ブロックチェーン技術活用ガイドライン

2025 年 2 月

株式会社 NTT データ

1　本書において前提とする資源循環モデル 7
1.1　本ガイドラインの活用方法 7
1.1.1 想定読者 7
1.1.2 ドキュメント構成と活用方法 7
1.2　本ガイドラインの目的 8
1.2.1 背景 8
1.2.2 目的 8
1.2.3 資源循環モデル化対象業務 9
1.3　資源循環モデルのあるべき姿 10
1.4　資源循環モデルの課題 11
1.4.1 加工組立型産業全体における課題 11
1.5　動脈産業の特徴 13
1.5.1 本節の目的 13
1.5.2 動脈産業の特徴 13
1.6　静脈産業の特徴 15
1.6.1 本節の目的 15
1.6.2 静脈産業の特徴 15
1.6.3 クローズドループ 16
1.6.4 オープンループ 17
1.7　モデルに考慮すべき指標 18
1.7.1 規制・標準化類 18
1.7.2 価値測定 19
1.8　ツールチェーン整備 24

1.8.1 ツールチェーン整備の必要性 24
1.9 プラットフォーム全体像 25
1.9.1 プラットフォームに求められる要件 25
1.9.2 プラットフォーム全体像 26
2 ブロックチェーンの利点と課題 29
2.1 ブロックチェーンについて 29
2.2 ブロックチェーン検討の必要性 31
2.2.1 システム要件 32
2.2.2 主なデータ管理関連技術 33
2.2.3 システム要件に対する技術比較 33
2.3 技術的特性 34
2.3.1 分散台帳 35
2.3.2 非中央集権性（コンセンサスアルゴリズム） 35
2.3.3 スマートコントラクト（自動執行） 36
2.3.4 データ構造（ハッシュチェーン） 37
2.3.5 デジタル署名（トランザクション） 37
2.3.6 ブロックチェーンの分類 38
2.4 機能面における利点と課題 39
2.4.1 利点 39
2.4.2 課題 40
2.5 非機能面における利点と課題 42
2.5.1 セキュリティ 42
2.5.2 性能・拡張性 45

2.5.3 可用性 46
2.5.4 運用・保守性 48
2.5.5 移行性 51
3 対象業務におけるブロックチェーン技術の適用範囲と利点・課題 53
3.1 システムイメージ：全体像 / 適用範囲 53
3.2 ブロックチェーン適用の理由・利点の検討 55
3.2.1 1 章（業務観点のシステム要件）についての整理 55
3.2.2 2 章（ブロックチェーンの利点と課題）についての整理 55
3.2.3 要件に対するブロックチェーンの適合性 56
3.2.4 ブロックチェーンの適合性の判断理由 57
3.2.5 ブロックチェーン適用範囲について 59
3.3 ブロックチェーン適用による課題 61
4 対象業務におけるブロックチェーン技術要件 62
4.1 ブロックチェーン適用に関する要件 62
4.1.1 ブロックチェーンにより実現すべき事項および解決すべき事項 62
4.2 性能を確保するためのブロックチェーン要件 63
4.2.1 性能モデル定義 63
4.2.2 性能リスクと対策案 67
4.3 情報漏洩・改ざんを防止するブロックチェーン要件 71
4.3.1 秘匿の定義 71
4.3.2 秘匿要件の検討 71
4.3.3 秘匿要件の実現 75
4.3.4 関連する検討ポイント 79

4.3.5 ブロックチェーンノード構成の検討 82
4.3.6 改ざん防止の実現 84
4.3.7 処理ロジックの透明性と確実性 85
4.4 ブロックチェーンに格納する情報に関する要件 86
4.4.1 オフチェーンとは 86
4.4.2 ハッシュ値の利用 86
4.4.3 ブロックチェーンに格納しない（オフチェーン）データの必要性 88
4.4.4 情報の格納先に関する要件 89
4.5 認証方式に関するブロックチェーン要件 90
4.5.1 認証方式の要件検討 90
4.5.2 認証方式の要求実現 90
4.6 可用性に関するブロックチェーン要件 92
4.6.1 可用性の要件検討 92
4.6.2 可用性の要求実現 92
4.7 運用・保守性に関するブロックチェーン要件 94
4.7.1 各事業者の運用・保守に関する要件 94
4.7.2 運営事業者の運用・保守に関する要件 95
5 ブロックチェーン技術利活用時の注意点・考慮事項 97
5.1 ブロックチェーン技術を利用・開発する上での注意点 97
5.1.1 ブロックチェーン基盤の選定 97
5.1.2 海外事業者参画時の考慮事項 97
5.1.3 ノード管理に関する考慮点 97
5.1.4 スマートコントラクト開発時の注意点 98

5.2 CE 情報流通 PF の普及展開に関する課題への対応策 99
5.2.1 オンボーディング 99
5.2.2 相互運用性 99
5.2.3 継続性 99
5.3 海外の類似・関連システムとの連携 100
5.3.1 類似・関連システム 100
5.3.2 海外事例を踏まえて、将来的な相互連携のための検討事項 102
6 まとめ 104

1 本書において前提とする資源循環モデル

本章では、最初に本ガイドラインの活用方法について説明する。

次に、本ガイドラインにおいて前提とする資源循環モデルと、その業務要件およびシステム要件について説明する。

1.1 本ガイドラインの活用方法

1.1.1 想定読者

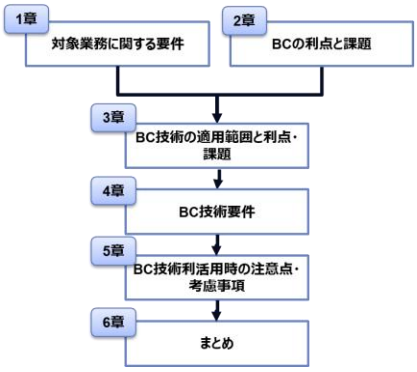
本ガイドラインは、以下の読者を想定している。

- 資源循環経済におけるデータ流通を行うシステム導入を検討する方
- 「サーキュラーエコノミー情報流通プラットフォーム（以降では CE 情報流通 PF と表記）」において、ブロックチェーン（以降では BC と略記する場合がある）技術の適用を検討する方

なお、本ガイドラインでは BC 技術の主な特性（利点や課題）について説明するが、その前提となる要素技術（暗号技術、ハッシュ関数等）や BC 技術の詳細（コンセンサスアルゴリズム、スマートコントラクト等）について理解している前提にて記述している。

1.1.2 ドキュメント構成と活用方法

本ガイドラインのドキュメント構成を以下に示す。



章	記載内容
1章	本ガイドラインの対象業務とその業務要件・システム要件について説明する。
2章	CE情報流通PFにおけるBCの必要性について説明する。 また、一般的なBCの利点と課題について説明する。
3章	対象業務で求められるシステム要件（1章）に対して、BCの利点（2章）を活かしてBCを適用する範囲を定め、それに伴う課題を説明する。
4章	3章で定めたBC適用範囲において、BCに対して必要となる要件や、活用方法の指針を説明する。
5章	BC技術を利活用する際の注意点や考慮事項について説明する。
6章	ガイドライン全体のまとめを示す。

図 *1-1*

本ガイドラインの活用方法を以下に示す。

- 資源循環経済におけるデータ流通を行うシステム導入において、本ガイドラインを参照して BC の利点を活かしつつ適用し、また課題への対策を行うことで、BC 活用を最適化する。
- 「ウラノス・エコシステム」に準拠したアーキテクチャにおいて BC 適用を検討する際に、本ガイドラインを参照して検討を行うことで、BC 活用を最適化する。

1.2 本ガイドラインの目的

1.2.1 背景

近年、廃棄物問題や気候変動問題等の環境制約に加え、世界的な資源需要と地政学的なリスクの高まりといった資源制約の観点から、資源の効率的・循環的な利用と付加価値の最大化を図る、循環経済（サーキュラーエコノミー）への移行が喫緊の課題となっている。そのため、経済産業省では、総合的な政策パッケージである「成長志向型の資源自律経済戦略」を昨年 3 月 31 日に策定している。

「成長志向型の資源自立経済戦略」において、資源循環に必要となる製品・素材の情報（製品中における、化学物質情報、再生材の使用割合、再生材の製造者情報等）や循環実態の可視化を進めるため、2025 年を目途に、データの流通を促す CE 情報流通 PF を立ち上げることを目指している。具体的には、CE 情報流通 PF が様々な製品・素材等のユースケースへ展開でき、情報の信頼性等の担保が可能となる中で、多数のユーザがシステムを利用できる共通基盤の確立を目指す。

1.2.2 目的

「令和 5 年度補正資源自律経済確立産官学連携加速化事業（サーキュラーエコノミー情報流通プラットフォームの調査・検証に関するオープンイノベーション事業）に係る企画競争募集要領」における「ブロックチェーンの活用に関する調査・検証」の事業として、CE 情報流通 PF においてブロックチェーン技術を用いる際の利点と課題、当該利点や課題を踏まえてブロックチェーン技術を用いる範囲を検討する。

また、データ流通を伴う検証内容を踏まえてガイドラインを作成し、CE 情報流通 PF を開発する事業者が開発時に参照可能なものとする。また、CE 情報流通 PF を開発する事業者が、普及のボトルネックとなる課題（相互運用性等）を解決するために業界標準等を議論の上構築・公開する。

1.2.3 資源循環モデル化対象業務

本節では、資源循環モデル化対象について示す。

1.2.3.1 資源循環モデル化対象業務

今回は情報特性、ニーズ特性、動脈産業、静脈産業のニーズ分析を行い、部品カバレッジの高い加工組立型産業をモデルケースとして資源循環シナリオの検討を実施する。

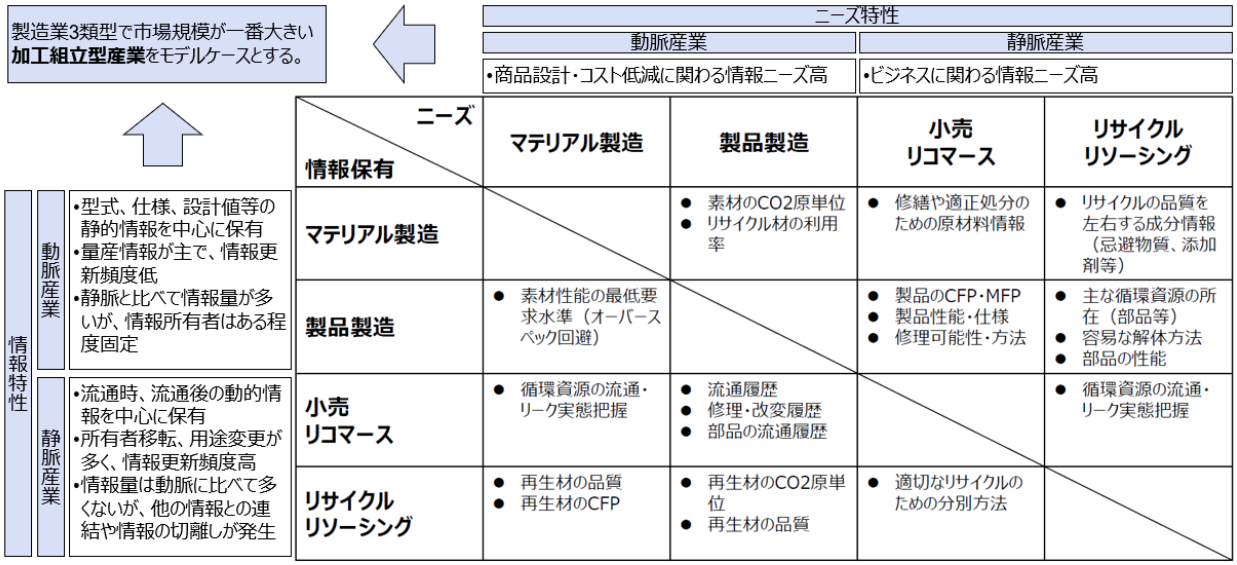


図 *1-2*

出典：令和５年３月 経済産業省 産業技術環境局「成長志向型の資源自立経済戦略（参考資料）」を一部改変

1.2.3.2 資源循環モデル化対象選定理由

日本の製造業における加工組立型産業は、三大類型の中で出荷額の 60%を占めているため、他の類型や産業のベースとして考えられる。他産業への展開も見据えられるため、今回は加工組立型産業をモデル化の対象として選定する。また、基礎素材型産業からの材料供給も行われるため、製造業全体のカバー範囲は広いと思料している。

三大類型は以下に分類される。

- 基礎素材型産業：鉄鋼、化学、セメントなど、基礎的な素材を生産する産業
  例: 鉄鋼業、化学工業、石油製品製造業
- 加工組立型産業：自動車、電気機器、機械など、素材を加工し組み立てる産業
  例: 輸送用機械器具製造業、電気機械器具製造業、電子部品・デバイス・電子回路製造業、一般機械器具製造業、精密機械器具製造業

- 生活関連型産業：食品、衣料品、家具など、日常生活に密接に関連する製品を製造する産業
  例: 食料品製造業、繊維工業、家具製造業

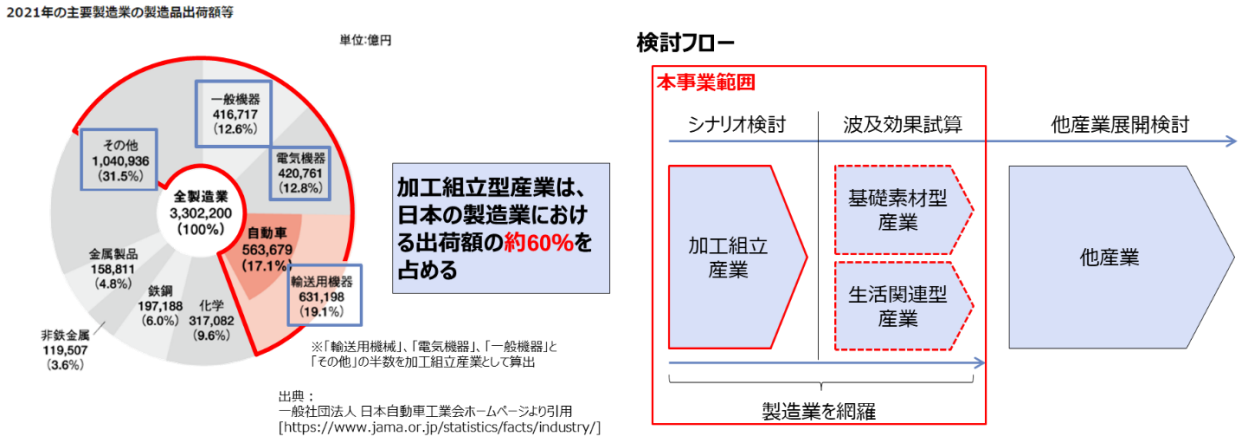


図 1-3

出典：「令和 3 年経済センサス-活動調査」の製造業に関する結果（概要版）より整理

1.3 資源循環モデルのあるべき姿

資源小国である日本において、サーキュラーエコノミー実現による資源循環を確立することは製造業の事業継続性を担保する上で急務であり、そのためには、製品の製造、流通、販売を行う「動脈産業」と、製品の回収、解体、再生を行う「静脈産業」との連携が不可欠であり、資源循環情報を効果的に共有・管理することが求められる。

具体的には動脈産業において、リユース（再使用）、リマニュファクチャリング（再製造）、リサイクル（再生）を前提とした環境配慮型製品の増産が求められる。また、製品が市場に流通した後は、静脈産業がこれを回収、解体して適切にリサイクルすることが重要である。リサイクルを効果的に行うためには、回収された製品や部品の使用履歴・修理履歴に基づいた適切な価値および性能評価、品質評価が重要である。

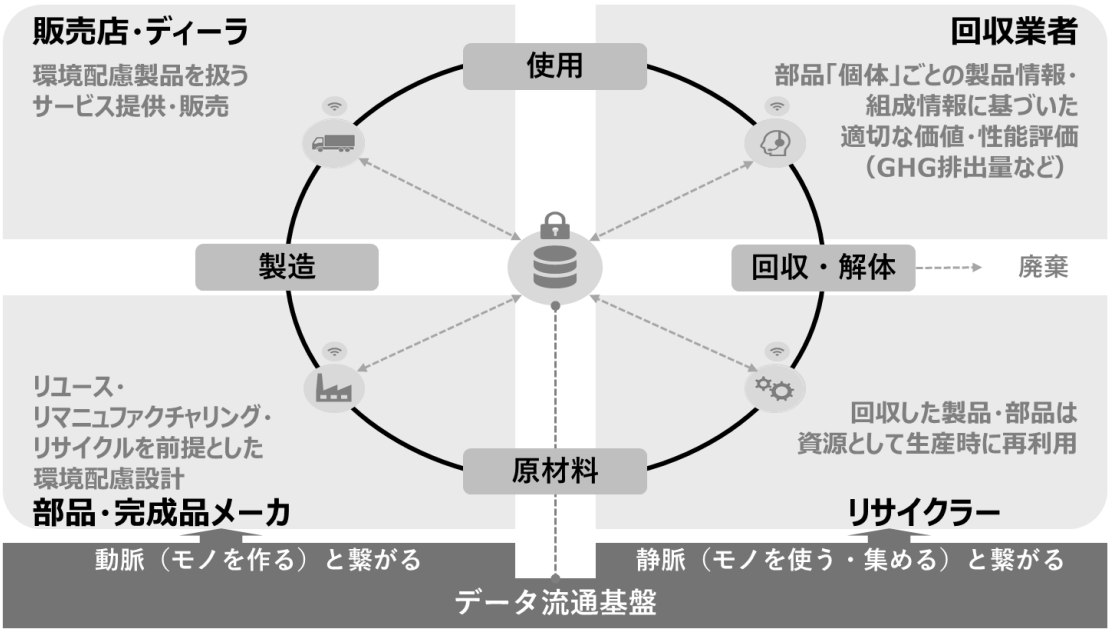


図 *1-4*

1.4 資源循環モデルの課題

本節では、資源循環モデルの課題について示す。

1.4.1 加工組立型産業全体における課題

加工組立型産業では、金属品・化学品等を多く消費しており、今後再生材確保が最重要課題となっている。動脈産業における製品製造プロセスでは、規制対象の原材料を使う際に、規制対応のために成分情報の事業者間伝達が行われる。そのため、バージン材同様、 再生材においても原料の成分等を明らかにすることで、再利用時に規制対応や品質保証を実施できることが期待される。こうした動静脈産業を統合したデータ流通およびデータ管理を実現することが CE 情報流通 PF に求められている。

一方で CE 情報流通 PF の実現に当たって大きく三つの課題が存在している。

- データの信頼性確保
- データの保管
- データ主権

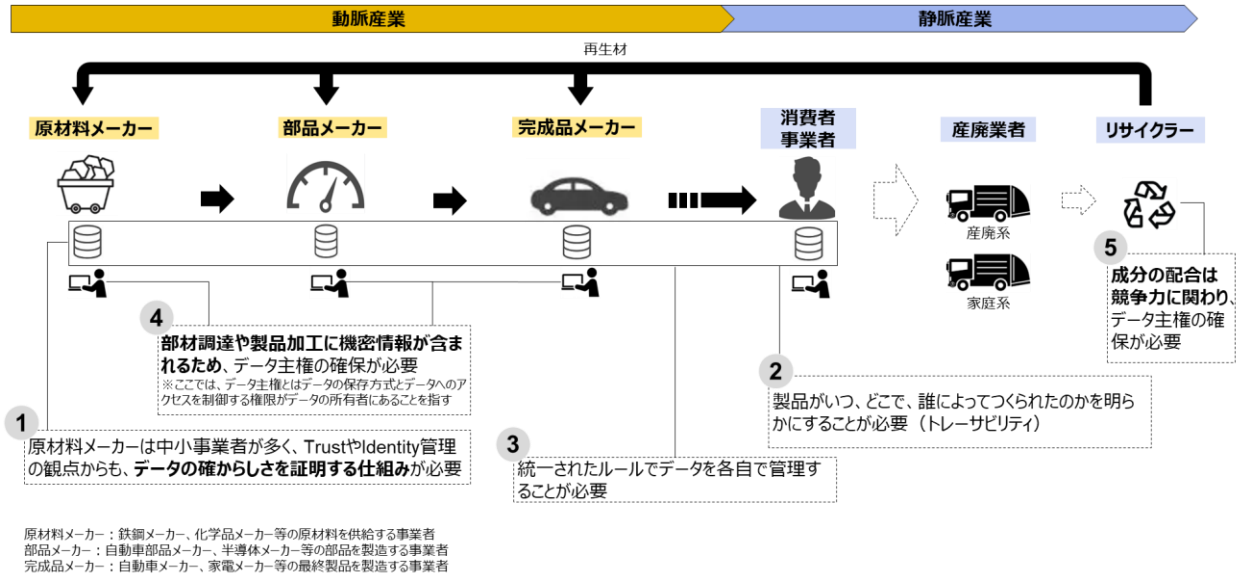


図 *1-5*

1.4.1.1 データの信頼性確保

上図の①、②が本課題に当たる項目となる。

CE 情報流通 PF には動静脈の様々な事業者が参加し、データを連携することが必要となる。再生材の更なる活用に向けては、法規要件や品質保証等を満たすデータの証拠能力の確保と責任追跡性を証明する仕組みやトレーサビリティの実現が動静脈産業を統合した形で必要となる。

1.4.1.2 データの保管

上図の③が本課題に当たる項目となる。

廃棄後の再利用を考慮する場合、製品保証期間を大きく超える長期間のデータ保管が必要となる。

データ保管に当たっては、各事業者間でデータの連携を容易に実施することを目的として、データフォーマットや連携の仕組み等のルールを統一することが求められる。

各事業者は部品の廃番等を実施することで、コスト増の抑制を図り、また長期間のデータライフサイクルの中では事業者の統廃合が発生するケースも想定されることから、静脈でのデータ利活用を考慮した長期間のデータ保管をどのようなスキームや仕組みで実現していくか検討をする必要がある。

1.4.1.3 データ主権

上図の④、⑤が本課題に当たる項目となる。

ここで開示が求められる製品の成分情報や部材の調達先は各事業者においては機密情報に当たることから、競合他社へ漏洩した場合、模倣品の製造が容易になるなど、競争上の不利益を与えるため、機密情報とし

て保護（トレードシークレットの保護）する必要がある。機密情報の取り扱いは契約等で定めることが一般的であるが、取り扱い方法が多岐にわたることから、原則的にはデータの所有者が開示先、開示対象、保管方法を規定するデータ主権の保護を前提として確保されることが主流である。

1.5 動脈産業の特徴

本節では、動脈産業の特徴について示す。

1.5.1 本節の目的

CE 情報流通 PF の全体像を定義するため、動脈産業、静脈産業のそれぞれの特徴や留意事項を整理する必要がある。本節では動脈産業の特徴と課題について整理する。

1.5.2 動脈産業の特徴

1.5.2.1 資源循環モデルにおける動脈産業のモノの流れ／情報の流れ

動脈産業におけるモノの流れは「原材料メーカー」→「部品メーカー」→「完成品メーカー」→「販売店」→「消費者」の流れとなっている。

完成品の品質や環境への配慮指標を管理するためには「原材料メーカー」～「完成品メーカー」までのモノの流れ／商流に基づき、情報連携が必要となる。

図 *1-6*

1.5.2.2 資源循環モデルにおける動脈産業の特徴／留意点

① 動脈産業では多数の部品／材料を組み合わせて最終完成品を製造する必要があるため、1 つの完成品に対して、多くのプレーヤが介在する。

② 資源循環モデルにおいてやり取りする情報には設計情報などの機密情報を含んでいるため、直接契約関係のある事業者へ必要な情報のみ開示可能であり、他のプレーヤへ知られることを防止する必要がある。

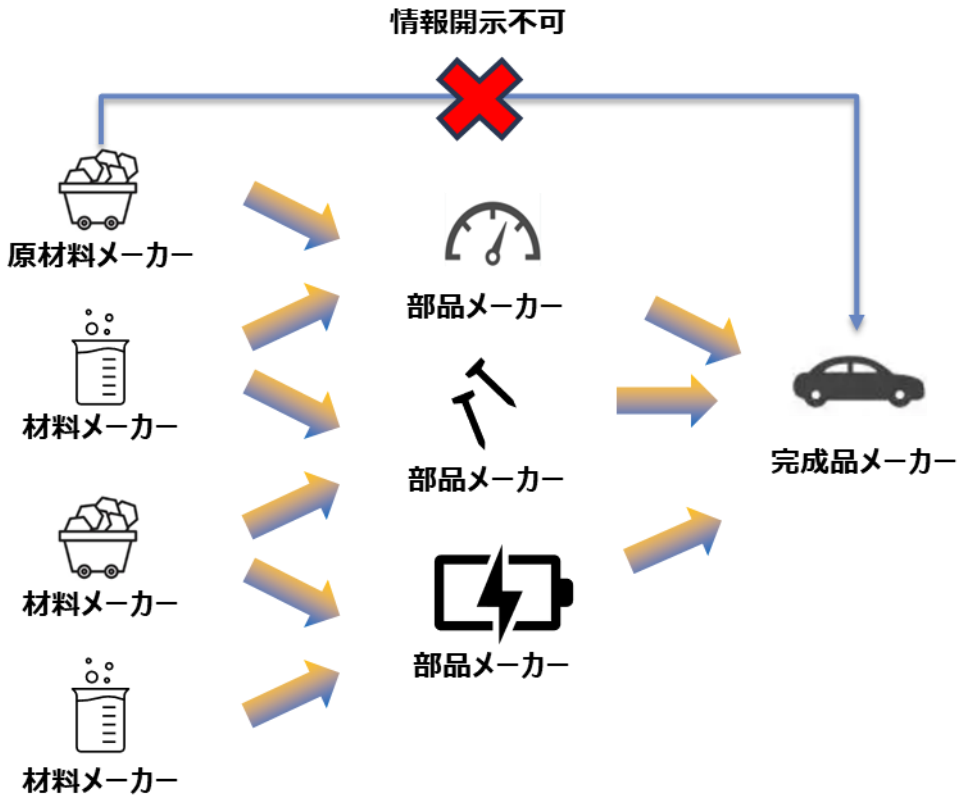


図 1-7

③ プレーヤには海外事業者／中小事業者など様々な事業者が存在する。多様な事業者が利用可能であり、多様な事業者の参画によりデータの信頼性を損なわない仕組みが必要となる。

④ リサイクルも含めた情報管理を行うことを考慮すると、データの長期保管が必要となる。

1.6 静脈産業の特徴

本節では、静脈産業の特徴について示す。

1.6.1 本節の目的

本節では静脈産業の特徴について、サプライチェーン上のモノと情報の流れを整理し、再資源化を促す上で現状と課題を記述する。

1.6.2 静脈産業の特徴

1.6.2.1 資源循環モデルにおける静脈産業のモノの流れ/情報の流れ

静脈産業において、モノは消費者を起点として「消費者」→「回収業者」→「リサイクラ―」の流れを辿る。動脈産業と異なり、モノは再資源化の過程で様々なルートから調達されるため、情報の流れは分断されることから、静脈産業に伝達される情報は限られ、効率的なリサイクルの実現には制約があるのが現状である。

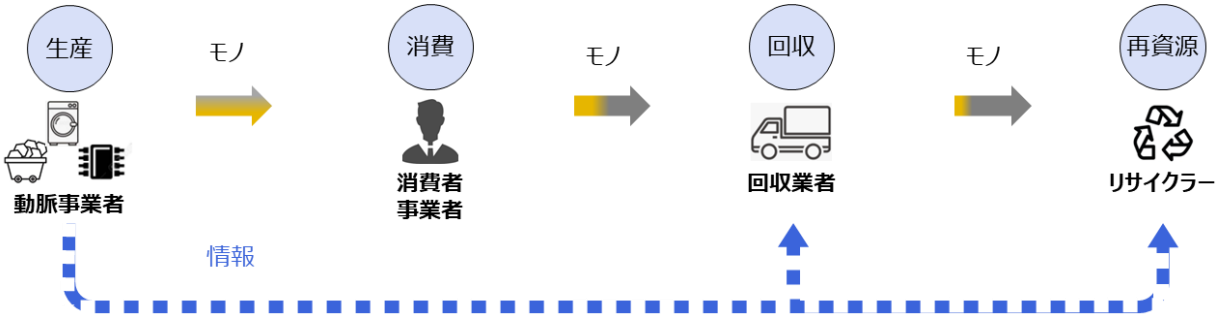


図 *1-8*

1.6.2.2 資源循環モデルにおける静脈産業の特徴/留意点

再資源化の概念として、クローズドリサイクルとオープンリサイクルの考え方がある。

クローズドリサイクルは、回収した自社の使用済み製品を、バージン材と同等の品質を持った材料として再生し、再び自社の材料として再利用する手法である。

一方、オープンリサイクルは、他社で回収・再資源化された材料を自社製品に再利用したり、回収した自社の使用済み製品を再資源化し、別の製品の材料として社外での利用を促したりする手法である。

循環型経済の社会実装では、再生材の品質確保という観点から、すり合わせや設計面での統制が実行しやすいクローズドループでのクローズドリサイクルが有利ではあるが、量的な確保に限界がある。オープンリサイクルでは再資源化の過程で性質の変化・劣化を伴うことから、製品要求に適合する品質を実現することに技術的に課題がある一方、幅広い再生材が利用可能なため、量的な確保において有利な面がある。品質保証にお

いて有利なクローズドループでのクローズドリサイクルを進めながら、品質確保を前提とした上でオープンループでのオープンリサイクルの活用可能性を検討するために、再資源化対象物に関するデータの信頼性※を確保することが重要となる。

※「1.4 資源循環モデルの課題」参照

今後世界規模で増加する再生材需要に対応するためには原材料の確保が必須となるが、品質の安定性や法規適合が要求される部品作りにはクローズドループの動静脈スキームを構築する一方で、汎用品向けの原材料においては、オープンループスキームから再生材を確保するなど、動静脈循環スキームの最適化が今後求められると考える。

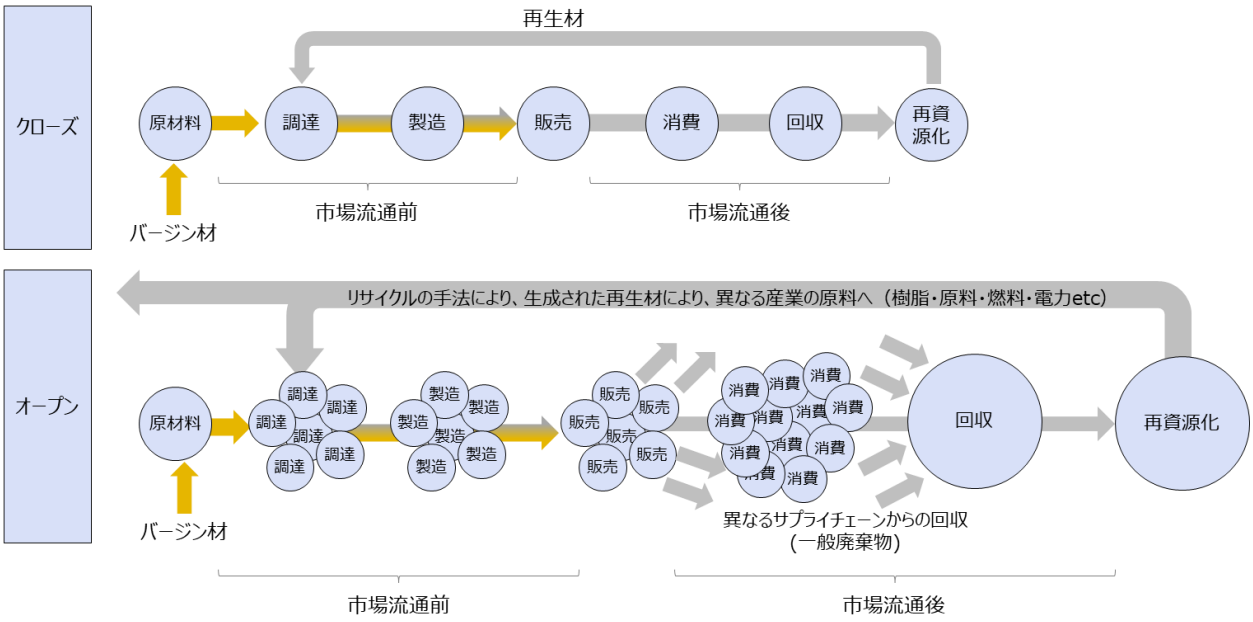


図 *1-9*

1.6.3 クローズドループ

クローズドループでは、信任された限られたプレーヤ間で供給網を構築し、市場に出た製品を完成品メーカー（あるいは部品メーカー）の要求に基づいて回収・解体し、リサイクラ―が要求スペックを満たす再生材を動脈産業に供給する。

動脈産業では、完成品メーカーの要求に従って、部品メーカーが再生材を活用し、法規に適合する部品を製造・販売する。従来の商流では、部品メーカーは原材料メーカーに対して、品質レベルと数量を仕様提示し、原料を仕入れるが、本スキームでは、部品メーカーが回収・解体事業者に対して回収依頼を出し、リサイクラ―に要求仕様を提示して、商社等を経由して再生材を確保しなければならない。

動脈産業から静脈産業への情報の流れは、回収したい製品によって変わる。例えば、自動車産業では、整備段階での後付け部品の取り付けや非純正部品を用いた改造等もあり、回収・解体事業者には、より広範な情報伝達が必要とされる。一方、家電製品等の場合は、型式等の指定によりスムーズな情報流通・物流が実現できているケースも存在する。

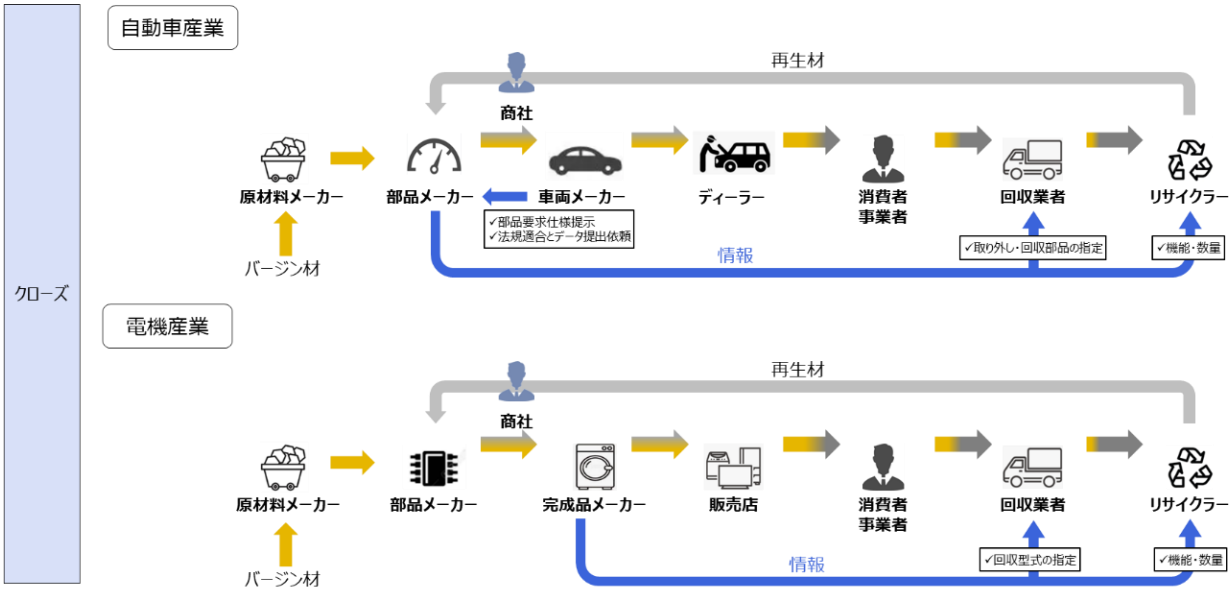


図 *1-10*

1.6.4 オープンループ

オープンループでは、広く市場で活用・廃棄されている製品を最終利用者が分別し、自治体や産業廃棄物事業者が選別、再資源化の判断を行う。有害物質等を含んでいる可能性の高い一部廃棄物については、排出事業者からの WDS により組成情報の取得も可能だが、その他の廃棄物に関しては、材料構成や材質情報が乏しく、各事業者のノウハウやシステムにより、再資源化処理を行い、品質よりもコストを優先するような大量消費製品向けの再生材として供給される。

JAN コード等が付与された市販品等については、メーカーが製品に貼付する法規適合ラベル等をもって最終消費者が回収事業者に情報伝搬を行う一方、海外等で生産された情報の無い製品や再資源化義務の無い製品は可燃物・不燃物として最終消費者によって分別されるため、静脈産業による再資源化の判断は、各事業者のノウハウや処理後の金銭的価値によって左右される。

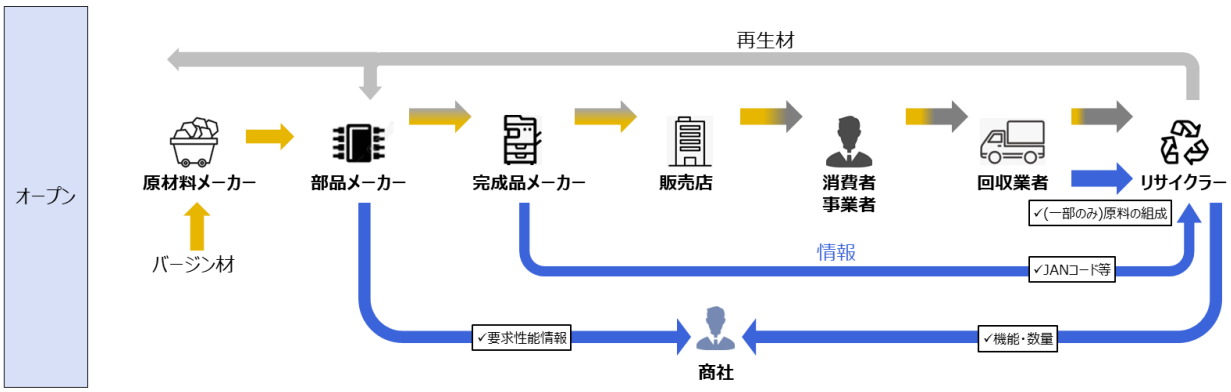


図 *1-11*

1.7 モデルに考慮すべき指標

本節では、加工組立型産業における資源循環モデルを検討するに当たって、考慮すべき指標類について示す。

前提として、資源循環モデルの設計においては、想定されるユースケースにおいて、流通する情報の内容や伝搬方法が規制に則した仕組みでなくてはならない。また、仕組みの導入にはサプライチェーン上の事業者に一定の負荷が発生するため、より多くの事業者に参画を促すために、モデルを活用し動静脈の連携を加速させることで生み出される価値を検討し、仕組みに反映すべきものと考える。

1.7.1 規制・標準化類

これまでも、動脈産業を中心とした規制・標準規格は存在し、製造プロセスにおいて原材料は厳格に管理されているが、サーキュラーエコノミーの時代には、その管理範囲が静脈産業まで拡大され、再び動脈産業に戻ってくる循環プロセスの中で管理を行う必要がある。

特に再生材の管理が追加されると、動静脈産業に大きな影響を与えると推察される。将来的に再生材は、前述したオープンループのスキームで製造された原料が広く流通すると見込まれるが、オープンループスキームでは、その過程においてコンタミネーションが発生する可能性がある。そのため、動静脈産業プレーヤは、規制・標準規格を正確に理解し、遵守することを求められる。

- 規制類

  環境負荷に関する国際的な規制としては、使用済みの自動車から出る廃棄物の削減目的とした EU-ELV 指令や電気電子機器に特定の化学物質を使用することを制限した RoHS 指令が存在し、日本国

内においても、日本自動車工業会の自主規制や化学物質審査規制法といった法規で化学物質の使用が制限されている。これらの規制は、使用を制限する環境負荷物質の拡大や、より厳しい数値目標を求める方向にあり、今後の動静脈連携においては、正確な情報伝達を即座に対応することが求められる。

一例として、EU-自動車設計の循環性要件及び廃自動車管理に関する規則（案）では、規則施行後72ヶ月経過後から新車製造にリサイクル樹脂25%（うち1/4はELV由来）の利用義務化することが議論されている。規制対応には、各製造プロセスにおけるリサイクル樹脂の使用割合の把握や、使用割合の正確な計測方法をサプライチェーンの細部に浸透させる必要がある。

- 標準化類

電気電子業界における製品含有化学物質に関する情報伝達の国際規格としてIEC 62474があり、これをベースに、材料情報の開示について対象をEEE業界を超えるマルチセクターに拡大したIEC/ISO 82474のDual Logo規格発行が計画されており、再生材の使用率を入れることが議論されている模様。

1.7.2 価値測定

資源循環モデルがサプライチェーン上で活用されることで、生み出される価値を環境、経済、社会観点から考察し、その価値がどのような波及効果を生み出すのか考慮する必要がある。
例えば、環境価値は、再生材を原料とした二次製品の製造者のコスト負担が大きい可能性があり、製品の活用によって低減した環境負荷の受益者にも公平に負担を分配する仕組みが将来的に導入される可能性がある。経済価値は、需要と供給のバランスによって材料の調達コストが変動するが、静脈産業の成長によって将来的にサプライチェーンのパワーバランスを大きく変える可能性がある。社会的価値は、経済合理性のみで測ることが困難であり、公共の利益に関わる価値である。経済安全保障推進法では、早期に法制化が必要な4分野を定め、重要物資のサプライチェーン強化をその1つに挙げており、経済産業省をはじめとして各省庁で様々な取り組みが強化される可能性がある。

- 環境価値

環境負荷効果の削減分（バージン材由来の素材製造にかかるGHG排出量と、再生材の製造時にかかるGHG排出量との差分）を、再生材の利用側（再生材を原材料とした二次製品の製造者）だけでなく、リサイクル原料の供給側（一次製品を製造し廃棄物を出した排出者）にも計上できる方法として、CFF（Carbon Footprint Formula）を例示する。なお、削減効果の配分については、下表計算式のパラメータAにて割合を設定する。

【計算式】

対象	計算式
物質	$(1-R_1)E_V + R_1 \times \left(A \times E_{recycled} + (1-A)E_v \times \frac{Q_{Sin}}{Q_p}\right) + (1-A)R_2 \times \left(E_{recyclingEoL} - E^*_V \times \frac{Q_{Sout}}{Q_P}\right)$ バージン資源の投入による排出 リサイクル材の投入による排出 マテリアルリサイクル・部品や製品のリユースプロセスによる排出から、回避されたバージン資源投入による削減効果を引いた排出

図 *1-12*

【パラメータ】

表 *1-1*

パラメータ	説明	
A	配分係数	リサイクル材の環境負荷及びその削減効果を供給者と需要者に配分する際の配分係数。0.2～0.8 の値を取り、0.5 よりも小さい値の場合はリサイクル材の需要量が供給量を上回るケースを、また大きい場合は供給量が需要量を上回るケースを指す。（例えば、金属では 0.2、プラスチックでは 0.5、繊維では 0.8 などとなっている。）
B		エネルギー回収の環境負荷及びその削減効果を供給者と需要者に配分する際の配分係数。環境フットプリントの枠組みにおいては常に 0 が適用される。
Q_{Sin}	品質	原材料調達段階におけるリサイクル材の品質を係数化したもの。
Q_{Sout}		使用後処理段階におけるリサイクル材の品質を係数化したもの。
Qp		バージン材の品質を係数化したもの。
R_1	割合	原材料調達段階におけるリサイクル材の投入割合。
R_2		使用後処理段階において材料がリサイクルされる割合を表し、当該の材料の回収率とリサイクル材の生成プロセスにおける歩留の双方を含む。
R_3		使用後処理段階において材料がエネルギー回収される割合。
$E_{recycled}$	環境負荷量	原材料調達段階において投入されるリサイクル材の生成プロセスに係る環境負荷量。回収、選別、輸送に係る環境負荷を含む。
$E_{recyclingEoL}$		使用後処理段階におけるリサイクル材の生成プロセスに係る環境負荷量。回収、選別、輸送に係る環境負荷を含む。
E_v		バージン材の調達に係る環境負荷量。
E^*_v		リサイクル材が代替すると考えられるバージン材の調達に係る環境負荷量。
E_{ER}		エネルギー回収プロセスに係る環境負荷量。
$E_{SE,heat}$ $E_{SE,elec}$		回収エネルギーが代替すると考えられるエネルギー（熱、電力）の供給に係る環境負荷量。
E_D		
$X_{ER,heat}$ $X_{ER,elec}$	エネルギー回収プロセスの効率（熱、電力）。	
LHV	エネルギー回収プロセスにおける材料の低位発熱量。	

出典:

令和４年度エネルギー需給構造高度化対策に関する調査等委託費

カーボン経済産業省ニュートラルと整合的な循環経済型のビジネスモデルへの移行に向けた課題等に関する調査分析調査報告書

より転用

なお、EU の Environmental Footprint methods では、製品（商品やサービス）、および組織の環境パフォーマンスを評価するためのライフサイクルアセスメント（LCA）に基づき、気候変動、水、空気、資源、土地利用、毒性など 16 の環境影響をカバーしている。特に、バッテリーのカーボンフットプリント計算には、CFF が使用される。この方法は、製品のライフサイクルの終わり（End-of-life）とリサイクルを考慮し、再生材の使用とリサイクル可能性を評価する。CFF は、入力側のリサイクル含有量と EOL でのリサイクル可能性の両方を考慮し、ライフサイクル段階間の材料品質の変化やリサイクル、およびエネルギー回収プロセスの割り当て係数を導入する。この方法は、EU の製品環境フットプリント（PEF）方法に基づいており、同様の製品や事業者の環境パフォーマンスを比較するための製品または組織固有の計算ルールが補完されている。

- 経済価値

希少資源・原料のリサイクルには、回収量の確保（リサイクル事業者に届かず海外へ流出）や技術開発に課題があり、市場価格次第ではリサイクルコストが新規採掘コストを上回る可能性がある。希少資源や原料は、バージン材・再生材での機能差は無いため、需要と供給のバランスによって、市場流通価格が大きく変動し、想定された商流にも影響を与える可能性がある。また、バージン材と再生材ではサプライチェーンが異なるため、まだ市場が成熟していない静脈産業では、バージン材製造以上のコストが発生することが懸念されるが、前述した環境価値との掛け合わせによって、経済価値が変わる可能性も秘めている。

【計算式】
バージン材の調達コスト（鉱石価格（CIF[1]）＋輸送費用―リサイクルの調達コスト（静脈物流費用＋中間処理費用）＋最終処分コスト削減効果（粉砕、償却、埋立））

（参考）調達コスト

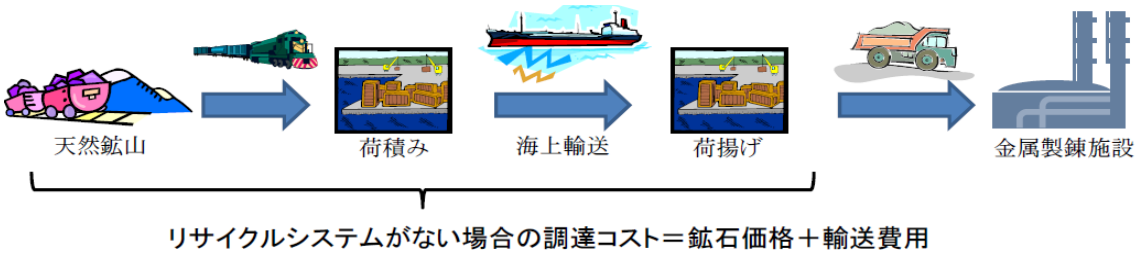


図 1-13

[1] CIF：輸出業者が貨物を荷揚げ地の港（輸入港）で荷揚げするまでの費用（輸出梱包費、輸出通関費、運賃、船荷保険料等）を負担し、荷揚げした以降の費用は輸入業者が負担するという取引条件。

図 1-14

（参考）最終処分コスト

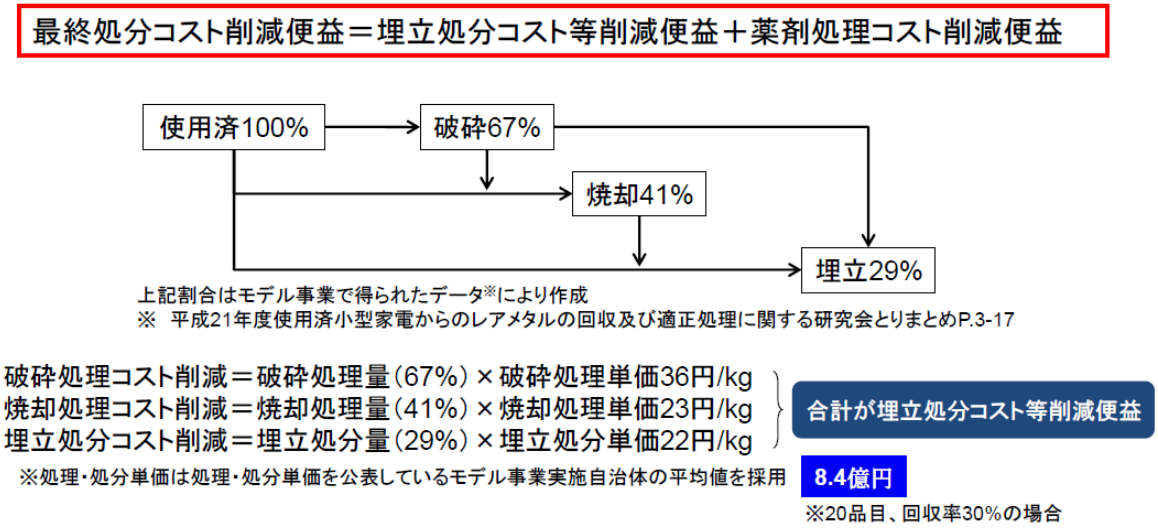


図 1-15

出典：
環境省リサイクルの費用対効果分析の考え方
[https://www.env.go.jp/council/former2013/03haiki/y0324-02/mat04.pdf]

- 社会価値

樹脂を含むあらゆる原料は、輸入によって国内産業に調達されているが、特に鉱物資源はその偏在性、希少性から安定供給の確保が課題となっている。

資源供給国との関係強化にとどまらず、サプライチェーンにおける動静脈産業連携を強化し、使用済み製品からの資源回収・リユース・リサイクルを加速させることは、資源の安定供給の確保に向けた取り組みとして、経済安全保障上の重要な意義を持つ。

近年の経済産業省における主要な資源回収にかかる取り組みを紹介する。

- 資源自立経済システム開発推進事業（23 年度当初：12.0 億円）
  排出・回収された廃製品に含まれる金属やプラスチック等の各種素材を、
  デジタル技術も活用しながら最大限利用可能とする基盤技術開発を実施

- 資源自律に向けた資源循環システム強靭化実証事業（22 年度補正：15.0 億円の内数）
  電気電子製品やバッテリー等を構成する金属類（レアメタル・レアアース等）について、自律型資源循環システムを構築するために必要となる資源循環のための技術開発や、実証に係る設備投資等への支援を実施経済環境変化に応じた重要物資サプライチェーン強靭化支援事業（永久磁石）（22 年度補正：253.0 億円）
  永久磁石サプライチェーンの多様化・強靭化を実現するため、省レアアース型永久磁石の開発や廃磁石からのレアアース原料リサイクル技術開発等への支援を実施

出典：
経済産業省 資源エネルギー省ウェブページ
第 3 部　第 1 章　第 3 節　鉱物資源の安定供給確保に不可欠なリサイクルの推進及び備蓄体制の強化等｜令和 5 年度エネルギーに関する年次報告（エネルギー白書 2024） HTML 版｜経済産業省・資源エネルギー庁
[https://www.enecho.meti.go.jp/about/whitepaper/2024/html/3-1-3.html]

（参考）政令で指定された特定重要物質

表 1-2

物質	現況
抗菌性物質製剤	注射用抗菌薬に多く用いられるβラクタム系抗菌薬は、その原材料のほぼ100%を海外に依存。
肥料	肥料の原料は、特定地域に資源が偏在しており、そのほとんどの供給を輸入に依存。 世界的な穀物需要の増加や紛争の発生等の国際情勢の変化により、原料の供給途絶リスクが顕在化
永久磁石	特にネオジム磁石およびサマリウムコバルト磁石は原材料(レアアース)を特定国へ依存
工業機械・産業用ロボット	日本メーカーは高い国際競争力を有し、安定供給を実現 DXやCN等のトレンドを受けて拡大するニーズに即した工作機械、産業用ロボット等の安定供給の確保が課題。
航空機の部品	基幹部品である、機体・エンジンの部素材について、 大型鋳造品は、日本を含む数か国のみが製造能力を有する。国際情勢により供給途絶のリスクあり、日本の供給力強化が不可欠。 CMCは、現行エンジンに使用されるCMCは海外に依存。 炭素繊維は、需要拡大への対応に課題。
半導体	日本の半導体産業の競争力が低下しており、多くを輸入。
蓄電池	車載用・定置用蓄電池について、日本のシェア低下(車載用2015年51.7%→2020年21.1%、定置用2016年27.4%→2020年5.4%)
クラウドプログラム	基盤クラウドプログラムの供給を海外に依存。
天然ガス	LNGを含む可燃性天然ガスの供給のほとんどを海外に依存
重要鉱物	多くの重要鉱物は埋蔵や生産国が特定国に偏在し、特定国からの輸入に依存
船舶の部品	日本・中国・韓国で世界の船舶の9割以上を建造、舶用機器の9割は国内調達

出典：
経済産業省 白書 2023 資料
第Ⅱ-1-2-2 表　政令で指定された特定重要物質 をより抜粋、一部変更
[https://www.meti.go.jp/report/tsuhaku2023/2023honbun/i2120000.html]

1.8 ツールチェーン整備

本節では、ツールチェーン整備の必要性について示す。

1.8.1 ツールチェーン整備の必要性

1 章でここまで述べてきた通り、動静脈産業においては様々な業種業態のプレーヤが存在している。各プレーヤにおける業務オペレーションは異なるため、それらを統一することは現実的ではない。

各プレーヤは業種業態、オペレーションにマッチしたアプリケーションを利用するため、それらのアプリケーション間で情報をチェーンのように連携できる仕組みを実現することが必要である。

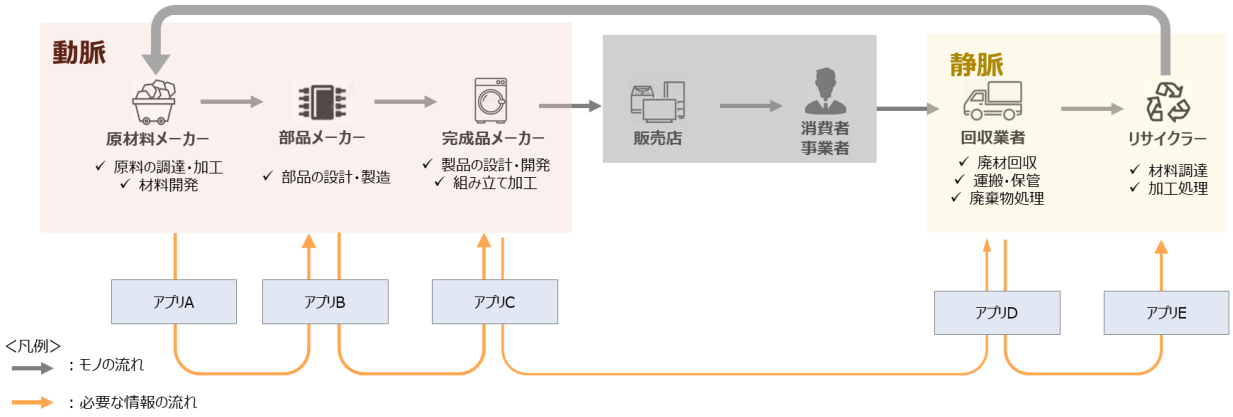


図 *1-16*

1.9 プラットフォーム全体像

本節では、プラットフォーム全体像について示す。

1.9.1 プラットフォームに求められる要件

プラットフォームに求められる要件は、「1.4 資源循環モデルの課題」で言及した資源循環モデルにおける課題を解決できることが求められる。

例えばトレードシークレットを保証しつつデータを流通させることが求められる。その一方で、サプライチェーンの多数の事業者が利用することによる性能面の課題への対応や、規制等によるデータ長期保管のためのシステム持続可能性の確保なども求められる。

資源循環モデルにおける課題と、それに対してプラットフォームに求められる要件を整理すると以下のようになる。

表 1-3

No.	課題（再掲）	内容	解決方法（業務要件）
1	データの信頼性確保	動静脈産業には様ーな事業者が参加することから、データの確からしさの証明が必要	・法規要件を満たす国際標準に準拠したデータフォーマットにて標準化を行う ・事業者間でデータ交換を行う際に法規要件を考慮した証拠能力を具備するトレーサビリティデータを記録する機能を具備する ・長期間でのデータ保管や法規要件への遵法性を保証する
2		証拠能力の確保を目的に、トレーサビリティ管理を実現することが必要	
3	データの保管	統一されたルールで保管し、再利用時にも利活用できる状態とする	
4		製品保証期間を大きく超えた長期間でのデータの保管が必要	
5	データ主権	部材調達や製品加工に競争力の源泉（トレードシークレット）があるため、保護が必要	・データの所有者が開示先、開示対象、保管方法を指定可能な機能を具備する ・攻撃への防御等含む、第三者への想定外の漏洩を防ぐために必要なセキュリティ対策を実施する
6		成分の配合は競争力（トレードシークレット）に関わり、保護が必要	

これらを実現するために求められるプラットフォーム像を本節では記述する。

1.9.2 プラットフォーム全体像

上述の通り、加工組立型産業における動静脈連携のプラットフォームには大きく 5 つの業務要件が存在する。

1. 国際標準に準拠したデータフォーマットの標準化
2. トレーサビリティ情報の記録・管理機能を具備することによる、証拠能力の確保
3. 想定外の第三者への情報漏洩やデータ改ざんを防ぐ等、必要なセキュリティ対策の具備
4. データ所有者が開示先、開示対象、保管方法を指定できる機能の具備による、データ主権の確保
5. 製品保証期間や事業者統廃合を考慮した、長期間のデータ保管

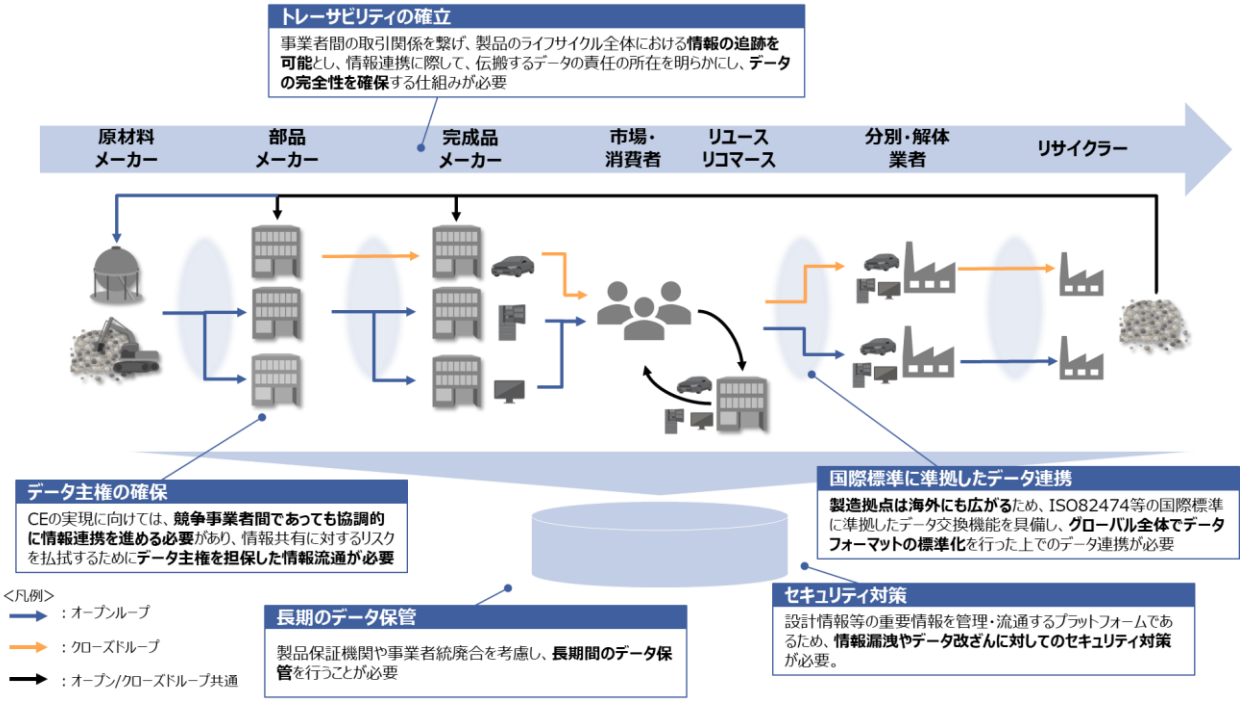


図 1-17

1.9.2.1 国際標準に準拠したデータフォーマットの標準化

製造拠点は海外にも広がることから、海外サプライヤの利用や、事業者間でやり取りするデータの信頼性確保、長期保管後のデータの利活用性を考慮し、法規要件へ対応できる ISO82474 等国際標準に準拠したデータ交換機能を具備すべきである。

1.9.2.2 トレーサビリティ情報の記録・管理機能を具備することによる、証拠能力の確保

トレードシークレット保護の観点から、サプライチェーン上に存在する事業者の全体像を把握可能な事業者は存在していない。上流から下流に順次バケツリレー方式でデータを交換し、完成品メーカーまで繋げることが必要となるが、データ交換都度に法規要件等を満たすトレーサビリティ情報の記録と管理を実施することにより、サプライチェーン全体で追跡可能なトレーサビリティ情報を管理する必要がある。

1.9.2.3 想定外の第三者への情報漏洩やデータ改ざんを防ぐ等、必要なセキュリティ対策の具備

事業者の設計情報と言った重要情報を管理・流通するプラットフォームであることから、サイバー攻撃などの対象となることを考慮し、情報漏洩やデータ改ざんに対して十分なセキュリティ対策を具備することが求められる。

1.9.2.4 データ所有者が開示先、開示対象、保管方法を指定できる機能の具備による、データ主権の確保

機密情報の保護方法や対象は各事業者の事情が色濃く反映されるため、多岐にわたる。こうしたことから、機密情報を保護するためには、原則として、データ所有者がデータの開示先、開示対象、保管方法を指定するデータ主権の確保が必要となる。トレードシークレットの保護が求められる機密情報を取り扱うことから、データ主権の確保を保証するデータ交換の機能を具備することが求められる。

1.9.2.5 製品保証期間や事業者統廃合を考慮した、長期間のデータ保管

製品保証期間や事業者統廃合も考慮し、再生材として利用される廃棄後のデータを活用することを見据えた長期のデータ保管が必要である。

2 ブロックチェーンの利点と課題

本章では、まず CE 情報流通 PF における BC の必要性について説明する。

次に、BC の一般的な利点と課題について示す。なお、課題については対策方法があり、その詳細については 4 章で示す。

2.1 ブロックチェーンについて

ブロックチェーンとは、ブロックと呼ばれる単位でデータを管理することに加え、それらを鎖（チェーン）のように連結してデータを保管する分散台帳技術を指す。[2]

技術的な詳細は 2.3 節以降で記載するが、本節では BC を活用したユースケースを示し、ビジネス的な視点でどのような利点があるかについて、下記引用資料の情報を基に示す。

出典：令和 5 年度　我が国におけるデジタル取引環境整備事業（ブロックチェーンに係る技術調査）より引用
[https://www.meti.go.jp/meti_lib/report/2023FY/000006.pdf]

BC には、主に図 2-1 のような使途がある。このうち、CE 情報流通 PF に求められる特性（耐改ざん性、透明性など）に近いユースケース（図中の赤枠）について、詳細を抜粋して示す。

[2] ブロックチェーンを含む分散台帳技術についての用語は ISO22739 で規定されている。また、国際標準化の取り組みとして ISO/TC307 Blockchain and electronic distributed ledger technologies (ブロックチェーンと電子分散台帳技術に係る専門委員会)(https://www.iso.org/committee/6266604.html)がある。

図 *2-1*

以下のユースケースでは、BC を用いることで「信頼性の高いデータ」を監査役無しで実現する。

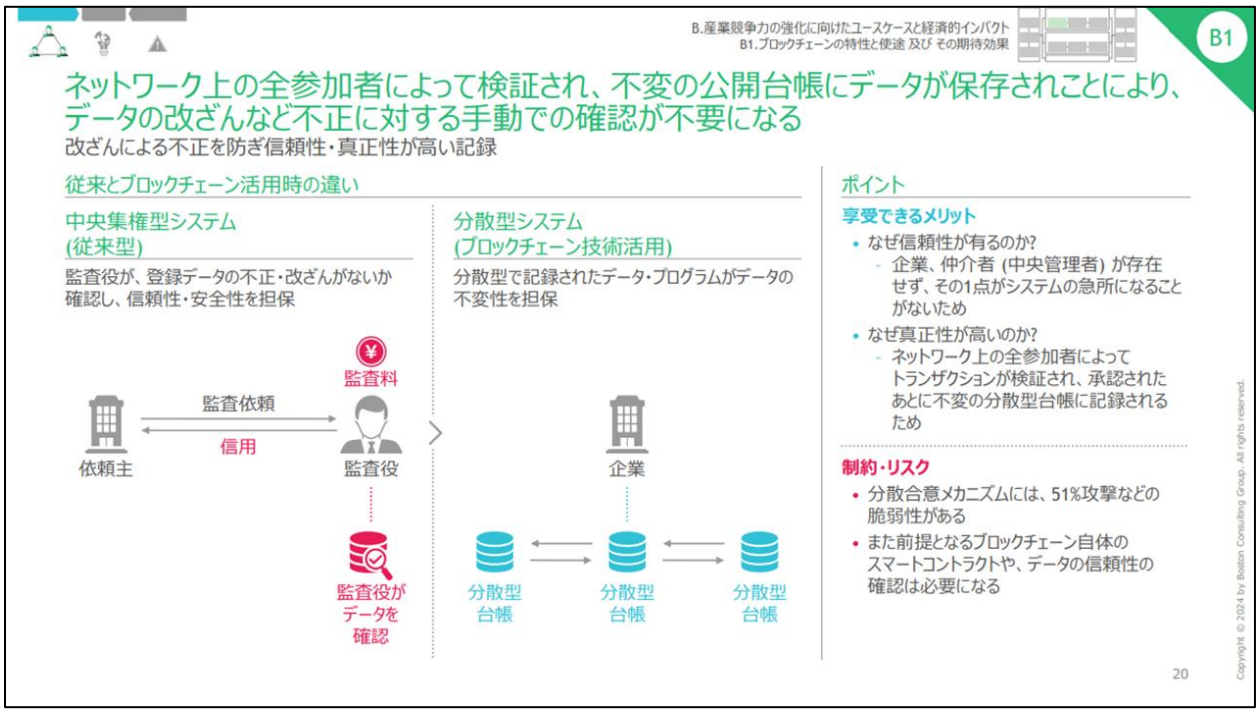


図 *2-2*

以下のユースケースでは、BC を用いることで「透明性・信頼性の高いトレーサビリティ」を実現する。

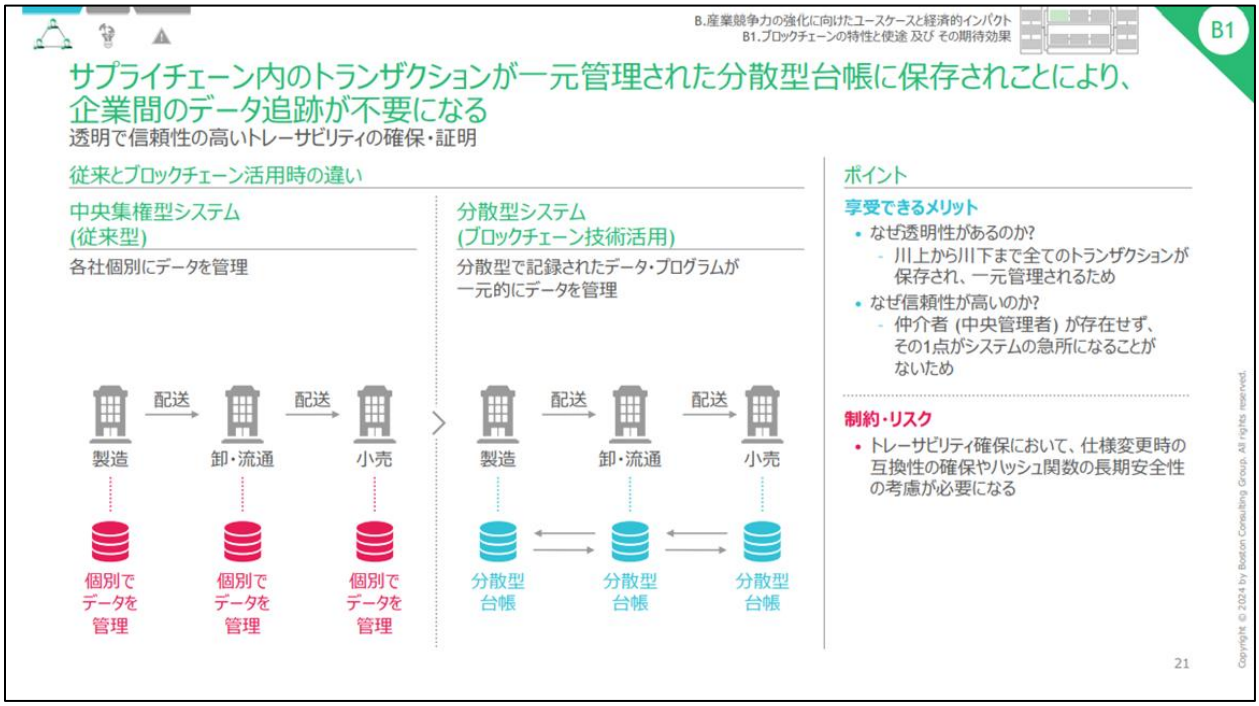


図 *2-3*

以上は BC の利点の一部であるが、本書では BC の特性（利点や課題）を整理した上で、CE 情報流通 PF へ活用すべきかどうか、また活用する場合はどこへどのように活用すべきかについて示す。

2.2 ブロックチェーン検討の必要性

本節では、BC とその他の技術を比較し、CE 情報流通 PF に BC を適用すべきかどうかについて整理する。

以降では、エンタープライズ領域においてデータ管理に用いられる主な技術と BC 技術について比較し、その上で BC を適用すべきかを検討する。

2.2.1 システム要件

1 章にて示した内容や公募[3]の募集要領を踏まえると、CE 情報流通 PF に対して求められるシステム要件として下記が挙げられる。

表 2-1

No.	システム要件	システム要件の内容
1	データ共有	• 事業者間において国際標準に準拠し、**データを共有**できること。
2	データの信頼性	• データの信頼性が確保されること。**耐改ざん性**や**否認防止性**、**可監査性**を有すること
3	処理ロジックの透明性と確実性	• データに対する処理ロジック**透明性**と**確実性**が確保されること。
4	通信先の信頼性	• 通信先の信頼性が確保されること。**通信先が確かにその事業者**であることが保証されること
5	データ主権の確保	• **データ所有者が認めた相手と情報に限りデータを開示されること** • **データ所有者の制御**にてデータ管理ができること（作成、変更、削除） • 運営者はデータ所有者の許諾なしに**データへのアクセスができない**こと • データ所有者が**データの保管場所を選択**できること • 各国の法規に従った配置場所を選択できること
6	システムの持続可能性	• データを**長期的に保持**する（データ長期保管） • システム運用が**長期的に持続可能**であること。
7	大量データ処理性能の確保	• **1万社規模のユーザ**からの要求を処理できること(利用規模は運用初期の想定) • 処理においては、レスポンス性よりも**確実性を重視**する。 • 海外拠点からの連携処理にも対応できること。
8	拡張処理性能の確保	• **参画事業者拡大に伴うシステム拡張**の要求を処理できること。

[3] 令和 5 年度補正資源自律経済確立に向けた産官学連携加速化事業委託費（サーキュラーエコノミー情報流通プラットフォームの調査・検証に関するオープンイノベーション事業）に係る委託先の公募について
（https://www.meti.go.jp/information/publicoffer/kobo/2024/k240920002.html）

2.2.2 主なデータ管理関連技術

エンタープライズ領域において、データ管理に用いられる主な技術（システム形態）として下記がある。本節では、これらを対象として CE 情報流通 PF に BC を適用すべきかどうかについて検討する。なお、BC は分散型システムと組み合わせて利用可能であり、このパターンについても比較する。

表 2-2

No.	技術	特徴
1	集中型システム	システムの一か所に集中してデータの配置・処理を行うシステム形態および関連技術
2	分散型システム	システムの各所に分散してデータの配置・処理を行うシステム形態および関連技術 配置・処理されるデータに対して、関係する二者間にて検証することが可能 また、BCを組み合わせることでBCに参加する複数企業間での相互検証が可能

上記の各技術について、以下にイメージ図を示す。

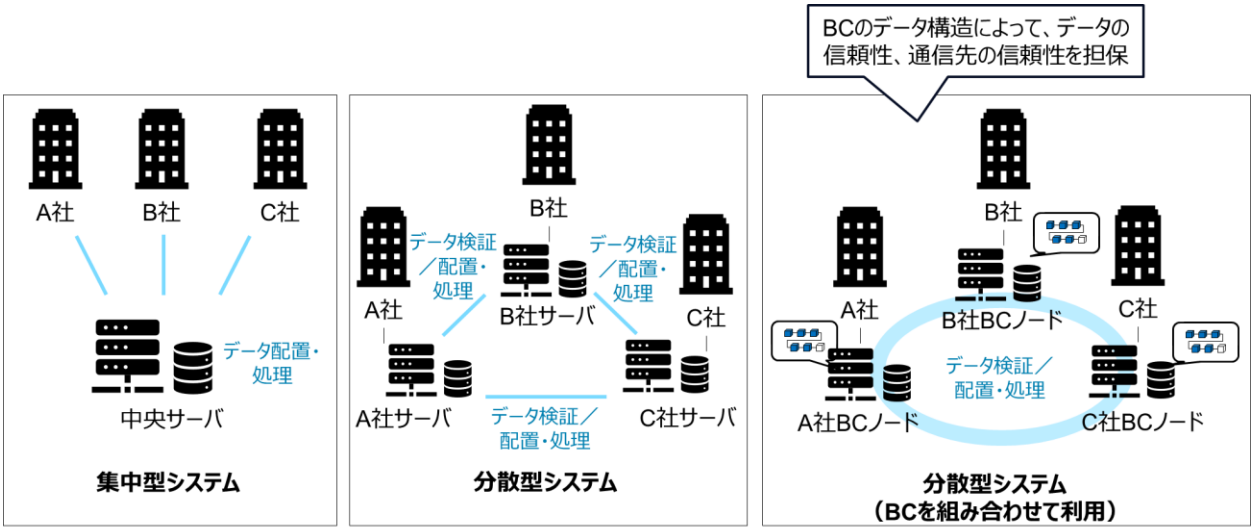


図 2-4

2.2.3 システム要件に対する技術比較

「2.2.1 システム要件」の要件について、「2.2.2 主なデータ管理関連技術」で示した技術を比較した結果として、**CE 情報流通 PF のシステム要件に対しては BC の適用が最適**である。その理由は次の通りである。

表 2-3

No.	システム要件	集中型システム	分散型システム	BC
1	データ共有	○	○	○
2	データの信頼性	△	△	○
3	処理ロジックの透明性と確実性	×	×	○
4	通信先の信頼性	△	△	○
5	データ主権の確保	×	○	○
6	システムの持続可能性	○	○	○
7	大量データ処理性能の確保	○	○	△
8	拡張処理性能の確保	△	○	△

【凡例】
○→単独の技術にて実現可能
△→他技術等の組み合わせにて実現可能
×→実現不可

- システム要件の No.5「データ主権の確保」について、中央サーバにデータは配置されてデータ所有者が保管場所を指定することができないため集中型システムがこの要件を実現することは不可能である。
- システム要件 No.3「処理ロジックの透明性と確実性」について、BC は後述の「2.3.3 スマートコントラクト（自動執行）」に示す通り、BC は格納するデータに対する処理ロジックの透明性を確保可能であるが、集中型システムおよび分散型システムについてはこれを実現することができない。
- システム要件の No.2「データの信頼性」および No.4「通信先の信頼性」について、BC を組み合わせることでより確実に実現可能である。
- システム要件のうち分散型システムと BC の組み合わせが他の技術より劣後するシステム要件（△の部分）もあるが、4 章にて示す対策適用により対応可能である。

2.3 技術的特性

BC は分散型のシステムであり、ノードと呼ばれるネットワーク上の複数のコンピュータが相互接続（P2P ネットワーク）し構成される。取引データは、暗号技術を用いて分散台帳に安全に記録・管理されるとともに、コンセンサスアルゴリズムと呼ばれる特定のルールに基づいて正当性が担保される。BC はビットコインの基盤として誕生したが、金融のユースケースを超えて、透明性のある情報共有という性質により企業間の情報伝達、サプライチェーンの領域における活用が期待されている。

BC 技術の一般的な技術特性を以降にて示す。

2.3.1 分散台帳

BC は、取引データを分散型の台帳データベースで管理する。ネットワーク内の複数のノードにより同じ台帳データが共有されていることで分散性を持つ。このため、ネットワーク内のノード（＝参加者）にデータを共有する機能を有しながら、システム全体の停止や、データ消失リスクを低減できる。

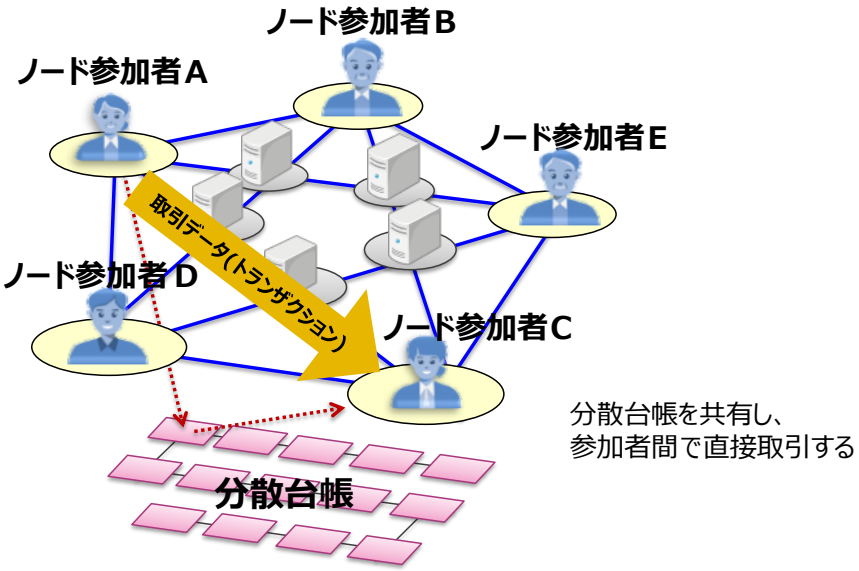


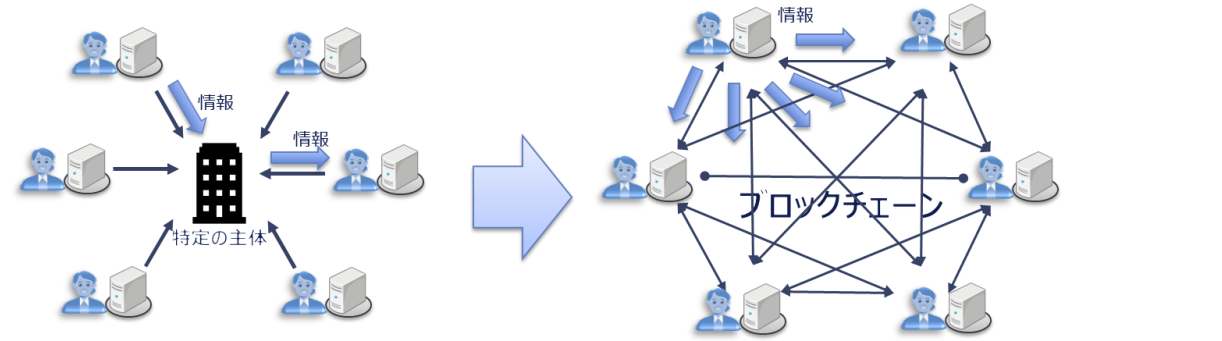
図 2-5

2.3.2 非中央集権性（コンセンサスアルゴリズム）

BC に参加するノードは、基本的に対等な関係でネットワークにアクセスでき、パブリック型 BC[4]の場合、中央サーバや管理サーバが存在しない。プライベート型 BC[4] では、非中央集権性よりも集中型管理とガバナンス機能に重点を置くものがある。この場合、一部のノードは管理者によって制御されるため、前述のような本来の非中央集権的 BC の利点は薄れる。

また、 参加ノード間では、コンセンサスアルゴリズムと呼ばれる合意形成のためのアルゴリズムを使用して、ネットワークを流れる取引情報のデータが正当であるかどうかを確認した上で、その取引データを分散台帳に記録する。

[4] パブリック型 BC とプライベート型 BC については「2.3.6 ブロックチェーンの分類」参照



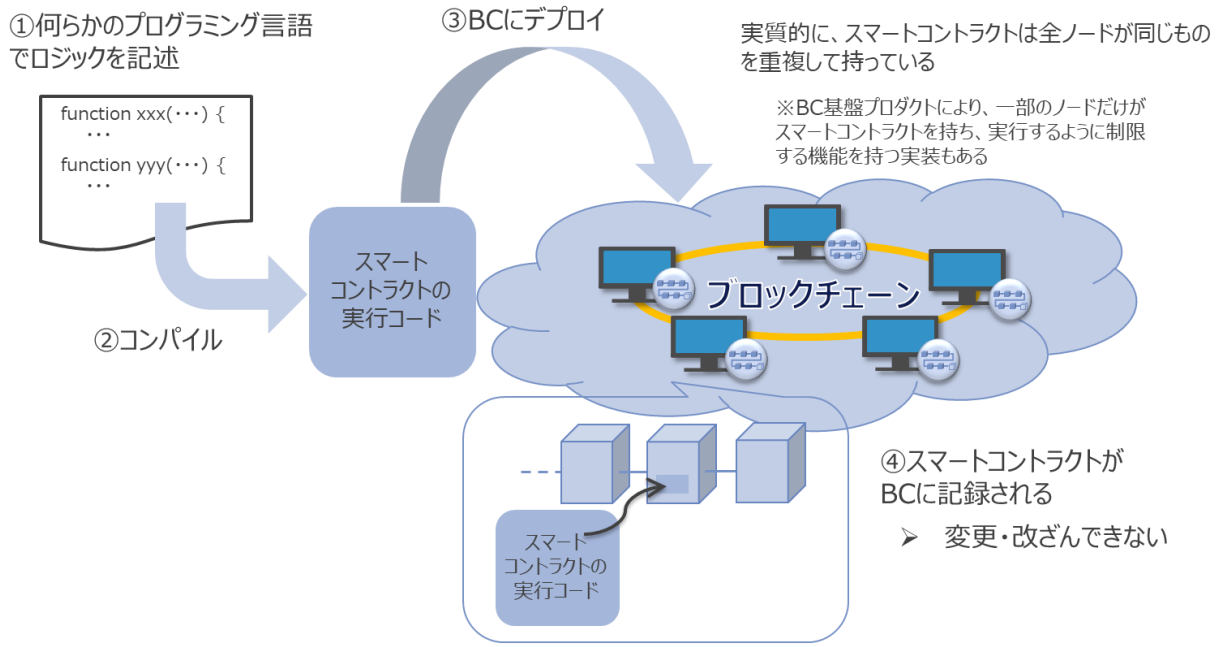
中央集権性：特定の主体が情報の流通を管理

非中央集権性：特定の主体を介さずに直接、情報を共有できる
コンセンサスアルゴリズム：取引情報が正当であるか確認して情報共有を行う

図 2-6

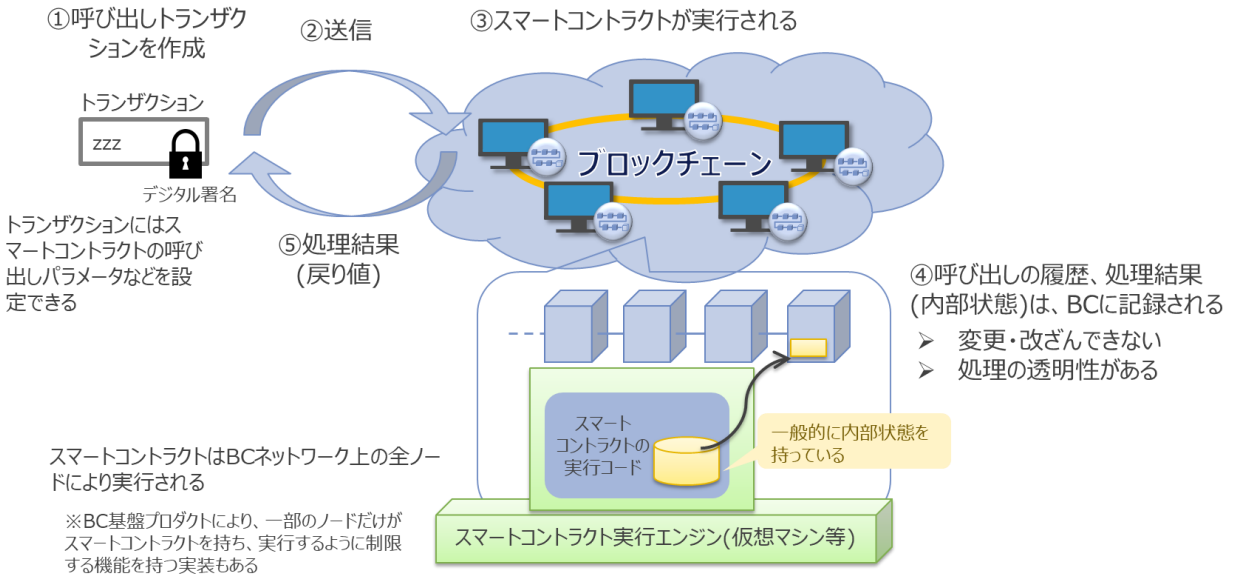
2.3.3 スマートコントラクト（自動執行）

スマートコントラクトは、BC 上で実行されるプログラムで、任意のロジックを記述できる。例えば、特定の条件が満たされた際に自動的に契約などの処理を行うことが可能である。スマートコントラクトのプログラムとデータは分散台帳上で共有されているが改ざんは困難であり、処理の透明性を確保し不正行為のリスクを低減できる。



スマートコントラクトの共有の例：プログラムとデータはBC上で共有されているので改ざんが困難

図 2-7



スマートコントラクトの実行の例：呼び出しの履歴・処理結果がBC上で共有されるので透明性がある

図 2-8

2.3.4 データ構造（ハッシュチェーン）

BC の取引データは、一定期間内に発生した他の取引データとともにまとめられ、ブロックと呼ばれるデータ構造内に格納される。この際、ブロックのハッシュ値を暗号学的ハッシュ関数により計算し、後続のブロックに埋め込むことにより、時系列的な連鎖構造（ハッシュチェーン）を作る。このハッシュ値により、各ブロックのデータは値の同一性について比較検証が可能となる。この仕組みを用いることにより、不正データ検知や改ざん検出などを容易に行えることから、BC の特徴である耐改ざん性が実現される。

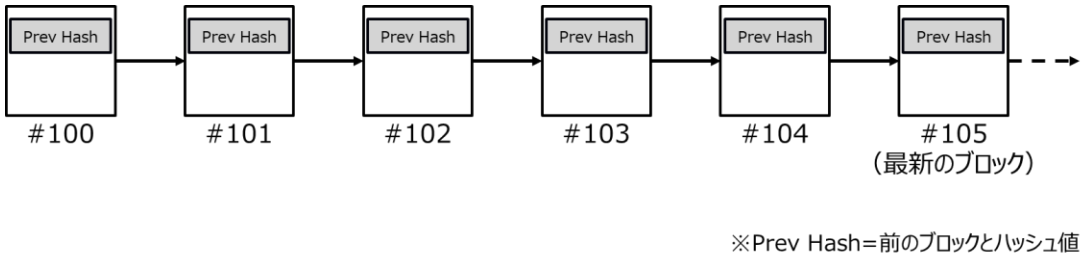


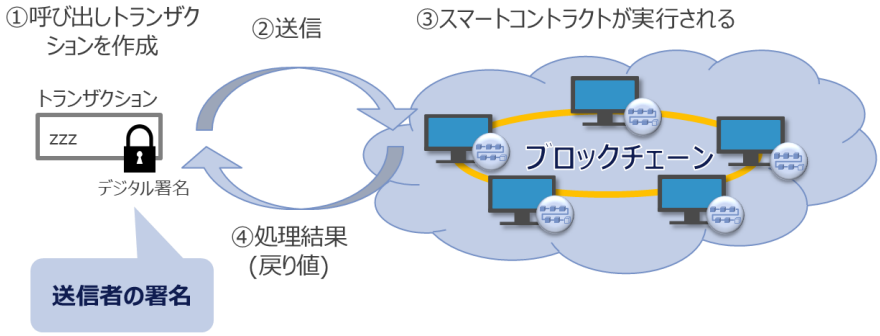
図 2-9

2.3.5 デジタル署名（トランザクション）

BC では、各トランザクションにデジタル署名を付与することにより、トランザクションの正当性を保証する。デジタル署名はトランザクションの送信者が保持する秘密鍵を用いて作成され、以下を実現する。

- 改ざん防止：デジタル署名の検証により、トランザクションのデータが改ざんされていないことが確認できる。

- なりすまし防止: デジタル署名は秘密鍵を持つユーザのみが作成できるため、秘密鍵の漏洩が無い限り、なりすましができない。



デジタル署名の例：スマートコントラクトの呼び出しトランザクションに対して送信者の署名をする

図 2-10

2.3.6 ブロックチェーンの分類

BC の利用モデルには以下の 2 つが存在する。以降の説明では、このモデルごとに説明している箇所があるため、本節にて各モデルの概要を示す。

- パブリック型：不特定多数が自由に参加できる。BC ネットワーク上のノードは基本的に対等な関係であり、参加者全員が共有台帳上のデータを参照できる。
- プライベート型：特定の関係者のみが参加できる。BC ネットワーク上には、管理ノードとそれ以外の一般ノードが存在し、管理ノードが合意形成やノードの参加等のネットワーク管理を担う。一般に、データ格納領域として、参加者全員が参照可能な共有台帳と、許可された参加者だけが参照可能なプライベートデータの 2 つを持つ。

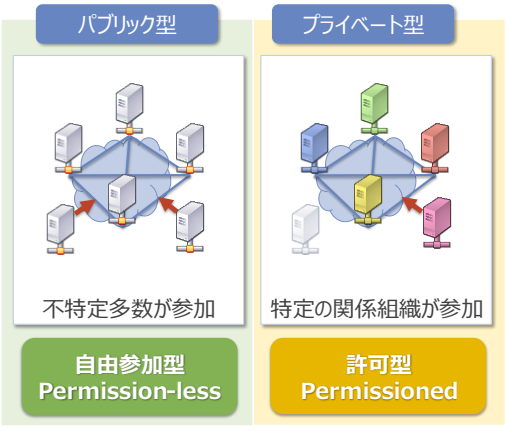


図 2-11

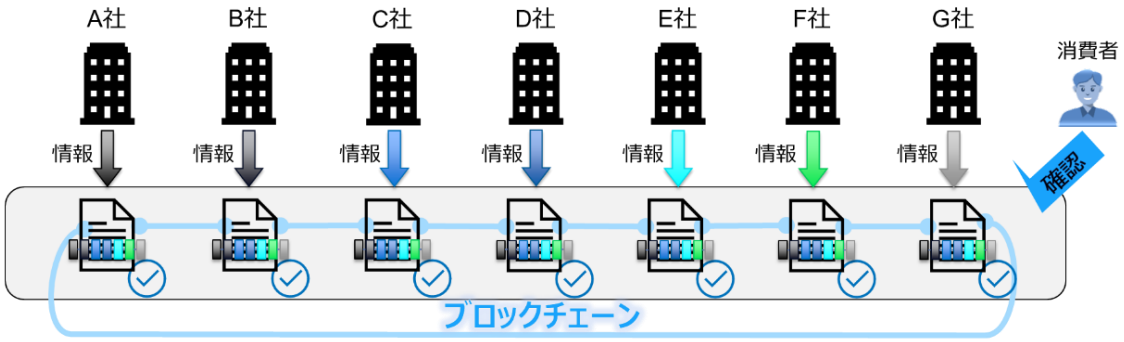
2.4 機能面における利点と課題

BC は前述の通りの技術特性から、従来型のクライアント・サーバ型システムなどと比較して機能的な利点と課題を持っている。以下に BC の機能的利点と機能的課題を記載する。

2.4.1 利点

2.4.1.1 情報の共有（透明性）

BC は、分散台帳によりネットワーク上のノードがデータを共有する。分散台帳には、過去の取引履歴を含む全データとスマートコントラクトに記述されたプログラムが格納されており、これらは誰でも内容を確認できる。このため、BC は従来型のシステムに比べて透明性の高いデータ共有を実現できる。



情報共有の例：原産地証明などに関する情報の透明性をBCで担保

図 2-12

2.4.1.2 公平性（分権）

パブリック型 BC はシステム的に中央管理サーバを必要とせず、システムを不特定多数が運営するノードを接続することで運用できる。ノードを運営している全ての参加者は対等な関係でパブリック型 BC のネットワークにアクセスできる。このように、パブリック型 BC では中央管理者を必要としないため、特定の組織の都合に左右されない分権的/非中央集権的な運営が可能である。

一方で、プライベート型 BC では、非中央集権性よりも集中型管理とガバナンス機能に重点を置くものがある。この場合、中央集権的な管理ノードをネットワーク上にいくつか配置することで参加者を管理し、合わせてデータ共有範囲も管理できる。このように、プライベート型 BC では、公平性を多少犠牲にすることで、確実なファイナリティの担保とコンプライアンスに重点を置いたシステムを実現できる。

2.4.1.3 コンセンサスによる不正防止（二重支払い防止）

「2.3.2 非中央集権性（コンセンサスアルゴリズム）」の技術特性により、分散台帳上の値は一意に確定され、同一のデータが共有された状態を確立する。合意形成に従わないデータはコンセンサスアルゴリズムにより不正とみなされ分散台帳には記録されないため、BC ではコンセンサスアルゴリズムに従う限りにおいて、二重支払いといった一意でないコピーデータの記録をはじめとした不正データを認めない。特に、ビザンチン耐性を持つコンセンサスアルゴリズムは 、アルゴリズムに従わないといった悪意のある攻撃に対しても高い耐性を有している。

2.4.1.4 効率性

「2.3.3 スマートコントラクト（自動執行）」の技術特性により、BC 上では処理ロジックを自動執行させることができる。これにより、業務自体の効率化に加え、BC の透明性の利点から、第三者による確認、監査といった業務の効率化を図れる。

2.4.2 課題

2.4.2.1 データ秘匿化

BC の分散台帳は BC ネットワーク内のノードに共有されているため、分散台帳上に格納するデータを適切に選定しなければ、取引に関わる個人情報や企業情報が第三者にアクセス可能になるリスクが存在する。

このような課題に対応するため、プライベート型 BC の一部には、特定の対象者のみでデータを共有できる機能を有しているものがある。BC でデータの秘匿化を実現する場合、このようなプライベート型 BC を利用することで、BC 上でも機密性の高い情報を扱うことが可能である 。

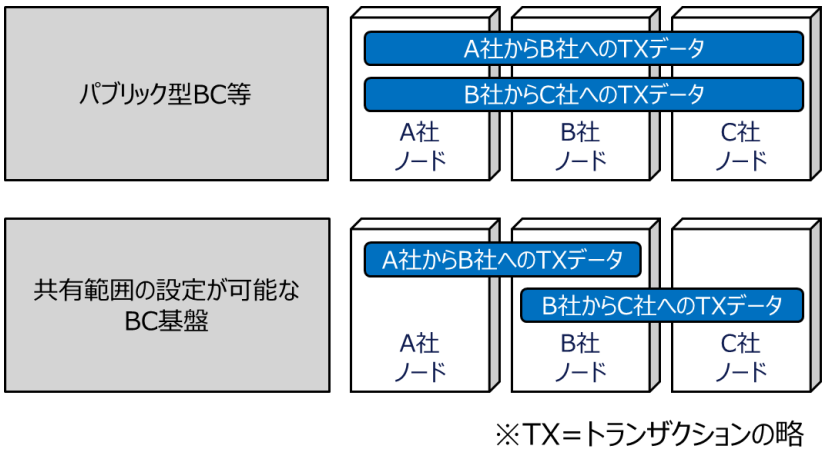
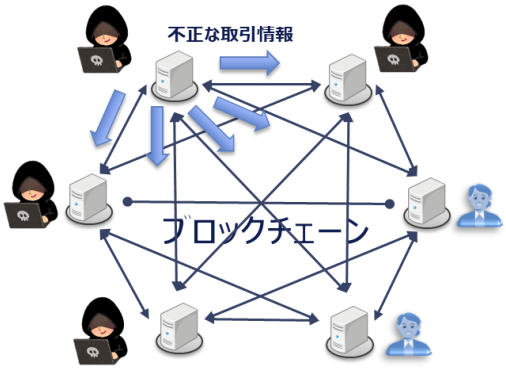


図 2-13

2.4.2.2 ネットワーク支配のリスク

BC の場合、非中央集権性という特性から、悪意のある主体が参加する場合を想定する必要がある。コンセンサスアルゴリズムによっては悪意のある主体が十分なリソースを持つことで合意形成をコントロールできる場合があり、ネットワークを支配し取引の改ざんや不正操作が可能となるリスクが存在する。

このような課題に対応するためには、ネットワークの分散度を高めることで単一の主体が支配するリスクを低減することが必要である。また、プライベート型においては、参加ノードの信頼性を BC システム外において確認することが求められる。



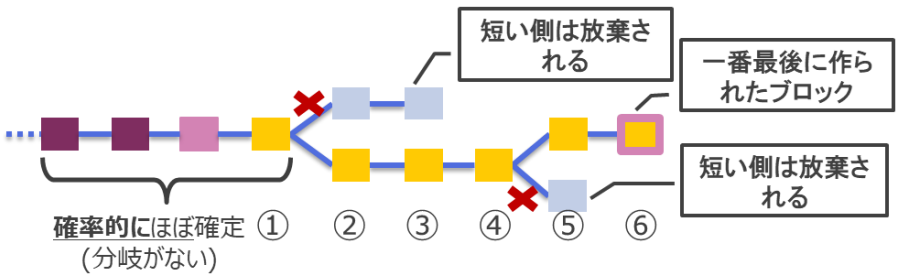
ネットワーク支配の例：悪意のある主体が十分な数のノードを乗っ取ると不正な取引が可能になる

図 2-14

2.4.2.3 ファイナリティ欠如

ファイナリティとは、一般的に「決済完了性」と呼ばれ、取引がある時点で確定し、取り消しできない状態になる性質を指す。

一部のコンセンサスアルゴリズムでは、合意形成でデータが一意の値に決まるまでに複数のブロック作成を要する場合がある（例えば、PoW）。このようなコンセンサスアルゴリズムを利用する場合、トランザクションがブロックに取り込まれて取引が確定したように見えても、合意形成で一意のデータに決まるまでの時間を経た結果、当該ブロックが廃棄される可能性がある。ブロックが廃棄された場合、トランザクションは未取引の状態となる。このような現象はファイナリティ欠如と呼ばれる。ファイナリティの有無はコンセンサスアルゴリズムに依存するため、ファイナリティが必須の場合、コンセンサスアルゴリズムの選定に注意を要する。



ファイナリティ欠如の例：ブロックが廃棄されるとそれに含まれるトランザクションは未取引の状態になる

図 2-15

2.5 非機能面における利点と課題

2.5.1 セキュリティ

BC における分散性、データ構造、デジタル署名、スマートコントラクトの技術的特性により、セキュリティ面で以下のような利点と課題が存在する。

2.5.1.1 利点

2.5.1.1.1 完全性（耐改ざん性）

BC は、データの改ざんを極めて困難にする特性を有し、高い耐改ざん性を持つ。これには以下の理由が挙げられる。

- 分散台帳

  「2.3.1 分散台帳」の技術特性により、データを改ざんするには、ネットワークに参加する大半のノードのデータを書き換える必要がある。現実的には、多数のノードが参加するネットワークでこれを実現することは極めて困難である。

- データ構造（ハッシュチェーン）

  「2.3.4 データ構造（ハッシュチェーン）」の技術特性により、一つのブロックのデータを改ざんするには、改ざん対象ブロックから現在に至るまでの全てのブロックを同時に改ざんしなければならない。膨大な計算リソースを要し、実質的に改ざんを不可能にしている。

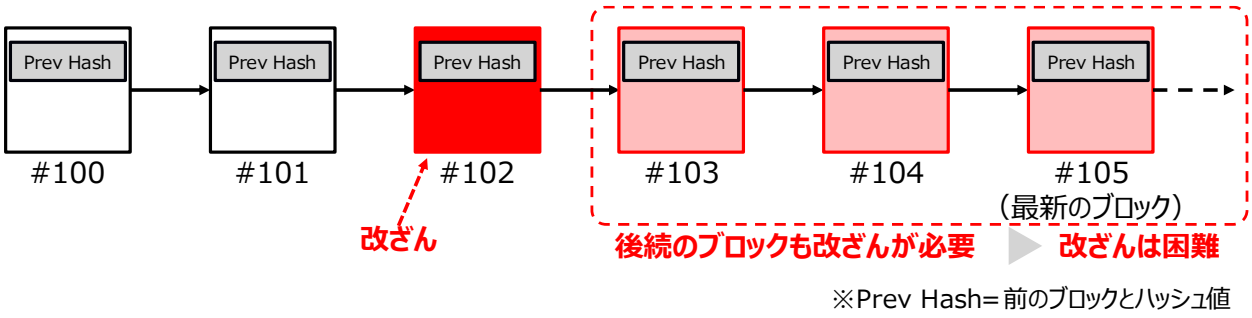


図 2-16

2.5.1.1.2 責任追跡性

BC 上のデータは高い耐改ざん性を持ち、一度記録されたデータは容易には改ざんできない。データを変更した際は、その変更履歴が記録されるため、高い責任追跡性を有する。また、ネットワーク参加者全員が BC 上のデータにアクセスできる高い透明性も備えている。この透明性により、データの確認と検証が容易となり高い責任追跡性を有している。

2.5.1.1.3 否認防止性

「2.3.5 デジタル署名（トランザクション）」の技術特性により、これにより発行者がその取引を実際に行ったことが証明される。さらに、前述の耐改ざん性、責任追跡性により否認防止性を確保している。

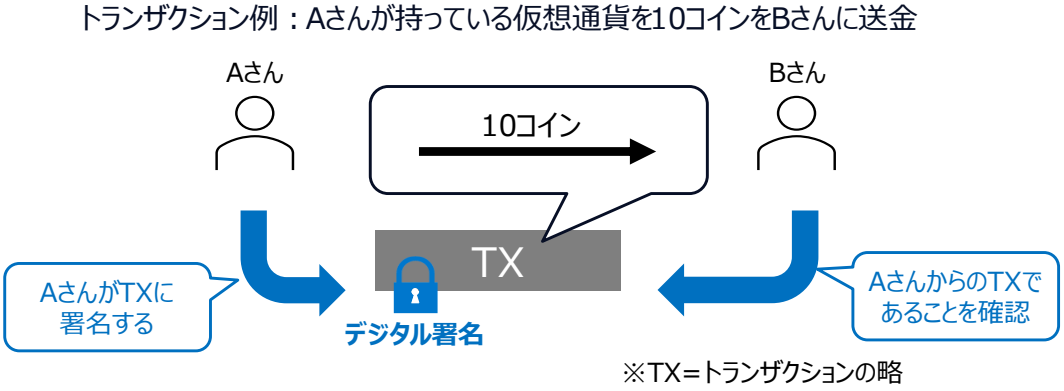


図 2-17

2.5.1.1.4 信頼性

「2.3.5 デジタル署名（トランザクション）」の技術特性により、全ての取引に対して発行者が証明されており、前述の否認防止性を有していることにより取引先の信頼性を担保できる。デジタル署名を使用することで、取引を行った主体が真正であることを確実に確認できるため、取引内容の正確性と信頼性が保証される。

2.5.1.2 課題

2.5.1.2.1 スマートコントラクトの脆弱性

BC は透明性が高く、BC 上にデプロイされたスマートコントラクトはネットワーク参加者全員に共有されるため、攻撃者に脆弱性が露呈しやすい。また、「2.3.1 分散台帳」の技術特性により、変更が容易ではないため、スマートコントラクトに脆弱性が発見された場合も迅速な対応が困難な場合がある。そのため、スマートコントラクトにバグや脆弱性が存在した場合、不正な操作を受けるリスクがある。

スマートコントラクトを変更可能なように設計し、定期的にセキュリティ監査を受けて事前にバグや脆弱性を除去することで、リスクを低減できる。

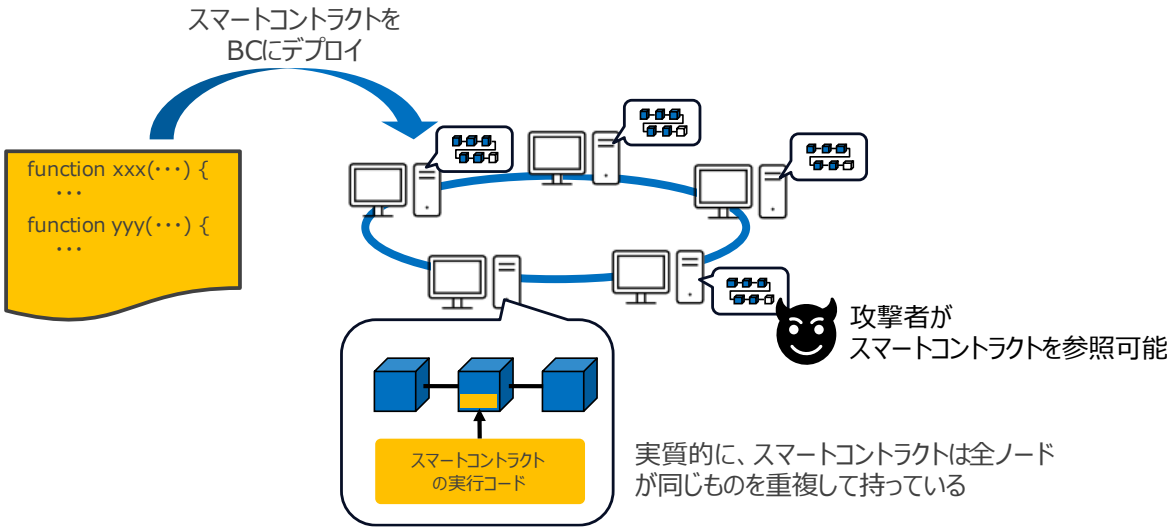


図 2-18

2.5.1.2.2 秘密鍵流出のリスク

BC ではユーザはトランザクションを発行する際に自身の秘密鍵を用いてトランザクションにデジタル署名を行う。そのため、秘密鍵が流出すると不正な取引が実行される可能性がある。

秘密鍵は外部からの接続が遮断され、通常のアクセスがあるアプリケーション側や基盤側とは異なる場所に配置することが重要である。これにより不正アクセスのリスクを低減できる。また、トランザクションの実行時に複数の秘密鍵を用いるマルチシグネチャを導入することも有効である。

2.5.1.2.3 共有済みデータの修正不可

BC では、データの改ざんを防ぎ、透明性と信頼性を確保する一方で、データの修正が困難である。そのため、誤ったデータや機密情報を含むデータを BC に記録してしまった場合でも、そのデータを削除することは難しい。

このリスクを低減するためには、データが BC に記録される前に、間違った入力を防ぐための仕組みを BC 外で整備することが重要である。具体的には、システム連携によるデータの自動入力や、入力内容を承認するためのワークフローの導入などが挙げられる。

2.5.2 性能・拡張性

BC では、分散性とデータ構造の技術的特性から性能・拡張性に課題が存在する。

2.5.2.1 利点

分散台帳、非中央集権性、データ構造という技術特性から、中央集権型システムと比較し、性能・拡張性の観点では優位性が認められない。

2.5.2.2 課題

2.5.2.2.1 性能（スループット、レイテンシ）問題

システムの性能評価おいて重要な指標であるスループットとレイテンシにおいて、BC システムは、中央集権型システムと比較して課題が存在する。

- スループット

  本ガイドラインでは、スループットを単位時間当たりに BC ネットワークにコミットされるトランザクション数と定義する。

  スループットの性能については、BC では一般的にトランザクションの検証に合意形成が必要であるため、中央集権型システムと比較してスループットは低くなる傾向がある。さらに、ブロックに保存できるデータ量の制約やブロック生成間隔によってもスループットには上限が存在する。

- レイテンシ

  本ガイドラインでは、クライアントがトランザクションを送信してから BC ネットワークでトランザクションが検証されコミットされるまでの時間と定義する。

  レイテンシの性能については、BC ではノードの分散性によるネットワーク遅延やトランザクションの検証時間により、一般的に従来の中央集権型システムと比較して高くなる。また、スループットを超えるトランザクションが発生した場合、トランザクションの待ち行列が発生し、レイテンシが急激に増加する。

これらの性能問題の対策としては、オンチェーンデータの選定や、ブロックサイズおよびブロック生成間隔の調整、迅速な合意形成が可能なコンセンサスアルゴリズムへの変更が挙げられる。また、オフチェーンスケーリングおよびサイドチェーンスケーリングの利用も有効である。

2.5.2.3 拡張性の課題

BC では、性能の向上を目的とした拡張性についての課題が存在する。システムの一般的な拡張方式として、スケールアウトとスケールアップの 2 つのパターンがある。それぞれのパターンにおける BC 固有の課題は以下の通りである。

- スケールアウト

  BC は各ノードが独立してデータを管理しているため、単純にノードを増やしてもネットワーク全体の処理能力は向上しない。むしろ、ノード増加に伴い分散性が高まり、合意形成のための通信量の増加やネットワーク遅延により、性能が低下する可能性がある。

- スケールアップ

  一つのノードの処理性能を向上させたとしても、他のノードの処理性能が低い場合、ネットワーク全体の処理性能は向上しない。ただし、特定のノードがボトルネックとなっている場合、そのノードの性能を向上させることで、全体の処理性能が改善する可能性はある。

これらの課題の対策としては、予め性能要件を満たすことが可能な BC 基盤の選定やコンセンサスアルゴリズムの選定が挙げられる。

2.5.2.4 履歴参照による性能劣化

BC では、ハッシュチェーンによってデータがハッシュ情報を用いて依存関係を持つ状態で記録されるため、トランザクション間に依存関係が生じることが一般的である。そのため、BC 上に大量のデータが蓄積されると、参照時に性能劣化を引き起こす可能性がある。

このような性能劣化を防ぐためには、参照頻度が高いデータはオフチェーンに格納することや、要件に合わせて過去データをアーカイブすることが考えられる。

2.5.3 可用性

BC は分散台帳という技術的特性により、可用性について独自の特徴を持つ。以下で可用性の利点と課題を示す。

2.5.3.1 利点

2.5.3.1.1 継続性/耐障害性

「2.3.1 分散台帳」の技術特性により、一部のノードが障害などにより停止しても、他のノードが正常に動作していれば処理が続行される。このため、BC ネットワーク全体として優れた継続性と耐障害性を持つ。

例えば、イーサリアムなどのパブリック型 BC では、数千ものノードが世界中に分散してデータを保存しており、ネットワーク全体で非常に高い継続性と耐障害性を確保している。しかし、機密性の高いデータのやり取りをするために、当事者のみでデータを共有し、保管する機能を持つ BC 基盤が存在する。そのような BC 基盤では、全てのデータがネットワーク全体に共有されるわけではないため、適切にノードを冗長化し、可用性を高める必要がある。

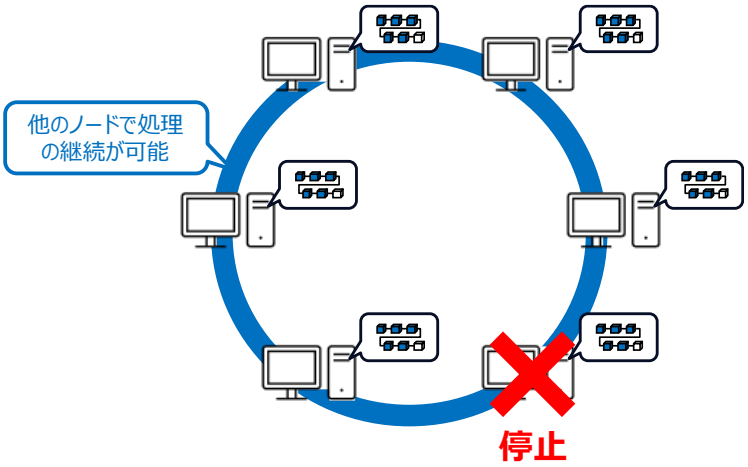


図 2-19

2.5.3.2 課題

2.5.3.2.1 トランザクション発行ノードの可用性確保

BC ネットワーク全体としては高い継続性と耐障害性を持っているが、BC を利用するアプリケーション側の視点にて可用性を考慮すると 、BC 上の各ノードの可用性も確保することが重要である。

BC システムにおいては、BC を利用するアプリケーション からリクエストを受け、BC に対してデータの更新やスマートコントラクトの実行などのトランザクションを発行するノードが存在する。

トランザクション発行ノードの可用性の確保は、BC システムにとって重要な課題である。トランザクション発行ノードが BC 上の処理の起点となるため、これが停止すると BC ネットワーク全体が稼働していても、停止したノードを利用するアプリケーションはサービスを停止するリスクがある。

特に、プライベート型チェーンを利用する場合、トランザクション発行ノードは各企業が保持することが多く、企業ごとにこのノードの可用性を確保することが求められる。

この課題の対策としては、トランザクション発行ノードの冗長性を高めることが重要である。複数のノードを運用し、フェイルオーバー機能を導入することで、単一障害点を排除することが効果的である。

2.5.3.2.2 ブロックチェーン特殊ノードの可用性確保

BC 基盤やコンセンサスアルゴリズムによっては、トランザクションの順序決定やその検証、参加者の管理、および証明書の管理を認証局の役割など、通常のノードとは異なる特別な役割を持つ BC 特殊ノードが存在する。この BC 特殊ノードは、BC ネットワーク全体における単一障害点となる可能性がある。そのため、BC 特殊ノードの冗長性を高めることが重要である。

2.5.3.2.3 コンセンサスの失敗による障害

BC においては、ノードの障害以外にも、ネットワーク断絶によるスプリットブレインなどによって適切にコンセンサスが取れず、BC システムが機能停止するケースが存在する。この場合、システム自体は稼働を続けているものの、ブロック生成ができなくなるなどの問題が発生する。このような事態に対しては、例えばシステムの一時停止を検討するなどの対応が重要である。

2.5.4 運用・保守性

BC は、運用・保守の観点で従来のクライアント・サーバ型システムとは異なる利点と課題を持つ。BC の導入検討では、以下に示す BC の運用・保守の利点と課題を踏まえることを推奨する。

2.5.4.1 利点

2.5.4.1.1 運用負荷軽減（バックアップ/リストア）

BC は、共有台帳により複数のノードで同一のデータを共有しているため、あるノードのデータが破損したとしても、他のノードのデータを利用できる。BC ネットワーク上に多数のノードが存在している場合、全てのノードのデータが同時に破損する可能性は事実上無く、破損したデータを復旧するためには、稼働中のノードから正しいデータをダウンロードできる。このため、BC の各ノードとしては、従来の中央サーバに比べてデータのバックアップ/リストアの観点で運用負荷を軽減できる可能性がある。

一方、プライベート型 BC では、データを共有せず、プライベート領域に秘匿化する機能を持つものがある。このようなプライベート機能を使う場合には、上記のような運用負荷の軽減という利点を享受できず、プライベート機能特有の課題が発生する。この点については、「2.5.4.2.2 運用オペレーションの複雑さ」で説明する。

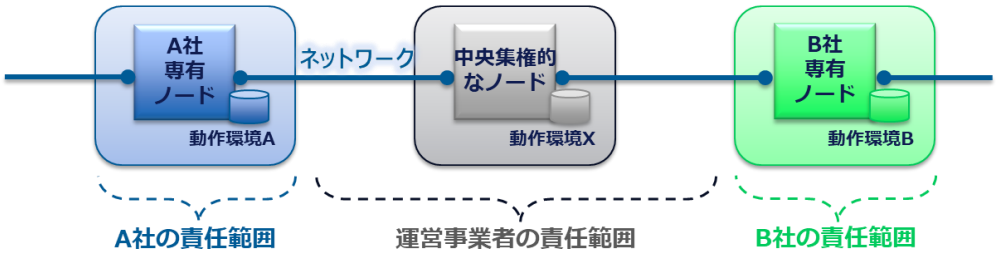
2.5.4.2 課題

2.5.4.2.1 責任所在

BC におけるシステムの責任所在は、自組織が持つノードの運用の観点と、多数のノード接続の集合である BC ネットワーク全体の運用の観点という 2 つの異なる観点がある。

パブリック型 BC の場合、自組織のノード運用に対しては責任所在があるものの、BC ネットワーク全体に対しては誰にも責任所在は無く、万一ネットワークが停止したとしても、責任追及先は無い。

一方で、プライベート型 BC の場合、管理ノードとそれ以外の一般ノードという区別を踏まえた責任所在の考慮が必要となる。まず、一般ノードにおいては、前述のパブリック型 BC と同様である。次に、管理ノードにおいては、BC ネットワークの運用との関係性を踏まえた考慮が必要となる。BC ネットワーク全体の保守・運用の責任を持つのは管理ノードの運用者である。管理ノードの運用者が単独ではなく、例えば複数の参加者で構成されるコンソーシアムがその運用主体となる場合、コンソーシアム内でネットワークの保守・運用の方針を決定し、安定運用に努める必要がある。このようなコンソーシアムをどのように運営するかは、BC 導入における課題となり、検討する必要がある。



責任所在の例：各事業者が管理する事業者専有ノードは各事業者が責任を負い、
運営事業者が管理するノードは運営事業者が責任を負う

図 2-20

2.5.4.2.2 運用オペレーションの複雑さ

BC の運用オペレーションに当たっては、BC の技術特性からくる固有の複雑さがある。複雑さが発生する要素を以下に示す。

- BC ネットワークの監視の複雑さ

  BC のシステム監視項目としては、自組織で持つノードを運用している場合、ノードのホストサーバのリソース監視がまず必要である。これは、従来型の中央サーバを運用している場合と同様である。BC では、このようなリソース監視以外にも次のような監視項目がある。

- P2P ネットワークで接続しているノードの構成
- ネットワークを流れるトランザクション数
- コンセンサスの状態
- スマートコントラクトのログ
- 秘密鍵へのアクセスログ

BC ネットワークは P2P ネットワークで構成され、ネットワーク上に多数のノードが配置される。このような多数のノードの稼働状況や、ネットワーク上を流れるトランザクション状況を統合監視するための設計や仕組み作りは一般に困難である。例えば、パブリック型 BC の場合、地理的にも全世界に点在する不特定多数の参加者が自由に参加離脱を繰り返しており、ノードを全て把握することは実質的に不可能である。

- プライベート型 BC における運用の複雑さ

パブリック型 BC とプライベート型 BC では、運用オペレーションの状況が異なる。パブリック型 BC のノード運用では、基本的にはネットワークへの参加は自由であり、ノードをどのようにネットワークに接続するかといった観点を中心とするだけであれば、運用の複雑さがあまり無いともいえる。

一方で、プライベート型 BC では状況はより複雑となる。プライベート型の BC の場合、管理ノードとそれ以外の一般ノードという種類の存在がある。管理ノードは、一般ノードの追加・離脱や、データの共有範囲といった管理を行うノードである。このような管理ノードの運用主体である場合、とりわけノード構成を大規模に展開したり、データの共有範囲をノード間の組み合わせパターンに応じて細かく設定したりする場合において、管理や運用、およびネットワークの監視は非常に複雑になる（前述した BC ネットワークの監視の複雑さも参照）。

また、プライベート型 BC では、データを共有せず、プライベート領域に秘匿化する機能を持つものがある。このようなプライベート機能を使う場合、プライベートデータの破損時に他のノードのデータを利用することはできない。従って、従来の中央集権型データベースシステムと同様な考え方で、自組織でのバックアップ/リストアの運用を考慮する必要があるとともに、共有台帳部とプライベート部のそれぞれの運用を考える必要があるなど、運用面で複雑化する可能性がある。

- BC ネットワークのバージョンアップ手順の複雑さ

BC ネットワークのバージョンアップを行う際、多数配置された各ノードに対してバージョンアップを実施する手順が必要となる。さらに、これらのノードが非中央集権的に運用されている場合、運用主体間での合意が必

要となり手順が複雑化する。仮にこの手順が容易である場合、BC ネットワークの完全性や信頼性等が低くなってしまう可能性がある。

- スマートコントラクト変更手順の複雑さ

  BC システムにおいて、使用しているスマートコントラクトの脆弱性が発見された場合など、スマートコントラクトの変更が必要な時がある。このスマートコントラクト変更は、BC ネットワークの全参加者が実行する処理ロジックの変更になるため、参加者間での合意を得た上で信頼できる主体が透明性のある手法でスマートコントラクト変更を実施する、といった複雑な手順が必要となる。仮にこの手順が容易である場合、スマートコントラクトの完全性や信頼性が低くなってしまう可能性がある。

2.5.5 移行性

BC は、移行性の観点で従来のクライアント・サーバ型システムとは異なる利点と課題を持つ。BC の導入検討では、以下に示す BC の移行性の利点と課題を踏まえることを推奨する。

2.5.5.1 ブロックチェーンの利点

移行性に関して、BC の利点は特に存在しない。

2.5.5.2 ブロックチェーンの課題

BC の移行性の観点では、異なる 2 つの BC 間での移行性と、従来のクライアント・サーバ型システムといった既存システムから BC への移行性という 2 つの検討課題がある。以下にそれぞれの課題を示す。

2.5.5.2.1 ブロックチェーン間での移行の困難さ

基本的に BC 間での移行を行うためのサポート機能は無く、データとスマートコントラクトの各観点で個別に移行を検討する必要がある。

- データの移行

  過去履歴を含む全データを移行先の BC に再投入するためのトランザクションを実行する必要がある。この際、データのフォーマット互換性が無い可能性が高く、移行先 BC 向けにフォーマット変換する独自プログラムが必要となる。また、過去履歴のデータ量によっては、全データの移行が困難（現実的な処理時間で行えないなど）、一部のデータ移行にとどまる可能性がある。

- スマートコントラクトの移行

  スマートコントラクトは、一部の例外（EVM 互換）を除き BC 間での互換性が無く、移行できない。このため、BC の移行ではスマートコントラクトのプログラム移植や、場合により新規開発が必要となる。

2.5.5.2.2 既存システムからブロックチェーンへの移行

BC と既存システムとは、データの取り扱いモデルが大きく異なるため、以下に示す課題が発生する可能性がある。

- BC の特性を考慮した登録データの峻別

  BC へのデータ移行の際、以下のような問題発生の可能性がある。

  - データ量が多く業務や性能に支障をきたす
  - データ検索の性能要求に応えられない
  - データの削除ができない
  - データの更新頻度が高く、処理が間に合わない

  これらを防ぐため、既存システムのデータのうち、まず、業務要求の観点で BC への登録が必要なデータを選定した上で、オフチェーンを活用することを考慮した設計方針を立てるなどのステップを踏むことを推奨する。

- データの登録手段

  BC システムへのデータ移行に当たっては、通常のシステムのようなストレージからのデータインポートではなくトランザクションの実行が必要となる。このため、データ移行用のトランザクション実行ツールなどの準備を検討する。

3 対象業務におけるブロックチェーン技術の適用範囲と利点・課題

本章では「1 章 本書において前提とする資源循環モデル」および、「2 章 ブロックチェーンの利点と課題」で論じた内容を用いて、CE 情報流通 PF において BC 技術の適用範囲とそれに伴う利点、課題を示す。

本章で論じる「適用範囲」は、本ガイドラインが「CE 情報流通 PF」を対象とし汎用的に活用できるものと位置付けることから、広義の適用範囲と定める。

- 広義の適用範囲 = BC の利点を活かせる要件/適用方針
- 狭義の適用範囲 = 機能およびデータ配置 （具体的な実装機能）

ガイドラインでの記載を参考に BC に実装する機能やデータの配置を検討できることを目的とする、

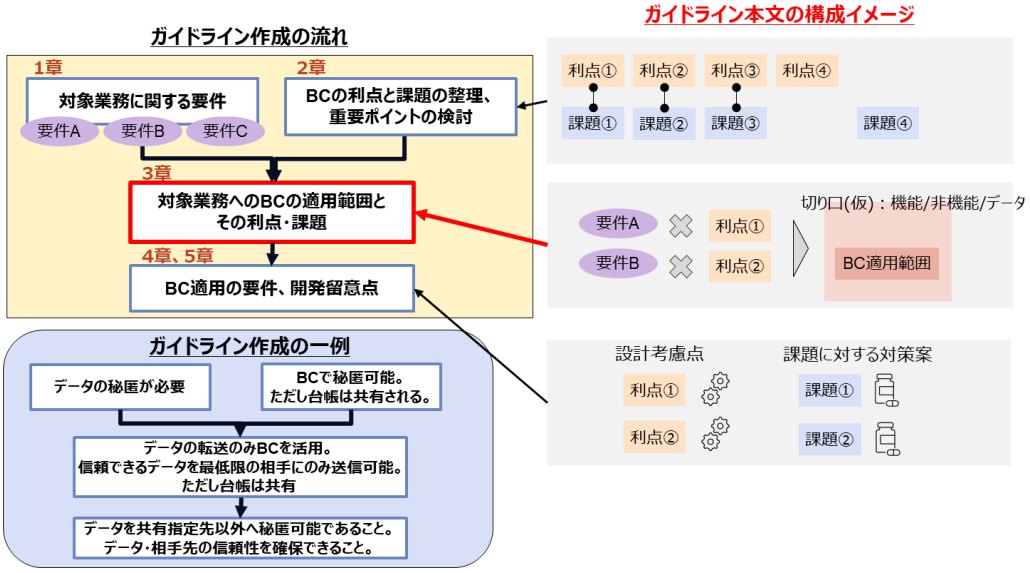


図 3-1

3.1 システムイメージ：全体像 / 適用範囲

BC は、従来のシステムにおけるデータベース等のデータ管理に関する各種要件や課題を全て充足するものではなく、BC の利点や課題を踏まえて最適な範囲へ適用し、その利点を最大限有効活用しつつ課題へ適切に対策を施すことが重要である。この BC 適用範囲を検討するに当たり、システム全体像においてどの範囲を検討対象としているかを明示する。

本ガイドラインにおける検討においては、「ウラノス・エコシステム」に準拠したアーキテクチャを基本としている。「ウラノス・エコシステム」に準拠したアーキテクチャは大きく 3 つのレイヤから成り立っている。詳細は下記の「ウラノス・エコススステム」のアーキテクチャガイドラインを参考にされたい。

出典：
サプライチェーン上のデータ連携の仕組み に関するガイドライン α 版（蓄電池 CFP・DD 関係）
[https://www.ipa.go.jp/digital/architecture/Individual-link/ps6vr7000001m4n6-att/guideline_for_datacooperation_in_BattCFPDD.pdf]

サプライチェーン上のデータ連携の仕組み に関するガイドライン β 版 （蓄電池 CFP・DD 関係）
[https://www.ipa.go.jp/digital/architecture/Individual-link/m42obm0000008rd4-att/guideline-for-datacooperation-in-BattCFPDD-beta.pdf]

- インダストリーサービス：個社・業界別の要件を実現する機能。競争領域
- トランザクションレイヤ、トラストレイヤ：データモデル管理や認証/認可などのデータ流通を担う機能。協調領域
- データレイヤ＋インダストリーサービス：トレーサビリティ管理やデータ主権確保など事業者間サプライチェーンの実現に必要な機能。協調領域

CE 情報流通 PF は、サーキュラーエコノミーにおける情報流通においてステークホルダ間での情報伝達の汎用的な仕組みの提供を目指すことから、「ウラノス・エコシステム」に準拠したアーキテクチャにおいて「データレイヤ＋インダストリーサービス」に位置付けられる。そのため、BC 適用範囲は「「データレイヤ＋インダストリーサービス」に要求される要件について、BC 技術に何を任せるか」ということを検討することとなる。

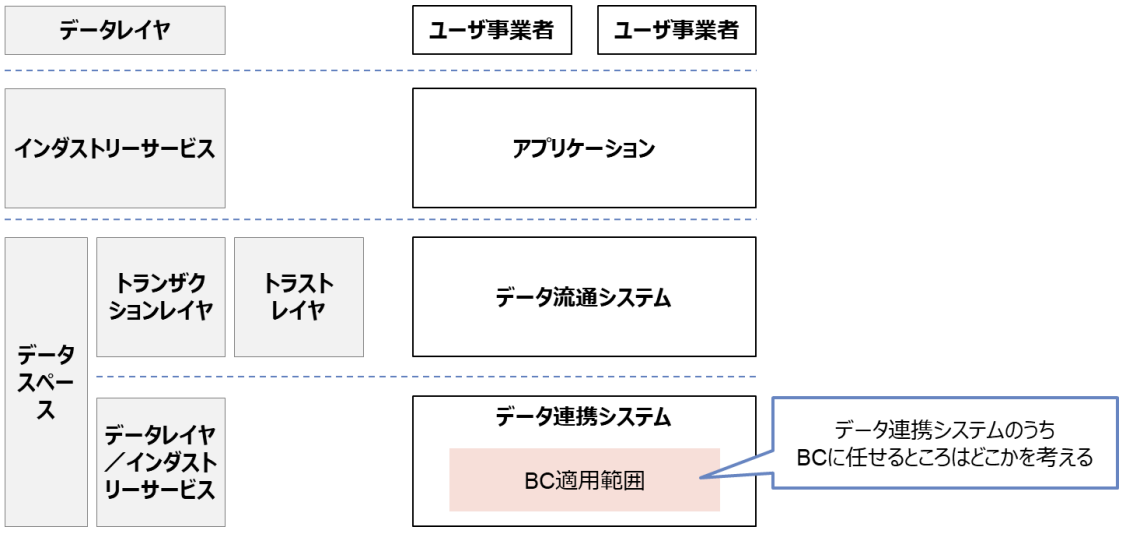


図 3-2

3.2 ブロックチェーン適用の理由・利点の検討

3.2.1 1 章（業務観点のシステム要件）についての整理

本節では 1 章で論じた要件を参照し、検討の前提とするための整理を行う。

「2.2.1 システム要件」で示した通り、業務観点におけるシステム要件を以下に再掲する。

表 3-1

No.	システム要件	システム要件の内容
1	データ共有	• 事業者間において国際標準に準拠し、**データを共有**できること。
2	データの信頼性	• データの信頼性が確保されること。**耐改ざん性**や**否認防止性**、**可監査性**を有すること
3	処理ロジックの透明性と確実性	• データに対する処理ロジック**透明性**と**確実性**が確保されること。
4	通信先の信頼性	• 通信先の信頼性が確保されること。**通信先が確かにその事業者**であることが保証されること
5	データ主権の確保	• **データ所有者が認めた相手と情報に限りデータを開示されること** • **データ所有者の制御**にてデータ管理ができること（作成、変更、削除） • 運営者はデータ所有者の許諾なしに**データへのアクセスができない**こと • データ所有者が**データの保管場所を選択**できること • 各国の法規に従った配置場所を選択できること
6	システムの持続可能性	• データを**長期的に保持**する（データ長期保管） • システム運用が**長期的に持続可能**であること。
7	大量データ処理性能の確保	• **1万社規模のユーザ**からの要求を処理できること(利用規模は運用初期の想定) • 処理においては、レスポンス性よりも**確実性を重視**する。 • 海外拠点からの連携処理にも対応できること。
8	拡張処理性能の確保	• **参画事業者拡大に伴うシステム拡張**の要求を処理できること。

これらは業務要件を整理した上で、システムに対する要求として記述されている。このことから、これらが CE 情報流通 PF に求められるものであり、この要件において BC を適用する範囲を後述にて検討していく。

3.2.2 2 章（ブロックチェーンの利点と課題）についての整理

本節では「2 章 ブロックチェーンの利点と課題」を参照し、検討の前提とするための整理を行う。

2 章においては、一般的な側面から論じるために、BC が備える技術特性を起点とし、そこから得られる利点、および生じる課題を分けて記述している。2 章の記載を構造的に整理すると以下の表となる。

表 3-2

表の見方として以下に例を挙げる。

- 「分散台帳」という技術特性から、台帳を共有することに伴い「情報共有」という機能的な利点が生じる一方、共有データの秘匿化という課題が生じる
- 「トランザクションへのデジタル署名」という技術特性から、トランザクションの出元とそのデータの正しさを検証できることにより「否認防止や取引先の信頼性」が非機能的な利点として生じるが、同時に署名に対する「秘密鍵の流出」が課題として生じる

2 章で論じた BC の利点と課題の内容については、上記の表にて整理することで後述の BC 適用範囲を検討する内容として用いる。

3.2.3 要件に対するブロックチェーンの適合性

本節では、上記で整理した通り 1 章における CE 情報流通 PF に対する要件、および 2 章の BC の利点と課題を用いて、要件に対して BC の適合性について検討する。

「1 章における CE 情報流通 PF に対する要件」を「行」、「2 章の BC の利点と課題」を「列」としてマトリクスで整理した結果を以下に示す。その上で、各要件に対して BC の各利点が特に適合する箇所を検討した。当該要件においては BC 活用において利点が強く得られる箇所であると想定されることから、BC を用いて実現することを検討する。

表 3-3

3.2.4 ブロックチェーンの適合性の判断理由

上記の整理結果を導くに当たり　、その理由を以下に詳細に記載する。また、適合しない箇所、つまり BC の利点が得られず、課題として想定される箇所についてもその内容を記載する。

- 要件：データの共有
  - 判断結果：BC 適用を推奨
  - 判断理由：BC はそもそもデータを共有することを得意とするため（「2.4.1.1 情報の共有（透明性）」参照）
- 要件：データの信頼性
  - 判断結果：BC 適用を推奨
  - 判断理由：時系列的な連鎖構造（ハッシュチェーン）を持つデータ構造による高い耐改ざん性、それらが変更履歴も含めて記録されることで実現される責任追跡性などのセキュリティ面の利点を活かし、複数事業者間での重要なデータ共有に活用（「2.5.1.1 利点」参照）
- 要件：処理ロジックの透明性と確実性
  - 判断結果：BC 適用を推奨
  - 判断理由：BC はスマートコントラクトによる処理ロジックを BC に参加している事業者は誰でも内容を確認できるため。（「2.4.1.1 情報の共有（透明性）」参照）

- 要件：通信先の信頼性
  - 判断結果：BC 適用を推奨
  - 判断理由：トランザクションに秘密鍵でデジタル署名を付与し、それらの正当性を取引ごとに検証する特性を活かす。通信先が確かにその事業者であることを能動的に受信側で検証することで利害関係のあるステークホルダ間での機密性の高いデータ共有に活用（「2.5.1.1.4 信頼性」参照）。
- 要件：データ主権の確保
  - 判断結果：BC 適用を推奨
  - 判断理由：BC 上のデータの read/write の機能を有するスマートコントラクト（プログラム）の実行権限を適切に設計することで、細かい権限制御が可能であり、かつそのプログラム自体の透明性を実現する（「2.4.1.1 情報の共有（透明性）」参照）。ただし、分散台帳であるという特性の相反するデータの開示（共有先）の制御においては BC 基盤の個別機能を用いて実現することが求められる。なお、保管場所の指定については、システムとして配置場所の選択肢を与えることなどを検討する。
- 要件：システムの持続可能性
  - 判断結果：BC 適用を推奨
  - 判断理由：耐改ざん性とシステム全体としての耐障害性の利点を活かして長期的なデータ保管を実現する。ただし、データ量に伴うコスト増、運用負荷について検討することが求められる。
- 要件：大量データ処理性能の確保
  - 判断結果：BC 利用時は課題へ対処必要
  - 判断理由：BC はその技術特性から高性能を求める要件においては課題が存在する（「2.5.2.2 課題」参照）。CE 情報流通 PF においては、高速に処理することより、確実に大量データの処理を完了することが求められるため、信頼のあるデータが確実に共有されるというトランザクションのアトミック性を検討するべきである。
- 要件：拡張処理性能の確保
  - 判断結果：BC 利用時は課題へ対処必要

- 判断理由：BC ではその利点を実現している技術的特性より、事業者数が大規模になる場合に BC ネットワーク全体の規模が大きくなる。このため、ノード数増大に伴い分散性が高まり、合意形成のための通信量の増加やネットワーク遅延が増加し、拡張処理自体の性能が劣化するリスクがある。

3.2.5 ブロックチェーン適用範囲について

上記で整理した要件への適合性を受けて、BC 適用範囲を検討する。

CE 情報流通 PF においては、公開情報（再生材の利用率、法規に関わる組成情報など）を取引関係のある事業者間で効率的に伝達する一方で、各事業者のトレードシークレット（製品中の化学物質情報、サプライヤ情報等）を守る必要がある。

データの活用範囲の観点においては以下のように区分できると想定する。

- 一つの事業者内でのみ利用：個社データ
- 事業者間・全事業者で利用：共有データ

「データレイヤ＋インダストリーサービス」は事業者間の情報伝達の管理を担うことから、「共有データ」を取り扱う。共有データはさらに以下のように整理できる。

1. 当事者の事業者間でのみ共有
    - 取引関係データ（例：取引関係情報）
    - 連携データ（例：成分情報）
2. 全ての参加事業者で共有
    - 法規関連情報などの共通利用データ（例：規制物質リスト）

「3.2.3 要件に対するブロックチェーンの適合性」の内容と、上記の観点の関係を整理すると下記表のようになる。

表 3-4

「BC活用の利点が得られる部分」と一致する点が多い

No.	システム要件	BC活用の利点が得られる部分	一つの事業者内でのみ利用（個社データ）	事業者間・全事業者で利用（共有データ）	
				当事者の事業者間でのみ共有	全ての参加事業者で共有
1	データ共有	○	-	○	○
2	データの信頼性	○	-	○	-
3	処理ロジックの透明性と確実性	○	-	○	-
4	通信先の信頼性	○	-	○	-
5	データ主権の確保	○	○	○	-
6	システムの持続可能性	○	○	○	○
7	大量データ処理性能の確保	-	○	○	-
8	拡張処理性能の確保	-	○	○	-

上記表に示した通り、**「当事者の事業者間でのみ共有するデータ」を BC の適用範囲として定めることを推奨する。**

理由としては以下である。

- 「当事者の事業者間でのみ共有するデータ」はシステム要件として定められた事項がより多く要求され、かつ BC 活用の利点が得られる部分との合致が多数であるため。

また、上記以外のデータへの BC 適用を推奨しない理由は以下である。

- 「一つの事業者内でのみ利用するデータ」は BC 活用の利点が得られる部分と合致する点が少なく、BC 適用には向かないため。
- 「全ての参加事業者で共有するデータ」は、システム要件および BC 活用の利点が得られる部分のいずれの観点においても合致する点が少ないため。

3.3 ブロックチェーン適用による課題

BC 適用範囲を定める一方、利点と対をなす課題や特徴的な BC 技術を適切に用いる考慮点が存在する。

表 3-5

No.	課題	内容	対策記載の章節
1	性能リスクへの対策	BCは一般的に性能におけるリスクがあり、CE情報流通PFにおいては多数の事業者が参加する計画であるため、より性能リスクが高い。	4.2 性能を確保するためのBC要件
2	情報漏洩・改ざん防止のための実現方法の検討	BCは一般的に全参加者へデータを共有する。一方で、CE情報流通PFにおいてはトレードシークレットが要求され、BC内で相手先を限定する「データ秘匿化」について、実現方法を検討する必要がある。また、秘密鍵流出を防ぐための鍵管理や、NW支配リスクへの対応も含めたBCノード構成も検討することが重要である。	4.3 情報漏洩・改ざんを防止するBC要件
3	BCに掲載する情報の検討	BC上に具体的に何のデータを格納するか、ということは非常に重要である。	4.4 BCに格納する情報に関する要件
4	認証方式に関する実現方法の検討	上記No.2の秘匿性に関連して、CE情報流通PFにおいて何を誰が認証するか、という点の検討が必要である。	4.5 認証方式に関するBC要件
5	可用性に関する実現方法の検討	CE情報流通PFにおいては海外連携することも視野に入れると、基本的に常時利用可能である必要がある。システムの障害耐性などについて検討する必要がある。	4.6 可用性に関するBC要件
6	運用・保守性に関する検討	CE情報流通PFにおいては多数の事業者が順次参画・拡大していく計画であり、その運用・保守を効率的かつ確実に実施するための検討が必要である。 また、各事業者と運営事業者の責任分解点の整理も必要である。	4.7 運用・保守性に関するBC要件

これらの課題に対する BC で検討するべき技術要件においては、4 章にて詳細に論じる。

4 対象業務におけるブロックチェーン技術要件

本章では、3 章にて示した CE 情報流通 PF における BC 適用範囲において、BC に対して必要となる要件について示す。また、BC の活用方法の指針についても示す。

4.1 ブロックチェーン適用に関する要件

本節では、CE 情報流通 PF において BC 適用により実現すべき事項および解決すべき事項（BC への要求事項）について示す。4.2 節以降において、具体的な対応指針を BC に対する要件として示す。

4.1.1 ブロックチェーンにより実現すべき事項および解決すべき事項

「3.2.1　1 章（業務観点のシステム要件）についての整理」にて、CE 情報流通 PF においてデータに対して求められるシステム要件を示した。これは、「3.2.5　ブロックチェーン適用範囲について」で整理した BC 適用範囲において BC の利点を活かして実現すべき事項と考えられる。

また、「3.3　ブロックチェーン適用による課題」にて CE 情報流通 PF において課題（解決すべき事項）を整理した。

本節では、この内容を改めて以下に示す。

表 *4-1*

No.	システム要件	システム要件の内容	実現方法・対策の記載章節
1	データ共有	• 事業者間において国際標準に準拠し、**データを共有**できること。	4.4 ブロックチェーンに格納する情報に関する要件
2	データの信頼性	• データの信頼性が確保されること。**耐改ざん性**や**否認防止性**、**可監査性**を有すること	4.3 情報漏洩・改ざんを防止するブロックチェーン要件
3	処理ロジックの透明性と確実性	• データに対する処理ロジック**透明性**と**確実性**が確保されること。	4.3 情報漏洩・改ざんを防止するブロックチェーン要件
4	通信先の信頼性	• 通信先の信頼性が確保されること。**通信先が確かにその事業者**であることが保証されること	4.5 認証方式に関するブロックチェーン要件
5	データ主権の確保	• **データ所有者が認めた相手と情報に限りデータを開示されること** • **データ所有者の制御**にてデータ管理ができること（作成、変更、削除） • 運営者はデータ所有者の許諾なしに**データへのアクセスができない**こと • データ所有者が**データの保管場所を選択**できること • 各国の法規に従った配置場所を選択できること	4.3 情報漏洩・改ざんを防止するブロックチェーン要件
6	システムの持続可能性	• データを**長期的に保持**する（データ長期保管） • システム運用が**長期的に持続可能**であること。	4.4 ブロックチェーンに格納する情報に関する要件
7	大量データ処理性能の確保	• **1万社規模のユーザ**からの要求を処理できること(利用規模は運用初期の想定) • 処理においては、レスポンス性よりも**確実性を重視**する。 • 海外拠点からの連携処理にも対応できること。	4.2 性能を確保するためのブロックチェーン要件
8	拡張処理性能の確保	• **参画事業者拡大に伴うシステム拡張**の要求を処理できること。	4.2 性能を確保するためのブロックチェーン要件

表 4-2

No.	課題	内容	対策記載の章節
1	性能リスクへの対策	BCは一般的に性能におけるリスクがあり、CE情報流通PFにおいては多数の事業者が参加する計画であるため、より性能リスクが高い。	4.2 性能を確保するためのBC要件
2	情報漏洩・改ざん防止のための実現方法の検討	BCは一般的に全参加者へデータを共有する。一方で、CE情報流通PFにおいてはトレードシークレットが要求され、BC内で相手先を限定する「データ秘匿化」について、実現方法を検討する必要がある。また、秘密鍵流出を防ぐための鍵管理や、NW支配リスクへの対応も含めたBCノード構成も検討することが重要である。	4.3 情報漏洩・改ざんを防止するBC要件
3	BCに掲載する情報の検討	BC上に具体的に何のデータを格納するか、ということは非常に重要である。	4.4 BCに格納する情報に関する要件
4	認証方式に関する実現方法の検討	上記No.2の秘匿性に関連して、CE情報流通PFにおいて何を誰が認証するか、という点の検討が必要である。	4.5 認証方式に関するBC要件
5	可用性に関する実現方法の検討	CE情報流通PFにおいては海外連携することも視野に入れると、基本的に常時利用可能である必要がある。システムの障害耐性などについて検討する必要がある。	4.6 可用性に関するBC要件
6	運用・保守性に関する検討	CE情報流通PFにおいては多数の事業者が順次参画・拡大していく計画であり、その運用・保守を効率的かつ確実に実施するための検討が必要である。 また、各事業者と運営事業者の責任分解点の整理も必要である。	4.7 運用・保守性に関するBC要件

4.2 性能を確保するためのブロックチェーン要件

本節では、CE 情報流通 PF において重要となる性能に関する BC 要件について示す。

4.2.1 性能モデル定義

本節では、CE 情報流通 PF において性能面で目標となる「性能モデル」を定義する。

4.2.1.1 性能モデルとは

本節における性能モデルとは下記事項を指す。

表 4-3

<性能モデルの定義事項>

No.	定義事項	主な内容
1	対象物	性能要件を定義する対象とする物（業務、機能、データ、拠点、アクターなど）
2	性能目標	性能要件の測定項目と性能目標（例：処理時間が1日以内）

<性能モデル定義のステップ>

No.	ステップ	内容
1	対象物リストアップ	3章にて議論した結果（BCには共有データを格納し、共有する機能を活用する）を踏まえて、性能モデル定義の対象物の候補をリストアップする。
2	モデル抽出	上記1の候補のうち、対象業務の要件「特定多数のユーザオペレーション性の確保」に関する課題が顕在化する可能性があるものを抽出する。
3	モデル定義	上記2のリストアップした対象物について、性能目標を定義する。

4.2.1.2 性能モデルの定義対象

4.2.1.2.1 フォーカスエリア

本節では、「3.2.5　ブロックチェーン適用範囲について」にて示した BC の適用範囲を対象として性能モデルを定義する。

4.2.1.2.2 対象産業

本節では、以下の前提にて性能モデルを定義する。

- 動脈産業は、製品含有化学物質管理をベースに性能モデル定義を行う。
- 動脈産業と静脈産業の相互接続については、現状は業務モデル定義が難しいため本書作成時点では検討対象外とする。

4.2.1.3 ステップ 1：対象物リストアップ

性能モデル定義の対象物の候補をリストアップする。

表 4-4

No.	分類	対象物	主な内容
1	業務	非共有データ管理系業務	• ユーザ情報の登録・更新・削除など • 組成情報の登録・更新など
2		共有データ管理系業務	• 購入品の組成の川上への調査依頼・川下への回答など • 規制物質リストの全社への配信など • 規制物質の照会および川下への回答など
3	機能・非機能	データ共有（透明性）	• 事業者間で組成データ等を共有する
4		公平性（分権）	• 事業者間でBC書き込みデータを合意する
5		業務効率性	• スマートコントラクトにて自動処理を実行する
6		不正防止（二重支払防止）	• 同じデータを二重に取引に用いさせない
7		セキュリティ	• 耐改ざん性、否認防止、信頼性、追跡性などの非機能的な要件
8		性能・拡張性	• 参加事業者追加などの非機能的な要件
9		可用性	• 耐障害性などの非機能的な要件
10		運用保守	• システム監視、システム更新などの非機能的な要件
11		移行性	• 移行性に関する要件
12	データ	非共有データ	• ユーザマスタや製品マスタなどの他社へ共有しないデータ（例：組成情報マスタ）
13		共有データ	• 組成情報の回答データなどの事業者間で共有されるデータ（例：回答組成情報）
14	拠点	国内	• 国内からCE情報流通PFへアクセスするユーザ
15		海外	• 海外からCE情報流通PFへアクセスするユーザ
16	アクター	CE情報流通PF参加事業者	• CE情報流通PFを利用する事業者
17		CE情報流通PF非参加事業者	• CE情報流通PFを利用しない事業者（ただし、サプライチェーンに参加している事業者）
18		運営事業者	• CE情報流通PFを運営する事業者
19		アプリケーションベンダ	• CE情報流通PFアプリケーションを開発する事業者
20	環境	本番環境	• データ連携システムの本番運用環境
21		開発環境	• データ連携システムの開発環境

「非共有データ」はBCへ格納しないため、以降の検討対象外とする。

「移行性」に関する要件は特に無いため、以降の検討対象外とする。

「非共有データ」はBCへ格納しないため、以降の検討対象外とする。

CE情報流通PFに対する直接的な関与はないため、以降の検討対象外とする。

4.2.1.4 ステップ 2：モデル抽出

「対象物リストアップ」の候補のうち、「4.1　ブロックチェーン適用に関する要件」にて示した要件「大量データ処理性能の確保」や「拡張処理性能の確保」に関する課題が顕在化する可能性があるものを抽出する。

対象物の組み合わせを検討し、そのうち課題顕在化の可能性があるものを対象「○」とする。

表 4-5

No.	対象物１	対象物２	対象物３	対象物４	対象物５	対象物６	対象	モデル概要
1	共有データ管理系業務	データ共有	共有データ	国内、海外	CE情報流通PF参加事業者	本番環境	○	組成データ等の共有
2		公平性					○	BC書き込み時の合意
3		業務効率性					○	BC上のスマートコントラクト実行
4		不正防止						BCによる二重取引防止
5		セキュリティ						耐改ざん性、否認防止、信頼性、追跡性の実現
6		性能・拡張性					○	参加事業者の拡張（BCネットワークの拡張）
7		可用性						耐障害性の実現
8		運用保守					○	システム運用保守の実施（システム更新等）
9		データ共有		国内	運営事業者			運営事業者の規制物質リスト配信
10		ALL			アプリケーションベンダ	開発環境		アプリケーションベンダによる開発

「二重取引防止」について、ここではPoWによるマイニング処理は、CE情報流通PFにおける採用は想定しない。
ビザンチン耐性のあるコンセンサスアルゴリズムなどによる対策が存在するが、その処理負荷は軽微な想定として、課題顕在化の対象外とする。

「セキュリティ」、「可用性」のBCによる実現方法は、BCの仕組みそのもので実現可能であり処理が実行されるわけではないため、課題顕在化の対象外とする。

「規制物質リスト」はBCへの格納対象外とするため、課題顕在化の対象外とする。

4.2.1.5 モデル定義

「モデル抽出」にてリストアップした対象物について、性能目標を定義する。

性能目標は、絶対的な合格条件ではなく目標であり、それを充足することを目指すものとする。また、「常時これを充足する」のではなく、「ピーク時の性能目標」という位置付けとする。なお、下記に記載の性能目標は今後変更される場合がある。

表 4-6

No.	モデル概要 (前ページNo.)	性能目標	性能目標値の根拠
1	組成データ等の共有 (No.1)	国内・海外のCE情報流通PF利用事業者1万社程度が同様のタイミングで100点程度の組成データ（100点のデータサイズ0.01MB程度の想定）を相手事業者へ共有する際に、BCへの共有データの書き込み処理完了時間が**「8時間以内」**であること。 なお、サプライチェーン全体の全ての共有処理ではなく、各社が必要な共有先へ1階層分共有する処理を対象とする。	他社への回答依頼から、回答を受領するまでの目標を24時間と定義。 その内訳として下記とし、BCは①と③部分が該当する。 ①回答依頼が相手に届くまで：8時間 ②回答依頼受領後に回答するまで：8時間 ③回答実施から回答が相手に届くまで：8時間
2	BC書き込み時の合意 (No.2)	上記No.1に同じ。	上記No.1に同じ。
3	BC上のスマートコントラクト実行 (No.3)	上記No.1に同じ。	上記No.1に同じ。
4	参加事業者の拡張（BCネットワークの拡張） (No.6)	1万社程度が既に参加している状況において、50社程度が同様のタイミングでCE情報流通PFに新規参画する際に、システム上の新規参画事業者のBC部分の拡張処理完了時間が**「24時間以内」**であること。	1万社が1年間で順次参画すると想定し、平均的に**約28社／日**となるため、**50社・1日**とした。
5	システム運用保守の実施（システム更新等） (No.8)	1万社程度が既に参加している状況において、バックアップやスマートコントラクト変更が所定の時間内に完了すること。	執筆時点では非機能要件が明確ではないため、ここでは「所定の時間内」とした。

上記表の性能モデルのイメージを下記に示す。

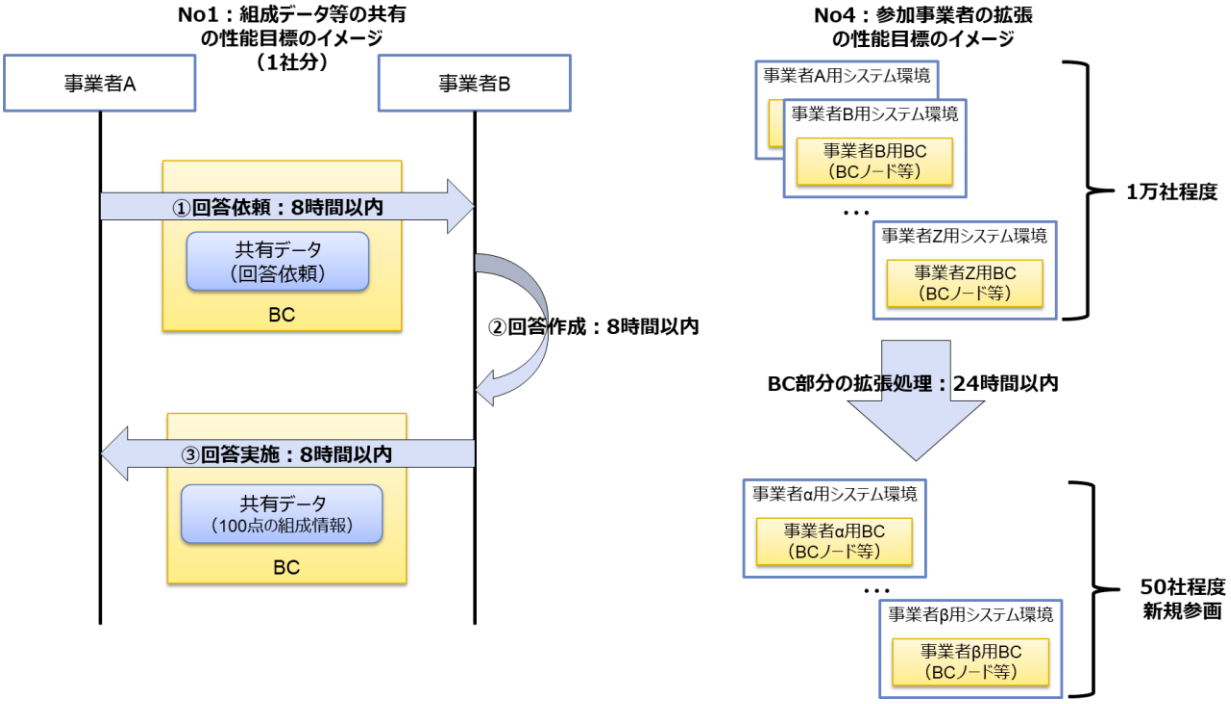


図 4-1

4.2.2 性能リスクと対策案

本節では、前節にて定義した「性能モデル」を充足するに当たり、リスクとなる事項とその対策案を示す。

4.2.2.1 性能リスク一覧

表 4-7

No.	リスク	内容	影響する性能モデル
1	BCの特性としての性能リスク	BCは特性として性能面のリスクがある。	No.1 組成データ等の共有 No.2 BC書き込み時の合意 No.3 BC上のスマートコントラクト実行
2	利用者増に伴う性能劣化	システム利用事業者数が増大することに伴い、BCの合意形成処理やスマートコントラクト処理時間が長期化して、システム全体として処理遅延につながるリスク	No.1 組成データ等の共有 No.2 BC書き込み時の合意 No.3 BC上のスマートコントラクト実行 No.5システム運用保守の実施（システム更新等）
3	利用者追加の性能劣化	システム利用事業者数が増大することに伴い、BCのノード追加等の利用事業者追加処理が遅延するリスク	No.4 参加事業者の拡張（BCネットワークの拡張）
4	データ蓄積に伴う性能劣化	システム利用事業者数が増大することに伴い、BCに格納するデータが累積して蓄積され処理遅延につながるリスク	No.1 組成データ等の共有 No.2 BC書き込み時の合意 No.3 BC上のスマートコントラクト実行 No.5 システム運用保守の実施（システム更新等）

4.2.2.2 対策案

本節では、前節にてリストアップした性能リスクに対して、対策方法の案を示す。

表 4-8

No.	対策案	内容	対応するリスク
1	非同期アーキテクチャの検討	インダストリーサービスレイヤにおいて、他社への依頼や回答処理の応答と、BCへの書き込み処理を非同期とし、ユーザへの応答性を確保しつつ、BCへの書き込み処理はバックグラウンドで処理するように検討する。	BCの特性としての性能リスク
2	コンセンサスアルゴリズムの選択	BCへ書き込みする際に行われる合意形成処理において、処理時間が増大しないようなコンセンサスアルゴリズムを選定する。	BCの特性としての性能リスク 利用者増に伴う性能劣化
3	共有先指定方法の選択	BCにて共有先を指定する方法はいくつかある。共有先の指定方法として、処理時間が増大しないような方法を選択する。	BCの特性としての性能リスク 利用者増に伴う性能劣化
4	BC拡張方法の選択	BCのノード追加等の利用事業者追加処理を行う方法として、処理時間が増大しないような方法を選択する。	利用者追加の性能劣化
5	履歴データの容量の削減	BCに格納するデータが累積して蓄積されることに対して、その容量を削減する。	データ蓄積に伴う性能劣化

4.2.2.2.1 非同期アーキテクチャの検討

BC はその特性として性能面のリスクがある。具体的には、BC への書き込み処理や参照処理速度が遅い傾向にある。このため、BC を含めたシステム全体として非同期アーキテクチャの検討を行い、性能モデルの充足を狙う。

インダストリーサービスレイヤにおいて、他社への依頼や回答処理の応答と、BC への書き込み処理を非同期とし、ユーザへの応答性を確保しつつ、BC への書き込み処理はバックグラウンドで処理するようなアーキテクチャを検討する。

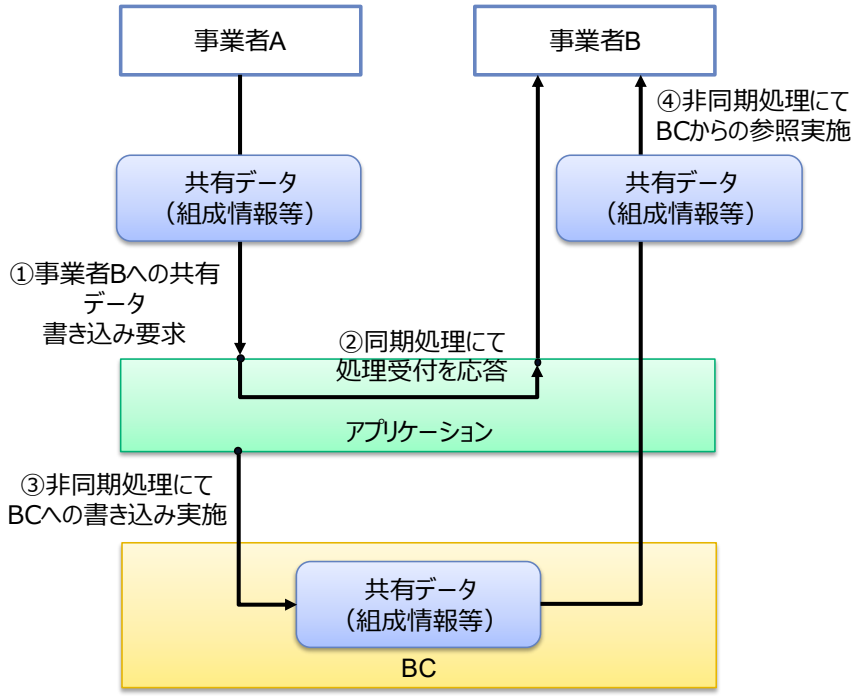


図 4-2

4.2.2.2.2 コンセンサスアルゴリズムの選択

コンセンサスアルゴリズムは種類や特徴も様々であり、性能面においても特性に差異がある。このため、特性の差異に留意してコンセンサスアルゴリズムを選択する。以下にコンセンサスアルゴリズムの一例を示すが、これ以外のコンセンサスアルゴリズムも含めて性能モデルを充足するものを選択すること。

- PoW（Proof of Work）

  ブロックの生成に当たり、マイナー（採掘者）と呼ばれる複数の第三者にインセンティブを与えてデータに関する特定の計算（マイニング）を依頼し、そのうち最初に計算を終えたマイナーのブロックが有効となるというコンセンサスアルゴリズム。ファイナリティが確定的でなく、ブロック生成速度が比較的遅い。

- PoS（Proof of Stake）

  抽選によってブロックを生成する者を決定する仕組みであり、その際にステークと呼ばれる掛け金を多く持つ者ほど当選確率が高くなるようにすることで、PoW における計算量増大の問題を回避したコンセンサスアルゴリズム。PoW に比べトランザクション処理量が高いとされている。

- PoA（Proof of Authority）

  電子署名にて身元を証明した特定の複数人がブロック生成者となり、authority ノードと呼ばれるノード上で持ち回りでブロックを生成する仕組みのコンセンサスアルゴリズム。ブロック生成者を信頼していることが前提となっており、余分な計算などが発生しないことから、トランザクション処理量は高い。

- Raft

  ブロック生成を担う Leader と呼ばれるノードとそれ以外の Follower と呼ばれるノードで構成され、Leader を中心に合意を形成するコンセンサスアルゴリズム。ブロック生成者を信頼していることが前提となっている。余分な計算などが発生しないことから、トランザクション処理量は高い。

4.2.2.2.3 共有先指定方法の選択

共有先の指定方法によっては、性能へ影響する場合がある。詳細については、「4.3.3.2　実現方式：共有範囲」を参照されたい。

4.2.2.2.4 ブロックチェーン拡張方法の選択

参加事業者を CE 情報流通 PF へ追加する際に、BC においてはノード追加等の処理が発生する。この際に、ノード追加のシステム上の処理や、ノード追加に伴う BC 上の承認処理などを伴うケースがある。

このため、以下のような点に留意して拡張方法を選択する。

- ノード構成の検討

  BC を構成するノードについて、例えばコンテナを採用するなど、システム上の処理負荷が大きくならないような構成を検討する。

- ノード追加時の承認処理

  ノード追加時には、BC 上で承認処理が行われる。この処理において、追加先のネットワーク上のノード数規模に応じて処理が増大するケースがあるため、この点に留意する。

4.2.2.2.5 履歴データ容量の削減

BC では一般的にデータはハッシュ情報により依存関係がある状態で記録（ハッシュチェーン）される特性があるため、長年システムを運用していくとこのチェーンが肥大化する恐れがある。これにより、大量データが BC に格納されていることによる影響で参照時の性能劣化やデータ領域ひっ迫のリスクがある。

この対策方法として、下記の 2 つが挙げられる。

- 外部データストアとの連携

  BC 上にはハッシュ値などの軽量データを登録し、実データは BC 外のデータストアに格納する方法。大きく分けると、RDB などを利用した集中型のデータストアを使用する場合と IPFS などの分散型ファイルストレージを構築する場合が考えられる。

- データアーカイブ

  BC 上には新しいデータのみを保持し、一定期間が過ぎたデータや検証に不要なデータはチェーンから切り離し、コールドストレージへの保管やデータ最適化を検討する。

4.3 情報漏洩・改ざんを防止するブロックチェーン要件

本節では、CE 情報流通 PF において非常に重要となる「当事者の事業者間でのみ共有するデータ」の情報漏洩・改ざんを防止するための BC 要件について示す。

4.3.1 秘匿の定義

BC は参加者間での情報共有を前提とした仕組みであるが、CE 情報流通 PF においては共有先を特定者に限定する必要がある。BC の一部の参加者しか見られない状態にすることを**「秘匿」**と定義する。

また、本書では 3 章でも述べたように、BC へ格納する情報は**「他社へ共有するデータ（組成データ）」**であり、以降ではこの前提にて記述している。

4.3.2 秘匿要件の検討

秘匿の実現には、何を、誰から、いつ、秘匿するのか、という秘匿の要件を整理する必要がある。

表 4-9

秘匿対象 (何を秘匿するか)	**取引先としてどこが存在するのか**や、共有する**情報の中身を秘匿**したい場合、**情報を共有した事実**を秘匿したい場合がある。
共有範囲 (誰に共有/秘匿するか)	**ネットワーク参加者全員**に共有したい場合と**特定の参加者**に共有したい場合がある。
秘匿期間 (いつまで秘匿するか)	秘匿した情報の秘匿期間として、**いつまで秘匿するか**、という点がある。
秘匿変更 (秘匿先の追加・削除)	**開示⇔秘匿を変更したい**場合が存在する。 また、これまで**秘匿していた情報を開示に変更**したり、反対にこれまで**開示していた情報を秘匿に変更**したい場合がある。

4.3.2.1 要件検討：秘匿対象

何を誰から秘匿するのか、という点に関する要件を定義する。

秘匿対象として下記の候補が考えられる。

- ①取引先としてどこが存在するのかという情報を秘匿
- ②組成データの中身を秘匿
- ③共有した事実の存在を秘匿

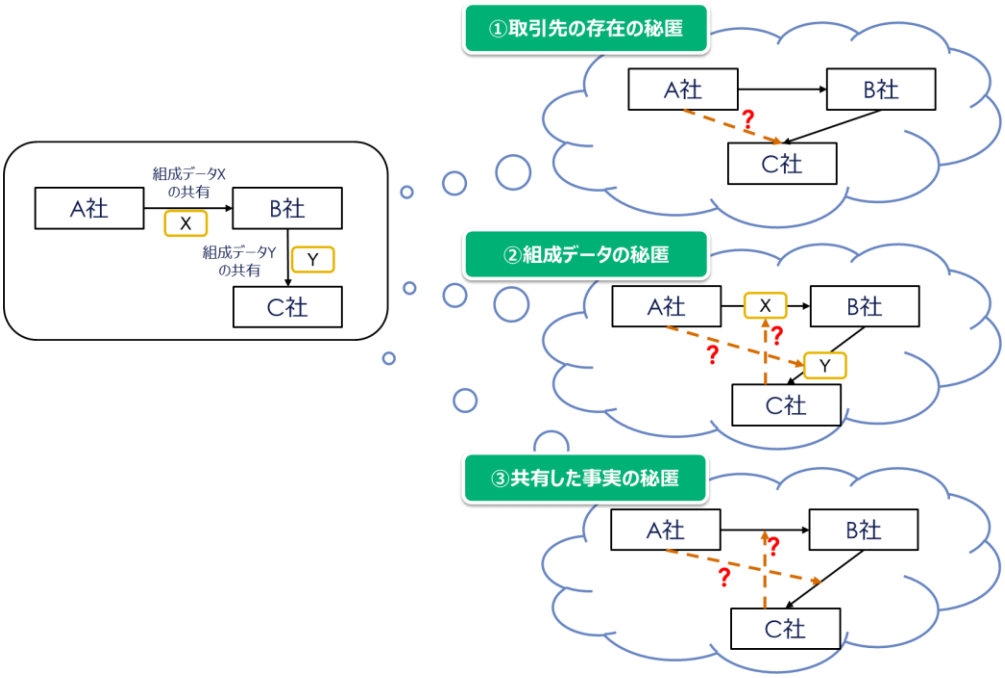


図 4-3

CE 情報流通 PF の要件としては、下記となる。

組成データの秘匿は必ず実現する必要があるが、その他の要件については可能な限り実現が求められる。

表 4-10

No.	秘匿対象	CE情報流通PFの要件	要求レベル
1	取引先の存在の秘匿	全事業者に対して、自社が取引のある取引先以外については、取引先として他にどこが存在するかを秘匿すること。	任意
2	組成データの秘匿	組成データを共有する取引先以外に対して、組成データの中身を秘匿すること。	必須
3	共有した事実の秘匿	組成データを共有する取引先以外に対して、共有した事実を秘匿すること。	任意

4.3.2.2 要件検討：共有範囲

誰が、誰に共有するのか、という点に関する要件を定義する。

CE 情報流通 PF においては、組成データを共有する事業者が、共有先事業者を都度 1 社選択して共有することが要件となる。

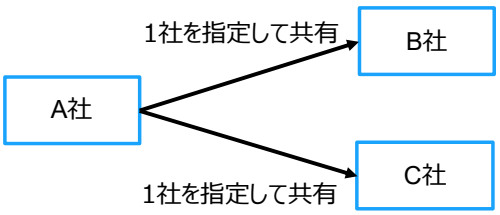


図 4-4

4.3.2.3 要件検討：秘匿期間

いつからいつまで秘匿するのか、という点に関する要件を定義する。

CE 情報流通 PF においては、組成データを共有する事業者が秘匿を開始した時点から秘匿を停止するまでは、共有先事業者以外へ秘匿されることが要件となる。つまり、秘匿を停止しなければ、CE 情報流通 PF が存続し続ける限りは長期的に秘匿する必要がある。

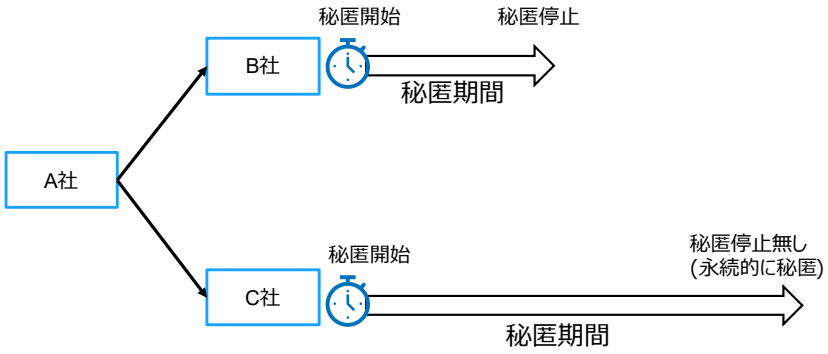


図 4-5

4.3.2.4 要件検討：秘匿変更

秘匿状態を変更するケースがあるのか、という点に関する要件を定義する。

- ①これまで情報を秘匿していた相手に今後共有したい
- ②これまで情報を共有していた相手に今後は秘匿したい
- ③秘匿していた過去の情報について遡って共有したい
- ④共有していた過去の情報について遡って秘匿したい

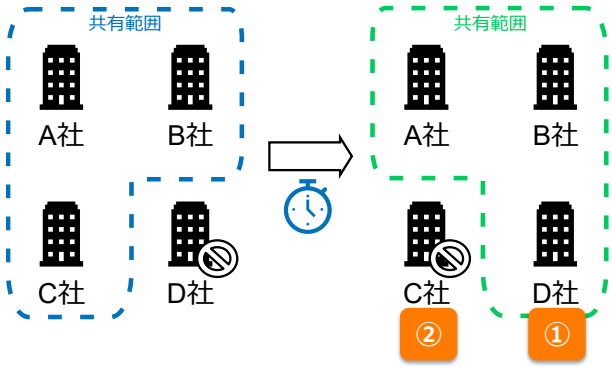


図 4-6

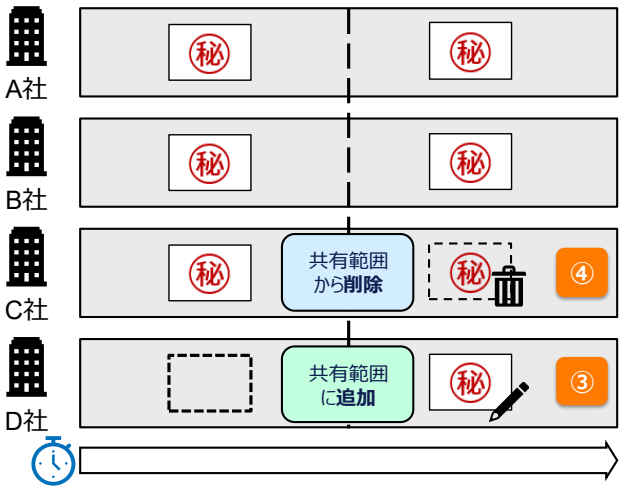


図 4-7

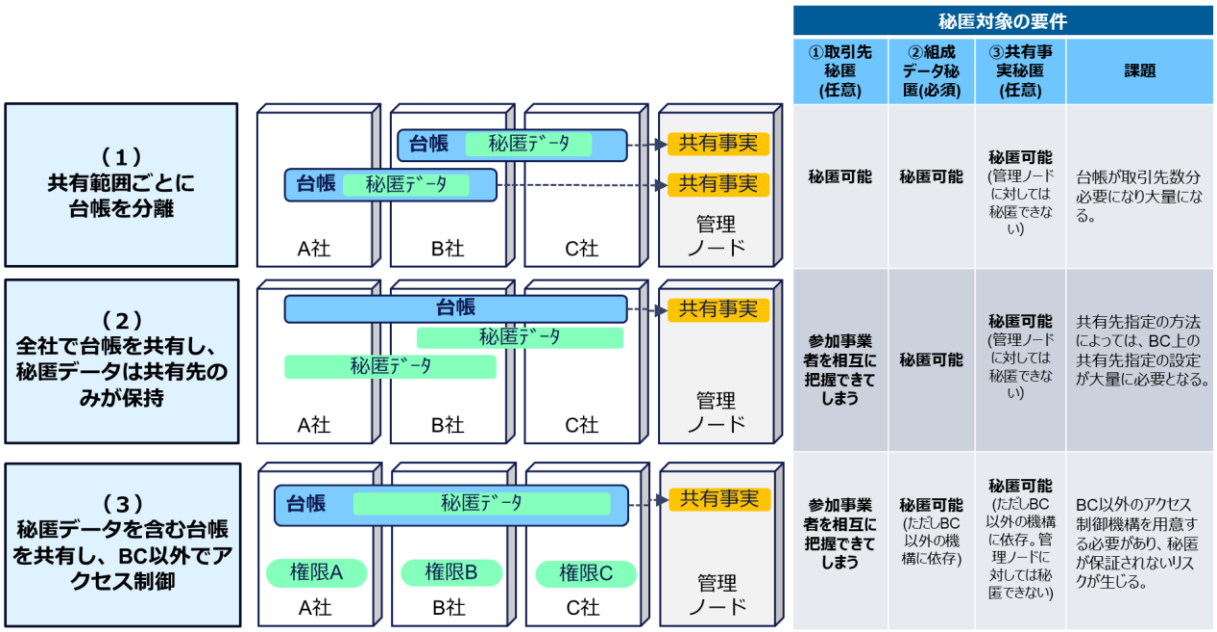
CE 情報流通 PF においては、①～④のいずれのケースもありうる。

例えば、合併等により取引先が変更となり、これまで共有していた相手に対して秘匿する必要が生じるケース（上記の②）などが考えられる。

4.3.3 秘匿要件の実現

4.3.3.1 実現方式：秘匿対象

秘匿対象の要件の実現に関しては、BC の台帳の構成と秘匿データをどのように保持するかで実現方式がいくつか考えられる。



秘匿対象の要件			
①取引先秘匿(任意)	②組成データ秘匿(必須)	③共有事実秘匿(任意)	課題
秘匿可能	秘匿可能	秘匿可能(管理ノードに対しては秘匿できない)	台帳が取引先数分必要になり大量になる。
参加事業者を相互に把握できてしまう	秘匿可能	秘匿可能(管理ノードに対しては秘匿できない)	共有先指定の方法によっては、BC上の共有先指定の設定が大量に必要となる。
参加事業者を相互に把握できてしまう	秘匿可能(ただしBC以外の機構に依存)	秘匿可能(ただしBC以外の機構に依存。管理ノードに対しては秘匿できない)	BC以外のアクセス制御機構を用意する必要があり、秘匿が保証されないリスクが生じる。

図 4-8

上図（1）の実現方式が最も秘匿性が高いものの、台帳が大量に必要となりシステムリソースに要するコストや運用保守性が懸念される。

上図（2）の実現方式は、①取引先秘匿の任意要件については充足できないものの、その他の要件は実現可能であり、最も現実的な方式と考えられる。ただし、共有先の指定方法については注意が必要である。

上図（3）の実現方式は、秘匿の保証が BC 以外のアクセス制御機構に委ねられてしまい、②組成データ秘匿の必須要件であっても保証されなくなるリスクがある。

また、上記いずれの実現方式においても、BC の合意形成の実施方法（コンセンサスアルゴリズム）によっては、承認ノードや管理ノードに対して②組成データ秘匿の必須要件を実現できずに、これらのノードを保持する事業者や運営事業者に秘匿データの中身が見えてしまうことがあるため、そのような合意形成の実施方法を選択しない等の考慮が必要である。

4.3.3.2 実現方式：共有範囲

共有範囲について、BC では下記の 2 つの共有先指定方法がある。

- （A）事前に共有先事業者を登録し、その登録情報を指定して共有を実施
- （B）共有実施の都度、共有先事業者を指定

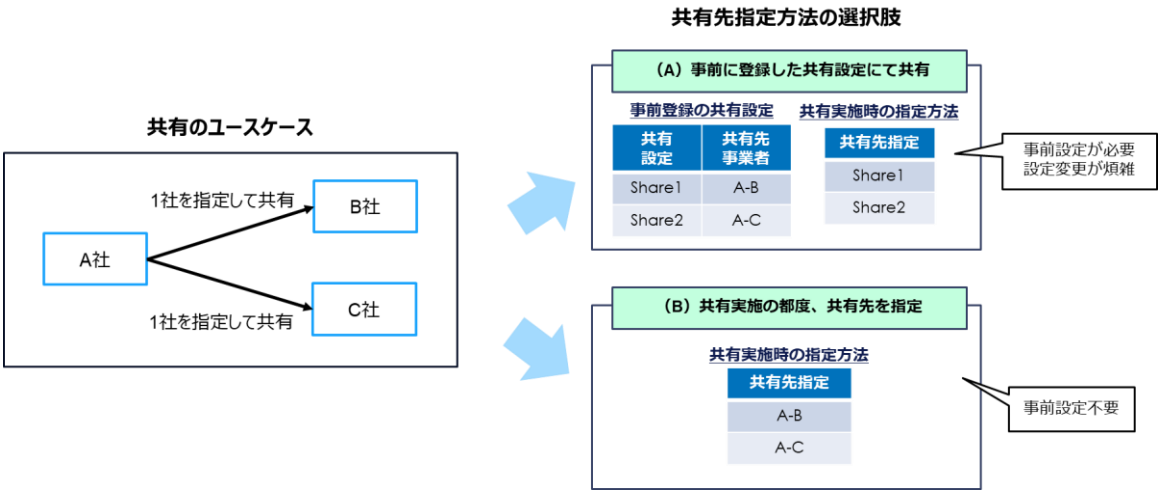


図 4-9

上記（A）の方法の場合は共有先事業者数が多数となった場合にこの登録情報が大量に必要となってしまうため、（B）の方法のほうが望ましい。

4.3.3.3 実現方式：秘匿期間

秘匿期間の要件に関して、BC への書き込み時のデジタル署名（「2.3.5 デジタル署名（トランザクション）」参照）の公開鍵暗号技術や BC に格納するデータ自体を暗号化する場合などの「暗号アルゴリズム危殆化リスク」がある。また、BC への書き込み時のハッシュ値計算（「2.3.4 データ構造（ハッシュチェーン）」参照）や BC に格納するデータ自体のハッシュ値を計算する場合などの「ハッシュアルゴリズム危殆化リスク」への対策が求められる。これらのアルゴリズムは、時間の経過とともにアルゴリズムの危殆化のリスクが高まる。[5,6]

この対策として下記が考えられる。これらの対策を初期の段階で検討しておくことが、重要である。なお、下記表中に示している「最新の有効なアルゴリズム」については CRYPTREC の資料[7]を参照すること。

---

[5] NIST SP800-130「A Framework for Designing Cryptographic Key Management Systems」（https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-130.pdf）

[6] 暗号鍵管理ガイドライン（IPA）（https://www.ipa.go.jp/security/crypto/guideline/ckms.html）

[7] CRYPTREC 暗号リスト(電子政府推奨暗号リスト)（https://www.cryptrec.go.jp/list.html）、暗号強度要件（アルゴリズム及び鍵長選択）に関する設定基準（https://www.cryptrec.go.jp/list/cryptrec-ls-0003-2022r1.pdf）

表 4-11

No.	対策案	内容	対応するリスク
1	暗号鍵長の変更	デジタル署名に用いる暗号鍵の鍵長を変更する。鍵長を増やすことで暗号強度を高めることができる。例えば、Bitcoinで使われている署名方式「ECDSA（鍵長256ビット）」を384bitのECDSA に変更する等の対応が考えられる。 ただし、暗号アルゴリズムの脆弱性に対する対策とはならない。	暗号アルゴリズム危殆化
2	暗号アルゴリズムの変更	デジタル署名時の公開鍵暗号に用いる暗号アルゴリズムを変更する。最新の有効なアルゴリズムを用いることで暗号強度を高めることができる。 ただし、変更をどのように行うかや、データ移行などについてよく検討する必要がある。	暗号アルゴリズム危殆化
3	最新のハッシュアルゴリズムの採用	脆弱性のより少ない最新の有効なアルゴリズムを用いる（SHA-3等）。	ハッシュアルゴリズム危殆化
4	パディング困難なフォーマットの採用	BCに格納するデータのフォーマットとして、JSONなどのパディングが困難なフォーマットを用いる。	ハッシュアルゴリズム危殆化

なお、いずれの対策においても下記の点に留意する必要がある。

暗号アルゴリズムやハッシュアルゴリズムが危殆化してしまった際は、それらのアルゴリズム等を最新化することでそれ以降の格納データに対するリスク回避はできると考えられるが、それ以前に格納されたデータへの考慮も必要となる。

4.3.3.4 実現方式：秘匿変更

「4.3.2.4　要件検討：秘匿変更」で述べたように、CE 情報流通 PF においては下記 4 つのいずれのユースケースも発生し得る。このため、これらを踏まえた BC の設計を行う必要がある。

なお、下記の④については BC 上のデータ削除はできないが、このケースへの対応方法については後述の「4.3.4.1 情報漏洩時の対処」や「4.4 ブロックチェーンに格納する情報に関する要件」を参考されたい。

①これまで情報を秘匿していた相手に今後共有したい ②これまで情報を共有していた相手に今後は秘匿したい	共有範囲の指定方法はBC製品によって異なる。 詳細は「実現方式：共有範囲」を参照。
③秘匿していた過去の情報について遡って共有したい	これまで秘匿していた情報を開示する際には、**情報所有者から明示的にトランザクションを発行**し、過去の情報を連携する
④共有していた過去の情報について遡って秘匿したい	一度開示していた情報を秘匿に変更することは、**BCでは原則としてできない**。

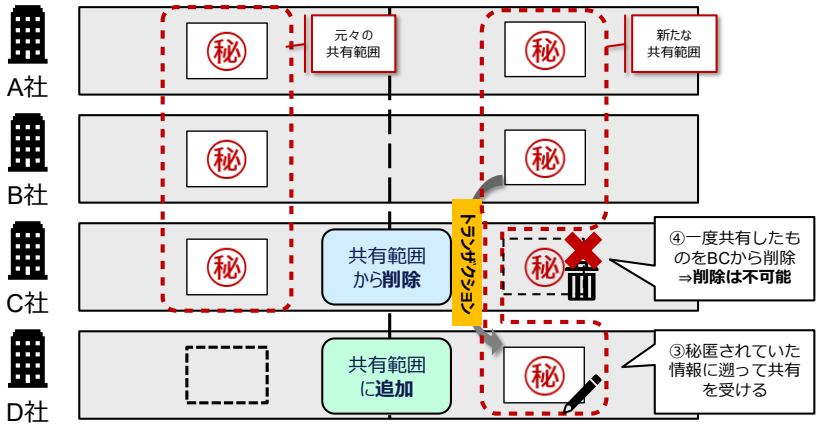


図 4-10

4.3.4 関連する検討ポイント

秘匿に関連する検討ポイントとして、下記が挙げられる。

表 4-12

情報漏洩時の対処	BCは一度書き込みを行うと削除ができないため、誤って開示不可の情報を開示ししてしまった（BCへ書き込んでしまった）場合など、情報漏洩時の対処方法について検討しておく必要がある。
鍵管理	BCではデータ書き込み時に秘密鍵にて電子署名を行うことで、自身が作成したデータであることを証明する。このため、この鍵が漏洩した場合、不正なデータの書き込みなど悪用される恐れがあり、また紛失時はBCへの書き込みができなくなり、鍵管理は重要である。
暗号化	秘匿性確保のための方法として「暗号化」が考えられる。 暗号化の適用領域について、検討が必要である。

4.3.4.1 情報漏洩時の対処

機密情報（組成データ）が当該事業者外部へ漏洩した場合、事業者の競争力低下・信用度低下などの悪影響が考えられる。一方で、BC は一度書き込みを行うと削除ができないため、誤って開示不可の情報を

開示ししてしまった際などに当該データのみを削除することは困難である。このため、情報漏洩時の対処方法を検討しておく必要がある。以下に対処方法の選択肢を示す。

表 4-13

No.	対処方法案	対処内容	影響
1	オフチェーン・ハッシュ値の利用	オフチェーン（BC以外の格納場所）に組成データを格納し、そのハッシュ値をオンチェーン（BC）に格納する。 この方法では、BCの耐改ざん性を活かしつつ様々なメリットがある。詳細は「4.4 ブロックチェーンに格納する情報に関する要件」を参照。	BCとオフチェーンを連携させて利用するための制御部分を別途用意する必要がある。 詳細は「4.4 ブロックチェーンに格納する情報に関する要件」を参照。
2	台帳削除	当該データを格納する台帳を削除する。 物理的にBC上からは削除される。	データ永続化の観点より、BCデータのバックアップ＆当該データを除外してリカバリが必要（長期運用時はリカバリ負担＆業務停止が長期化）
3	アプリケーション非表示	アプリケーションにより当該データを画面非表示とする。物理的にはBC上に残存する。	物理的に残存することにより一定リスクは残存。

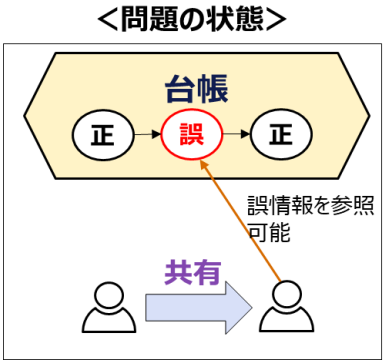


図 4-11

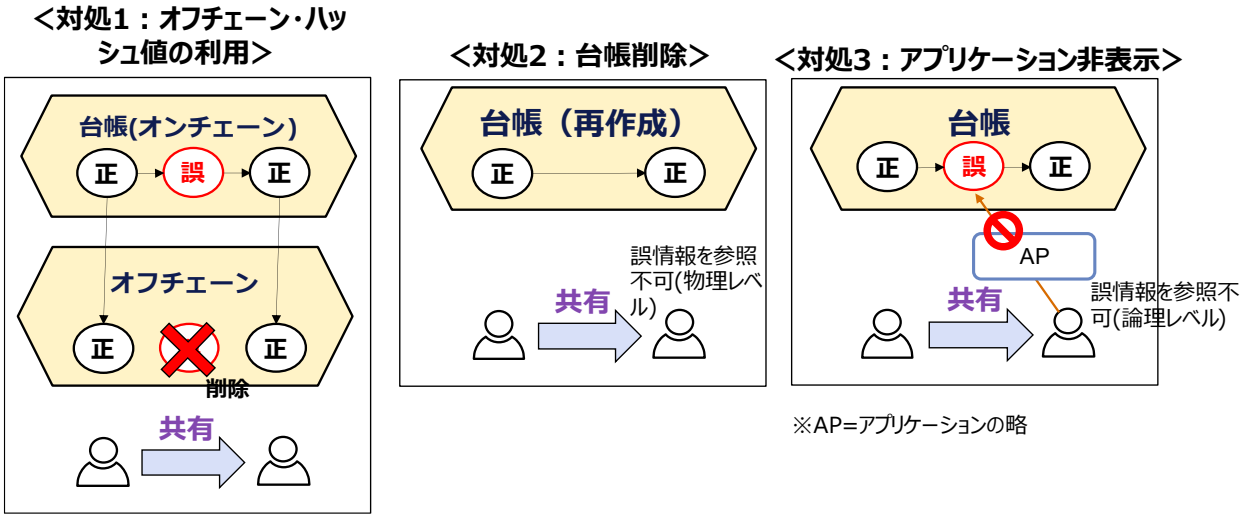


図 4-12

4.3.4.2 鍵管理

BC ではデータ書き込み時に秘密鍵にてデジタル署名を行うことで、自身が作成したデータであることを証明する。このため、この鍵が漏洩した場合、不正なデータの書き込みなど悪用される恐れがあり、鍵管理は重要である。以下に鍵管理において検討すべきポイントを示す。

表 4-14

No.	検討ポイント	内容
1	鍵管理者	各社の鍵を誰が管理するのか？ セキュリティ・データ主権の観点より**「各社にて管理」**が適切と考える。
2	管理場所	各社の鍵をどこに保管するのか？ **外部からのアクセスが制限可能な場所**に保管する。 また、アプリケーションやBCのノードなど、**通常のアクセスが行われる場所には保管しない。** 鍵へのアクセスは、それを利用する**アプリケーションのみに許可する。**
3	管理方法	**暗号強度の高い鍵**を利用。 また、**鍵のローテーション**を行う（鍵漏洩、暗号危殆化等への対応）。 ただし、BCの製品ごとに使用可能な暗号方式やローテーション可否が異なる点に注意する。

<鍵管理イメージ>

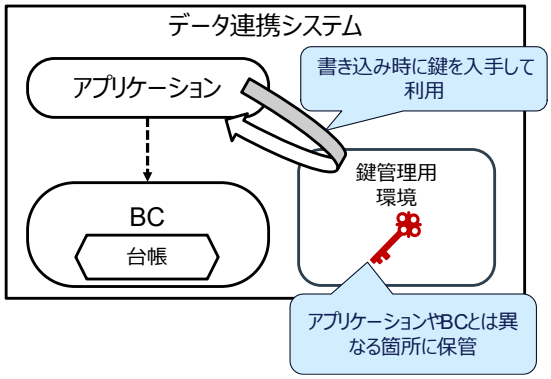


図 4-13

4.3.4.3 暗号化

秘匿性確保のための方法として「データの暗号化」が考えられる。ただし、BC 自体には格納データを暗号化する機能は一般的には備えていないため、実現にはアプリケーション等での対応が必要となる。

表 4-15

No.	目的	暗号化適用方法	BCにおける対応
1	データの保護強度を向上させる	データを暗号化した上で共有する。	特に無し（暗号化されたデータを格納するのみ）
2	回答相手先の指定を誤った際の漏洩リスクを低減する	当該事業者間のみが知りうる暗号鍵にてデータを暗号化した上で共有する。 回答相手先を誤った場合は、暗号化されたデータが共有されるものの、中身は見ることができない。	特に無し（暗号化されたデータを格納するのみ）
3	回答データ内容を誤った際の漏洩リスクを低減する （相手先は正しい）	暗号化では漏洩は防止できない。	ー

4.3.5 ブロックチェーンノード構成の検討

秘匿性や性能といった観点で、BC のノード構成を検討する必要がある。

4.3.5.1 ブロックチェーンのトリレンマ

ブロックチェーンのトリレンマとは、イーサリアムの開発者 Vitalik Buterin が提唱したとされている概念で、「分散性」「スケーラビリティ」「セキュリティ」の 3 つを同時に実現できないことを指す。

- 分散性とセキュリティを確保しようとした場合

  分散性に関しては多数のノードを配置することで非中央集権構造となり分散性は確保できる。また、セキュリティに関してはノードが多数存在することで悪意のある攻撃への耐性が高まり、セキュリティが確保できる。一方、ノードを分散させることにより、全ノードのネットワーク同期等に時間的なコストが生じ、処理速度が低下することでスケーラビリティは犠牲になる。

- スケーラビリティとセキュリティを確保しようとした場合

  スケーラビリティに関しては少数のノードでの構成や、役割を持った信頼できるノードに処理を任せることにより比較的処理が高速に行われ高いスケーラビリティを実現できる。また、セキュリティに関しては信頼できるノードで構成することで確保できる。一方、少数のノードでネットワークを構成するため分散性は犠牲になる。

- 分散性とスケーラビリティを確保しようとした場合

  分散性に関しては多数のノードを配置することで非中央集権構造となり分散性は確保できる。また、スケーラビリティに関しては合意形成を特定のノードのみで行うなどのアルゴリズムを選択することで実現できる。一方、障害点が特権ノードに集中するためセキュリティの観点では悪意のある攻撃への耐性が低くなる。

「分散性」「スケーラビリティ」「セキュリティ」のうちエンタープライズ利用において最優先とするべきは「セキュリティ」と考えられる。したがって、「分散性」と「スケーラビリティ」のトレードオフを考慮した着地点を求めることが重要となる。

4.3.5.2 オラクル問題

- オラクル問題とは

  「BC に登録する際に、BC 外のオフチェーンデータが正しいことをどのように担保するか」という問題である。 オンチェーンとオフチェーンを繋ぐ役割を持ちスマートコントラクトに外部の情報を提供するサードパーティ製のサービスのことをオラクル[8]という。外部情報を共通の事実としてスマートコントラクトの判断条件に用いるような場合には必要となる。

- 集権型オラクルと分散型オラクルの選択

  オラクルには大きく分けて集権型オラクルと分散型オラクルが存在し、それぞれオラクル問題を考える上で課題がある。

  集権型オラクルにおけるオラクル問題では、単一のオラクルおよび情報提供元を信頼しなくてはならないという課題がある。この課題の解決策としては以下が考えられる。

  - 集権型オラクルでデータの参照を複数の情報提供元から行う
  - 分散型オラクルで互いのノードを相互に監査することにより、意図的なインプットデータの改ざんを防ぎ、異常値の検知性を上げる

  一方で、分散型オラクルにおけるオラクル問題では、単一のオラクルおよび情報提供元を信頼する必要は無く、オラクル自体が単一障害点となることを防げる反面、一般的に集権型オラクルよりもコストがかかるという課題がある。コストを抑えるためにはオラクルおよび情報提供元の数を減らす、あるいは集権型オラクルでも安定稼働しているサービスを信頼し、コストメリットを享受する方針を取ることが必要である。

  以上のことから、集権型オラクルと分散型オラクルともに利点と課題が存在するため、要件に応じて柔軟に選択することが重要である。

[8] 企業名の「Oracle」を指すものでは無い点に注意する。

4.3.5.3 コンテナの利用

分散性と性能はトレードオフとなるため、参加者が多数いる場合はノード数への配慮が必要になる。各参加者の台帳を同一ノードにコンテナとして配置することで、台帳を分離しつつノード数を削減できる。しかし、その場合はコンテナノードを他社と共有することとなり、アプリケーションレベルでの論理的制御となるため、秘匿の厳密性が求められる場合はコンテナを採用することは適していない。

4.3.5.4 合意形成への参加有無の判断

各参加者は、BC の合意形成に参加するかどうかを選択できる。 合意形成に参加することで、BC ネットワークがより信頼できるものとなるが、 その反面、安定運用への責任が生じる。また、合意形成に参加しない場合に比べてノードの運用コストも上がる。 各参加者は、このトレードオフを考慮して合意形成に参加するかどうかを決定すべきである。

4.3.6 改ざん防止の実現

本節では改ざん防止を実現するための方法について示す。

4.3.6.1 耐改ざん性の特性

「2.5.1.1.1 完全性（耐改ざん性）」の通り、BC はデータの改ざんを極めて困難にする特性を有し、高い耐改ざん性を持つ。

4.3.6.2 改ざん検知の実施

BC は改ざんを検知可能な技術であるが、一般的に改ざん検知機能自体は備えていない。このため、真に改ざんを防止するには、改ざん検知を実施する必要がある。

具体的には、ハッシュ値を検証する機能を用意し、データの検証を行う。

ただし、BC の仕様上、運用期間が長くなるにつれてチェーンが肥大化し、それに伴い検証するハッシュ値も個数が増加するため、頻繁なハッシュ値の検証は処理速度の低下を招くことが予想される。 そのため、ハッシュ値検証の頻度に関しては調整していく必要がある。

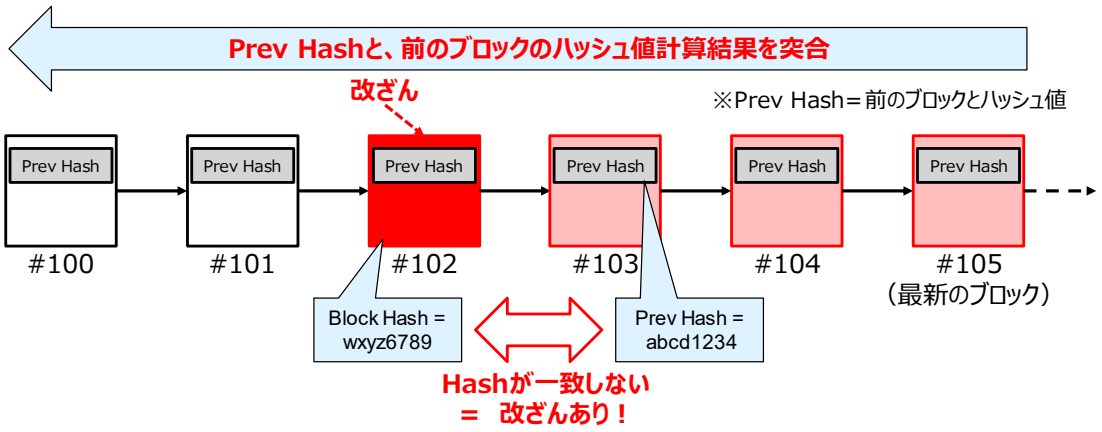


図 4-14

4.3.7 処理ロジックの透明性と確実性

「2.3.3 スマートコントラクト（自動執行）」の技術特性により、BC 上の処理について、ロジック透明性と確実性を実現できる。

一方で、「4.2.2.1 性能リスク一覧」の通り、スマートコントラクトの実行には性能面でのリスクが存在する。特に高負荷の処理や複雑な計算が要求される場合、BC の性能がボトルネックとなり、処理の実行速度が遅延する可能性がある。

こうした性能面のリスクを考慮すると、CE 情報流通 PF においては、以下のような観点を考慮してスマートコントラクトを利用することが推奨される。

- 同一処理の保証が必要な処理を対象

  スマートコントラクトを利用することで、事業者間で同一の処理を保証できるため、合意事項が確実に実行される必要がある処理を対象に利用することが有効である。

- 高負荷や複雑な処理の回避

  データの共有のみなど軽量な処理のみをスマートコントラクトで実装し、透明性と確実性と信頼性を確保する。一方で、高負荷の処理や複雑なロジックはオフチェーンで実装することにより、性能リスクを軽減する。

- 汎用性の確保

  一度デプロイしたスマートコントラクトは更新できないため、汎用性の高いスマートコントラクトを設計することで、他の業務や業界にも容易に転用できるようにする。

これらの観点に基づくスマートコントラクトの利用は、CE 情報流通プラットフォームにおける処理ロジックの透明性と確実性を高めるために重要である。

また、スマートコントラクト開発の注意点は、「5.1.4　スマートコントラクト開発時の注意点」を参照されたい。

4.4 ブロックチェーンに格納する情報に関する要件

本節では、まず、一般的な BC の特性を踏まえ、BC に格納する（オンチェーン）データと、BC に格納しない（オフチェーン）データとの使い分けの必要性を示す。また、オフチェーン格納時のハッシュ値の利用方法についても示す。その後、CE 情報流通 PF において、情報の格納先に関する要件について示す。

4.4.1 オフチェーンとは

BC には耐改ざん性などの利点がある反面、サイズの大きいデータを格納するのには向かず、検索性能は一般的に低いという欠点がある。これらの決定を補うため、BC に格納する（オンチェーン）データと、BC に格納しない（オフチェーン）データとの使い分けをする方法がある。

なお、オフチェーンという用語は、一般に BC に格納しない場合全般を指すこともある。しかし本書では、データの性質上、BC への格納が適さない場合や BC との併用によるメリットが考えられる場合などに利用する対象をオフチェーンとして定義する。

4.4.2 ハッシュ値の利用

BC では、業務データをオフチェーンに格納し、そのハッシュ値を BC（オンチェーン）に格納するという使い方がある。この利用方法とメリット・デメリットについて示す。

4.4.2.1 ハッシュ値の利用方法

オフチェーンおよびハッシュ値の利用方法について以下に示す。

- 組成データの書き込み時は、オフチェーン（BC 以外の格納場所）に組成データを格納し、そのハッシュ値をオンチェーン（BC）に格納する。

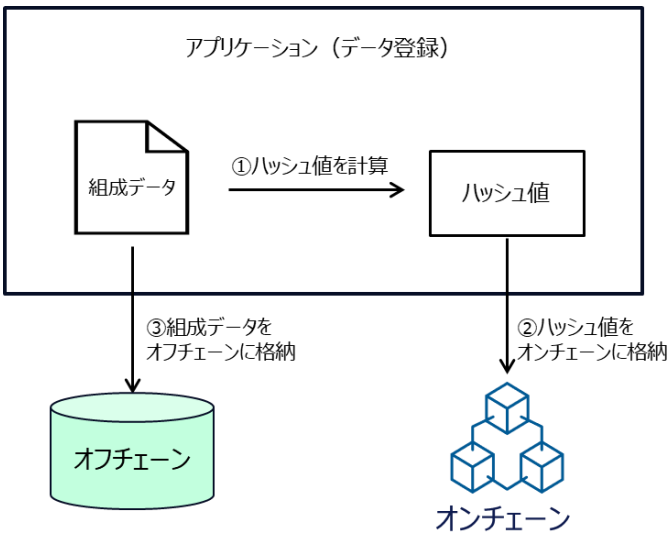


図 4-15

- 組成データの読み取り時は、オンチェーン（BC）に格納されたハッシュ値と、オフチェーン（BC 以外の格納場所）の組成データから計算したハッシュ値の一致を確認して用いる。

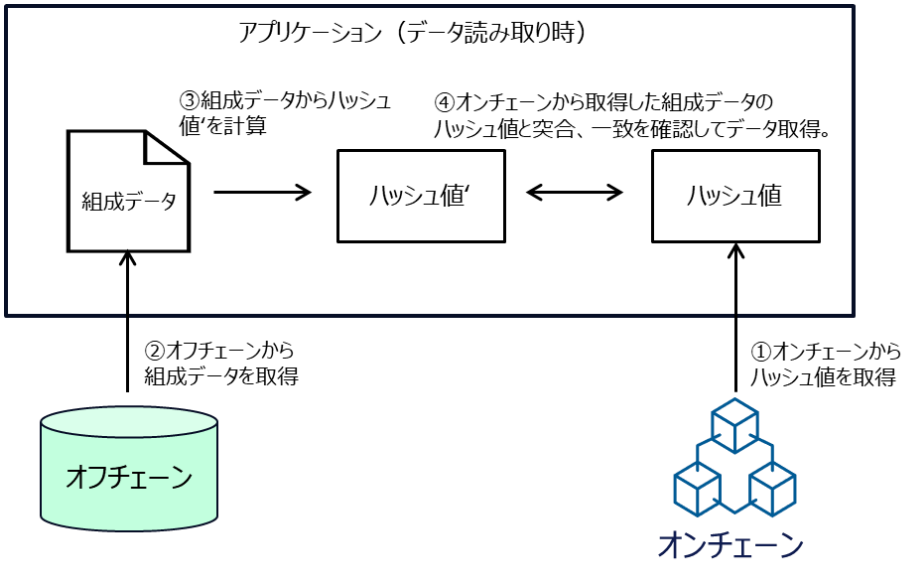


図 4-16

4.4.2.2 ハッシュ値利用のメリット･デメリット

ハッシュ値の利用においては技術的な BC の弱点を克服することが期待される一方、デメリットも存在する。

- メリット
  - 耐改ざん性

    組成データから計算したハッシュ値を BC に格納することにより、これらは改ざん不可能な情報となる。BC に格納したハッシュ値と、オフチェーンのデータから計算したハッシュ値の一致を確認することで改ざんされていないことが証明できる。

  - データ削減

    容量の大きいデータをオフチェーンに格納、そのデータのハッシュ値のみをオンチェーンに格納することにより、オンチェーンのデータが削減され、BC のデータサイズの制限を解決できる。

  - データ削除の実現

    オンチェーンのハッシュ値から組成データを復元することはできないので、オフチェーンに格納した組成データ本体を削除することで実質的なデータ削除が可能となる。

- デメリット
  - 制御部分の開発

    組成データのハッシュ値計算、オフチェーンへの格納・取得、オンチェーンおよびオフチェーンデータ間での整合性の確保等の BC に標準では実装されていない制御部分の開発が必要となる。この時、耐改ざん性を保証するための品質が求められる。

  - 性能面への影響

    ハッシュ値計算等の処理が制御部分に新たに追加となるため、それに伴う性能面への影響を考慮する必要がある。

4.4.3 ブロックチェーンに格納しない（オフチェーン）データの必要性

「2.5 非機能面における利点と課題」で示した通り、BC には耐改ざん性などの利点がある反面、データの削除ができず、データの更新頻度が高い場合は処理が間に合わない等の欠点がある。

BC にはこれらの特性があるため、全ての情報を BC に格納することは推奨されず、BC に格納しない（オフチェーン）情報と使い分けることが必要になる。

4.4.4 情報の格納先に関する要件

CE 情報流通 PF において、BC と BC 以外のどちらに情報を格納するか検討する場合、格納したい情報に対して、以下の観点を検討すべきである。

- 情報共有の必要性：他社へその情報を共有する必要があるか
- 情報の性質：改ざん防止の要求が高い情報、格納後に削除を考えている情報や、頻繁に更新を考えている情報といった情報性質があるか

4.4.4.1 情報共有の必要性に基づく格納先

前節で示した通り、BC へ格納した情報は共有データとなるため、共有を必要とする情報を BC へ格納し、それ以外は BC 以外へ格納すべきである。そのため、CE 情報流通 PF においては、以下のような使い分けが考えられる。

- BC へ格納すべき情報：他社へ共有する情報（規制物質に関する組成情報等）
- BC 以外へ格納すべき情報：上記以外の個社内でのみ利用する情報（ユーザ情報、開示前の組成情報等）

4.4.4.2 情報の性質に基づく格納先

以下のような BC の利点を活かせる性質を持つ情報は、BC へ格納する。

- 改ざん防止の要求が高い情報

  事業者間で伝達する情報は、伝達の証跡としての性質があり改ざん防止の要求が高いと考えられる。また、長期保管という観点においても、長期間安全にデータを保管することが求められる情報は、改ざん防止の要求が高いと考えられる。

「4.4.4.1 情報共有の必要性に基づく格納先」で示したような共有を必要とする情報であっても、以下の性質を持つ情報は、BC 以外への格納を検討すべきである。

- 一定量を超えるサイズのデータ

  BC に問題なく格納できるデータのサイズは、製品により差異があるもののおおよそ数 KB 程度であることが多い。これを上回るサイズのデータを扱う場合には、BC とオフチェーンストレージを組み合わせることが考えられる。この組み合わせでは、BC が耐改ざん性を担い、オフチェーンストレージが実際の情報の保管を担う。この時、BC には実際のデータのハッシュ値を格納する。ハッシュ値の利用については「4.4.2 ハッシュ値の利用」参照。

- 検索の柔軟性を求められるデータ

  一度 BC に格納されたデータは、スマートコントラクトの I/F として定義された検索手段でしか検索ができず、リレーショナルモデルを検索する際の SQL のような柔軟なクエリは不可能である。そのため、どのように検索するか事前に決定できないような情報は BC 以外に格納すべきある。

- 格納後に削除が必要なデータ

  一度 BC に登録された情報は消去できないため、後から完全消去することが必要なデータはオフチェーンに格納し、データのハッシュ値のみをオンチェーンに格納する方法がある（「4.4.2 ハッシュ値の利用」参照）。

- 更新頻度が高いデータ

  BC は一般的に更新処理性能が高くないため、短時間に多くのデータの登録や更新が発生する場合に性能問題が発生する可能性がある。オフチェーンに複数データを格納した後、まとめて BC に登録するような方法が考えられる。

4.5 認証方式に関するブロックチェーン要件

本節では、CE 情報流通 PF において信頼性の担保された情報をやり取りするために重要な認証方式に関する BC 要件について示す。

4.5.1 認証方式の要件検討

CE 情報流通 PF においては、信頼性の担保された情報をやり取りすることが求められる。そのためには、「4.1 ブロックチェーン適用に関する要件」に記載の通り、通信先の信頼性とデータの信頼性の 2 つを担保する必要がある。

また、CE 情報流通 PF においては、データの所有者は個人ではなく事業者であり、トラストレイヤで事業者認証を実施することが想定される。

4.5.2 認証方式の要求実現

信頼性の担保された情報のやり取りを行うためには、通信先の信頼性とデータの信頼性の 2 つを担保する必要がある。本節では、通信先の信頼性担保の実現方法について示す。データの信頼性担保については、「4.3 情報漏洩・改ざんを防止するブロックチェーン要件」で示す。

4.5.2.1 要求実現：通信先の信頼性

4.5.2.1.1 ブロックチェーンにおける通信先の信頼性担保

BC においては、一般的にユーザごとにキーペア（公開鍵と秘密鍵）を生成し、公開鍵暗号方式によってユーザの認証が行われる。そのため、BC 上ではそのユーザの秘密鍵を保有（アクセス権を保有）していることが、そのユーザであることの証明となる。

通信先の信頼性を担保するためには、認証認可により各ユーザの秘密鍵には、そのユーザしかアクセスできないようにする必要がある。

4.5.2.1.2 CE 情報流通 PF における通信先の信頼性担保

CE 情報流通 PF において、データの所有者が事業者単位であることを考慮すると、事業者単位でキーペア（公開鍵と秘密鍵）を生成することが推奨される。また、トラストレイヤにおける事業者認証など信頼のおける認証結果に基づき、各事業者の秘密鍵へのアクセス権を付与することが重要である。これにより、事業者に対して信頼性を担保した形で秘密鍵へのアクセス権を付与することが可能となり、通信先の信頼性を担保できる。

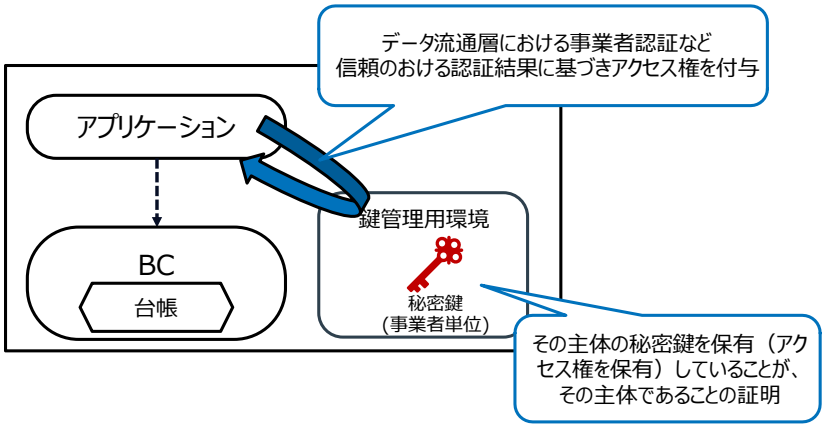


図 4-17

なお、秘密鍵の管理方法については、「4.3 情報漏洩・改ざんを防止するブロックチェーン要件」で示している。

4.5.2.2 要求実現：DID/VC の利用検討

通信先の信頼性とデータの信頼性の担保方法として DID（Decentralized Identifier）/VC（Verifiable Credential）[9]の利用が検討される。共有先の信頼性については、「ウラノス・エコシステム」に準拠したアーキテクチャおいて事業者の認証が実施されるため、DID/VC の必要性は低い。一方で、対外連携においては、事業者情報を共有するためのプロトコルとして VC の利用について検討の余地がある。

データの信頼性の担保に関しては、「1.6.3 クローズドループ」で記載の通り、信任された限られたプレーヤ間で供給網を構築されるクローズドループにおいては、事業者間の契約により信頼性が担保される。このため、DID/VC のシステムによって担保する必要性は低い。一方で、オープンループにおいては、そのような体制が整っていないため、第三者機関によってデータの信頼性を担保する必要がある可能性があり、DID/VC の利用について検討の余地がある。

4.6 可用性に関するブロックチェーン要件

本節では、CE 情報流通 PF における可用性についての BC の要件を示す。

4.6.1 可用性の要件検討

BC システムにおいては、各ノードが分散してデータを管理しているため、優れた可用性の仕組みを持つ。一方で、利用する BC 基盤やコンセンサスアルゴリズムによっては、単一障害点となるコンポーネントも存在する。

CE 情報流通 PF では、BC システム特有の単一障害点について対処を考慮しておくことが望ましい。

4.6.2 可用性の要求実現

BC における可用性を確保する観点としては、ノードの可用性とデータの可用性の 2 つが存在する。

- ノードの可用性：BC ネットワークを構成する各ノードの可用性
- データの可用性：BC 上でやり取りされるデータに対する可用性

それぞれについて、単一障害点に関する考慮点を示す。

4.6.2.1 実現方式：ノードの可用性

単一障害点になる可能性があるノードとしては以下の 2 つが挙げられる。

---

[9] DID（Decentralized Identifier）：分散型 ID。
VC（Verifiable Credential）：検証可能なデジタル証明書。

- トランザクション発行ノード

  トランザクション発行ノードとは、「2.5.3.2.1 トランザクション発行ノードの可用性確保」で述べた通り、BC に対してトランザクションを発行するノードであり、エンタープライズでの BC 利用のユースケースにおいては、各事業者がノードを保有し、管理することが多い。このノードは、アプリケーションから各社の処理を受け付けるノードであるため、システムの設計によっては単一障害点となる可能性がある。

- BC 特殊ノード

  BC 特殊ノードとは、「2.5.3.2.2 ブロックチェーン特殊ノードの可用性確保」で述べた通り、ブロックを作る機能やネットワーク全体の二重取引を監視する機能などの権限が集中したノードのことを指す。この BC 特殊ノードについては、BC ネットワーク全体における単一障害点となる可能性がある。

このような単一障害点となり得るノードについては、冗長化することが望ましい。ノード冗長化の方法については、以下の方法が考えられる。

4.6.2.1.1 複数ノード構成

ノードを複数構築し冗長化する方法である。これにより、トランザクション発行ノードや BC 特殊ノードの停止による BC システムの停止の可能性を低減することが可能である。この際、自然災害に備え、ノードを地理的分散し配置することも有効な手段である。一方で、トランザクション発行ノードの冗長化については、ノード間の通信増加による性能劣化発生の可能性や各事業者のノードの運用コスト増加といったデメリットも存在する。ノード間の通信増加に対しては、他のノードとの通信をするなどの対策が考えられる。ノードの運用コストの増加に対しては、コストと可用性のトレードオフを考慮した判断が必要となる。

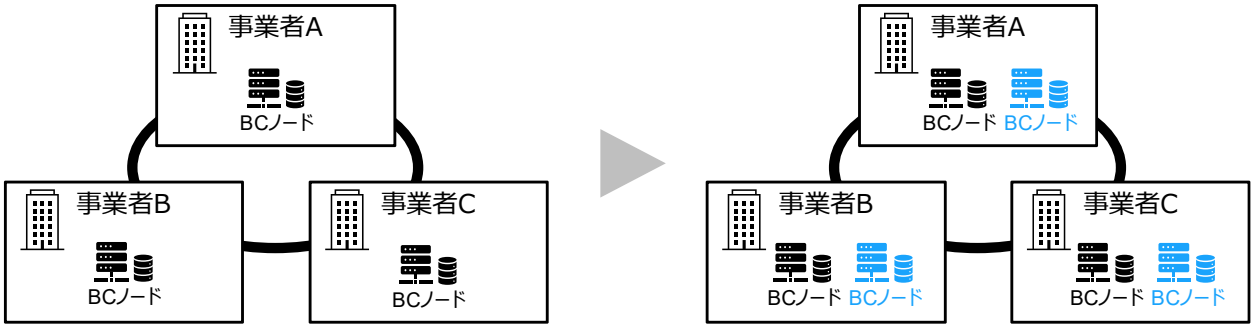


図 4-18

4.6.2.1.2 コンテナオーケストレーションの導入によるノードの自動復旧

コンテナオーケストレーションは、ノードの自動復旧を実現するための効果的な手段である。コンテナオーケストレーションツールは、ノードの状態を常時監視し、異常が検知されると自動的に再起動や再配置を行う。この自

動化されたプロセスにより、手動での復旧作業が不要となり、ダウンタイムを最小限に抑え、システムの可用性を向上させることが可能である。

4.6.2.2 実現方式：データの可用性

一般的に BC においては、同じデータを全ノードで持ち合うため、高いデータの可用性を有している。そのため、BC 上に存在しないオフチェーンデータや秘密鍵などのデータをバックアップすることが重要である。一方で、BC 基盤や設計によっては、データが一部のノードにしか保存されない場合が存在する。特に、秘匿データを扱える基盤においては、秘匿データは特定のノードにのみ保存される。そのため、各ノードでデータのバックアップを取っておくことが重要である。

4.7 運用・保守性に関するブロックチェーン要件

本節では、CE 情報流通 PF における運用・保守に関する要件を示す。この運用・保守の主体としては、運営事業者と各事業者の 2 種類が考えられ、それぞれの主体に対して運用・保守の要件を示す。

4.7.1 各事業者の運用・保守に関する要件

各事業者が運営するノードに対して、運用・保守の要件を示す。

4.7.1.1 通常運用に関する要件

各事業者が事業者ノードを日々運用していく上で考慮すべき要件について記載する。

4.7.1.1.1 運用時間

CE 情報流通 PF は、海外接続を考慮し極力システムの稼働は継続させる必要がある。そのため、各事業者のノードは、基本的に 24 時間 365 日間、安定稼働できることが推奨される。

4.7.1.1.2 バックアップ

CE 情報流通 PF では、各事業者ノードがバックアップを取得しておくことが推奨される。バックアップの必要性については、「4.6.2.1 実現方式：ノードの可用性」を参照。

4.7.1.1.3 運用監視

各事業者ノードは、安定運用のため、パフォーマンスと稼働状況をリアルタイムで監視できることが望ましい。そのため、以下のような一般的な BC の監視項目を監視しておくことが推奨される。

- CPU 使用率・メモリ使用率：処理速度に影響するため監視しておくことが望ましい。
- ディスク使用率：台帳のデータがディスクを圧迫しやすいため監視しておくことが望ましい。

- コンセンサスの状態：自社のノードがネットワークに参加できているかを確認するために監視しておくことが望ましい。
- スマートコントラクトのログ：スマートコントラクトの処理結果を確認するために監視しておくことが望ましい。
- 秘密鍵へのアクセスログ：不正な秘密鍵へのアクセスを防ぐために監視しておくことが望ましい。

4.7.1.2 保守運用に関する要件

各事業者が各事業者ノードを改修・調整する際に考慮すべき要件について記載する。

4.7.1.2.1 システム改修

各事業者ノードでは、システム改善のため、アプリケーション、OS、BC 基盤の改修が想定される。各事業者ノードを改修・調整する場合、必要に応じて計画停止を行い、改修・調整ができるように検討すべきである。

4.7.1.2.2 スマートコントラクト変更

CE 情報流通 PF では、スマートコントラクトに対して、各事業者が独自にロジック変更などの改修・調整をできないようにしておくべきである。このスマートコントラクトの変更に関しては、運営事業者が運用することが望ましく、詳細は「4.7.2.3 合意形成を伴うスマートコントラクト変更」を参照。

4.7.1.2.3 履歴データ容量の削減

各事業者ノードでは、データの無制限増大を防ぐため、定期的に BC の履歴データを削除する運用を検討しておくことが望ましい。履歴データ削除の実現方式については、「4.2.2.2.5 履歴データ容量の削減」参照。

4.7.1.3 障害時運用に関する要件

4.7.1.3.1 ノードの復旧

各事業者ノードでは、プロセスダウンやデータ消失などの障害により、最新の台帳と差分が生じる可能性がある。この差分が生じた場合に、最新の状態に復旧するための運用を検討しておくべきである。このノード復旧の実現方式としては、ノードをバックアップからリストア後、他ノードとの同期が考えられる。1 つのノードのデータが消失した際に、他ノードが持つデータと同期を取ることで最新の状態への復旧が可能となる。ただし、他ノードとの同期については、他事業者の協力が必要となる点に注意する。

4.7.2 運営事業者の運用・保守に関する要件

運営事業者が BC 全体を運営する場合に考慮すべき要件について記載する。

4.7.2.1 事業者追加・削除

CE 情報流通 PF は、参加事業者が拡大していく計画であり、事業者の追加・削除が適宜行われることが想定される。多数の事業者が参加するため、参加事業者の拡張操作が効率的に実施できるような仕組みを検討しておくことが望ましい。この効率的な仕組みの 1 つとしては、コンテナ運用による負荷軽減が考えられる。コンテナオーケストレーションサービスを利用して複数ノードを一括で管理することでノード追加・削除を効率的に実施することが可能となる。

4.7.2.2 監視対応

CE 情報流通 PF における BC では、コンセンサスの状態やクリティカルな障害点となるノードについては、運営事業者が把握し対応できる必要がある。そのため、これらのノードの運用を各事業者単位で行っている場合であっても、運営事業者が保守・障害対応できるような運用を検討しておくことが重要である。

4.7.2.3 合意形成を伴うスマートコントラクト変更

CE 情報流通 PF における BC では、スマートコントラクトの変更時、より分権的にするため、各事業者のしかるべき合意をもって変更をすることが望ましい。このスマートコントラクト変更の実現方式については「5.1.4 スマートコントラクト開発時の注意点」参照。

4.7.2.4 ブロックチェーンシステム全体の復旧

CE 情報流通 PF における BC では、大規模障害による全ノードのブロック生成が停止するような障害が発生した場合に復旧できる必要がある。復旧方式としては、全ノードをバックアップから復旧後に各ノード間で同期を取ることが考えられる。この方式を取る場合、各参加事業者の間で合意形成が必要である。

4.7.2.5 ブロックチェーン特殊ノードの運用保守

CE 情報流通 PF において、BC 特殊ノードの運用・保守は運営事業者が行う必要がある。そのため、運営事業者は BC 特殊ノードの運用・保守について検討しておくことが重要である。例えば、BC 製品によっては、認証局を担う BC 特殊ノードが存在し、以下のような運用を検討する必要がある。BC 特殊ノードについては「2.5.3.2.2 ブロックチェーン特殊ノードの可用性確保」を参照。

- 新規ノード構築時の初期ユーザ・秘密鍵の払い出し
- 秘密鍵紛失時の再払い出し
- 署名書の有効期限が切れた場合の更新対応
- 証明書が失効した際の運用

5 ブロックチェーン技術利活用時の注意点・考慮事項

5.1 ブロックチェーン技術を利用・開発する上での注意点

5.1.1 ブロックチェーン基盤の選定

「2.5.5.2.1 ブロックチェーン間での移行の困難さ」で述べた通り、BC 間での移行が困難である。そのため、プロジェクトの要件に適した BC 基盤を選定することが極めて重要である。BC の基盤選定に際しては、単に機能の適合性だけではなく、長期間の運用を考慮し、サポート体制や将来の製品ロードマップも考慮することも重要である。

5.1.2 海外事業者参画時の考慮事項

CE 情報流通 PF では、海外事業者が参画して事業者ごとにノードを保有するケースがある。海外拠点にノードや台帳のデータを配置する可能性がある。海外の拠点にノードを配置する際の注意点について示す。

- 法令準拠：法令によってデータを全て自国内に置く必要があるなど、物理的な配置箇所が限定される場合が考えられる。
- 距離的要因による性能劣化：海外拠点のノードをコンセンサスに含める場合、距離的要因により通信速度の低下が考えられる。

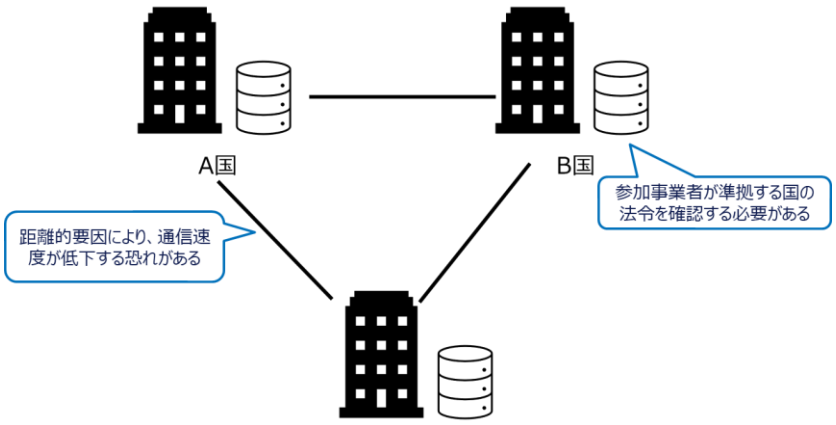


図 *5-1*

5.1.3 ノード管理に関する考慮点

CE 情報流通 PF においては、多数の参加者が想定されており、中小事業者などの BC ノードの運用が負担となり、管理が困難な事業者が存在することが予想される。このような中小事業者からの BC 以外で情報連

携を受けるための方策が必要となる。ノードを保有できない事業者と取引関係にある事業者がファイル授受等により情報連携を受け代理登録する方法や、共同のサーバを構築する方法などが考えられる。

5.1.4 スマートコントラクト開発時の注意点

一般的にスマートコントラクトは一度デプロイされると、そのコードを更新できないため、バグの修正や機能改善が困難である。そのため、開発においては以下のような考慮点が必要である。

5.1.4.1 柔軟なスマートコントラクト設計

スマートコントラクトは更新できないため、拡張性や将来のロジック更新に備えた設計が重要である。BC の基盤によってロジック更新可能な設計方法は異なるが、プロキシコントラクトの利用が一例として挙げられる。プロキシコントラクトとは、トランザクションを別のコントラクトに転送するコントラクトである。ロジックを更新したい場合は、プロキシコントラクトがトランザクションを転送する先を新たなコントラクトに変更することで、ユーザから呼び出すコントラクトは同一のまま、ロジックが更新することが可能である。また、スマートコントラクトの一時停止など利用を制限するための設計を検討することも重要である。

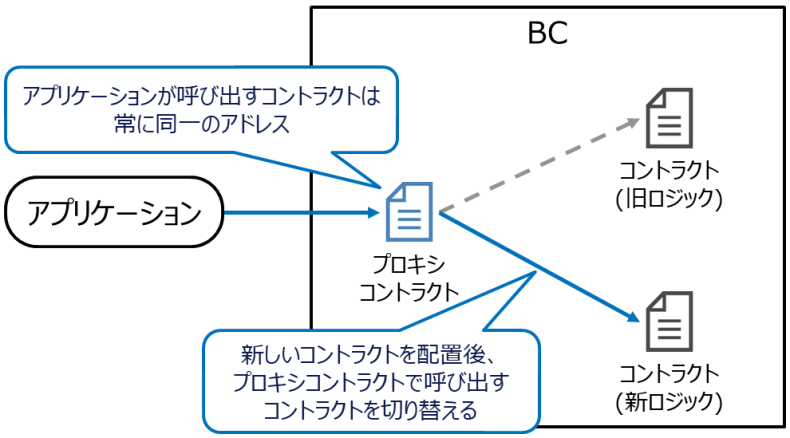


図 5-2

5.1.4.2 セキュリティ監査の活用

スマートコントラクト開発においては、初期段階での徹底したセキュリティ対策が重要である。そのためには、第三者によるセキュリティ監査など専門機関によるコード監査を受けることも有効である。

5.1.4.3 ブロックチェーン有識者のアサイン

スマートコントラクトの開発には高度な専門知識が必要であり、プロジェクトの各フェーズ（設計、実装、テスト、監査）において、BC 技術やセキュリティに精通した専門家をアサインすることが求められる。また、チーム内の技術者のスキルアップを図るため、定期的な教育や研修を実施し、最新の技術やセキュリティ知識を習得させることも重要である。

5.2 CE 情報流通 PF の普及展開に関する課題への対応策

本節では、CE 情報流通 PF の普及において想定される課題をリストアップし、その解決方法を検討し対策案を示す。

5.2.1 オンボーディング

CE 情報流通 PF において、事業者の PF への参画障壁が大きいと普及展開に支障が出る。この課題を解決するため、オンボーディング（新規事業者の PF への適応を促進する活動）のハードルが高くならないような注意が必要である。例えば、既存システムから CE 情報流通 PF に全面的に乗り換えるのではなく、既存システムを活用しつつ CE 情報流通 PF を使ってもらうといった既存システムとの並行運用を想定した設計思想が重要である。

5.2.2 相互運用性

BC を外部システムと接続するケースが考えられる。この点について、当初から検討しておく。

外部システムとの接続を実現させる方法の選択肢として、BC レイヤの接続、アプリケーションレイヤの接続が考えられる。

- BC レイヤの接続

  2 つの BC 間での相互運用となるが、ほとんどの BC は相互運用が考慮されていない。相互運用に特化したミドルウェアか、相互運用機能を持つ BC を別途導入する。

- アプリケーションレイヤの接続

  BC と従来型システムの間で、データ共有のための分散トランザクションを実現する必要がある。この際、BC と従来型システムでは、データの取り扱いモデルやトランザクション処理時間が大きく異なることを考慮する必要がある。例えば、BC はロールバックができず、トランザクション処理に数秒程度かかることを考慮した上での分散トランザクションとなる。このために、独自の実装（上記のような SDK 提供）、ミドルウェアの導入を行う。

5.2.3 継続性

CE 情報流通 PF の普及展開において、システム改善や機能拡充の継続性が課題である。そのため、CE 情報流通 PF では、BC 製品選定において、継続性（開発体制・規模、サポートなど）や実績の評価をしておくことが重要である。

また、業界・業務の拡大に繋げるため、BC を信頼性の高いデータ共有の仕組みとして汎用的なアーキテクチャで活用することで、アーキテクチャを横展開可能なものとすることも検討するべきである。

5.3 海外の類似・関連システムとの連携

本節では、海外のデータプラットフォームに関する事例を踏まえて、将来的に相互連携するために検討するべきことを示す。

5.3.1 類似・関連システム

データプラットフォームに関する海外の取り組み事例として、欧州におけるコンソーシアム Catena-X とモビリティにおける BC 推進組織 MOBI を取り上げる。

5.3.1.1 Catena-X

Catena-X はサプライチェーン全体でデータ連携可能な共通基盤の提供を目指しており、連携モジュールの標準化により各社が市場投入するまでの時間と実装コストを削減し自動車業界の競争力強化を実現することを目的としている。

表 *5-1*

2021 年 3 月	コンソーシアム設立
2023 年 1 月	Catena-X の運営・運用を担当する合弁会社 Cofinity-X 設立
2023 年 10 月	Cofinity-X がサービスを開始

Catena-X は通信コンポーネント標準 EDC（Eclipse Data Space Connector）を定義している。EDC は分散型であり各参加者は自身の側に EDC を設定することで他の参加者とのピアツーピア接続が可能となる。EDC を介してデータ交換することで Catena-X はデータ主権を確保している。データの所有者はその制御権を保持し、誰がデータ交換に関与するのか、どのように、いつ、どこで、どのような条件下でデータ交換が実現されるのかを個別に決定できる。

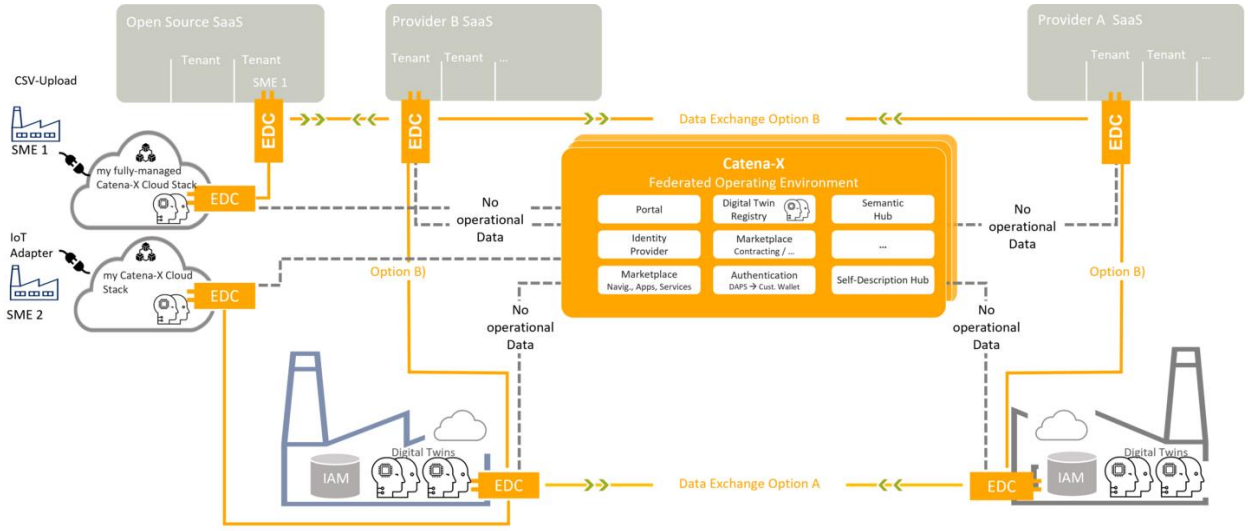


図 5-3

出典：EDC - The Central Component | Catena-X より引用
[https://catena-x.net/en/1/offers/edc-the-central-component]

5.3.1.2 MOBI

MOBI はモビリティ業界における BC 推進と標準規格策定に取り組むグローバルコンソーシアムである。全世界に 100 以上の会員事業者・組織を抱えており、メンバは自動車メーカーだけでなく金融機関、保険会社なども含まれる。自己主権型 ID のための標準とインフラ構築を推進することで、デジタル経済をより効率的、公平、分散化、循環型にすると同時に全ての人のデータプライバシが確保された社会の実現を目指している。

表 5-2

2018 年 5 月	発足
2019 年 9 月	自己主権型 ID の事例として車両 ID を定義し、複数の OEM と PoC を実施
2020 年 6 月	車両 ID を機能させるためのネットワークを稼働開始
2022 年 1 月	車両が排出する CO2 の正確な測定と収集の標準化のために欧州委員会とともに共同パイロットを実施
2024 年 4 月	MOBI と Gaia-X 4 moveID は、業界横断的な相互運用性を推進することを目的として共同で取り組むことを発表
2024 年 7 月	Web3 Global Battery Passport の MVP 開発マイルストーンを発表し、MOBI が定義するバッテリー出生証明書と W3C の自己主権 ID という標準を使用し、9 つの組織間でバッテリーID・データ検証と交換を実証したことを報告

バッテリーパスポート対応が直近の主な活動であり、DID/VC を活用してバッテリーパスポートクレデンシャルを発行するフロー例を提示している。

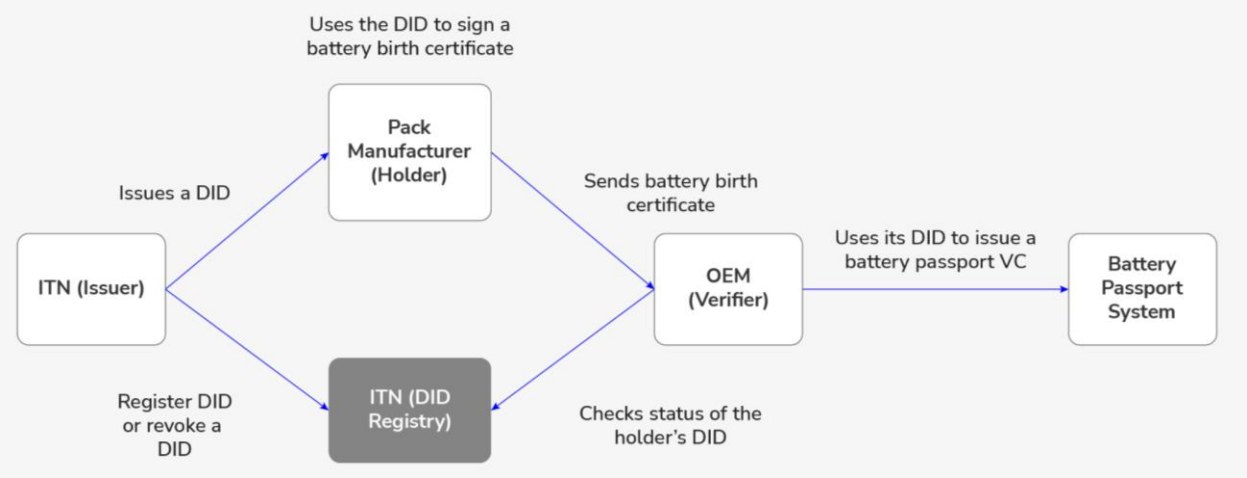


図 5-4

出典：GLOBAL BATTERY PASSPORT IMPLEMENTATION TECHNICAL GUIDANCE MOBI BP0001/TG/2023 Version 1.1 より引用
[https://dlt.mobi/wp-content/uploads/2024/10/MOBI-BP0001TG2023-Version-1.1.pdf]

5.3.2 海外事例を踏まえて、将来的な相互連携のための検討事項

本節にて取り上げた Catena-X や MOBI を始めとして世界には複数のデータエコシステム構想が進行中であるものの、それらは自身のエコシステム内におけるデータ主権の確保が重要視されておりエコシステムを横断した統一的なデータ交換の方法が確立されているわけではない。

5.3.2.1 エコシステム間連携に向けた取り組み事例

5.3.2.1.1 自動車業界向けデータ共有エコシステム間の相互運用性実証

IPA と Catena-X は自動車業界向けデータ共有エコシステム間の相互運用性を実現し、最終的には各自動車業界相互間でのデータ共有・利活用の実現を目指すことを目的として、両者の相互運用性の実現に必要な要件を評価し、検証を実施している。ここではシステム接続方法やユーザ認証方法、データ転送方法などが議論され、その結論として相互運用の実現可能性について発表がなされる予定である。

5.3.2.1.2 国連透明性プロトコル（UNTP）

UNTP は、サプライチェーンの追跡可能性と透明性を実現することによって、グリーンウォッシュに対抗するための実践的な対策で政府と業界を支援することを目的としている。そのためにはサプライチェーンを追跡可能かつ透明化することが求められるが、既存のソリューションの多くは特定のバリューチェーンにおける全ての関係者が同じプラットフォームに加入することが期待されている。これは実現可能性が高いとは言えないという指摘があり、

UNTP はサプライチェーンのデータは各所有者に保持されることを前提とし、プラットフォームに依存しない標準プロトコルを提供する。

5.3.2.2 将来的なエコシステム間の相互運用に向けて

現在は各エコシステムにおいて認証やデータ交換の手法が定義されているため、エコシステムを横断した統一的な方法は確立されていない。データ交換は一般的に通信相手の認証、データ転送の 2 段階で行われることになる。認証について W3C は検証可能な認証情報（VC）と呼ばれる標準を定義している。VC は発行者によってデジタル署名され、改ざん防止、プライバシ保護、取消可能、デジタル検証が可能であり、国境を越えた認証処理に有効であると考えられている。一方のデータ転送では Catena-X では EDC という独自のコネクタを用意することを求めていることやデータフォーマットも国際的に統一されているとは言えない状況にあり、エコシステム間の相互連携の面において課題となっている。その状況の中で各団体によってエコシステム間の相互運用性実証やプロトコル標準化の取り組みは現在もなお進められている。またデータ連携手法が技術的に確立されたとしても、特定の情報を外国に流通させることに対して各国政府が一定の制限を課すということも考えられる。以上を踏まえて、将来的にエコシステム間の相互運用が実現されることを見据えて、相互運用手段の標準化動向を注視し、その仕組みに容易に準拠できる形態であることが望ましい。

6 まとめ

本書では、資源の循環経済（サーキュラーエコノミー）のデータ流通を実現する「CE 情報流通 PF」を対象として、BC 技術を用いる際の利点と課題を踏まえた上で BC 技術を活用すべきかどうかを検討し、また BC 技術の適用範囲や活用方針を示した。

サーキュラーエコノミーにおいては、トレードシークレットを保証しつつデータを流通させることが求められる。その一方で、サプライチェーンの多数の事業者が利用することによる性能面の課題への対応や、規制等によるデータ長期保管のためのシステム持続可能性の確保なども求められる。

BC 技術は、その他の技術と比較して CE 情報流通 PF に最適と考えられる。一方で、セキュリティや性能などの様々な観点において対応すべき課題があるが、本書に示した対応策を検討することで、BC 技術を適切に利用するための一助とされたい。

なお、本ガイドライン別紙の「ブロックチェーン技術ガイドライン別紙　チェックリスト」に、本ガイドラインにて示した検討ポイントをチェックリストの形で用意しており、検討漏れ防止のために活用いただきたい。