

ブロックチェーンに関する官民推進会合 報告



2021年6月30日
一般社団法人 新経済連盟
内閣官房 情報通信技術(IT)総合戦略室

本資料の構成

I. 会合の概要

II. ヒアリング結果のまとめ

[参考 1] 事例集

[参考 2] 構成員からのご意見

I. 会合の概要

検討の経緯

1. 令和2年度の世界最先端デジタル国家創造宣言・官民データ活用推進基本計画（IT戦略2020）において「ブロックチェーン技術の行政や公共性の高い分野への導入を検討する際に課題となる安全性・即時性の検証や持続可能なモデル構築に必要な運用面・ルール面の課題抽出とその解決のための実証を行う。これらの取組を進めるにあたっては、民間における先導的な取組を行うグループとの対話により、継続的な運用を見据えた社会実装を推進する。」とされた
2. 新経済連盟より「国内外の最新動向やユースケースの共有、社会実装に向けた課題の洗い出し」のため、官民協議会の設置に関する提言が発表された
3. ポストコロナ、ウイズコロナの社会課題の解決手段として、ブロックチェーンの有用性に関し、民間団体（新経連等）と連携して検討を開始

◆ 令和2年9月から「ブロックチェーンに関する官民推進会合」を開催（全5回）

◆ 「地方公共団体の取り組み事例」「分散型ID」「教育」「配布」「中央省庁の取り組み事例」をテーマに計19件の事例紹介と議論を実施

ブロックチェーンに関する官民推進会合 概要

ポストコロナ、ウイズコロナの社会課題の解決手段として、ブロックチェーンの有用性を官民連携して検討、主に公共性が高い分野への適用を見据えた出口戦略を策定する

事務局	 新経済連盟 Japan Association of New Economy	内閣官房 Cabinet Secretariat IT室
民間企業及び関係省庁以外の参加組織	 JBA Japan Blockchain Association	  国立研究開発法人科学技術振興機構 研究開発戦略センター  IPA Better Life with IT 情報処理推進機構
形態	● 民間側は新経連、行政側は内閣官房IT室の共同事務局 ● 【ポストコロナの社会課題を解決する手段】として【ブロックチェーン技術】が適切と思われる事例について、事前に事務局にて情報収集する ● そのうち複数個の実装例につき、各回ごとにテーマを絞って議論 ● 議論の結果は翌年度IT戦略に反映する	
補足	● 民間企業の意見は新経連がJBA,BCCCなどの協力を得て整理する ● 原則、非金融分野を取り上げる。金融分野では既に制度整備が進んでおり、民間からの制度改善要望等は本協議会のテーマとしない	

本会合の構成員

氏名(敬称略)	所属
座長 楠 正憲	Japan Digital Design株式会社 CTO 内閣官房 政府CIO補佐官
加納 裕三	一般社団法人日本ブロックチェーン協会 代表理事 株式会社bitFlyer Blockchain 代表取締役
平野 洋一郎	一般社団法人ブロックチェーン推進協会 代表理事 アステリア株式会社 代表取締役
増島 雅和	森・濱田松本法律事務所 パートナー弁護士
落合 孝文	渥美坂井法律事務所・外国法共同事業 パートナー弁護士
安田 クリスティーナ	Microsoft Corporation, Identity Standards Architect
福島 良典	株式会社LayerX 代表取締役CEO
小木曾 稔	一般社団法人新経済連盟 政策部長
向井 治紀	内閣官房情報通信技術(IT)総合戦略室 室長代理(副政府CIO)
江口 純一	経済産業省大臣官房サイバーセキュリティ・情報化審議官 内閣官房情報通信技術(IT)総合戦略室 室長代理(副政府CIO)
平井 淳生	内閣官房情報通信技術(IT)総合戦略室 参事官
窪山 富士男	農林水産省大臣官房 参事官
松田 洋平	経済産業省商務情報政策局情報経済課長

本会合のオブザーバ

区分	所属
中央官庁	内閣官房デジタル市場競争本部事務局、内閣府政策統括官(科学技術・イノベーション担当)付、内閣府地方創生推進事務局、金融庁、総務省、文部科学省、厚生労働省、環境省
地方公共団体	広島県、会津若松市、加賀市、茨城県
政府関係機関	国立研究開発法人科学技術振興機構(JST) 研究開発戦略センター(CRDS)、独立行政法人情報処理推進機構(IPA)
ブロックチェーン推進団体	一般社団法人日本ブロックチェーン協会(JBA)、一般社団法人ブロックチェーン推進協会(BCCC)
ゲストスピーカー企業等	株式会社野村総合研究所、NRIセキュアテクノロジーズ株式会社、一般社団法人OpenIDファウンデーション・ジャパン、合同会社Keychain、xID株式会社、ソラミツ株式会社、一般社団法人超教育協会、株式会社techtec、株式会社ソニー・グローバルエデュケーション、EYストラテジー・アンド・コンサルティング株式会社、アクセンチュア株式会社、トッパン・フォームズ株式会社、株式会社TRUSTDOCK
一般社団法人新経済連盟 会員企業	

開催スケジュール

開催回	開催日時	討論テーマ	ゲストスピーカー（敬称略）
第1回	9月17日(木) 14:00～16:00	趣旨説明 スマートシティ	広島県、加賀市、会津若松市
第2回	10月29日(木) 14:00～16:00	DID(#1)	野村総合研究所/NRIセキュア・テクノロジーズ、 OpenIDファウンデーション・ジャパン、 内閣官房デジタル市場競争本部事務局、 Keychain
第3回	12月3日(木) 14:00～16:00	DID(#2) 教育	xID、bitFlyer Blockchain、ソラミツ、 超教育協会、techttec、 ソニー・グローバルエデュケーション
第4回	1月14日(木) 14:00～16:00	配布 中央省庁取組	アクセンチュア、 EYストラテジー・アンド・コンサルティング、 総務省、経済産業省、農林水産省、 内閣官房情報通信技術（IT）総合戦略室
第5回	3月4日(木) 14:00～16:00	まとめ	

II. ヒアリング結果のまとめ

課題意識

ブロックチェーンの長所

- **高い耐改ざん性・透明性**（トレーサビリティ等）
- 取引における仲介者・中立的第三者が不要であり、**取引コストの削減や迅速化**（自動取引等）が見込まれる

…等

ブロックチェーンの短所（制約）

- 処理するトランザクションに対して計算量が膨大であり、**計算リソースや電力の使用効率が低い**、また**即時性に欠ける**
- パブリックBCにおける特定ユーザー（グループ）による過半の計算リソース掌握リスク

…等

**制約が顕在化せず利点を活かせるユースケースを見出し、
当該ユースケースにおける課題を明確化することが重要**

検討のフォーカス

1. ポストコロナ、ウイズコロナの社会課題において、先導的な活用事例のヒアリング調査を通じ、その解決手段としてブロックチェーンが有効と考えられる項目を洗い出す
2. 各課題において、ブロックチェーンを適用する上での課題（技術的・法的制約など）、得失について明確化し、今後の社会実装へ向けての必要事項を議論する
3. 上記課題を公共性が高い分野への出口戦略として考えるにあたり、民間及び行政における先導的取り組みの成果を共有するとともに地方自治体のニーズを把握して、適切な提案につなげる

地方公共団体のスマートシティ取組及びブロックチェーン活用の先進事例

ICT活用やスマートシティに向けた取組事例として、各地方公共団体では下記のように、農産物トレーサビリティ、ヘルスケアにおける情報共有、行政・公共情報の活用、行政手続きのオンライン化等のユースケースや、それらを支える情報基盤について、多岐にわたる分野で取り組んでいる。

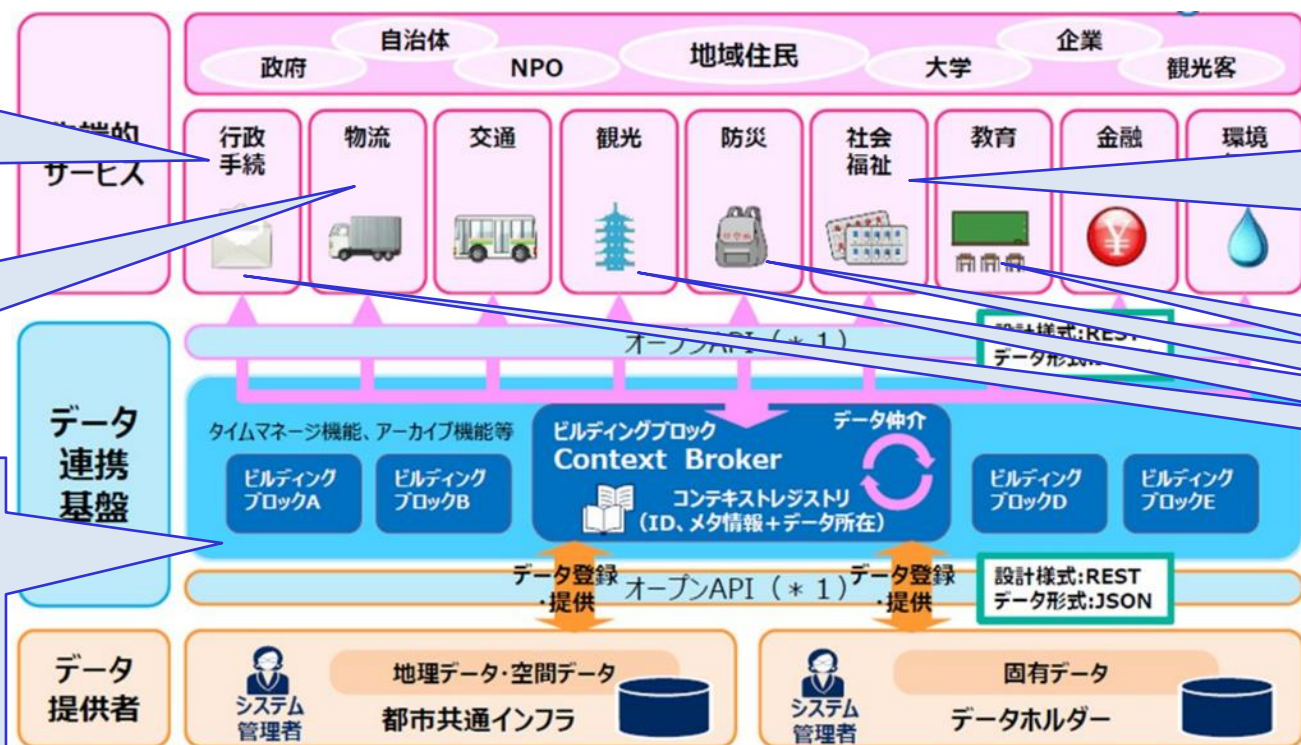
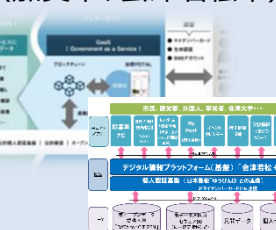
電子申請（加賀市）



農産物トレーサビリティ（広島県）



地方公共団体PF（加賀市、会津若松市）



ヘルスケア情報共有（広島県）



行政ポータル・公共情報ポータル（加賀市、会津若松市）



今後の活用促進のポイントとして、①ユーザの受容性観点では**住民への理解の浸透**や**レピュテーションリスクへの対処**、②サービス提供者観点では**ブロックチェーン技術のより深い理解**と**適切な設計ノウハウの習得**、③技術観点では**相互運用性の確保**、が挙げられた。

事業者等ヒアリングから得られた示唆①

■ 分散型IDを活用したID基盤の構築・提供における課題

➤ IDの有効性・安定性の確保

- 例えば既存の認証業務との関係

- 認証業務を行う特定の事業者が不在となるシステム構成の場合に、真正性確認の現在やあるべき姿とどのように整合させていくのか

➤ 公的資格など国・政府が提供するサービスとIDのリンクの確立

- システムにおける相互運用性

- 異なるブロックチェーン間の接続
- データ解釈など、高いレイヤでの接続

- 制度面における課題の整理

➤ 実装の考え方

- JPKI等の既存の認証の仕組みとのリンク

- 民間システムとのAPI連携

- 民間視点では「接続性の良い実装に」

事業者等ヒアリングから得られた示唆②

■ トレーサビリティ(ID基盤の利活用)における課題

- データのオーナーシップの整理とポータビリティの確保
 - ・ 個人と企業・団体の関係
 - ・ 複数企業間の関係
 - ・ データの内容によっては、オーナーシップの関係が複雑になる可能性
 - － データをある程度細分化したうえで、所有、制御実行、制御決定のシステム権限をそれぞれ設定するなどの整理が必要ではないか。
 - － 例えば、公開してよい情報とそうでない情報を、どのように整理・管理・制御できるか。
- 個人情報保護(含む2000個問題)との関係整理
 - ・ データのオーナーが自治体の場合のルール作り

■ 商用サービスにおけるノウハウ例

- 個人情報保護への対応として、ブロックチェーンにはハッシュや鍵だけを書き込み、データそのものはブロックチェーンの外に置いている例が多い

ブロックチェーンの特徴をふまえた留意事項

■ セキュリティの技術的要件と運用ルール

- ユースケースにより達成すべきセキュリティとそのレベルは異なることから、その見極めが必要
 - ユースケースに応じた適切なアーキテクチャの選択
(例えば「51%攻撃リスク」が懸念される用途における、プライベートBCの採用)
 - 市場のブレーキングチェンジへの対策
- 個人情報など秘匿性が必要なデータを扱う可能性があるユースケース等における技術的制約の認識・理解

■ トランザクションに対するスケーラビリティ、計算リソース・計算量

- 最終的にはトランザクション量と処理速度とシステム規模のバランス、例えば下記のような方策により落としどころを見つけていく必要がある
 - トランザクション更新の頻度を下げる
 - BCに書き込むデータサイズを削減する
 - データそのものを小さく
 - サイドチェーンなどの技術による計算の分散
 - パブリック・プライベート・コンソーシアム型の使い分け(=合意形成方式を変える)
 - 計算リソースを増やす
- 例えばマイクロペイメント等のユースケースではトランザクションを処理しきれない場合の影響大

今後の検討の方向性①

- 政府では、デジタル・ガバメント実行計画を策定し、情報セキュリティ対策の最新化等に対し、民間の人材・知恵やオープンな技術を活用するなど技術トレンドに対応する方針を示している。
- また、今後、デジタル庁の設立を見据え、政府等の情報システムの整備方針を策定することとしている。
- 整備方針は特定の技術の採用を前提とするものではないが、今後の情報システムの設計・構築にあたっては、目的や要求仕様に応じて、新技術導入の利点・欠点を客観的に分析・検討し、最適な技術の採用を図る必要がある。ブロックチェーンの活用についても、先導事例で示唆された利点・先進活用事例、及び、課題・留意事項を踏まえて検討することが重要。

デジタル・ガバメント実行計画（令和2年12月25日閣議決定）の記述

情報システムに関する技術トレンドへの対応

- ・情報システムは、汎用技術の組合せにより整備されており、日々変化する技術トレンドに対応していくことが重要である。現状、どのような技術を採用するかは情報システムごとに判断されているが、技術トレンドに対応した製品・技術の選定や情報セキュリティ対策の最新化に対して、政府全体としてのガバナンスが効きにくくなっている。今後、民間の人材・知恵やオープンな技術を活用しつつ徹底した見直しを行うことで、事業者の提案への過度の依存による、いわゆるベンダーロックインから脱却するとともに、今後主流になると考えられる技術の導入を進めていく。
- ・情報システムの技術トレンドへの対応方針、脱却すべき技術、今後採用すべき技術及びこれらに関する移行方針について、継続的な検討と見直しを実施する。

整備方針における検討事項

国・政府が提供するサービスにおけるインターオペラビリティ

- ・庁内連携・団体間連携・民間との対外接続に一貫した設計で対応できる仕組みが必要ではないか。
 - ・そのために、後方互換性を維持したまま柔軟にデータ項目などの仕様を拡張でき、中央サーバーを介在させずにリアルタイムでシステム間のAPI連携ができる、柔軟かつ簡素な構成とすることができないか。
 - ・分野ごとに定められる、データの相互運用性を確保するための標準的なデータ交換モデル（※）が必要ではないか。
- （※） 参照モデルとも呼ばれ、データ項目やメタデータの関係性を整理するもの。

今後の検討の方向性②

民間システムとのAPI連携

- ・公費で作られたデータは原則として民間に提供していくオープンバイデフォルト原則に基づき、**原則としてAPIの公開又は提供を検討すべき**ではないか。

データのオーナーシップの整理とポータビリティの確保

- ・濫用や漏えいによる問題が発生したり、プライバシー侵害が発生したりすることのないよう、**データベースの分散管理**とアクセスコントロールを前提に、新たな手法を検討すべきではないか。

※個別分野での取組の例

- ・学習者のIDとマイナンバーカードとの紐付け、転校時等の**教育データの持ち運び**
- ・保健医療情報の適切かつ効果的に活用できる環境の整備

個人情報保護

個人情報保護（含む2000個問題）との関係

- ・近年、情報化の進展や個人情報の有用性の高まりを背景として、官民や地域の枠を超えたデータ利活用が活発化しており、民間、行政機関、独立行政法人等、地方公共団体の個人情報の保護に関しては、それぞれ異なる法律や条例により規定され、現行法制の縦割りに起因する規制の不均衡や不整合がデータ利活用の支障となっていると指摘されている。
- ・国の行政機関、独立行政法人等に係る個人情報保護制度について、個人情報保護法と統合するとともに、地方公共団体の個人情報保護制度についても全国的な共通ルールを法律で規定した上で、これらの制度を個人情報保護委員会が一元的に所管する仕組みとすることとし、このための個人情報保護法等の改正法^(注)が5月12日に可決・成立した。

(注)「デジタル社会の形成を図るための関係法律の整備に関する法律」

[参考 1] 事例集

※ 各講演内容及び資料に基づき、事務局にて作成
※ 図表等は各講演資料より転載

ひろしまサンドボックスにおけるブロックチェーン活用の事例として、以下に取り組んでいる。

- ① 島しょ部傾斜地農業に向けたAI/IoTの適用（レモンプロジェクト）
- ② 県民の医療・健康等個人情報管理への適用（医療プロジェクト）

【レモンコインによる農産物取引へのブロックチェーン活用】

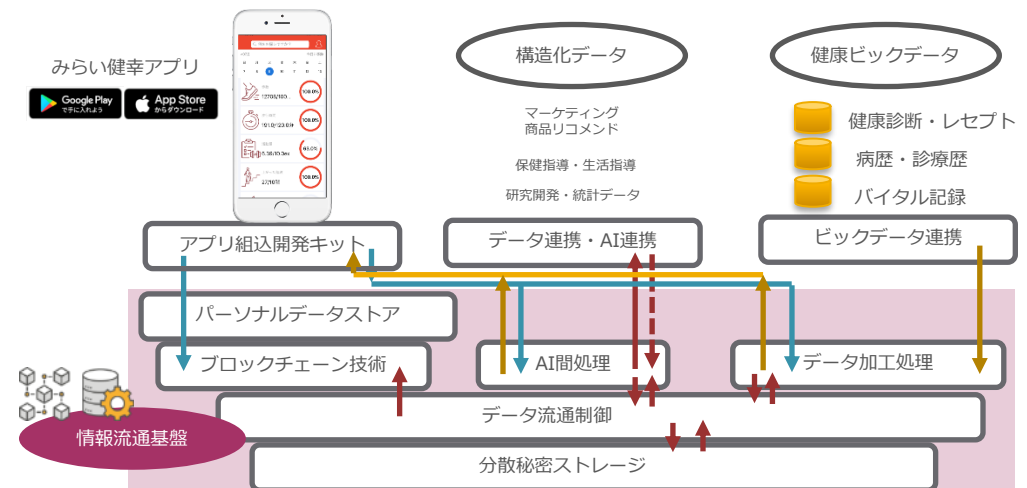
ブロックチェーンを活用した新規事業アイデアの創出プロジェクト「クロステックチャレンジ」で取組中。AI/IoT/ロボット等の活用で農業における地域課題の解決と活性化を図り、生産者の人手不足解消を目指す。

レモンコインのフロー 兼 クロステックメンバーステークホルダー



【ブロックチェーン型情報管理と情報信託機能を付与した情報流通基盤の構築】

個々人が自身のデータを把握しセキュアに管理するとともに、個人の判断で第三者へのデータ提供や対価の授受ができる情報信託機能を、AI/IoTプラットフォームに付加することで、データ流通を促進する。現在、ヘルスケア用アプリを公開中。

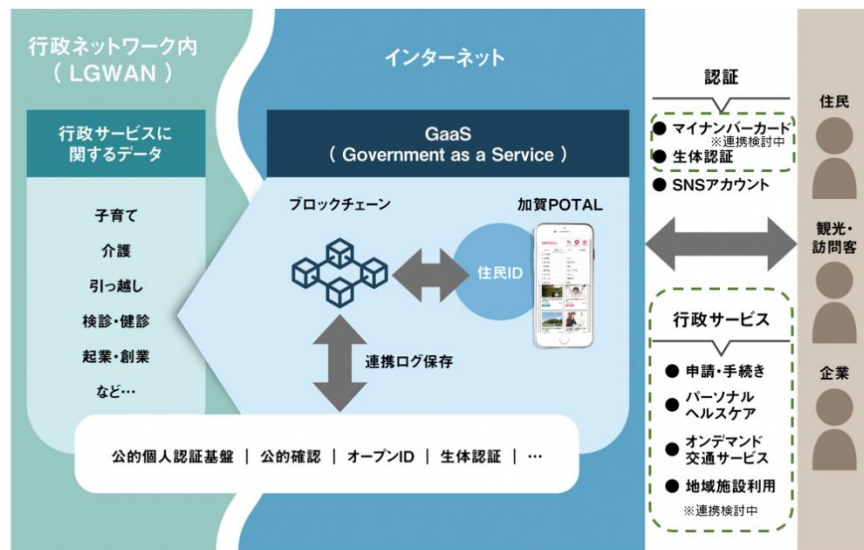


「市民のQOL向上、来訪者の満足度向上、稼ぎ力の向上」を目指し「スマートシティ加賀」を推進、特にブロックチェーン活用に関して、以下に取り組んでいる。

- ① 自治体サービス基盤へのブロックチェーン適用実証中（加賀POTAL）
- ② マイナンバーやスマートフォンと連携した電子行政実用化の取組

【加賀POTALのシステム全体構成】

登録した個人の属性（生年月日、地域、家族構成など）に応じて、市政情報や施設等の情報をカスタマイズし提供。ログインやサービス利用ログの記録にブロックチェーンを活用。



【xIDを活用した行政サービスの電子申請を開始】

トラストバンク社提供の行政向け申請ツールに個人認証・電子証明の機能をxIDで組み込んだ「LoGoフォーム電子申請」は、マイナンバーカードとスマートフォンアプリで申請可能。認証と電子証明のログ記録にブロックチェーンを活用。



- ・「対面・紙・ハンコ」に頼らず
- ・マイナンバーカードによる個人認証
- ・スマートフォンから行政手続
- ・ブロックチェーン技術による改ざん防止

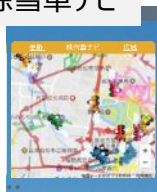
加賀市、トラストバンク、xIDによる記者会見
(2020年8月12日)

「スマートシティ会津若松」の全体像とこれまでの取組、主な事例としてレコメンド型の情報提供プラットフォーム「会津若松＋(プラス)」と、その全体アーキテクチャ等が紹介された。

【会津若松＋(プラス)】

登録した個人の属性（年齢・性別・家族構成、趣味嗜好等）に応じて、必要な情報をおすすめ表示したり、各種サービスと連携。
ヘルスケア実証におけるデータ閲覧ログにブロックチェーンを活用。

除雪車ナビ



母子健康情報
サービス



あいづっプラス
(学校情報配信)



ポータル画面



LINE de ちゃチャット
問い合わせサービス

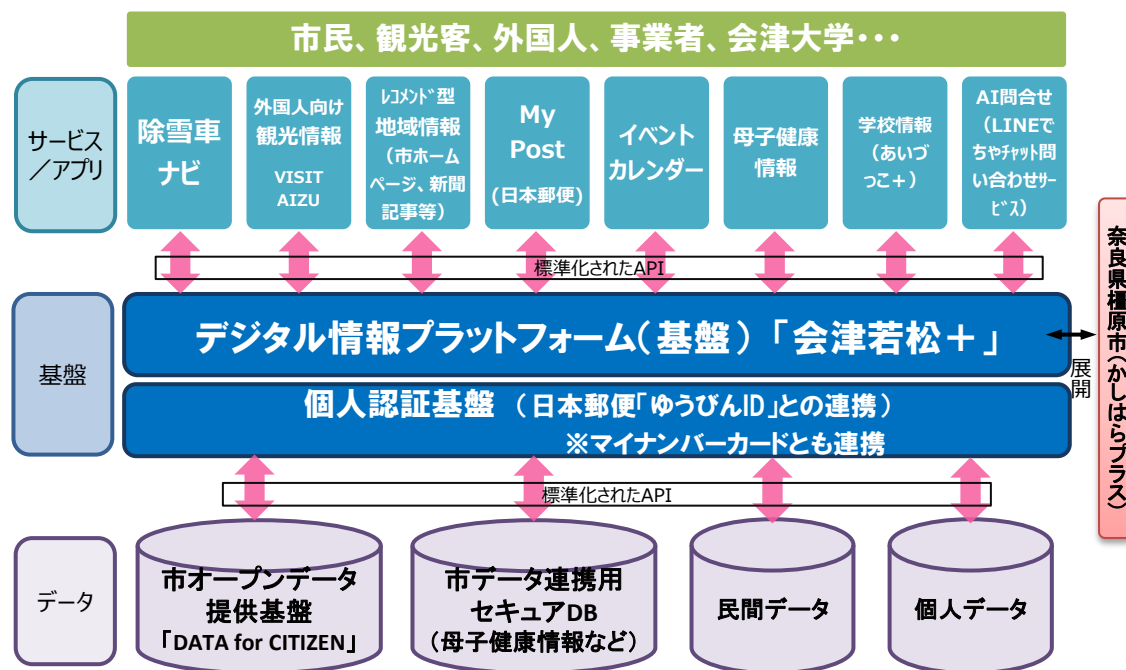


ヘルスケア
実証



【会津若松市の「デジタル情報プラットフォーム」のイメージ】

まちで生活していく上で欠かすことのできない基盤、いわゆる「都市OS」とも言えるものを目指し、様々なデータとサービスを連携することで各種サービスを充実。このような標準化されたアーキテクチャの横展開により、サービスの相互展開などが行いやすくなることで、持続可能で力強い地域社会の実現を目指す。

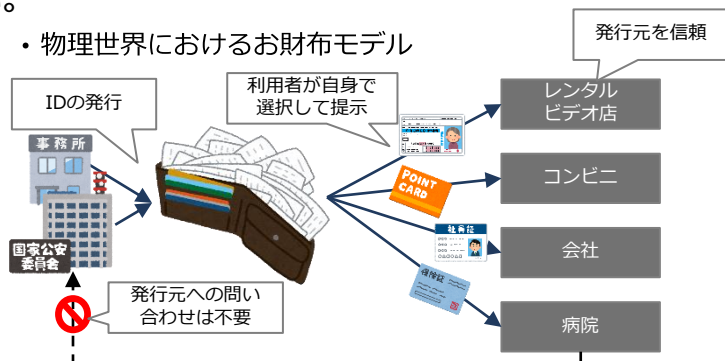


デジタルID分野における検討に基づき、SSI/DIDの概念・定義や、それらのブロックチェーンとの関係性、適用形態の考え方等が紹介された。

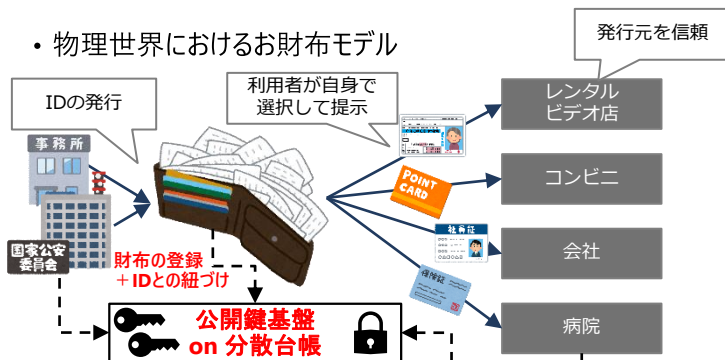
【物理世界におけるIDとのアナロジーによるモデル】

発行元への問い合わせを不要としつつ、発行されたものの信用を担保する仕組みとして分散台帳上の公開鍵基盤が有望であり、ブロックチェーンとの親和性が高い。

・物理世界におけるお財布モデル



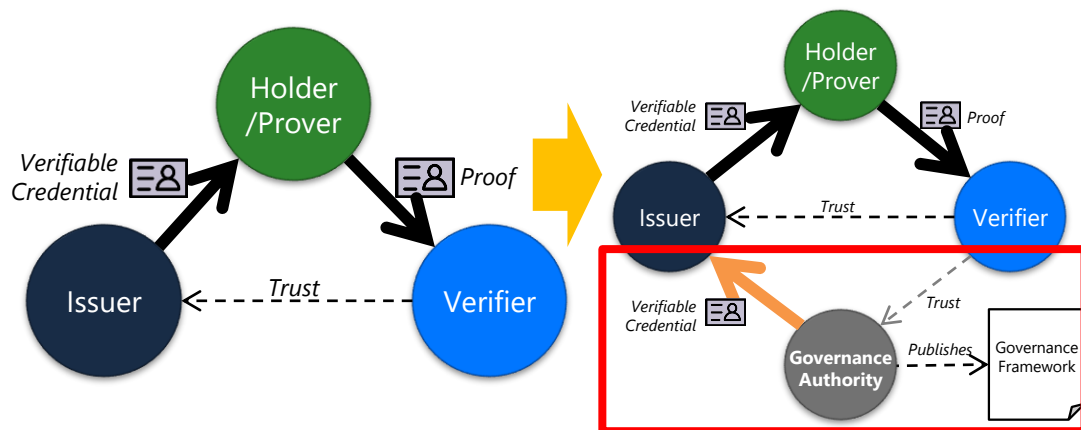
・物理世界におけるお財布モデル



【DIDにおけるステークホルダーの関係】

DIDの発行者（Issuer）、所有者（Holder）、検証者（Verifier）の間でやり取りが行われる。

Issuerの発行の法的根拠を担保する方法として、信頼された証明体（Governance & Authority）と連携することを検討可能。



【DIDにおける分散台帳の使いどころ】

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

Verified Credentials：検証を継続的に行うためにパブリックチェーンが有効

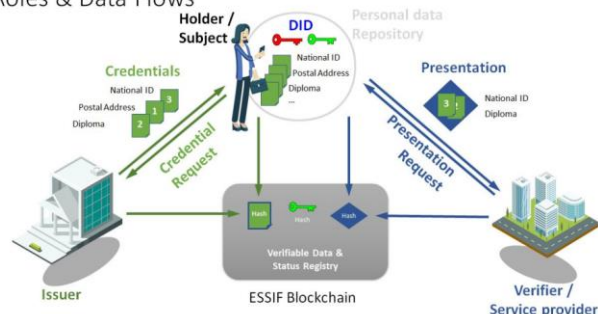
海外におけるSSI/DIDの導入事例として、ESSIF、ドイツ連邦印刷会社、バルセロナ市とアムステルダム市のパイロットプロジェクト「DECODE」の事例が紹介された。

【European Self-Sovereign Identity Framework (ESSIF)】

欧州委員会と欧州ブロックチェーンパートナーシップの共同イニシアティブとして、欧州ブロックチェーンサービスインフラプロジェクトが進行中。

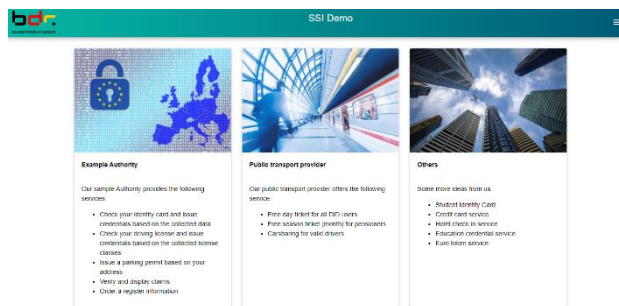
本プロジェクトではEU横断でEU市民が様々なサービスで活用できるSSI/DIDベースのアイデンティティモデルを構築予定。

Roles & Data Flows



【ドイツ連邦印刷会社の取組】

市民はSSIウォレットを搭載したモバイル端末に国民IDカードや運転免許証、住民票等の行政機関が発行したデジタル版証明書を取得できる。市民はこれを再利用して、様々な公的・民間部門のサービス（カーシェアや学生証の受取り、公共交通機関の割引など）を利用。2020年度中の本格導入に向けて検討中。



【Decentralized Citizen-Owned Data Ecosystem (DECODE)】

アムステルダム市では「匿名での身分証明」を行う実証を実施。パスポートのRFIDチップを元にQRコードを作成し、そのQRコードの提示で身分証明が可能。

居住地のみ、年齢のみ等の提供を実現する仕組みとして本実証を実施し、スマートシティにおけるデジタルアイデンティティの活用モデルとしての可能性が示された。

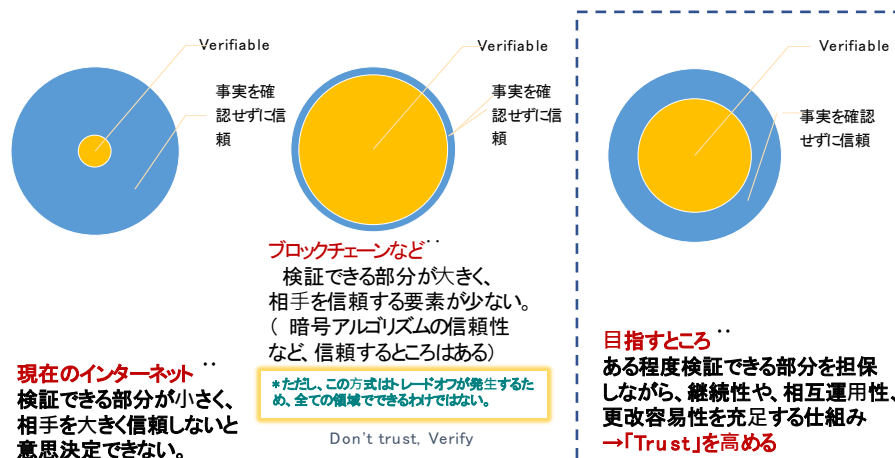


特定のサービスに依存せず、識別子の管理も含め、データのコントロールや合意形成の仕組みを取り入れて検証できる領域を拡大し、インターネットの上に重ね合わせていく仕組みとして、「Trusted Web」を推進。(3月にホワイトペーパー公表)

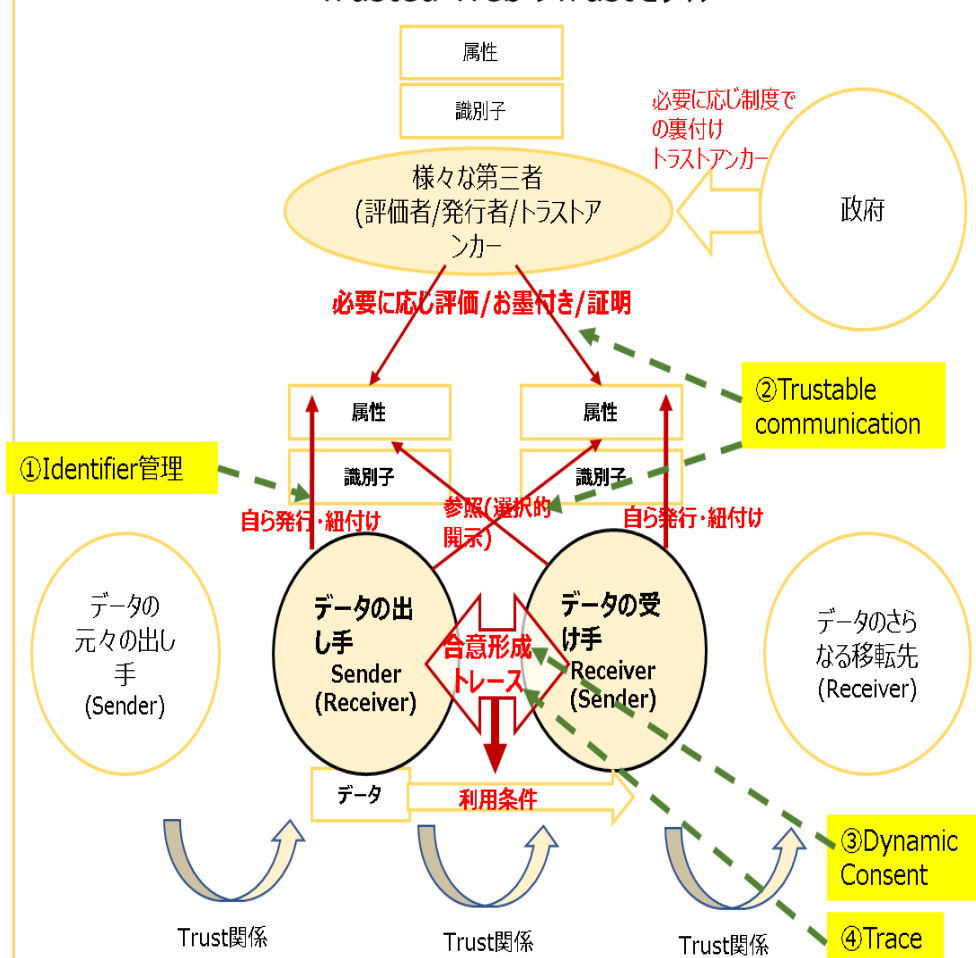
- 目的**：デジタル社会における様々な社会活動に対応するTrustの仕組みをつくり、多様な主体による新しい価値の創出を実現。
- Trustの仕組み**：特定サービスに依存せず、
- ・相手に開示するデータのコントロールを可能とし、
 - ・データのやりとりにおける合意形成の仕組みを取り入れつつ、
 - ・検証（Verify）できる領域を拡大し、これまで事実を確認せずに信頼していた領域を縮小することにより、Trust（相手が期待したとおりに振る舞うと信じる度合い）を高めていく。
- アプローチ**：インターネットとウェブのよさを活かし、その上に重ね合わせるオーバーレイのアプローチ
- *Trust: 事実の確認をしない状態で、相手先が期待した通りに振る舞うと信じる度合い

目指すべき方向性

仕組みによりVerifiable(検証可能)な部分が変わる



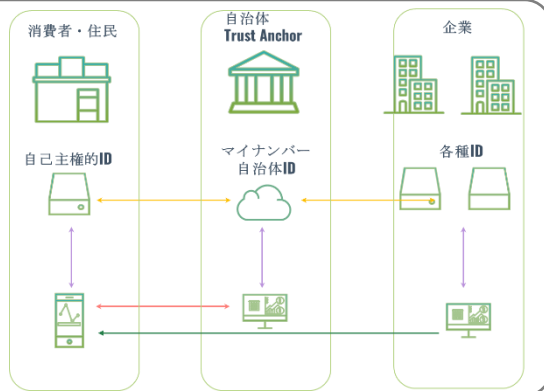
Trusted WebのTrustモデル



開発環境Keychain COREを提供、官民のID連携、医療データ連携、IoT認証、環境価値取引、トレーサビリティ等のユースケースでの活用を見込む。

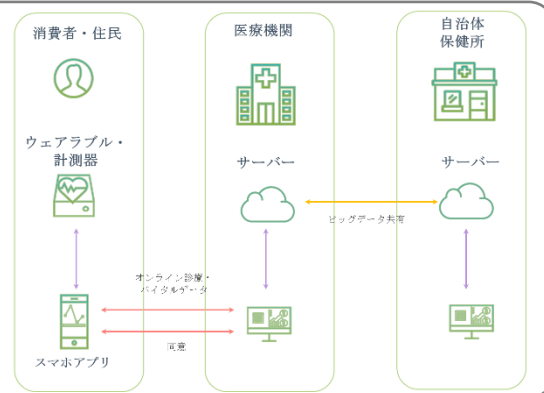
【官民のID連携】

トラストアンカーとの連携により、企業と個人の間のデジタル取引の信頼性を向上。
自治体が住民票や自治体ごとのカスタマイズ情報をセキュアに通信可能。



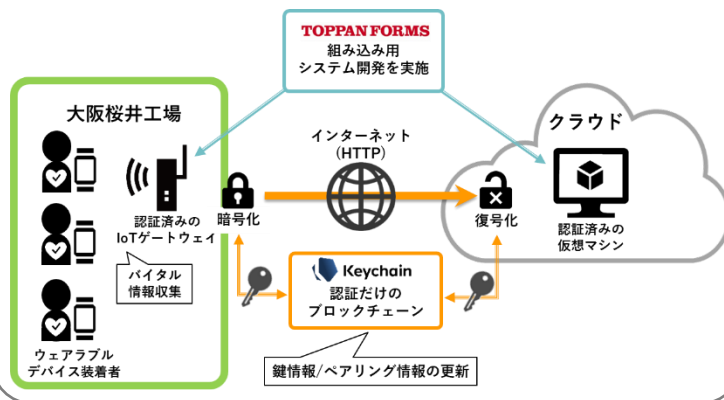
【オンライン診療・医療データ連携】

ウェアラブルデバイス等から取得したデータの本人同意に基づく流通制御により、PDSの利活用を促進し、診療精度向上等を目指す。



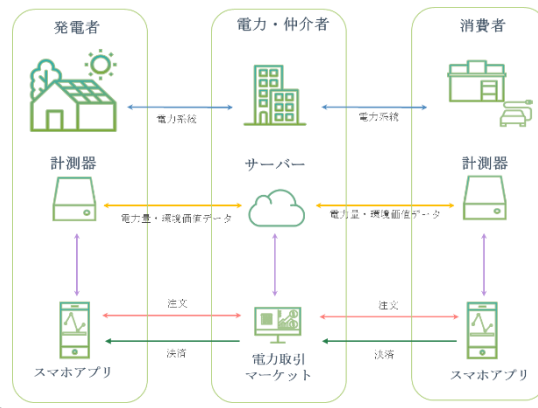
【IoT認証】

認証情報の通信と暗号化されたデータ本体の通信を分離し、前者のみブロックチェーンで扱うことで、セキュリティと端末数の増加に対するスケーラビリティを両立するアプリケーションを実現。



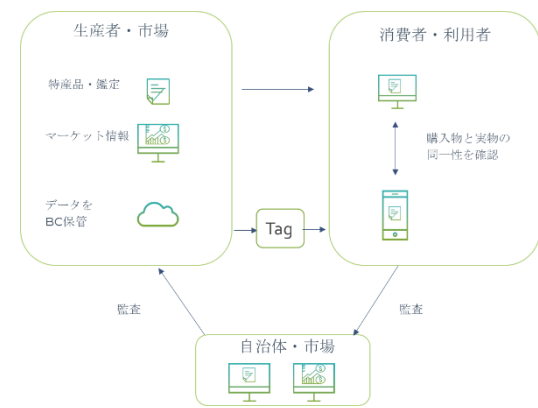
【環境価値取引】

環境価値等の取引プラットフォームとしてブロックチェーンを活用することで、電力の効率的利用等を目的とした個人間での安全な取引を実現。



【トレーサビリティ】

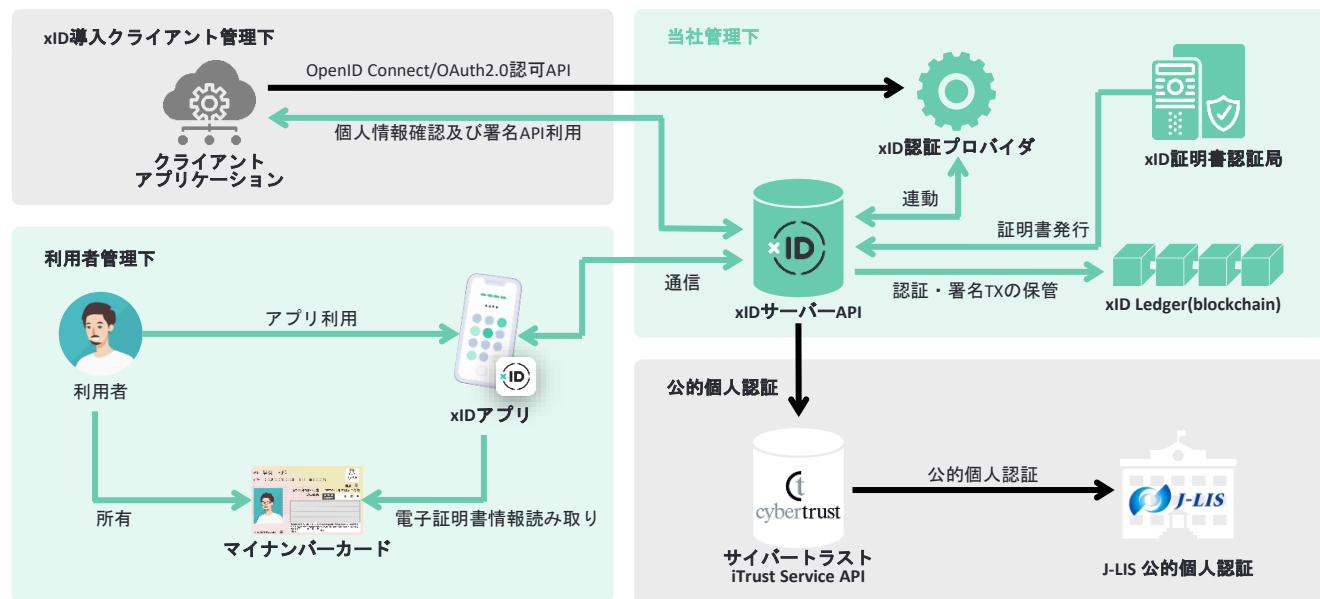
出荷時の箱やタグと紐づけてDIDや付帯情報等を登録しトレースすることで、偽造品の検知を可能とし、特産品・ブランド品流通の信頼性を向上。



マイナンバーカードと連携したデジタルID「xID」を開発、複数サービスで統一的に利用できるIDの実現を目指す。

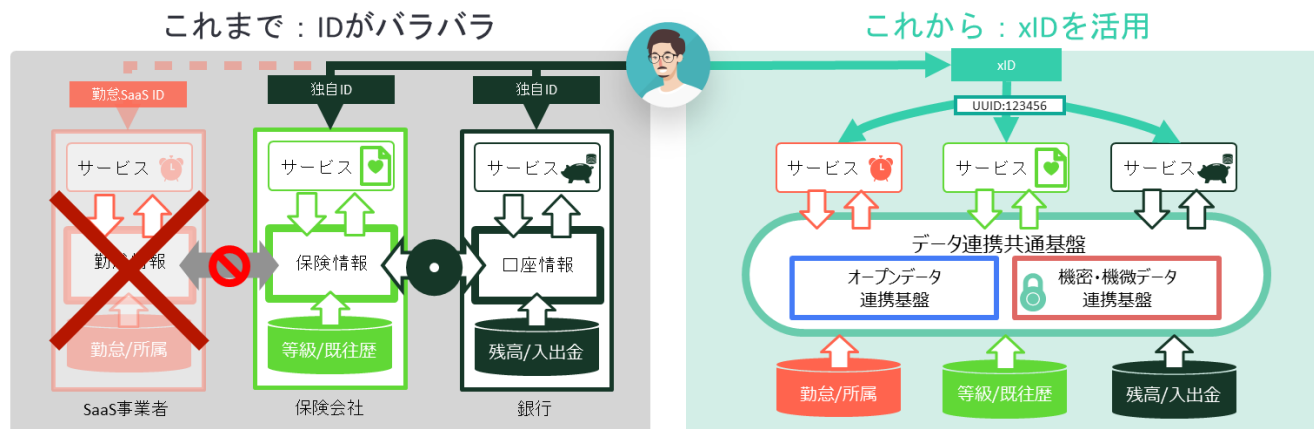
【xIDの基本構成】

xIDサーバAPIを介してスマホアプリ、サーバアプリ、公的個人認証が連携。
xIDサーバは個人情報確認、電子署名、電子認証、マイナンバー要求等の機能をAPIで提供する。
xIDサーバへのアクセス履歴の保管にブロックチェーンを活用。



【データ連携基盤とxIDで実現するパーソナルデータの連携】

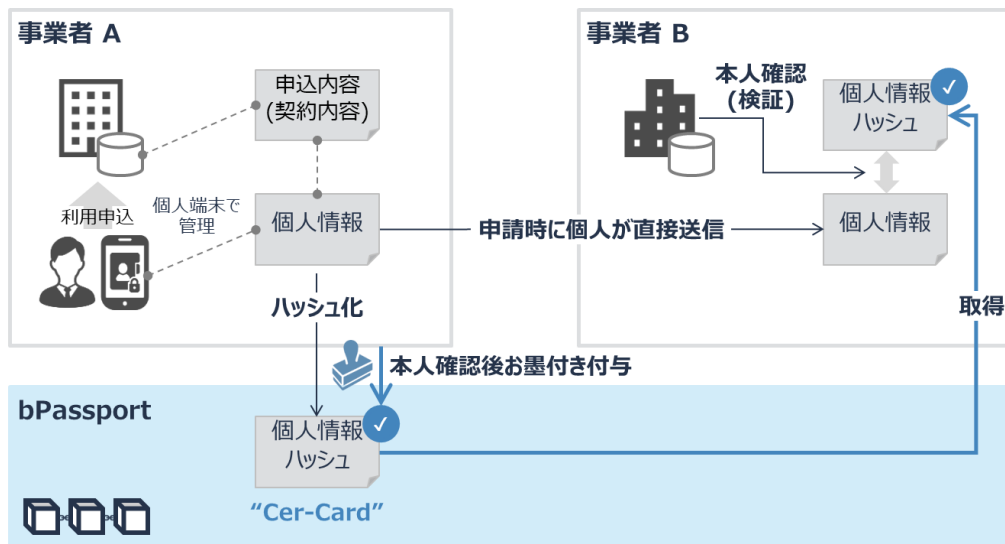
xIDを用いた本人認証の共通化により、本人同一性、一意性を担保。サービスをまたいだユーザデータ連携が可能となる。公共性の高い民間デジタルIDを用いることにより、情報連携の拡張性が高まる。



プライベートブロックチェーンmiyabiを活用した、自己主権型アイデンティティと分散型IDの基盤であるbPassportを提供。

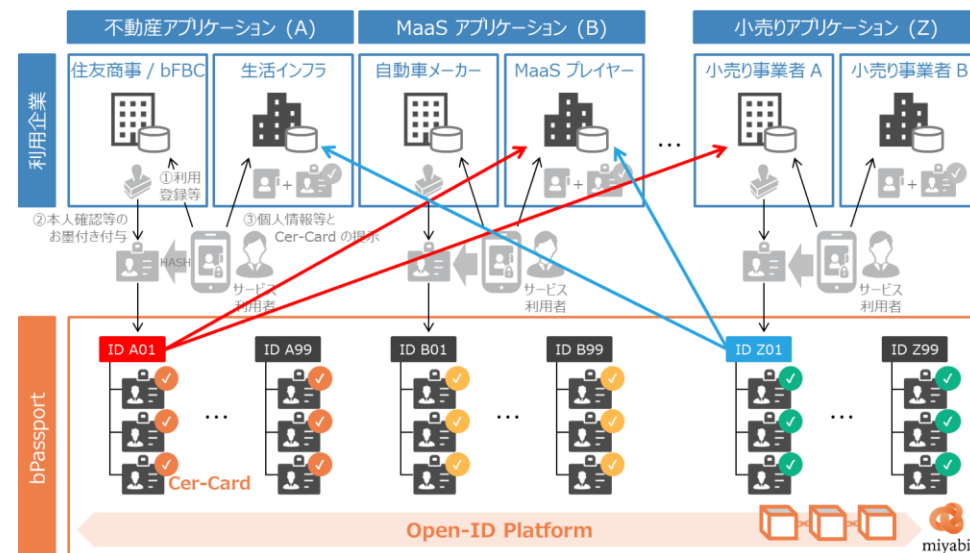
【bPassportの利用イメージ】

bPassportでは、個人情報の真正性を証明する“お墨付き”であるハッシュをブロックチェーン上で管理。ユーザが管理・保有する個人情報に対し、その情報を保証・証明する事業者が個人情報のハッシュをbPassportに登録。他事業者は、ユーザから直接受け取った個人情報を、bPassport上のハッシュと照合することでその個人情報の真正性を確認。ユーザが自身の情報に関する制御権を確保しながら、他者による本人確認を可能とする。



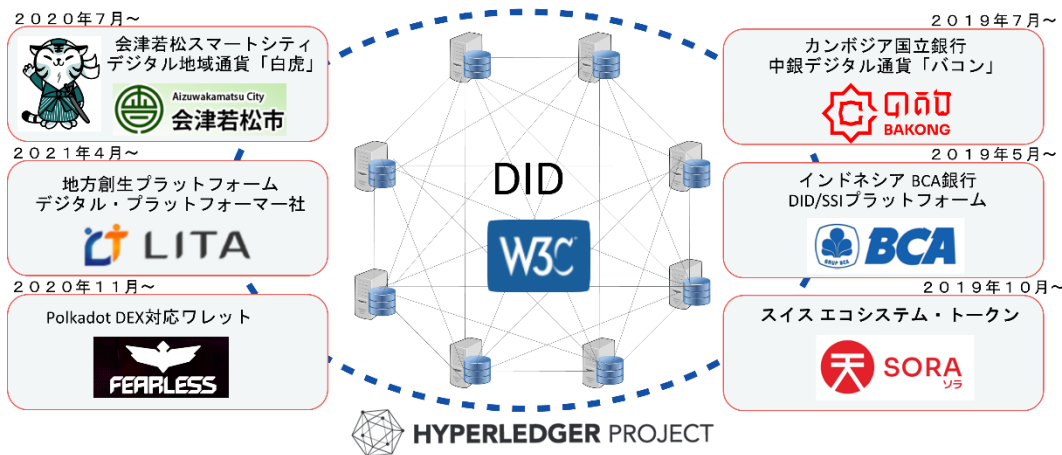
【将来的なID利活用の構想】

bPassportはOpen-IDであり、サービス横断での認証機能、ユーザの本人確認やサービス適合性判断向け認可機能を提供。将来的には各プラットフォーム内に所属する利用企業間のID連携、プラットフォーム間での相互送客等への展開を目指す。

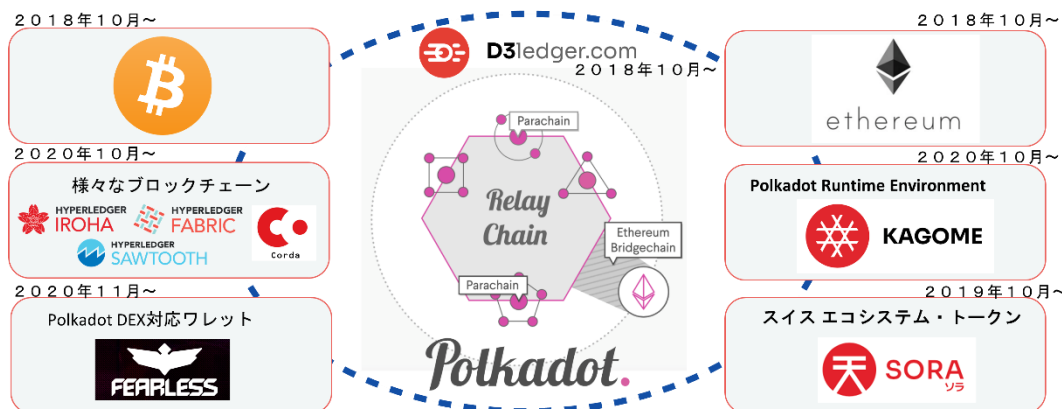


HyperLedger Irohaを基盤としたDIDが、デジタル通貨、本人確認、暗号資産ウォレット等に活用されている。DIDのグローバルな相互運用も視野に、プロジェクトが立ち上がっている。

【ソラミツ社のDIDの活用実績】



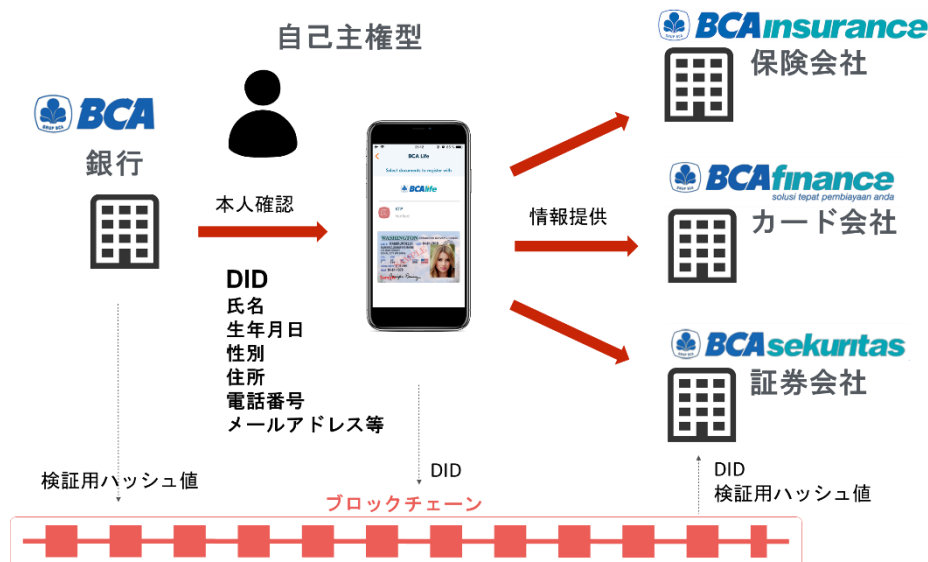
【ブロックチェーン間のインターオペラビリティ開発】



【インドネシアにおける銀行の本人確認プラットフォーム】

インドネシアBCAで一度本人確認を行うと、傘下企業での本人確認も簡易化。

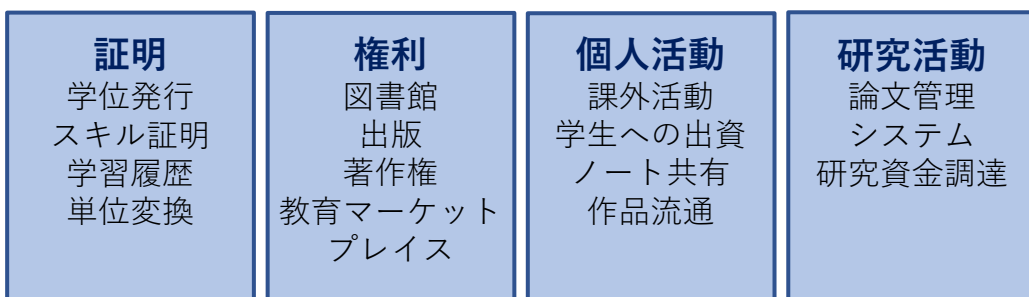
DIDのアーキテクチャに則したシステム構成となっている。ブロックチェーンには、個人情報の検証用のハッシュ値を保存、非改竄性を担保。



IoT、ブロックチェーン、AIなどの超スマート技術がもたらす教育（超教育）の実現に向けた検討の一環として、様々なユースケースでのブロックチェーン活用の可能性についてもWGを立ち上げ研究中。

【ブロックチェーン×教育 活用例】

現時点での応用は証明書発行にとどまっているが、ブロックチェーンが普及した状況を想定し、様々な活用可能性について検討。



証明

- 学歴から個別のスキルまで
→学習履歴を含む個性を表す情報を記録
自由度の高い学習環境・進路設計
- 履歴書から学習履歴書へ
→デジタル証明が可能となり就活等へ応用

権利

- 教育向けマーケットプレイス
→講義や教材を取りし、単位を与えることが可能に？
- 著作物の権利への応用
→権利の流れをブロックチェーンで管理し講義へ活用

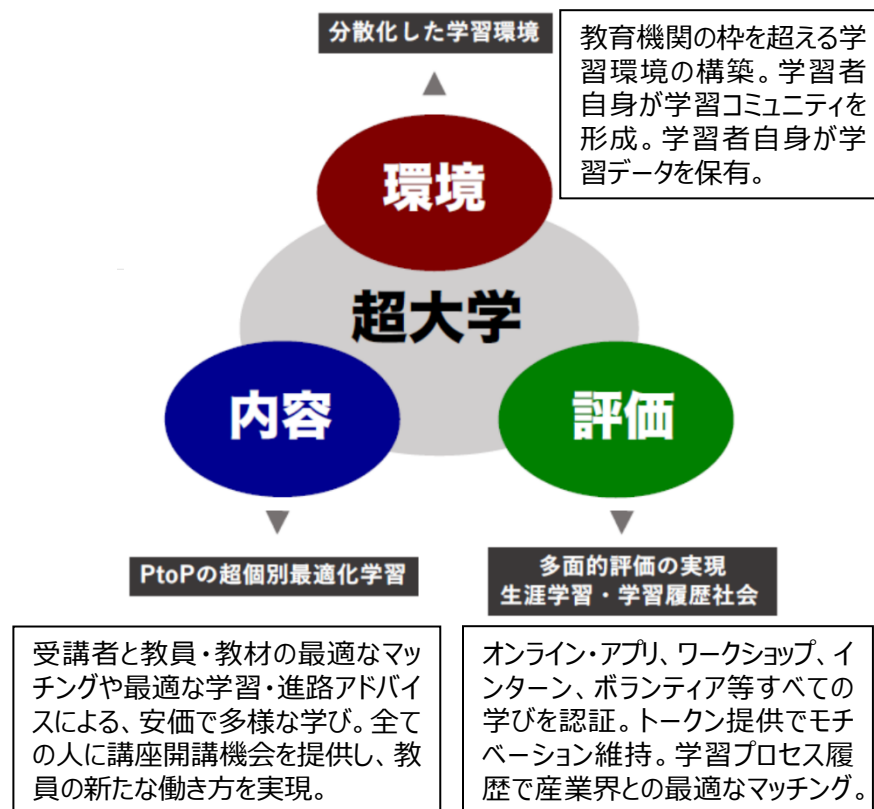
個人活動

- ボランティアやチャリティー活動を証明
→参加履歴を記録し実績を付与など
- 学生への出資
→経済的支援をするプラットフォーム

研究活動

- 研究管理プラットフォーム
→論文やデータを適切に管理するプラットフォーム
- 論文承認システム
→引用論文からの承認・通知等、研究活動の活性化

【ブロックチェーンが重要な役割を担う可能性】



教育データをブロックチェーンで管理する基盤としてPoLを提供。学位・研究データの不正防止、学位・学歴の確認コスト削減、オンライン学習の継続率改善、学習プロセス評価の実現を促進する。



【PoLが解決する課題】

学位や研究データの詐称による不正の防止や、その不正の有無を確認するための手間の削減をもたらす。また、トークン獲得やプロセス評価による日々の学習のインセンティブ向上が図れる可能性がある。

【ブロックチェーンによる教育データの管理プロセス】

オラクル問題（ブロックチェーンに記録する時点でデータに誤りがあった場合に意味をなさなくなる）に対するアプローチとして、証書等ではなく学習行動そのものに対してトークンを発行することで、本当に学習した実績をブロックチェーンに記録。



01

学位・研究データの不正

ブロックチェーンによって保証された正しい学位証明が実現する。論文や研究データの不正利用も発生しない。

02

人事部の確認コストが肥大化

学位の詐称を前提としない仕組みの上では、 unnecessary 確認コストを削減することができる。

03

オンライン学習における継続率の改善

学習するほどトークンが獲得できるため、学習意欲が高まり継続率を向上させることができる。

04

学歴社会の弊害

プロセスに焦点があたりにくい学歴社会とは別の評価軸として、学習歴社会の実現が近づく。

ブロックチェーンを活用した学習サービスの例として、「学籍情報のデータベース」「学習に関する多様な情報のユニバーサル・データストア」「教材等コンテンツの権利情報の保証」に関する実証実験を実施。

【貴重な学籍情報の記録】

世界算数（Global Math Challenge）の成績証明や、外国人留学生在が来日前に得た日本語検定結果、小中学校におけるロボットプログラミングの授業の学習実績管理を、ブロックチェーン基盤で提供し、情報の真正性を保証。



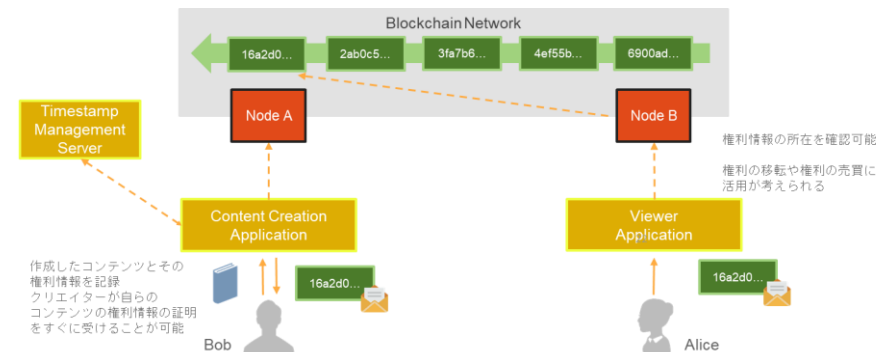
【ユニバーサルデータストア】

高校生のインターンシップ先での所見を、学外活動の情報として高校側で閲覧可能とするなど、学内・学外のデータ授受を検証。評価データはブロックチェーンに直接保存。



【権利情報を保証する基盤】

作成したコンテンツとその権利情報をブロックチェーン上に記録し、クリエイターが自らのコンテンツの権利情報の証明を受け取れるような著作権管理スキームについて実証実験中。



自治体や小中高の保有するビッグデータをAI分析し、アドバイスや教材の個別化、進路支援等に活用する実践研究事業を埼玉県と取り組み中。

県に蓄積されたビッグデータ



ビッグデータのAI分析



小中高の学校が保有するデータ

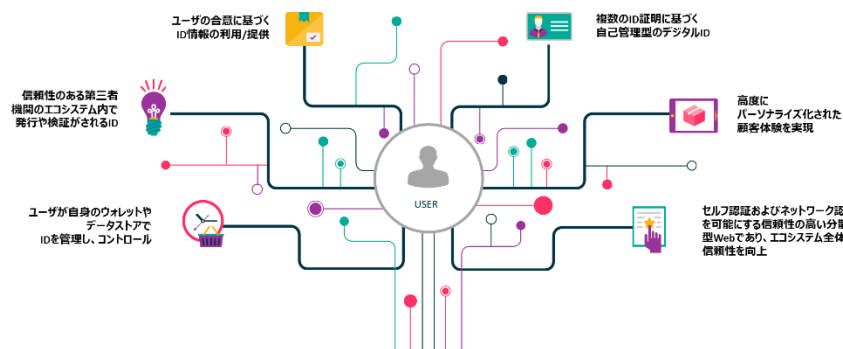


AI分析結果の活用の実践・検証

ID管理やサプライチェーン等の分野を中心にブロックチェーンの活用に取り組んでいる。デジタルID基盤、KTDI、給食配給に導入している他、電子カルテ・雇用プロセスの透明性向上・災害時等の物品配布への応用に可能性あり。

【IDENTITY REDEFINED】

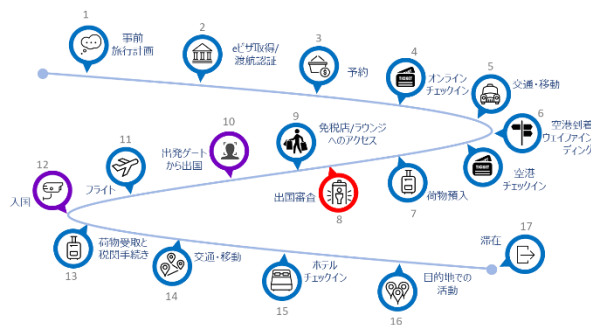
中央管理型から分散型で自己管理可能なデジタルIDへ、ID再定義の必要性を指摘。



【KTDI : Known Traveller Digital Identity】

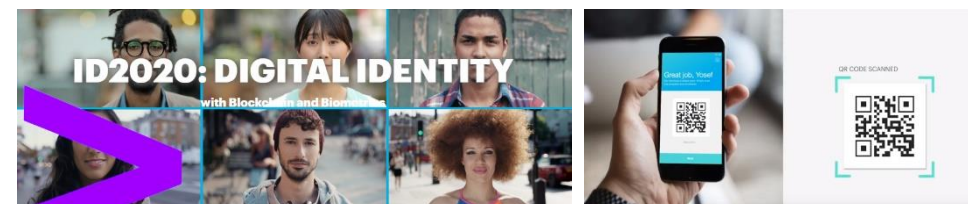
世界旅行のセキュリティ強化のために、世界経済フォーラムが取り組む国際コンソーシアム。

Hyperledger Indyを基盤に使用。カナダ・オランダでパスポートフリー入国の試験導入がされている。



【ID2020】

世界のすべての人々にユニークで公的なデジタルIDを提供するという、SDGsの目標を推進する官民コンソーシアム。アクセンチュア、Microsoft、Advanceが提携し、ブロックチェーン等の最新テクノロジーを活用したプロトタイプを開発、発表。



【NPO法人Akshaya Patraによる給食配給】

低所得者の子供向けの公立学校での給食提供プログラムについて、AIによる需要予測、IoTを活用した調理プロセスの最適化、ブロックチェーンによる透明性が確保された管理などにより、提供可能な給食数を指数関数的に増加させることに成功。毎年100万食を増やすことを目標としている。

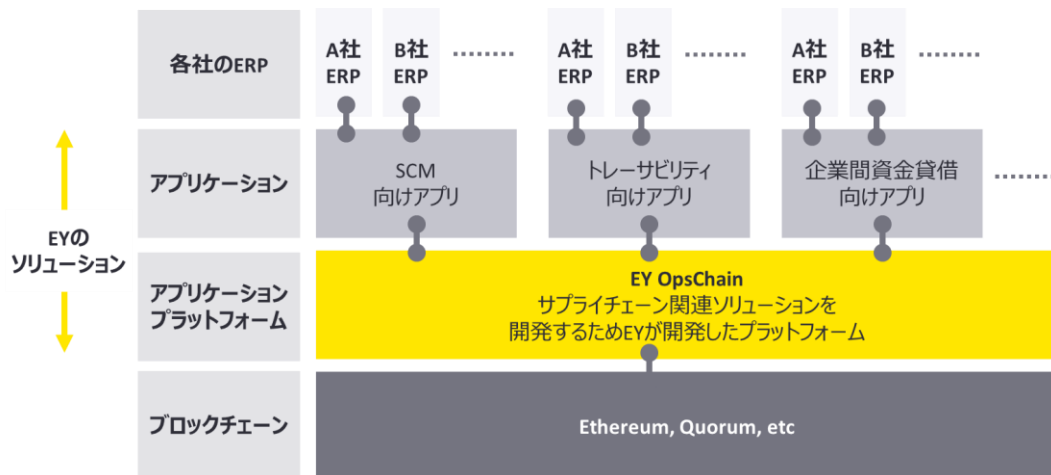


EYは、様々なブロックチェーンやシステム・サービスを連携可能な基盤であるEY OpsChainを提供。特にモノのトレーサビリティへの応用としてワイン、水産物等の食品流通で活用。その他にも製造業のSCM、環境価値取引、動物用ワクチン配布等にも取り組んでいる。

【EY OpsChainのアーキテクチャ】

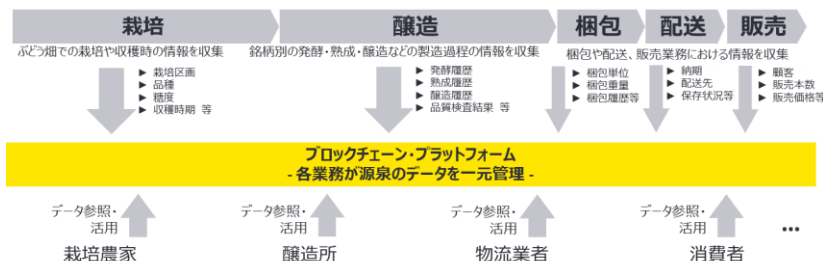
ブロックチェーンに必要なID管理やトークン管理などの共通機能を持ったソリューションであるOpsChainを展開。パブリックやプライベートのブロックチェーンと接続可能、また一方で企業のERPとも接続可能なミドルウェア。

同ミドルウェア上でのアプリケーション群として、例えばサプライチェーン管理、トレーサビリティ、金融向けアプリ、シェアリングエコノミー、予算管理等もリリース。



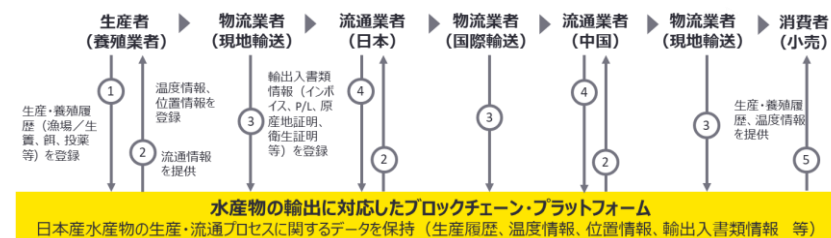
【ワインブロックチェーン】

ブドウの栽培からワインの醸造、物流までの状況を小売業者や消費者に提示、ワインの偽造品を見分けることを可能とする。



【水産物のトレーサビリティ】

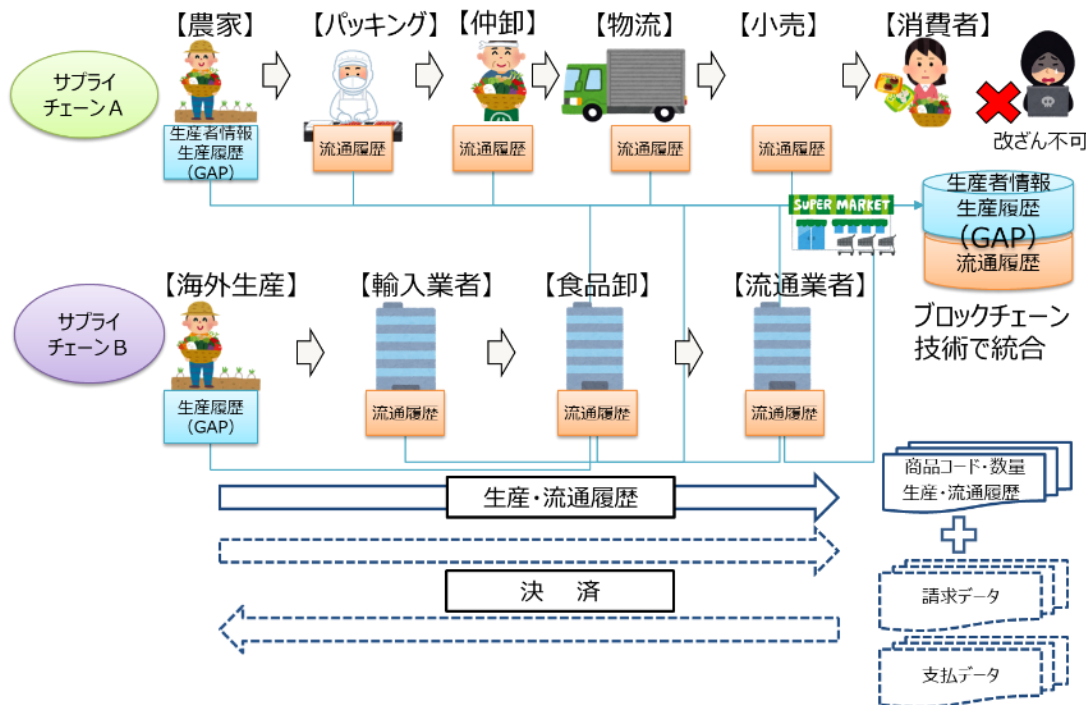
日本の水産物の中国向け輸出のトレーサビリティを確保。



食品流通におけるトレーサビリティの確保やコスト削減のためのデータ活用を目的としたブロックチェーン応用の実証実験を実施。

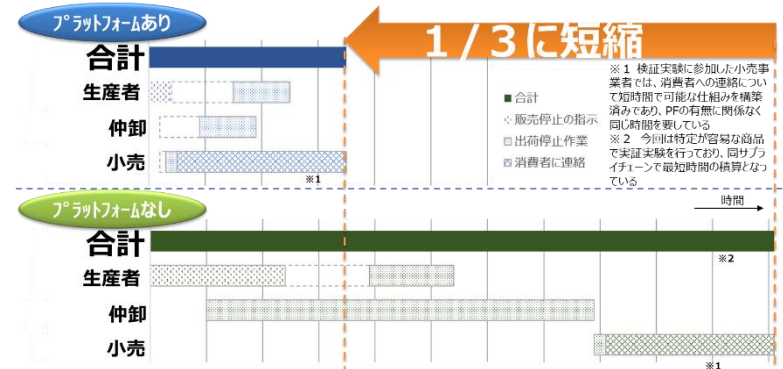
【トレーサビリティ等のためのデータ連携実証】

生産者から消費者まで、各段階での生産履歴や流通履歴を記録してブロックチェーン上に保存する実証実験を実施。食品事故の発生をモデルケースとして、流通段階での耐改ざん性や、商品の回収コストの削減効果等について調査。



【実証実験における事故品流通拡大抑止効果】

本実証実験のケースでは、出荷停止を含めた商品の回収作業に要する時間が、サプライチェーン全体で3分の1に、事業者によっては7分の1に短縮。



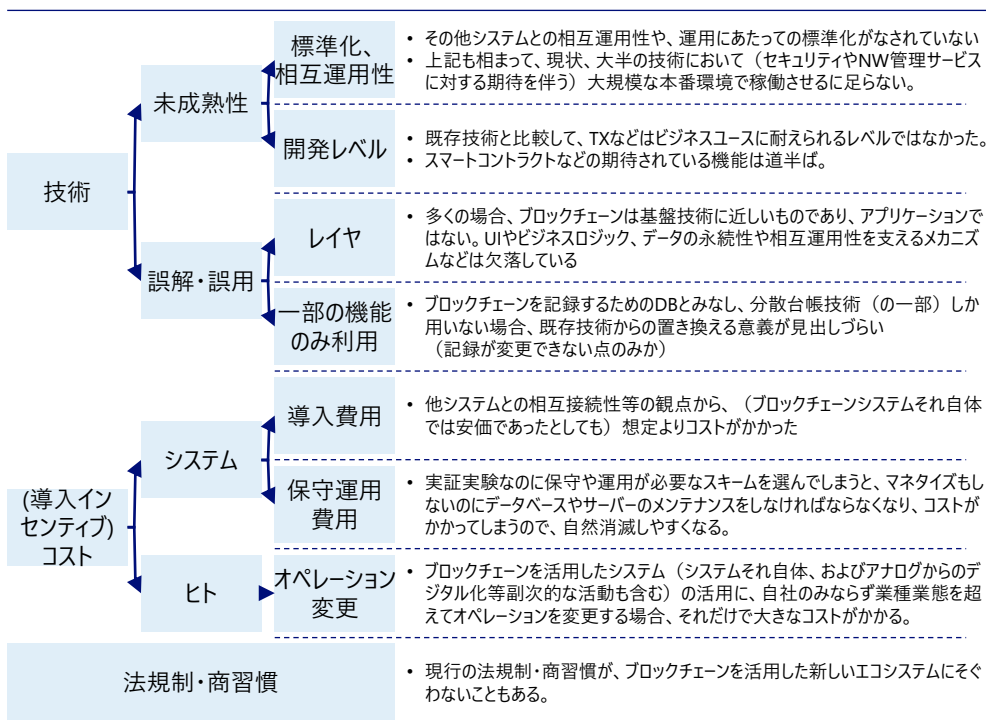
本実証実験のケースでは、回収範囲を必要な当該ロットに限定することができたため、180分の1に削減可能。



ブロックチェーンの活用に関して、PoCから社会実装への展開を促進するため、現状の確認と阻害要因、日本における普及促進に有効な施策に着目して調査・分析を実施。

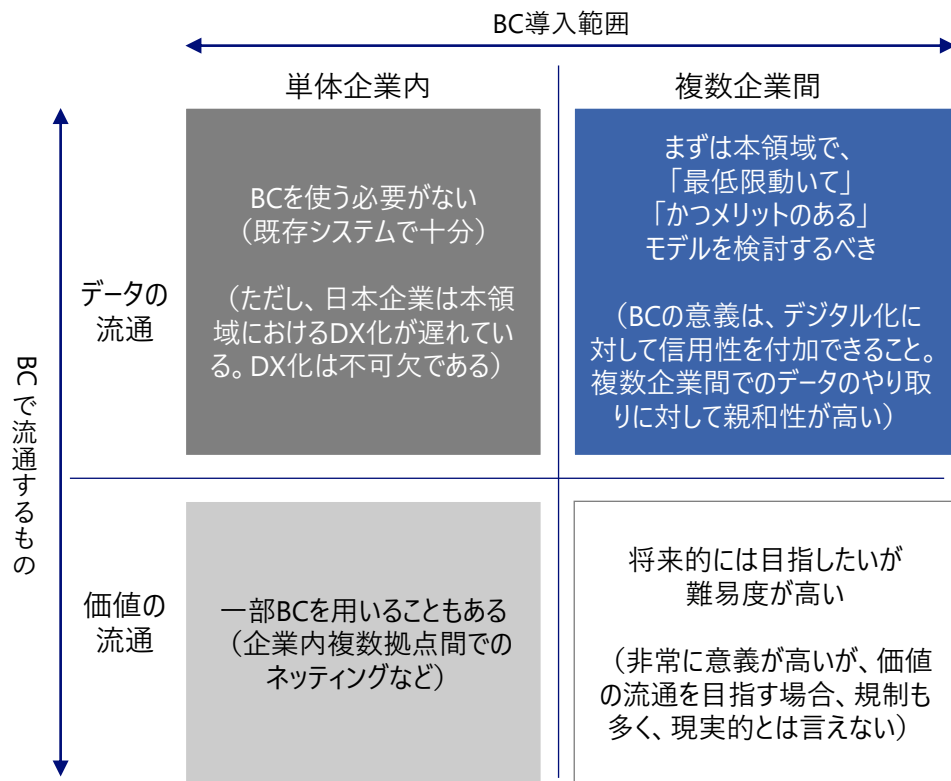
【ブロックチェーン導入に係る一般的な課題】

実際の事例をモデルに、検討プロセスに沿って各フェーズでの導入成否に関わるポイントから成功/失敗の判断要因を整理。ブロックチェーン導入における課題を体系化。



【日本にフィットする導入モデルの考え方】

ブロックチェーンの導入範囲、および流通するものに鑑みるに、まずは複数企業間×データ流通の領域で「最低限動いて」「メリットのある」モデルを検討すべきとの見解が得られた。



[参考 2] 構成員からのご意見

構成員からのご意見①

行政への期待・官民の役割整理

- 戦略に書き込んで実行していくだけでなく、国としてブロックチェーンを戦略の中心に据えることを宣言するなどしてほしい（平野構成員@第4回）
- 政府が取りまとめる戦略文書にブロックチェーン国家戦略を盛り込んでほしい（加納構成員@第1回、第5回）
- いろいろなハypeが去った今の段階で、政府が関わった形でブロックチェーンについての公式な成果物が出て、発信されることは重要（増島構成員@第1回）
- 行政のみでやるもの、民間のみでやるもの、民間と行政の両方の関わりがどうしても必要なもの、がきれいに整理されると今後の施策が打ちやすくなるのではないかと（安田構成員@第4回）
- 公共性が高いもの、ビジネスモデルの確立が難しいものは、政府が完全に提供するものもひとつの選択肢たりえるのではないかと（安田構成員@第4回）
- IDだけでは何もできず、いろいろなアプリやデータと連携してこそ有用になるので、国がID基盤を設置・運用する場合は、接続性の良い実装としてほしい（福島構成員@第2回）

分散型IDについて

- 検討を進めているTrusted Webの認知の向上の意味でも、分散IDの議論が進むことに期待している（増島構成員@第1回）
- 自分自身をどのように証明するかが一番の課題（加納構成員@第2回）
- 本人性の担保を伝搬させる方法として、中央集権的な仕組にアンカリングさせる他、個人から個人にアンカリングさせるという概念もありうる（加納構成員@第2回）
- 国がオーソリティを与えないIDに対しても、法的安定性を伝えられるようにしてほしい（技術的に本人性を証明できる場合には効力を認めるなど）（福島構成員@第2回）
- 本人確認の手法のひとつとして認められると、分散IDが意味のあるものになる（落合構成員@第2回）
- マイナンバーを活用するなどの短期的な話と、国から独立した自己主権型を実現する長期的な話を、両方考える必要がある（落合構成員@第2回）
- 自己主権型IDへの分散ID・ブロックチェーン適用にはメリットがあると思っている、マイクロペイメントのようにトランザクションが処理しきれない可能性があるところにあえてブロックチェーンを使う必要はないと思っている（加納構成員@第3回）
- DIDの有効性について、単純に認証に利用する場合と、実際にIDに紐づく属性情報を利用する場合の2つがあり、混同しない方がよい（安田構成員@第2回）

構成員からのご意見②

普及に向けた環境整備・支援

- スタートアップへの投資や人材をどう増やすか、あるいは国外流出をどう防ぐかも重要（平野構成員@第1回）
- スタートアップや人材の戦略的な育成を、普及施策とセットで推進する必要があるのでは（安田構成員@第4回）
- 定量的に効果が示されていると、今後の議論の促進が期待できる（加納構成員@第4回）

ユーザへの訴求

- インセンティブ設計や免責の導入など、政策推進につながる具体的な規定の導入などの議論ができるとよい（落合構成員@第1回）
- ブロックチェーンは基盤技術であり、一般の人が触れるものではないことから、ユーザが触れる部分のデザインも、普及に向けてはしっかり考えるべき（平野構成員@第4回）

グローバル視点

- 常に国際比較を意識した検討とアクションにすべき（平野構成員@第1回）
- 今回のような議論や今後の実装などを英語で発信してほしい（平野構成員@第5回）
- グローバルなイニシアチブやエンジニアリングへのリーチを強化していくべき（平野構成員@第5回）

相互運用性・データポータビリティ

- 分散IDを社会活動の基盤としていくときには相互運用性について整理をしていくことが必要、問題提起だけでも今後につながると思われる（落合構成員@第3回）
- 相互運用性により、個人の事業者選択が自由になることに対して、事業者側のインセンティブをどのように考えるかは論点（安田構成員@第3回）
- 分散IDの活用に当たり、サービス側に求める機能として情報のポータビリティを考えていくことが重要（落合構成員@第3回）

ガバナンス

- ガバナンスモデルやグローバル規格の策定への積極的な関与が必要（安田構成員@第1回）
- 分散IDにおけるガバナンスとして、データレベル、鍵管理レベル、制度レベルで論点を整理して議論できると広がりが出るのではないか（安田構成員@第3回）

構成員からのご意見③

ブロックチェーンの使いどころ

- 複数企業や複数産業、全く異質なものの間でのデータ共有などに効果を発揮すると思われる（福島構成員@第4回）
- 日本の法体系は「紙の元本性×対面での認証・承認」を正とする体系になっているが、今後は、「デジタル×非対面」でどう真正性・元本性を保証するかという点が、ブロックチェーンを使うポイントと思われる（福島構成員@第5回）

パブリックチェーンとプライベートチェーン

- パブリックチェーンとプライベートチェーンの違いは「ブロックを作る権限を持っている人」が誰かであり、プライベートチェーンでもデータ参照や検証は誰でも可能にできる（福島構成員@第5回）
- パブリックチェーンは組織によらないデータの永続性が重視されるユースケースで、プライベートチェーンはデータの信頼性を上げつつ制御を利かせたいユースケースで、それぞれ使われる傾向がある（福島構成員@第5回）
- プライベートブロックチェーンの利用により、計算量や電力消費といった短所は解決されていると考えている（加納構成員@第5回）
- 政府が考えているユースケースのほとんどはプライベートチェーンとコンソーシアムチェーンで対応可能と思われる（福島構成員@第5回）

ルール整備について

- ブロックチェーンの活用の障害を除去する基本的整理、問題の有無の明確化が有用（落合構成員@第1回、第5回）
- 個々の法律での要件にブロックチェーンが当てはまるか、検討会をひとつ立ち上げて行えば、結構検証でき、類型化できる気がしている（増島構成員@第5回）
- 電磁的記録の管理者が1人であることが暗黙的に定められている場合などが、アプローチが難しい例（増島構成員@第5回）
- 忘れられる権利について、オフチェーンにデータを出すだけで十分かどうかという議論が欧州では行われている（安田構成員@第5回）

今後に向けて

- 実用の普及に向けて進むよう、議論を終わらせずに継続してほしい（平野構成員@第1回、第5回）
- Trusted Webでの議論との接続性のようなものを作れるとよい（増島構成員@第5回）
- ブロックチェーン技術は安定してきており、運用面が大事になってくる時期に来ている（安田構成員@第5回）
- 今後の検討の方向性として、暗号技術に基づくトラストと、法的に定められているトラストのバランスをいかに策定していくかというのが重要と思われる（安田構成員@第5回）

