資料 53－1－7

情報通信審議会　情報通信政策部会
IoT 政策委員会　基本戦略ワーキンググループ

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

目次

１　検討の経緯 1
２　ブロックチェーン技術の基本的な特徴 1
（１）「事実上落ちない（正しく動作）」 2
（２）「事実上改ざん不可能」 3
（３）オープン性 3
（４）スマートコントラクト 4
３　ブロックチェーン技術の活用ユースケース 4
（１）行政手続など公的分野での活用 5
①　法人設立手続 5
②　政府調達手続 5
③　電子自治体 6
④　公共データの利活用促進 7
⑤　デジタルコンテンツの権利処理 8
（２）IoT など民間サービスでの活用 9
①　遠隔制御システム等におけるソフトウェアのバージョンアップ管理 9
②　IoT 機器の信頼性向上 10
③　シェアリングサービスにおける本人確認手続 10
④　顧客データの更新 11
⑤　電力取引の自動化・効率化 12
⑥　自動車のトレーサビリティ 12
⑦　宅配ボックスの配達・受取記録 13
⑧　医療データの真正性確認 14
（３）諸外国の動向 15
①　エストニア 15
②　英国 17
③　その他 17
４　今後の取組の方向性 18

１　検討の経緯

ブロックチェーン技術は、インターネット以来の革新的な技術として世界的に注目されている。従来の高いセキュリティに守られた中央管理型の堅牢なデータベースではなく、ネットワーク上に置かれた複数のサーバ（ノード）に電子署名やハッシュ関数などの技術を組み合わせることにより比較的安価でセキュアなデータベースが実現できるとして、金融分野を始めとしてさまざまな分野での活用が期待されている。

政府の成長戦略（日本再興戦略 2016 ―第４次産業革命に向けて―（平成 28 年 6 月 2 日））においても、「本格的な IoT 時代には、クラウド集中型のデータ管理・処理構造から分散コンピューティングの考えを中心に据えた構造に移行する」ことが指摘されているが、昨今、分散処理の一形態であるブロックチェーン技術が、データを安全に保管するのに最適なソリューションではないかと注目を集めている。しかし、ブロックチェーン技術については、具体的には金融分野（FinTech）での活用について語られることが多く、現に、これまでの国内での取組も金融分野をターゲットとしたものが多い。

総務省情報通信審議会においては、「IoT／ビッグデータ時代に向けた新たな情報通信政策の在り方」（平成 27 年９月 25 日付け諮問第 23 号）について検討を行う中、本年１月にとりまとめた第三次中間答申において、IoT 時代のプラットフォームレイヤーに関する具体的施策の一つとして、ブロックチェーン技術の活用の在り方について、同審議会の基本戦略ワーキンググループの下に新たな検討の場を設けて検討を行い、本年夏を目途に第一次とりまとめを行うこととされた。

そこで、基本戦略ワーキンググループの下に「ブロックチェーン活用検討サブワーキンググループ」（主任：谷川史郎　東京藝術大学客員教授）を設けることとし、別紙の構成員及びオブザーバーの参加を得て本年２月から５月にかけて会合を５回開催した。本報告書は、金融分野での先行事例や非金融分野でのブロックチェーン技術の活用ユースケースについてのヒアリング等を経て、ブロックチェーン技術の活用に関する今後の取組の方向性についてとりまとめたものである。

２　ブロックチェーン技術の基本的な特徴

ブロックチェーン技術とは、電子署名とハッシュポインタを使用して改ざん検出が容易なデータ構造を持ち、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と言われている。[1]

---

[1] 日本ブロックチェーン協会「ブロックチェーンの定義」
[http://jba-web.jp/archives/2011003blockchain_definition]参照

ここでは、本サブワーキンググループにおいて紹介された基本的な特徴をいくつか整理している。

（1）「事実上落ちない（正しく動作）」

ブロックチェーン技術では、データを保管するノードを多数配置し、当該データをネットワーク全体で共有する分散処理構造を採っているため、仮にいずれかのノードが何らかの原因により動作しなくなったとしても、他のノードが動き続けることでデータベースとしての高可用性を実現している。

一般に、分散処理構造のデータベースにおいては、参加している関係者の中に、悪意をもってデータを改ざんしたり消去したり、否認したりすることによって完全性を損なうリスクが存在する。これに対して、ブロックチェーン技術は、ノード間の Peer to Peer 通信によってデータの同期を行い、「ビザンチン障害」への実用的な解を示したと言われる点が特徴と言える。すなわち、コンピュータネットワークに参加するノードが意図的に、またはソフトウェアのバグにより意図せずエラーが起きるような通信をする状況において、ネットワークを構成するノード全体でデータの同期を正しくとることができるかという問題（ビザンチン将軍問題）を、合意形成プロトコル（コンセンサスアルゴリズム）によって実用レベルで解消している。

合意形成プロトコルは、コンピュータどうしの間で共通のデータの同期をとる「ルール」ということができ、この存在により、異なる事業者がノードを運用するなどノード間の信頼関係がない場合でも、この「ルール」によってデータの一貫性を保つことができる仕組みを実現している。

なお、オープンネットワーク上のノード間で形成する「パブリック型」と、一定の信頼関係がある者の間で形成する「パーミッションド型」[2]とでは、利用できるコンセンサスアルゴリズムが異なり、パブリック型で代表的な Bitcoin は Proof of Work[3]を、パーミッションド型の Hyperledger Fabric

---

[2] 本報告書では、「パーミッションド型」を、「プライベート型」（同一の者の中で運用されるもの）と「コンソーシアム型」（複数の者により共同で運用されるもの）両方を包含するものとして用いることとする。

[3] ブロックチェーンは、多数のトランザクション（取引）とナンス（ブロックを生成するときにマイナーによって生成される 32 ビットの数値）等を含んだブロックの連鎖から構成され、このブロックに含まれる取引のみを「正しい取引」と認めている。これを前提に、P2P ネットワーク上でマイニングを行う各ノードが、全探索・総当りによりナンス値を変化させながら、多数のトランザクション等と合わせてそのハッシュ値を計算し、特定条件を満たすハッシュ値を見つけたノードが、計算資源を正しく使ったことの証明として、生成したブロックを他ノードに配信し、ネットワーク上の全てのノードが当該ブロックのハッシュ値を検算し、これを新たなブロックとして認めることによって合意形成する方式。

はPBFT（Practical Byzantine Fault Tolerance）[4]を使っている。

パブリック型の場合には、ブロック形成に向けた反復計算（マイニング）を行う「マイナー」の確保やいわゆる「51%攻撃[5]」への対応が必要となる。また、基本的にはマイニングのインセンティブを付与するためのコイン、トークンが必要となる[6]が、インセンティブのコスト負担モデルの設計が重要となる。

パーミッションド型の場合には、コンセンサスに参加できる者が限定されるため、合意形成に対する信頼、ブロックチェーン上のデータの確かさを担保するための工夫が求められる。

（２）「事実上改ざん不可能」

現在、広く普及しているリレーショナルデータベース(RDB)においては、不正アクセスや操作ミスにより、データベース中の項目を改ざんされるリスクがある。あるデータが改ざんされた場合にはそのログが残るものの、そのログ自体も改ざんしてしまえば、改ざんした事実自体が検出不能となってしまうためである。

他方で、ブロックチェーン技術は、その名前に由来するとおり、取引データ等の電文を一定数とりまとめてブロックを形成し、当該ブロックごとに不可逆のハッシュを生成して「ダイジェスト」を作成するという仕組みを採っている。この「ダイジェスト」をチェーンのように後続のブロックへと次々につなげていくことによって、あるブロック内のデータが改ざんされた場合には、その後続のブロックの「ダイジェスト」と整合しなくなるため、改ざんの検出が容易になることから、事実上改ざんが不可能という特徴を有している。

（３）オープン性

インターネットという技術は、「切れない通信」をオープンテクノロジー（TCP/IP、HTTP、WWW 等）で実現したのに対し、ブロックチェーン技術は「落ちない」「消えない（事実上改ざん不可能）」データベースをオープンプロトコルにより監査性を確保することで、オープンなネットワーク上のノード（サーバの集団）により実現したと言える。

---

[4] ネットワークが信頼できるノードで形成されていることを前提として、書き込まれたデータが改ざんされていないことを一定数以上のノードにおいて確認（例えば多数決による承認）できた場合に、ブロックを形成する方式。

[5] 悪意のあるグループまたは個人（攻撃者）が、ネットワーク全体が持つ計算量の過半数を支配し、不正な取引を行うこと。

[6] なお、地域コミュニティにおけるコミュニケーションや環境にやさしい生活など、公共的価値のある行動へのインセンティブとして、ブロックチェーン上で発行・管理されるコインなどを活用するというアイデアもある。

同時に、技術進歩や世の中のニーズに呼応して、インターネットをベースとして仮想プライベートネットワーク（VPN）など特定の者の間でセキュリティを確保した通信環境も用意するようになったのと同様に、特定の限られた者の間で改ざんの極めて困難なデータを効率的に[7]共有するニーズに対応したパーミッションド型のブロックチェーンも登場してきている。

また、ブロックチェーン技術は、データベースの高可用性、耐改ざん性を実現するものである一方、データの秘匿性や入力されるデータの真正性[8]までを保証するものではない点においても、インターネット技術もそれ自体がセキュリティやコンテンツの真正性までを保証するものではない点と共通していると言える。

（4）スマートコントラクト

ブロックチェーンのさらなる特徴として、データを自動処理するプログラムをブロックチェーン上で動かすことにより、人手を介さなくとも、手続や契約を履行することができる「スマートコントラクト」が挙げられる。

これは、ブロックチェーンというプラットフォーム技術の機能を拡張するアプリケーションとしてさまざまな分野への応用可能性が期待され、現実社会のさまざまな手続や取引の在り方に変革をもたらしうる重要な要素といえると同時に、IoT システムの付加価値を向上させることで IoT ビジネスのマネタイズにも寄与することが期待される。

３　ブロックチェーン技術の活用ユースケース

我が国では、これまでに主に金融分野において実証実験などの取組が進められてきた。具体的には、国内の銀行間振込や国際送金・クロスボーダー証券取引のほか、仮想通貨による決済、証券のポストトレード業務などにおけるブロックチェーン技術の適用可能性について検討・検証が進められてきている。

今後、２で述べたようなブロックチェーン技術の基本的な特徴を活かして、現在我が国が抱える課題を解決できる可能性についても構想を広げ、ブロックチェーン技術のプラットフォームとしての活用可能性を幅広く検討する観点から、本サブワーキンググループでは、主として、金融分野以外のさまざまな分野におけるユースケースを扱った。

---

[7] パーミッションド型のブロックチェーンは、パブリック型のブロックチェーンと比較して、参加者を許可された者（お互いに信用できる者）に限定することで、改ざん耐性を補完しつつ、合意形成作業を簡易にすることで処理を効率化（高速化）している。

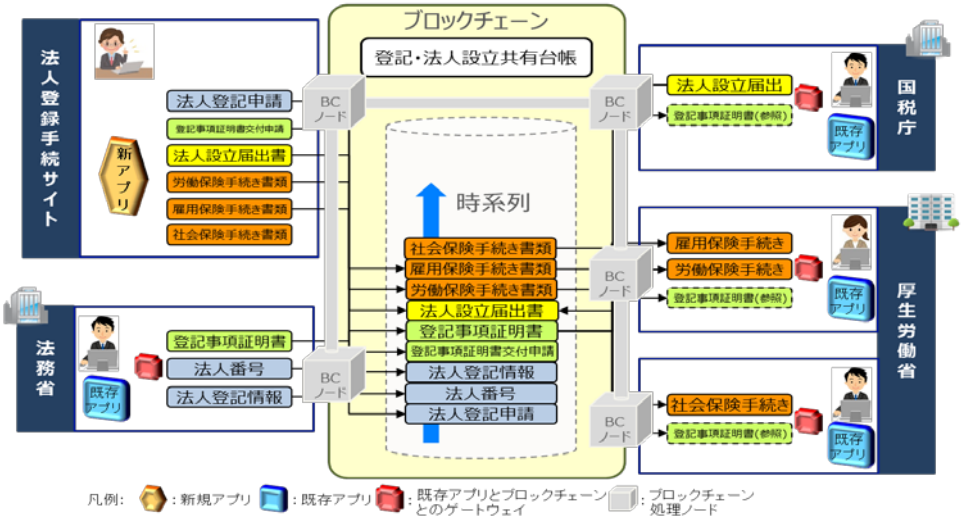
[8] データが作成者の意思に基づいて作成され、改ざんされていないこと。

（１）行政手続など公的分野での活用

①　法人設立手続

法人の設立に際しては、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など複数の手続を個別に行う必要があり、これらの手続に添付が必要な登記事項証明書を複数取得するなど、法人を設立しようとする者の負担となっているとの指摘もある。

こうした法人の設立等に伴う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ことで、オンラインでの登記事項証明の真正性を確保するとともに、手続の負担・コスト軽減と迅速化を実現できる可能性がある。



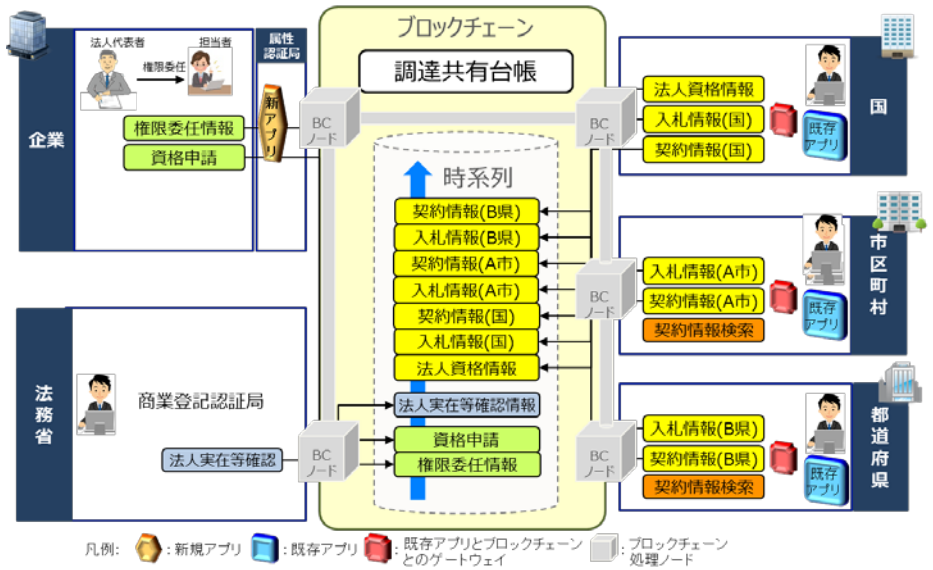
貝塚構成員プレゼンテーション資料に基づき作成

> 法人登録手続きサイトから法人登記の申請等 法人の設立に必要な手続きが開始されると、ブロックチェーン上のスマートコントラクトにより一部の手続きが自動化され、関係行政機関において必要な情報が共有される。

②　政府調達手続

現在、国や自治体の調達手続に参加しようとする者は、国と各自治体にそれぞれ資格審査を申請する必要があり、手続上の負担となっているとの指摘もある。また、国・自治体を通じた調達実績を把握・共有する仕組みが整備されておらず、調達コストの削減にはさらなる改善が求められる。

そこで、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できる可能性がある。



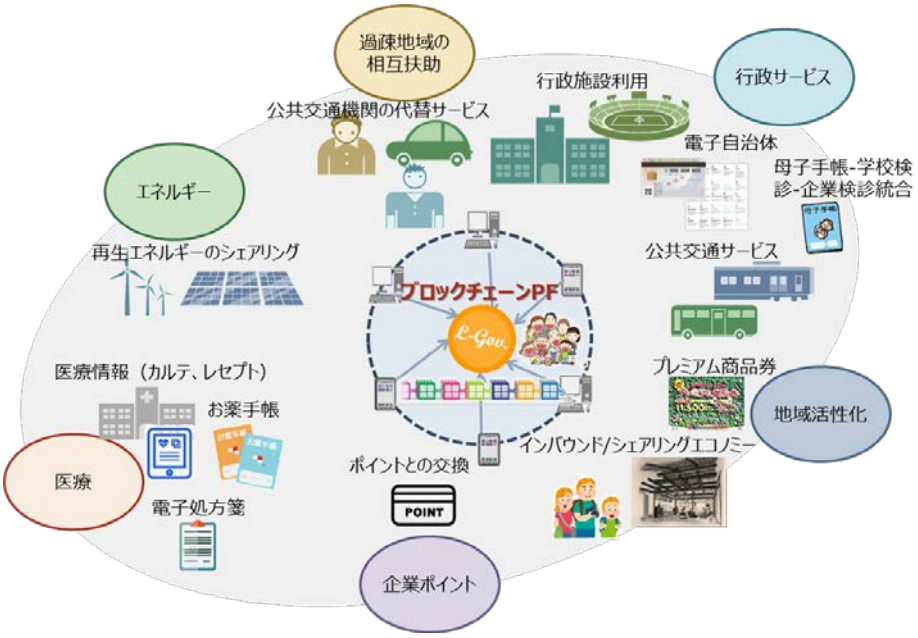
貝塚構成員プレゼンテーション資料に基づき作成

入札参加資格登録申請が開始されると、ブロックチェーン上のスマートコントラクトにより法人の実在等確認の手続き等が自動的に行われる。資格情報や調達実績はブロックチェーンを通じて国・自治体に共有される。

③　電子自治体

自治体の業務は多岐にわたるため、電子自治体を進めるに当たっては、業務ごとにデータを管理するシステムを整備するよりも、可能な限り共通プラットフォーム化することで費用対効果を向上させることが求められる。

そこで、地域振興ポイント等の各種ポイントの運用管理、受注先との手形債権の管理、母子保健・学校検診・企業検診をカバーする PHR の管理など、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ことで、効率的な電子自治体の構築に資する可能性がある。



中村構成員プレゼンテーション資料に基づき作成

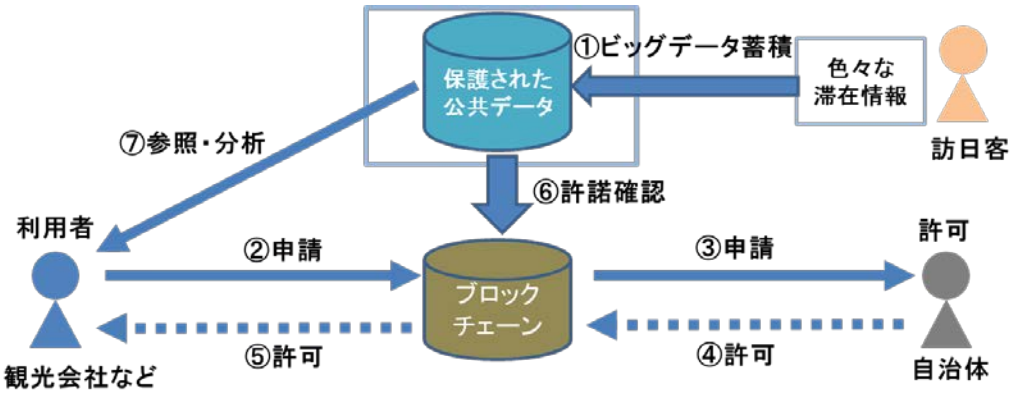
自治体等のデータ管理システムをブロックチェーンにより様々な業務にまたがる共通プラットフォームとして構築することで、安全性を確保しつつ、多数当事者間でのデータ共有等を安価に実現する。

④　公共データの利活用促進

自治体等が保有する公共データの利活用を進めるに当たって、単にデータを共有するだけでなく、データの利用状況を把握したり、データの利用価値に応じて有料制や許可制も導入したりするなど、共有方法の多様化のニーズが存在しうる。

そこで、公共データについて、利用申請・許諾プロセスや有料の場合の課金処理などをブロックチェーンで効率的かつ適正に管理することで、公共データの利用許諾等の真正性を確保しつつ、その利用を促進することが考えられる。

なお、公共データの利用価値を把握・向上させる観点から、誰が、いつ、どんな分析をしたのかという使用履歴を管理することも考えられる。

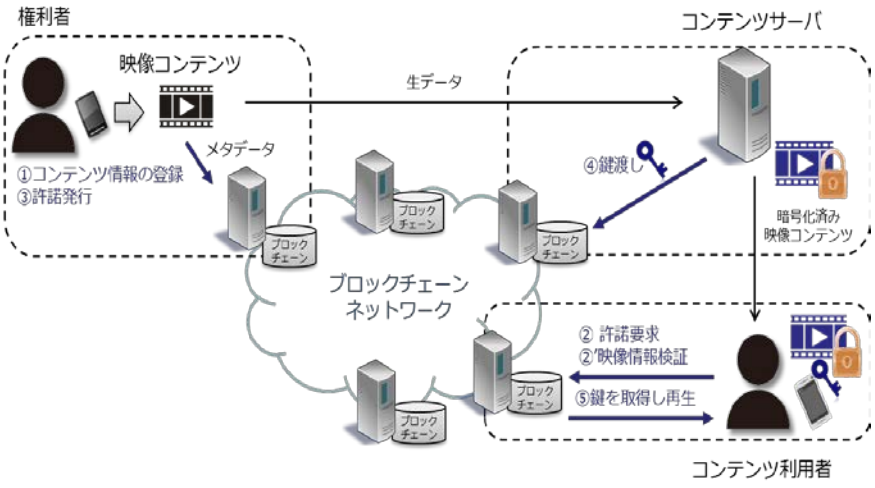


岸上構成員プレゼンテーション資料に基づき作成

自治体等のデータベースに蓄積された公共データを利用したい場合、利用者はブロックチェーンを通じて許諾申請や料金支払手続きを行う。ブロックチェーンでは許諾手続きの自動化やプロセスの記録が行われ、手続きが完了すると利用者は公共データの参照が可能になる。

⑤　デジタルコンテンツの権利処理

デジタルコンテンツの権利処理について、YouTuber など個人がデジタルコンテンツを創造し発信することが急増する可能性も視野に入れると、デジタルコンテンツの権利者情報、有効期間、価格など、コンテンツに付随するデータ（メタデータ）をブロックチェーン上に記録することで、中央管理機関などの第三者に委ねない形でコンテンツを管理するとともに、その権利関係についての真正性を保証することが、より時代にふさわしい管理の在り方となる可能性がある。



岸上構成員プレゼンテーション資料に基づき作成

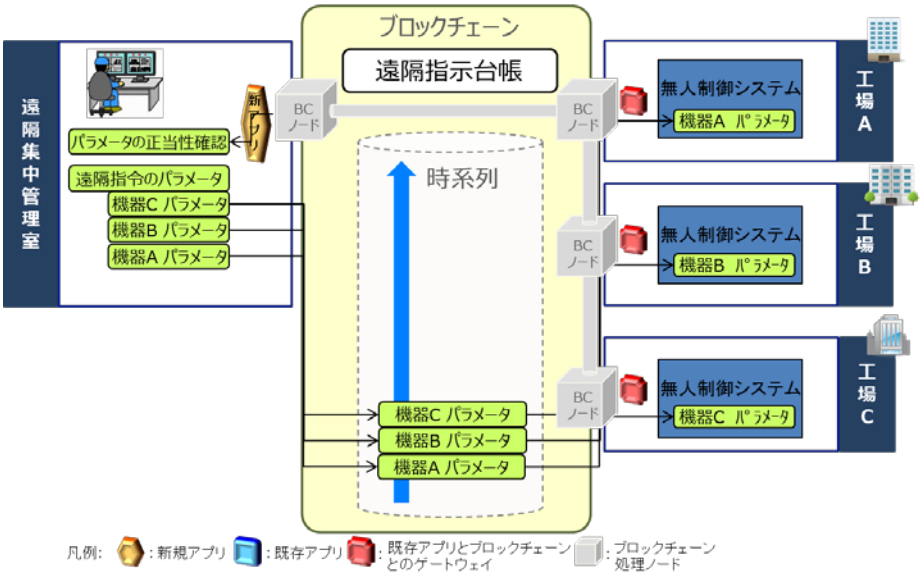
デンタルコンテンツの権利者は、コンテンツ管理サーバにデータを登録するとともに、ブロックチェーンにそのメタデータを保存し、これらを比較することでコンテンツの登録者であることを自ら証明できる。利用者はブロックチェーンを通じて利用許諾申請を行い、許諾を受けることでコンテンツを利用することができる。

（２）IoT など民間サービスでの活用

①　遠隔制御システム等におけるソフトウェアのバージョンアップ管理

石油生産設備等での遠隔制御システム等において、無人制御システムへの遠隔指示が不正に書き換えられるリスクは、人類にとっての脅威であり、可能な限り低減することが望ましい。

そこで、遠隔制御システム等の稼働パラメータ等のソフトウェアについて、ブロックチェーンの耐改ざん性を活かして管理することでその不正書換えを防ぐとともに、脆弱性を突かれるおそれのある箇所にセキュリティ対策を緊急に施す等の措置により、サイバー攻撃に対処することが考えられる。



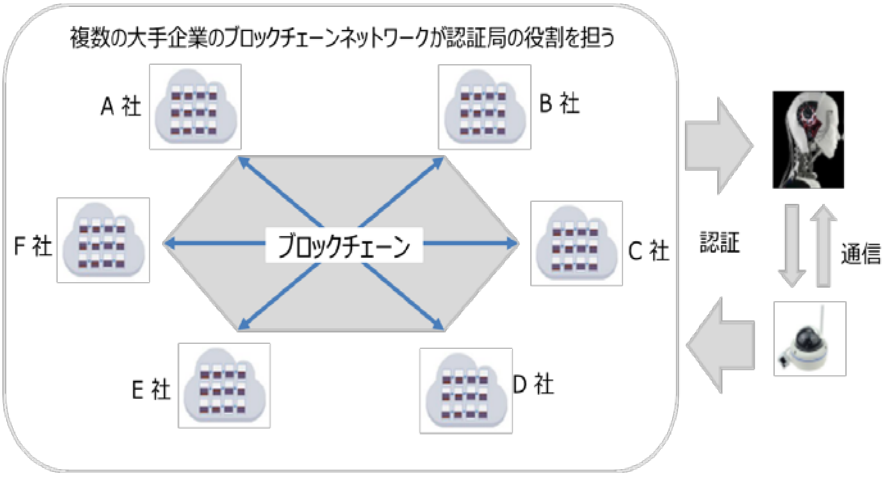
貝塚構成員プレゼンテーション資料に基づき作成

遠隔制御システムに接続された各工場の機器のパラメータ等の状態をブロックチェーンに記録し、不正書き換えの検知を行うとともに、ソフトウェアの脆弱性が発見された場合には、ブロックチェーン上の履歴を確認することで、対象の機器について特定し、緊急に対策を施すことができる。

②　IoT 機器の信頼性向上

IoT 機器を認証する仕組みとして、典型的には、ある認証局が発行する電子証明書等を IoT 機器に格納する方法が考えられる。

今後、本格的な IoT 時代を迎えるに当たり、認証情報（どの IoT 機器が通信したのか）をブロックチェーンで管理することで、認証情報の信頼性を向上するという直接の目的のほか、サイバー攻撃を探知して IoT 機器のセキュリティ回復、IoT 機器間の通信の暗号化や IoT 機器が生成するデータの真正性確保を通じたビッグデータの信頼性向上を実現することなどが期待される。



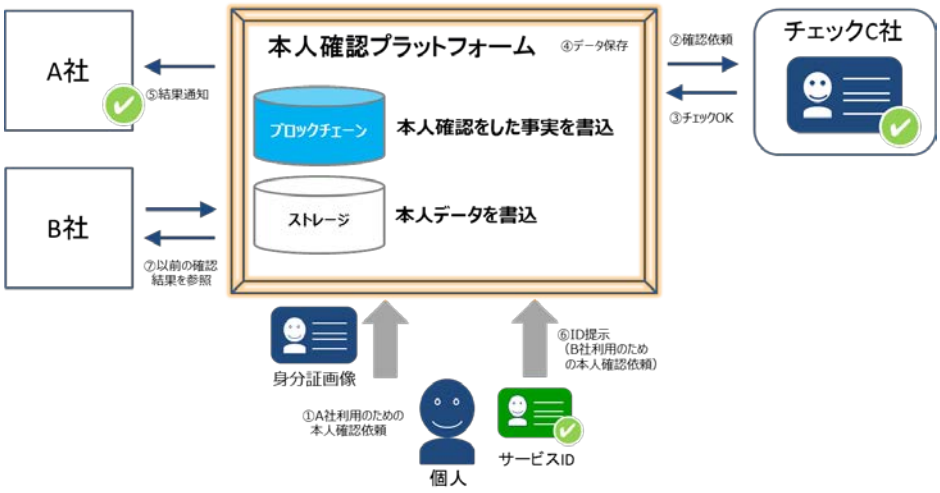
合同会社 Keychain　三島様プレゼンテーション資料に基づき作成

IoT 機器は相手方との通信許可を認証局に求める。認証局は複数の企業によるブロックチェーンネットワークにより構築されており、可用性が高く改ざん検知も容易である。

③　シェアリングサービスにおける本人確認手続

シェアリングエコノミーを提供する事業者にとっては、本人確認の手続が煩雑であり、これらの事業者間で本人確認結果を共有したいニーズがあるとの指摘がある。

そこで、運転免許証やマイナンバーカード等により本人確認を行った結果をパブリックブロックチェーンに記録することにより、本人確認サービスの信頼性の向上を図るとともに、シェアリングサービスにおける本人確認を業界で共通化し、本人確認の煩雑さを解消することが期待される。



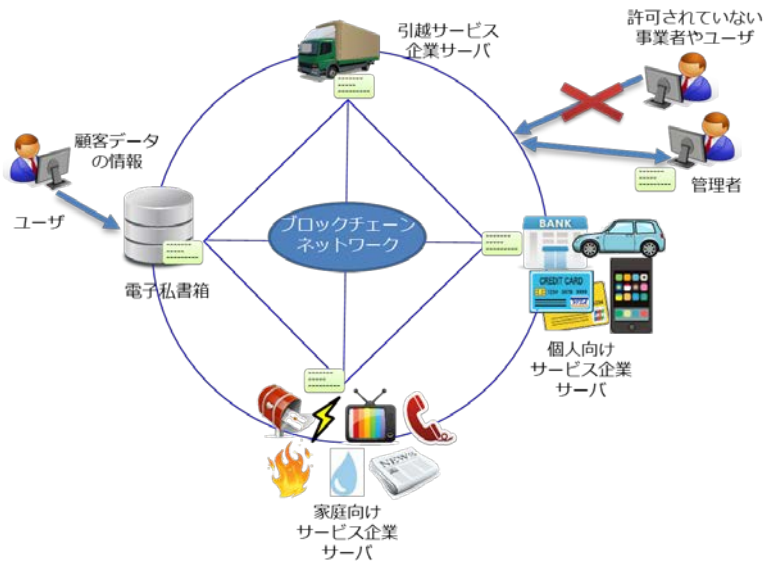
北村構成員・肥後構成員プレゼンテーション資料に基づき作成

プラットフォームは本人確認をした事実をブロックチェーンに書き込み公開する。サービス提供事業者は利用者の申請に応じてブロックチェーンを参照することで本人確認が完了していることを確認できる。

④　顧客データの更新

日常生活において多種多様なサービスを利用するに当たり、各サービス提供事業者に対し、本人が自らの情報の登録や更新について、それぞれ個別に伝える必要があり、本人は煩雑な作業を強いられている現状がある。

そこで、各サービス提供事業者が保有する顧客データについて、本人がブロックチェーンに書き込んだ情報を、ブロックチェーンに参加する事業者間で共有することで、顧客データの一括更新手続を効率的に実現することが期待される。

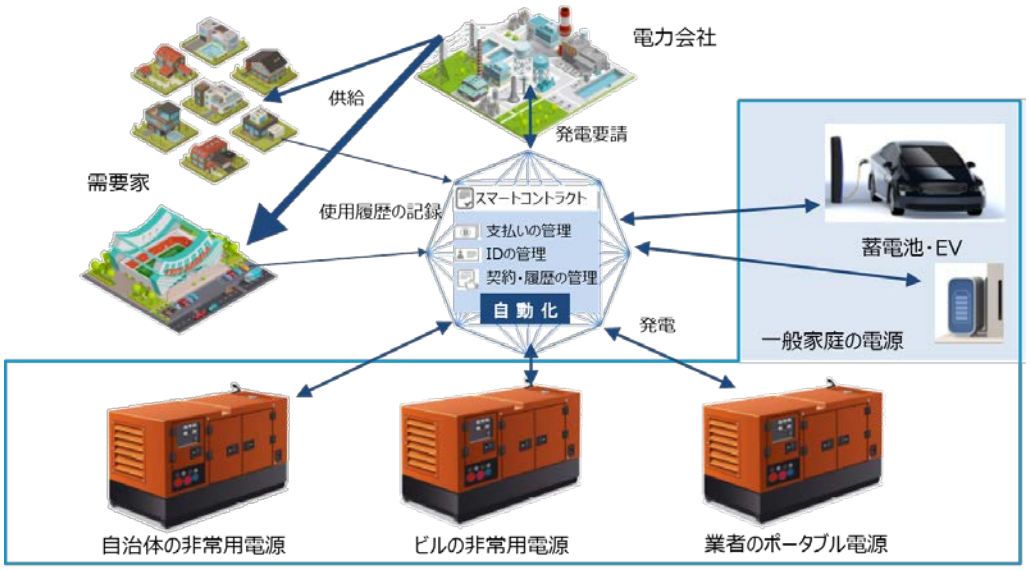


阿部構成員プレゼンテーション資料に基づき作成

ユーザは電子私書箱に自らの顧客データの更新情報を登録する。登録情報はユーザが承認した企業等にブロックチェーンネットワークを通じて共有され、一括更新手続が完了する。

⑤　電力取引の自動化・効率化

電力需要に対して余剰電源から電力を調達する方式について、第三者を介在させることによる手数料等のコストを低減するため、電力会社から分散型電源（自治体などが保有する非常用電源や一般家庭の太陽光発電など）への発電要請、対価支払いといった電力取引の履歴をブロックチェーンで管理し、スマートコントラクトを活用して自動で処理することで、透明かつ効率的な電力シェアリングエコノミーを形成できる可能性がある。



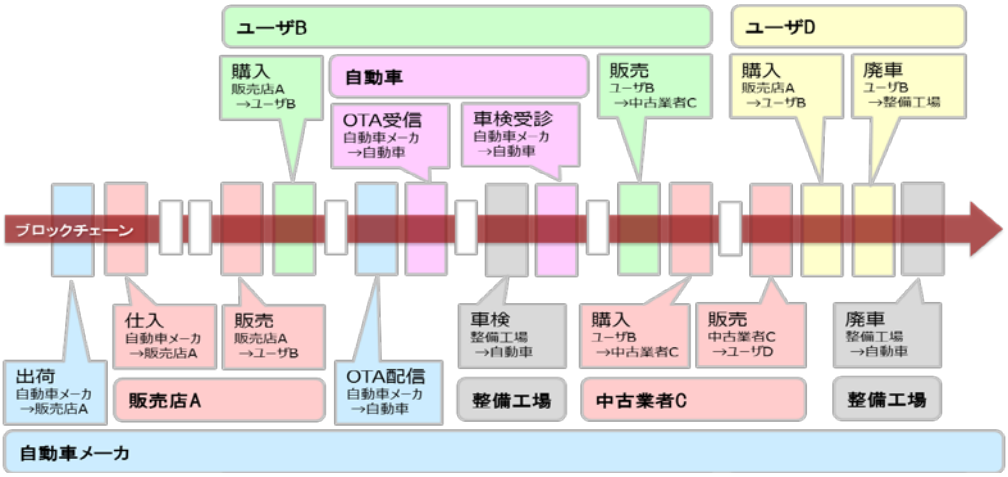
肥後構成員プレゼンテーション資料に基づき作成

電力会社からの発電要請に応じて分散型電源において電力の共有が行われる。取引についてはスマートコントラクトにより自動処理され、その履歴がブロックチェーンに保存される。

⑥　自動車のトレーサビリティ

自動車には、今後さまざまな機器・サービスが搭載されていくと見込まれており、これまで以上に多種多様な関係者が自動車の製造や不具合の検査・処理に携わることが想定される中、自動車の製造から中古販売に至るまでの多数の関係者による情報共有がこれまで以上に必要となる。

そこで、Connected Car に関して「誰（どの機器）が、いつ、何を行ったか」をブロックチェーン上に記録することで、自動車のライフサイクルにおける正確なトレーサビリティを関係者間で確保することが期待される。

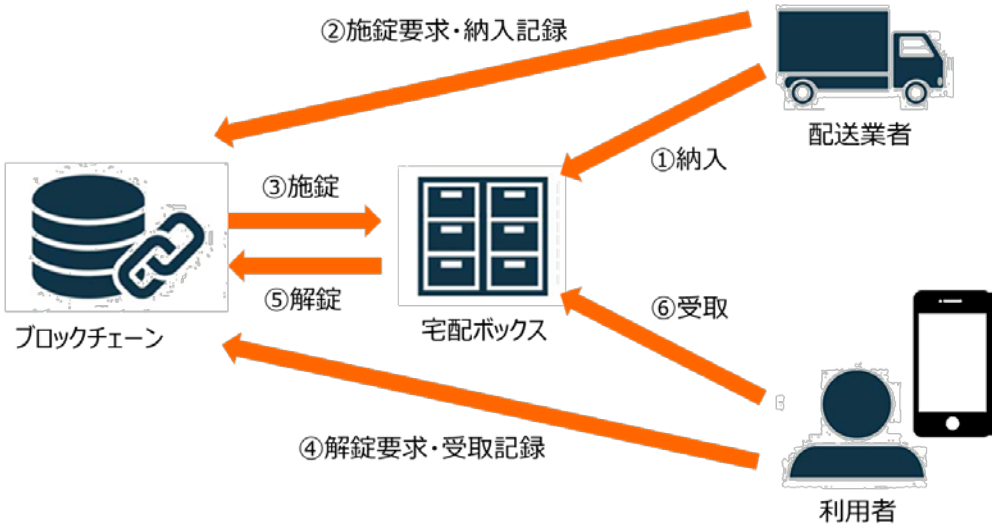


北村構成員プレゼンテーション資料に基づき作成

自動車の製造・販売・点検・修理等に携わる事業者において、自動車に対して行った手続きをブロックチェーンに記録することで、出荷から転売、廃車までの記録が一括管理される。

⑦　宅配ボックスの配達・受取記録

宅配ボックスを用いた配達・受取について、その利便性を確保しつつ、授受に伴うトラブル発生のリスクを可能な限り低減するため、宅配ボックスの開閉記録をブロックチェーンで管理することで、荷物の受け渡し・受け取りの事実を、改ざんのない形で客観的に把握可能とすることが有用と考えられる。



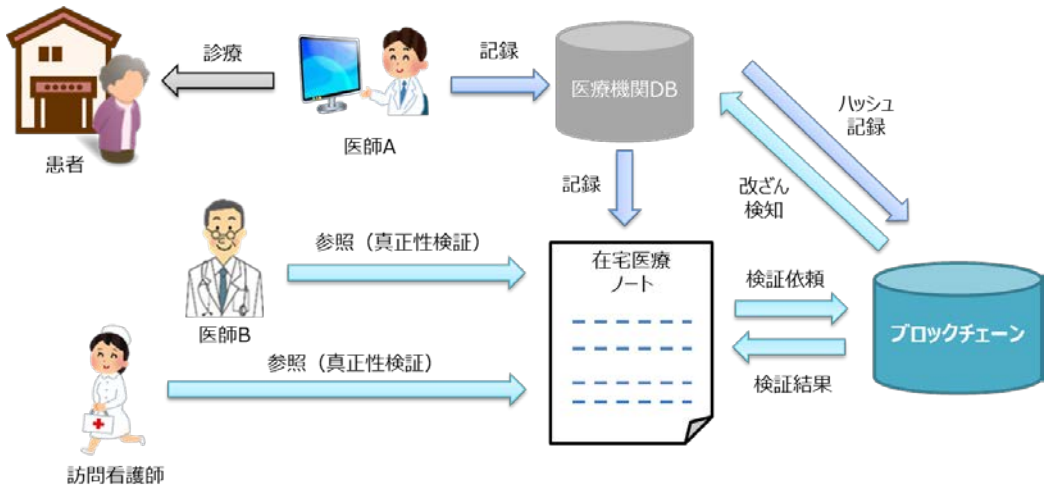
山下構成員プレゼンテーション資料に基づき作成

配送業者は宅配ボックスに荷物を納入し、その記録をブロックチェーンに書き込むとともに、宅配ボックスの施錠を要求する。利用者はブロックチェーンに解錠要求を行い、荷物を受け取るとその記録がブロックチェーンに書き込まれる。

⑧　医療データの真正性確認

在宅医療においては、一人の患者に対して医師、看護師、救急隊員などの多数の関係者が容態を観察し、処置を施すことになるため、「データに誤りはないか」とともに、「誰が、どのデータを見てよいか」といった点を効率的に管理するニーズがあるとの指摘がある。

そこで、在宅医療に携わる関係者が、ブロックチェーン上で管理されている署名済みの在宅医療データの「ハッシュ」（アクセス可能な範囲でグルーピングされたもの）を検証することで、アクセスコントロールを効かせつつ、別のデータベースに格納されている患者のデータの真正性を確認することが考えられる。



慶應義塾大学 鈴木様プレゼンテーション資料に基づき作成

一人の患者について時系列・項目別に記録された署名済みの在宅医療データのハッシュをブロックチェーンに記録することで、データの監査性を高める。

（３）諸外国の動向

ブロックチェーン技術についての世界的な潮流としては、仮想通貨、サプライチェーン、証券取引といった分野で実用化が現実的なものとなっているほか、実証的な取組が始まっている分野として金融基幹業務や送金、決済やポイント交換などの商取引のほか、IoT などが挙げられる。

また、我が国と諸外国との間では、上記の各分野においては、程度の差こそあれ、いずれでも取組が進んできているのに対して、特に、公的サービスや政府系システムに対する取組状況は、我が国に比べて諸外国のほうが進んでいると言われている。

そこで、本サブワーキンググループでは、特に、公的サービスや政府系システムに関する諸外国の取組事例を中心に扱った。

①　エストニア

エストニアでは、各省庁や民間のデータベースをインターネット経由で相互参照可能とするプラットフォーム（X-ROAD）において、ブロックチェーン技術を採用している。[9]このプラットフォームと ID カードを用いた電子認証とを組み合わせることで、世界最先端レベルの電子政府を実現

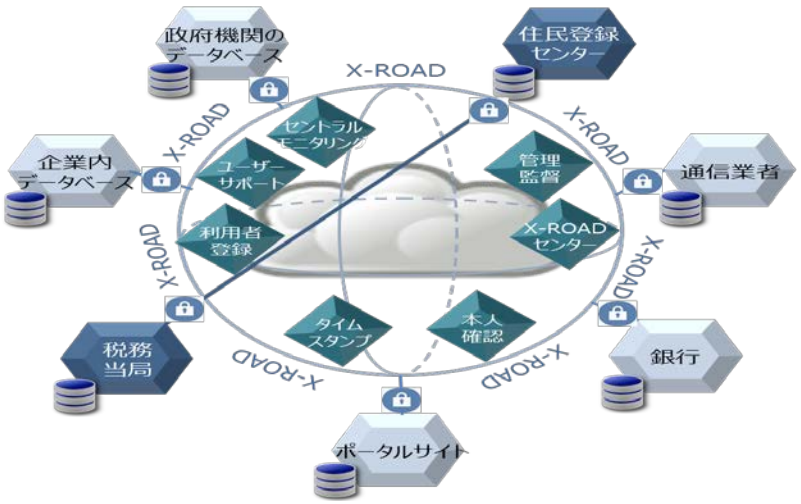
[9] X-ROAD は既存システム間の情報を連携するためのプラットフォームであり、このプラットフォーム上を流通するデータの改ざんをリアルタイムに検知するため、ブロックチェーン技術（KSI（Keyless Signature Infrastructure）：データのイベントログ（いつ、どこで発生したか）をチェーン化する技術）を採用している。

している。

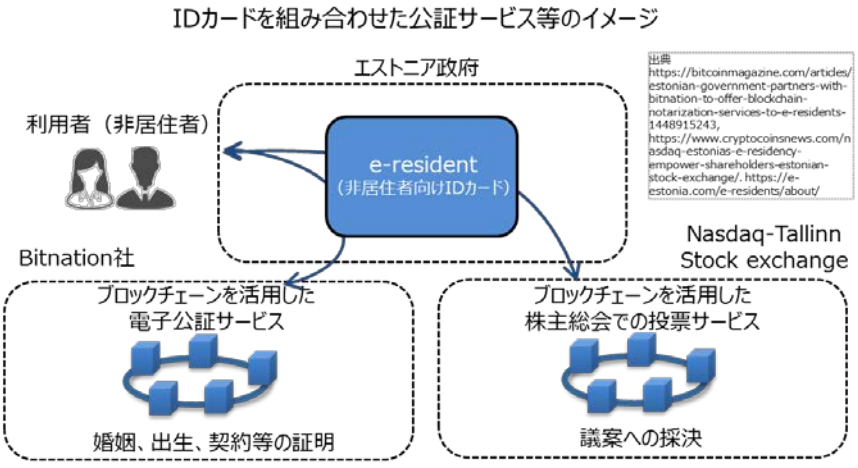
これにより、官民合わせて 2,500 以上のオンラインサービスが利用可能となっており、例えば、銀行の本人確認や納税、選挙の投票、法人登記などについて ID カードの電子署名による手続が可能となっている。

また、民間が運営するブロックチェーン上の情報を信頼して、ID カードによる認証により、婚姻・出生等の証明（公証サービス）や株主総会での投票サービスなど民間による公的サービスの提供を実現している。

さらに、すべての病院、薬局がシステムに接続されているため、自らの過去の病歴をすべてオンラインで閲覧可能となっているほか、身分証明書を提示するだけでいつでもどこでも電子処方箋に基づいて薬を受け取ることができる。



中村構成員プレゼンテーション資料に基づき作成



高木構成員プレゼンテーション資料に基づき作成

② 英国

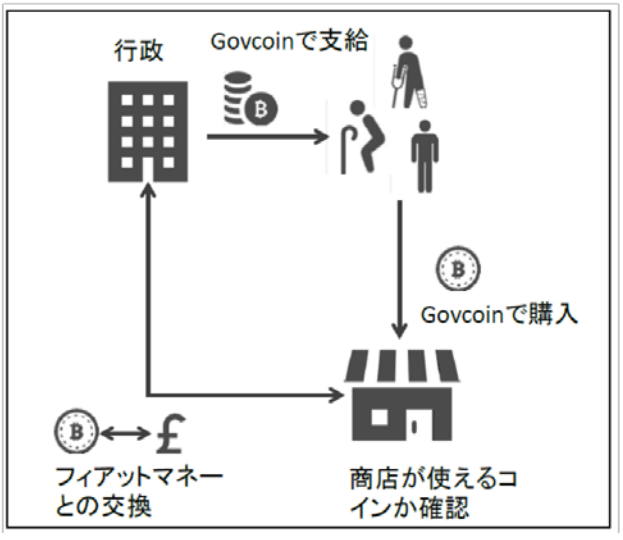
英国は、政府がブロックチェーン技術を公共分野で活用する５つのユースケースを提案するなど、ブロックチェーン技術の活用について非常に積極的に取り組んでいる国の一つと言える。

その提案では、社会保障給付、国際援助といった金銭給付をはじめ、知的財産、特許等の登録データベースへの活用やソフトウェア改ざん検知による重要インフラ防御など、行政全般にわたってブロックチェーン技術を活用するアイデアが盛り込まれている。

特に、社会保障給付については、英国の労働年金省が生活保護費の支給にブロックチェーン上の仮想通貨を利用する実証実験を実施しており、使途が限定できるという仮想通貨の特徴（カラードコイン）を活用して、生活保護制度の目的に合致しない支出を抑制する取組を試行している。

また、国際援助については、国際機関の世界食糧計画（WFP）による現金及び食料給付をブロックチェーンに記録することで、処理の透明性を確保しつつ多様なステークホルダーでの情報共有を可能とするとともに、現地政府や NGO などの中間組織を介在せずに、支援を必要とする人に直接的に給付できる仕組みの構築を提唱している。

社会保障給付での活用イメージ



高木構成員プレゼンテーション資料に基づき作成

③ その他

エストニアや英国のほかにも、世界各国で、公共分野や行政へのブロックチェーン技術の導入は活発に検討されていると言える。

例えば、不動産登記や取引の記録については、スウェーデン、米国、オランダなどの欧米諸国のみならず、ジョージア（グルジア）、ホンジュラス、ガーナといった途上国でもブロックチェーン技術の活用が検討されて

きている。特に、スウェーデンでは、土地管理局のシステムとして、不動産の売主・買主、ブローカー、登記所、銀行が参加・利用するスマートコントラクトを設計し、多数のステークホルダー間での信頼できる情報共有を容易にして売買から登記までの処理をシームレスに実現したと言われている。

このほか、投票システムへの導入がオーストラリアや韓国などで検討され、また、身分や学位の証明をブロックチェーン上で管理する取組がオーストラリア、スペイン、米国などで進められてきている。

なお、欧米諸国を始めとする先進国では、既存システムと比較して手続、取引のコスト削減やセキュリティ向上などの可能性を探るため、ブロックチェーン技術の導入が検討されていると考えられるが、既存システムを上回る明確なメリットを検証している段階にあると考えられる。これに対して、途上国ではそもそも公共サービスや行政手続などの業務プロセスやシステムが確立していない等の事情があり、安価でセキュアという性質を有し、かつ、スマートコントラクトによる業務プロセスのビルトインが可能なブロックチェーン技術の導入が積極的に検討されているのではないかと考えられる。

4　今後の取組の方向性

今後、IoT 時代のプラットフォームとしてブロックチェーン技術の活用を進めるために我が国が当面取り組むべき方向性を検討するに当たり、これまでの本サブワーキンググループでの議論を通じて、以下のような示唆が得られた。

- ブロックチェーン技術は、可用性が高く、かつ、事実上改ざん困難なデータベースを、オープンプロトコルにより監査性を確保することで実現した。例えばビットコインのように、不特定多数の者がオープンネットワーク上で参加しながら取引内容の透明性と耐改ざん性を確保するという特徴は、ブロックチェーン技術の革新的な点である。加えて、複数のノード間を確実に同期させ、データベース全体の強靭性を高める機能や、スマートコントラクトによって処理の自動化を容易にする機能についても、ブロックチェーンならではの重要な特徴と考えられる。
- 本サブワーキンググループで報告された活用事例には、不特定多数の者が参加してオープンネットワーク上で耐改ざん性等の確保を図る「パブリック型」と、認証されたノードによるネットワークを前提とする「パーミッションド型」の双方が見られた。
- 以上にかんがみれば、ブロックチェーン技術の社会実装を進めていく上では、共通の特徴やそれぞれの相違点を踏まえた上で、ニーズに応じて「パブリック型」と「パーミッションド型」の双方の活用を視野に進

めていくことが適当と考えられる。

- ブロックチェーン技術自体は、データの秘匿性や入力されるデータの真正性を保証するものではない。そのため、ブロックチェーン技術の活用に当たっては、特にビジネスユースや行政においてセンシティブな情報を扱う場合においてデータの秘匿性を確保するためのアクセス制御や、参加者の本人性や入力されるデータの真正性を確保するための公的個人認証サービスなど、他のソリューションを適切に組み合わせることで、活用ニーズに応じたデータベースを設計・構築していくことが必要である。[10]
- 国内では金融分野での取組が先行しているが、商取引や IoT 分野でも徐々に進みつつある。他方、諸外国に比べ、公的サービスや政府系システムへの導入に向けた取組は遅れている。
- ブロックチェーンはデータベースの代わり、仮想通貨やトークン機能、自立的サービス稼働の仕組みとして活用できるが、特定の信頼できる組織を前提として、単に既存のデータベースの代わりとしてデータを登録するためだけにブロックチェーン技術を活用するメリットは少ないと考えられる。他方、スマートコントラクトを活用して処理の自動化、前後の業務プロセスとの連携を行う場合や、異なる組織・団体間で多様なステークホルダーが連携する業務（特に、生産性向上の観点から、異なる業態の組織・団体が現状それぞれ行っている顧客データの確認・更新など競争の働かない業務）への適用、IoT とスマートコントラクトの活用や既存システムとの API 連携による決済処理への組み込みなど、既存システムでは容易に実現できないメリットを見出せるようなユースケースに導入することによって、大きな改善効果が得られると考えられる。

上記のような認識の下、今後、以下の方向性のもとに、早急に取組を進めていくべきである。

- 他国に後塵を拝することなく、世界に先駆けてブロックチェーン技術の社会実装を推進するため、まず、処理の自動化等による業務プロセスの改善や多数当事者間での共有などにより、具体的にどのような課題が解決されるのかを明確にした上で、ブロックチェーン技術のメリットがより発揮されうるユースケースとして、①政府調達システムなどの政府情報システム（特に、多数の行政機関・事業者が関わり自動処理や情報共

[10] なお、最近では、２（２）②「IoT 機器の信頼性向上」の取組のように、ブロックチェーン技術を活用して、データの秘匿性や真正性そのものを確保する仕組みの開発も進められている。

有のメリットが見込まれる政府調達システム）への適用や、②異なる業態の組織・団体間の生産性向上に向け、実証実験に早期に着手する。
具体的な検証イメージとしては、

- ①については、具体的な省庁と地方公共団体の参加を得て、事業者の資格審査及び入札・契約手続にブロックチェーン技術を活用し、スマートコントラクトの活用による自動処理を含め、導入した場合のシステムのコスト軽減効果や、国・地方公共団体の業務プロセスの見直しの可能性等について検証を行う
- ②については、例えば、シェアリングエコノミー事業者やFinTech事業者[11]等もっぱらオンラインでサービスを提供する事業者や、郵便局、通信事業者、金融機関その他の民間事業者など、具体的な事業者の参加を得て、顧客データの確認や登録・更新の場面で本人が書き込んだ情報をブロックチェーン上で共有することによる事業者や本人（利用者）のコスト削減効果や、サービスとしての運用可能性、情報の秘匿性確保の方法等について検証を行う

といった方向性が考えられる。

- また、これらの実証実験において、電子委任状に係る制度やブロックチェーンに記録されるデータの真正性確保、アクセス権確認のための公的個人認証の活用、スマートコントラクトを活用した手続の効率化の促進等の実現に向け、運用面、ルール面の課題について検討する。その検討結果も踏まえ、ブロックチェーンなど新たな技術も盛り込んだ業務改革により、効率性や利便性の向上に資する革新的な電子行政の実現に向けた計画を、来年度を目処に策定する。
- あわせて、我が国における民間分野でのブロックチェーン活用の取組を後押しするため、具体的な検証等を通じて、開発のノウハウや技術的課題のフィードバックとともに、ブロックチェーン上のデータの取扱いなどに関する運用面・ルール面での課題を抽出し、具体的な対応方策を検討する。

  具体的に運用面の課題として想定されるものは、例えば、ブロックチェーン上のデータにアクセスするための鍵の管理のあり方が考えられる。ブロックチェーンの利用者が持つ秘密鍵はブロックチェーン上のデータの信頼性の土台であり、その管理主体や紛失等のインシデントが発生したときの処理や責任のあり方等について整理していくことは、ブロ

[11] 本サブワーキンググループにおいても、「FinTech ビジョン」（平成 29 年 5 月 8 日経済産業省）の中で、本人確認がデジタルで完結することが課題として掲げられている旨に言及があった。

ックチェーン技術が社会に受け入れられ、安心して利用されるために必要な要素と考えられる。

また、ブロックチェーンを活用したシステムの社会への定着を見据え、インターネットの TCP/IP や DNS などがメジャーな技術としてアップデートされていく仕組みが自律的に構築され低コストで継続的に運営されているという先例も踏まえつつ、ブロックチェーンがネットワーク上で有機的につながっていくための「ブリッジ」への対応等も含め、ブロックチェーンがサステナブルに運営されていくための工夫を実証実験とあわせて検討することも重要である。

さらに、ルール面の課題として、例えば、ブロックチェーン上の記録が監査に耐える品質であるかどうか、裁判上の証明力（証拠能力）がどの程度認められうるかという点に関する検討・研究を進めることも社会実装を進める観点からは重要である。

加えて、IoT 時代のデータ活用の在り方や業務プロセスに変革をもたらす可能性のあるスマートコントラクトに関して、契約の成立・履行・変更等に関する法解釈の整理や、プログラムにバグがあった場合やバグが生じた場合の紛争解決ルールの検討にも取り組む。

なお、その際には、社会のニーズに即して、ブロックチェーン技術による社会変革を促す観点から必要なルール整備の在り方を検討するという視点を持つことが重要である。

ブロックチェーン技術によるデジタル社会の変革は、我が国が早急に取り組むべき課題の一つである。上記で方向性を示した取組を着実に推進し、国際的にも主導的地位を確立するなど我が国の取組が功を奏するためには、総務省のみならず、経済産業省などの関係各省庁との連携・協力が不可欠であるとともに、本サブワーキンググループの構成員を含め、ブロックチェーン技術の開発・実装や研究に携わる我が国の企業や有識者の叡智を結集してオールジャパンで取り組むことが必要である。

今後、本とりまとめも一つの契機として、我が国におけるブロックチェーン技術の開発や社会実装、これに必要なルール整備の機運が一段と高まることを期待する。