

平成30年度

ブロックチェーン技術が行政に与える影響に関する調査研究

報告書

2019年3月31日

一般社団法人 行政情報システム研究所

はじめに

我が国の行政機関は、人的・予算的資源の制約が強まる中、ますます多様化・複雑化する行政課題に取り組むことが求められており、その課題解決の糸口となり得る新たなデジタル技術の活用への期待が高まっている。

こうした技術の中で昨今、官民で特に注目を集めているものの一つがブロックチェーン技術である。ブロックチェーン技術とは、公開鍵暗号や P2P 等の要素技術を特定の方式で組み合わせることで、登録・更新等の記録の耐改ざん性や耐障害性を担保する技術である。同技術については、諸外国の政府・自治体や民間企業において、活用に向けた実証実験その他の取組が活発に行われている。我が国政府でも、「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」（平成 30 年 6 月 15 日閣議決定）において「III. 抜本改革を支える新たな基盤技術等」の一つとして「ブロックチェーン等の新技術の利用」が掲げられており、いくつかの行政機関や自治体で実証実験等が行われているところである。

しかしながら、行政のどの分野にブロックチェーン技術の活用可能性があるかについては、典型的な事例は挙げられているものの、いまだ体系的な整理は行われていない。そして、検討が進んでいない背景には、ブロックチェーン技術そのものの多義性や曖昧さがある。識者によって、ビットコインを構成する技術をすべて使用する場合にのみブロックチェーンと呼ぶこともあれば、ハッシュ値を用いた改ざん防止技術のみを用いた場合をも含むこともあるといった状況だからである。

そこで本調査研究では、第一に、ブロックチェーン技術そのものの概念や特性等について、特に行政での利用という観点を念頭に置きつつ体系的に整理する。第二に、実際の事例をもとに、現時点で想定し得る具体的な利用用途を汎用的なユースケースとして設定した上で、ブロックチェーンの特性や機能・性能等がどのようなユースケースと関連しているのかを分析する。そして第三に、整理したユースケースにおいてブロックチェーン技術を導入する場合に想定される前提や制約条件を明確にする。最後に、これらの結果を踏まえて、今後の公共分野におけるブロックチェーン技術活用の可能性と課題を検討する。

結論として、ブロックチェーン技術の行政での利用には様々な課題が横たわっており、ただちに行政に大きなインパクトを与える可能性は低い。他方で、将来的にはインターネットに比肩し得るような大きな変化を行政の業務・サービスに与える可能性を秘めていると考えられる。

本調査研究の成果が、行政機関や自治体において、従来の技術では解決できなかった課題を、ブロックチェーン技術を活用することで解決しようとする際の検討の一助となれば幸いである。

なお、本調査研究は、株式会社三菱総合研究所の協力を得て当研究所において実施した。また、実施に当たっては、自治体、民間企業、有識者など多くの方々インタビュー等を通じて協力いただいた。この場を借りて深くお礼申し上げたい。

一般社団法人 行政情報システム研究所 主席研究員 狩野英司
主任研究員 栗田祐一
研究員 松本智史
研究員 細井悠貴

目次

1. 本報告書の構成と調査研究の流れ.....	1
1.1 本調査研究の流れ.....	1
1.2 調査研究の手法.....	2
2. ブロックチェーンの技術特性.....	5
2.1 ブロックチェーン技術特性調査の進め方.....	5
2.2 ブロックチェーンの特徴的な仕組み.....	6
(1)ブロックチェーンの概念.....	6
(2)非許可型（パブリック型）と許可型（コンソーシアム／プライベート型）.....	8
(3)ブロックチェーンを構成する要素技術.....	9
2.3 ブロックチェーンの技術特性.....	12
(1)文献から収集した技術特性の例.....	12
(2)ブロックチェーン特性の類型化.....	14
(3)技術特性により実現される機能・性能等.....	17
2.4 技術特性に関するまとめ.....	18
3. ブロックチェーンの活用事例と行政分野への適用考察.....	20
3.1 ブロックチェーン活用可能分野のカテゴリ.....	20
3.2 国内外の事例の整理.....	22
(1)国内事例.....	22
(2)海外事例.....	24
(3)ユースケース設定の考え方と根拠事例.....	24
3.3 ユースケースの想定.....	28
(1)地域ポイント.....	29
(2)電子投票.....	33
(3)生産物トレース.....	37
(4)公証・KYC.....	41
(5)文書管理.....	45
(6)不動産登記.....	48
(7)ICO/STO.....	52
(8)貿易情報連携.....	56
3.4 特性とユースケース機能との関係整理.....	60
3.5 ブロックチェーン特性マップ全容.....	61
4. 行政におけるブロックチェーン導入時の前提・制約.....	63
5. 公共分野におけるブロックチェーン活用の可能性と導入時の留意事項.....	67

5.1	インパクトの試算に関する考察.....	67
5.1.1	試算1 生産物トレースによるブランド力向上.....	67
5.1.2	試算2 地域通貨によるキャッシュレス化の売上げ増効果.....	70
5.1.3	試算3 ブロックチェーン適用による行政文書管理.....	73
5.1.4	試算結果についてのまとめ.....	76
5.2	行政におけるブロックチェーン技術の今後の適用領域.....	77
5.3	ブロックチェーン技術の利用に際しての留意点.....	79
6.	今後の展望.....	81
6.1	公共分野におけるブロックチェーン活用の意義①：社会課題解決の仕組みの拡大.....	81
6.2	公共分野におけるブロックチェーン活用の意義②：コミュニティの誘発.....	82
6.3	公共分野におけるブロックチェーン活用の限界.....	82
6.4	公共分野におけるブロックチェーン活用の未来.....	83

1. 本報告書の構成と調査研究の流れ

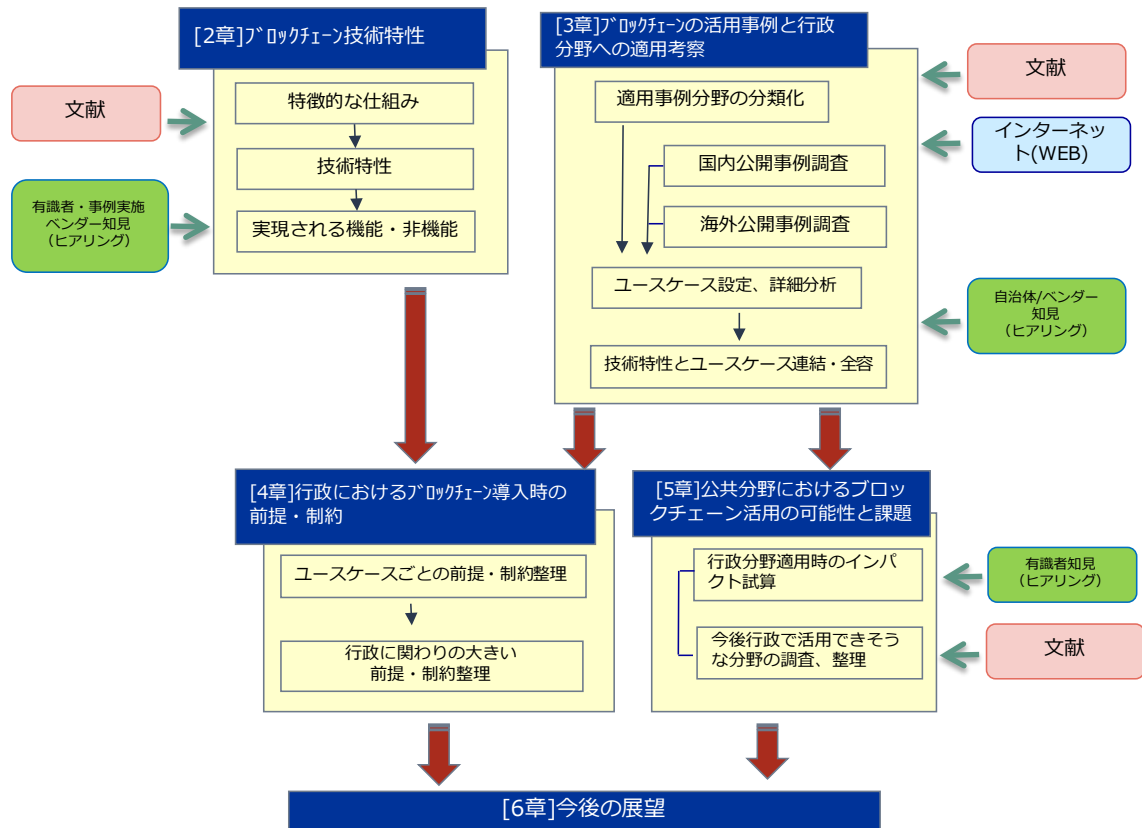
1.1 本調査研究の流れ

本調査研究は、以下の手順で実施した。

- ① ブロックチェーン技術の活用に向け、検討の論点を明らかにするため、ブロックチェーンの特徴的な仕組み、文献で記載されている特性、情報システムにおける機能、性能等との結び付きを整理した。(第2章)
- ② ブロックチェーン技術の事例、また行政に関わりの大きい分野におけるユースケース(主要な利用者がその業務で何を行うかを示したもの)でのブロックチェーン技術の利用場面、制約等について、文献やインターネット公開情報を基に調査、整理を行い、各ユースケースにおけるブロックチェーン活用における留意事項、ブロックチェーンの特性との結び付きを整理した。(第3章)
- ③ 各ユースケースにおける前提、制約をブロックチェーンの特性毎に集約化し、行政におけるブロックチェーンの利用に際し共通して検討すべき前提及び制約を整理した。(第4章)
- ④ ブロックチェーンの活用が今後行政分野にどのようなインパクトをもたらし得るかを把握するため、いくつかの試算を行うとともに、近い将来、活用可能性がある用途を検討した。また、実際のブロックチェーン導入にあたって留意すべき事項を整理した。(第5章)
- ⑤ 公共分野におけるブロックチェーンの意義や活用にあたっての限界、今後の活用の方向性、ブロックチェーンがもたらす行政の未来について考察を行った。(第6章)

上記の調査研究の流れと各章での具体的な調査内容、および調査で利用した知識・情報のソースを図表 1-1 のとおり整理した。

図表 1-1 本調査研究の流れ



1.2 調査研究の手法

本調査研究における知識・情報の収集は主に以下の3つの方法で実施した。

- (ア) 文献調査
- (イ) インターネット (Web) 調査
- (ウ) ヒアリング調査

(ア) 文献調査

近年発刊されたブロックチェーン関連の書籍のうち、ビットコイン等の仮想通貨(暗号資産)にとどまらず新たなビジネスの仕組みの創出について言及している書籍や実際のブロックチェーンアプリケーション開発に関する技術書籍について調査を行った。調査対象文献を図表 1-2 に示す。

図表 1-2 文献一覧

(ア)「ブロックチェーン 仕組みと理論 サンプルで学ぶ FinTech のコア技術」, 赤羽喜治, 愛敬真生 (著), リックテレコム,(2016)
(イ)「徹底理解ブロックチェーン ゼロから着実にわかる次世代技術の原則」, Daniel Drescher (著), 株式会社クイープ (翻訳), インプレス,(2018)
(ウ)「ブロックチェーン技術の教科書」, 佐藤 雅史, 長谷川 佳祐, 佐古 和恵, 並木 悠太, 梶ヶ谷 圭祐, 松尾 真一郎 (著), セコム株式会社 IS 研究所, NEC (編集), シーアンドアール研究所,(2018)
(エ)「未来 IT 図解 これからのブロックチェーンビジネス」, 森川 夢佑斗(著), エムディエヌコーポレーション, (2018)
(オ)「ブロックチェーンの革新技術—Hyperledger Fabric によるアプリケーション開発」, 清水 智則, 田町 京子, 上ノ原 勇人, 佐藤 卓由, 齋藤 新, 近藤 仁, 平山 毅, 笠原 章弘, 岩崎 竜矢, 小笠原 万値 (著), 早川 勝 (監修), リックテレコム,(2018)
(カ)「ブロックチェーン技術入門」, 岸上 順一, 藤村 滋, 渡邊 大喜, 大橋 盛徳, 中平 篤 (著), 森北出版,(2017)
(キ)「ブロックチェーンシステム設計」, 中村誠吾, 中越恭平(著), 牧野友紀, 宮崎英樹 (監修), リックテレコム (2018)
(ク)「ブロックチェーンアプリケーション開発の教科書」, 加壽 長門, 篠原 航 (著), 丸山 弘詩 (編集), マイナビ出版,(2018)
(ケ)「試して学ぶスマートコントラクト開発」, 加壽 長門, 篠原 航, 金 志京, 河西 紀明, 田中 克典, 佐々木 亮彰, 平野 浩司, 前川 彰, DMM.com ブロックチェーン研究室 (著), 丸山 弘詩 (編集), マイナビ出版,(2019)

(イ) インターネット (Web) 調査

インターネット (Web) により、ブロックチェーン技術を適用して実証実験や事業を行った事例について調査を行った。国内、海外事例の中から、地域ポイント、電子投票といったカテゴリ毎に 1、2 事例を抽出した。内容の詳細は後述 3.2 及び 3.3 のとおり。

(ウ) ヒアリング調査

行政分野において、実際にブロックチェーン技術を使用して実証実験を実施した自治体やそのシステム構築に携わった事業者¹、ブロックチェーン技術の普及や基盤の研究、開発を行っている事業者、及びブロックチェーンの研究を行っている有識者にヒアリングを実施した。ヒアリング先を図表 1-3 に示す。

¹ 以後、ブロックチェーン技術を使った情報システム開発の実績のある社のことを言う

図表 1-3 ヒアリング先一覧

カテゴリ	氏名、組織名	ブロックチェーンに関する経歴、実績
有識者	京都大学公共政策大学院教授 岩下直行	ブロックチェーンに係る各種委員会の委員を務めており、日本における第一人者の一人として知られる。
自治体	石川県加賀市	ブロックチェーン都市を宣言。ブロックチェーン技術を活用した KYC 認証基盤整備に取り組んでいる。
	茨城県かすみがうら市	ブロックチェーン技術を活用した地域ポイント実証実験を実施した。
	茨城県つくば市	マイナンバーカードとブロックチェーン技術を活用した電子投票を導入した。
	大分県竹田市	ブロックチェーン技術を活用し文書の改ざんを防ぐ公文書管理の実証実験を実施した。
	宮崎県綾町	ブロックチェーン技術を活用した有機野菜トレーサビリティの実証実験を実施した。
事業者	株式会社 NTT データ	ブロックチェーン技術を利用した貿易手続データ連携システム構築の他、食品トレーサビリティや KYC 等海外含め多数のシステム構築実績あり。
	株式会社 Sound-Fintech	かすみがうら市で実施されたブロックチェーン技術を活用した地域ポイント実証実験でシステム構築を担った。
	GMO インターネット株式会社	Ethereum を利用してブロックチェーン上に分散型のアプリケーションを構築できる PaaS 型サービスベースの Z.com Cloud を提供している。
	株式会社スマートバリュー	ブロックチェーン技術を活用した KYC 認証基盤を構築し、加賀市に提供した。
	日本アイ・ビー・エム株式会社	Hyperledger Fabric を採用した IBM Blockchain Platform を提供している。ブロックチェーン技術を活用した多数のシステム構築実績あり。
	株式会社 bitFlyer	仮想通貨交換業及び独自ブロックチェーン (miyabi) サービス事業を展開している。不動産登記に関する講演多数あり。
	一般社団法人ビヨンドブロックチェーン	オープンソースのブロックチェーン基盤 BBc-1 を開発し、普及活動を行っている。
	株式会社 VOTE FOR	つくば市における電子投票で、ブロックチェーンを適用したシステム構築を担い、実証実験を実施した。
	株式会社リクルート	ブロックチェーン技術を利用した履歴書、卒業証等を管理する情報システム構築、実証実験を実施した (株式会社リクルートテクノロジーズ)。なお、経済産業省の産業技術調査事業 (国内外の人材流動化促進や研究成果の信頼性確保等) に向けた大学・研究機関へのブロックチェーン技術の適用及びその標準獲得に関する調査) の事務局を務めた (株式会社リクルート R & D)。

2. ブロックチェーンの技術特性

2.1 ブロックチェーン技術特性調査の進め方

ブロックチェーン技術はまだ新しく、また急速に進歩しつつある情報技術と言うこともあり、定義や特徴についての記述も様々である。

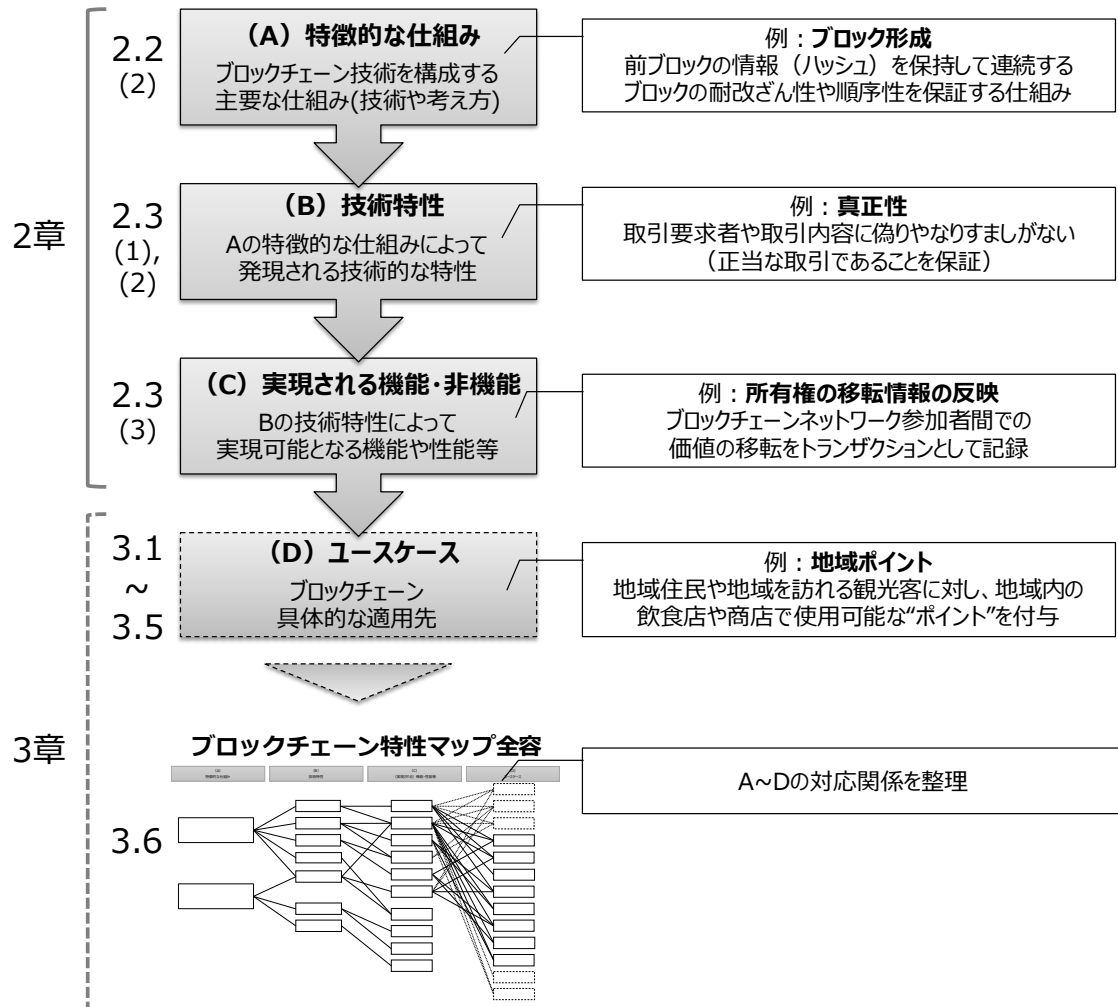
本章では、ブロックチェーン技術の活用に向けた検討の基礎となる概念、構成要素、技術的な特性（技術特性）等を明らかにする。本調査研究において技術特性とは、ブロックチェーンを実業務に適用した際に、情報システムにおいて発揮される機能上の性質、特質のことを指す。技術特性は以下の手順で整理する。

- (A) ブロックチェーン技術を構成する要素技術を基にブロックチェーンの「特徴的な仕組み」を整理する。具体的には、ブロック形成や分散管理が該当する。
- (B) (A) の特徴的な仕組みやそれらの組合せによって発現される技術的な特性を「技術特性」として整理する。具体的には真正性や透明性等を指す。
- (C) (B) のブロックチェーンの技術特性によって情報システムとして実現可能となる機能や性能等を「(実現される) 機能・性能等」として整理する。システムとして実装される際には、ブロックチェーン技術が機能や性能等の一要素として現れる。

本調査研究では、「(A) 特徴的な仕組み」を起点とし、「(A) 特徴的な仕組み」によって発現される「(B) 技術特性」、そして「(B) 技術特性」によって「(C) (実現される) 機能・性能等」の対応関係について、文献調査及びヒアリングによる調査及び整理を行う。(図表 2-1)

なお、(D) については、実際にブロックチェーンの活用が期待される領域や業務をユースケースとして第3章にて調査し、(A)、(B)、(C) 及び (D) の対応関係について整理を行う。

図表 2-1 技術特性に関する調査の進め方



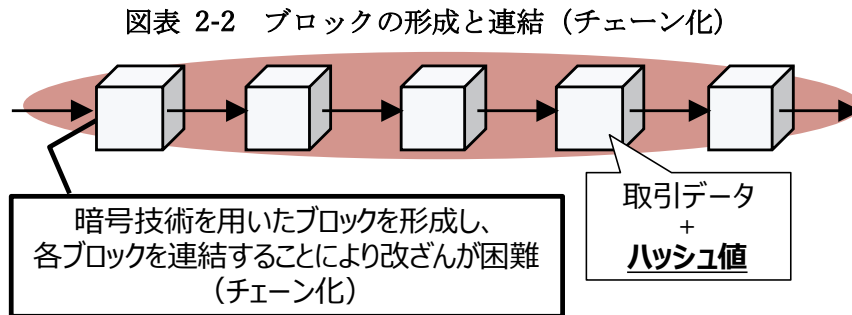
2.2 ブロックチェーンの特徴的な仕組み

ブロックチェーン技術は、全く新規に考案された情報通信技術ではなく、複数の既存の情報技術を組合せることで、それまで使われていなかった用途や新たな価値を見出すことに成功した概念と考えられる。本節では、まず本調査研究における「ブロックチェーン技術」の概念を整理する。その上で、ブロックチェーンを構成する要素技術を抽出し、その組合せによりブロックチェーンに現れる特徴を整理する。

(1) ブロックチェーンの概念

ブロックチェーンでは、データを「ブロック」と呼ばれる単位にまとめ、それらのブロックを前後のブロック間で連結（チェーン化）してデータを管理する（図表 2-2）。各ブロッ

には、一定のトランザクション（取引）と前ブロックのハッシュ値²を合わせて格納する。ブロックのチェーン化により、ブロックチェーン上のデータを改ざんするには、対象のデータが格納されたブロックだけでなく連結されたブロックを全て改ざんする必要があり、実質的に改ざんは不可能とされている。



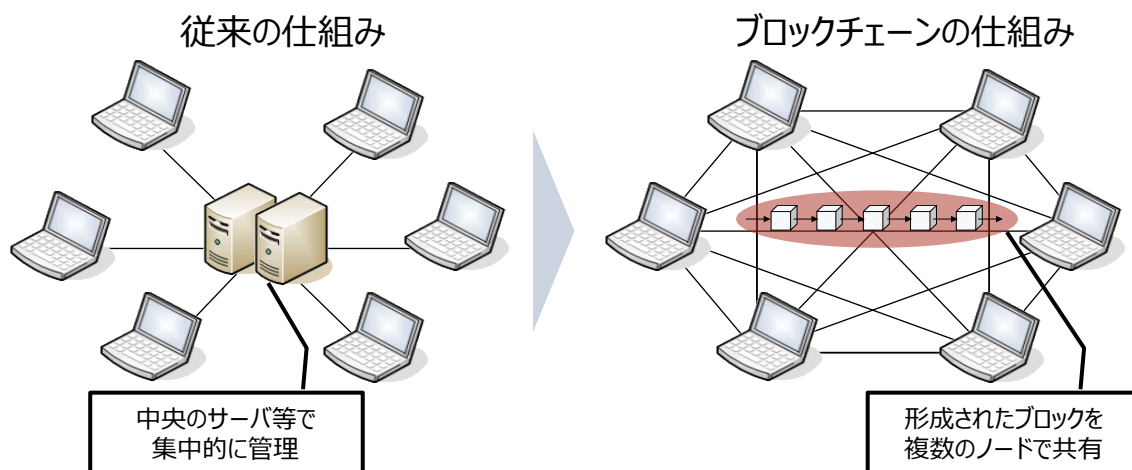
また、総務省では、ブロックチェーンを「情報通信ネットワーク上にある端末同士を直接接続して、取引記録を暗号技術を用いて分散的に処理・記録するデータベースの一種」³としている。ブロックチェーンは、前述のブロックの情報をネットワーク上にあるノードに分散格納⁴することにより、たとえ一部のノードが機能不全になった場合であってもシステム全体として機能不全になることを防ぐことができる。（図表 2-3）

² ハッシュ値はハッシュ関数によって算出される値であり、ハッシュ関数は入力された値が少しでも異なる場合は出力される値が異なるという特徴を持つ。ハッシュ値は、例えばあるデータの受け渡しにおいて、そのデータが途中で改ざんされていないことを示す際に用いられる。ブロックチェーンではこのハッシュ値をポインタ（ハッシュポインタ）として使用し、データに連続性を保持させることにより、耐改ざん性を高め、改ざんされた場合でも検知を容易にしている。

³ ICT によるイノベーションと新たなエコノミー形成に関する調査研究，総務省，
http://www.soumu.go.jp/johotsusintokei/linkdata/h30_02_houkoku.pdf, 2019/3/28 確認

⁴ ブロックチェーンは分散台帳技術（Distributed Ledger Technology（DLT））の一種であるが、従来の分散台帳技術との違いとして、ブロック化されたデータを連結して保持することがあげられる。

図表 2-3 ブロックチェーンにおけるデータの分散格納



(2)非許可型（パブリック型）と許可型（コンソーシアム／プライベート型）

ブロックチェーンは、ノードのネットワークへの接続方法（参加方法）によって、大きく非許可型（パブリック型）と許可型（コンソーシアム／プライベート型）に分けられる。（図表 2-4）

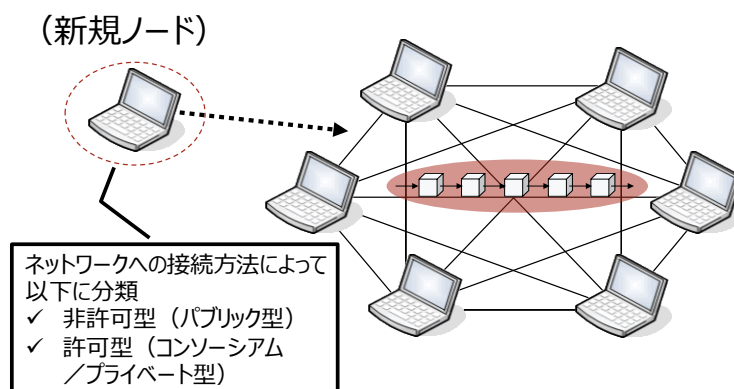
非許可型（パブリック型）は、ネットワークに接続できれば誰でも参加することができ、参加者の役割は基本的に同一である。管理者が不在のため、不特定かつ悪意のある参加者を含む可能性もあるが、取引の内容は参加者全員に公開され、更に正しい行動にインセンティブを与える仕組み⁵などにより、ネットワーク全体としては悪意のある行動を抑えることが可能となっている。

許可型には、コンソーシアム型とプライベート型とがある。特定の複数主体で構成するブロックチェーンをコンソーシアム型と呼び、単一の企業や企業グループ等で利用するブロックチェーンをプライベート型と呼ぶ。どちらもネットワークへの参加者を限定するという点では同じ特徴を持ち、参加者の承認を行う管理者が存在する。取引記録は限られた参加者のみが参照することができ、パブリック型と比べて処理性能も高い⁶ことが多い。ただし、管理面では図表 2-3 で示した従来の中央のサーバ等で集中的に管理するシステム構成との差異が見えにくくなる。

⁵ 例えばマイニングと呼ばれるような仕組みで、仮想通貨ではノードの運用者（マイナー）に対して運用報酬として仮想通貨が与えられる。

⁶ 許可型では悪意のある参加者を想定しておらず、予め許可された信頼性の高いノードが取引の承認を行うため、高速な処理が可能となる。

図表 2-4 ブロックチェーンにおける新規ノードの接続方法



(3) ブロックチェーンを構成する要素技術

ブロックチェーンは前述の総務省によるものも含め様々な定義がなされているが、ここでは技術的な観点に焦点を当てた分析を行い、ブロックチェーンを構成する要素技術に関する整理を行う。ブロックチェーンに関する技術的な視点に基づく定義として、日本ブロックチェーン協会では Satoshi Nakamoto⁷の論文等を踏まえ、以下の2つ⁸の定義を公開⁹している。

- 1) 「ビザンチン障害を含む不特定多数のノードを用い、時間の経過とともにその時点の合意が覆る確率が0へ収束するプロトコル、又はその実装をブロックチェーンと呼ぶ。」
- 2) 「電子署名とハッシュポインタを使用し改ざん検出が容易なデータ構造を持ち、かつ、当該データをネットワーク上に分散する多数のノードに保持させることで、高可用性及びデータ同一性等を実現する技術を広義のブロックチェーンと呼ぶ。」

上記の定義において「電子署名」や「合意が覆る確率が0へ収束するプロトコル」、「ネットワーク上に分散」といったキーワードが言及されているように、ブロックチェーンは「様々な要素技術の組合せ」によって実現されるものである。図表 2-5 で示した文献、報告書でもブロックチェーンは「要素技術の組合せ」として説明されている。

⁷ ビットコイン（ブロックチェーン）に関する構想を論文にまとめてネット上に公表した人物であるが、正体は不明とされている。

⁸ 日本ブロックチェーン協会では、1)はオリジナルを意識した「狭義のブロックチェーン」、2)は昨今の技術の展開等も踏まえた「広義のブロックチェーン」と表現している。

⁹ ブロックチェーンの定義, 日本ブロックチェーン協会, <https://jba-web.jp/>, 2019/3/22 確認

図表 2-5 ブロックチェーンを構成する要素技術への言及

No.	ブロックチェーンを構成する要素技術への言及	出典
1	P2P や公開鍵暗号等の既存の技術の組合せ	ブロックチェーン入門～その仕組みと IoT への適用の可能性、応用を探る～ ¹⁰
2	ブロックチェーンは「P2P ネットワーク」や「コンセンサスアルゴリズム」「スマートコントラクト」「偽造防止・暗号化技術」といった複数の技術の組合せで実現	ブロックチェーンの仕組み ¹¹
3	ビットコインは、「ハッシュ・電子署名」「PoW」「P2P」といった主な技術により構成	平成 27 年度 我が国経済社会の情報化・サービス化に係る基盤整備（ブロックチェーン技術を利用したサービスに関する国内外動向調査）報告書 平成 28 年 3 月 ¹²

次に、組合せの基となる要素技術を整理する。

本調査研究では、前述の日本ブロックチェーン協会と図表 2-5 の考え方を踏まえ、上記の中でも暗号技術等に係る「公開鍵暗号」、不特定多数のノードが参加する場合であっても全体として正しい選択を可能とする「コンセンサスアルゴリズム」及びネットワークの分散保持といった「P2P」の 3 点をブロックチェーンを構成する要素技術とした。（図表 2-6）

なお、図表 2-6 の各要素技術の「概要」に関しては、各種文献^{13, 14, 15}を参考として記載した。

¹⁰ 株式会社ハウインターナショナル, <https://www.ipa.go.jp/files/000055833.pdf>, 2019/3/22 確認

¹¹ 株式会社 NTT データ, <http://www.nttdata.com/jp/ja/services/sp/blockchain/mechanism/>, 2019/3/22 確認

¹² 株式会社野村総合研究所, <https://www.meti.go.jp/press/2016/04/20160428003/20160428003-2.pdf>, 2019/3/22 確認

¹³ （公開鍵暗号）公的個人認証サービスの利活用について、総務省, http://www.soumu.go.jp/main_content/000324414.pdf, 2019/3/22 確認

¹⁴ （コンセンサスアルゴリズム）PKI day 2017 ブロックチェーンとは何か, セコム株式会社, https://www.jnsa.org/seminar/pki-day/2017/data/170419_sato.pdf, 2019/3/22 確認

¹⁵ （P2P）P2P とは, 一般社団法人日本ネットワークインフォメーションセンター, <https://www.nic.ad.jp/ja/basics/terms/p2p.html>, 2019/3/22 確認

図表 2-6 本調査研究におけるブロックチェーンを構成する要素技術

No.	要素技術	概要
1	公開鍵暗号	秘密鍵と公開鍵のペアとなっており、片方の鍵で暗号化されたものは、もう一方の鍵でしか復号できない性質を持つ。
2	コンセンサス アルゴリズム	ブロック生成者の決定や、ブロックに記載する取引情報に関する承認方法で、仕組みはネットワーク参加方法により前提が異なる。
3	P2P	ネットワークを構成する各ノードがデータを保持し、他のノードに対して対等にデータの提供及び要求・アクセスを行う自律分散型のネットワークモデル。

次に、上記の要素技術に対し、それらの組合せによって実現される特徴的な仕組みについて検討を行った。

「公開鍵暗号」は、各ノード間の取引の真正性を保証するものであり、「コンセンサスアルゴリズム」と組合せることによって、ブロックの耐改ざん性や順序性をネットワークの参加者による総意¹⁶として保証する仕組みである。本調査研究では、この仕組みを「ブロック形成」と呼ぶ。

ブロックチェーンにおける「P2P」は、参加者全員が同じ情報を持ち、ネットワーク内で分散的に管理することを可能としている。本調査研究では、これを「分散管理」と呼ぶ。広義の「分散管理」は、データを分割して参加者が部分的に情報を持ち合うことも含まれるが、ブロックチェーンにおいては、同じ情報（台帳）を参加者全員が持ち、さらに自動更新する仕組みを指す。前者の部分的な情報を持ち合う仕組みは、大量な情報処理において効率化・高速化が期待されるのに対し、ブロックチェーンにおける分散管理は、ほぼ同時更新されるためノード間で複製を保持することとなり、故障したノードを復旧しやすいといった、不正に対する頑健性等が期待される。

上記のように整理した結果、ブロックチェーンの特徴的な仕組みとして、「ブロック形成」と「分散管理」にまとめられた。(図表 2-7)

¹⁶ 実際には合意形成の提案を行うリーダーを選出し、ほかの参加者によりその提案を検証する。非許可型では作業量(計算量)や暗号資産の保有量及び保有期間でリーダーを選出するのに対し、許可型では予め合意形成を担うリーダーを選出する場合が多い。

図表 2-7 ブロックチェーンの特徴的な仕組み

要素技術	特徴的な仕組み	内容
公開鍵暗号	ブロック形成	公開鍵暗号による取引の真正性や、前ブロックの情報（ハッシュ）を保持して連続するブロックの耐改ざん性や順序性を保証する仕組み
コンセンサスアルゴリズム		
P2P	分散管理	同じ台帳を参加者全員が持ち、自動更新する仕組み

2.3 ブロックチェーンの技術特性

本節では、前節で整理した既存技術を組合せ、ブロックチェーンとなったことで現れる技術特性の整理を試みる。ここで言う技術特性とは、ブロックチェーンを実業務に適用した際に、情報システムにおいて発揮される機能上の性質、特質のことで、例えば「耐改ざん性（特定の情報が、登録されたとおりの状態で保持される）」のようなものを指す。

まずは図表 1-2 に示した書籍等の各種文献において示されるブロックチェーンの特徴や技術的なキーワード（例 分散型システム、耐改ざん性、信頼性等）を抽出し、整理を行った。各文献によって共通的に認識されている技術的なキーワードを技術特性の1次案とし、それに対してブロックチェーンを専門領域とする有識者や事業者へヒアリングを行って聴取した意見を参考に再度整理を行った。

(1)文献から収集した技術特性の例

図表 1-2 に示す各文献をベースとし、各文献において言及されている技術的なキーワードを抽出した。（図表 2-8）

図表 2-8 各文献における技術的なキーワード（抽出結果）

(ア)ブロックチェーン仕組みと理論 サンプルで学ぶFinTechのコア技術	(イ)徹底理解ブロックチェーン:ゼロから着実にわかる次世代技術の原則	(ロ)ブロックチェーン技術の教科書	(ハ)未来IT図解 からのブロックチェーンビジネス	(ニ)ブロックチェーンの革新技術—Hyperledger Fabricによるアプリケーション開発	(ホ)ブロックチェーン技術入門	(ヘ)ブロックチェーンシステム設計	(ニ)ブロックチェーンアプリケーション開発の教科書	(ケ)試して学ぶスマートコントラクト開発
<ul style="list-style-type: none"> ● 改ざんが難しい ● 取引記録の作成タイミングが客観的にわかる ● 分散型システムであり、巨大な中央システムが不要 ● 取引記録の妥当性が参加者の総意として検証済である 	<ul style="list-style-type: none"> ● イミュータブル(不変) ● 追加専用 ● 順序 ● タイムスタンプ ● 開放性と透明性 ● セキュア(識別、認証、承認) ● 結果整合性 	<ul style="list-style-type: none"> ● ビザンチン故障に対する耐性(ただしこれを持たないブロックチェーンもある) ● システム管理者の特権の悪用の抑止 ● 履歴データの管理に適した構造 ● データの改ざんを防ぐために適した構造 ● スマートコントラクト 	<ul style="list-style-type: none"> ● 障害や攻撃に極めて強い ● ネットワーク内の出来事を網羅的かつ透明に記録する ● 改ざんやコピーができない ● 管理者不在の平等なネットワーク 	<ul style="list-style-type: none"> ● 複数の参加者が、同じ内容の台帳を分散保持できる ● 台帳間の整合性を維持する仕組み(コンセンサス)により、同じ内容が維持される ● 第三者(中央機関)の介在が不要(参加者同士のピア・ツー・ピア(P2P)取引) ● 暗号技術により、取引の透明性を確保しつつ、署名によりトランザクションの作成元を特定できる ● 台帳の1つに障害が発生しても、残りの台帳で業務を継続できる(システム可用性の向上) 	<ul style="list-style-type: none"> ● (中央集権的な)集中管理機構が不要 ● 信頼性が高い 	<ul style="list-style-type: none"> ● 真正性がある(なりすましがなく、取引要求者に偽りが無い) ● 改ざん耐性が高い ● 特定の管理者の仲介を必要としない参加者間での直接取引ができる ● 複数の参加者とデータを共有できる ● データ消失時の回復性が高い ● 過去の権利移転が全て記録され、取引を追跡できる(トレーサビリティ) 	<ul style="list-style-type: none"> ● セキュア ● 可用性が高い 	<ul style="list-style-type: none"> ● マイクロペイメント(超少額決済) ● 即時支払 ● 耐改ざん性 ● データの民主化 ● スマートコントラクト

(2) ブロックチェーン特性の類型化

図表 2-8 に示される各文献の技術的なキーワードに共通する内容を抽出・整理し、技術特性の 1 次案とした。(図表 2-9)

なお、各文献で言及されていたキーワードのうち、ここで整理しようとしている技術特性の元となっている「特徴的な仕組み」に該当するもの (P2P 等) や、逆に技術特性を活用して発揮される機能・性能 (スマートコントラクト等)、複数の特性の組合せによって実現した技術特性については、2.2(3)及び 2.3(3)において整理するものとし、整理の対象外とした。

図表 2-9 技術特性の整理結果

(7)ブロックチェーン仕組みと理論(2016)	(9)ブロックチェーン技術の教科書(2018)	(1)これからのブロックチェーン(2018)	(4)HyperledgerFabricによるアプリケーション開発(2018)	(8)ブロックチェーン技術入門(2017)	(6)ブロックチェーンシステム設計(2018)	(9)ブロックチェーンアプリケーション開発の教科書(2018)	(7)試して学ぶスマートコントラクト開発(2019)	各文献において共通的な特性(技術特性の1次案)
取引記録の妥当性が参加者の総意として検証済である			台帳間の整合性を維持する仕組み(コンセンサス)により、同じ内容が維持される		真正性がある(なりすましがなく、取引要求者に偽りが無い)			真正性
取引記録の作成タイミングが客観的にわかる		ネットワーク内の出来事を網羅的かつ透明に記録する	暗号技術により、取引の透明性を確保しつつ、署名によりトランザクションの作成元を特定できる					透明性
	履歴データの管理に適した構造	ネットワーク内の出来事を網羅的かつ透明に記録する	暗号技術により、取引の透明性を確保しつつ、署名によりトランザクションの作成元を特定できる		過去の権利移転が全て記録され、取引を追跡できる(トレーサビリティ)			追跡可能性
改ざんが難しい	システム管理者の特権の悪用の抑止データの改ざんを防ぐために適した構造	改ざんやコピーができない			改ざん耐性が高い		耐改ざん性	耐改ざん性
	ビザンチン故障に対する耐性(ただしこれを持たないブロックチェーンもある)	障害や攻撃に極めて強い	台帳の1つに障害が発生しても、残りの台帳で業務を継続できる(システム可用性の向上)	信頼性が高い	データ消失時の回復性が高い	可用性が高い		可用性
分散型システムであり、巨大な中央システムが不要			複数の参加者が、同じ内容の台帳を分散保持できる		複数の参加者とデータを共有できる			同時共有性
以下、特性として当てはまらないキーワード								
	<ul style="list-style-type: none"> スマートコントラクト ⇒ (C) 機能に分類 	<ul style="list-style-type: none"> 管理者不在の平等なネットワーク ⇒ (P2Pとして) (A) 特徴的な仕組みに分類 	<ul style="list-style-type: none"> 第三者(中央機関)の介在が不要(参加者同士のピア・ツー・ピア(P2P)取引) ⇒ (A) 特徴的な仕組みに分類 	<ul style="list-style-type: none"> (中央集権的な)集中管理機構が不要 ⇒ (P2Pとして) (A) 特徴的な仕組みに分類 	<ul style="list-style-type: none"> 特定の管理者の仲介を必要としない参加者間での直接取引ができる ⇒ (P2Pとして) (A) 特徴的な仕組みに分類 	<ul style="list-style-type: none"> セキュア ⇒ 複数の特性の組合せのため省略 	<ul style="list-style-type: none"> スマートコントラクト ⇒ (C) 機能に分類 マイクロペイメント(超少額決済) ⇒ ユースケースに紐づく応用機能のため省略 即時支払 ⇒ ユースケースに紐づく応用機能のため省略 データの民主化 ⇒ 抽象度が高く分類困難なため省略 	

以上の結果、ブロックチェーンの技術特性の1次案として「真正性」、「透明性」、「追跡可能性」、「耐改ざん性」、「可用性」及び「同時共有性」が導出された。

これらに加え、ヒアリングにおいて、二重処理などの不正なトランザクションの防止¹⁷という観点で「耐改ざん性」とは異なる分散トランザクション処理（分散合意）がブロックチェーンの特徴であるという見解¹⁸を受け、「分散合意性」を技術特性として追加した。

以上の結果、整理された技術特性とその内容を図表 2-10 に示す。

図表 2-10 ブロックチェーンに関する技術特性

技術特性	内容
真正性	電子署名により取引要求者のなりすましを防ぐことができる。
透明性	取引記録がネットワーク内で共有（公開）され、誰でも取引履歴を閲覧することができる。
追跡可能性	取引記録をチェーン化することにより、取引履歴のトレースができる。（トレーサビリティ）
耐改ざん性	ブロック内に記載され、チェーン化した後は改ざんしようとしても自動で検知し、事実上改ざんを防ぐことができる。
分散合意性	参加者の総意としての妥当性が検証される。
可用性	一部で障害（単純な故障）が起こって停止しても、完全に止まることなく更に容易に回復することができる。（単一障害点がない）
同時共有性	参加者が同じ情報（台帳）を分散して持ち合い、同時に情報共有することができる。

なお、技術特性は情報システムにおいて発揮される機能上の性質や特質であり、ブロックチェーンがシステム全体に対してよい影響を与えるものがある一方で、システムに対して制約として働くものもある。例えば、ブロックチェーンが制約的に働くものとして、次のような点が指摘¹⁹されている。

- ノード数やユーザ数（トランザクション数）が増加すると処理性能が低下²⁰する。

¹⁷ 例えば仮想通貨であれば同じコインを異なる相手に支払うこと。

¹⁸ 日本 IBM ヒアリングより

¹⁹ ブロックチェーン技術の活用可能性と課題に関する検討会報告書, ブロックチェーン技術の活用可能性と課題に関する検討会, <https://www.zenginkyo.or.jp/fileadmin/res/news/news290346.pdf>, 2019/3/22 確認

²⁰ ノード数が多くなると、同期のタイムラグ等によって一時点におけるデータ不整合が発生する可能性も高くなる。

- コンセンサスアルゴリズムやブロックサイズなどの実装方式によっては、機能や性能にトレードオフとなるものが生じる。例えばコンソーシアム型を前提としたコンセンサスアルゴリズムである PBFT では、パブリック型と比べて処理性能の向上が期待されるが、信頼されたノードが単一障害点となりうる。また、ブロックサイズが大きくなると一度に処理できるトランザクション量が増え、処理性能の向上が期待される一方で、ブロック形成に関わる合意形成に時間を要するほか、合意形成の参加者における非匿名化や寡占化が発生する可能性がある。

(3)技術特性により実現される機能・性能等

上記の技術特性に対し、実際にシステムとして技術特性を具現化した際に初めて機能や性能として発現されるものも存在する。例えば、取引要求者等のなりすましを防ぐ「真正性」という技術特性により、価値の移転を記録する「所有権の移転情報の反映」がシステムの機能として実現される。

ブロックチェーンの技術特性を活用して発現されるそれらの機能・性能等を整理した。

(図表 2-11)

図表 2-11 技術特性により実現される機能・性能等

機能・性能等	内容
所有権の移転情報の反映	ブロックチェーンネットワーク参加者間での価値の移転をトランザクション（取引記録）として記録する。
主体とその内容の真正性が証明された情報の登録・参照	以下の二点で真正性が保証された情報を登録・参照する。 - 秘密鍵を持っている正しい主体（なりすましでない主体）が発した内容を登録・参照 - 参加するノードの総意として妥当性が確認できた内容を登録・参照（ビザンチン耐性 ²¹ も含む。）
誰でも閲覧することが可能	取引記録がネットワーク内で共有（公開）され、誰でも取引履歴を閲覧することができる。
スマートコントラクト	プログラムによってあらかじめ契約とその履行条件を定めておき、条件が満たされた際に契約（処理）が自動的に実行される。

²¹ ビザンチン耐性とは、ビザンチン将軍問題（またはビザンチン故障やビザンチン障害）を克服できる性質を指す。ビザンチン将軍問題とは、特定の管理者がいないネットワークで悪意を持った参加者や不正確な情報により正しい合意形成ができなくなるものであり、ブロックチェーンではコンセンサスアルゴリズム等によってビザンチン将軍問題を克服している。

機能・性能等	内容
履歴・過程情報の参照が可能	取引記録をチェーン化することにより、取引履歴のトレースができる。（トレーサビリティ）
二重処理の防止	参加者全員による検証（監視）を行い、二重処理（例えば仮想通貨であれば同じコインを異なる相手に支払うこと）を防ぐ。
改ざんに強いシステム	ブロック内に記載され、チェーン化した後は改ざんしようとしても自動で検知し、事実上改ざんを防ぐことができる。
バックアップシステムが不要	従来のシステムだと追加対応が必要な作り込みやバックアップサーバ等が不要となる。
安定したシステム	一部で障害（単純な故障）が起こって停止しても、完全に止まることなく、容易に回復することができる。（単一障害点がない）
情報の同時共有	台帳を持つ参加者に同じ情報が共有される。

2.4 技術特性に関するまとめ

本節では、前節までで整理してきたブロックチェーンにおける、

(A)特徴的な仕組み

(B)技術特性、及び

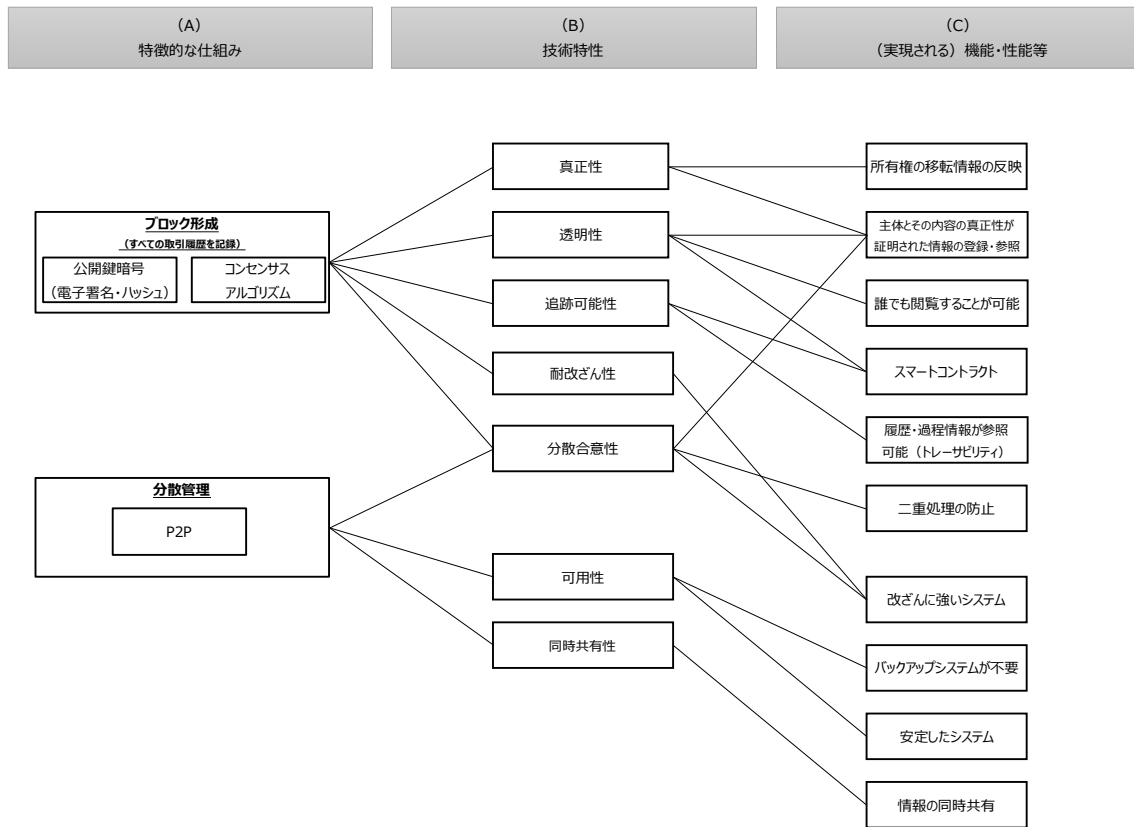
(C)実現される機能・性能等

の間の一連の対応関係について整理を行う。

図表 2-11 の機能・性能等が技術特性によって発現されるように、技術特性自体も図表 2-7 に示す特徴的な仕組みに基づき発揮される機能上の性質、特質である。

ブロックチェーンにおける「ブロック形成」及び「分散管理」の2つの特徴的な仕組みから、「真正性」といった技術特性が発現し、さらにそれらが情報システムにおいて「所有権の移転情報の反映」といった機能・性能等として発現されるまでの一連の対応関係について、図表 2-12 のとおり整理した。

図表 2-12 特徴的な仕組み、技術特性、機能・性能等の関係



3. ブロックチェーンの活用事例と行政分野への適用考察

3.1 ブロックチェーン活用可能分野のカテゴリ

ブロックチェーン技術は、様々な分野への活用の可能性が期待されている。本節では、ブロックチェーン技術を活用できる可能性のある事例を抽出し、分類することを試みる。

ブロックチェーンの活用事例について幅広く言及されている文献を調査した結果を図表 3-1 に示す。

図表 3-1 既存文献におけるブロックチェーン活用事例

文献	ブロックチェーンと生産性向上	情報通信白書 (平成30年版)	ブロックチェーン技術の真の実力—金融分野 にとどまらないイノベーションの可能性
著者	国際大学グローバル・コミュニケーション・センター 准教授/主幹研究員、研究部長 高木聡一郎	総務省	三菱総合研究所
日付等	2017年12月	2018年7月	2016年4月
URL	https://www.mof.go.jp/pri/research/conference/fy2017/inv2017_04_01.pdf	http://www.soumu.go.jp/johotsusintokei/whitepaper/ja/h30/html/nd133330.html	https://www.mri.co.jp/opinion/mreview/pdf/mr201604.pdf
活用事例	<ul style="list-style-type: none"> ➢ ビットコイン ➢ ダイヤモンド ➢ 著作権 ➢ サプライチェーン ➢ 学歴 ➢ 投票 ➢ 公証 ➢ カラードコイン ➢ オルトコイン ➢ 食品偽装 ➢ チケット ➢ 医療 ➢ 難民ID ➢ ICO ➢ 地域通貨、社内通貨 ➢ クラウドファンディング ➢ データ売買、IoT ➢ 電力取引 ➢ 土地登記 ➢ シェアリング ➢ クラウドソーシング 	<ul style="list-style-type: none"> ➢ 災害時の物質マッチング ➢ シェアリングサービスのKYC ➢ 電力取引 ➢ 不動産取引 ➢ 宅配ボックス ➢ 農産物の生産情報管理 ➢ 金融分野 	<ul style="list-style-type: none"> ➢ 仮想通貨 ➢ 金融分野（銀行間送金、海外送金等） ➢ 商取引 ➢ 知的財産 ➢ 地方創生 ➢ サプライチェーン ➢ 医療・教育 ➢ 証券取引所 ➢ IoT ➢ 政府系 ➢ 公共サービス

本章では、それぞれの文献で記載された事例について、類似している事例を集約、整理し、活用事例のカテゴリとした（図表 3-2）。なお、「貿易情報連携」については図表 3-1 で記載した既存文献上では触れられていなかったが、実運用に近い実際の事例があるためカテゴリの1つとして追加している。

これらの整理は公共・非公共といった区分をせずに行ったが、このうち特に行政が主体、若しくは主要なステークホルダとして関わると考えられるカテゴリに対しては、「行政分野」列に「●」を記載している。

図表 3-2 本調査報告書におけるカテゴリ

ブロックチェーン活用事例 (図表 3-1)	本調査研究におけるカテゴリ	行政分野	想定される行政の関わり方
地域通貨、社内通貨、地方創生、チケット	地域ポイント	●	地域ポイントの発行主体
投票	電子投票	●	住民投票の実施
農産物の生産情報管理、サプライチェーン、食品偽装、商取引、ダイヤモンド、データ売買、IoT、災害時の物質マッチング、宅配ボックス	生産物トレース	●	農産物認証付与情報の登録、登録情報を用いた監査業務の実施
学歴、難民 ID、シェアリングサービスの KYC、公証、教育	公証・KYC ²²	●	公証・認証情報の登録・参照
政府系、公共サービス	文書管理	●	公文書の管理
不動産取引、土地登記	不動産登記	●	不動産登記に係る情報の登録
ICO、クラウドファンディング	ICO/STO	●	ICO/STO 実施
金融分野（銀行間送金、海外送金等）、証券取引所	金融分野	—	—
仮想通貨、ビットコイン、カレードコイン、オルトコイン、シェアリング、クラウドソーシング	仮想通貨	—	—
電力取引	電力取引	—	—
医療	医療情報	—	—
著作権、知的財産	著作権管理	—	—
—	貿易情報連携 ²³	●	貿易情報の参照

²² 公証と KYC はいずれも提示された書類の真正性を確認する作業を代替するものであり、類似度が高いと考えられるため、本調査報告書内では同一のカテゴリとして取り扱うこととした。

²³ 本文中にも記載のとおり、文献中に記載はなかったが、有望な事例と考えられるため「貿易情報連携」を追加。

3.2 国内外の事例の整理

(1)国内事例

国内におけるブロックチェーン技術を利用した情報システム構築や実証実験の事例について公開情報から調査した。

図表 3-2 において、行政が主体、若しくは主要なステークホルダとして関わるとカテゴリについて、公開情報が多い事例を1～2事例ずつ抽出した（図表 3-3）。

図表 3-3 国内におけるブロックチェーン活用事例

カテゴリ	実施主体	事例概要
地域ポイント	会津大学	学内仮想通貨「白虎コイン」を立ち上げ、学内のみならず会津地方の地域仮想通貨に発展させようとイベント会場などで実証実験を行っている。
	茨城県かすみがうら市	ブロックチェーンを活用した湖山ウォレット（アプリ）により「湖山ポイント」を発行し、当該ポイントを市内の飲食店等で使用できる仕組みを実証した。
電子投票	茨城県つくば市、株式会社 VOTE FOR	「平成 30 年度つくば Society 5.0 社会実装トライアル支援事業」の事業選定のためのネット投票 ²⁴ において、ブロックチェーン技術を適用する実証実験を実施した。
生産物トレース	カレンシーポート株式会社、株式会社ベジテック、株式会社三菱総合研究所	アマゾンジャパン合同会社及び株式会社日本アクセスが有する食品サプライチェーンにおいて「国内生産者→仲卸→小売」と「海外生産→輸入商社→国内流通商社」の2ルートにて食品トレースを実施した。
	宮崎県綾町、シビラ株式会社、株式会社電通国際情報サービス	生産者、収穫時期、農薬使用の有無など、野菜の生産履歴をブロックチェーンに保存し、情報の真正性を担保・可視化する実証実験を実施した。
公証・KYC	石川県加賀市、株式会社スマートバリュー	地域内サービスの認証を一元化しながら、各サービスで保有するデータを連携するために、KYC 認証基盤を構築している。
	株式会社リクルートテクノロジーズ	ブロックチェーン技術を用いた履歴書公証データベースの実証実験を実施。
文書管理	大分県竹田市、インフォテリア株式会社	文書のハッシュ値をブロックチェーンに登録し、改ざんを検知することができる仕組みを構築した。
不動産登記	株式会社 LIFULL	異業種間で保有されている不動産に関する情報の一元的な管理を目指し、ブロックチェーン基盤の開発や不動産情報コンソーシアム（ADRE）を設立した。 ²⁵
ICO/STO	岡山県西粟倉村	新たな財源を確保して先行投資による地域作りを行っているための手段として、自治体としてトークンを発行して仮想通貨を集める ICO による資金調達の導入を検討している。
貿易情報連携	株式会社 NTT データ	NEDO ²⁶ よりブロックチェーン技術を活用した貿易手続データ連携システムの実現に向けた実証事業を受託し、貿易手続

²⁴ インターネットを通じた投票。

²⁵ カテゴリとしては「不動産登記」としたが、不動産登記の国内の事例はなく、当該事例は「不動産売買」である。

²⁶ 国立研究開発法人新エネルギー・産業技術総合開発機構

		業務に関わる事業者の生産性向上と輸出リードタイム短縮の実現を目指した実証を実施した。
	株式会社三井住友銀行	貿易実務におけるブロックチェーン技術の適用可能性に関する実証実験を実施。書類の作成や点検に係る時間の削減を狙う。

(2)海外事例

海外におけるブロックチェーン技術を利用した情報システム構築や実証実験の事例について、公開情報から調査した。

図表 3-2 において、行政が主体、若しくは主要なステークホルダとして関わるとされたカテゴリについて、公開情報が多い事例を1～2事例ずつ抽出した（図表 3-4）。

図表 3-4 海外におけるブロックチェーン活用事例

カテゴリ	国名	事例概要
地域ポイント	韓国	韓国・江原道が、韓国の法定通貨ウォンと1対1で紐付けた地域通貨をブロックチェーン上で発行する計画を発表した。
電子投票	米国	2018年11月のウエストバージニア州の中間選挙において、海外に駐留する兵士を対象にブロックチェーン投票アプリを利用して投票できる環境を整備した。
	スイス	2018年7月にブロックチェーンを活用した市民投票の実証実験を実施した。
生産物トレース	イギリス	牛肉のサプライチェーンモニタリングシステムにブロックチェーンを活用した。
	中国	豚肉の生産から小売までの流通経路をブロックチェーン上に記録し、生産物の動きをリアルタイムに追跡可能とした。(IBM、Walmart、JD.com(京東商城)、中国の清華大学が共同で実施)
公証・KYC	米国	2018年2月にMITを卒業した学生全員にブロックチェーンに基づく電子卒業証書を授与した。
	マレーシア	NEM ²⁷ を活用し、学位証明を検証するシステムを構築した。
文書管理	イギリス	イギリス国立公文書館が公文書管理にブロックチェーンを適用するプロジェクト(Archangel)に着手した。
	米国	ブロックチェーンを活用した医療免許発行用システムのパイロット運用を実施した。
不動産登記	オランダ	国内の不動産賃貸借契約に係るデータをブロックチェーン上に記録するシステムの構築を予定している。
	スウェーデン	2017年3月ブロックチェーンを活用した土地登録プラットフォームの初期実験を完了した。
ICO/STO	米国	バークレー市がブロックチェーンを活用した地方債を発行した。
	オーストリア	オーストリア政府が、パブリック型ブロックチェーン(イーサリアム)で国債を発行することを予定している。
貿易情報連携	米国等	コンテナ輸送で発生する全ての出荷イベントと関係書類をリアルタイムに共有するために、IBMと海運大手のMaerskが、ブロックチェーンを活用したプラットフォームを提供している。(Tradelens)。
	香港	ブロックチェーンを活用した貿易金融プラットフォーム「eTrade Connect」を用いて、貿易融資申請の承認に必要な時間を短縮し国際貿易の資金調達の効率向上を目指している。

(3)ユースケース設定の考え方と根拠事例

本節では前節で抽出した事例について、その業務や使用する情報システムの中でのプロ

²⁷ ブロックチェーンプラットフォームの一つ。トークン発行や送金などの機能をWebAPIで提供している。

ブロックチェーン技術の具体的な関わり方、事例内における前提、制約等を整理し、次節で検討する汎用的なユースケースの基礎情報として整理する。ここでユースケースとは、ブロックチェーンの活用事例を調査・分析した結果を踏まえ、基本となる業務及びシステム機能を机上で想定し、汎化したものとする。なお、本調査研究では、各事例特有の機能・システムについてはユースケースには含めていない。

図表 3-5 各ユースケースで参考とした事例

ユースケース名	参考とした事例・概要
地域ポイント	<p>かすみがうら市では、ブロックチェーンを活用した湖山ウォレット（アプリ）により「湖山ポイント」を発行しており、市が実施する特定の事業（又はイベント）の参加者にポイントを付与し、参加者が取得したポイントを市内の取扱店で使用することで、定住人口・交流人口の増加及び消費喚起による市内経済の活性化に寄与することを目指している。</p> <p>なお、その他にもブロックチェーンを活用した地域ポイントや地域通貨としては会津若松の白虎コイン²⁸など²⁹、様々な地域において取り組まれており、特に直近³⁰では、「プレミアム付商品券」として、静岡県³¹及び大阪府³²等において実証実験が行われている。</p> <p>湖山ポイントは自治体から参加者（住民）、参加者（住民）から取扱店（店舗）という一方向の流れであるが、その他の事例では参加者間でのポイントの譲渡・交換等、様々な仕組みや、それを実現するためのシステム構成が検討されている。</p>
電子投票 ³³	<p>茨城県つくば市では、IoT・AI・ビッグデータ解析などの革新的な技術を活かした市内での実証実験の支援を行っており、平成 30 年 8 月に行われた「平成 30 年度つくば Society 5.0 社会実装トライアル支援事業」の企画提案の最終審査において、マイナンバーカードとブロックチェーンを活</p>

²⁸ 白虎コインは会津大学の学内仮想通貨であり、会津大学ではそのほかに電子バウチャーの「キマ☆チケ」等の実証実験を実施している。

²⁹ 飛騨高山のさるぼコインは実証実験においてブロックチェーンの利用を検討したものの、決済処理に要する時間が長かったため、本番のサービスでは導入を見送っている。

³⁰ 本稿執筆時点(2019年3月)

³¹ 地域コイン社会実験の実施について、「地域コイン社会実験」実行委員会、
<https://www.city.hamamatsu.shizuoka.jp/shise/koho/koho/hodohappyo/h31/2/documents/2019020602.pdf>,
2019/3/22 確認

³² ～「実証事業都市・大阪」実現に向けた実証事業支援～ 大阪上本町駅周辺でのデジタル地域通貨の実用化に向けた実証の実施について、大阪商工会議所、http://www.osaka.cci.or.jp/Chousa_Kenkyuu_Iken/press/190201dmoney.pdf,
2019/3/22 確認

³³ つくば市の実証実験を支援した VOTE FOR 社では、「電子投票」は投票所内で電子機器を用いる投票を指すことが多いため、それらと明確に区別するためにつくば市の事例を「インターネット投票（ネット投票）」と位置付けている。

ユースケース名	参考とした事例・概要
	<p>用したネット投票(電子投票)を導入した。</p> <p>当該実証実験により、マイナンバーカードによる本人認証によって投票の真正性を担保し、更にブロックチェーンによって投票データの改ざんや消失を防止できることを実証した。</p>
生産物トレース	<p>宮崎県綾町は、「有機 JAS 登録認定機関」に登録されている町である。</p> <p>2016 年から 2017 年にかけて、株式会社電通国際情報サービスの企画により、シビラ株式会社の製品 Broof を活用して構築するブロックチェーン上に野菜の生産履歴を書き込む実証実験を行った。この情報は購買者が購買時点で参照することができ、価格を 2 倍に設定したにもかかわらず、早々に完売する結果が得られている。</p>
公証・KYC	<p>米国マサチューセッツ工科大学（以下、MIT）は 2018 年 2 月に卒業した学生の卒業証書を電子化しブロックチェーン上に卒業証書のハッシュ値を保存した。企業側は学生から提出された卒業証書の真正性を、ブロックチェーン上に保存されたハッシュ値と比較することで確認可能となり、従来照会に要していた労力の削減が期待される。</p> <p>国内の KYC の事例としては、加賀市とスマートバリュー社の取組が挙げられる。地域内サービスの認証を一元化しながら、各サービスで保有するデータを連携するために、KYC 認証基盤を構築している。</p>
文書管理	<p>大分県竹田市では IT による地域活性化を模索しており、2018 年 7 月に市職員向けに開催した「ブロックチェーン技術勉強会」で紹介された文書改ざん検知ソリューションを試用した。</p> <p>当該ソリューションでは文書のハッシュ値を生成し、それをブロックチェーン上に格納することで文書の改ざんの有無を確認できるとしている。</p>
不動産登記	<p>不動産登記システムについては、登記情報に求められる透明性や追跡可能性、耐改ざん性からブロックチェーンとの親和性が各国で論じられており、日本では bitFlyer 等による不動産登記への応用に関する検討資料が公表されている。そこでは全国の登記所からのアクセスと登記された情報の恒久的なデータ保持を可能とするシステムが論じられている。</p>
ICO/STO	<p>法整備途上ではあるが、資金調達の一手段として ICO/STO の導入が検討されている。現在、幾つかの自治体で ICO/STO の実施が予定されており、ERC20 トークン³⁴を用いた自治体独自トークンの発行が検討されている。自治体主体の ICO/STO は構想段階であるが、仮想通貨（暗号資産）における ICO/STO 事例が参考となり得る。国内では岡山県西粟倉村の取組が事例</p>

³⁴ ERC20 トークンとは、「ERC20」というイーサリアムの統一規格に基づいて発行されたトークンを指す。

ユースケース名	参考とした事例・概要
	として挙げられる。
貿易情報連携	<p>貿易に関する手続は、契約のような民間企業同士のやり取りの他、税関における輸出入許可等の行政に係る手続もあり、多数の文書やステークホルダが存在する。それらの手続において、未だ多くの文書が紙でやり取りされており、各ステークホルダにおいて膨大な手間やコストがかかっている。</p> <p>このような状況に対し、2018年12月よりIBMとMaersk³⁵が提携してサービス展開している TradeLens は効率的かつ安全な国際貿易の促進を目指すものであり、ブロックチェーンを活用した情報共有や透明性の確保を提供しようとしている。</p> <p>また NTT データにおいても同じくブロックチェーン技術を活用して貿易手続データの共有、電子書類の原本性確保を目指している。国内において2017年度より、貿易に関する主要5業界の企業が企業/グループ/業態の枠を超えた公平性・中立性の高い貿易コンソーシアムを発足し、実用化に向けた検討を進めている一方、海外ではシンガポール当局やタイでの接続実験を実施している。官民連携においても2018年度のNEDO事業として、貿易手続データ連携システムの実現に向けた実証事業を受託しており、貿易手続業務に関わる事業者の生産性向上と輸出リードタイム短縮の効果を検証している。</p>

³⁵ A.P. Moller – Maersk はデンマークに本社を持つ海運会社

3.3 ユースケースの想定

前節で整理した情報に基づき、事例個別の事情を捨象し、汎化したブロックチェーン技術適用のユースケースを、図表 3-6 に示す観点に基づき 3.4(1)~3.4(8)のとおり想定する。

図表 3-6 各ユースケースの説明項目

番号	説明項目	内容
①	ブロックチェーン活用の背景・課題認識	ブロックチェーンを活用に取り組んだ背景や課題認識、並びに業務及びブロックチェーンを活用したシステムの概要
②	ブロックチェーン利用イメージ	ブロックチェーンを活用したシステムの主たる利用者とシステム利用のイメージ
③	システムに必要な機能	各ユースケースの実現に必要な機能（ブロックチェーン以外を含む）と、当該機能の中でのブロックチェーンの特性が発揮される場面
④	ブロックチェーン導入後の業務フロー	ブロックチェーンの導入後に想定される業務フロー
⑤	ヒアリング先の評価	ヒアリング時に聴取したユースケースに対するコメント
⑥	ブロックチェーン活用の前提・留意事項等	ユースケースにおいてブロックチェーン技術を活用するにあたっての前提・留意事項
⑦	備考・特記事項	上記以外の備考・特記事項

(1)地域ポイント

本項では、地域ポイントにブロックチェーンを使用するユースケースについて検討する。

① ブロックチェーン活用の背景・課題認識

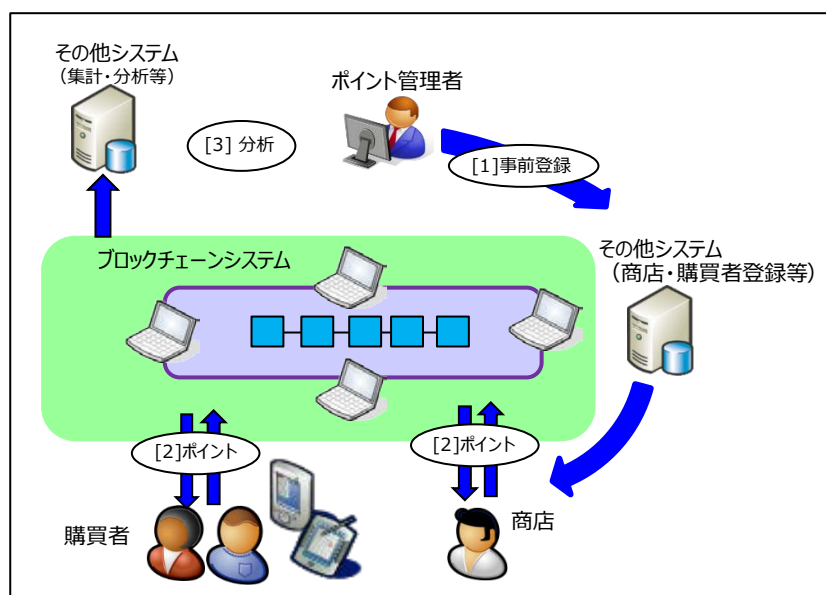
- ・地域ポイントとは、当該地域の経済活性化等を目的として、地域住民や地域を訪れる観光客に対し、地域内の商品やサービスの購入時に用可能な“ポイント”を付与するものである。
- ・従来の方法は、紙にポイント額を印刷し、それを対象者に配布することでポイントの付与を行っていた。
- ・しかしながら、それらの方法は印刷や偽造防止等にコストを要し、更にポイントの流通状況（利用状況）が不明であるなど、効率性や検証性に欠けていた。
- ・本ユースケースで対象とする地域ポイントは、紙を使用せず電子的なやり取りで完結するものを指し、これらは二次元コードやスマートフォンアプリによる決済や参加者などの顧客管理等と合わせ、我が国におけるキャッシュレス化を推進していく可能性を持っている。

② 地域ポイントとブロックチェーン利用イメージ

本ユースケースにおける主たる利用者とシステム利用イメージを図表 3-7 に示す。

地域ポイントは、ポイントの発行や管理を行う「ポイント管理者」が「購買者」や「商店」に対してポイントを付与し、「購買者」及び「商店」は地域内の商品やサービスとポイントを交換する。

図表 3-7 地域ポイントとブロックチェーン利用イメージ



③ システムに必要な機能

想定するシステム全体の主たる機能及びブロックチェーンが対応する機能を整理した。

(図表 3-8)

図表 3-8 地域ポイントに関連するシステム機能 (例)

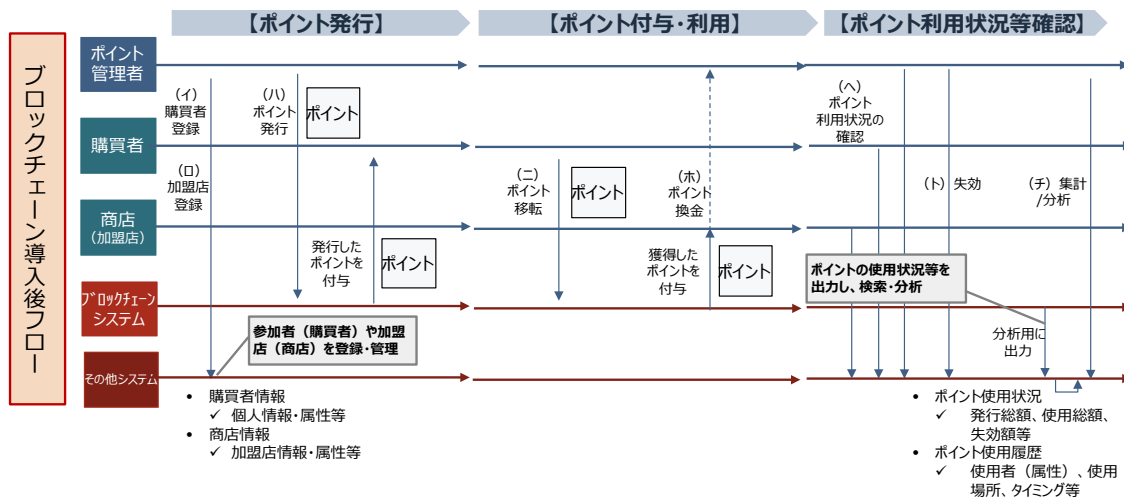
地域ポイントに関連するシステム機能 (例)				
業務	搭載機能	利用者	機能内容	対応する ブロックチェーン機能
[1] 事前登録	(イ) 購買者登録	ポイント管理者	ポイントを使用する購買者の情報をシステムに登録する。	
	(ロ) 加盟店登録	ポイント管理者	ポイント購入に対応する加盟店(商店)をシステムに対応する。	
[2] ポイント	(ハ) ポイント発行	ポイント管理者	購買者に相応分 ³⁶ のポイントを付与する。 (発行ポイントの利用は1回限りとし、循環しないことを前提)	所有権の移転情報の反映
	(ニ) ポイント移転(商品購入、決済)	購買者	加盟店から商品をポイントで購入することより、購買者の保有ポイントを減じ、加盟店の保有ポイントを増やす。	所有権の移転情報の反映、主体とその内容の真正性が証明された情報の登録・参照、二重処理の防止
	(ホ) ポイント換金	購買者、商店	加盟店、購買者の保有ポイントを換金し、応分のポイントを消費する。	
	(ヘ) ポイント利用状況の確認	ポイント管理者、購買者、商店	加盟店、購買者のポイント利用状況や残高を確認する。	
	(ト) 失効	ポイント管理者、購買者、商店	有効期限の切れた、又は別事情により発行したポイントを失効化する。「ポイント全体」と「部分(参加者、加盟店に紐付いたポイント)」がある	
[3] 分析	(チ) 集計/分析	ポイント管理者	ポイントの利用状況について、購買者、加盟店属性をパラメータとし、各種の分析を行う。	

³⁶ 金銭と交換、又は別理由による個別付与

④ ブロックチェーン導入後の業務フロー

システム導入後の業務の流れについて、主たる利用者、実施場面、利用機能が明確になるよう整理した。(図表 3-9)

図表 3-9 ブロックチェーン導入後の業務フロー (地域ポイント)



⑤ ヒアリング先の評価

- ・ブロックチェーンが優位性を発揮するのは、オープンで、価値移転を伴う仕組みが必要なシステムである。シンプルな価値移転を淡々と反復継続するような業務であれば、セキュリティの担保も軽く済み、明確なコスト削減の効果が期待できる。
- ・一方、ブロックチェーン技術を適用しても、一概にコストが安くなったり、セキュリティが高まったりするわけではない。通常システムと同様に、作り手が慣れているか、既存のもの流用か、といった要素に大きく左右される。既存システムの仕組みに被せるような形で構築しようとしても、複雑になってしまい、メリットはあまり出ない。
- ・価値移転をトレースできる仕組みを活用すれば、地域ポイントがどのような乗数効果を生んだかを定量的に把握することも可能となる。

(以上、Sound-FinTech ヒアリングより)

⑥ ブロックチェーン活用の前提・留意事項等

- ・地域ポイントを実現する方法として様々なシステム構成が考えられるが、ブロックチェーンを利用する場合であっても、ユーザ登録や決済用のアプリケーションなど、周辺のシステムを整備する必要がある。
- ・その中でブロックチェーンに期待されるのはセキュリティ面である。ブロックチェーンを使うことで、不正な取引や二重の支払いなどがなされないような機能の開発が不要になるのであれば優位性は高い。
- ・一方、ブロックチェーン以外でも地域ポイントを電子的に実現する方法は存在し、処理速度等の要件によってはブロックチェーンの利用が難しくなることも想定される。

⑦ 備考・特記事項

図表 3-5 で示したとおり、各地域において「プレミアム付商品券」としてブロックチェーンを活用した実証実験が行われている。これは総務省における「行政や公共性の高い分野におけるブロックチェーン技術の活用及び社会実装に向けた調査研究」事業の検討テーマの1つとして取り上げられており、地域ポイントへのブロックチェーン活用の期待が存在することを示している。

(2)電子投票

本項では、電子投票にブロックチェーンを使用するユースケースについて検討する。

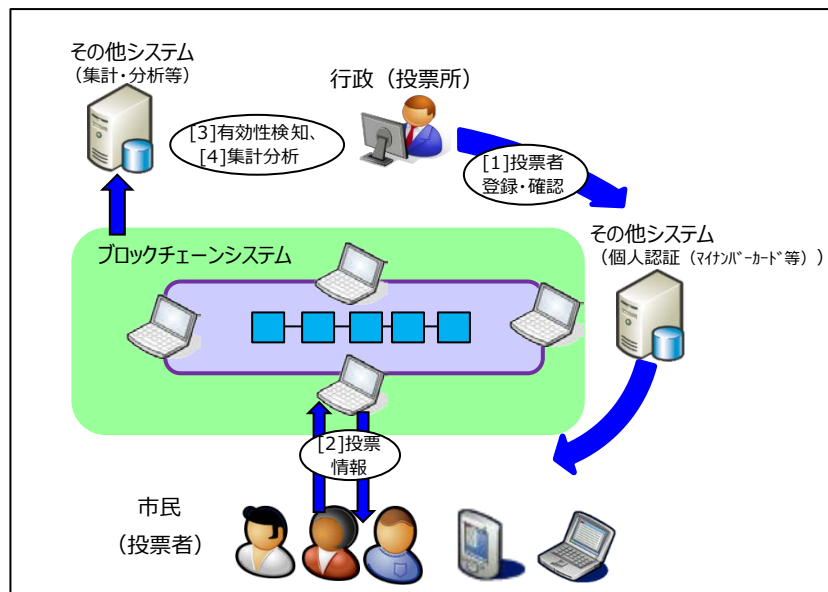
① ブロックチェーン活用の背景・課題認識

- ・従来の投票方法は、紙の投票用紙を使用し、指定された投票所で本人確認を行った上で投票を実施し、それを集計して結果を得るものである。
- ・電子投票とは、紙の投票用紙ではなく、インターネット等の通信手段を用いて投票を行うものである。本人確認の点で課題はあるものの、投票所への来所不要、投票記載内容の上書きなどを行える可能性を持っている。その中でもブロックチェーンに投票結果を格納する方式は、投票結果の改ざん防止において特に優位なものとして期待されている。

② 電子投票システムとブロックチェーン利用イメージ

本ユースケースにおける主たる利用者とシステム利用イメージを図表 3-10 に示す。

図表 3-10 電子投票システムとブロックチェーン利用イメージ



③ システムに必要な機能

想定するシステム全体の主たる機能及びブロックチェーンが対応する機能を整理した。

(図表 3-11)

図表 3-11 電子投票に関連するシステム機能 (例)

電子投票に関連するシステム機能 (例)				
業務	搭載機能	利用者	機能内容	対応する ブロックチェーン機能
[1] 投票者 登録・確 認	(イ) 投票者登 録	行政	投票する権利を持つ投票者情報 をシステムに登録する。	
	(ロ) 投票対象 者確認	行政	投票時に、システムにアクセスし た者が投票する権利を持った者 かどうかを確認する。	
[2] 投票情 報	(ハ) 投票情報 記録	市民	投票権利者が何に ³⁷ 投票した、と いう情報を記録する。	主体とその内容の真正 性が証明された情報の 登録・参照、二重処理の 防止
	(ニ) 投票情 報参照	市民	投票した内容について、投票者 本人がその内容 ³⁸ を確認する。	履歴・過程情報が参照 可能 (トレーサビリティ)
[3] 有効性 検知	(ホ) 投票有効 性検知	行政	投票情報について、有効/無効判 断や多重集計されてないか検知 する。	
[4] 集計分 析	(ヘ) 集計、出 力	行政	投票結果を集計し、出力 (画面、 帳票) する。	
	(ト) 分析	行政	年代別、地域別等の投票状況、傾 向を分析する。	

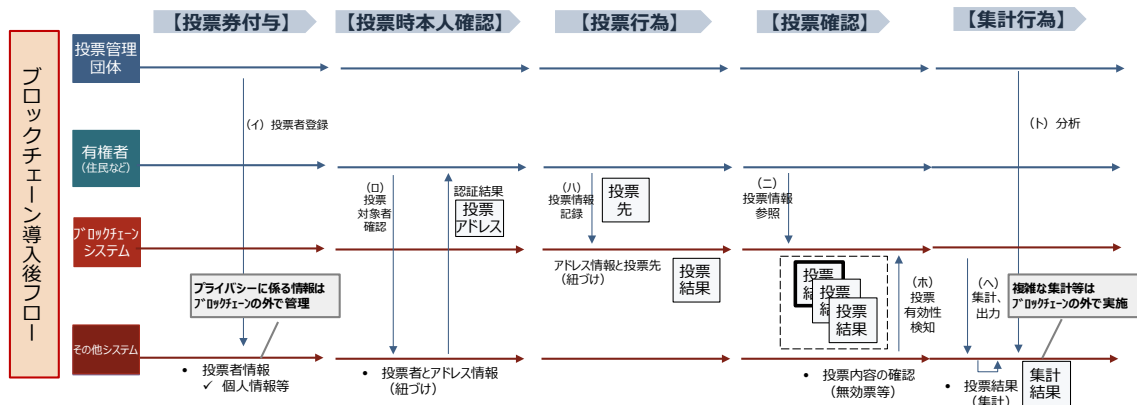
³⁷ つくば市の実証実験では、投票の秘密を担保するため、投票者情報と投票内容を紐付けず、管理者からも見られない仕様としている。

³⁸ 投票者は自身の投票先を把握できるが、行政等は集計結果を参照可能なものの、各投票者個人の投票先までは確認できない。

④ ブロックチェーン導入後の業務フロー

システム導入後の業務の流れについて、主たる利用者、実施場面、利用機能が明確になるよう整理した。(図表 3-12)

図表 3-12 ブロックチェーン導入後の業務フロー（電子投票）



⑤ ヒアリング先の評価

- ・電子投票は投票結果に対する透明性とそれに紐付く投票内容の真正性が重要であり、投票結果に対して第三者による確認や検証を可能とする必要がある。
- ・投票において自分の一票が確実に集計されているというのは民主的な選挙の大前提であり、ブロックチェーンはデータの透明性の観点からも意義深い仕組みである。
- ・また、開票結果について集計ミスがないかどうか、ブロックチェーンによって第三者による検証が可能である。
- ・世界的に見ても投票へのブロックチェーン適用、ネット投票の実現は様々なところでニーズがある。特に途上国では、投票環境を自分で選べるようになること自体重要な意味を持つ。

(以上、VOTE FOR ヒアリングより)

⑥ 本ユースケースにおけるブロックチェーン活用の前提・留意事項等

- ・ブロックチェーンは、投票結果の改ざん防止に効果を発揮するが、投票者の本人確認は別の仕組み（補完システム）³⁹が必要となる。
- ・また、投票者の個人情報や投票者と投票先の対応関係については、漏洩防止の対策が必要である。

³⁹ つくば市の事例ではマイナンバーカードを用いた本人認証を行っており、その他、米国のウエストバージニア州の取組では生体認証等を用いている。

- ・集計の内容や投票の規模にもよるが、後述のアンケート調査のように電子投票を拡張的に捉え、複雑な集計等を行う場合は、投票結果をブロックチェーンから出力する仕組みが必要となる。

⑦ 備考・特記事項

投票を「投票者がいずれかの選択肢を選択すること」と捉えると、これはアンケートなどの調査と共通する部分が多い。ブロックチェーンによる電子投票を拡張することにより、透明性や真正性を担保しつつ、多様なアンケート調査の電子的な実現も可能になるのではないか、という示唆が得られた。

(3)生産物トレース

本項では、生産物トレーサビリティにブロックチェーンを使用するユースケースについて検討する。

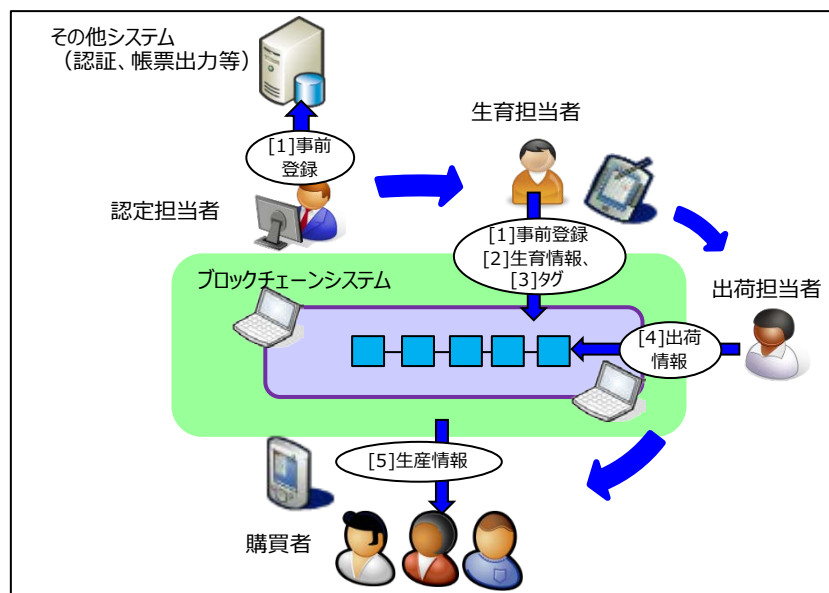
① ブロックチェーン活用の背景・課題認識業務・システム

- ・有機 JAS など品質基準や表示基準に合格した農林物質（生産物）について、生産者、生産過程をブロックチェーンに記録し、購入時に各商品の履歴を個別にトレースできるようにする。
- ・生産物トレースにより、購買者に他の生産物と品質の差を明確に示せることで店頭単価を上げることが期待される。その行政区や農産物自体のブランド力向上に繋がると考える。

② 生産物トレースシステムとブロックチェーン利用イメージ

本ユースケースにおける主たる利用者とシステム利用イメージを図表 3-13 に示す。始めに生産物、生産者の認定登録をした後、生産物の生育状況や出荷情報を担当者が登録する。購買者は、購買時にこの登録された情報をスマートフォン等により照会でき、生産過程を確認することができる。

図表 3-13 生産物トレースシステムとブロックチェーン利用イメージ



③ システムに必要な機能

想定するシステム全体の主たる機能及びブロックチェーンが対応する機能を整理した。(図表 3-14)

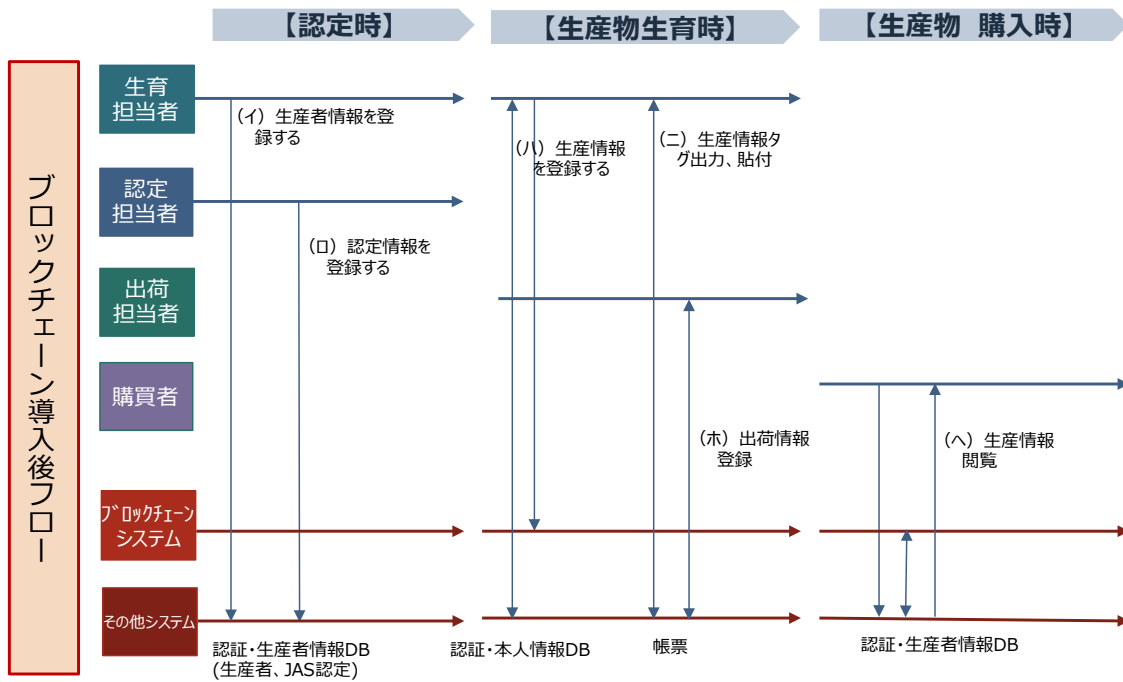
図表 3-14 生産物トレースに関連するシステム機能 (例)

生産物トレースに関連するシステム機能 (例)				
業務	搭載機能	利用者	機能内容	対応する ブロックチェーン機能
[1] 事前登録	(イ) 生産者登録	生育担当者	生産者情報をシステムに登録する。	
	(ロ) 生産物認定情報登録	認定担当者	公的機関等が認定した生産物や生産環境(土壌等)に登録する。	
[2] 生育情報登録	(ハ) 生育情報登録 (生産物×生産者・認定情報)	生育担当者	生産者が認定された条件下で生産物を作ったということを自身と紐付けて登録する	主体とその内容の真正性が証明された情報の登録・参照
[3] タグ出力	(ニ) 生産情報タグ出力	生育担当者	上記で登録された生産情報について固有のタグを出力する。このタグは生産物のパッケージに貼る。	
[4] 出荷情報登録	(ホ) 出荷情報登録	出荷担当者	タグを貼った生産物パッケージの出荷の情報をシステムに登録する。	主体とその内容の真正性が証明された情報の登録・参照
[生産情報閲覧]	(ヘ) 生産情報閲覧	購買者	購買者がスマートフォン等のアプリを通し、タグ情報を基にブロックチェーン内のデータ等を閲覧し、認定された生産物であること、生育情報を確認する。	履歴・過程情報が参照可能(トレーサビリティ)

④ ブロックチェーン導入後の業務フロー

システム導入後の業務の流れについて、主たる利用者、実施場面、利用機能が明確になるよう整理した。(図表 3-15)

図表 3-15 ブロックチェーン導入後の業務フロー (生産物トレース)



⑤ ヒアリング先の評価

- 生産物トレースのケースでは、ブロックチェーン技術を NFC タグ⁴⁰と組み合わせることで記録の改ざんを防止できる仕組みを作ることができ、安全性が担保されていることを証明するために役立つ。
- 消費者が価値を感じるのは、情報システムを通じて写真等により特定の生産物の履歴を追えるということである。それを証明するプロセスまで理解してもらうことは困難なのかもしれない。ただし、ブロックチェーンは、改ざんに対する安全性の担保という点でその力を発揮できる余地があるのではないか。
- 実証実験で販売した野菜は市価の 2 倍以上の価格を設定したにもかかわらず 2, 3 時間で完売するなどの成果を得た。
(以上、宮崎県綾町ヒアリングより)

⑥ 本ユースケースにおけるブロックチェーン活用の前提・留意事項等

- ブロックチェーン内に記録された情報については改ざんされることはない。ただし、

⁴⁰ 無線によるタッチ通信が可能な安価で製造できる IC チップ付のタグ

ブロックチェーン内に記録する「生産物が認定された環境、生産者により作られたかどうか」についてはブロックチェーンシステム外で第三者が確認、証明し、それを登録する仕組みや補完するシステムが必要となる。このシステム間でデータの紐付けに（例えば、生産者と生産物）ついて登録漏れや不整合があった場合、システム全体としての信頼を失うことになる。

- ・ 購買者はスマートフォン等、自身が所有するモバイル機器を通じて生産物の生育履歴情報を確認することになる。ただし、購買者自身の機器にブロックチェーンのデータを入れることはなく、アプリケーションを通じて確認することになる。モバイル機器側のアプリケーションを含めて、ブロックチェーンのデータをスムーズに検索、表示できるようにする必要がある。

(4)公証・KYC

本項では、公証・KYC にブロックチェーンを使用するユースケースについて検討する。なお、公証と KYC はいずれも提示された書類の真正性を確認する作業を代替するものであり、類似度が高いと考えられるため、本調査報告書内では同一のカテゴリとして取り扱うこととした。

① ブロックチェーン活用の背景・課題認識

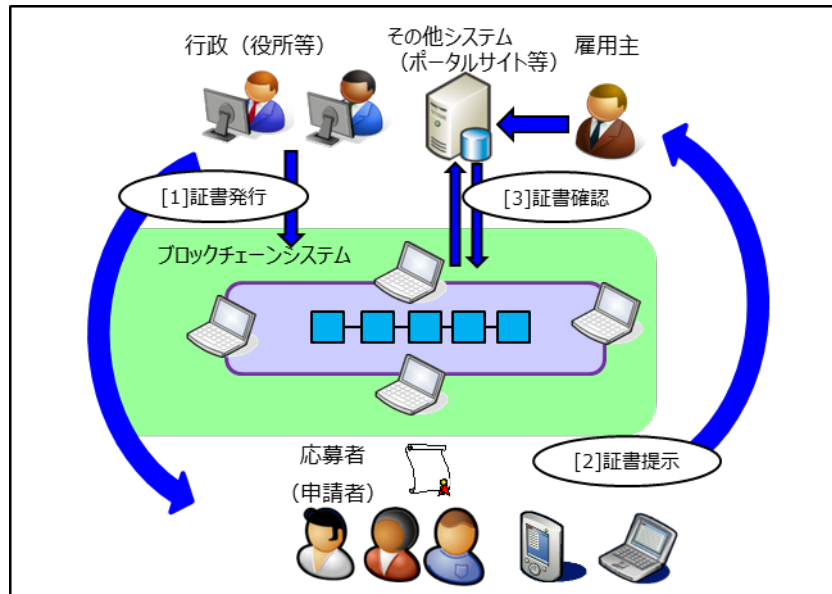
- ・公証とは本来的には、公証人が特定の事実を証明する行為である。MIT の事例であれば、MIT が公証人の立場で卒業証書を発行する。雇用主（発行主体以外）が当該資料を確認したい場合、MIT に問い合わせをしない限りは、改ざんの有無を確認することはできなかったが、卒業証書（証書）のハッシュ値をブロックチェーンに登録し、ハッシュ値を計算し、ブロックチェーン上に登録されたハッシュ値と一致するか確認することで改ざんの有無を検証することを可能とした。
- ・KYC（Know Your Customer）とは、本人確認に係る書類や手続の総称であり、特に銀行で口座開設をする際など等に使用される。提出された書類の真正性確認に係るコストが問題視されていたが、ブロックチェーンに一度確認した結果を登録し、当該データを活用することで、確認に係るコストを抑えることが可能になった。

② 公証・KYC とブロックチェーン利用イメージ

本ユースケースにおける主たる利用者とシステム利用イメージを図表 3-16 に示す。

- ・本ユースケースでは、公証人として行政（役所等）がブロックチェーン上に、証書のハッシュ値を登録する。証書の真偽を確認する者（雇用主等）は応募者から提出された証書からハッシュ値を計算し、ブロックチェーン上に登録されたハッシュ値と一致するか確認することで改ざんの有無を検証することができる。

図表 3-16 公証・KYC とブロックチェーン利用イメージ



③ システムに必要な機能

想定するシステム全体の主たる機能及びブロックチェーンが対応する機能を整理した。
 (図表 3-17)

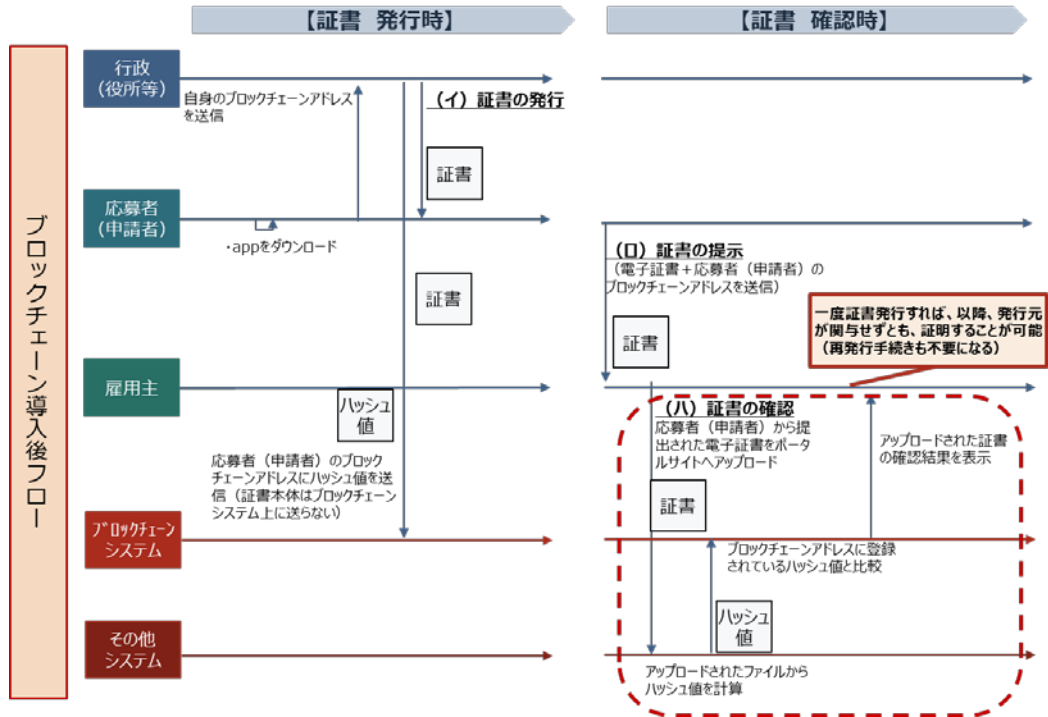
図表 3-17 公証に関連するシステム機能（例）

公証に関連するシステム機能（例）				
業務	搭載機能	利用者	機能内容	対応する ブロックチェーン機能
[1] 証書の発行	(イ) 証書の発行	行政（役所等）	証書を発行する。	主体とその内容の真正性が証明された情報の登録・参照
[2] 証書の提示	(ロ) 証書の提示	応募者（申請者）	証書を提出する。	
[3] 証書の確認	(ハ) 証書の確認	雇用主	提出された証書が正しいものかを確認する。疑いがある場合は、証書の発行主体に事実確認を行う。	誰でも閲覧することが可能（透明性の高い取引）

④ ブロックチェーン導入後の業務フロー

システム導入後の業務の流れについて、主たる利用者、実施場面、利用機能が明確になるよう整理した。(図表 3-18)

図表 3-18 ブロックチェーン導入後の業務フロー (公証)



⑤ ヒアリング先の評価

- ・大学の統廃合や働き方の多様化が進展する中、統廃合により存続しなくなった大学での学位やスタートアップでの経歴などの真正性をどうやって検証するかが課題になりつつある。米国のマサチューセッツ工科大学やキプロス共和国のニコシア大学などではすでにブロックチェーン技術を用いた学位発行が実施されていることから、ブロックチェーン技術を適用した公証の仕組みはそうした社会的課題の解決手段の1つになり得ると考えられる。
- ・近年、研究データの不正が大きな問題となっている。海外では研究データ管理におけるブロックチェーン技術の適用可能性が検討されている (ドイツの Blockchain for Science や米国の Enigma など)。ブロックチェーン技術を活用することで、プライバシー保護や、スマートコントラクトによる研究プロセスの整合性向上を図ることができる可能性がある。

(以上、リクルートヒアリングより)

- ⑥ 本ユースケースにおけるブロックチェーン活用の前提・留意事項等
- ・ブロックチェーン内の本人識別情報と補完システムとの紐付けにミスがあると信頼を失う。
 - ・有効期限のある証明情報については別途それを管理するための機能が必要。

(5)文書管理

本項では、文書管理にブロックチェーンを使用するユースケースについて検討する。

① ブロックチェーン活用の背景・課題認識

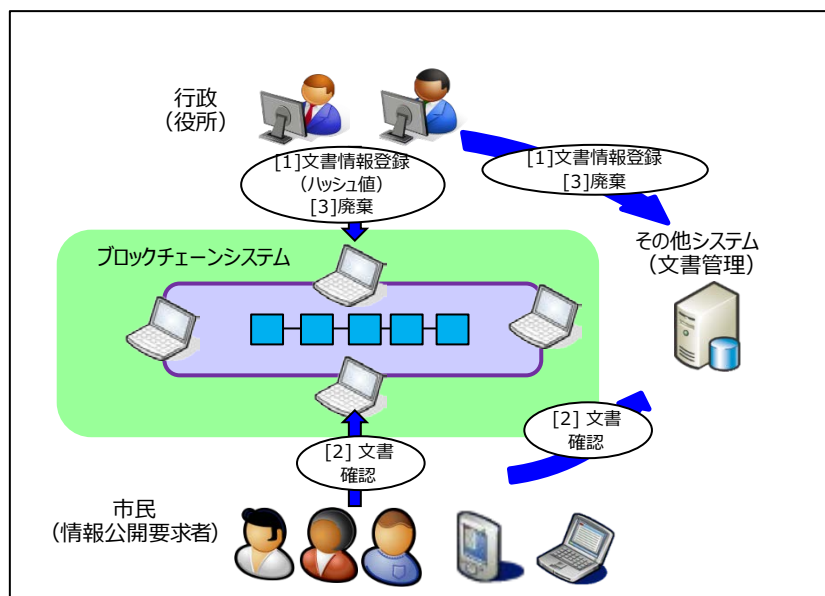
- ・行政における文書管理は真正性や耐改ざん性が強く求められるものの、大半を紙で保有していることもあり、文書の作成、保存、移管等の過程で紛失するリスクがある。また、内容が改ざんされた場合でもそれを検知することは困難である。
- ・現在、政府としては、文書を電子化し、作成から保存、移管又は廃棄まで一貫して電子的に管理することを目指している⁴¹。
- ・上記のような課題認識に対して、ブロックチェーン技術によって故意又は過失による文書の改ざんを容易に検知することが期待できる。

② 文書管理とブロックチェーン利用イメージ

本ユースケースにおける主たる利用者とシステム利用イメージを図表 3-19 に示す。

本ユースケースでは、「行政」が作成した電子ファイルのハッシュ値をブロックチェーンに格納することにより、それらの文書が改ざんされていないことを「市民」が確認するシステムを検討する。

図表 3-19 文書管理とブロックチェーン利用イメージ



⁴¹ 行政文書の電子的管理についての基本的な方針（骨子案），第 72 回公文書管理委員会資料

③ システムに必要な機能

想定するシステム全体の主たる機能及びブロックチェーンが対応する機能を整理した。

(図表 3-20)

図表 3-20 文書管理に関連するシステム機能 (例)

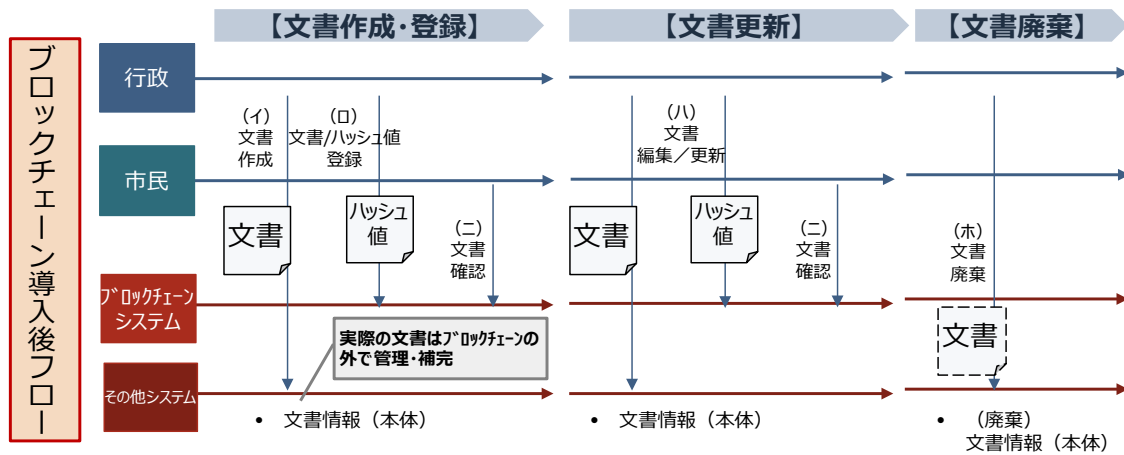
文書管理に関連するシステム機能 (例)				
業務	搭載機能	利用者	機能内容	対応する ブロックチェーン機能
[1] 文書情報登録/ ハッシュ値登録	(イ) 文書作成	行政	文書を作成する。	
	(ロ) 文書・ハッシュ値登録	行政	作成した文書及びハッシュ値を登録する。	主体とその内容の真正性が証明された情報の登録・参照
	(ハ) 文書編集／更新	行政	作成した文書を編集し、文書及びハッシュ値を更新 ⁴² する。	主体とその内容の真正性が証明された情報の登録・参照
[2] 文書確認	(ニ) 文書確認 (真正性確認)	市民	登録された文書を信頼できるものか確認する。	主体とその内容の真正性が証明された情報の登録・参照
[3] 廃棄	(ホ) 文書廃棄	行政	登録された文書を廃棄する。	

④ ブロックチェーン導入後の業務フロー

システム導入後の業務の流れについて、主たる利用者、実施場面、利用機能が明確になるよう整理した。(図表 3-21)

⁴² 初回の文書登録時と同様にハッシュ値を登録し直す。

図表 3-21 ブロックチェーン導入後の業務フロー（文書管理）



⑤ ヒアリング先の評価

- ・実証実験では、ブロックチェーンを用いて電子文書の不当な改ざんを検知することが可能であるかを検証した。
- ・実験の結果はあらかじめ見えていたが、分かりやすい実験を行うことで、ブロックチェーンとは何かについて市職員に目を向け、知ってもらうことを意図した。
- ・実証実験を通じて、導入時の課題として新たに認識されたことは特になかったが、敢えて言えば、登録時に不正をされたり、出力後に不正をされたりすると防ぎようがないことが挙げられる。こうしたシステム外の部分は今後も人間が監視せざるを得ないだろう。

(以上、竹田市ヒアリングより)

⑥ 本ユースケースにおけるブロックチェーン活用の前提・留意事項等

- ・行政文書は、作成から廃棄までのプロセス全体で電子化することと併せて、電子化した文書の真正性確保に関するニーズも強く存在する。
- ・真正性の確保について、文書ファイルの改ざん検知を実現するのであれば、文書そのものではなく文書のハッシュ値をブロックチェーンに格納する方が現実的である。
- ・ブロックチェーン登録後の文書データ（ハッシュ値）に対する真正性や対改ざん性は高まるといえる。ただし、登録前の文書作成時点における不正抑止や登録時の誤りの扱いについては別途検討が必要である。

(6)不動産登記

本項では、不動産登記にブロックチェーンを使用するユースケースについて検討する。

① ブロックチェーン活用の背景・課題認識

- ・不動産登記とは、土地や建物の所在や大きさ、所有者の住所氏名を登記簿に登録し、国民に公開する一連の業務を指す。これによって、不動産にかかる権利関係が明らかにされ、取引や権利主張の確認が円滑に行えるようになる。
- ・不動産登記システムは、不動産における権利や現況に係る情報の申請や提供、及びそれに伴う各種登記事務を担うシステムであり、1988年以降、コンピュータシステム化が整備され、現在では全国にある登記所拠点からオンラインでアクセスすることができるようになっている。
- ・行政サービスとして、平日の行政窓口対応時間に停止することなく稼働することが求められており、日々大量に発生する登記事項の読み込みや書き出しに対応できることが求められる。
- ・ブロックチェーン技術を不動産登記システムへ適用できるかについては bitFlyer 社の竹井氏が技術検証を行っており、不動産登記情報が持つ特徴として図表 3-22 に示す要件を挙げている。

図表 3-22 不動産登記情報の特徴⁴³

要件	内容
完全性が極めて重要である	<ul style="list-style-type: none"> ● 登記された事項について、一切の改変が許されない ● 記載事項の消去が存在せず、抹消線を引いて履歴は残す
高い公共性がある	<ul style="list-style-type: none"> ● 公示の原則の基、誰もが閲覧できることが重要（住民登録と異なる点） ● 障害等によりシステムが稼働できない状況が許されない
記載された情報について、利害関係が明確に存在する	<ul style="list-style-type: none"> ● 土地の権利の移転など、大きな価値のやり取りが発生しうる

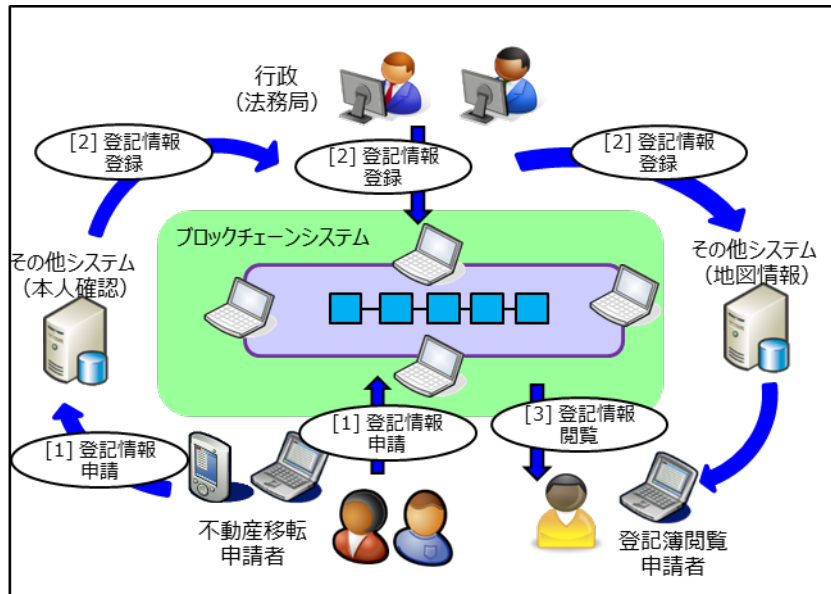
② 不動産登記システムとブロックチェーン利用イメージ

本ユースケースにおける主たる利用者とシステム利用イメージを図表 3-23 に示す。不動産登記に係る申請は、ブロックチェーン外にある本人確認システムによる確認を経て、申請者が指定する不動産について登記申請がなされる。行政側は本人確認情報と申請内容を踏まえ登記情報を登録し、適宜地図情報システムと連携する。登記簿閲覧申請においては、申請者が申請し指定する不動産についてのブロックチェーン上の情報とそ

⁴³ bitFlyer 竹井悠人氏「ブロックチェーンの不動産登記への応用に関する検討」, 2018/11/27, 第6回リーガルテック展 2018, <https://www.slideshare.net/YutoTakei/ss-124129518>, 2019/3/18 確認、転記

の不動産の地図情報が閲覧できる。

図表 3-23 不動産登記システムとブロックチェーン利用イメージ



③ システムに必要な機能

想定するシステム全体の主たる機能及びブロックチェーンが対応する機能を整理した。(図表 3-24)

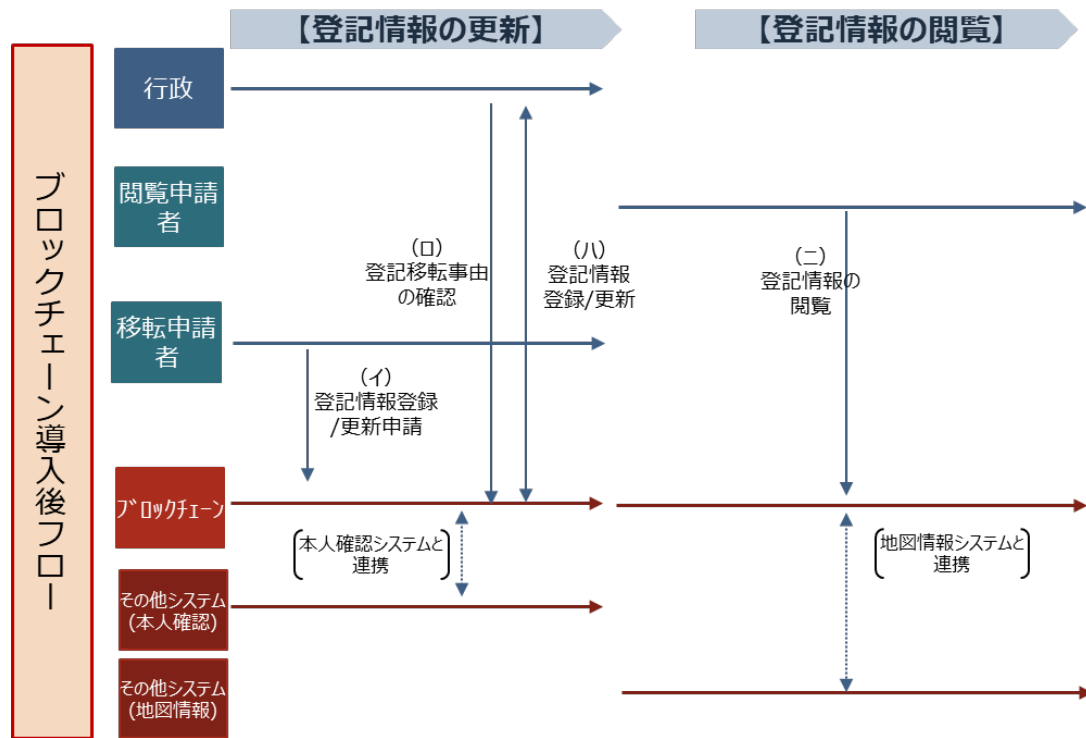
図表 3-24 不動産登記に関連するシステム機能 (例)

不動産登記に関連するシステム機能 (例)				
業務	搭載機能	利用者	機能内容	対応する ブロックチェーン機能
[1] 登記情報申請	(イ) 登記情報登録/更新申請	市民	登記情報を新たに登録又は更新する申請を行う。	
[2] 登記情報登録	(ロ) 登記移転事由の確認	行政	登記移転事由として、相続や売買等の証拠を確認する。	
	(ハ) 登記情報登録/更新	行政	正しい申請者及び登記移転事由を確認した上でその登記情報を登録又は更新する。	所有権の移転情報の反映、主体とその内容の真正性が証明された情報の登録・参照
[3] 登記情報閲覧	(ニ) 登記情報の閲覧	市民	自身又は他者が保有する土地の登記情報を確認する。	誰でも閲覧可能、主体とその内容の真正性が証明された情報の登録・参照

④ ブロックチェーン導入後の業務フロー

システム導入後の業務の流れについて、主たる利用者、実施場面、利用機能が明確になるよう整理した。(図表 3-25)

図表 3-25 ブロックチェーン導入後の業務フロー (不動産登記)



⑤ ヒアリング先の評価

- ・不動産登記制度においては登記申請にかかる住所証明情報の提供や、登記事項証明書の取得など、依然として紙の文書が多く利用されており、大きな手間になっていると考えられる。ブロックチェーンであれば、マイナンバーカードの署名用電子証明書を用いた本人確認等との親和性が非常に高く、正確かつ迅速な不動産登記申請、登記事項の証明等を電子的に完結させやすくなる。
 - ・ブロックチェーンを導入すれば、登記情報提供サービス等を通して法務局のデータベースに都度アクセスせずとも、民間企業が自社内で参照できるようになる。これは利便性が高く、国民経済の発展に寄与するというメリットもあると考えられる。
 - ・不動産登記へのブロックチェーン技術の適用はスウェーデンを始め海外でも取組が始まっている。ブロックチェーンの思想が適合しやすい事例と言えるだろう。
- (以上、bitFlyer ヒアリングより)

⑥ 本ユースケースにおけるブロックチェーン活用の前提・留意事項等

- ・不動産登記情報は、ユーザ情報の管理システムとの連携の他、登記移転事由などを示す証跡文書との紐付けが求められる。
- ・ブロックチェーンは格納されたデータ（ハッシュ値）に対する真正性や対改ざん性は高めることができるものの、申請者の確認や登記情報移転事由の確認の過程における不正やミスはブロックチェーン以外のシステムで防がなければならない。

(7)ICO/STO

本項では、ERC20 トークン等による ICO 事例を参考に、資金調達手法としての ICO/STO にブロックチェーンを活用するユースケースを検討する。なお、ICO/STO については法整備途上であり、健全な資金調達手段とみなされない事例も多い。また、ICO/STO では発行したトークンについて、何らかのトークンエコノミーを示し、その有望性に対する資金を集めるが、本項で着目するのは ICO/STO 行為そのものにおけるユースケースである。

① ブロックチェーン活用の背景・課題認識

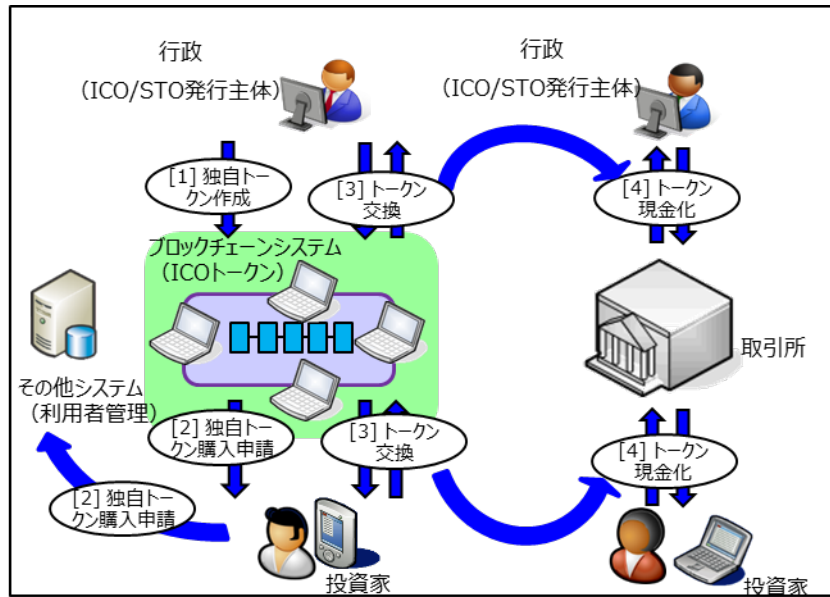
- ・ICO/STO は、自治体や企業が独自に発行するトークンと、既に価値が付いている Ethereum 等のトークンを交換することで資金調達を行う。このとき、独自トークンが ERC20 トークン⁴⁴であれば、Ethereum アドレスを用いたトークンの交換が可能である。
- ・トークンの交換後、交換用トークンは別途取引所等で他の暗号資産、又は法定通貨に交換される。独自トークンについては、ICO/STO で謳われたトークンの使用形態で用いられるか、又はそのトークンが上場後、他の暗号資産や法定通貨と交換される。

② ICO/STO とブロックチェーン利用イメージ

本ユースケースにおける主たる利用者とシステム利用イメージを図表 3-26 に示す。ICO/STO 発行主体の行政が独自トークンを作成し、そのトークンのブロックチェーンを構成する。購入を希望する投資家は、別途保有する交換用トークン（イーサリアムなど）を用意し、購入申請を行う。行政側は利用者毎の購入希望量を踏まえ、総発行量を決め、購入申請者毎に交換用トークンと独自トークンとの交換を行う。そして、行政は交換用トークンを取引所で現金化する。投資家は、その独自トークンが取引所に上場後、又は独自トークンをさらに別のトークンと交換後、取引所で現金化を行う。

⁴⁴ ERC20 トークンとは、イーサリアムのプラットフォームで使用されることを目的に、イーサリアムのコミュニティが定めるいくつかの基準（ERC20）を満たすように作られたトークンを指す。ERC20 を満たしていれば、独自のウォレットを用意せずともイーサリアムのウォレットで管理することができるため、ICO では ERC20 を満たすトークンが選択されることが多い。

図表 3-26 ICO/STO とブロックチェーン利用イメージ



③ システムに必要な機能

想定するシステム全体の主たる機能及びブロックチェーンが対応する機能を整理した。

(図表 3-27)

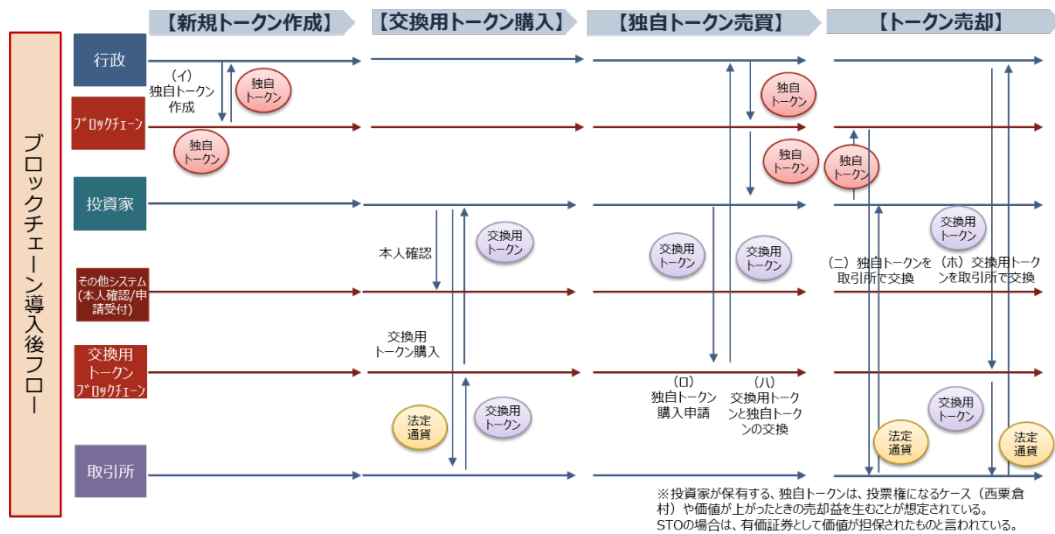
図表 3-27 ICO/STO に関連するシステム機能 (例)

ICO/STO に関連するシステム機能 (例)				
業務	搭載機能	利用者	機能内容	対応する ブロックチェーン機能
[1] 独自トークン作成	(イ)独自トークンの作成	行政	発行枚数、通貨名、取引単位、通貨記号等を定め新規に暗号資産を作成する。	所有権の移転情報の反映
[2] 独自トークン購入	(ロ)独自トークン購入申請	投資家	独自トークンの受け取り用アドレスと購入量とともに購入申請を行う。	
[3] トークン交換	(ハ)交換用トークンと独自トークンの交換	行政・投資家	独自トークン、交換用トークンそれぞれのブロックチェーン上で対応する価値のトークンを送付し合うトランザクションを作成する。	所有権の移転情報の反映
[4] トークン現金化	(ニ)独自トークンを取引所で交換	投資家	独自トークンを、それが上場している取引所で他の暗号資産又は法定通貨に交換する。	所有権の移転情報の反映
	(ホ)交換用トークンを取引所で交換	行政	交換用トークンを、それが上場している取引所で他の暗号資産又は法定通貨に交換する。	所有権の移転情報の反映

④ ブロックチェーン導入後の業務フロー

システム導入後の業務の流れについて、主たる利用者、実施場面、利用機能が明確になるよう整理した。(図表 3-28)

図表 3-28 ブロックチェーン導入後の業務フロー (ICO/STO)



⑤ ヒアリング先の評価

・ICO/STO の問題点

- これまでの ICO を見ると、ホワイトペーパーに信用がおけない（内容に不備がある、いつの間にか書き換えられている）ものが見られる。
- 有価証券における目論見書では購入者の権利や配当が記載されるが、それに相当する ICO のホワイトペーパーではこうしたことが全く書かれていない。発行体にとって ICO は返さなくていい借金であり、転売されて最後に持つ投資家には何の権利もない。自治体がそうした身勝手なことをしていいのか、慎重に考えるべき。
- ICO における行政当局の見解、勧告にも留意すべきである。

・地方 ICO について

- トークンの値上がりを期待させて資金を調達するようなやり方よりも、北海道寒川町の自治体株主制度など、純粹に町を応援する形の制度の方がよい。
- ICO 自体は違法ではないが、自治体がトークンを販売する際にはリスクの説明が必要であり、金融商品取引法で管理されるべきである。
- 地方債という仕組みがある中で、敢えて地方 ICO を行う必要があるか考えるべき。

（以上、京都大学岩下教授ヒアリングより）

⑥ 本ユースケースにおけるブロックチェーン活用の前提・留意事項等

- ・購入者の本人情報確認システムによる補完が必要である。
- ・独自トークン又は交換用トークンを現金化しようとする場合、別途取引所で法定通貨等に交換する必要がある。また独自トークンの現金化には、その独自トークンが取引所

に上場しているか、又は独自トークンを他の上場しているトークンに交換できることが前提条件となる。

(8)貿易情報連携

本項では、貿易情報連携にブロックチェーンを活用するユースケースについて検討する。なお、本ユースケースは民間企業を中心として取り組まれているものの、通関業務とも密接に関連することから、行政に近い領域として検討対象に含めたものである。

① ブロックチェーン活用の背景・課題認識

- ・ 貿易手続は、商社等の荷主を始めとして、銀行、保険、船会社及び物流会社等の多くのステークホルダが関与しており、複数の書類や情報のやり取りを行っている。
- ・ 貿易に関わる情報は、物理的な貨物の状況と対応付ける必要があり、更に様々な書類間で整合性を担保するなど、入力された情報の真正性を確保する必要がある。
- ・ 既存の情報交換は紙や FAX、PDF などによって行われており、非効率な作業に加え、確認ミスや伝達ミスが起りやすい状況となっている。
- ・ 貿易に関する事務や手続等のうち、既に電子的な情報共有が実現されているもの⁴⁵を除き、ブロックチェーンを用いて関係事業者間の情報共有を実現する。

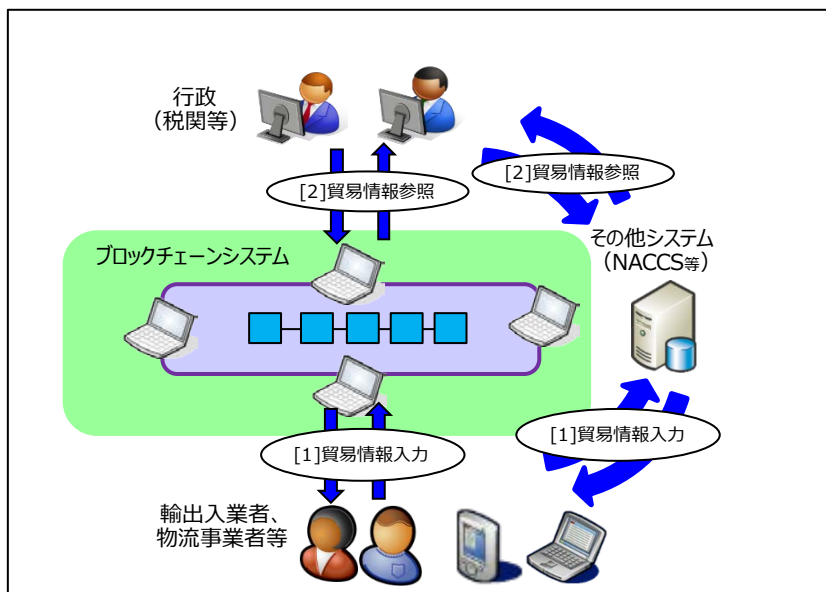
② 貿易情報連携とブロックチェーン利用イメージ

本ユースケースにおける主たる利用者とシステム利用イメージを図表 3-29 に示す。

本ユースケースでは、貿易手続に関する情報をシステムに入力し、それを多様な関係者と共有・連携する仕組みを検討する。

⁴⁵ NACCS（輸出入・港湾関連情報処理システム）における税関や関係行政機関に対する手続等

図表 3-29 貿易情報連携とブロックチェーン利用イメージ



③ システムに必要な機能

想定するシステム全体の主たる機能及びブロックチェーンが対応する機能を整理した。

(図表 3-30)

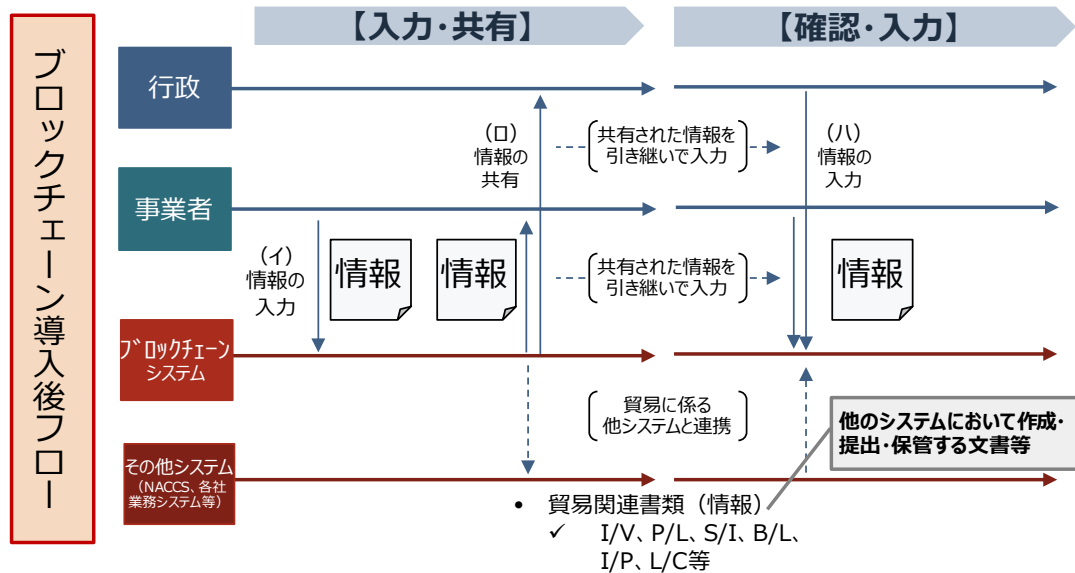
図表 3-30 貿易情報連携に関するシステム機能 (例)

貿易情報連携に関するシステム機能 (例)				
業務	搭載機能	利用者	機能内容	対応する ブロックチェーン機能
[1] 貿易情報入力	(イ) 情報の入力	輸出入事業者、物流事業者等	貿易に関する情報を入力する。	主体とその内容の真正性が証明された情報の登録・参照
	(ロ) 情報の共有 (提示)	行政、輸出入事業者、物流事業者等	入力した情報を関係者に共有 (提示) する。	履歴・過程情報の参照が可能
[2] 貿易情報参照	(ハ) 情報の入力 (次ステップ)	行政、輸出入事業者、物流事業者等	(ロにおいて) 確認した情報を使用し、次の手続を行うための情報を入力する。	所有権の移転情報の反映

④ ブロックチェーン導入後の業務フロー

システム導入後の業務の流れについて、主たる利用者、実施場面、利用機能が明確になるよう整理した。(図表 3-31)

図表 3-31 ブロックチェーン導入後の業務フロー (貿易情報連携)



⑤ ヒアリング先の評価

- ・ブロックチェーンは耐改ざん性及び追跡性が高く、技術的には情報の原本性及び真正性を担保することが可能である一方、法的にどう担保されるかの議論は必要。また、ブロックチェーン技術にはワンスオンリー（1度入力したデータを他の業務でも使う）の価値があり、かつ情報をやりとりした履歴が重要であるような業務領域が適している。
- ・ブロックチェーンは中央集権的なスキームができていて、あるいは容易に作れる領域では強い優位性を発揮しにくい。貿易のように特定の国家や企業が特権的な地位を得ることが許されないような領域でこそ真価を発揮する技術である。
(以上、NTT データヒアリングより)
- ・ビジネスネットワークが大きくなることで、ブロックチェーンの効果が大きくなる。
- ・参加するメンバーが多く、貿易物流など世界中から利用されるようなものは相性がよいと考える。
(以上、日本アイ・ビー・エムヒアリングより)

⑥ 本ユースケースにおけるブロックチェーン活用の前提・留意事項等

- ・また、各社の輸出入に関する情報は、事業上の営業秘密に該当する可能性もあり、閲覧

権限を管理することが望ましい。

- ・なお、貿易手続に係る書類は、原本性などの法的な観点から紙媒体の廃止が難しいものもある。仮にブロックチェーンによる情報共有等が可能となったとしても、別途紙媒体を共有する必要がある場合、二重管理となってしまう。
- ・一方、民間企業同士でやり取りする書類は特に決まったフォーマット等はないものが多く、ブロックチェーンで共有するためにはデータ項目の標準化等が必要となる。

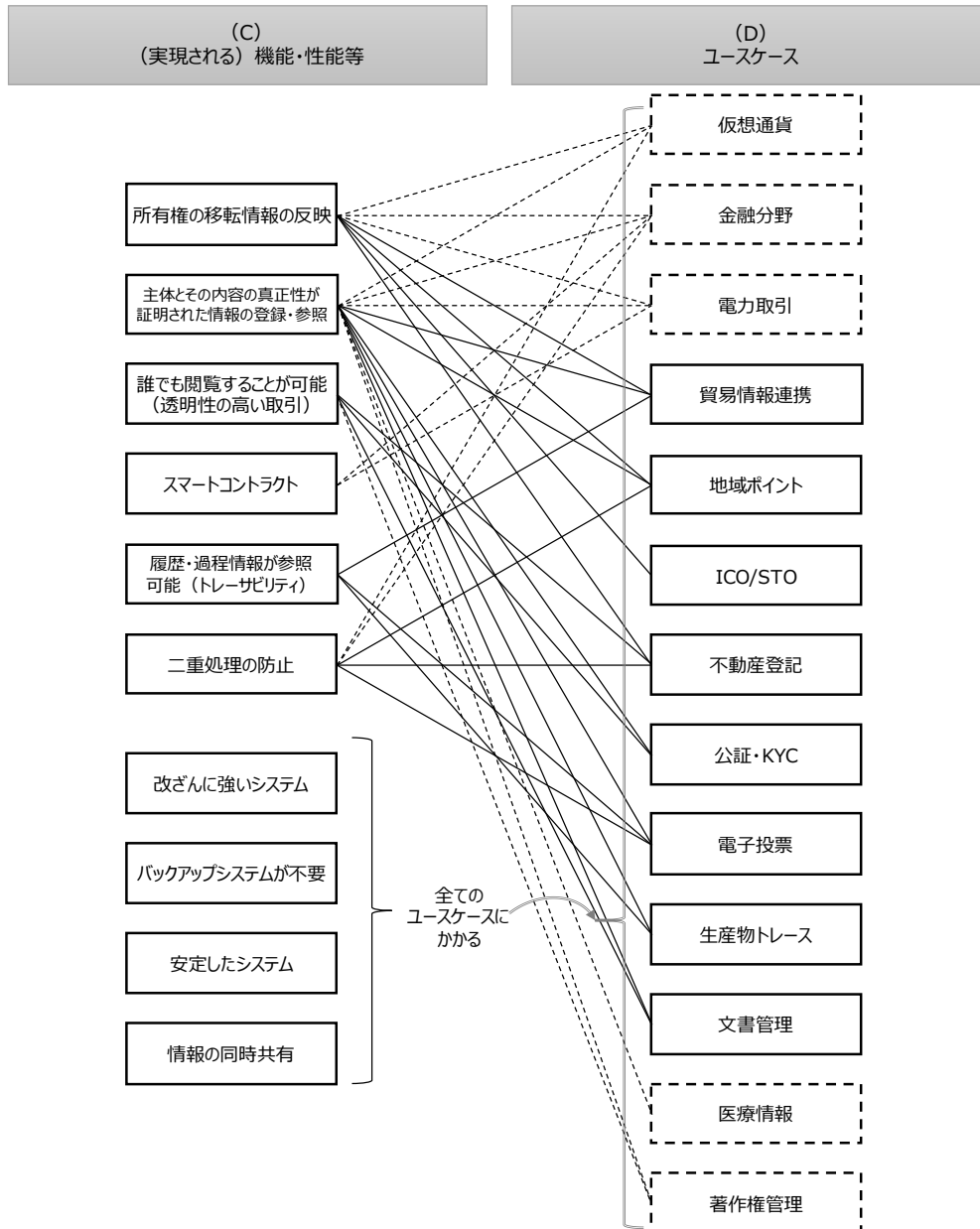
⑦ 備考・特記事項

貿易情報に関するブロックチェーン活用は、既に民間主導で事業化が進められている。しかしながら、関税などの手続や書類の原本性に係る議論など、行政の関与は必須であり、我が国においても国交省や NEDO において実証事業等が実施されている。

3.4 特性とユースケース機能との関係整理

前章で整理した「機能・性能等」が、本章のどのユースケースとして具現化し得るかについて図表 3-32 に示すとおり紐付けを行った。なお、図表 3-32 のユースケースのうち、実線のものには行政が主体、若しくは主要なステークホルダとして関わるユースケースであり、破線のものには行政以外のユースケースである。

図表 3-32 ブロックチェーンで実現される機能・性能とユースケースの対応



3.5 ブロックチェーン特性マップ全容

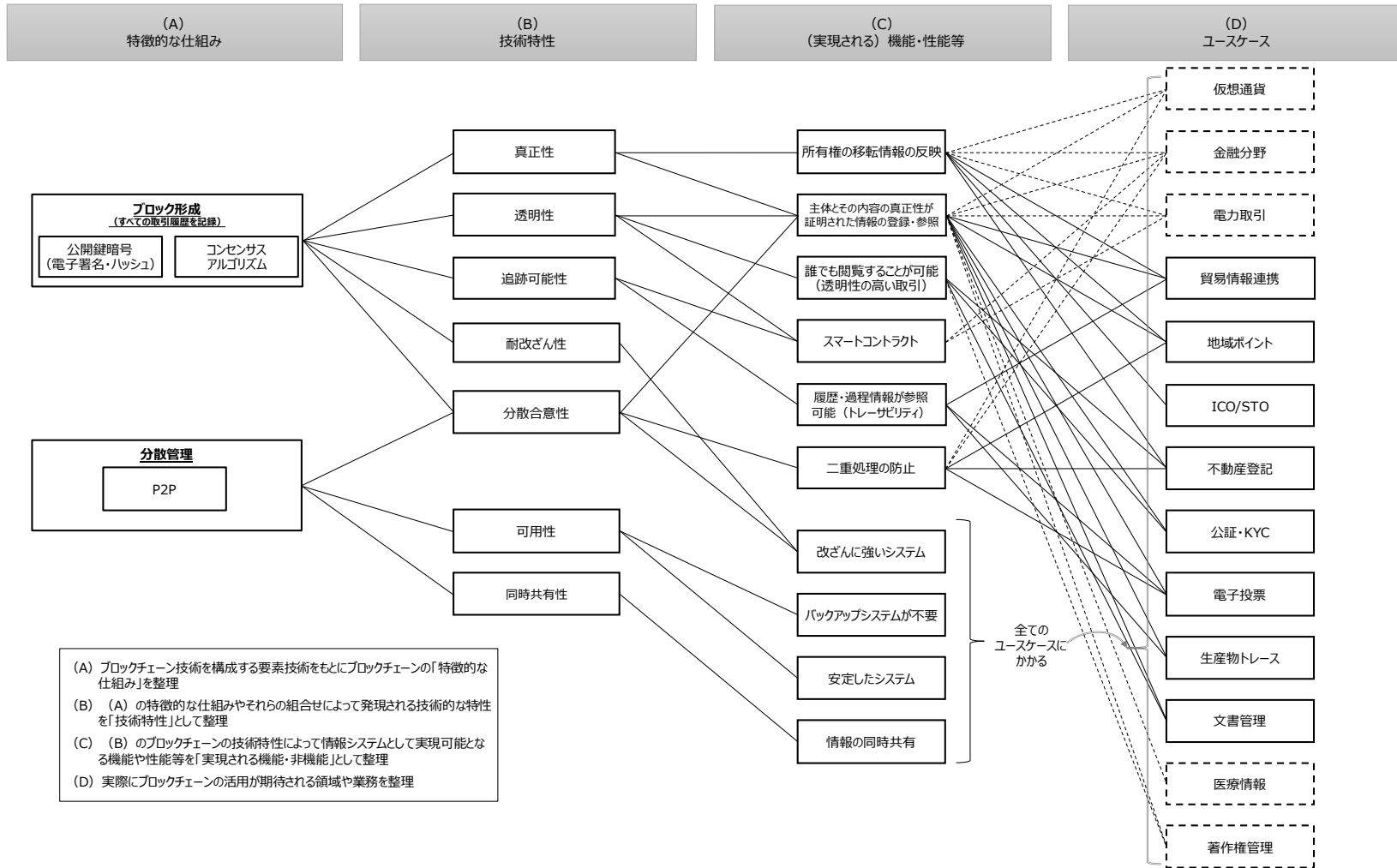
第2章のブロックチェーンの特徴的な仕組み、技術特性及び実現される機能・性能等と、本章で取り上げた各ユースケースの対応関係を図表 3-33 ブロックチェーンの特性に係る対応関係（マップ）に示す。

なお、同図表中の（A）から（D）の位置づけは以下のとおり。（2.1の再掲）

- （A）ブロックチェーン技術を構成する要素技術を基にブロックチェーンの「特徴的な仕組み」を整理した。具体的には、ブロック形成や分散管理が該当する。
- （B）（A）の特徴的な仕組みやそれらの組合せによって発現される技術的な特性を「技術特性」として整理した。具体的には真正性や透明性等を指す。
- （C）（B）のブロックチェーンの技術特性によって情報システムとして実現可能となる機能や性能等を「（実現される）機能・性能等」として整理した。
- （D）のユースケースは、実際にブロックチェーンの活用が期待されている業務に基づき設定した。

ブロックチェーン技術は新しく、また急速に進展中の情報技術ということもあり、定義や特徴についての記述も様々であるが、本調査研究では各文献において示されるそれらの用語や表記、概念等の体系的な整理を行った。その結果、以降の章で今後の公共分野におけるブロックチェーン技術適用領域の検討や分析を進めるための基盤となる知識を整理することができたと考える。

図表 3-33 ブロックチェーンの特性に係る対応関係 (マップ)



(A) ブロックチェーン技術を構成する要素技術をもとにブロックチェーンの「特徴的な仕組み」を整理
 (B) (A) の特徴的な仕組みやそれらの組合せによって発現される技術的な特性を「技術特性」として整理
 (C) (B) のブロックチェーンの技術特性によって情報システムとして実現可能となる機能や性能等を「実現される機能・非機能」として整理
 (D) 実際にブロックチェーンの活用が期待される領域や業務を整理

4. 行政におけるブロックチェーン導入時の前提・制約

本章では、行政におけるブロックチェーン導入時に考慮すべき前提・制約について検討する。第3章で整理した各ユースケースにおける前提、制約をブロックチェーンの技術特性毎に集約化し、行政におけるブロックチェーンの利用に際し共通して検討すべき前提及び制約を整理する。

まず、第3章で整理した各ユースケースにおける前提、制約を技術特性毎に整理した結果を以下（図表 4-1）に示す。

図表 4-1 ユースケース毎の前提・制約

特性	前提/制約	地域ポイント	電子投票	生産物トレース	公証・KYC	文書管理	不動産登記	ICO/STO	貿易情報連携
真正性	前提	ポイント購入者を判別するための情報を登録する場合は、それを登録する仕組み、その他システムが必要。	投票者がその本人かどうかを第三者により確認、証明し、それを登録する仕組み、その他システムが必要。	生産物がその生産者により作られたかどうかを第三者が確認、証明し、それを登録する仕組み、その他システムが必要。	申請情報が正しいものであることを第三者により確認し、それを登録する仕組み、その他システムが必要。	文書情報がその機関で正しく作られたものであることを第三者により確認し、それを登録する仕組み、その他システムが必要。	申請情報が正しいものであることを第三者により確認し、それを登録する仕組み、その他システムが必要。	交換用トークンとして入手したトークンを別途取引所で法定通貨等に交換する必要がある。	貨物に係る情報が正しく作られたものであることを第三者により確認し、それを登録する仕組み、その他システムが必要。
	制約	特になし。	ブロックチェーン内の本人識別情報とその他システムとの結びつけにミスがあると信頼を失う。	ブロックチェーン内の本人識別情報とその他システムとの結びつけにミスがあると信頼を失う。	ブロックチェーン内の本人識別情報とその他システムとの結びつけにミスがあると信頼を失う。有効期限のある証明情報については別途その機能作成が必要。	ブロックチェーン内の文書識別情報とその他システムとの結びつけにミスがあると信頼を失う。	ブロックチェーン内の取引者、不動産識別情報とその他システムとの結びつけにミスがあると信頼を失う。	特になし。	ブロックチェーン内の貨物に係る情報とその他システムとの結びつけにミスがあると信頼を失う。
透明性	前提	個人識別情報が外部からわからないようにする仕組み、その他システムが必要。	個人と投票内容とが外部からはわからないようにする仕組み、その他システムが必要。	ブロックチェーン記載内容を基に、生産物の生育、生産者の写真や詳細情報を取り出すための仕組み、その他システムが必要。	個人識別情報が外部からわからないようにする、また許可された範囲のみアクセスできる仕組み、その他システムが必要。	許可された範囲のみアクセスできる仕組み、その他システムが必要。	許可された範囲のみアクセスできる仕組み、その他システムが必要。	個人識別情報が外部からわからないようにする仕組み、その他システムが必要。	許可された範囲のみアクセスできる仕組み、その他システムが必要。
	制約	閲覧の際、ブロックチェーン内から所定データを検索するのに時間がかかる。	閲覧の際、ブロックチェーン内から所定データを検索するのに時間がかかる。	閲覧の際、ブロックチェーン内から所定データを検索するのに時間がかかる。	閲覧の際、ブロックチェーン内から所定データを検索するのに時間がかかる。	閲覧の際、ブロックチェーン内から所定データを検索するのに時間がかかる。	閲覧の際、ブロックチェーン内から所定データを検索するのに時間がかかる。	閲覧の際、ブロックチェーン内から所定データを検索するのに時間がかかる。	閲覧の際、ブロックチェーン内から所定データを検索するのに時間がかかる。
追跡可能性	前提	特になし。	上書きを許す場合、過去の記載内容や最新内容がわかるようにする仕組み、その他システムが必要。	特になし。	この特性よりその他システムや別途業務が必要となる前提は無い。	文書の更新を許す場合、過去の記載内容や最新内容がわかるようにする仕組み、その他システムが必要。	特になし。	特になし。	文書の更新を許す場合、過去の記載内容や最新内容がわかるようにする仕組み、その他システムが必要。
	制約	閲覧の際、ブロックチェーン内から所定データを検索するのに時間がかかる。	閲覧の際、ブロックチェーン内から所定データを検索するのに時間がかかる。	閲覧の際、ブロックチェーン内から所定データを検索するのに時間がかかる。	閲覧の際、ブロックチェーン内から所定データを検索するのに時間がかかる。	閲覧の際、ブロックチェーン内から所定データを検索するのに時間がかかる。	閲覧の際、ブロックチェーン内から所定データを検索するのに時間がかかる。	閲覧の際、ブロックチェーン内から所定データを検索するのに時間がかかる。	閲覧の際、ブロックチェーン内から所定データを検索するのに時間がかかる。
耐改ざん性	前提	特になし。	特になし。	特になし。	特になし。	特になし。	特になし。	特になし。	特になし。
	制約	単なる操作ミスによる誤った選択や記述を完全に消去することができない。	単なる操作ミスによる誤った選択や記述を完全に消去することができない。	単なる操作ミスによる誤った選択や記述を完全に消去することができない。	単なる操作ミスによる誤った選択や記述を完全に消去することができない。	単なる操作ミスによる誤った選択や記述を完全に消去することができない。	単なる操作ミスによる誤った選択や記述を完全に消去することができない。	単なる操作ミスによる誤った選択や記述を完全に消去することができない。	単なる操作ミスによる誤った選択や記述を完全に消去することができない。
分散合意性	前提	特になし。	特になし。	特になし。	特になし。	特になし。	特になし。	特になし。	特になし。
	制約	処理（トランザクション）確定までに時間を要する。	処理（トランザクション）確定までに時間を要する。	処理（トランザクション）確定までに時間を要する。	処理（トランザクション）確定までに時間を要する。	処理（トランザクション）確定までに時間を要する。	処理（トランザクション）確定までに時間を要する。	処理（トランザクション）確定までに時間を要する。	処理（トランザクション）確定までに時間を要する。
可用性	前提	特になし。	特になし。	特になし。	特になし。	特になし。	特になし。	特になし。	特になし。
	制約	急な業務停止が難しい。	急な業務停止が難しい。	急な業務停止が難しい。	急な業務停止が難しい。	急な業務停止が難しい。	急な業務停止が難しい。	急な業務停止が難しい。	急な業務停止が難しい。
同時共有性	前提	ブロックチェーン保有の範囲を定める必要がある。保有しないユースケース参加者は別途、その他システムで管理する必要がある。	ブロックチェーン保有の範囲を定める必要がある。保有しないユースケース参加者は別途、その他システムで管理する必要がある。	ブロックチェーン保有の範囲を定める必要がある。保有しないユースケース参加者は別途、その他システムで管理する必要がある。	ブロックチェーン保有の範囲を定める必要がある。保有しないユースケース参加者は別途、その他システムで管理する必要がある。	ブロックチェーン保有の範囲を定める必要がある。保有しないユースケース参加者は別途、その他システムで管理する必要がある。	ブロックチェーン保有の範囲を定める必要がある。保有しないユースケース参加者は別途、その他システムで管理する必要がある。	ブロックチェーン保有の範囲を定める必要がある。法的な観点から紙媒体の廃止が難しいものもあり、別途紙媒体を共有する必要がある。二重管理となってしまう。	ブロックチェーン保有の範囲を定める必要がある。法的な観点から紙媒体の廃止が難しいものもあり、別途紙媒体を共有する必要がある。二重管理となってしまう。
	制約	分散されたシステム環境に同じ情報が行渡るのに時間を要する。	分散されたシステム環境に同じ情報が行渡るのに時間を要する。	分散されたシステム環境に同じ情報が行渡るのに時間を要する。	分散されたシステム環境に同じ情報が行渡るのに時間を要する。	分散されたシステム環境に同じ情報が行渡るのに時間を要する。	分散されたシステム環境に同じ情報が行渡るのに時間を要する。	分散されたシステム環境に同じ情報が行渡るのに時間を要する。	分散されたシステム環境に同じ情報が行渡るのに時間を要する。

図表 4-1 の取りまとめ結果を踏まえ、各ユースケースに共通して出現する前提及び制約をブロックチェーンの技術特性毎に抽出・整理した。併せて、それらの前提が崩れたり、制約条件が満たせなかった場合の社会的影響度も評価した。社会的影響度の判断基準としては、事故やミスがあった際に国民への影響が大きいもの、また行政に対する信頼が損なわれる可能性があるものを、社会的影響度「大」とし、業務上の制約にはなるものの、国民に対して直接的に影響を与えるものでないものについては、社会的影響度を「小」とした。なお、業務上の制約とは、中央集権型のデータベースと比較してデータの検索に時間を要する、急な業務停止が困難（ブロックチェーン外での運用により回避できるものを含む）といった状態を指す。

図表 4-2 ブロックチェーン技術特性に対する前提及び制約

ブロックチェーン技術特性	前提/制約	前提及び制約	社会的影響度
真正性	前提	現実世界に関する情報について、真正性を担保した状態でデータ化し、ブロックチェーン内に取り込む必要がある。	大
	制約	識別情報と補完システムとの紐付けにミスがあると、データに対する信頼性を失う。	
透明性	前提	秘匿にする必要があるデータは、生データはブロックチェーン外に保存し、ハッシュ値のみをブロックチェーンに登録にするなど、プライバシー保護の観点での検討が必要。	大
	制約	閲覧の際、ブロックチェーン内から所定のデータを検索するのに時間がかかる。	
追跡可能性	前提	食品トレーサビリティの場合、食品自身に二次元コードなどを用いた個体管理が必要となるように、現実世界のハードとのリンクが必要。また、確認タイミングをどこに設定するか検討が必要。	小
	制約	閲覧の際、ブロックチェーン内からデータを検索するのに時間がかかる。	
耐改ざん性	前提	上書きの仕組みについて事前検討が必要。	大
	制約	単なる操作ミスによる誤った選択や記述を完全に消去することは困難であり、修正に係るコストも大きい。	
分散合意性	前提	コンソーシアムを形成するにあたり、参加者をどのように募るか検討が必要。ブロックチェーン自身の管理者が不要な場合でも、データの標準化やルールを決める統治者・団体が必要。	大
	制約	トランザクションが確定するまでに時間を要する。	

可用性	前提	(特になし)	小
	制約	急な業務停止が困難。	
情報同時共有	前提	ブロックチェーンの共有範囲について検討が必要。(保有しない参加者は、別途その他のシステムで管理する必要がある。)	小
	制約	分散されたシステム環境に同じ情報が行き渡るのに、一定の時間を要し、タイムラグが発生する。	

社会的影響については、前述の基準で分類したところ、特に、真正性、透明性、対改ざん性、分散合意性に係る前提・制約が、システムの企画や導入の際に十分留意する必要があると判断された。

5. 公共分野におけるブロックチェーン活用の可能性と導入時の留意事項

本章では、ブロックチェーンの活用が公共分野にどのようなインパクトをもたらし得るかを把握するため、いくつかの試算を行うとともに、近い将来、活用可能性がある用途を検討する。また、実際のブロックチェーン導入にあたって留意すべき事項を整理する。

5.1 インパクトの試算に関する考察

本節では、ブロックチェーンが今後様々な行政分野に適用された際のインパクトを推計する。

ブロックチェーンは社会的実装前夜であるものの、既に行政機関でも実用事例が多数出始めている AI 技術や RPA (Robotic Process Automation) と比べると、その実利用が広まるのはまだ先の段階である。また、ブロックチェーン単体でシステムを実現するものではなく、ほかの様々な技術によって補完されその効果を発揮する基盤としての技術であり、それぞれのシステムやサービスがもたらす効果への寄与は間接的である。

本節ではこれらの状況及び前提条件を踏まえた上で、ブロックチェーンの活用シーンとして、現時点で想定し得るユースケースであって効果の定量的試算に比較的向いているものを選定した。そのうえで、ブロックチェーン適用の実現によって期待される様々な効果や影響を一定の仮定の下、概括的に把握することを目的に試算を行う。

5.1.1 試算 1 生産物トレースによるブランド力向上

(1) 概要

有機農業の町として知られる宮崎県綾町における有機農産物について、ブロックチェーン技術を用いて品質を保証する実証実験に見られるように、ブロックチェーン技術は農作物のトレーサビリティ管理に用いることが有望視されている。

農作物のトレーサビリティ管理は、米⁴⁶や牛肉⁴⁷を中心に法整備が進んでおり、ブランド価値を維持するために不可欠な活動として位置付けられる。また地方再生の観点から見ても、地域ブランド化は有効策の一つとして注目される⁴⁸。

一方でトレーサビリティ管理は、管理コストが高く、必ずしも全ての品目で実施できていくわけではない。また、生産者、農協、スーパー等の販売店、地域の行政主体という様々な関係者が共通に利用できるシステムの構築が容易でなく、信頼性の確保のためには第三者

⁴⁶ 農林水産省、「お米の流通に関する制度」, <http://www.maff.go.jp/j/syouan/keikaku/beikoku/index.html>, 2019/3/22 確認

⁴⁷ 農林水産省、「牛・牛肉のトレーサビリティ」, <http://www.maff.go.jp/j/syouan/tikusui/trace/index.html>, 2019/3/22 確認

⁴⁸ 日本政策投資銀行「地方再生にはブランド化 ～トレーサビリティの活かし方～」
https://www.dbj.jp/reportshift/area/s_kyusyu_s/pdf_all/0402.pdf

による確認以外に有効な方法がないことが課題として言及されている。⁴⁹

(2) 推計方針

ここでは、ブロックチェーン技術による農作物のトレーサビリティ管理システムが実現した状況を想定する。現時点ではブランド価値を低く見られている農作物について、ブロックチェーン技術によるトレーサビリティ管理をきっかけとしそのブランド価値が高まり、その価格が向上することを仮定し、農業総生産額を押し上げる効果を推計する。

(3) 推計式

推計式：

$$\frac{\text{(ブロックチェーンによる生産物トレースによるブランド農作物の市場拡大効果)}}{\text{補正係数}} = \text{(日本農業総生産額)} \times \text{(潜在ブランド農作物割合)} \times \text{(ブランド化価格上昇率)} \times \text{補正係数}$$

(4) 推計に利用するデータ

推計に利用するデータを以下に示す。

図表 5-1 推計に利用するデータ（生産物トレースによるブランド力向上）

データ名	値	参考
H29 年度の日本の農業総生産額	9 兆 2,742 億円	H29 年度農林水産統計 ⁵⁰ より
潜在的なブランド農作物	3%	潜在的なブランド農作物（一般価格帯だがブランド化できる農作物）の存在割合仮定値とし対生産額比 3%とした。 ※参考：食肉としてブランド化している鹿児島黒豚は全国において 3~4%の市場シェア ⁴⁸
ブランド価値上昇率	+0.58 倍	米のブランド農作物（新潟コシヒカリ魚沼産）の価格と全銘柄平均価格の日を参考にした。 25,382(円 /60kg) ÷ 16,099(円 /60kg)=1.58 ※参考：2014 年 8 月から全国に先駆けトレーサビリティシステムを導入した松阪牛では、偽装がなく

⁴⁹ 農林中金総合研究所 「食品のトレーサビリティ導入状況と課題」 2006.1

<https://www.nochuri.co.jp/report/pdf/r0601in2.pdf>, 2019/3/22 確認

⁵⁰ 農林水産省大臣官房統計部 「平成 29 年 農業総産出額及び生産農業所得（全国）」, H30.12.25 公表

http://www.maff.go.jp/j/tokei/kouhyou/nougyou_sansyutu/attach/pdf/index-5.pdf, 2019/3/22 確認

		なり販売単価が従前の倍になったとされている ⁵¹ 。
補正係数	1/2	地域ブランドとしての「信頼性」と「独自性」が顧客ロイヤリティを生み価格プレミアムが付くという考え方 ⁵² に基づき、ブロックチェーンが特に寄与する信頼性について着目するため要素数を勘案し 1/2 を乗ずる。

(5) 推計結果

推計結果：

ブロックチェーンによる生産物トレースによるブランド農作物の市場拡大効果

= 約 807 億円 ※トレーサビリティ管理によりブランド力が確立した後に現れる年間農業総生産額に対する寄与

(6) 推計結果についての留意点

上記推計ではトレーサビリティ管理が農作物の信頼性に寄与し結果としてブランド力が向上すると仮定した。しかしながら農作物への信頼性はトレーサビリティ管理だけでなく、生産手法の内容などほかの複数の要素が関係する。この試算の前提では、ほかの要素は捨象している。

またトレーサビリティ管理によりブランド価値が向上するという効果は、短期間に実現することはなく、比較的長期間かけて確立される効果と考えられる。ただし、米では偽装米、牛肉では BSE といった社会的にその品質に懸念生じうる事態を防止し、そのブランド価値を損うリスクを防止するという点は、本推計で言及した直接的な経済効果以外に大きなメリットとして考えられる。

⁵¹ 日本政策投資銀行 「地方再生にはブランド化」 2004 年 2 月，

https://www.dbj.jp/reportshift/area/s_kyusyu_s/pdf_all/0402.pdf, p15, 2019/3/29 確認

⁵² 押久保 政彦氏 「地域ブランドの競争優位性の獲得メカニズム」, 2015 年 3 月

https://tus.repo.nii.ac.jp/?action=pages_view_main&active_action=repository_view_main_item_detail&item_id=171&item_no=1&page_id=13&block_id=21, 2019/3/29 確認

5.1.2 試算2 地域通貨によるキャッシュレス化の売上げ増効果

(1) 概要

地域通貨は、特定の地域やコミュニティ内に限定して使用できる通貨である。地域活性化を主目的に近年では電子化ひいてはキャッシュレス決済の実現手段として用いられている。事務手数料が高いなどの理由でクレジットカード決済の導入が普及していない地域でも、比較的安価にキャッシュレス決済を導入できる手段として商業化、実証実験が広く実施されている。電子化された地域通貨は、二次元コード決済等によってキャッシュレス化を実現する。専用端末が不要でスマートフォンやタブレット等で決済処理が可能となるため、導入の敷居が低いといえる。

キャッシュレス化が重要視されている背景には、クレジットカード決済が普及していない地域における訪日外国人のインバウンド消費の機会ロスがある⁵³。実際、キャッシュレス化により店舗の売上げの増加が期待されることが経済産業省から公開されている調査報告書⁵⁴でも言及されている。

(2) 推計方針

ここでは、特に観光消費に係るキャッシュレス化による売上増効果に着目する。ブロックチェーン技術を活用したキャッシュレス化が全国の観光先で実現したと仮定し、そのキャッシュレス化による売上げ増効果を推計する。また、その際、近年の主要な地域通貨のうちブロックチェーン技術を活用したものの種類数の割合を踏まえ、ブロックチェーン技術を活用したキャッシュレス化による観光消費額の増分を推計する。

(3) 推計式

推計式：

$$\begin{aligned} & \underline{\underline{(\text{ブロックチェーンを用いた地域通貨導入時のキャッシュレス化による売上げ増効果})}} \\ & \underline{\underline{= (\text{観光総消費額}) \times (\text{キャッシュレス化効果}) \times (\text{地域通貨のうちブロックチェーンを用いたもの割合})}} \end{aligned}$$

⁵³ 事業構想, 2017年7月号, 外国人旅行者の利便性を高める インバウンド消費喚起の決め手, <https://www.projectdesign.jp/201707/cashless-innovation/003750.php>

⁵⁴ 平成29年度産業経済研究委託事業, 我が国におけるFinTech普及に向けた環境整備に関する調査検討 経過報告, 「キャッシュレス化推進に向けた国内外の現状認識」, 2018/2/8, p14 でキャッシュレス決済の導入による店舗の売上増効果が言及されている。 https://www.meti.go.jp/committee/kenkyukai/shoryu/credit_carddata/pdf/009_03_00.pdf, 2019/2/1 確認

(4) 推計に利用するデータ

図表 5-2 推計に利用するデータ（地域通貨導入による売上げ増効果）

データ名	値	参考
観光消費額	26.7 兆円	H29 年年間値（日外国人の旅行消費額も含めた、日本における旅行消費額は 26.7 兆円） ⁵⁵
キャッシュレス化効果	+3.7%	キャッシュレス化による店舗の売上げ増効果（客数の増効果+2.1%×客単価の増効果+1.6%） $1.021 \times 1.016 = 1.037$ なお、「客数の増効果」、「客単価の増効果」については、現金・キャッシュレス決済に関するアンケート調査分析結果 ⁵⁶ を参考とした。
地域通貨のうちブロックチェーンを用いたものの割合	36.8%	近年の主要な地域通貨の発行事例のうちブロックチェーンを活用した種類の割合（19 通貨中 7 通貨=36.84%） ⁵⁷

(5) 推計結果

推計結果：

ブロックチェーンを用いた地域通貨導入時のキャッシュレス化による売上げ増効果＝約 3,635 億円

(6) 推計結果についての留意点

本推計においては、地域通貨によるキャッシュレス化における事務コストや、主にプレミアム分として用いられる地域振興にかかる補助金については考慮していない。なお、後者については現状の観光消費額の中に一定程度含まれている可能性はある。

また、地域活性化に係る交付金を活用した過去の地域振興の例ではプレミアムを数%から 20%付与し、例えば 5,000 円分の購入権利で、実質 6,000 円の買い物ができるような振興策が取られることがある。ブロックチェーンを用いた地域通貨では、専用端末不要となるコスト削減分を更にプレミアムに回すことができる。このため、地域消費活動が更に促進されると考えられる。

⁵⁵ 国土交通省観光庁旅行・観光消費動向調査 2018 年年間値（速報）2018/2/21

http://www.mlit.go.jp/kankocho/news02_000344.html, 2019/2/1 確認

⁵⁶ 平成 29 年度産業経済研究委託事業，我が国における FinTech 普及に向けた環境整備に関する調査検討 経過報告，「キャッシュレス化推進に向けた国内外の現状認識」，2018/2/8, p14

https://www.meti.go.jp/committee/kenkyukai/shoryu/credit_carddata/pdf/009_03_00.pdf, 2019/2/1 確認

⁵⁷ 大和総研 「地域通貨は地域金融システムに何をもたらすか」 2018/4/23,

https://www.dir.co.jp/report/research/policy-analysis/regionalecnmy/20180423_030004.pdf, 2019/2/21 確認

5.1.3 試算3 ブロックチェーン適用による行政文書管理

(1) 概要

大分県竹田市⁵⁸やイギリス国立公文書館のプロジェクト「ARCHANGEL^{59,60}」の取組に見られるように、ブロックチェーンによる文書管理は改ざんを防止しつつ行政文書を管理する仕組みとして注目されている。このような文書管理では、文書の電子ファイルのハッシュ値をブロックチェーンに格納しておくことで、文書の変更履歴が改ざん不能な形態で管理する。仮に改ざんが行われた場合、そのハッシュ値の相違から改ざんが検知できる仕組みである。

今般、平成30年7月に閣議決定された「公文書管理の適性の確保のための取扱いについて」を受けて、行政文書の電子管理の方針⁶¹が議論されているが、今後作成される行政文書には電子媒体を整体・原本として管理することが原則とされている。現在の公文書管理法によると、行政文書区分によっては30年の最低保存期間が設定されている⁶²。このような長期間に渡り、改ざんを防止しながら文書を管理する必要がある。ブロックチェーン技術はこれを実現する有力な手段の一つとなる可能性がある。

(2) 推計方針

現在行政で保有している、また、今後10年間新規に発行される文書に着目し、10年後も保存することが求められる文書について、ブロックチェーンでその変更履歴の管理を行うことを想定し、どの程度の文書がその対象となりうるかを推計する。

(3) 推計式

推計式：

(ブロックチェーンによる長期保存の対象となる文書数)

$$= \{ (\text{現行の長期保存対象文書数}) + (\text{年間新規に発行される文書}) \times 10 \text{ 年} \times (\text{うち 10 年以上の長期保存対象となるものの割合}) \} \times (\text{秘密文書以外の文書の割合})$$

⁵⁸ 大分県竹田市企画情報課、「公共におけるブロックチェーン」, 2019/3/7,

<https://www.kiai.gr.jp/jigyuu/h30/PDF/0307p3.pdf>, 2019/3/22 確認

⁵⁹ open data institute, “Blockchain’s potential role in the future of archiving”, <https://theodi.org/article/blockchains-potential-role-in-the-future-of-archiving/>, 2019/3/22 確認

⁶⁰ イギリス国立公文書館 “Trustworthy technology: the future of digital archives”, 2018/6/5,

<https://blog.nationalarchives.gov.uk/blog/trustworthy-technology-future-digital-archives/#>, 2018/3/22 確認

⁶¹ 内閣府大臣官房公文書管理課, 「行政文書の電子的管理についての基本的な方針 (骨案)」 2019/1/31,

<https://www8.cao.go.jp/koubuniinkai/iinkaisai/2018/20190130/shiryuu2-2.pdf>, 2019/3/22 確認

⁶² 総務省, 行政文書の最低保存期間基準, http://www.soumu.go.jp/main_sosiki/gyoukan/kanri/gaido_1.html, 2019/3/22 確認

(4) 推計に利用するデータ

図表 5-3 推計に利用するデータ（ブロックチェーン適用による行政文書管理）

データ名	値	参考
現行の長期保存対象文書数	1,467 万ファイル	内閣府大臣官房公文書管理課の報告によれば、最も過去の数値として 2011.4.1～2012.3.31 に約 1,467 万ファイル ⁶³ であることが分かる。現在までこのファイル数から単純増加しているため、これに相当する文書数が現時点で 10 年以上保存すべき文書数であると推計する。
年間新規に作成される行政文書	273 万ファイル	内閣府大臣官房公文書管理課によれば、2017.4.1～2018.3.31 における新規公文書数は 273 万ファイルである。
10 年以上の長期保存対象となるものの割合	約 3.9%	東京都における文書保存期間の調査結果より新規に作成する文書の約 3.9%が 10 年以上の保存期間の対象となる。日本政府における行政文書でも同等の割合と仮定する。
秘密文書以外の文書の割合	約 98%	内閣府大臣官房公文書管理課によれば、新規作成・取得されたファイルのうち、秘密文書を含む行政文書の割合は、2.0% ⁶⁴ 。

(5) 推計結果

推計結果：ブロックチェーンによる長期保存の対象となる文書数＝約 1,542 万ファイル

※ブロックチェーン技術の導入が長期保存文書の電子化の契機になると想定する。公文書管理のガイドラインによれば、公文書 1 ファイルは 100±50 枚程度の用紙に相当する⁶⁵。これはダンボール約 18 万箱～55 万箱に相当することから⁶⁶、約 6,119 坪～18,357 坪相当のスペースの節約に寄与する⁶⁷と考えられる。

⁶³ 内閣府大臣官房公文書管理課、「平成 29 年度における公文書等の管理等の状況について」H31 年 2 月, p.7, 表 2 を参考 https://www8.cao.go.jp/chosei/koubun/houkoku/heisei29nendo_houkoku.pdf, 2019/3/22 確認

⁶⁴ 内閣府大臣官房公文書管理課、「平成 29 年度における公文書等の管理等の状況について」H31 年 2 月, p.22, 表 13 を参考 https://www8.cao.go.jp/chosei/koubun/houkoku/heisei29nendo_houkoku.pdf, 2019/3/22 確認

⁶⁵ 内閣府大臣官房公文書管理課、行政文書の管理に関する手引き, <https://www8.cao.go.jp/koubuniinkai/iinkaisai/2011/20110908/20110908haifu1-1-1-1.pdf>, 2019/3/29 確認

⁶⁶ 全て A4 用紙と仮定すれば、A4 用紙 7 億 7100 万枚～23 億 1300 万枚となる。一般的なダンボール（高さ 268mm 幅 430mm 奥行き 325mm, 参考：KING JIM, 保存ボックス 4370, <https://www.kingjim.co.jp/products/detail/4370.html>）には A4 用紙 700 枚収容のバインダーが 6 個格納できる。

⁶⁷ 文書管理サービスで謳われる 1 坪 30 箱の必要スペース（事務所内管理の場合）を勘案した。

(6) 推計結果についての留意点

本推計では参考値として、ブロックチェーンによる変更履歴の管理の対象となりうる長期保存文書の数について着目した。推計において、特定秘密が含まれる等の理由で秘密文書とされる行政文書はブロックチェーンでの管理対象外とした。ただし、ハッシュ値のみをブロックチェーンに載せ文書の改ざんを監視するのであれば、ブロックチェーンにアクセスするユーザには文書内容を伏せた形でその改ざんが無いことを示す形の運用も可能である。

また、今回は公文書管理法の対象となっている行政機関等のみを対象としたが、公文書管理法の対象外となっている地方自治体についても近年厳しい文書管理ルールを敷く動きが見られる⁶⁸。このような動きがより進展すればブロックチェーンによる文書管理の対象文書数は更に拡大する可能性がある。

なお、現行の行政文書のうち既に電子化が行われているものは、6.7%にすぎない⁶⁹。ブロックチェーンによる行政文書管理は、文書の電子化が前提となる。先に述べたように、このたび議論されている行政文書の管理方針では、今後行政文書が電子媒体であることが原則とされるが、既存の紙文書で長期保存対象となる文書については改めて電子化を行うことが必要となる。

⁶⁸ 日本経済新聞, 「公文書管理、地方が独自色 21 道都県が条例制定・検討」, 2018/20/8, <https://www.nikkei.com/article/DGXMZO36188500V01C18A0ML0000/>, 2019/3/22 確認

⁶⁹ 内閣府大臣官房公文書管理課, 「平成 23 年度における公文書等の管理 等の状況について」 H31 年 2 月, p.7 https://www8.cao.go.jp/chosei/koubun/houkoku/heisei29nendo_houkoku.pdf, 2019/3/22 確認

5.1.4 試算結果についてのまとめ

5.1.冒頭で述べたように、ブロックチェーン技術は社会実装前夜の段階にあり、実際に応用事例が増えていくのはこれからである。他方で、いくつかの仮定を置く必要はあるものの、基盤技術としてのブロックチェーン技術は、単なる技術の置替えとしてのコストメリットだけでなく、上記で試算したように、多様な効果が、一定規模の社会的インパクトを伴って発現する潜在的な可能性を有する技術であると捉えることができる。

5.2 行政におけるブロックチェーン技術の今後の適用領域

近年公表された報告書やブロックチェーンに関連するセミナーの内容から、今後行政分野で期待されているブロックチェーン技術の適用例を抽出、整理した。(図表 5-4～図表 5-6)

図表 5-4 行政分野への今後のブロックチェーン技術適用例：総務省情報通信審議会 情報通信政策部会「ブロックチェーン活用検討サブワーキンググループ取りまとめ」より

行政分野適用例	内容
法人設立手続	登記の申請のほか、国税庁への設立の届出、各種社会保険の手続にブロックチェーンを活用し、登記事項証明書を関係行政機関で共有する。
政府調達手続	国と自治体の電子調達手続にブロックチェーンを活用し、入札参加資格申請の簡素化・共通化による官民の事務処理の効率化を図るとともに、国・自治体を通じた調達実績を共有することによって、国・自治体での調達コストの削減を実現する。
母子保健・学校検診・企業検診をカバーする PHR ⁷⁰ の管理	安定的かつセキュアな環境の下で、多数当事者間でのデータ共有等が必要となる住民向けサービスをブロックチェーン上でリーズナブルに提供する。

図表 5-5 行政分野への今後のブロックチェーン技術適用例：経済産業省 平成 27 年度 我が国経済社会の情報化・サービス化に係る基盤整備（ブロックチェーン技術を利用したサービスに関する国内外動向調査）報告書より

行政分野適用例	内容
電子図書館	電子書籍の閲覧権をブロックチェーンで管理することで、電子図書館が実現可能になる。
遺言	遺言をあらかじめスマートコントラクトとして定めておくことにより、当人が死亡したことをきっかけとして、遺言が自動的に執行されるようにすることが可能になる。
徴税と公的サービスの最適化	IoT 活用の世界にスマートコントラクトによるマイクロペイメントを組み合わせることで、受益者負担をより正確に反映したコスト負担の仕組みが構築可能となり、自治体行政の見える化を図ることが可能となる。

⁷⁰ Personal Health Record(パーソナル・ヘルス・レコード)

図表 5-6 行政分野への今後のブロックチェーン技術適用例：一般財団法人機械システム振興協会 ブロックチェーン技術の応用に関する戦略策定報告書より

行政分野適用例	内容
ICO スキーム等による国際的な公的ファンド創生	仮想通貨を用いた公的なファンド、地域通貨等を創生し、ICO の仕組みを応用して世界中から投資を呼び込む。
行政業務間連携の促進	省庁間、本省-外郭団体間、国-地方間など、異なる組織間での情報共有・連携に活用する。
防災等における公的センサーネットワークへの決済の導入	公的機関が保有する IoT、例えば防災用のセンサーネットワークなどを拡充し、一般市民のデバイスとも連携させ、情報の提供や展開等に貢献することに対して仮想通貨で自動的に支払いを行うなど、仮想通貨を媒介とした情報ネットワークを構築する。
仮想通貨による公的資金給付	年金や生活保護等の給付や拠出金の支払い等を仮想通貨で行う。
納税用途の見える化	納めている税金（所得税、消費税等）と受けているサービス（福祉、教育、整備等）の関係性を見える化する。

また、本調査研究のプロジェクト内でも、ブロックチェーン技術の適用領域についてデザイン思考に基づくワークショップを行ったところ、下記に示すような適用例が導出された。（図表 5-7）

図表 5-7 行政分野への今後のブロックチェーン技術適用例：当調査研究ワークショップより

行政分野適用例	内容
乗用車用センサー（IoT）と連携した走行記録共有	トラックやバスなどに取り付けたセンサーやカメラの走行情報や操作情報等を事業者 ⁷¹ 間でブロックチェーン技術を適用して共有し、それを安全に関する情報として公開する（業界の信頼向上や違反への牽制が期待できる）。
ペットの識別、飼主情報登録	動物の誕生時にブロックチェーン技術を適用して、血統書等の真正性を表す動物の生体情報（DNA や虹彩）を登録する。販売時に飼主がそれを確認した上で、所有者情報（マイナンバー等）を紐付け、共有できる仕組みを作る。また、この情報を自治体間（保健所間）でも共有できるようにし、動物が保健所等に届けられた場合でも迅速に照会できるようにする。

⁷¹ 事業協同組合や運送会社等

上記の 4 表で挙げられた例から、行政分野でブロックチェーン技術の適用が期待されているのは「自治体や行政区間でデータを共有したい」、「データに高い真正性や透明性が必要」、「センサー等 IoT 機器のデータ、スマートフォン等のデバイスと連携したい」といった要件が顕著な分野、領域であると見られる。限られた者のみにサービスを提供する分野ではなく、これまでは実現が容易ではなかったネットワーク同士の連携を通して自治体間、地域住民間といった広範囲で多数の利用者にサービスの提供が求められる分野、領域に適していると考ええる。

5.3 ブロックチェーン技術の利用に際しての留意点

ブロックチェーン技術の適用が期待される分野、領域はデータの真正性の担保などブロックチェーンの技術特性の発現や他システム、ネットワークとの連携が強く求められる領域である。

今後、行政が、ブロックチェーン技術の利用を検討する際に留意すべき事項をヒアリング結果から抽出し、図表 5-8 のとおり整理した。

図表 5-8 ブロックチェーン技術の利用に際しての留意点

検討場面	留意事項
サービスの企画	<ul style="list-style-type: none"> ・業務、サービスで期待する要件を、ブロックチェーンの技術特性によってどの程度要件を満たせるのかを検討することが必要である。不足する要件がある場合、他のどのような技術やサービスによって補完するかを検討することが必要となる。また、ブロックチェーンのプラットフォームは年々機能やサービスが拡充されているので、その動向と今後の見通しを的確に把握しながら、プラットフォームの選定やスクラッチでの機能開発を検討していくことが必要となる。
システム開発・運用	<ul style="list-style-type: none"> ・現在、ブロックチェーンを用いたシステム開発が行えるエンジニアは、需要に供給が追いついておらず、社会全体として不足している。開発規模や地域によっては十分な人材を確保できない可能性があるため、事業を開始するにあたっては事前に今後の見通しを確認しておくことが必要である。 ・いったん特定のブロックチェーンのプラットフォームを選定すると、その後、乗り換えることは容易ではない。主要プラットフォーム間では、主な機能やサービスに大きな差異は見られないが、実装レベルでは、それぞれに特有の制約条件が存在する。他の事例やコミュニティ形成の状況および今後の開発の方向性等を踏まえて、慎重に選定する（調達する際には要件定義を行う）ことが必要となる。 ・ブロックチェーンは技術進歩が非常に早い領域であり、今後、新たなサ

	<p>サービスが徐々に開発された結果、当初は想定していなかったようなサービスとの相互連携が求められるようになる可能性も十分に考えられる。システム的设计に際しては、他のシステムやサービスと容易に連携できるように、汎用的な標準インターフェースを通じた相互運用性の確保を前提とした仕様としておくことが必要となる。</p> <ul style="list-style-type: none"> ・ブロックチェーンを導入すると開発コストや運用コストを低減できるかのような報道が多いが、実際に、コストが下がるかどうかは、サービスの特性（特にトランザクションの頻度や参加者数など）や開発・運用にあたる技術者の熟練度や組織としての知識やノウハウの蓄積、開発するサービスとプラットフォームとの親和性、関連機能の開発規模など様々な要因によって決まってくる。コスト削減への過剰な期待は禁物である。
<p>許可型（コンソーシアム／プライベート型）の場合のコミュニティ形成</p>	<ul style="list-style-type: none"> ・システムの構築と同じかそれ以上に、事業全体としてのスキーム的设计が重要となる。コミュニティのルール设计のあり方（例：ノードへの参加や退出）、統治者（団体）の役割や権限など、様々な論点を整理しながら全体の事業スキームを设计し、参加者間での合意形成を図っていく必要がある。

6. 今後の展望

行政におけるブロックチェーンの活用に向けた取組はまだ始まったばかりであり、特に国の行政機関については参考にできる事例自体が極めて限られ、本調査研究では十分かつ客観的な根拠に基づく分析によって、実務に役立つ具体的な知見や示唆を得ることまでできていない。本調査研究はあくまで今後のブロックチェーンの利活用に向けた研究の端緒として、利活用の可能性を模索したにとどまっている。

本章ではこうした限界を踏まえた上で、今回の調査研究を通じて抱かざるを得なかった所感を参考までに述べ、本報告書を締め括ることとしたい。

6.1 公共分野におけるブロックチェーン活用の意義①：社会課題解決の仕組みの拡大

公共分野におけるブロックチェーンの本質的価値は、社会課題の解決に向けた官民の取組の中で必要とされる記録の真正性を、行政機関の関与が生み出す信用によってではなく、“仕組み”によって保証できるということである。したがって、ブロックチェーン導入の帰結は、行政機関は必ずしも社会課題の解決において自ら情報システムの構築主体や住民サービスの提供主体となる必然性はなくなる可能性が出てきたということである。こうした状態に移行したとき、行政機関が最低限果たすべき役割は、究極的には個々の記録の真正性を保証することではなく、ブロックチェーンの運用を成り立たせるコンセンサスアルゴリズムが適切に運用されていることを保証することへと移行すると思われる。このとき行政が行わなければならないのは、ブロックチェーンにコンソーシアム参加者として参画することによる“お墨付き”の付与となる。

※なお、プライベートチェーンの場合は、こうしたお墨付きの意味はなくなるのでブロックチェーン導入にメリットがあるかどうかはコスト比較を中心に論じられようになる。しかし、ブロックチェーンの技術が用いられる部分は情報システム全体の中の一部に過ぎないし、情報システムのコストはソフトウェアやハードウェアよりも人件費などの技術以外の要素に左右されるところが大きいので、一般論としてコストが削減できるということとはできない。単なる実装方式の選択肢の一つでしかなくなるということである。

ここで論点となるのは、そうしたブロックチェーンのコンソーシアムが民間主導で成り立ちうるかということである。民間企業側にブロックチェーンのシステムを必要とする強い動機があれば、民間主導でのネットワークは成り立ちうるであろう。モデルケースになるような成功例はまだ現れていないが、貿易情報連携やトレーサビリティなど、多数の関係者間で、多数の価値交換が連鎖的に起こるような領域では、民間主導での注目すべきブロックチ

チェーンのコミュニティが生まれつつある。今後、公共領域で新たなコミュニティを構築する場合は、行政機関がオーナーとなることに拘らず、始めから民間のブロックチェーンを前提とすることを選択肢として検討すべきである。

6.2 公共分野におけるブロックチェーン活用の意義②：コミュニティの誘発

ブロックチェーンのいまひとつの公共的意義はコミュニティにおける価値交換の可視化・具現化である。感謝、評価、敬意など無形の対価への期待が活動の原動力となっているコミュニティにおいて、これらの対価への価値をトークンという形で計測可能な形に具現化し、交換できるようになるということである。ブロックチェーンがこれらの価値の存在を保証する“仕組み”がうまく機能するようになれば、既存のコミュニティの強化・拡張・活性化に繋がる可能性があるほか、コミュニティ創出の敷居を下げ、新たなコミュニティの発生を誘発することも期待できる。また、感謝や評価などの価値を目に見える形で交換し、流通できるようになることで、コミュニティ内の関係性は、対面の範囲を超えて、より広い範囲で、より複雑で緻密なものへと発展していく可能性がある。さらに、そこに経済的なインセンティブが付与されれば、大きなムーブメントとなる可能性も出てくる。

6.3 公共分野におけるブロックチェーン活用の限界

ブロックチェーン構築の敷居は大きく下がってきている。プラットフォームの機能やコミュニティは日進月歩で充実しつつあり、予め一定の部品を備えた PaaS 型サービスも登場している。しかし、行政が担っている全ての保証機能がブロックチェーンに代替されることは想定しにくい。そこには以下のような本質的な限界があるからである。

限界 1：ブロックチェーン外での不正は防げない

実体（例：有機野菜）とブロックチェーンのアセット（例：生産履歴）との対応関係が真正であることはブロックチェーンによっては保証できない。ブロックチェーンの外で行われた不正はブロックチェーンによって防ぐことはできず、両者が正しく結びついていないことはほかの手段で担保しなければならない。ここで論点となるのは、行政機関以外の主体が、真正性の保証を代替できるかどうかである。完璧を期そうとすれば、行政が、適正な主体が適正な方法で真正の関係性が存在することを保証せざるを得なくなる。行政によるお墨付きが必要となるのであれば、部分的にブロックチェーンに移管しても意味をなさないであろう。すなわち、両者の関係性の真正性の確認を行政以外に委ねられるかどうか、ブロックチェーンへの移管が成り立つかどうかの分水嶺になるということである。これは分野や案件によって判断が分かれてくるであろう。

他方で、保証すべき対象が完全にデジタルネイティブなデータであれば、ブロックチェーンによって対象となるデータの真正性を完全に保証することが可能である。例えば、行政文書の原本がデジタルデータとなれば、ブロックチェーンによってその真正性

を担保することが可能となる。この点、政府が目指すデジタルファーストの戦略と公文書管理の電子化が実現すれば、ブロックチェーンが役立つ可能性は大きく広がることとなる。

限界 2：あくまで台帳システムでしかない

デジタルファーストが実現したとしても、全てのサービスがブロックチェーンに置き換わることは考えにくい。ブロックチェーンが実現できるのはあくまで記録に対する保証である。許認可などの行政判断は引き続き行政職員が実施する必要がある。これらの行政判断を実施した後の記録及びもともと行政判断を要しない届出等の台帳記録のみがブロックチェーンへの移行対象となり得る。

なお、スマートコントラクトの機能で自動承認を行うことも考えられるが、判断を伴わないのであれば、制度自体、承認を不要とするよう変更すべきであろう。

行政情報システムのうち台帳としてのデータベースないしアーカイブの真正性を保証する機能が、当面ブロックチェーンで代替し得る範囲の限界であろう。

限界 3：自律自走は期待できない。

Bitcoin におけるマイニングのような仕掛けを持たないコンソーシアム型ブロックチェーンにおいては、ブロックチェーン自体の自律自走は期待できない。ネットワークを構築し、拡大する推進者は必ず必要となる。これは官民間問わずどのような主体であってもよいが、公共サービスの維持向上に利害関係を持つ最大の主体は行政機関であることから、今後もその役割は行政機関が中心となって担うことになると考えられる。ただし、分野によっては、公益団体や業界団体、専門職団体なども推進主体となり得る。

6.4 公共分野におけるブロックチェーン活用の未来

以上のようにブロックチェーンには、一定の制約や限界はあるものの、公共の幅広い領域に大きな変動をもたらす可能性がある。そこで、こうしたブロックチェーンの可能性が最大限に発現した場合に、どのような可能性が出てくるのかを展望してみる。今後の公共分野でのブロックチェーンの活用の方向性としては、以下のような可能性が考えられる。

① ブロックチェーン・バイ・デフォルト

記録の保証という機能については、官民間問わずブロックチェーンによって保証するのが当たり前の社会に移行することが考えられる。現在、情報や価値の交換・流通がインターネットで行われるのが当たり前になっているように、それらの交換の結果としての記録の保証が、政府や金融機関などの権威によってではなく、ブロックチェーンによって行われるのが当たり前の社会が来るということである。

②ブロックチェーン・エコシステムへの移行

現在、様々な領域で無数のブロックチェーンが生まれつつあるが、今後は、それらのブロックチェーン同士が接続され、大きなブロックチェーンのネットワークが構成されていくことが考えられる。ブロックチェーン間での価値交換は、台帳の記録という行為を介して間接的に行われるほかなく、そのプロトコルやルールが精緻化・洗練され、共通化・標準化されていく必要があるが、現在、こうしたブロックチェーン間での価値交換の方法については、様々な研究開発が行われているので、いずれ実用的な仕組みが整備・実用化されてゆくと見込まれる。その結果、個々のブロックチェーンを包含した、新たな大きな価値交換のネットワークが出現する可能性がある。

③トークン・ソサエティへの移行

今後、我が国を待ち受ける超高齢化社会においては、場としての互助や共助の仕組み化と、それを動かすエンジンとしての感謝と奉仕の価値の循環が重要なカギとなってくる。ブロックチェーンがそれらの場と価値交換を具現化する方向で発達していくことで、社会福祉は金銭での交渉での対価ではなく、自発的なトークンの価値の交換によって担われる方向へと移行していく。行政機関には、こうしたブロックチェーンを基盤としたコミュニティの創発や参画の推進役として、また、ブロックチェーンにお墨付きを与えるコンソーシアム参加者としての積極的な役割を果たすことが期待されるようになる。行政主導で高コストなシステムを構築・運用することは、もはや行政の役割ではなくなる。

④ブロックチェーンによるデータ流通

今後、データ流通が経済社会の中で大きなウェイトを占めていくにつれ、データの真正性の保証が重要な課題になってくると考えられる。オープンデータその他の行政提供データもその例外ではない。ブロックチェーンは低コストでデータの改ざん防止を可能にするとともに、データの直接取引をも可能とする可能性がある。スマートコントラクトの機能を活用することで、提供条件を細かく設定し、自動的に契約を取り交わすことも技術的に可能である。さらに、セキュリティの懸念が指摘されている IoT から取得されるデータについても、ブロックチェーンに記録することによって改ざんを防止する仕組みを構築することも可能となる。既にブロックチェーンを活用したデータ流通の仕組みを構築したサービスも実用化されている。このように、今後はブロックチェーンがデータ流通社会の基盤として機能するようになっていく可能性がある。

初版：2019年3月31日

一般社団法人 行政情報システム研究所

本冊子の利用ルールは「政府標準利用規約（第2.0版）」に準じるものとします。

<https://www.kantei.go.jp/jp/singi/it2/cio/dai66/gjjsidai.html>