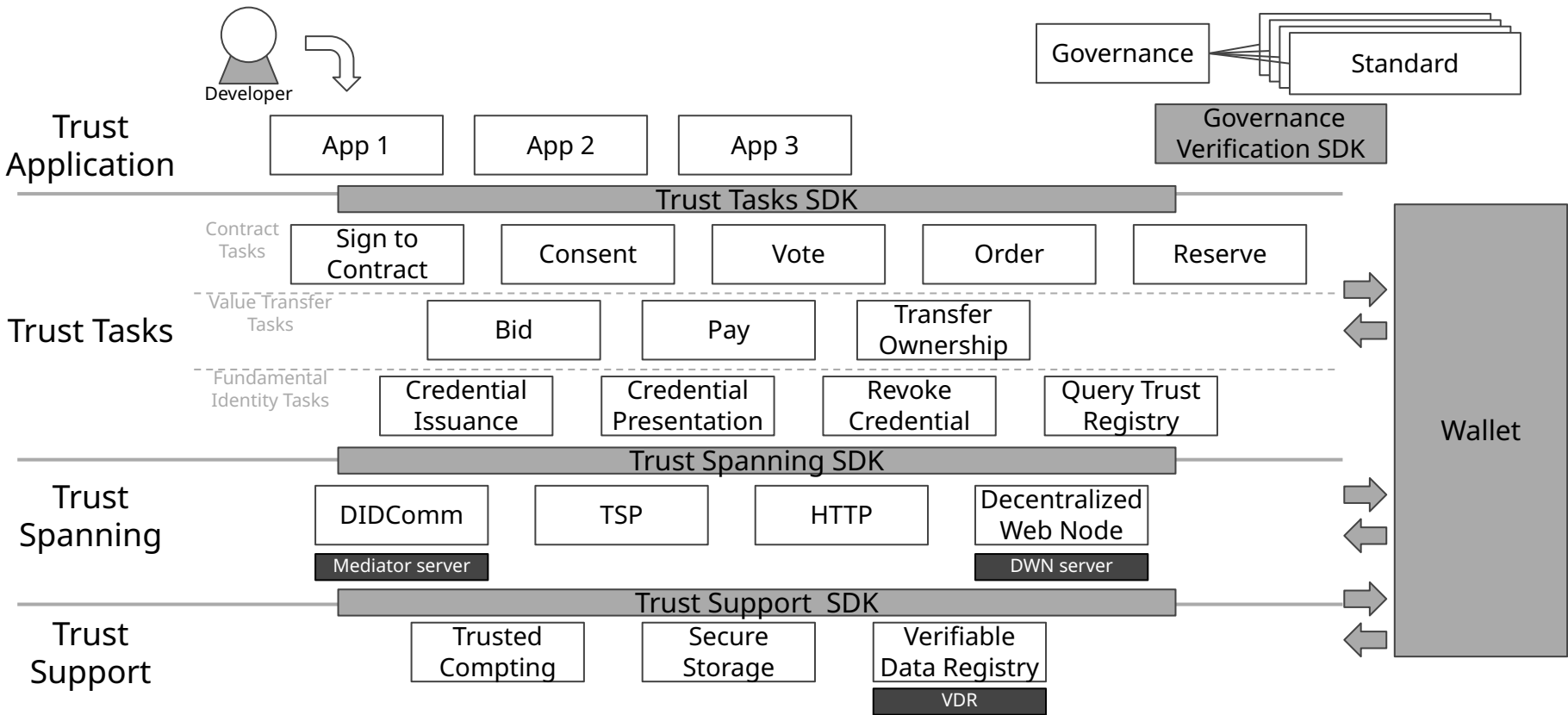
component-level topology and communication flow

General

- DWNに基づく分散型 Web コンセプト「Web5」を開発する TBD 社は DID/VC を用いて Payment を Coordinate する TBDex プロトコルを発表。仕様は <https://tbdex.dev/> で公開されている。
- TBDex プロトコルでは、支払い者が支払いを行う際に決済事業者へ見積依頼 (RFQ) を発行。決済事業者は支払い者の KYC を行い、リスクなどに応じて手数料と送金所要時間を返答。
- 支払い者は見積もりの中で最も良い条件の支払い事業者を選択。

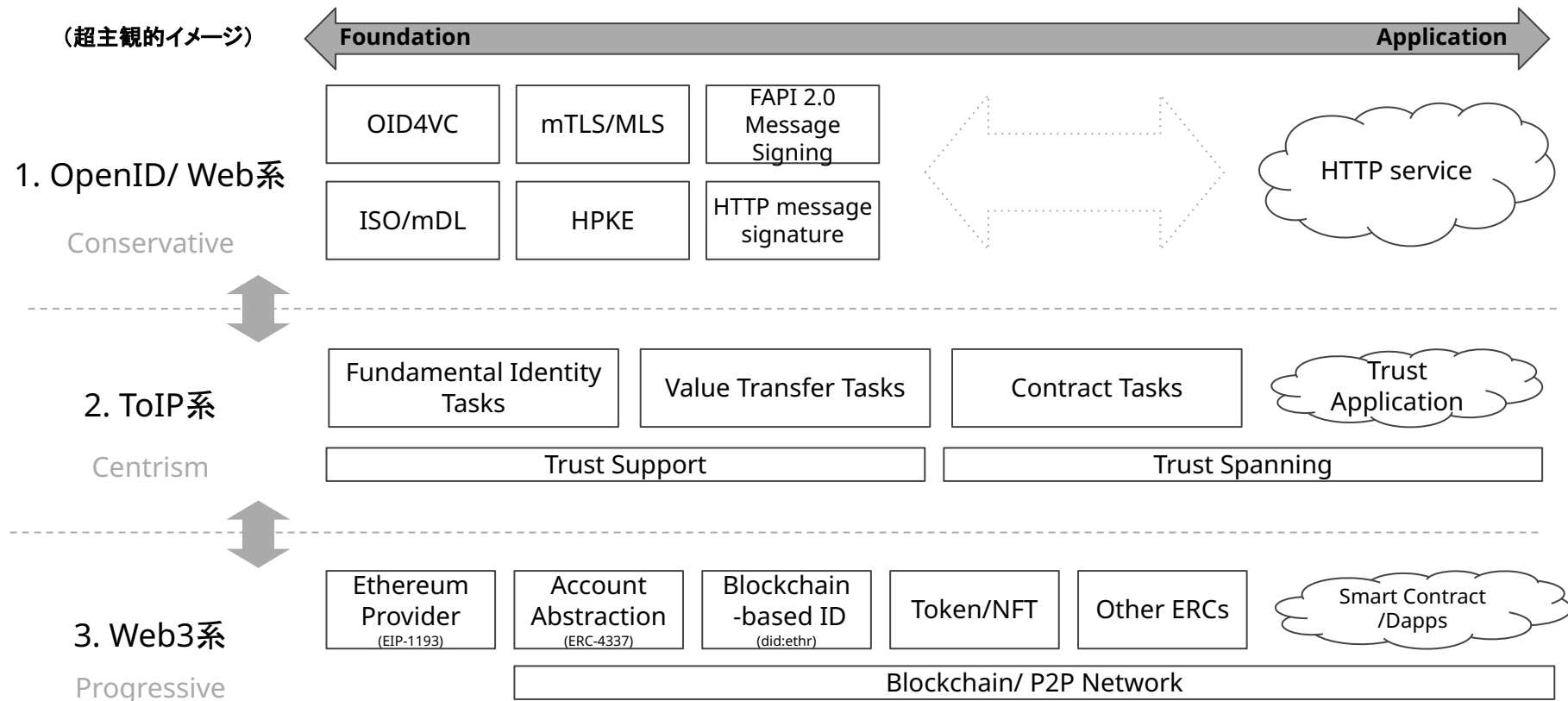
出所: TBD, TBDex Whitepaper, <https://github.com/TBD54566975/tbdex-whitepaper/blob/main/whitepaper.pdf>

普及するためには、タスクの共通化とハイレベルなSDKが必要です



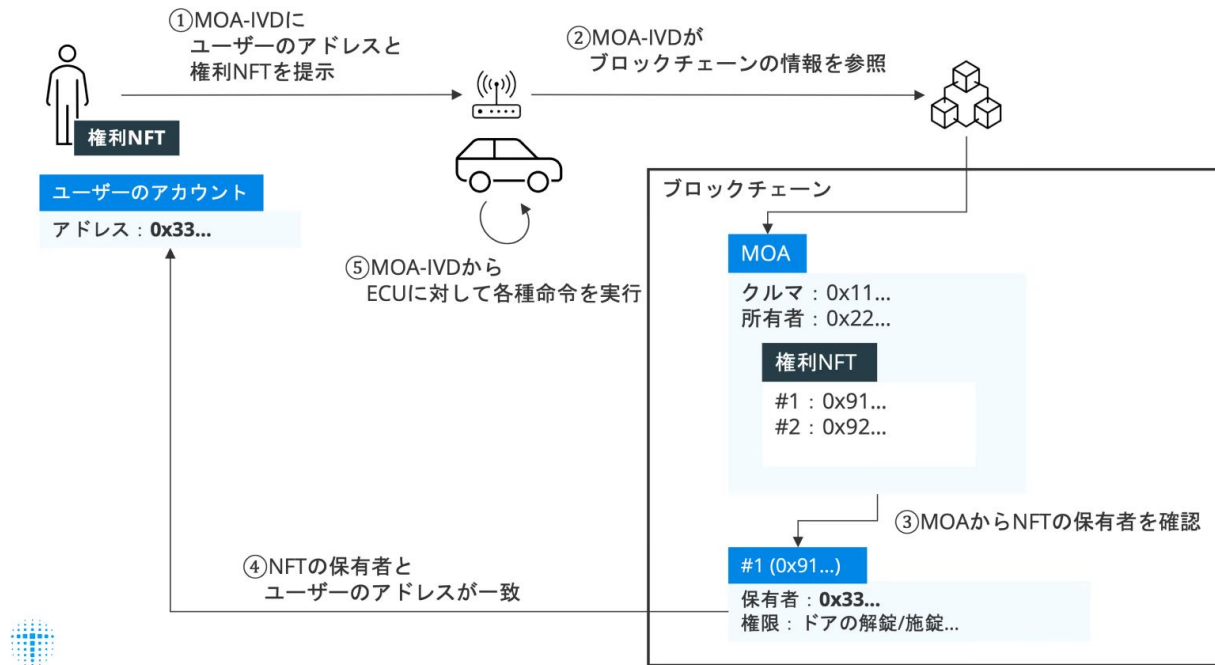
分散型ID/VC普及に向けた課題

現時点では確立した主流がなく、全体を俯瞰し動向を見守る必要があります



(ご参考)Toyota Blockchain LabではAccount Abstractionも研究しています

Mobility-Oriented Account(MOA) Concept



出所: Toyota Blockchain Lab, モビリティをパブリックブロックチェーンに登場させるには? ,<https://www.toyota-blockchain-lab.org/ja/library/how-to-introduce-mobility-into-the-public-blockchain>

VC発行者に対してインセンティブを作らなければなりません

- Verifiable Credential発行にかかる追加費用の負担
 - ほとんどの消費者向けビジネスでは顧客の受け入れを無料で行っており、消費者が自身に対する証明書に追加で費用を支払うには心理的抵抗が強い。(例: クレジットカード入会金無料)
 - 現在でも有償と認識されている法人向けの監査やセキュリティ診断は手数料を払うことが一般的であることから、顧客に証明書発行費用を転嫁することが比較的容易な可能性がある
- Verifiable Credential発行に伴う法的責任範囲の増加
 - 証明書に誤りが含まれていて、それがその証明書に依拠した他者に被害を与えた場合、証明書発行者は損害賠償請求を受けるリスクが生じる可能性がある。
 - 法人向け保証業務の場合、監査報告書や証明の利用範囲や流通範囲は契約で限定するなどノウハウがある。(例: SoC2報告書取得のために秘密保持契約が必要)

個人の証明を電子化よりも、法人向け証明の方がビジネス化しやすい可能性

「信頼できる情報」の価値は分かりにくく、顧客に再提出を求めにくいです

- 従来の情報の中には誤りや虚偽も含まれている可能性があるが、現時点でどれほど含まれているかわからない。
 - 例)従来の与信モデルは誤りや虚偽も含まれたノイズの含まれるデータに基づき構築されている。データのうち、誤りや虚偽を明確に識別することは困難であり、また、そのノイズが与信判断精度に与えている結果もわからない。(「Verifiable Dataコールドスタート問題」)
- 現時点ですでに情報を手に入れている中で、相手に証明を求めるのは失礼
 - 現時点で存在する取引関係では、従来の関係性に基づき、すでに必要な情報を手に入れている中で、改めて「証明付きの情報」の提示を取引相手に求めるのは、「疑われている」と相手を思わせてしまう危険性がある。

従来プロセスに適用するより、
新しいプロセスに適用する方が価値が理解されやすい可能性

まとめ

- これからビジネスがエコシステムとして相互接続する重要性が高まる中で、DID/VCがサービスを分散型で接続していくことを期待している
- DID/VCによりヒト、組織のアイデンティティが保証され、契約やシステムの証跡を自動的に検証できるようになると、サービスがエコシステムに自動的に接続できる
- ビジネスではエコシステムに接続したあとに、アプリケーションを開発する必要がある。それを実現するためにレイヤー化されたアーキテクチャーとライブラリの整備が必要
- 現時点では様々な取り組みがあり、どれが主流になるか分からない。また、法人向けに新規ビジネスを行う方が価値を訴えやすいと考えている。

DID/VCの活用拡大にむけて議論しましょう！

Thank you