

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)

公表用調査報告書

2025年2月

株式会社NTTデータ

【内容】

- ・ サーキュラーエコノミー情報流通プラットフォームの仕様の標準化に関する調査報告書
- ・ CMP 基盤/CMP アプリ標準仕様書別紙 非機能要件一覧
- ・ ブロックチェーン技術活用ガイドライン
- ・ BC 技術活用ガイドライン別紙 エグゼクティブサマリ

サーキュラーエコノミー情報流通プラットフォーム の仕様の標準化に関する調査報告書

2025年2月

株式会社 NTT データ

はじめに

本資料の位置づけ	<p>本資料は、令和 6 年 12 月 10 日から令和 7 年 2 月 28 日に実施された「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）」におけるプラットフォーム構築の仕様の標準化に関する調査報告書である。</p> <p>今後、サプライチェーン全体で幅広い業種の関与が予想される製品含有化学物質の情報伝達をユースケースとして、ウラノス・エコシステムと連携したサーキュラーエコノミー情報流通プラットフォームを実現するための仕様の標準化の調査を行った。</p> <p>なお、調査報告書には、本事業の期間（令和 6 年 12 月 10 日から令和 7 年 2 月 28 日）以後の状況変化については含まれていない。</p>
調査の目的	<p>2025 年度中のサーキュラーエコノミー情報流通プラットフォームの立ち上げを目指し、共通基盤に必要となる標準的な仕様を明確化することが、本調査の目的である。</p>
調査方法	<p>本調査では、多角的な視点と手法を取り入れることで調査結果の信頼性を高めることに注力した。具体的なアプローチは以下の通りである。</p> <ul style="list-style-type: none">・各業界ユーザで構成される CMP-TF との協議およびヒアリングを実施し、ユーザの実業務に即した標準仕様となっている事を確認した。また、CMP-TF におけるこれまでの検討結果である要件定義書（CMP システム要件定義書 v1.1）との整合性を確認した。・共通基盤と連携して動作するアプリケーション開発について知見のある企業数社と協議し、標準仕様に基づくプロトタイプを作成を通じて、技術的な実現性を検討した。・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）との整合性を確認した。・ウラノス・エコシステムのアーキテクチャとの整合性を確認した。・様々な製品・素材等のユースケースへの展開が可能な仕様であることを確認した。
調査結果	<p>デジタル・ガバメント推進標準ガイドライン準拠の「標準仕様書」として、調査結果をとりまとめたものを次頁から記載する。</p>

1 目次

はじめに.....	2
1 全体編	5
1.1 背景・目的	5
1.1.1 サーキュラーエコノミー情報流通プラットフォーム整備の目的	5
1.1.2 CE 基盤立ち上げに当たっての産官学の役割と取り組み	11
1.1.3 製品含有化学物質・資源循環情報プラットフォーム（CMP）構築の目的	12
1.1.4 標準仕様策定の目的と対象	13
1.2 CMP-製品含有化学物質・資源循環情報管理.....	15
1.2.1 製品含有化学物質・資源循環情報管理の目的と課題	15
1.2.2 製品含有化学物質・資源循環情報管理に関連する規制・業界基準	16
1.2.3 現状課題と対応方針	18
1.3 システム全体図.....	20
1.3.1 システム全体	20
1.3.2 業務全体	25
1.4 データの流れと機能構成.....	26
1.4.1 標準機能	26
1.4.2 標準データモデル.....	43
1.5 機能分割	73
1.5.1 機能分割方針.....	73
1.5.2 データ分割方針.....	74
1.5.3 機能構成図	75

2	機能編	76
2.1	機能一覧.....	77
2.2	機能別処理内容	80
2.2.1	インターフェース仕様	80
2.2.2	システム化対象業務フロー	83
3	データ編.....	101
3.1	データモデル.....	101
3.2	データ一覧.....	102

1 全体編

1.1 背景・目的

1.1.1 サークュラーエコノミー情報流通プラットフォーム整備の目的

■ 現代の社会課題とビジネスモデル変革の必要性

社会課題解決のため、サステナブルな社会への転換がグローバルで進んでいく中で日本が直面する危機への対応のためにも、サーキュラーエコノミー(CE)への転換を推進していく必要がある。

「環境」「社会」「経済」の好循環を生み出し、「サステナブル(持続可能)な社会」を実現することによる、「Planetary boundaries(地球の限界)を超えない活動の維持」と「Well-Being(幸福)の実現の同時達成」を目指す。



[出典]

経済産業省、成長志向型の資源自律経済戦略

<https://www.meti.go.jp/press/2022/03/20230331010/20230331010-2.pdf>

■ 成長志向型の資源自律経済の実現に向けた 3 つのギア

成長志向型の資源自律経済の実現に向けて、3 つのギアにより、日本における CE の市場化を加速し、成長志向型の資源自律経済の確立を通じて国際競争力の獲得を目指していく。

情報流通プラットフォームの構築は規制・ルール、政策支援、産官学連携いずれにおいても CE 実現に寄与することが期待できる。

成長志向型の資源自律経済の確立のトランスミッション：3つのギア

凡例： 本取り組みに関連する事項

政策措置をパッケージ化して、日本におけるCEの市場化を加速し、 成長志向型の資源自律経済の確立を通じて国際競争力の獲得を目指していく。		
ギア① 競争環境整備 (規制・ルール)	ギア② CEツールキット (政策支援)	ギア③ CEパートナーシップ (産官学連携)
<p>■ 4R政策の深掘り</p> <ul style="list-style-type: none"> ・循環配慮設計の拡充・実効化 ・循環資源供給の拡大：効率的回収の強化 ・循環資源需要の拡大：標準化・LCAの実装 ・表示の適正化：循環価値の可視化 ・CEコマース市場の整備：製品安全強化等 <p>■ 海外との連携強化</p> <ul style="list-style-type: none"> ・クリティカルミネラルの確保 ・規制・ルールの連携（プラスチック汚染対策（UNEP）、CEの国際標準化（ISO）、情報流通プラットフォーム構築等） 	<p>■ CE投資支援</p> <ul style="list-style-type: none"> ・研究開発・PoC(概念実証)支援 ・設備投資支援（CEコマース投資支援を含む） <p>■ DX化支援</p> <ul style="list-style-type: none"> ・トレサビ確保のためのアーキテクチャ構築支援 ・デジタルシステム構築・導入支援 <p>■ 標準化支援</p> <ul style="list-style-type: none"> ・品質指標の策定支援 <p>■ スタートアップ・ベンチャー支援</p> <ul style="list-style-type: none"> ・リスクマネーの呼び込み（CE銘柄） 	<p>■ 民：野心的な自主的目標の設定とコミット/進捗管理</p> <p>■ 官：競争環境整備と目標の野心度に 応じたCEツールキットの傾斜的配分</p> <p>■ ビジョン・ロードマップ策定</p> <p>■ 協調領域の課題解決</p> <ul style="list-style-type: none"> ・CE情報流通プラットフォーム構築、標準化、広域的地域循環等のプロジェクト組成・ユースケース創出 <p>■ CEのブランディング</p> <ul style="list-style-type: none"> ・CEの価値観の普及・浸透、教育、経営方針等

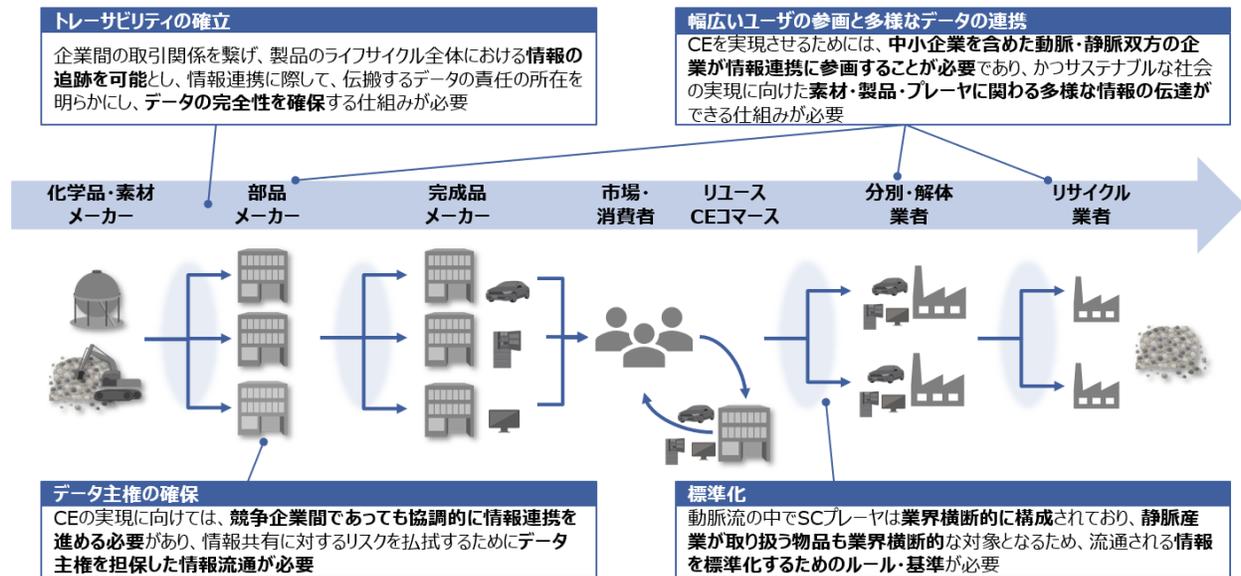
[出典]

経済産業省、成長志向型の資源自律経済戦略

<https://www.meti.go.jp/press/2022/03/20230331010/20230331010-2.pdf>

■ CE 実現に向けて構築すべきプラットフォーム像

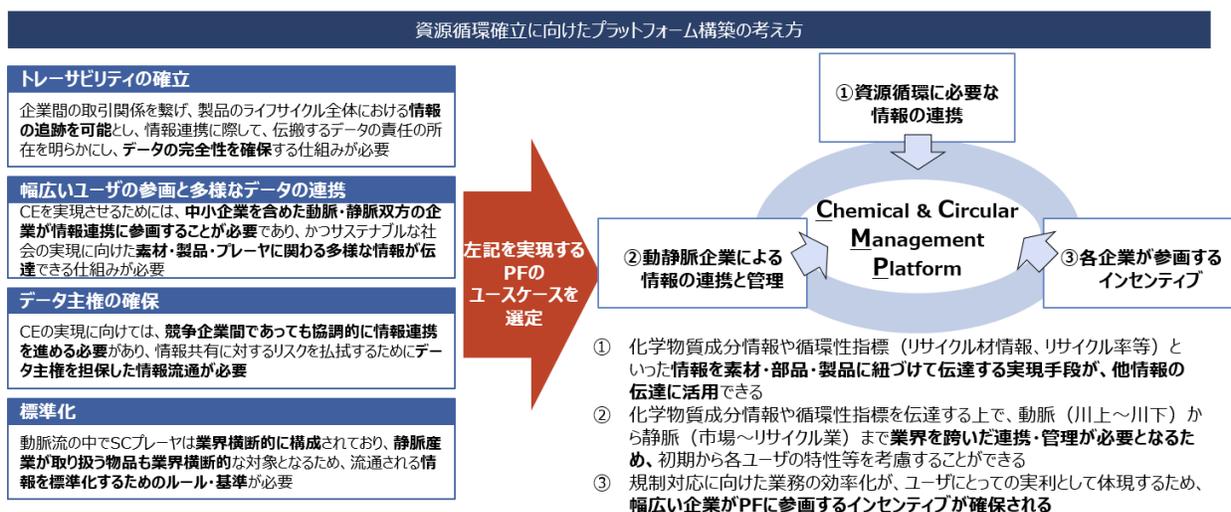
情報流通プラットフォームは、バリューチェーン全体(動静脈)における企業・業界を跨いだ協調的な取り組みが求められることから、現状の懸念・課題を解消できる連携基盤の構築が必要となる。



■ ユースケース選定

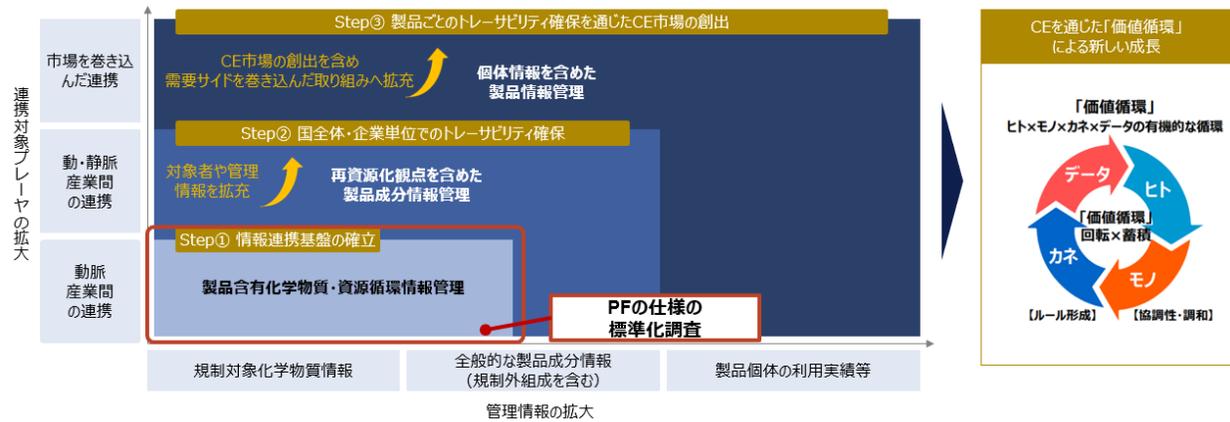
CE 情報流通プラットフォームのユースケースを選定する上で、将来的なユーザ展開を踏まえた幅広いユーザが対象となり、管理情報が拡大しても連携方式の活用性が高い領域である製品含有化学物質・資源循環情報管理からスタートすることで、参画企業にとっての参画意欲も高く早期のプラットフォーム安定運用が可能になると考える。

資源小国である日本において、CE 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と成長を確保する上で急務であり、そのためには資源循環情報を動脈企業から連携・管理していくことが必要である。



■ 将来的な拡張ロードマップ

製品含有化学物質・資源循環情報管理からスタートし、将来的な製品デジタル情報の実現に向け管理対象情報や、関連プレーヤの拡大を見据えたプラットフォーム構築を実現する。



[出典]

経済産業省、成長志向型の資源自律経済戦略

<https://www.meti.go.jp/press/2022/03/20230331010/20230331010-2.pdf>

■ 参考：循環性指標

循環性指標については IEC/ISO 82474 を参考にデータを構成する想定。

循環性指標の例																																																							
<ul style="list-style-type: none"> Product (製品) Class : ACA001 <ul style="list-style-type: none"> ProductPart (部品) Class : ACA002 <ul style="list-style-type: none"> Material (材料) Class : ACA007 <ul style="list-style-type: none"> Substance (物質) Class : ACA009 <ul style="list-style-type: none"> Mass (質量) Class : ACA004 MassPercent (含有率) Class : ACA005 MaterialCircularity (材料資源循環) Class : TBD <ul style="list-style-type: none"> RecycledContentInformation (リサイクル材) Class : TBD <ul style="list-style-type: none"> RecycledContent Class : ACA<TBD> RenewableContent (再生可能材) Class : ACA<TBD> RecyclingRate (リサイクル率) Class : ACA<TBD> Substance (物質) Class : ACA009 <ul style="list-style-type: none"> Mass (質量) Class : ACA004 MassPercent (含有率) Class : ACA005 ProductCircularity (製品循環) Class : TBD <ul style="list-style-type: none"> RecycledContentInformation (リサイクル材) Class : TBD <ul style="list-style-type: none"> RenewableContent (再生可能材) Class : ACA<TBD> ReusedContent (リユース品) Class : ACA<TBD> RecyclingRate (リサイクル率) Class : ACA<TBD> 	<table border="1"> <thead> <tr> <th colspan="2">RecycledContentInformation (リサイクル材情報)</th> </tr> </thead> <tbody> <tr><td>TotalRecycledContent</td><td>全体の平均リサイクル率</td></tr> <tr><td>PreConsumerRecycledContent</td><td>プレコンシューマリサイクルの平均リサイクル率</td></tr> <tr><td>PostConsumerRecycledContent</td><td>ポストコンシューマリサイクルの平均リサイクル率</td></tr> <tr><td>description</td><td>コメント欄</td></tr> <tr> <th colspan="2">RecycledContent (リサイクル材)</th> </tr> <tr><td>Mass</td><td>質量</td></tr> <tr><td>MassPercent</td><td>含有率</td></tr> <tr><td>Attachment</td><td>添付ファイル</td></tr> <tr><td>description</td><td>コメント欄</td></tr> <tr><td>recyclingInformation</td><td>リサイクル手法 (リストから選択、マテリアル、ケミカルリサイクル等)</td></tr> <tr><td>otherRecyclingInformation</td><td>その他リサイクル手法</td></tr> <tr> <th colspan="2">RenewableContent (再生可能材)</th> </tr> <tr><td>Mass</td><td>質量</td></tr> <tr><td>MassPercent</td><td>含有率</td></tr> <tr><td>Attachment</td><td>添付ファイル</td></tr> <tr><td>description</td><td>コメント欄</td></tr> <tr> <th colspan="2">ReusedContent (リユース材)</th> </tr> <tr><td>Mass</td><td>質量</td></tr> <tr><td>MassPercent</td><td>含有率</td></tr> <tr><td>Attachment</td><td>添付ファイル</td></tr> <tr><td>description</td><td>コメント欄</td></tr> <tr> <th colspan="2">RecyclingRate (リサイクル率)</th> </tr> <tr><td>MassPercent</td><td>含有率</td></tr> <tr><td>Attachment</td><td>添付ファイル</td></tr> <tr><td>description</td><td>コメント欄</td></tr> <tr><td>calculationMethod</td><td>リサイクル率計算手法</td></tr> </tbody> </table>	RecycledContentInformation (リサイクル材情報)		TotalRecycledContent	全体の平均リサイクル率	PreConsumerRecycledContent	プレコンシューマリサイクルの平均リサイクル率	PostConsumerRecycledContent	ポストコンシューマリサイクルの平均リサイクル率	description	コメント欄	RecycledContent (リサイクル材)		Mass	質量	MassPercent	含有率	Attachment	添付ファイル	description	コメント欄	recyclingInformation	リサイクル手法 (リストから選択、マテリアル、ケミカルリサイクル等)	otherRecyclingInformation	その他リサイクル手法	RenewableContent (再生可能材)		Mass	質量	MassPercent	含有率	Attachment	添付ファイル	description	コメント欄	ReusedContent (リユース材)		Mass	質量	MassPercent	含有率	Attachment	添付ファイル	description	コメント欄	RecyclingRate (リサイクル率)		MassPercent	含有率	Attachment	添付ファイル	description	コメント欄	calculationMethod	リサイクル率計算手法
RecycledContentInformation (リサイクル材情報)																																																							
TotalRecycledContent	全体の平均リサイクル率																																																						
PreConsumerRecycledContent	プレコンシューマリサイクルの平均リサイクル率																																																						
PostConsumerRecycledContent	ポストコンシューマリサイクルの平均リサイクル率																																																						
description	コメント欄																																																						
RecycledContent (リサイクル材)																																																							
Mass	質量																																																						
MassPercent	含有率																																																						
Attachment	添付ファイル																																																						
description	コメント欄																																																						
recyclingInformation	リサイクル手法 (リストから選択、マテリアル、ケミカルリサイクル等)																																																						
otherRecyclingInformation	その他リサイクル手法																																																						
RenewableContent (再生可能材)																																																							
Mass	質量																																																						
MassPercent	含有率																																																						
Attachment	添付ファイル																																																						
description	コメント欄																																																						
ReusedContent (リユース材)																																																							
Mass	質量																																																						
MassPercent	含有率																																																						
Attachment	添付ファイル																																																						
description	コメント欄																																																						
RecyclingRate (リサイクル率)																																																							
MassPercent	含有率																																																						
Attachment	添付ファイル																																																						
description	コメント欄																																																						
calculationMethod	リサイクル率計算手法																																																						

[出典]

CMP タスクフォース/要件定義 WG/システム WG、CMP システム要件定義書 v1.1、2025 年 2 月掲載予定

1.1.2 CE 基盤立ち上げに当たっての産官学の役割と取り組み

CE 情報流通プラットフォームの立ち上げに当たっては、産官学が独立しつつも相互に支え合う協調的な仕組みにより、市場環境を整備する必要がある。

	役割	取り組み
 官の役割と取り組み	<ul style="list-style-type: none"> ・戦略的な政策に基づく事業立案や予算策定、法整備 ・ルール形成、国際標準化 	<ul style="list-style-type: none"> ・ビジネスモデル転換への積極支援 <ul style="list-style-type: none"> - 投資促進策による投資支援（補助金・助成金・低金利融資等） ・ビジョン・ロードマップ策定（環境規格への対応、KPI設定） ・ルールの明確化（国内/国際ルール標準化）：規制・ルールに関する国際連携 ・クリティカルミネラルの確保 ・循環資源の標準化活動の積極支援 ・国際貿易循環を促す協力関係構築/国際条約への対応
 学の役割と取り組み	<ul style="list-style-type: none"> ・基礎研究・応用研究による知財開発 ・研究成果や知財の確保・蓄積 ・次世代教育の達成 	<ul style="list-style-type: none"> ・社会実装に向けた検証の場の提供 ・国際標準：情報収集/情報発信 ・技術交流 ・CEブランディング：価値観の普及・浸透、教育
 産の役割と取り組み	<ul style="list-style-type: none"> ・技術確立や研究の社会実装 ・知財を活用した持続的な価値提供を実施 ・経済的な価値創出や市場獲得、市場ルールの形成 	<ul style="list-style-type: none"> ・ビジネスモデル転換の社会実装に向けてのトップリーダーシップ <ul style="list-style-type: none"> - チャレンジングな目標設定とコミット/進捗管理 ・CEコマースのDX投資負担 ・循環資源の量的/質的確保 <ul style="list-style-type: none"> - 設計やオペレーションが形式知化され民主化の進展 ・需要の安定化（SC横断の在庫適正化等）
本事業での取り組み	産官学一体で進めるCE情報流通プラットフォームの立ち上げ・組織化を目指す	

1.1.3 製品含有化学物質・資源循環情報プラットフォーム（CMP）構築の目的

CE 情報流通プラットフォームのユースケースとなる製品含有化学物質・資源循環情報プラットフォーム：
Chemical and Circular Management Platform（以下 CMP）における構築目的は以下 3 点である。

① 製品含有化学物質

- REACH 規制など、年々厳しくなる化学物質規制に迅速に対応する（再調査効率化）
- 精度向上、業務効率の向上を図ると同時に秘匿物質の確実な情報管理を実現

② 資源循環

- 欧州エコデザイン規則※1 を睨み、製品デジタル情報を意識したバリューチェーンでの資源情報を共有する
- CMP は、製品・部品・材料・化学物質のヒエラルキー情報を持つ予定であり、資源循環情報をも加味することで効率的にサーキュラーエコノミーに資する情報共有を実現させる
- 部品リユース情報、リサイクル材情報（含有率、純度、ソースなど）の伝達を実現

③ グローバル連携

- 現在策定が進む国際規格（IEC/ISO 82474、Material Declaration）の内容（資源循環情報を含む）を盛り込むことで、グローバル連携を可能とする
- グローバルに展開されている製品含有化学物質情報に関する基盤（自動車・IMDS など）との連携を目指す

※1：様々な製品に対し、再利用や修理可能性、エネルギー効率等製品仕様における持続可能性の要件の枠組みを設定する規則

European Union, Regulation - 2024/1781 - EN - EUR-Lex

<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024R1781&qid=1719580391746>

[出典]

化学物質審議会・産業構造審議会製造産業分科会化学物質政策小委員会、CMP（仮称）構想について

https://www.meti.go.jp/shingikai/sankoshin/seizo_sangyo/kagaku_busshitsu/pdf/011_08_00.pdf

1.1.4 標準仕様策定の目的と対象

■ 目的

本標準仕様書は、企業を跨いだサプライチェーン間で、データ主権の確保を実現しながら、情報伝達を実施するユースケースの標準仕様として作成する。

従って、製品含有化学物質・資源循環情報管理以外にも、他ユースケースに応用可能な標準仕様として整理する。

また、標準仕様書を公開することで、異なる業界や製品分野でも応用可能な共通基盤の確立を目指す。

■ 対象

本標準仕様書は、製品含有化学物質・資源循環情報管理におけるユースケースとして作成する。

情報伝達の仕組みやデータ主権などの考え方・仕様は、他ユースケースへ応用可能であるが、情報伝達対象データは、ユースケースごとに異なるため個別に整理が必要である。

■ 標準仕様策定の対応方針

- ウラノス・エコシステムのアーキテクチャに準ずるプラットフォームとして満たすべき基本的な設計要件については、「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）」を参考とする。
- CMP において満たすべき非機能要件については、「CMP 基盤/CMP アプリ 標準仕様書別紙 非機能要件一覧」を参考とする。
- CE 実現に向けて議論が進められている国際標準規格：IEC/ISO 82474 並びに IEC 62474 への準拠の行うことで、多くのアプリケーションとの接続や静脈企業・他業界への拡張、海外を含む他プラットフォームとの相互運用性を実現する。

【参考】CEの実現を目指した国際標準規格

以下に示すような CE 実現を目指した標準規格の議論が進められている。本事業においては動脈側の構築をスコープとするものの、将来的な CE 実現を担保するために、下記規格にて議論されているデータ項目、特に循環性指標の取り込みを行う。

➤ IEC/ISO 82474

背景

- IEC 62474(電機電子分野における国際標準規格)の改正検討に当たり、電気電子業界からISOがカバーする業界群に拡張対応する規格として提案された。
- 製品含有化学物質に関する伝達項目、および構造を定義した様式により、複数の業界・企業にて相互に情報交換が可能となる。

進捗

- IEC、ISOともに最終国際規格案(FDIS)が承認され、未発行の状態。

標準への準拠により得られる価値

項目	標準への準拠に取り組む意義
幅広い業界・製品への適応	<ul style="list-style-type: none">• IEC製品分野からISO製品分野への拡大することで、業界横断的なデータ連携が必要となるCEの実現を促進する。
既存の情報伝達スキームとの統合	<ul style="list-style-type: none">• 既存の規格であるIEC62474を拡張することで、既存システムのスキームと今後開発される新たなシステムのスキームが統合可能。• スキームのみならずデータ自体の互換性の確保が可能。
拡張性の担保	<ul style="list-style-type: none">• 標準化することでデータの互換性確保が容易となり、データの利活用が促進される。これにより、新たなニーズへの対応も可能。

[出典]

みずほ情報総研株式会社、令和2年度産業標準化推進事業委託費(戦略的国際標準化加速事業：ルール形成戦略に関する調査研究(製品含有化学物質の情報伝達方式に関する調査研究))調査報告書

https://www.meti.go.jp/meti_lib/report/2020FY/000686.pdf

1.2 CMP-製品含有化学物質・資源循環情報管理

1.2.1 製品含有化学物質・資源循環情報管理の目的と課題

市場に出回る様々な製品には多くの化学物質が使われており、不適切な廃棄等により、環境・人体へ悪影響を及ぼすリスクが高いため各国のルール・法律で厳しく規制されており、これらの規制対応への取り組みはこれまででも実施されてきた。

他方、日本が今後自立的な資源循環が行えなければ、製造業の事業継続性が危ぶまれる状況であることは自明であり、リサイクルを効率化するためには化学物質を始めとする製品成分情報が静脈産業へ連携できる仕組み構築が急務となる。

製品含有化学物質・資源循環情報管理の目的		目的達成に向けた課題
環境・人体保護の観点 (これまでの主眼)	化学物質の不適切な使用や廃棄によって 環境や人体に及ぼす悪影響が非常に大きい ことから、利用や含有量に対して 各国で規制 がかけられており、規制への適合性を証明するためにSC全体を通して 情報を積み上げ正しく報告 する必要がある	<ul style="list-style-type: none"> ✓ 各業界での取り組みとして異なる標準・ツールでの管理 ✓ 頻繁に変わる規制内容への対応が非効率的
資源確保・再資源化の観点 (今後の主眼)	リサイクル時の分別、前処理、再資源化等のプロセスにおいて 廃棄物の成分情報に基づいた適切な処理 を実施するため、動脈産業で積み上げた情報を 静脈産業とも連携 してリサイクルの効率化を図る	<ul style="list-style-type: none"> ✓ 再資源化観点での情報連携が一部企業・業界で限定的に行われていない ✓ SC全体で積み上げた情報を静脈産業へ連携する仕組み・基盤がない

環境保護・資源循環の双方の観点から、製品含有化学物質・資源循環情報管理は日本にとって重要性が高く、現状の課題解決に向けた迅速な取り組みが必要である

1.2.2 製品含有化学物質・資源循環情報管理に関する規制・業界基準

製品含有化学物質管理・資源循環情報に関する規制・業界基準は以下の通り。

【各国法規】

<日本>

- 化学物質の審査及び製造等の規制に関する法律（化審法）

<米国>

- Toxic Substances Control Act（TSCA／有害物質規制法）

<欧州>

- Directive 2000/53 on end-of life vehicles（ELV 指令）
- Directive 2011/65 on the restriction of the use of certain hazardous substances in electrical and electronic equipment（RoHS 指令）
- Regulation 2019/1021 on persistent organic pollutants（POPs 規則）
- Regulation 1907/2006 of concerning the Registration, Evaluation, Authorisation and Restriction of Chemicals（REACH 規則）
- Regulation 2017/745 on medical devices（医療機器規則）

<中国>

- 電器電子製品有害物質使用制限管理弁法

【業界基準】

<自動車業界>

- Global Automotive Declarable Substance List (GADSL)

[出典]

American Chemistry Council, GADSL | The GADSL is the result of the efforts of a global team from the automotive, automotive parts supplier (tier supplier) and chemical/plastics industries who have organized the Global Automotive Stakeholders Group (GASG).

<https://www.gadsl.org/>

<電機電子業界>

- International Electrotechnical Commission 62474 (IEC 62474)

[出典]

International Electrotechnical Commission, IEC 62474 - Material Declaration for Products of and for the Electrotechnical Industry

<https://std.iec.ch/iec62474>

1.2.3 現状課題と対応方針

1.2.3.1 現状課題

Trusted web※1 に記載の内容をもとに、化学物質管理業務の現状について、以下 3 つの課題を抽出。

No	課題	内容
①	個社ごとの回答内容・フォーマットの違い	電機・電子、自動車それぞれの業界ごとに様式・フォーマットは統一されているものの、業界横断での情報伝達の際に複雑化してしまい、サプライチェーン全体に多大な負荷がかかっている。
②	開示範囲の制御・情報精度	各企業の営業秘密情報(CBI)の保護、開示範囲の制御も個別に行われるため、情報伝達の漏れや情報精度の低下が発生している。
③	法規変更に対応した情報伝達	法規制変更や 4M 変更※2 に対応した情報の伝達の際に情報のバケツリレーが発生しており、トレースに手間と時間がかかっている。

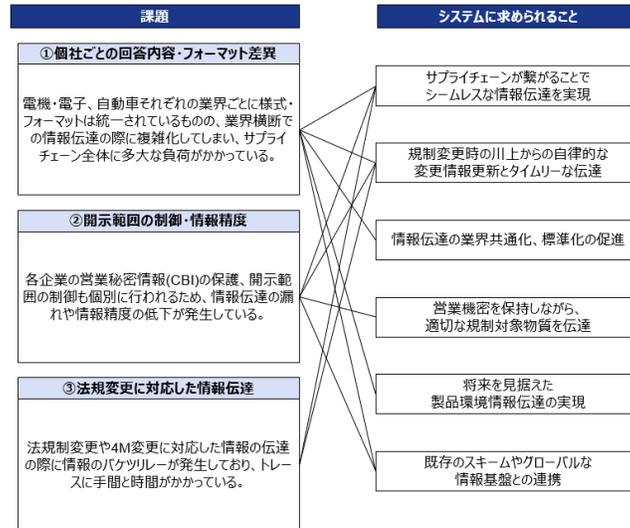
※1：みずほリサーチ&テクノロジーズ株式会社、「ものづくりのサプライチェーンにおける製品含有化学物質情報等の 確実な伝達を可能とする Chemical Management Platform(CMP)」

https://www.kantei.go.jp/jp/singi/digitalmarket/trusted_web/2023seika/files/06_mizuho_research_technologies_report_agenda.pdf

※2：4M は、製造プロセスにおける 4 要素で人(Man)、機械(machine)、材料(Material)、方法(Method)を指す。製品含有化学物質管理においては、4M が変更されることにより、過去に伝達済みの成分情報が変更になる場合があるが、その成分情報の変更についてサプライチェーンを通じて迅速に情報伝達することが重要となる。

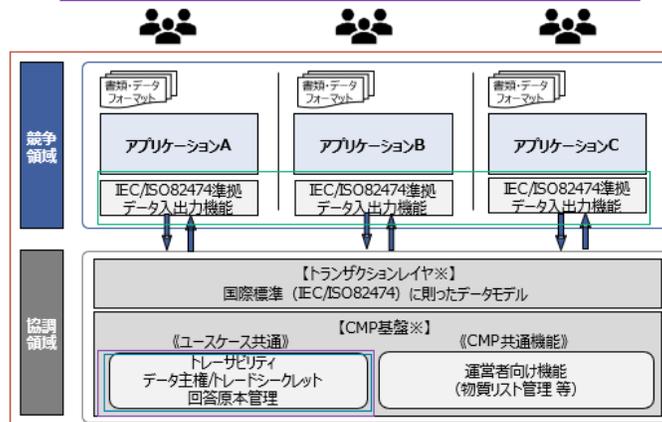
1.2.3.2 対応方針

国際標準である IEC/ISO 82474 に準拠しつつ、サプライチェーンのデータを適切な形で繋げることで課題の解決に寄与する。



CMPにおける実現方式

- (A) 事業者間・各種システムを繋げるプラットフォームの提供
- (B) 国際標準への準拠や適切なマスタ管理による標準化
- (C) 企業の営業秘密の保持やデータ主権の確保
- (D) サプライチェーン間の情報伝達のトレーサビリティの確保



※IEC/ISO82474 について : 1.1.4 参照

※物質リストの詳細について : [出典] CMP タスクフォース/要件定義 WG/システム WG、CMP システム要件定義書 v1.1、2025 年 2 月掲載予定

※トランザクションレイヤ、CMP 基盤の詳細について : 1.3.1 参照

1.3 システム全体図

1.3.1 システム全体

1.3.1.1 設計方針

以下 2 点を設計方針とする。

- ① 「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」※1 記載のアーキテクチャ設計方針を参考にする。

アーキテクチャ設計方針（ガイドラインa版から要約引用）	CMPでの対応方針
データ主権の確保 <ul style="list-style-type: none"> データ所有者が以下を決定できること <ol style="list-style-type: none"> ① 利用相手 ② 利用条件 ③ 保存場所 	✓ 以下考え方で対応 <ol style="list-style-type: none"> ① 調査依頼・回答/更新などのデータ連携時に、相手先を明示的指定する仕組みを提供 ② データ提供者が、データ単位で登録・更新・削除を実施できること。 ③ 以下のいずれかを選択可能とする <ul style="list-style-type: none"> - 運営事業者が提供する基盤に保管 - 自社基盤（オンプレ・クラウド等）に保管
UX※2・導入容易性の確保 / デジタル完結 <ul style="list-style-type: none"> ユーザ負担（工数・金額）が小さいこと 自動化等でユーザオペレーションの省力化に寄与すること 	✓ 提供機能内容に応じた価格設定など、ユーザの導入・金銭負担を下げる形態で提供 ✓ 事前に登録しておいた成分情報をもとに依頼受領時に回答するなど、現行業務の効率化に寄与する機能を提供
トラストの確保 <ul style="list-style-type: none"> ソシキ、モノ、データの真正性・完全性を確保 <ol style="list-style-type: none"> ① 接続先/元は正しい相手か ② 接続元が生成し改ざんされていないデータか ③ 属性・機能はCertificationされているか 	✓ 以下考え方で対応 <ol style="list-style-type: none"> ① CMPへの利用申し込みの際に、外部認証機関が発行したIDと紐づけを行うことで確認 ② 企業間データ連携時のデータチェック機能を提供 ③ CMPアプリの認証プロセスで担保
共通基盤の利用 <ul style="list-style-type: none"> 競争領域・協調領域のレイヤ化 	✓ 競争領域はCMPアプリ、協調領域はCMP基盤で区別 ✓ CMPアプリは規制物質管理業務を支援する機能を提供、CMP基盤は業務には踏みこまず企業間データ連携機能を提供する
相互運用性の確保 <ul style="list-style-type: none"> 国内外の他システムとの相互接続性 	✓ IMDS、chemSHERPAとの連携を見据えるとともに、データ連携はIEC/ISO 82474の標準に準拠し相互接続性を担保する

※1：[出典]経済産業省・デジタルアーキテクチャ・デザインセンタ（DADC）、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a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

※2：UX（User Experience）は、ユーザがサービス利用を通じて得られる体験全般を指す。

② 既に本番稼働中の蓄電池トレサビシステムのデータ連携方式、データモデル、基盤構成を最大限活用し、不足する部分は機能拡充する方針とする。

	蓄電池のトレーサビリティ管理システムの実装	CMP基盤での活用ポイント
データ連携方式	<ul style="list-style-type: none"> 依頼回答方式による企業間のデータ連携、また連携時のデータチェック機能※1を実装 データ開示先の設定や開示後のデータ削除など、データ主権を考慮した機能も実装 <small>※1:連携データが確かに連携元企業からのデータであることをチェックする機能</small>	<ul style="list-style-type: none"> トレサビと同様のサプライチェーン間の情報伝達方式、データ主権を保持するための設計思想を参考
データモデル	<ul style="list-style-type: none"> ユースケース共通部分・固有部分を区別 ユースケース共通：「自社製品と調達品の構成」および「取引先との関係」を繋げることでSCのトレサビを表現 ユースケース固有：CFP※2値やDQR※3値など欧州電池規則に則したデータを表現 <small>※2:カーボンフットプリント (Carbon Footprint of Products) ※3:データ品質情報 (Data Quality Rating)</small>	<ul style="list-style-type: none"> ユースケース共通はそのまま活用、ユースケース固有部分を規制物質管理に関わるデータモデルを追加 また、蓄電池のトレーサビリティ管理システムの基盤には存在しない物質リストのような企業横断的に配信するデータモデルを追加
基盤構成	<ul style="list-style-type: none"> 部品情報やCFP※2値などのトレードシークレットを保管する個社領域を参加企業ごとに構築 個社領域はBC※4で構成され、これらトレードシークレットはBC上 (On-Chain) に保管する仕組み <small>※4:ブロックチェーン</small>	<ul style="list-style-type: none"> 蓄電池のトレーサビリティ管理システムの基盤のノウハウを活用し、製品含有化学物質管理に関わるトレードシークレットを個社領域で管理 参加企業横断的に共有される規制物質リストは、新規に専用データベース構築を想定

■用語のマッピングについて

レイヤとしての表現は、原則 Whitepaper の記載に則る。

各レイヤで CMP 標準仕様書に登場するシステム名は、右列「CMP 標準仕様書登場システム名」の通り。

レイヤ定義 対応表		本書で登場するシステム名
旧アーキテクチャ上の記載(*1)	Whitepaperの記載(*2)	CMP標準仕様書登場システム名
データ連携システム層 (データ流通層+連携サービス層)	データスペース	- (該当なし)
データ流通層	トランザクションレイヤ	- (Whitepaperに準拠)
ユーザ認証・システム認証	トラストレイヤ	- (Whitepaperに準拠)
連携サービス層	データレイヤ+インダストリーサービス	CMP基盤
各者システム層	データレイヤ	- (該当なし)
アプリケーション層	インダストリーサービス	CMPアプリ
関係サービス層	インダストリーサービス/ データスペースコンプリメンタリサービス	- (該当なし)

*1 引用元：経済産業省・デジタルアーキテクチャ・デザインセンタ（DADC）、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

*2 引用元：経済産業省・情報処理推進機構・デジタルアーキテクチャ・デザインセンター、Whitepaper ウラノス・エコシステム データスペース リファレンスアーキテクチャモデル、2025 年 2 月掲載予定

1.3.1.2 CMP システムの全体構成

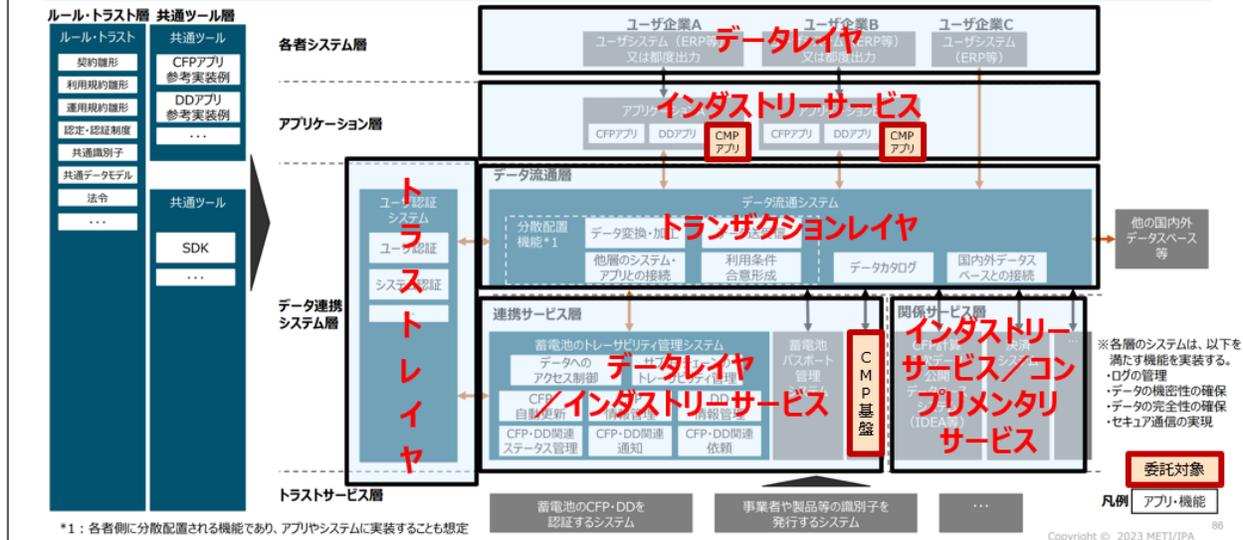
CMP は、ウラノス・エコシステム上に化学物質情報伝達をユースケースとしたシステム群であり、本書では委託対象に必要な機能・データを標準仕様として定義する。

なお、各層の役割は以下の通り。

- データレイヤ
 - CMP 参加事業者の社内システム（回答情報のデータソースなどに該当）
- インダストリーサービス
 - 法規要求事項やユーザ業務要件に基づいた、製品含有化学物質・資源循環情報管理を支援する機能を提供
 - CMP 参加事業者向けアプリ、運営事業者向けアプリが存在
- トラストレイヤ
 - CMP 参加事業者の管理や認証機能を提供
- データスペース
 - トランザクションレイヤ
 - アプリと CMP 基盤間の API 連携機能を提供
 - データレイヤ／インダストリーサービス
 - CMP データ（データレイヤ）や、企業間の情報伝達管理に係る機能、物質リストなど参加事業者間で横断的に共有されるデータ管理機能（インダストリーサービス）を提供

データ連携基盤のシステムアーキテクチャ

各者システムやアプリケーションが利用するサプライチェーンデータ連携基盤は、ルール・トラスト層、共通ツール層、データ連携システム層、トラストサービス層に分けて、それぞれを構成するシステムが疎結合するアーキテクチャとする。先行的に青い箇所の具体化を進めている。



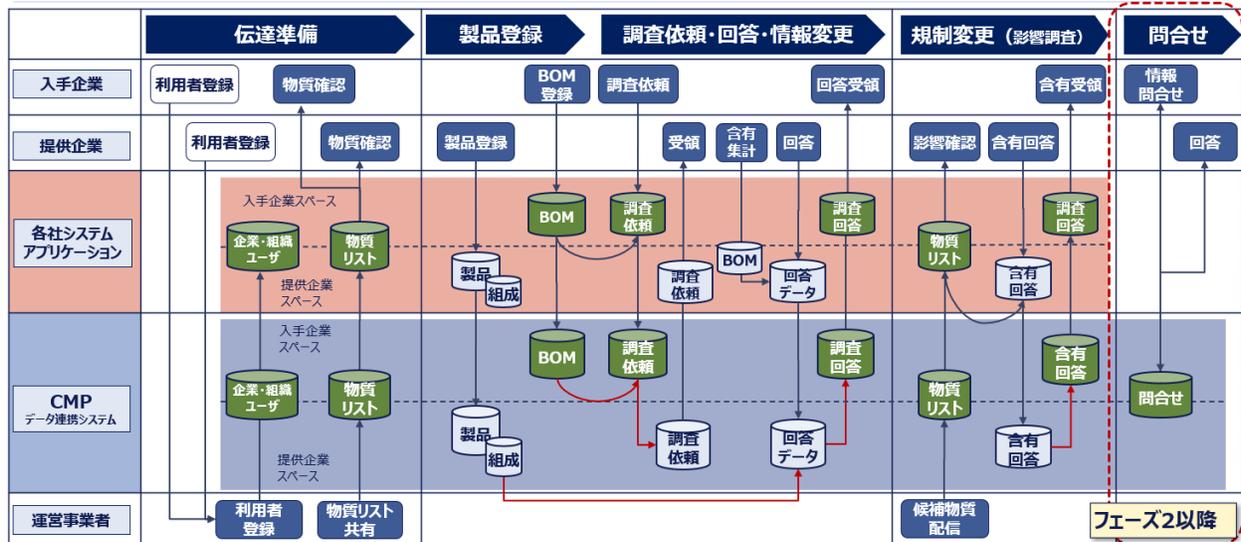
[出典]

経済産業省・デジタルアーキテクチャ・デザインセンタ（DADC）、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

1.3.2 業務全体

含有化学物質情報伝達の各業務でアプリケーションとCMPが連動しながら企業間のデータ連携を実行する。



[出典]

CMP タスクフォース/要件定義 WG/システム WG、CMP システム要件定義書 v1.1、2025 年 2 月掲載予定

1.4 データの流れと機能構成

1.4.1 標準機能

1.4.1.1 データスペース

■ データスペースの役割

➤ データスペース導入の背景

データスペース（いわゆるデータ連携システム層）は、Ouranos Ecosystem Initiativeとして推進されている DFFT（Data Free Flow with Trust：信頼性のある自由なデータ流通）という基本方針に則り、日本の産業界/組織が持つデータを、企業、業界、国境を跨いで自由にデータ連携・利活用するための仕組みを効果的に構築するために導入する。

➤ データスペースにおけるトラストレイヤの役割

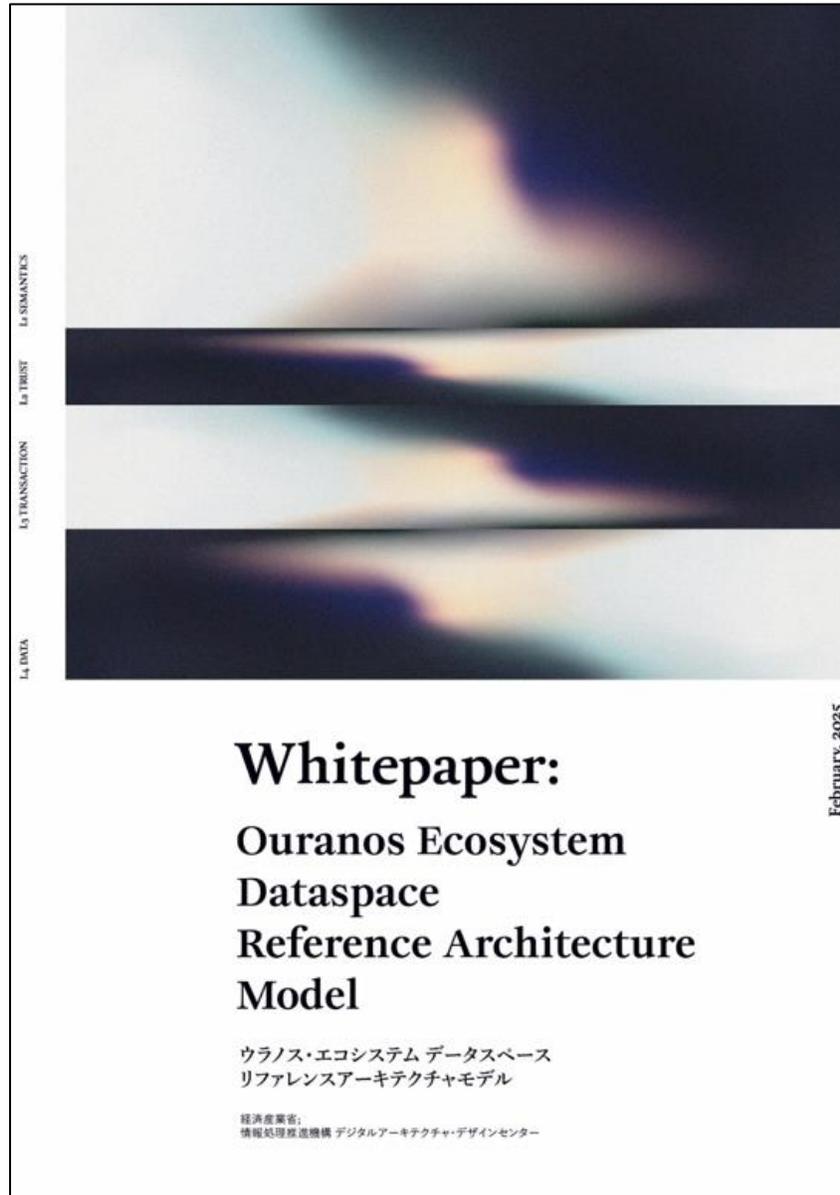
データスペースにおける認証・認可機能は、この Ouranos Ecosystem を実現するに当たり**多数の参加者の真正性や、アクセス権限の管理、流通するデータの信頼性を効率的に担保**すること等を目指す機能となる。**他データスペースとの相互運用時において、両データスペースのトラスト解決をシームレスに実施する役割**を担う。

➤ データスペースにおけるトランザクションレイヤの役割

データスペースコネクタを用いてトランザクションレイヤを利用する価値として、多数の競争サービスの業者（アプリケーションベンダ等）に**共通的な I/F やデータモデルを提供**し、バリデーションの実装によるデータ品質の確保等も可能となることから、**参入時の開発規模を削減、新たなデータスペース相互運用の際にも改修負荷の低減**が見込まれる。

■ データスペースの利用方針

データスペースのアーキテクチャ設計については、ウラノス・エコシステム データスペース リファレンスアーキテクチャモデル Whitepaper※1 で示される指針に沿いながら、適切な設計の検討を行う。



※1：経済産業省・情報処理推進機構・デジタルアーキテクチャ・デザインセンター、Whitepaper ウラノス・エコシステム データスペース リファレンスアーキテクチャモデル、2025年2月掲載予定

1.4.1.2 トランザクションレイヤ

■データ転送機能の要求仕様

- CMP 基盤におけるデータモデルの要求仕様を以下に示す。
- データスペースの役割を踏まえ、動静脈連携、他産業、他ユースケースへの展開を効率的に行うため、データ転送機能としての対応方針を以下に示す。

CMP基盤の要求仕様とトランザクションレイヤの対応方針

CMP基盤の要求仕様		データ転送機能としての対応方針
データモデル	<ul style="list-style-type: none"> • サプライチェーン間のデータ交換におけるトレーサビリティを確保するために、以下2層のデータモデルが必要となる ① 企業間の取引関係の管理と、依頼・回答/更新などのデータ連携を行うための共通的なデータモデル ② IEC/ISO 82474などユースケース固有の連携データモデル 	<ul style="list-style-type: none"> • <u>業務的なデータ構造に依存せず、サプライチェーンのトレーサビリティ確保を実現するために共通的に利用できるインターフェースを共通データモデルを定義し、トレーサビリティ共通APIとして提供する。(左記①へ対応)</u>

■データ転送機能

- トランザクションレイヤを利用するためのデータスペースコネクタに要求する想定機能を以下に示す。
- **CMP 基盤の要件を踏まえ、共通 I/F の機能としてノード取得/登録/削除、取引関係取得/登録/削除、連携データ取得/登録/削除を提供する方針となる。**

No	機能	機能概要
1	共通 I/F	データ転送で提供する共通的な API。API は RESTAPI を採用し、PUT、POST、GET、DELETE を提供する。
2	データ送受信機能	API によるデータ受信およびバックエンド API、データレイヤへのデータ送信を行う。
3	共通バリデーション	API によるデータ受信時における共通的なバリデーションを行う。
4	来歴管理機能	送信元や実行 API、実行時間のログ保存を行う。
5	変換機能	データスキーマの変換を行う機能を備える予定。

1.4.1.3 トラストレイヤ

■ユーザ認証機能の要求仕様

- CMP 基盤における認証・認可の要求仕様を以下に示す。
- 蓄電池トレサビシステムと CMP 基盤間で認証機能を一体的に提供する要件については、**関係各所と連携し、調整を行った上で実現方式を具体化する想定となる。**

CMP基盤の要求仕様とトランザクション/データレイヤの対応方針

CMP基盤の要求仕様		ユーザ認証機能としての対応方針
認証	<ul style="list-style-type: none"> • 蓄電池トレサビシステムとCMP基盤を並行して利用する企業が存在する • CMP基盤のユースケースは事業者単位の認証で実現可能 	<ul style="list-style-type: none"> • CMP基盤と蓄電池トレサビシステムとの認証連携を視野に、ユーザ認証の単位は事業者単位とする
認可	<ul style="list-style-type: none"> • ユーザ企業ごとの利用契約状況に応じて実行可能なサービスを適切に制御する • ユーザ企業ごとのデータアクセス可能範囲の制御を蓄電池トレサビシステムと連携して行う 	<ul style="list-style-type: none"> • アプリケーション、トランザクションレイヤ、データレイヤで役割分担を実施し、データスペースで提供するものはAPIへのアクセス認可までとする • 事業者単位の各制御はCMP基盤で、CMP基盤のユースケースとして想定されるユーザ（ヒト）やロール、事業所情報を加味したアクセス制御は、CMPアプリで実現する

■ ユーザ認証機能

- トラストレイヤに要求する想定機能を以下に示す。
- CMP 基盤の要求仕様より、ユーザ認証の単位は事業者単位とし、事業者の接続形態に合わせてユーザ本人認証か、クライアントシステム認証を選択する方針とする。

No	機能	機能概要
1	ユーザ本人認証	送信元となるアプリの利用事業者を認証する。
2	クライアントシステム認証	送信元となるシステムを認証する。
3	トークンイントロスペクション	事業者およびシステムのトークンを検証する。
4	パスワード変更	事業者の登録パスワードを変更する。
5	アクセストークン更新	リフレッシュトークンを用いて事業者の認証トークンを更新する。
6	事業者情報更新	事業者識別子（内部）の事業者情報を更新する。
7	事業者情報一覧取得	指定された識別子をもとに、事業者情報を取得する。
8	事業所情報更新	事業者識別子（内部）に紐づいた事業所を登録または内容を更新する。
9	事業所情報一覧取得	事業者識別子（内部）に紐づけられている事業所識別子（内部）の一覧を取得する。

■ 複数ユースケースを跨る認証・認可機能実現時の考慮事項（メタ識別子）

- トランザクションレイヤ／CMP 基盤は、蓄電池トレサビシステムと CMP 基盤を並行利用する企業の利便性を考慮し、蓄電池トレサビシステムと同様の識別子、ID 体系で管理を行う方針とする。
- CMP 基盤のユースケースとして想定されるユーザ（ヒト）やロール（部署等）を加味したアクセス制御を実現するための情報は、CMP アプリで管理を行う想定となる。
- CMP 基盤として事業者を「法人」、事業所を「組織」に修正する要望があがっている。名称を変更する場合、公開済みの蓄電池ガイドラインに影響があるため、修正範囲等について関係各所と調整を行う想定となる。

トランザクションレイヤ 管理対象	IDライフサイクル、更新運用等（想定）	備考
事業者 →「法人」への名称変更 を調整予定 システム／アプリケーション	<ul style="list-style-type: none"> プラットフォームを運営する運営事業者が、事業者からの登録申請に基づいて情報の登録、IDの払い出し、管理を行う 登録情報の削除を行いたい場合は、削除申請を提出する 登録した事業者情報の更新、修正を行うために、ユーザ企業から変更できるよう更新用のAPIを提供する 	<ul style="list-style-type: none"> CMP基盤においてユースケースをヒアリングし、<u>事業者情報登録、削除APIの開発要否を検討する</u>
事業所 →「組織」への名称変更 を調整予定	<ul style="list-style-type: none"> 事業者からの登録申請に事業所情報を記載する運用とすることで、プラットフォームを運営する運営事業者が事業所情報をトラストレイヤ内に登録、管理する 登録した事業所情報の更新、修正を行うために、ユーザ企業から変更できるよう更新用のAPIを提供する 	<ul style="list-style-type: none"> CMP基盤においてユースケースをヒアリングし、<u>事業所情報登録、削除APIの開発要否を検討する</u>

■ 補足：事業者識別子について

- トランザクションレイヤ／CMP 基盤のシステム内で利用される**事業者をユニークに識別するための識別子は、以下蓄電池トレサビシステムと同様のフォーマット、識別子を採用する想定となる。**

識別対象	識別子フォーマット	参考_設定値	参考_API名 (OperatorModel)	補足
事業者識別子 (内部)	・UUID	1bcdfa9b-86c4-41df-bff8-1ec4690225a4	operatorId	トランザクションレイヤやデータレイヤのシステム内で利用される事業者をユニークに識別するためのID
事業者識別子 (国内データ連携)	13桁数字 【国内企業】 ・法人番号(13桁の数字) 【海外企業】(未運用) ・海外企業の識別番号	1234567890001	openOperatorId	・ISO15459-2やISO6523-2に準拠しており、かつ法人であれば既に所持している識別子となるため、国際標準と普及率の観点から、法人番号を採用 ・海外企業の識別番号は保留 (未運用) となる。CMP基盤のユースケースをヒアリングした上で、必要に応じて次年度以降に具体化を行う方針とする。
グローバル識別子 (海外データ連携)	20桁英数字 (未運用) ・法人番号(13桁の数字)+α ・LEI(20桁の英数字)	1234ABCD5678EFGH0001	operatorAttribute	海外データ連携用の識別番号は保留 (未運用) となる。CMP基盤のユースケースをヒアリングした上で、必要に応じて次年度以降に具体化を行う方針とする。

■ 複数レイヤを跨る認証・認可機能実現時の考慮事項（認証の役割分担）

- CMP 基盤における、認証の対象と役割分担について以下に示す。基本的に**蓄電池トレサビシステムと同様の役割分担となる想定であり、ユーザ（ヒト）の認証が必要となる場合は CMP アプリで実施する想定となる。**

認証対象と役割分担

※赤字がCMP基盤として固有の記載

トラスト対象		インダストリーサービス (CMPアプリ)		トランザクションレイヤ		データレイヤ／インダストリーサービス (CMP基盤)	
ソシキ	事業者	○	・事業者によるログイン認証を実施する	○	・事業者の認証を実施する ・事業者情報を管理する	○	・アクセストークンの検証を実施する
	システム						
システム	モノ						
	各社システム	—	・システムに払い出すクライアントID、クライアントシークレット、アクセスキー (APIキー) を保持する	○	・システムの認証を実施する ・システム情報を管理する	○	・アクセストークンの検証を実施する
	アプリケーション	—	・システムに払い出すクライアントID、クライアントシークレット、アクセスキー (APIキー) を保持する	○	・アプリケーションの認証を実施する ・アプリケーション情報を管理する	○	・アクセストークンの検証を実施する
	製品/部品/原材料	—	—	—	—	—	—
	ヒト						
空間	ユーザ	○	・ユーザによるログイン認証を実施する	—	—	—	—
	事業所	—	—	—	—	—	—
	ロール	—	—	—	—	—	—

■ 複数レイヤを跨る認証・認可機能実現時の考慮事項（認可の役割分担）

- CMP 基盤における、認可の対象と役割分担について以下に示す。トランザクションレイヤで提供するのは API へのアクセス認可までで、事業者単位の各制御は CMP 基盤、CMP 基盤のユースケースとして想定されるユーザ（ヒト）やロール、事業所情報を加味したアクセス制御は、CMP アプリで実現する想定となる。

認証対象と役割分担

※赤字がCMP基盤として固有の記載

トラスト対象		インダストリーサービス（CMPアプリ）		トランザクションレイヤ		データレイヤ/インダストリーサービス（CMP基盤）		
ソシキ	事業者	—	<ul style="list-style-type: none"> • 認証後に受け取るアクセストークンとアクセスキー（APIキー）を送付する 	○	<ul style="list-style-type: none"> • CMP基盤のAPIへのアクセス認可を実施する • 事業者向けAPIキー、アクセストークンを管理する 	○	<ul style="list-style-type: none"> • アクセストークンに含まれる認証済み事業者IDを用いてCMP基盤の機能、データへのアクセス制御を実施する 	
	モノ	各社システム	—	<ul style="list-style-type: none"> • 認証後に受け取るアクセストークンとアクセスキー（APIキー）を送付する 	○	<ul style="list-style-type: none"> • CMP基盤のAPIへのアクセス認可を実施する • システム向けAPIキー、アクセストークンを管理する 	○	<ul style="list-style-type: none"> • アクセストークンに含まれる認証済みIDを用いてCMP基盤の機能、データへのアクセス制御を実施する
アプリケーション		—	<ul style="list-style-type: none"> • 認証後に受け取るアクセストークンとアクセスキー（APIキー）を送付する 	○	<ul style="list-style-type: none"> • CMP基盤のAPIへのアクセス認可を実施する • アプリケーション向けAPIキー、アクセストークンを管理する 	○	<ul style="list-style-type: none"> • アクセストークンに含まれる認証済みIDを用いてCMP基盤の機能、データへのアクセス制御を実施する 	
製品/部品/原材料		—	—	—	—	—	—	<ul style="list-style-type: none"> • 業務データを管理する
システム	ヒト	ユーザ	○	<ul style="list-style-type: none"> • ユーザと事業者のマッピング情報を保持し、CMP基盤の機能、データへのアクセス制御を実施する 	—	—	—	—
	空間	事業所	○	<ul style="list-style-type: none"> • 事業所と事業者のマッピング情報を保持し、CMP基盤の機能、データへのアクセス制御を実施する • 多層層での認可要件がある場合もインダストリーアプリケーションで制御する 	—	—	—	—
		ロール	○	<ul style="list-style-type: none"> • ロールと事業者のマッピング情報を保持し、CMP基盤の機能、データへのアクセス制御を実施する • 多層層での認可要件がある場合もインダストリーアプリケーションで制御する 	—	—	—	—

■ 補足：トラストに関する識別対象の定義

- ・ トラストに関する識別対象の定義は、蓄電池ガイドラインの考え方を流用する。
- ・ CMP 基盤のユースケースとして「ロール」の概念を考慮する必要がある。「ロール」は事業者・企業の部署相当という理解であり、その場合「システム」を構成する一要素となり、「事業所」と並列に整理できるものと想定する。

ガイドラインにおけるトラストの定義



[出典]

経済産業省・デジタルアーキテクチャ・デザインセンタ（DADC）、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

1.4.1.4 CMP 基盤

1.4.1.4.1 トレーサビリティ管理

各種法規におけるトレーサビリティ要求に遵守しつつ、CMP によって適切な情報伝達を実現する。

主な法規	主要なトレーサビリティに関する要求事項
Regulation 1907/2006 of concerning the Registration, Evaluation, Authorisation and Restriction of Chemicals (REACH 規則)	<ul style="list-style-type: none">• 製品中に含まれる高懸念化学物質 (SVHC) について、成形品 (article)重量の 0.1%以上含まれている場合、供給者は受領者 (顧客) にその情報を提供しなければならない。• 特定の条件下で、製品中の物質の合計量が年間 1 トンを超え、かつ意図的に放出される場合、その物質の登録が必要となる。
Directive 2011/65 on the restriction of the use of certain hazardous substances in electrical and electronic equipment (RoHS 指令)	<ul style="list-style-type: none">• 製造者、輸入者、および販売業者は、製品が RoHS 指令に準拠していることを保証し、関連する文書 (例えば適合宣言書) を作成・保管する義務がある。
Toxic Substances Control Act (TSCA/有害物質規制法)	<ul style="list-style-type: none">• 化学物質の製造や処理を行う者 (小規模製造業者や処理業者を除く) に対し、必要な報告書を提出し、記録を保持することを義務付ける。また、混合物や少量の化学物質の製造・処理に関しても同様に、必要な範囲で記録を保持し、報告書を提出することが求められる。
化学物質の審査及び製造等の規制に関する法律 (化審法)	<ul style="list-style-type: none">• 特定一般化学物質および優先評価化学物質の取り扱い事業者は、これらの化学物質を他の事業者に譲渡または提供する際に、物質の名称およびその特定化学物質であることの情報を提供するように努めることが求められる。

1.4.1.4.2 データ主権

データ主権の基本方針は、『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）（蓄電池 CFP・DD 関係）』を参考にする。

データ主権の確保（1 / 2）

本ガイドラインでは、事業者に関する情報であって、公にすることにより、当該事業者の権利、競争上の地位その他正当な利益を害するおそれがあるものについて、当該事業者が、他の事業者に同情報の利用を認めるに当たって、同情報の①利用相手、②利用条件、③保存場所等を決定することができる権利をデータ主権という。

データ主権確保の対象

スコープ	データ種別	データ主権確保の対象
各者単体	各者保有データ	各者が自由に扱うデータ
企業間	各者保有データ	各者が自由に扱うデータ
	流通データ	当事者間の合意のもとで扱うデータ
国・業界等	各者保有データ	各者が自由に扱うデータ
	流通データ	各コミュニティの合意のもとで扱うデータ

①利用相手の決定

利用相手を決定する例

対象	データアクセス	
	許可	不許可
直接取引あり	A社	許可・不許可
	B社	許可・不許可
今後取引可能性あり	C社	許可・不許可
	D社	許可・不許可
	E社	許可・不許可
自動車OEM	F社	許可・不許可
海外取引先	G社	許可・不許可
	H社	許可・不許可
第三者認証機関	I社	許可・不許可
データ連携システム運営事業者	J社	許可・不許可

Copyright © 2023 METI/IPA 60

データ主権の確保（2 / 2）

再掲：本ガイドラインでは、事業者に関する情報であって、公にすることにより、当該事業者の権利、競争上の地位その他正当な利益を害するおそれがあるものについて、当該事業者が、他の事業者に同情報の利用を認めるに当たって、同情報の①利用相手、②利用条件、③保存場所等を決定することができる権利をデータ主権という。

②利用条件の決定

利用条件の設定例

項目	具体例
第三者提供等の制限	第三者提供・利用許諾の禁止、事前同意の義務付け等
加工	加工処理や統計データ化されたデータの利用に制限
セキュリティ	データの暗号化を義務付け、高度な安全管理措置・セキュリティ環境の要求、守秘義務契約の締結等
データ粒度・範囲	営業秘密やノウハウを除去もしくは希薄化する程度にデータ内容を限定
利用目的・利用範囲	利用目的や範囲を制限
期間	利用できる期間を制限
利益配分・損失負担	当該データの利用により得た経済的利益や被った損失についてあらかじめ合意した方式に従って分配・負担することを規定
地域	データを活用できる国・地域を制限

出典：経済産業省データの活用に関する契約ガイドラインから一部抜粋

③保存場所の決定

データ提供者のニーズに合わせてデータ保存場所を選択する例

社内システムで一括管理したい

企業A

既存アプリと連携して管理したい

企業B

データを保持するコストを低減したい

企業C

データ保存場所	企業A	企業B	企業C
各者	✓	□	□
アプリ	□	✓	□
データ連携システム	□	□	✓

Copyright © 2023 METI/IPA 61

[出典]

経済産業省・デジタルアーキテクチャ・デザインセンタ（DADC）、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

データ主権とは、データ所有者が「利用相手」、「利用条件」、「保管場所」を決定できる権利である。

データ主権の確保を実現するため、CMPとして求める仕様は以下の通りとする。

データ主権の要件とCMPにおける仕様

データ主権の要件		CMPにおける仕様	実現レイヤ/システム
①利用相手の決定	• データの利用相手を自分で決定できる。	• データ提供者が、データ単位で開示先を指定できること。	CMPアプリ
		• データ提供者が指定した開示先以外には、データを開示しないこと。 • データ連携システム運営事業者は、データ提供者の許諾なしにデータへのアクセスができないこと。	CMP基盤
②利用条件の決定	• データの利用条件を自分で決定できる。	• データ提供者が、データ単位で登録・更新・削除を実施できること。	CMPアプリ
③保管場所の決定	• データの保管場所を自分で決定できる。	• データ提供者が、データの保管場所を指定できること。	CMPアプリ CMP基盤

1.4.1.4.3 トレードシークレット

トレードシークレットとは、企業活動における機密情報を守る行為を指し、CMP における製品に含有する成分情報や製品情報、製造手順、取引先情報などが該当する。

トレードシークレットに関する基本方針は、『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）』を参考にする。

トレードシークレットに関する基本方針



企業の営業秘密の保持やデータ主権の確保を実現するため、以下の4つの方針をトレードシークレットに関する基本方針とする。

- 1 国内外の法令の遵守に必要な情報は適正な契約のもとに必要最小限の相手や内容で共有する。
- 2 データの公開範囲はデータ利用者の意向を踏まえることを原則としてデータ提供者の同意を必要とする。
- 3 各者や業界の利益になるデータはデータ提供者が同意をした上で共有する。
- 4 第三者としてデータを取扱う事業者はデータ利用者・データ提供者にとって公正・公平を確保できる組織、プロセス、ガバナンスの仕組み等のもとに運営する（第三者とはデータ利用者・データ提供者以外を意味する）。

Copyright © 2023 METI/IPA 43

[出典]

経済産業省・デジタルアーキテクチャ・デザインセンタ（DADC）、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

トレードシークレットの基本方針を実現するための業務要件および機能要件は、『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 a 版（蓄電池 CFP・DD 関係）』と同じである。

トレードシークレットに関する要件			Duranos Ecosystem		
トレードシークレットの基本方針を実現するための業務要件及び機能要件をシステム又はルールに反映させること。					
方針定義	要件定義（業務要件）		実現手段定義（機能要件）	システム	ルール
1. サプライチェーン間で参照が必要な情報を必要最小限の相手や内容で共有する。	データ提供者はサプライチェーン間で参照が必要な情報を共有する。	①②	① 参加企業の正当性を確認する機能		
	共有データ毎に適切な公開範囲を設定可能とする。 - データ提供者のみ - 直接取引先 - 規則遵守等のため共有が必要な組織 - データ連携システム運営事業者*1	④⑤⑥⑦ ⑭⑮	① 参照が必要な情報の在処に関する参照データ所在登録(データカタログ)機能 ② 参照が必要な情報を登録する参照データ登録機能 ③ 利用ユーザを認証する機能 ④ 共有データ（所在・参照データ）の公開範囲を制御できるアクセス制御機能 ⑤ データ提供者が共有データ公開範囲を設定できる機能 ⑥ アクセス制御ログ用いた不正アクセス監視機能		
	データ連携システム運営事業者は取得したデータを目的外利用しない。	⑪	⑦ 第三者への漏えいを防ぐ参照データ暗号化機能 ⑧ 複数の管理者合意が必要なデータ管理項目作成・変更機能		
	データの管理項目(項目や公開範囲種別等)の変更はステークホルダから選出された複数管理者の合意を必要とする。	⑧ ⑫	⑨ 各者で作成可能なデータ管理項目作成・変更機能 ⑩ データの改ざんを防止する機能		
	企業やユーザのなりすましを防止できること。	⑩③⑬	⑪ データ連携システム利用の約款や各者間の契約雛形への反映 ⑫ 管理者（複数）を選定する基準の作成・運用		
データの改ざんを防止できること。	⑩⑬	⑬ データ連携システム運営は国又は国が指定する中立公平な立場の組織が行う。 ⑭ 不正アクセス者に対してペナルティを科す。 ⑮ データの公開範囲の初期設定基準の作成・運用 ⑯ データ不正利用・破損時のデータ提供者への補償に対応する。			
2. 公開範囲はデータ提供者の同意を必須とする。	データ提供者がビジネスニーズに応じてデータ公開範囲を決めることができる。	①②⑤			
3. 各者・業界の利益になるデータは同意の上共有する。	データ提供者がビジネスニーズに応じたデータを登録することができる。	①②④⑤ ⑨			
4. データ連携基盤の公正・公平性確保	データ連携システム運営者を公正・公平な組織・仕組みで実施する。	⑬			

*1：企業の機微な情報が含まれるため、データ連携システム運営事業者であってもすべてのデータが閲覧できるような権限は持たない。

Copyright © 2023 METI/IPA 44

[出典]

経済産業省・デジタルアーキテクチャ・デザインセンタ（DADC）、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a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

トレードシークレットを実現するため、CMPとして求める仕様は以下の通りとする。

トレードシークレット要件とCMPにおける仕様		システム	ルール
トレードシークレット実現手段定義（機能要件）	CMPにおける仕様	実現レイヤ/システム	
⑩参加企業の正当性を確認する機能	<ul style="list-style-type: none"> CMP参加登録時に、外部から識別できる情報（法人番号等）と紐づけることで、参加事業者の正当性を確認すること。 	トラストレイア	
①参照が必要な情報の在処に関する参照データ所在登録(データカタログ)機能	<ul style="list-style-type: none"> CMPとしては該当する業務要件はないため、対象外 	-	
②参照が必要な情報を登録する参照データ登録機能	<ul style="list-style-type: none"> データ提供者が、データ単位で登録・更新・削除を実施できること。 	CMPアプリ	
③利用ユーザを認証する機能	<ul style="list-style-type: none"> アプリケーションへアクセスする際に、利用ユーザ認証を実施すること。 	CMPアプリ	
	<ul style="list-style-type: none"> 基盤へアクセスする際に、アプリケーション認証または登録された事業者/システムの認証を実施すること。 	トラストレイア	
④共有データ（所在・参照データ）の公開範囲を制御できるアクセス制御機能	<ul style="list-style-type: none"> データ提供者が指定した開示先以外には、データを開示しないこと。 データ連携システム運営事業者は、データ提供者の許諾なしにデータへのアクセスができないこと。 	CMP基盤	
⑤データ提供者が共有データ公開範囲を設定できる機能	<ul style="list-style-type: none"> データ提供者が、データ単位で開示先を指定できること。 	CMPアプリ	
⑥アクセス制御ログ用いた不正アクセス監視機能	<ul style="list-style-type: none"> データの不正アクセス監視対策を実施すること。 	トランザクションレイア	
⑦第三者への漏えいを防ぐ参照データ暗号化機能	<ul style="list-style-type: none"> データの暗号化を実施すること。 	CMPアプリ CMP基盤	
⑧複数の管理者合意が必要なデータ管理項目作成・変更機能	<ul style="list-style-type: none"> 事業者間で共有するデータ項目の作成/変更は、運営事業者/アプリケーション事業者等のステークホルダ合意のもと実施するルールとする。 	CMPアプリ CMP基盤	
	<ul style="list-style-type: none"> データ提供者が、データ開示対象を指定できること。 	CMPアプリ	
⑨各者で作成可能なデータ管理項目作成・変更機能	<ul style="list-style-type: none"> データ提供者が指定した開示対象以外には、データを開示しないこと。 	CMP基盤	
	<ul style="list-style-type: none"> データの改ざん防止対策を実施すること。 	CMPアプリ CMP基盤	
⑪データ連携システム利用の約款や各者間の契約雛形への反映	<ul style="list-style-type: none"> CMPの運用ルールとして、実現手段定義の内容を整理すること。 	-	
⑫管理者（複数）を選定する基準の作成・運用			
⑬データ連携システム運営は国又は国が指定する中立公平な立場の組織が行う。			
⑭不正アクセス者に対してペナルティを科す。			
⑮データの公開範囲の初期設定基準の作成・運用			
⑯データ不正利用・破損時のデータ提供者への補償に対応する。			

以下条件に合致する対象をトレードシークレット対象とする。

- 企業間の取引関係情報（取引先としてどこが存在するのか）
- 企業の機密情報であり、取引関係が存在する企業間でのみ伝達が可能な情報
- 法規対応に必要な情報（製品情報、成分情報、ファーストアールティクルフラグ※1、遵法判断フラグ等）

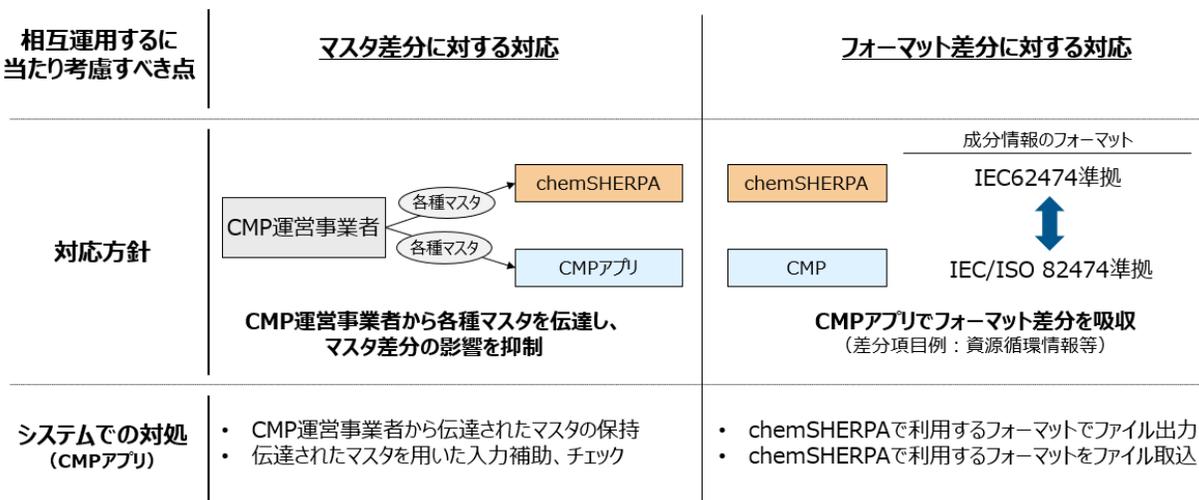
※1：ファーストアールティクルは、化学物質／混合物から、化学物質の含有量が固定される成形・乾燥・加熱・塗布等の製造工程を経て製造された最初の成形品（材料）を指す用語であり、ファーストアールティクルフラグは、ファーストアールティクルであることを示すフラグ。

1.4.1.5 他システムとの相互運用

1.4.1.5.1 CMP-chemSHERPA 間での相互運用の考え方

CMP 導入に伴い、chemSHERPA との相互運用を想定する。

相互運用期間中は、CMP 運営事業者からマスタ※1 を伝達することでマスタ差分影響を抑制し、フォーマット差分は CMP アプリにて変換することで吸収する。

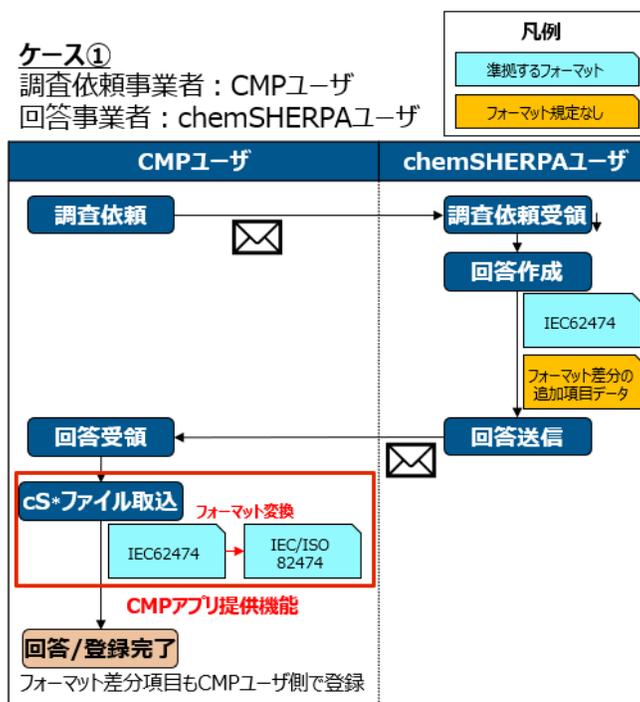


※1：情報伝達に際して、事業者間で解釈齟齬を起こさないために統一化された情報のリスト。データ入力時のチェックや入力補助にも利用する。(例：物質リスト)

1.4.1.5.2 CMP-chemSHERPA 間での相互運用を確保した業務の流れ

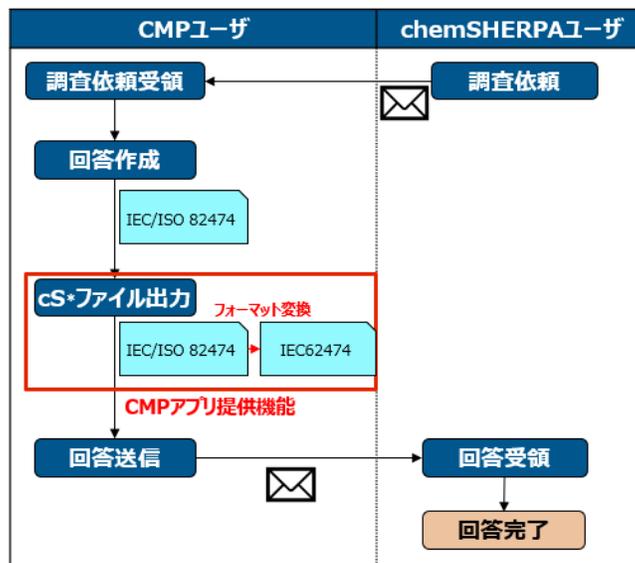
CMP-chemSHERPA 間での相互運用する際の業務の流れは以下の通り。

フォーマット差分に対しては、CMP アプリにて提供するフォーマット変換機能によって相互運用を実現する。



*cS = chemSHERPA

ケース②
 調査依頼事業者：chemSHERPAユーザ
 回答事業者：CMPユーザ



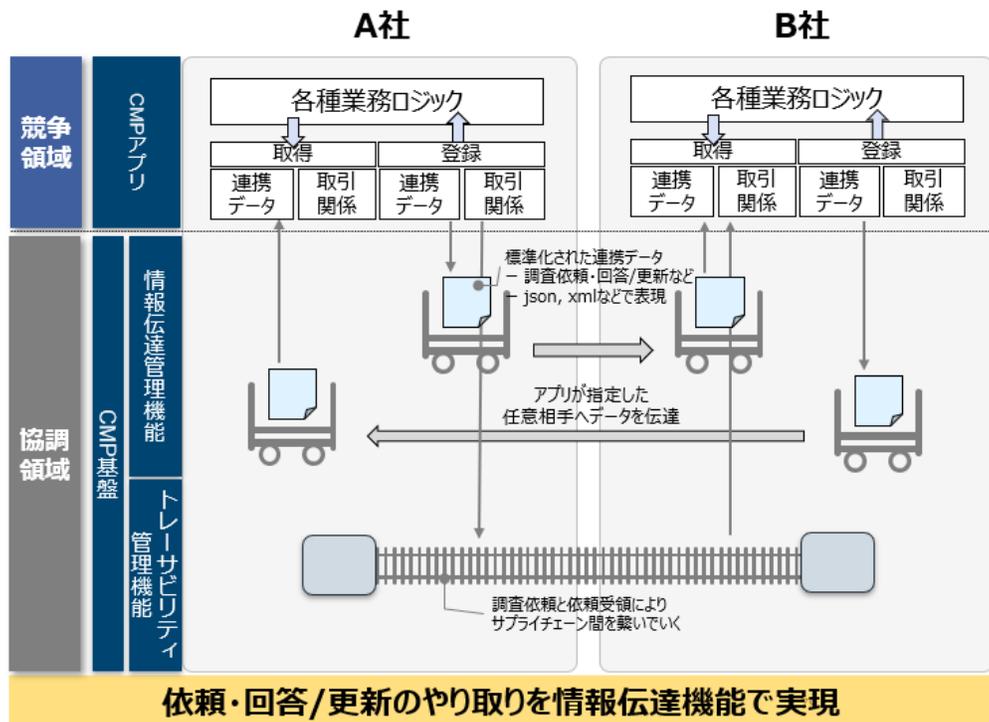
*cS = chemSHERPA

1.4.2 標準データモデル

1.4.2.1 CMP 基盤の基本機能について

■ 概要

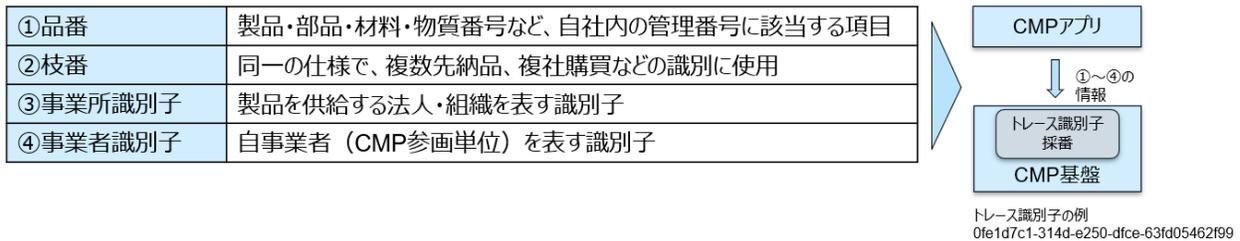
CMP 基盤は、依頼・回答/更新などの情報伝達機能とトレーサビリティ確保のための取引関係などを作成するトレーサビリティ管理機能で構成される。法規要件に基づく含有量などの算出ロジックや、個社内業務サポート機能は CMP アプリにて実施する前提である。



領域	役割
CMP アプリ	<ul style="list-style-type: none"> 法規要求内容、業務要件の実現 企業間で連携する業務データの作成機能の実現 業務効率化、利便性向上に資する機能の実現
CMP 基盤	<ul style="list-style-type: none"> 企業間の情報伝達を行う 情報伝達先は CMP アプリが指定し、CMP に参加する任意企業へ伝達可能とする（基盤では連携先の制御は行わない） 業務ロジックは保持せず、連携データ内容には関知しない、送り先へ運ぶ役割に徹する 連携データの履歴保持

■トレーサビリティ管理機能

- CMP 基盤にてデータとして管理する「モノ」をノードと呼び、ノードに対して採番される一意の ID をトレーサ識別子と呼ぶ。
- ノード同士を紐付けることで、「製品と購入品の関係」および「事業者間の取引関係」を CMP 基盤で管理して、サプライチェーンの追跡を可能にする。
- 各事業者のアプリにて登録される以下①～④の情報をもとに、トレーサ識別子が採番される。



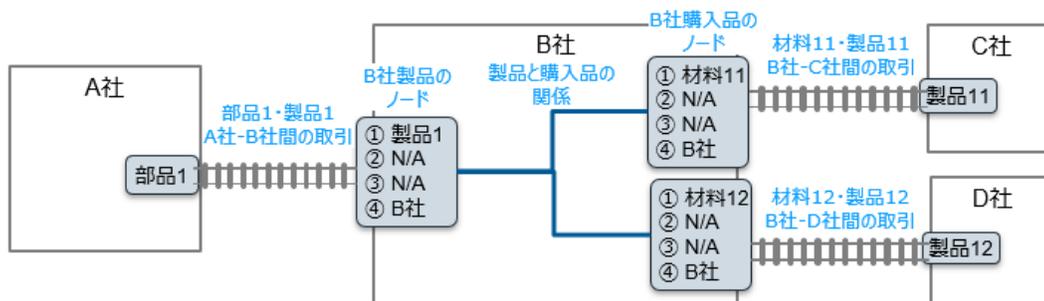
ノードと取引関係と製品と購入品の関係のイメージ

- ノードの作成粒度
 - 自事業者製品および購入品単位に作成
- 取引関係の作成粒度
 - 川下側との取引関係：自事業者製品単位に作成
 - 川上側との取引関係：購入品単位に作成
- 製品と購入品の関係の作成粒度
 - 自事業者製品と購入品の組み合わせ単位に作成

□ : ノード

||||||| : 取引関係 (事業者間での購入品・製品の紐付き)

— : 製品と購入品の関係 (自事業者内での製品・購入品の紐付き)

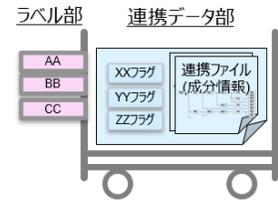


■ 情報伝達管理機能

- 事業者間での調査依頼・回答/更新は CMP アプリで登録された連携データを利用して伝達する。
- 連携データはトレーサビリティ管理機能で登録済みの取引関係上でのみ伝達可能とする。
- 連携データに含まれる情報は以下の通りとする。

連携データ

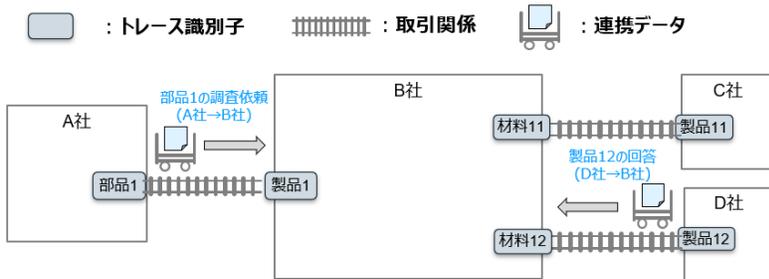
- ラベル部：CMP基盤にて利用する、連携元/先事業者や連携データの種別を識別するための情報
⇒主な連携項目：宛先事業者識別子、差出人事業者識別子、データ種別
- 連携データ部：CMP基盤にて関与しない、調査依頼および回答の業務的な情報
⇒主な連携項目：セクター、用途、ジャンル、ファーストアールティクルフラグ、成分情報ファイル



連携データのイメージ

■ 連携データの作成粒度

- 1回の調査依頼、1回の回答の都度作成



1.4.2.2 標準化ルール

1.4.2.2.1 ステータス管理

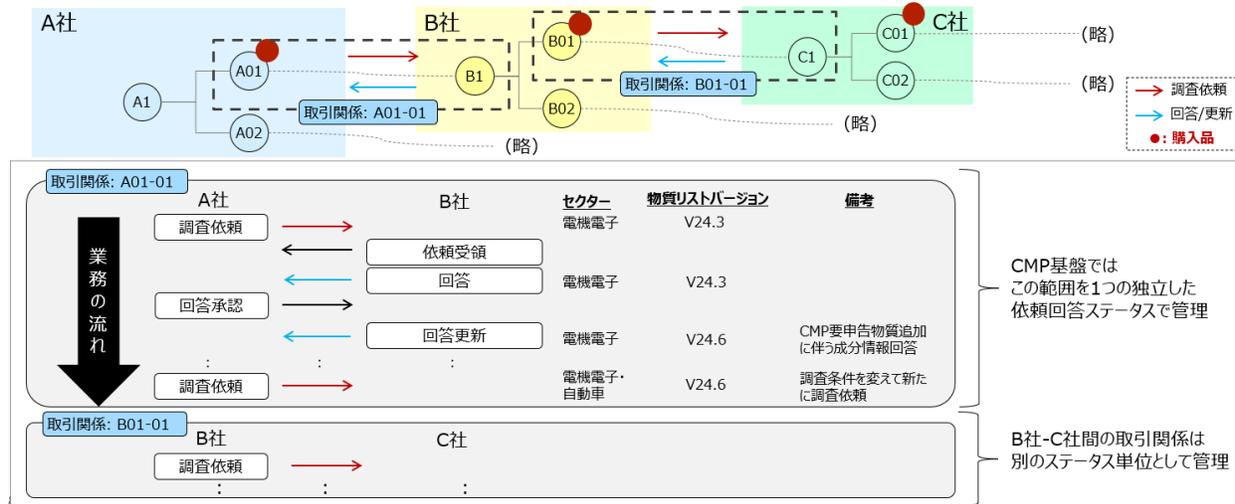
CMP 基盤において、管理するステータスは以下の通りである。

No	業務大分類	ステータス名	概要
1	調査依頼 回答登録 規制変更	依頼回答ステータス	調査依頼から回答に至る一連のプロセスの進捗状況を把握するためのステータス ※規制変更対応としての回答更新も含む
2	物質リスト共有 外部マスタ共有	通知確認ステータス	運営事業者が物質リスト等の情報更新通知をした際、各事業者の確認状況を把握するためのステータス

■ 1 : 依頼回答ステータス

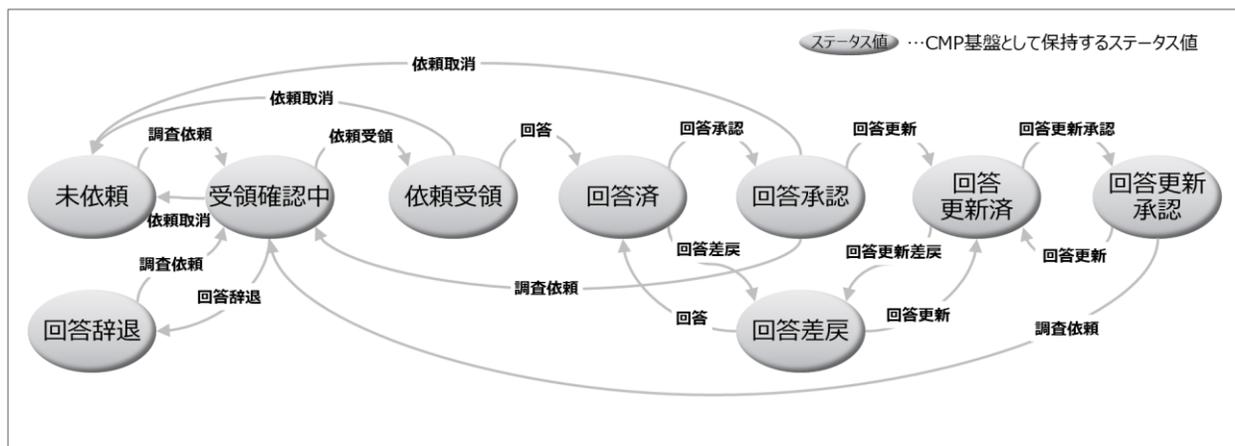
【概要】

- ・調査依頼から回答に至る一連のプロセスの進捗状況を把握するためのステータス。
- ・取引関係単位で保持する。（2社間のみに関じたステータスであることを意味する）
- ・再調査依頼をするケースにおいても、既存の取引関係で保持しているステータスで管理する。



【ステータス遷移】

- ・CMP アプリは、各事業者のユーザ操作に基づき遷移先のステータスを指定する。
- ・CMP 基盤は、CMP アプリにて指定されたステータスへ遷移させる。
- ・ステータス遷移のモデルケースを以下に示す。



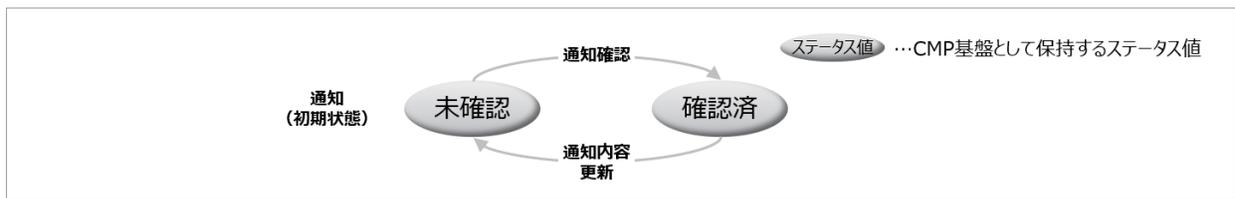
■ 2 : 通知確認ステータス

【概要】

- ・運営事業者が物質リスト等の情報更新通知をした際、各事業者の確認状況を把握するためのステータス。
- ・「通知単位 × 通知先事業者」の組み合わせ単位で保持する。
- ・CMP 基盤としては、運営事業者から配信された通知のみ管理対象とする。

【ステータス】

- ・CMP アプリは、運営事業者、参加事業者の以下のユーザ操作に基づき遷移先のステータスを指定する。
 1. 運営事業者による各事業者への通知情報（例：物質リスト更新）の配信または配信内容の更新
 2. 各事業者による通知の確認（開封）
- ・CMP 基盤は、アプリケーションにて指定されたステータスへ遷移させる。
- ・ステータス遷移のモデルケースを以下に示す。



1.4.2.2.2 データフォーマット

CMP 基盤において、製品含有化学物質管理の主たる伝達情報である成分情報は IEC/ISO 82474 準拠とする。

IEC/ISO 82474 では定義されていない伝達情報については、CMP 独自のデータフォーマットを定義する。以下のデータは CMP アプリで作成され、CMP 基盤の情報管理機能にて伝達される。

ファイルの種類	フォーマット	表記ルール
成分情報	IEC/ISO 82474 形式準拠	・表記言語は英語とする (IEC/ISO 82474 形式の表現方法に準拠する)
CMP 要申告物質ステータスフラグ※1	CMP 独自様式	
CMP 要申告候補物質ステータスフラグ※2	CMP 独自様式	

上記定義範囲外の CMP 独自の連携項目における表記は、別途表記ルールを定義する。

(連携項目の用途に応じて、表記言語についてはローカル言語を許可する方針で検討)

※1：CMP 要申告物質リストの更新に伴う伝達済みの成分情報への影響を示すフラグ。成分情報と同等の階層構造を保持する。

※2：CMP 要申告候補物質リストの更新に伴う成分情報への影響を示すフラグ。成分情報と同等の階層構造を保持する。

1.4.2.3 標準データモデル一覧

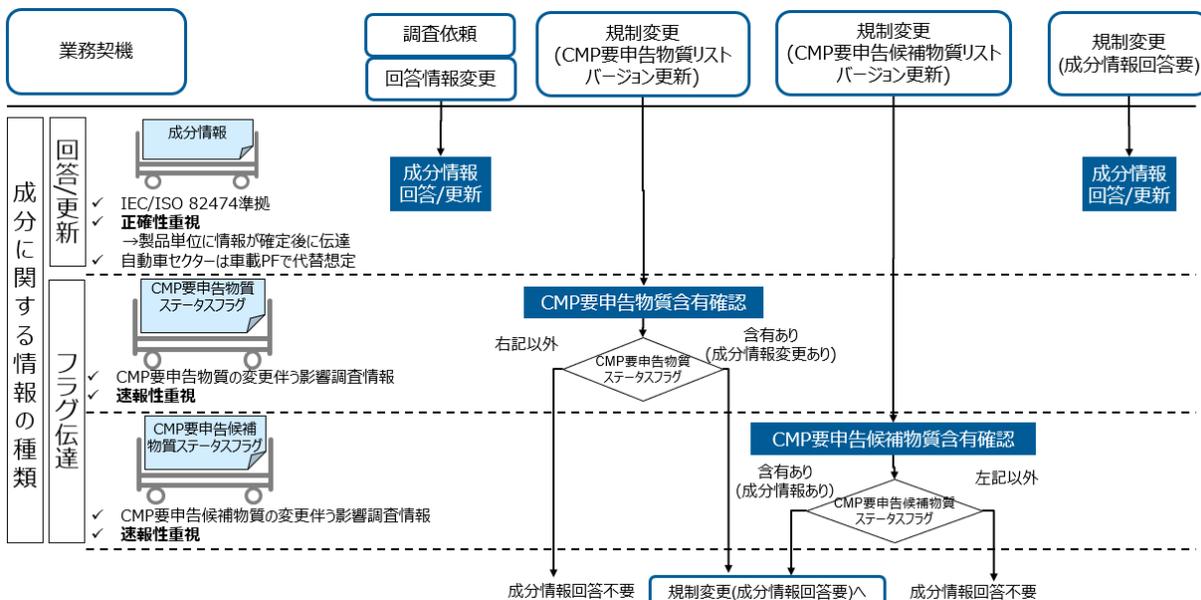
CMP を利用した場合の製品含有化学物質情報伝達における基本的なパターンを標準データモデルとして、以下の 3 モデルを定める。以降この 3 モデルの詳細について説明する。

モデル#	標準データモデル	業務契機	主な伝達対象	業務の流れ			
				川下事業者	川中事業者	川上事業者	運営事業者
1	川下事業者から調査依頼 ^{*1}	川下事業者	・成分情報				
2	規制変更に伴いCMP要申告物質ステータスフラグを伝達	運営事業者	・CMP要申告物質ステータスフラグ ・成分情報				
3	規制変更に伴いCMP要申告候補物質ステータスフラグを伝達	運営事業者	・CMP要申告候補物質ステータスフラグ				

*1) 本モデルでは、川下事業者から調査依頼を開始するケースを扱うが、CMPの仕組み上は、サプライチェーン上の任意の事業者から調査依頼を実施することが可能

■ 事業者間で伝達する成分に関連する情報の種類について

CMP を通じて事業者間で伝達する成分に関連する情報は「成分情報」、「CMP 要申告物質ステータスフラグ」、「CMP 要申告候補物質ステータスフラグ」の 3 種類を利用する。以下の通り、業務契機によって 3 種類の情報を使い分ける運用とする。



1.4.2.4 標準データモデル詳細

標準データモデルにおいて以下の凡例を用いて説明する。

凡例

- | | | |
|--|--|--|
|  : 一般物質 |  : 非申告物質
(非開示物質) |  : 調査依頼の流れ |
|  : CMP要申告物質 | |  : 回答/更新の流れ |
|  : 購入品 | |  : その他情報の流れ |
|  : 製品/部品/材料の親子関係 | | |
|  : 購入品である部品/材料と仕入先製品との紐付き | | |

1.4.2.4.1 標準データモデル# 1: 川下事業者から調査依頼

モデル#	標準データモデル	業務契機	主な伝達対象	業務の流れ			
				川下事業者	川中事業者	川上事業者	運営事業者
1	川下事業者から調査依頼	川下事業者	・成分情報	①調査依頼	②調査依頼	③回答	④回答

① 調査依頼登録 (A 社→B 社)

- ・ C 社にて製品い情報を登録する
- ・ A 社にて製品 1 情報と製品に関連する購入品情報 (材料あ) を登録する
- ・ A 社は登録した購入品情報を対象の B 社に調査依頼を行う
- ・ B 社は調査依頼を受領したことを確認する
- ・ B 社にて製品あ情報と製品に関連する購入品情報 (材料い) を登録する

製品構成イメージ



② 調査依頼登録 (B 社→C 社)

- ・ B 社は登録した購入品情報を対象の C 社に調査依頼を行う
- ・ C 社は調査依頼を受領したことを確認する

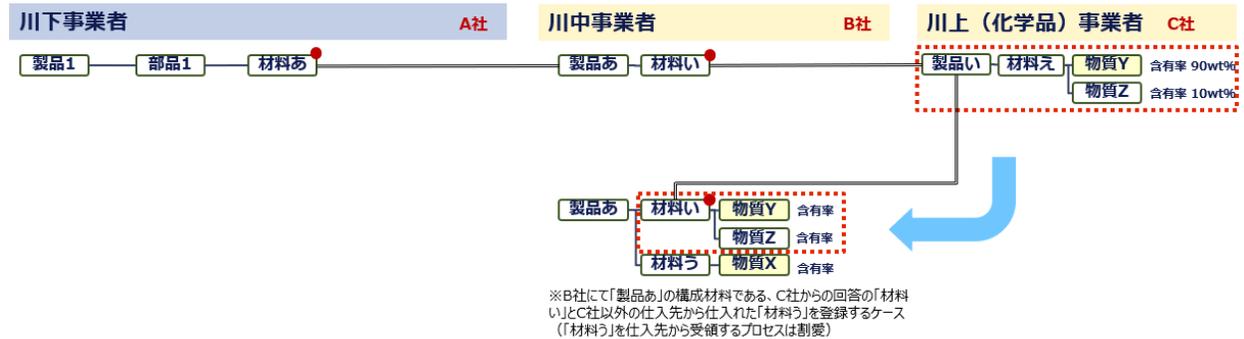
製品構成イメージ



③ 回答登録 (C社→B社)

- C社にて回答データを作成し、回答データをB社へ伝達を行う
- B社にて回答データを確認し、承認を行う

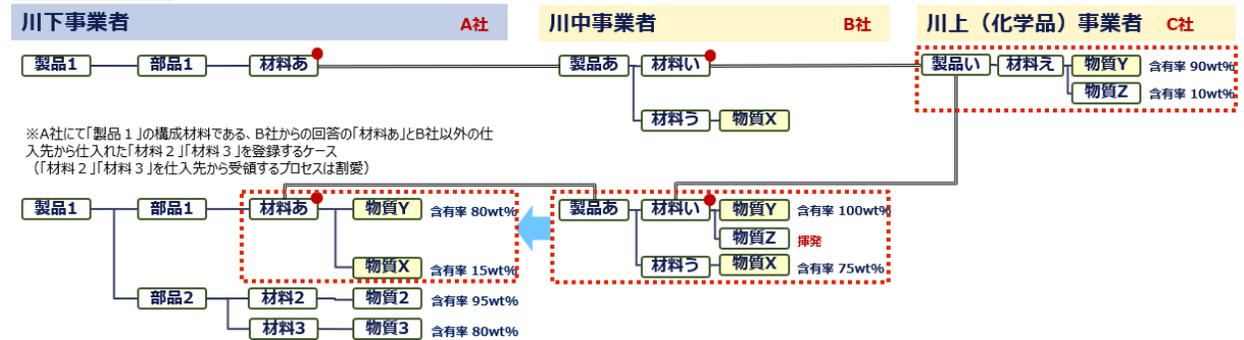
製品構成イメージ



④ 回答登録 (B社→A社)

- B社にて回答データを作成し、回答データをA社へ伝達を行う
- A社にて回答データを確認し、承認を行う
- A社はB社や他の購入品に対する回答データを踏まえて製品1としての製品登録を行う

製品構成イメージ



1.4.2.4.2 標準データモデル#2: 規制変更に伴い CMP 要申告物質ステータスフラグを伝達

モデル#	標準データモデル	業務契機	主な伝達対象	業務の流れ			
				川下事業者	川中事業者	川上事業者	運営事業者
2	規制変更に伴いCMP要申告物質ステータスフラグを伝達	運営事業者	・CMP要申告物質ステータスフラグ ・成分情報	③フラグ伝達 ⑤回答更新	①物質リスト更新通知 ②フラグ伝達	④回答更新	CMP要申告物質ステータスフラグ 成分情報

① 物質リスト更新及び通知受領確認

- ・ 運営事業者から各者へ物質リストの更新を通知する
- ・ 各者は通知されたバージョンの物質リストを取得する
- ・ 各者は通知情報に受領確認を意味するタイムスタンプを打刻する



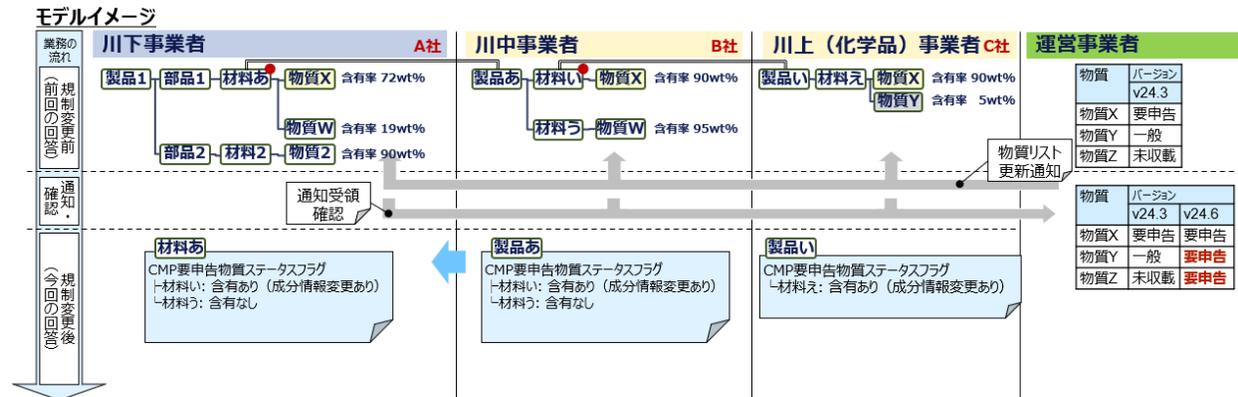
② CMP 要申告物質ステータスフラグの伝達 (C社→B社)

- ・ C社は対象の物質リストを用いて製品いに含まれる材料の回答更新の要否を確認し、CMP 要申告物質ステータスフラグに「含有あり(成分情報変更あり)」を設定する
- ・ C社はB社からの過去の調査依頼に対して、CMP 要申告物質ステータスフラグの伝達を行う



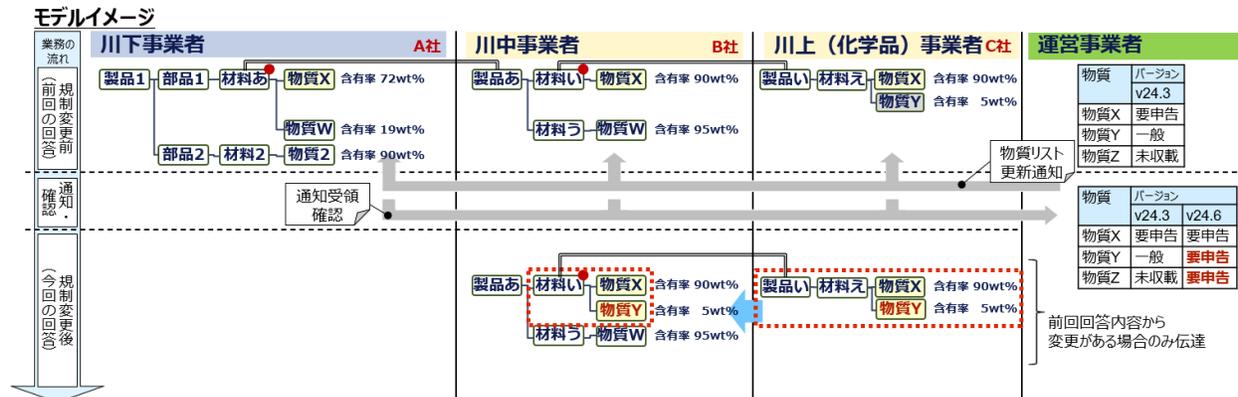
③ CMP 要申告物質ステータスフラグの伝達 (B社→A社)

- B社はC社から伝達されたCMP 要申告物質ステータスフラグを確認する
- B社は対象の物質リストを用いて製品あに含まれる材料の回答更新の要否を確認し、CMP 要申告物質ステータスフラグに「含有あり(成分情報変更あり)」を設定する
- B社はA社からの過去の調査依頼に対して、CMP 要申告物質ステータスフラグの伝達を行う



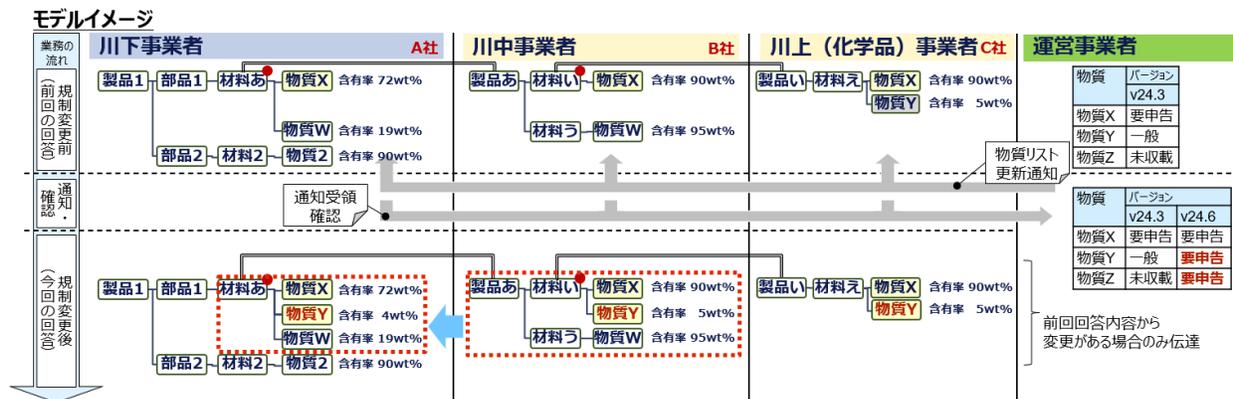
④ CMP 要申告物質を踏まえた回答更新 (C社→B社)

- C社は製品い に物質 Y が含まれていることを確認し、物質 Y を追加登録した回答データを登録する
- C社はB社からの過去の調査依頼に対して、回答更新を行う



⑤ CMP 要申告物質を踏まえた回答更新 (B社→A社)

- B社はC社から受領した回答内容を取得し、製品あとしての成分情報を再計算する
- B社は製品あの回答データを登録する
- B社はA社からの過去の調査依頼に対して、回答更新を行う
- A社はB社や他の購入品に対する回答データを踏まえて製品1としての製品情報の更新を行う



1.4.2.4.3 標準データモデル#3: 規制変更に伴い CMP 要申告候補物質ステータスフラグを伝達

モデル#	標準データモデル	業務契機	主な伝達対象	業務の流れ			
				川下事業者	川中事業者	川上事業者	運営事業者
3	規制変更に伴いCMP要申告候補物質ステータスフラグを伝達	運営事業者	・CMP要申告候補物質ステータスフラグ	①物質リスト更新通知 ②フラグ伝達 ③フラグ伝達			

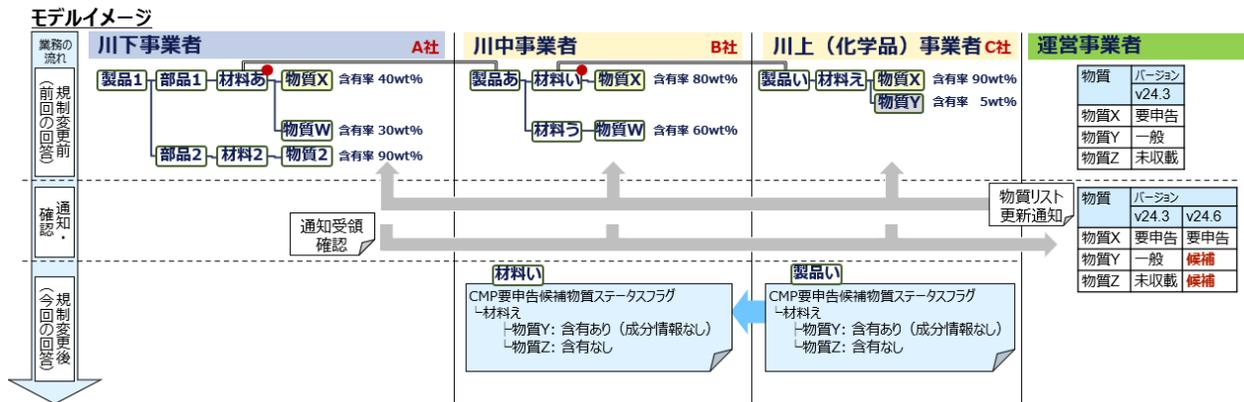
① 物質リスト更新及び通知受領確認

- ・ 運営事業者から各者へ物質リストの更新を通知する
- ・ A社、C社は通知されたバージョンの物質リストを取得する
- ・ A社、C社は通知情報に受領確認を意味するタイムスタンプを打刻する
- ・ B社は通知に対し受領確認を行わず、運営事業者から通知の受領確認を督促される



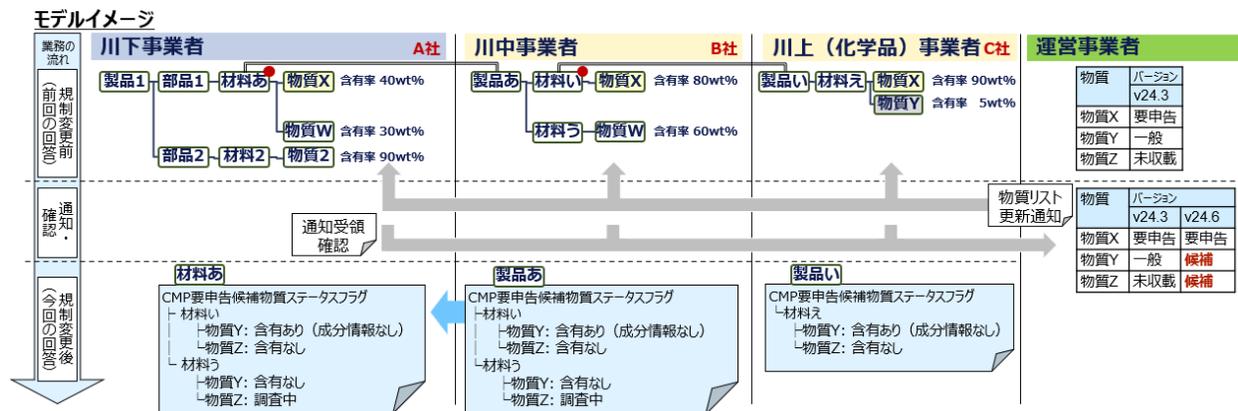
② CMP 要申告候補物質ステータスフラグの伝達 (C社→B社)

- 製品いに対象物質 Y の含有を確認し、CMP 要申告候補物質ステータスフラグに「含有あり(成分情報なし)」を設定する
- 製品いに対象物質 Z の含有を確認し、CMP 要申告候補物質ステータスフラグに「含有なし」を設定する
- C社はB社からの過去の調査依頼に対して、CMP 要申告候補物質ステータスフラグの伝達を行う



③ CMP 要申告候補物質ステータスフラグの伝達（B 社→A 社）

- B 社は C 社からの CMP 要申告候補物質ステータスフラグを踏まえて製品あとしての CMP 要申告候補物質ステータスフラグを設定する
- B 社は A 社からの過去の調査依頼に対して、CMP 要申告候補物質ステータスフラグの伝達を行う
- A 社は B 社や他の購入品に対する CMP 要申告候補物質ステータスフラグを踏まえて製品 1 としての製品情報の更新を行う
- A 社は製品 1 の CMP 要申告候補物質ステータスフラグを設定する



1.4.2.5 特殊な商流・業務パターンにおける運用について

特殊な商流における運用については、原則、標準データモデルを利用する。

主体者：○ 関連者：△

番号	業務大分類	業務中分類	業務小分類	業務概要	化学品事業者	川中事業者	最川下事業者	運営事業者
70	サプライチェーン支援	バススルー	バススルー	ものに対し変更を加えない商社等は、取引先の回答情報を過去提供した顧客へ自動転送を可能とする	○	○	○	
71		代理登録	代理登録	依頼先がCMP未登録の場合、依頼先の代わりに部品、材料、組成登録を行う	○	○	○	
72			依頼代行	さらに川上の企業に調査依頼を行う	○	○	○	
73		支給品登録	支給品登録	支給部品・材料の成分情報を川上企業へ提供する	○	○	○	
74		複数購買	調査依頼	同一部品、材料を複数社への調査依頼を可能とする	○	○	○	
75			回答登録・伝達	最悪値など一定ルールに基づき当該部品、材料の組成とし、川下へ伝達	○	○	○	
76		依頼先変更	調査依頼・回答	調査済みの依頼に関し、依頼先を変更する	○	○	○	
77			伝達停止	伝達停止	廃業、EOL等で伝達停止になった事象を情報伝達する	○	○	△

[出典]

CMP タスクフォース/要件定義 WG/システム WG、CMP システム要件定義書 v1.1、2025 年 2 月掲載予定

■ケース1：パススルー

モノに対し変更を加えない商社等の事業者は、納入先事業者からの調査依頼や仕入先事業者からの回答/更新を自動転送可能とする。

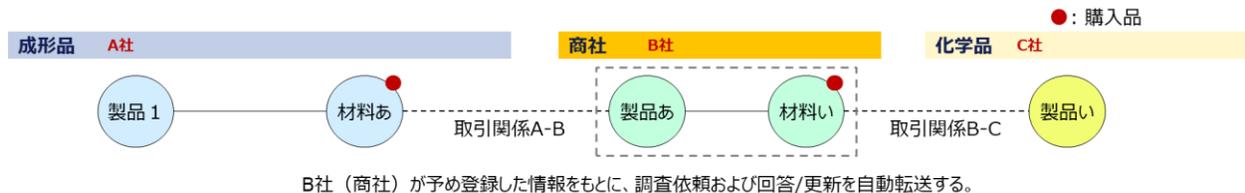


【出典】

経済産業省・デジタルアーキテクチャ・デザインセンタ（DADC）、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

【モデル】



【前提】

自動転送された調査依頼・回答内容については転送元である直送企業が責任を負う。

【ルール】

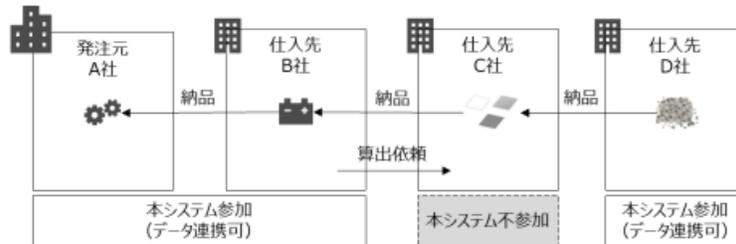
なし

【システムでの対処】

- CMP アプリ : パススルー自動転送
- CMP 基盤 : 対処なし（標準データモデルに準ずる）

■ケース 2 : 代理登録 (1/2) – CMP 未登録事業者と CMP 外で依頼・回答を行う –

回答事業者が CMP 未登録の場合、調査依頼事業者が CMP 外にて回答事業者との調査依頼・回答/更新のやり取りを行うことで、調査依頼事業者が CMP にて成分情報を登録することを可能とする。



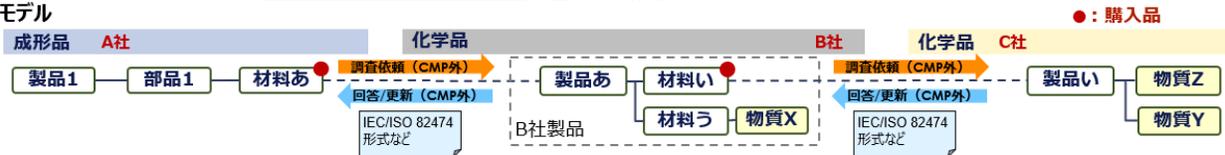
[出典]

経済産業省・デジタルアーキテクチャ・デザインセンタ (DADC)、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

【モデル】

モデル



- ・ B社がB社製品としての「製品あ」の成分情報を回答/更新を、B社の責任においてCMP外で実施する。
- ・ B社が「製品あ」の成分情報作成に必要なB社の仕入先であるC社からの情報収集を、B社の責任において実施する。

【前提】

CMP 未登録事業者が仕入先/納入先事業者と CMP 外で調査依頼・回答/更新の手段をもつ。

【ルール】

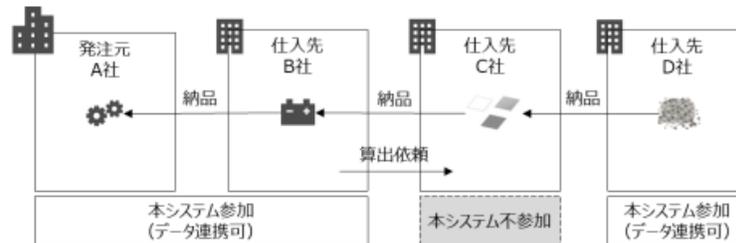
なし

【システムでの対処】

- CMP アプリ : 対処なし
- CMP 基盤 : 対処なし (標準データモデルに準ずる)

■ケース 2 : 代理登録 (2/2) - CMP 未登録事業者の納入先事業者が代行して調査依頼 -

回答事業者が CMP 未登録の場合、回答事業者の代わりに調査依頼事業者が CMP にて回答事業者の仕入先事業者との調査依頼・回答/更新のやり取りを行うことで、調査依頼事業者が成分情報を登録することを可能とする。

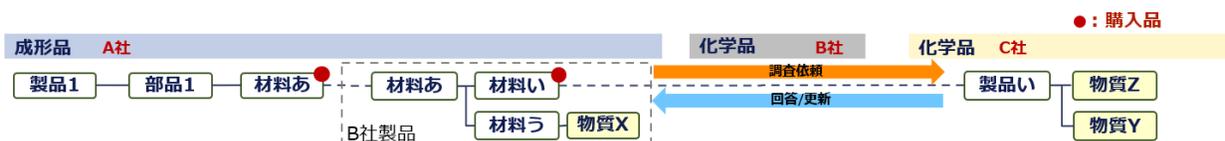


[出典]

経済産業省・デジタルアーキテクチャ・デザインセンタ (DADC)、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

【モデル】



- ・ B社は、CMPに未登録である。A社は、B社に了解の上、B社の代わりに「材料あ」、「材料い」、「物質X」の登録を行う。
- ※ ただし、A社がB社の依頼代行をする場合、B社-C社の取引関係を知ることになり得るため、事前にB社との合意形成が必要。

【前提】

調査依頼事業者 (上図 A 社)、CMP 未登録事業者 (上図 B 社)、CMP 未登録事業者の仕入先事業者 (上図 C 社) は、各事業者間のルールに基づき、調査依頼事業者から CMP 未登録事業者の仕入先事業者へ直接調査依頼をしてよい旨の承諾を、三者間で得る。

【ルール】

CMP 未登録事業者 (上図 B 社) の購入品・仕入先の情報や、製品 (上図「材料あ」) の製造プロセスにおける組成変化や材料構成 (比率、重量) など、調査依頼事業者にとって必要な情報は、CMP 外で問合せをする。

【システムでの対処】

CMP アプリ : 対処なし

CMP 基盤 : 対処なし (標準データモデルに準ずる)

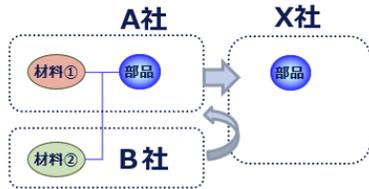
■ケース3：支給品（1/2） - 自社で材料構成（比率、重量）が認識できていない場合 -

実際のモノの流れに合わせて CMP 上の取引関係を作成することで支給品を含めた成分情報の伝達を可能とする。

支給品のイメージ

A社は自社から指定された（支給された）材料や部品を使ってB社の材料と組み合わせて自社向けの部品を製造

例



[出典]

CMP タスクフォース/要件定義 WG/システム WG、CMP システム要件定義書 v1.1、2025 年 2 月掲載予定

【モデル】



処理の流れを材料（B社⇔X社⇔A社）と部品（A社⇔X社）に展開することで標準データモデルに準ずる

【前提】

なし

【ルール】

なし

【システムでの対処】

CMP アプリ : 対処なし

CMP 基盤 : 対処なし（標準データモデルに準ずる）

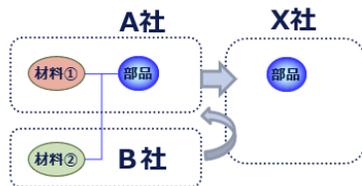
■ケース3：支給品（2/2） - 自社で材料構成（比率、重量）が認識できている場合 -

支給品メーカーと部品メーカーそれぞれから成分情報を受領し、それをもとに支給品を含めた成分情報の登録を可能とする。

支給品のイメージ

A社は自社から指定された（支給された）材料や部品を使ってB社の材料と組み合わせて自社向けの部品を製造

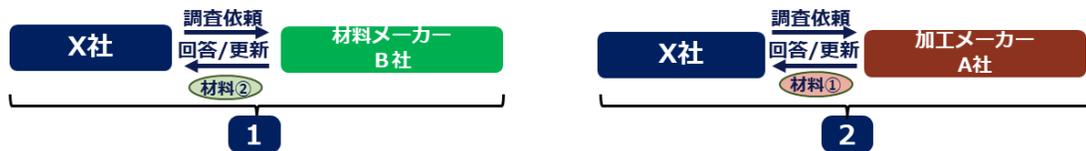
例



[出典]

CMP タスクフォース/要件定義 WG/システム WG、CMP システム要件定義書 v1.1、2025 年 2 月掲載予定

【モデル】



処理の流れを材料①（A社↔X社）と材料②（X社↔B社）に展開することで標準データモデルに準ずる。
A社、B社から受領した回答をもとに、X社にて認識する材料構成（比率、重量）を用いて部品の成分を算出する。

【ルール】

なし

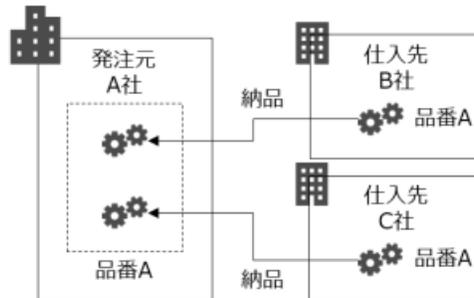
【システムでの対処】

CMP アプリ : 対処なし

CMP 基盤 : 対処なし（標準データモデルに準ずる）

■ケース4：複社購買

同一部品、材料について複数社への調査依頼を可能とする。



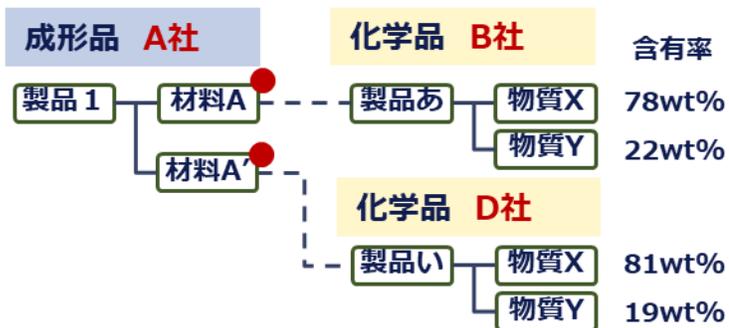
[出典]

経済産業省・デジタルアーキテクチャ・デザインセンタ（DADC）、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

【モデル】

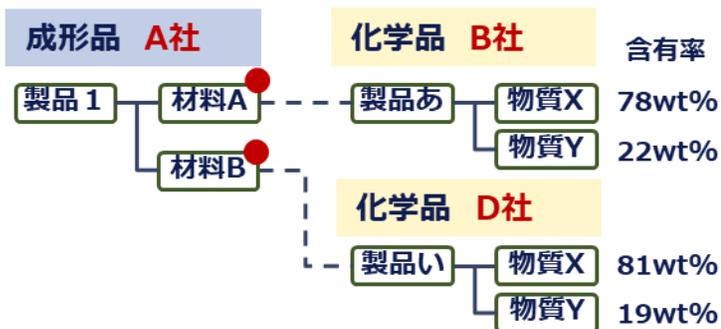
1 A社において同一品番で購入品を管理している場合



品番の補助項目を用いて区別する。

（CMP 基盤上は異なる購入品として扱い、アプリ側で同一のものとして扱う）

2 A社において別品番で購入品を管理している場合



別品番であるため、CMP 基盤上も別の部材として扱う。

【前提】

なし

【ルール】

調査依頼事業者（上図 A 社）は納入先事業者へ納入する自社製品の成分情報を作成する際に、事業者間のルールに基づき成分情報を作成し伝達する。

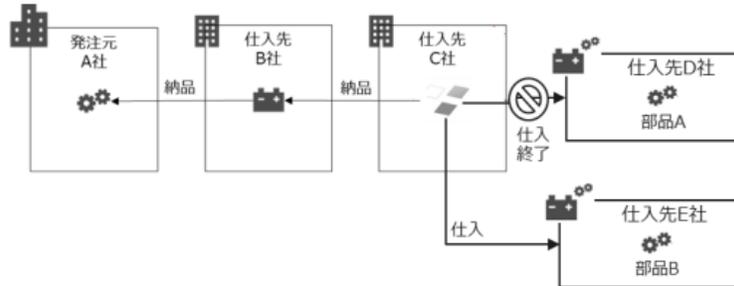
【システムでの対処】

CMP アプリ : 対処なし

CMP 基盤 : 対処なし（標準データモデルに準ずる）

■ケース 5 : 依頼先変更

調査済みの依頼に関し、依頼先を変更することを可能とする。

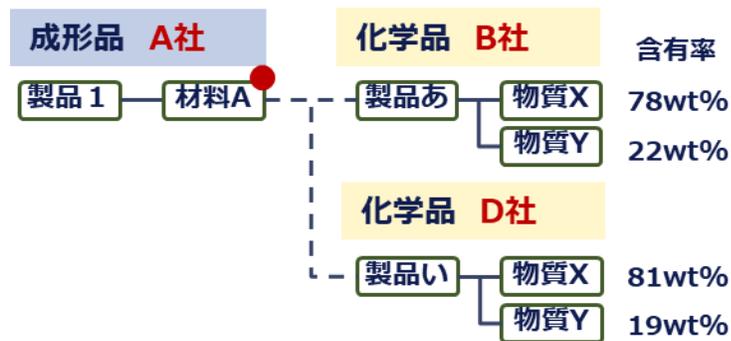


【出典】

経済産業省・デジタルアーキテクチャ・デザインセンタ（DADC）、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

【モデル】



依頼先が B 社から D 社に変更された場合は、新規に調査依頼を実行する。

【前提】

なし

【ルール】

なし

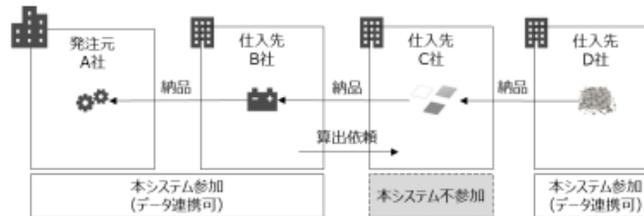
【システムでの対処】

CMP アプリ : 対処なし

CMP 基盤 : 対処なし (標準データモデルに準ずる)

■ケース6：伝達停止

廃業、EOL（End-of-life）等で伝達停止となった事象を情報伝達する。



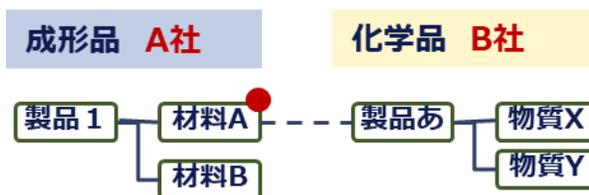
- 廃業は、CMP に不参加状態となることを意味し、EOL は製品の生産・販売停止を意味する。
- いずれのケースにおいても、その後の情報伝達は停止することとなるが、停止後も過去データは原則削除されない。

[出典]

経済産業省・デジタルアーキテクチャ・デザインセンタ（DADC）、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

【モデル】



【前提】

なし

【ルール】

事業者間での廃業・EOLに関する情報は、CMPの情報問合せ機能の利用により伝達するか CMP 外で個別に伝達をする。

【システムでの対処】

CMP アプリ : 対処なし

CMP 基盤 : 対処なし（標準データモデルに準ずる）

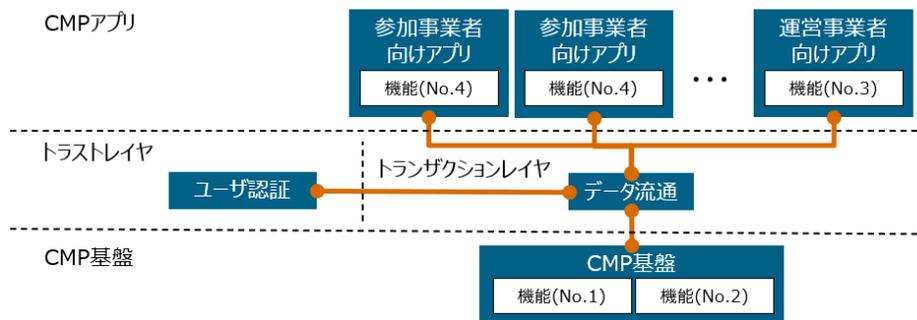
1.5 機能分割

1.5.1 機能分割方針

CE 情報流通プラットフォームのユースケースとして CMP を実現するに当たり、ユースケース固有の機能はトラストレイヤ、トランザクションレイヤには実装しないため、CMP 基盤/CMP アプリに対して以下の機能分割方針を定めている。

サプライチェーン上の幅広い企業での情報伝達に必要となる機能は CMP 基盤に配置し、各事業者の事業特性/業界特性に応じた機能は CMP アプリに配置することにより、将来的なユースケース拡張に対応する。

#	機能配置層	概要	利用ユーザ	機能特性	備考
1	CMP基盤	サプライチェーン内における企業間の情報伝達に必要な機能	-	・ユースケースに依存しない情報伝達に必要な機能（プラットフォーム標準）	蓄電池トレーサビリティ管理システムを流用
2				・製品含有化学物質・資源循環情報の伝達に必要な機能	
3	CMPアプリ	各事業者の事業特性/業界特性に依存する製品含有化学物質・資源循環情報管理固有の機能	運営事業者	・製品含有化学物質・資源循環情報に関する情報伝達を運営するために必要な機能	
4			参加事業者	・製品含有化学物質・資源循環情報を伝達するために必要な機能 ・各事業者の競争力の源泉となる機能 ・業務効率化・利便性向上に資する機能	



1.5.2 データ分割方針

CMP 基盤と CMP アプリに適切にデータ配置することで、プラットフォームとしての拡張性や柔軟性と、参画事業者の自由度の確保を目指す。

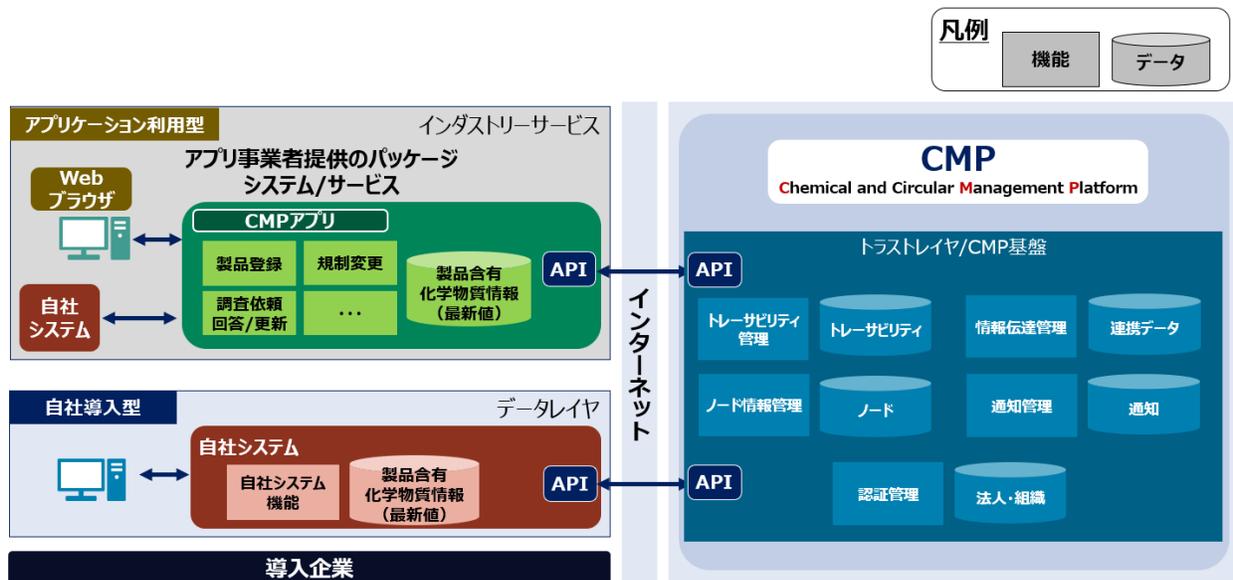
データの特性に応じた分割方針を以下に示す。

#	データ種別	観点	データ配置層		概要
			CMPアプリ	CMP基盤	
1	取引データ	活用範囲	事業者内	事業者間・全事業者	事業者の枠を超えて伝達する情報は、CMPの CMP基盤 を経て伝達
2		原本性	事業活動情報 (例：ユーザ利便性のための集計データ 等)	法規関連情報 (例：物質バージョンリストアップデート通知 等)	法規に関連する情報などCMP全体で共通的に定義すべき情報は CMP基盤 で保持 各事業者の事業活動に必要なデータは CMPアプリ で保持
3		秘匿性	CBIに抵触するデータ	公益性がある開示可能なデータ (例：回答 等)	参画事業者全体の便益に寄与する情報は、提供者の同意の上で CMP基盤 に保持し伝達
4			識別子 + 実データ	識別子	トレードシークレットを確保しつつ、サプライチェーン内の商流を構成するために必要な識別子は CMP基盤 に配置
5		時系列	最新値	報告値	CMP基盤 では、報告時点の値のみ保持
6		管理粒度	集計値、集計データ	単一データ	各事業者の業務遂行のために必要なデータの集計等については CMPアプリ に実施、管理
7	マスタデータ	活用範囲	事業者内	事業者間・全事業者	取引関係情報などの事業者の枠を超えて共有する情報は、CMPの CMP基盤 を経て伝達
8		原本性	事業活動情報	法規関連情報	法規に関連する情報などCMP全体で共通的に定義すべき情報は CMP基盤 で保持 各事業者の事業活動に必要なデータは CMPアプリ で保持
9		秘匿性	識別子 + 実データ	識別子	トレードシークレットを確保しつつ、サプライチェーン内の商流を構成するために必要な識別子 CMP基盤 に配置 ただし、物質リストなど CMPアプリ で原本管理するマスタは実データも保持

1.5.3 機能構成図

データ配置基準、機能配置基準を踏まえた CMP 全体のデータ・機能の配置は以下の通り。

CMP アプリや自社システムは、API を介して CMP が提供する機能を利用する。



2 機能編

本節では、システム化業務・機能に対して、機能配置基準に基づき実装するシステム（CMP アプリ、トラストレイヤ、CMP 基盤）を定義する。CMP 基盤・トラストレイヤに実装する API の一覧は、『2.2.1.2 API 一覧』に記載。

2.1 機能一覧

CMP システム要件定義書に記載の機能をもとに、実装レイヤ/システムの整理結果を以下に示す。

業務分類	業務名	機能名	概要	実装レイヤ/システム (主体：○、関連：△)				備考
				CMP 基盤	フロントレイヤ	CMP アプリ (運営事業者向け)	CMP アプリ (参画事業者向け)	
伝達準備	利用者 登録	企業部門 登録・更新	CMP への企業・部門の登録・更新を行う		△	○	○	
		取引関係登録・ 更新	CMP 企業一覧に基づき、取引先関係の登録・更新依頼を行う				○	
		取引関係承認	取引先関係依頼に対し、承認を行う				○	
		取引関係承認 受領	取引先関係依頼に対し、承認結果を受領する（調査依頼が可能となる）				○	
		ユーザ登録・ 更新	企業・部門に属するユーザ（管理者、担当者）・ロールの登録・更新を行う				○	
	物質 リスト 共有	物質リスト 登録・更新	物質リストの登録・更新を行う	△		○		
		物質リスト配信	登録（更新）された物質リストを全企業・部門へ配信する	△		○		
		物質リスト照会・ 受領確認	配信された物質リストの照会を行い、受領確認を返信する	△		○	○	
	外部 マスタ 共有	外部マスタ 登録・更新	各種外部マスタの登録・更新を行う	△		○		フェーズ 2 以 降実装検討 中
		外部マスタ配信	各種外部マスタを全企業・部門へ配信する	△		○		
外部マスタ照会		配信された外部マスタの照会を行う	△		○	○		
製品登録	化学品 登録	化学品・購入品 登録・更新・照 会	化学品の購入品を登録・更新・照会する	△			○	
		化学品登録・更 新・照会	購入品を引用して自社の化学品を登録・更新・照会する	△			○	
	成形品 材料 登録	成形品・購入品 登録・更新・照 会	成形品の購入品（材料）を登録・更新・照会する	△			○	
		成形品材料登 録・更新・照会	購入品を引用して自社の成形品を登録・更新・照会する	△			○	
	部品 登録	構成部品登録・ 更新・照会	自社の製品を構成する部品の構成表（BOM）を登録・更新・照会する	△			○	
		製品・部品登 録・更新・照会	自社の製品、または部品を登録・更新・照会する	△			○	

業務分類	業務名	機能名	概要	実装レイヤ/システム (主体：○、関連：△)				備考
				CMP 基盤	トラストレイヤ	CMP アプリ (運営事業者向け)	CMP アプリ (参画事業者向け)	
調査依頼 回答	調査依頼	調査依頼 登録・照会	調査依頼の登録・更新および状況の照会を行う	△			○	
	依頼受領 確認	依頼内容照会	顧客からの調査依頼の照会を行う	△			○	
		依頼受領登録	顧客からの調査依頼に対し、受領確認 (回答辞退含む)を行う	△			○	
	回答データ 作成	含有集計	化学品、材料、部品の成分情報から製品の含有化学物質の集計を行う				○	
		回答データ 作成	集計結果をもとに遵法確認し、顧客向けの回答データを作成する				○	
	回答登録	回答登録 ・更新	調査依頼に対する回答（成分情報）の登録・更新を行う	△			○	
		回答承認	調査依頼に対する回答（成分情報）の承認を行う	△			○	
	回答受領 確認	回答内容照会	取引先からの回答データを照会する	△			○	
		回答受領登録	取引先からの回答データに対し、承認 (差し戻しを含む)を行う	△			○	
	依頼伝達 確認	依頼伝達照会	川下からの調査依頼の伝達先がファースト ア－ティクルか否かを照会する	△			○	フェーズ 2 以降実装 検討中
	回答要求	回答要求	取引先への回答要求を行う	△			○	
	回答伝達 確認	回答伝達確認	回答情報の伝達先を確認する	△			○	フェーズ 2 以降実装 検討中
	情報変更	調査依頼変更	調査依頼変更	調査依頼・回答の各機能に実装				
回答情報変更			調査依頼・回答の各機能に実装					
規制変更	規制変更	物質リスト 登録・更新	物質リスト共有の各機能に実装					
		物質リスト配信	物質リスト共有の各機能に実装					
		物質リスト照 会・受領確認	物質リスト共有の各機能に実装					
		CMP 要申告 物質ステータス フラグ伝達	CMP 要申告物質ステータスフラグの更 新・伝達を行う	△			○	
		CMP 要申告 候補物質ステ ータスフラグ伝 達	CMP 要申告候補物質ステータスフラグの 更新・伝達を行う	△			○	

業務分類	業務名	機能名	概要	実装レイヤ/システム (主体：○、関連：△)				備考
				CMP 基盤	マイレスタブレット	CMP アプリ (運営事業者向け)	CMP アプリ (参画事業者向け)	
オプション 情報伝達	遵法判断 情報	遵法情報調 査依頼	調査依頼・回答の各機能に実装					
		遵法確認照 会・確認入力	顧客からの遵法確認依頼に基づき、遵 法確認を行う（回答登録と連動）	△			○	
	SCIP 情報	SCIP 情報 調査依頼	調査依頼・回答の各機能に実装					
		SCIP 情報 回答	顧客からの SCIP 情報要求に対し、 SCIP 情報を登録する（回答登録と連 動）	△			○	
	情報問合せ	情報問合せ 入力・照会	取引先・顧客に対し、非定型の問合せ を行う（さらに連携先への転送も可 能）	△			○	フェーズ2以降 実装検討中
		情報問合せ 履歴照会	問合せの履歴照会を行う	△			○	
システム 連携	車載 PF 連携	利用者連携	CMPと車載 PF 企業マスタを連携する				○	フェーズ2以降 実装検討中
		車載 PF 回答 登録	CMP と車載 PF の双方に回答登録を 行う				○	
		車載 PF-ID 取得更新	車載 PF-ID を CMP へ更新する				○	
	chemSHER PA 連携	cS-CI 登録・ 出力	cS-CI を化学品データとして登録・出力 する（個別・一括）				○	
		cS-AI 登録・ 出力	cS-AI を成形品データとして登録・出力 する（個別・一括）				○	
サプライチェ ーン支援	パススルー	変更情報自 動更新	取引先の回答情報を過去提供した顧 客へ自動転送を行う				○	
	代理登録	代理回答登 録	取引先企業に成り代わって調査依頼に 対する回答登録を行う				○	
		代理調査依 頼	取引先企業に成り代わって二次サブ ライヤへ調査依頼を登録する				○	
	支給品登録	支給品登録	支給品の調査依頼・回答データ登録、 送信を行う				○	
	複社購買	同一品番、 複数依頼先	構成部品登録、調査依頼・回答で対 応可能とする					
	依頼先変更	依頼先変更	調査依頼・回答で対応可能とする					
	伝達停止	伝達停止	回答登録にて対応可能とする					

2.2 機能別処理内容

2.2.1 インターフェース仕様

2.2.1.1 API 連携方針

既存システムおよび CMP アプリと CMP 基盤とのインターフェース仕様については、他のユースケースでも活用可能、かつ、様々な利用者が開発・利用することから、以下の観点を考慮した結果、REST-API の設計思想に則ったデータフォーマットとする。

- クライアントとサーバ間でデータのやり取りを行うこと
- サーバ側でアプリケーション状態を保持しないこと
- 標準的かつ統一的なインターフェースの設計であること
- 効率的な開発が行えること

以下に REST-API の特徴である 6 つの設計思想を記載する。

No	アーキテクチャスタイル	概要
1	クライアント／サーバ	ユーザインターフェースと処理を分離する
2	ステートレスサーバ	サーバ側でアプリケーション状態を保持しない
3	キャッシュ	クライアントとサーバの通信回数と量を減らす
4	統一インターフェース	インターフェースを固定する
5	階層化システム	システムを階層に分離する
6	コードオンデマンド	プログラムをクライアントにダウンロードして実行する

2.2.1.2 API 一覧

インターフェース仕様に則り必要な API を以下に示す。

No	API 分類	API 名	機能概要	実装レイヤ/システム
1	認証管理	事業者情報更新	利用者(企業・部門)の事業者情報を更新する。	トラストレイヤ
2	認証管理	事業者情報取得	利用者(企業・部門)の事業者情報を取得する。	トラストレイヤ
3	認証管理	事業所情報更新	事業者識別子 (内部) に紐づいた事業所を登録または内容を更新する。	トラストレイヤ
4	認証管理	事業所一覧取得	事業者識別子 (内部) に紐づいた事業所情報の一覧を取得する。	トラストレイヤ
5	認証管理	事業者情報一覧取得	他社の事業者識別子 (内部) を複数検索条件に設定し、条件に一致する他社事業者情報の一覧を取得する。	トラストレイヤ
6	認証管理	パスワード変更	API 実行事業者の事業者アカウントのパスワードを変更する。	トラストレイヤ
7	認証管理	ユーザ本人認証	事業者アカウントおよびパスワードによりログイン処理を行いアクセストークン、リフレッシュトークンの発行を行う。	トラストレイヤ
8	認証管理	アクセストークン情報更新	リフレッシュトークンによるアクセストークンの更新処理を行う。	トラストレイヤ
9	トレーサビリティ管理	取引関係取得	取引関係の情報をデータ連携層から取得する。	CMP 基盤
10	トレーサビリティ管理	取引関係登録	取引関係の情報をデータ連携層に登録する。	CMP 基盤
11	トレーサビリティ管理	取引関係更新	取引関係の情報を更新する。	CMP 基盤
12	情報伝達管理	連携データ取得	利用事業者間で連携された情報をデータ連携層から取得する。	CMP 基盤
13	情報伝達管理	連携データ登録	利用事業者間で連携する情報をデータ連携層に登録する。	CMP 基盤
14	情報伝達管理	連携データ更新	利用事業者間で連携した情報を更新する。	CMP 基盤
15	ノード情報管理	ノード取得	製品、部品等の情報をデータ連携層から取得する。	CMP 基盤
16	ノード情報管理	ノード登録	製品、部品等の情報をデータ連携層に登録する。登録済みの場合は更新する。	CMP 基盤
17	ノード情報管理	ノード削除	製品、部品等の情報をデータ連携層から削除する。	CMP 基盤
18	ノード情報管理	ノード構成取得	製品、部品等の構成情報をデータ連携層から取得する。	CMP 基盤
19	ノード情報管理	ノード構成登録	製品、部品等の構成情報をデータ連携層に登録する。登録済みの場合は更新する。	CMP 基盤
20	ノード情報管理	ノード構成削除	製品、部品等の構成情報をデータ連携層から削除する。	CMP 基盤
21	ノード情報管理	ノードデータ取得	製品、部品等の付加情報をデータ連携層から取得する。	CMP 基盤
22	ノード情報管理	ノードデータ登録	製品、部品等の付加情報をデータ連携層に登録する。登録済みの場合は更新する。	CMP 基盤
23	ノード情報管理	ノードデータ削除	製品、部品等の付加情報をデータ連携層から削除する。	CMP 基盤

No	API 分類	API 名	機能概要	実装レイヤ/システム
24	ノード情報管理	ノードファイル取得	製品、部品等に関するノードファイル情報をデータ連携層から取得する。	CMP 基盤
25	ノード情報管理	ノードファイル登録	製品、部品等に関するノードファイル情報をデータ連携層に登録する。	CMP 基盤
26	ノード情報管理	ノードファイル削除	製品、部品等に関するノードファイル情報をデータ連携層から削除する。	CMP 基盤
27	ノード情報管理	ファイルアップロード用 URL 取得	ファイルをアップロードする際に使用する URL を取得する。	CMP 基盤
28	トレーサビリティ管理	ノード関係取得	トレーサビリティ確保のための製品と購入品のつながりを取得する。	CMP 基盤
29	トレーサビリティ管理	ノード関係登録	トレーサビリティ確保のための製品と購入品のつながりを登録する。 登録済みの場合は更新する。	CMP 基盤
30	トレーサビリティ管理	ノード関係削除	トレーサビリティ確保のための製品と購入品のつながりを削除する。	CMP 基盤
31	通知管理	通知登録	通知情報を共通領域に登録する。	CMP 基盤
32	通知管理	通知取得	自社で登録した通知情報を共通領域から取得する。	CMP 基盤
33	通知管理	通知更新	自社で登録した通知情報を共通領域に更新する。	CMP 基盤
34	通知管理	受領通知取得	自社宛の通知情報を共通領域から取得する。	CMP 基盤
35	通知管理	通知確認更新	通知の確認情報を共通領域に更新する。	CMP 基盤
36	通知管理	通知確認取得	通知の確認情報を共通領域から取得する。	CMP 基盤

2.2.2 システム化対象業務フロー

「1.4.2.3 標準データモデル詳細」で整理した本ユースケースで想定される基本的な業務パターンに基づき、システム化する部分を抜粋する。機能構成を検討する際のインプット情報とすること。なお、トランザクションレイヤに関するシステム化業務フローの詳細は記載しない。

2.2.2.1 システム化対象業務フロー一覧

■モデル#1: 川下事業者から調査依頼



プロセス	プロセス概要	モデル
①調査依頼登録（A社→B社）	<ul style="list-style-type: none"> C社にて製品い情報を登録する A社にて製品1情報と製品に関連する購入品情報（材料あ）を登録する A社は登録した購入品情報を対象のB社に調査依頼を行う B社は調査依頼を受領したことを確認する B社にて製品あ情報と製品に関連する購入品情報（材料い）を登録する 	
②調査依頼登録（B社→C社）	<ul style="list-style-type: none"> B社は登録した購入品情報を対象のC社に調査依頼を行う C社は調査依頼を受領したことを確認する 	
③回答登録（C社→B社）	<ul style="list-style-type: none"> C社にて回答データを作成し、回答データをB社へ伝達を行う B社にて回答データを確認し、承認を行う 	
④回答登録（B社→A社）	<ul style="list-style-type: none"> B社にて回答データを作成し、回答データをA社へ伝達を行う A社にて回答データを確認し、承認を行う A社はB社や他の購入品に対する回答データを踏まえて製品1としての製品登録を行う 	

※本モデルである調査依頼に関しては、主に CMP 利用開始にあたっての初期移行または新規製品など、初期の取引関係作成時または取引関係変更時などでのみ実施する

■モデル#2: 規制変更に伴い CMP 要申告物質ステータスフラグを伝達

凡例：川下事業者 A社 ←→ 川中事業者 B社 ←→ 川上（化学品）事業者 C社

プロセス	プロセス概要	モデル
①物質リスト更新及び通知受領確認	<ul style="list-style-type: none"> 運営事業者から各者へ物質リストの更新を通知する 各者は通知されたバージョンの物質リストを取得する 各者は通知情報に受領確認を意味するタイムスタンプを打刻する 	
②CMP要申告物質ステータスフラグの伝達 (C社→B社)	<ul style="list-style-type: none"> C社は対象の物質リストを用いて製品いに含まれる材料の回答更新の要否を確認し、CMP要申告物質ステータスフラグに「含有あり(成分情報変更あり)」を設定する C社はB社からの過去の調査依頼に対して、CMP要申告物質ステータスフラグの伝達を行う 	
③CMP要申告物質ステータスフラグの伝達 (B社→A社)	<ul style="list-style-type: none"> B社はC社から伝達されたCMP要申告物質ステータスフラグを確認する B社は対象の物質リストを用いて製品あに含まれる材料の回答更新の要否を確認し、CMP要申告物質ステータスフラグに「含有あり(成分情報変更あり)」を設定する B社はA社からの過去の調査依頼に対して、CMP要申告物質ステータスフラグの伝達を行う 	
④CMP要申告物質を踏まえた回答更新 (C社→B社)	<ul style="list-style-type: none"> C社は製品いに物質Yが含まれていることを確認し、物質Yを追加登録した回答データを登録する C社はB社からの過去の調査依頼に対して、回答更新を行う 	
⑤CMP要申告物質を踏まえた回答更新 (B社→A社)	<ul style="list-style-type: none"> B社はC社から受領した回答内容を取得し、製品あとしての成分情報を再計算する B社は製品あへの回答データを登録する B社はA社からの過去の調査依頼に対して、回答更新を行う A社はB社や他の購入品に対する回答データを踏まえて製品1としての製品情報の更新を行う 	

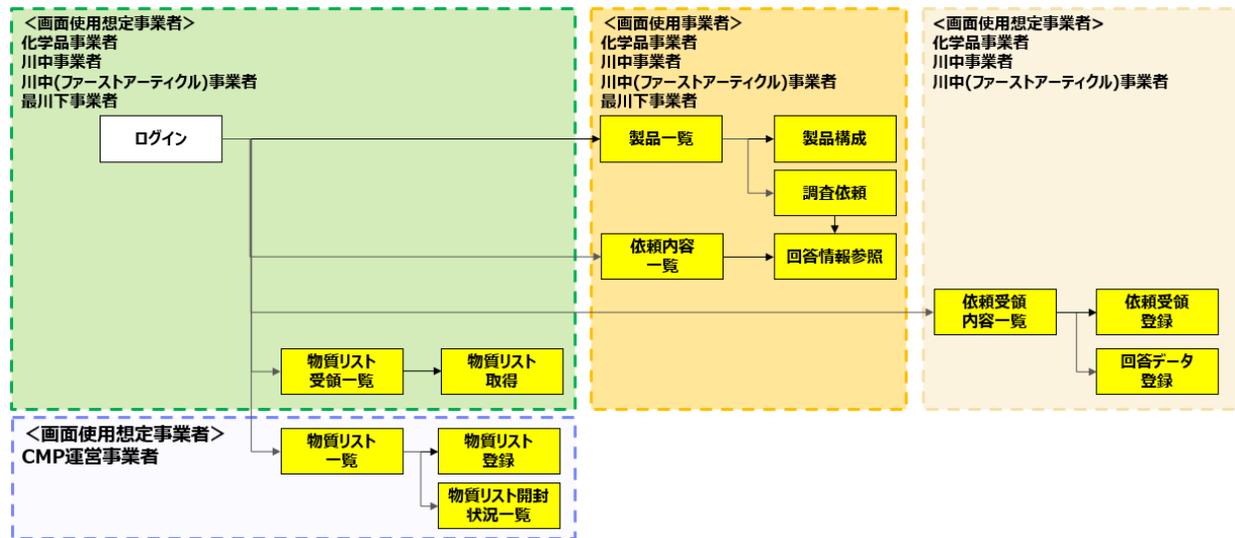
■モデル#3: 規制変更に伴い CMP 要申告候補物質ステータスフラグを伝達

凡例：川下事業者 A社 ←→ 川中事業者 B社 ←→ 川上（化学品）事業者 C社

プロセス	プロセス概要	モデル
①物質リスト更新及び通知受領確認	<ul style="list-style-type: none"> 運営事業者から各者へ物質リストの更新を通知する A社、C社は通知されたバージョンの物質リストを取得する A社、C社は通知情報に受領確認を意味するタイムスタンプを打刻する B社は通知に対し受領確認を行わず、運営事業者から通知の受領確認を督促される 	
②CMP要申告候補物質ステータスフラグの伝達 (C社→B社)	<ul style="list-style-type: none"> 製品いに対象物質Yの含有を確認し、CMP要申告候補物質ステータスフラグに「含有あり(成分情報なし)」を設定する 製品いに対象物質Zの含有を確認し、CMP要申告候補物質ステータスフラグに「含有なし」を設定する C社はB社からの過去の調査依頼に対して、CMP要申告候補物質ステータスフラグの伝達を行う 	
③CMP要申告候補物質ステータスフラグの伝達 (B社→A社)	<ul style="list-style-type: none"> B社はC社からのCMP要申告候補物質ステータスフラグを踏まえて製品あとしてのCMP要申告候補物質ステータスフラグを設定する B社はA社からの過去の調査依頼に対して、CMP要申告候補物質ステータスフラグの伝達を行う A社はB社や他の購入品に対するCMP要申告候補物質ステータスフラグを踏まえて製品1としての製品情報の更新を行う A社は製品1のCMP要申告候補物質ステータスフラグを設定する 	

■ 想定画面遷移

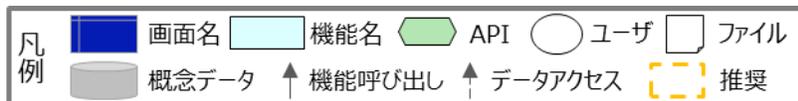
システム化対象業務フローにおける想定画面遷移について以下に示す。なお、以降記載されている CMP アプリにおける画面遷移、画面名及び機能名については、あくまで本資料を説明するための参考であり、実際の CMP アプリにおける制約ではない。（各機能、データの配置及び CMP 基盤で実行する API との関係を示すものである。）



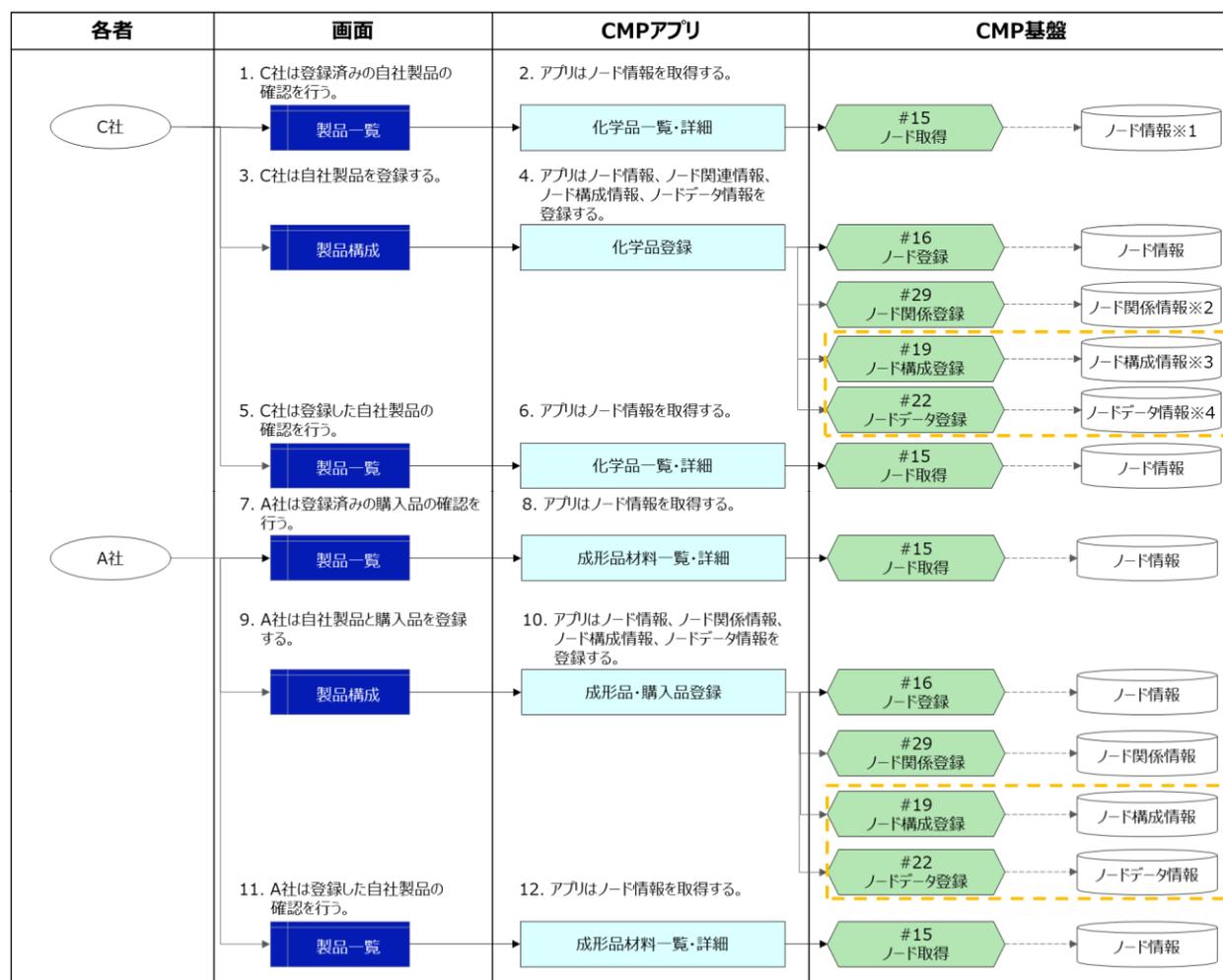
2.2.2.2 システム化対象業務フロー詳細

2.2.2.2.1 標準データモデル#1: 川下事業者から調査依頼

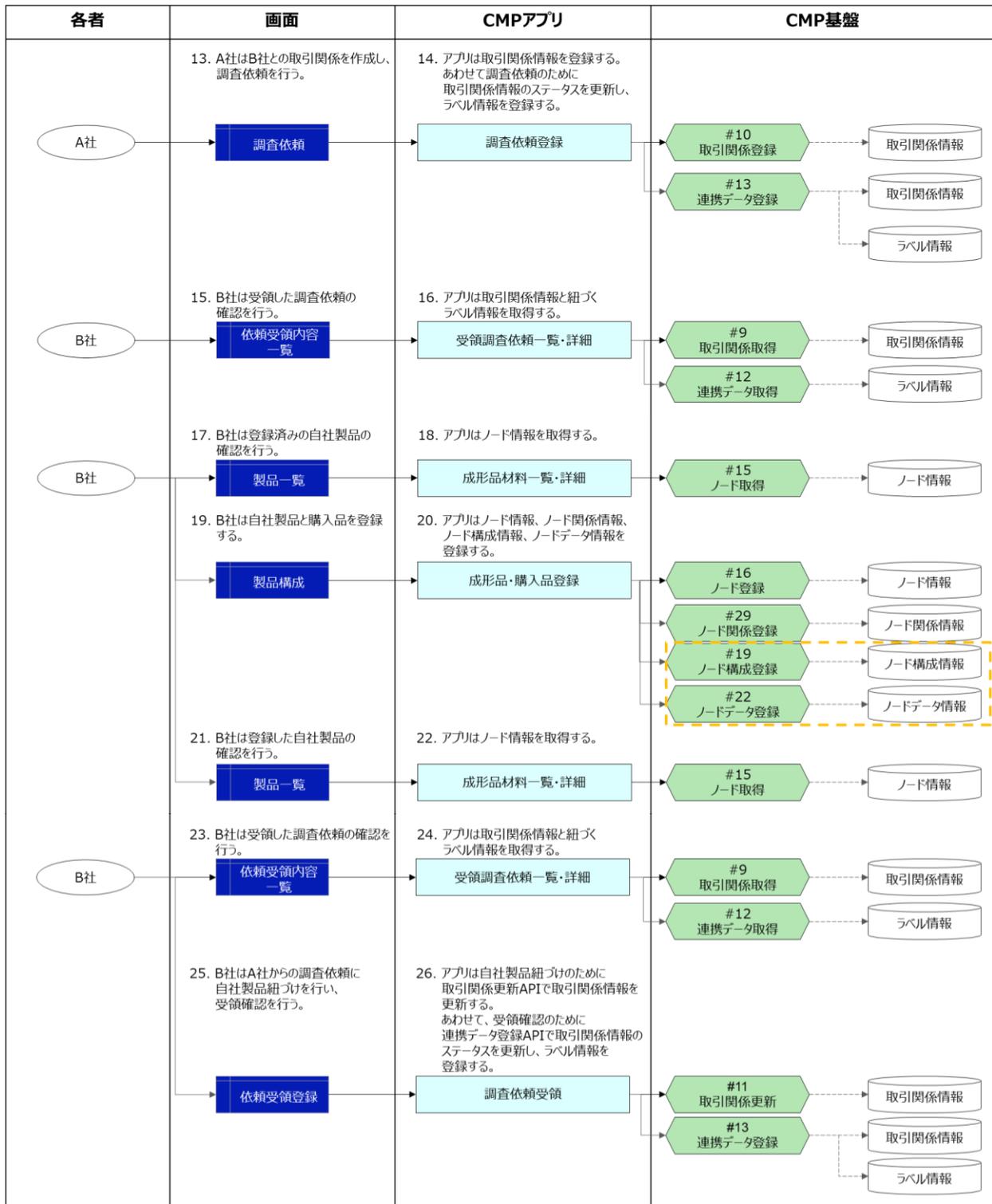
凡例は以下の通り。



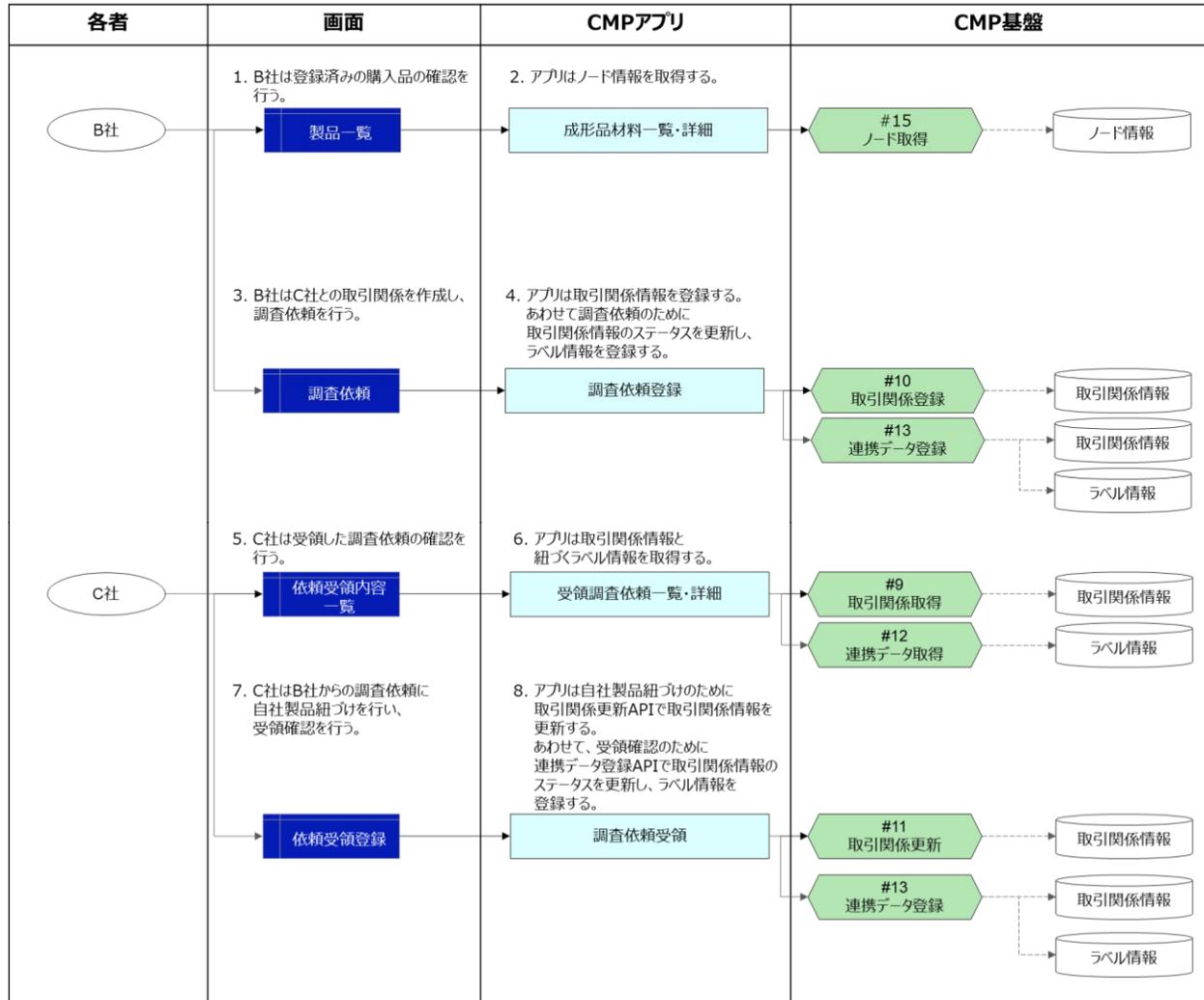
①調査依頼登録 (A社→B社)



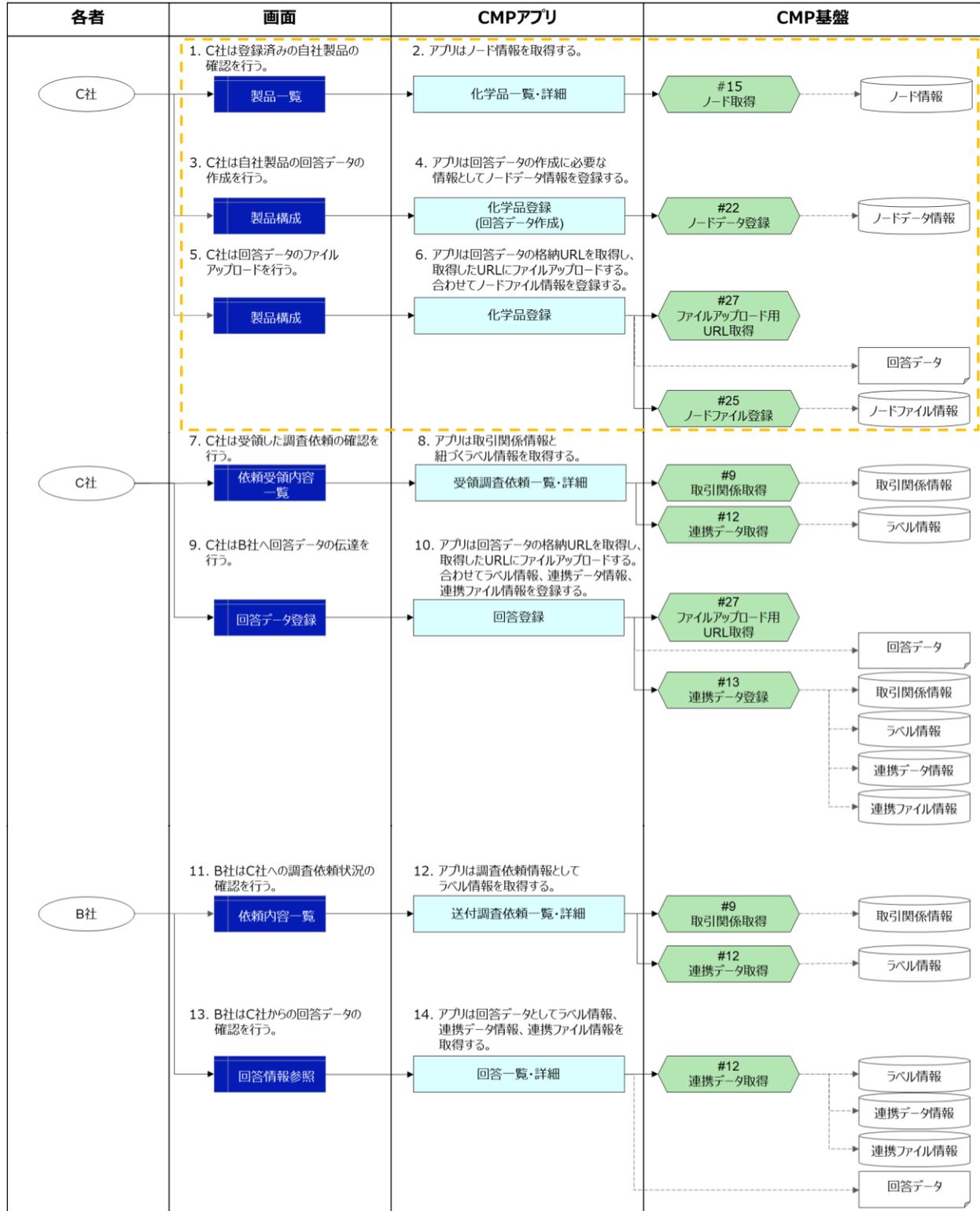
- (※1)各事業者が製造する製品や自社で購入している他社製造の購入品情報
 - (※2)トレーサビリティ確保のための各事業者内での製品と購入品のつながりを管理する情報
 - (※3)各事業者が製造する製品の構成情報
 - (※4)製品等に紐づく属性情報
- 以降のスライドも同様

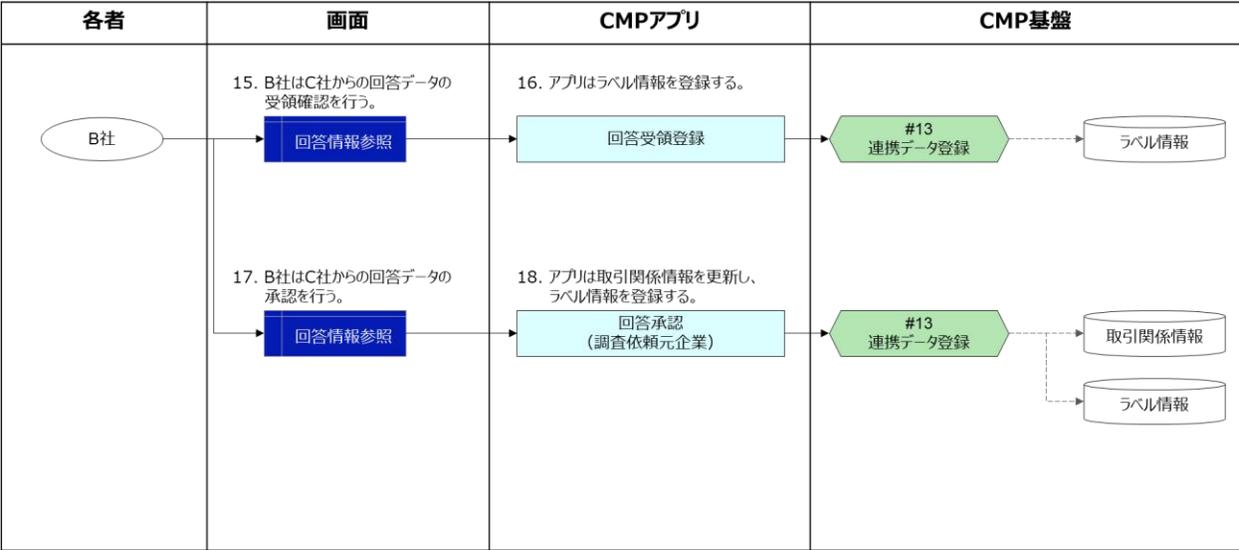


②調査依頼登録 (B社→C社)

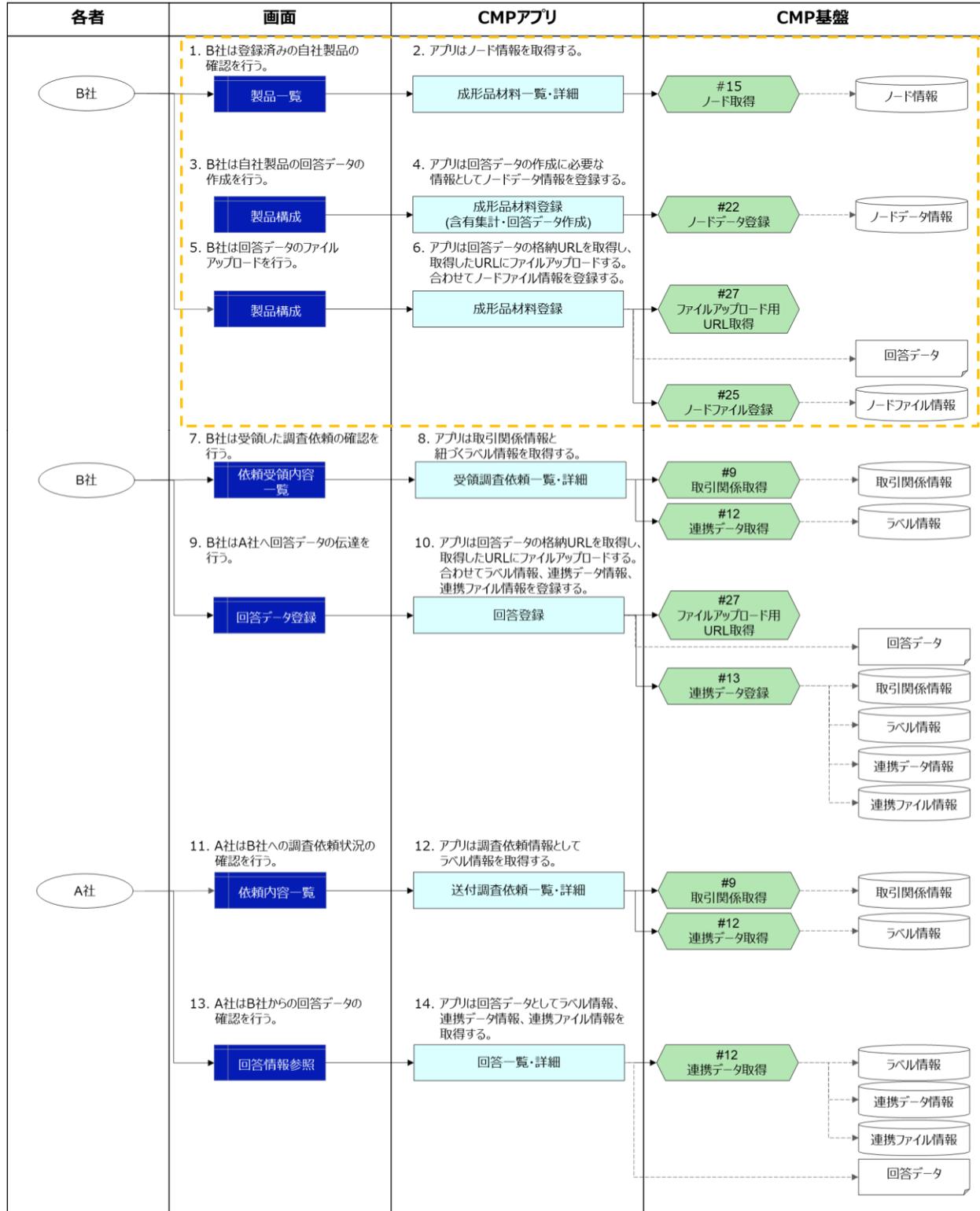


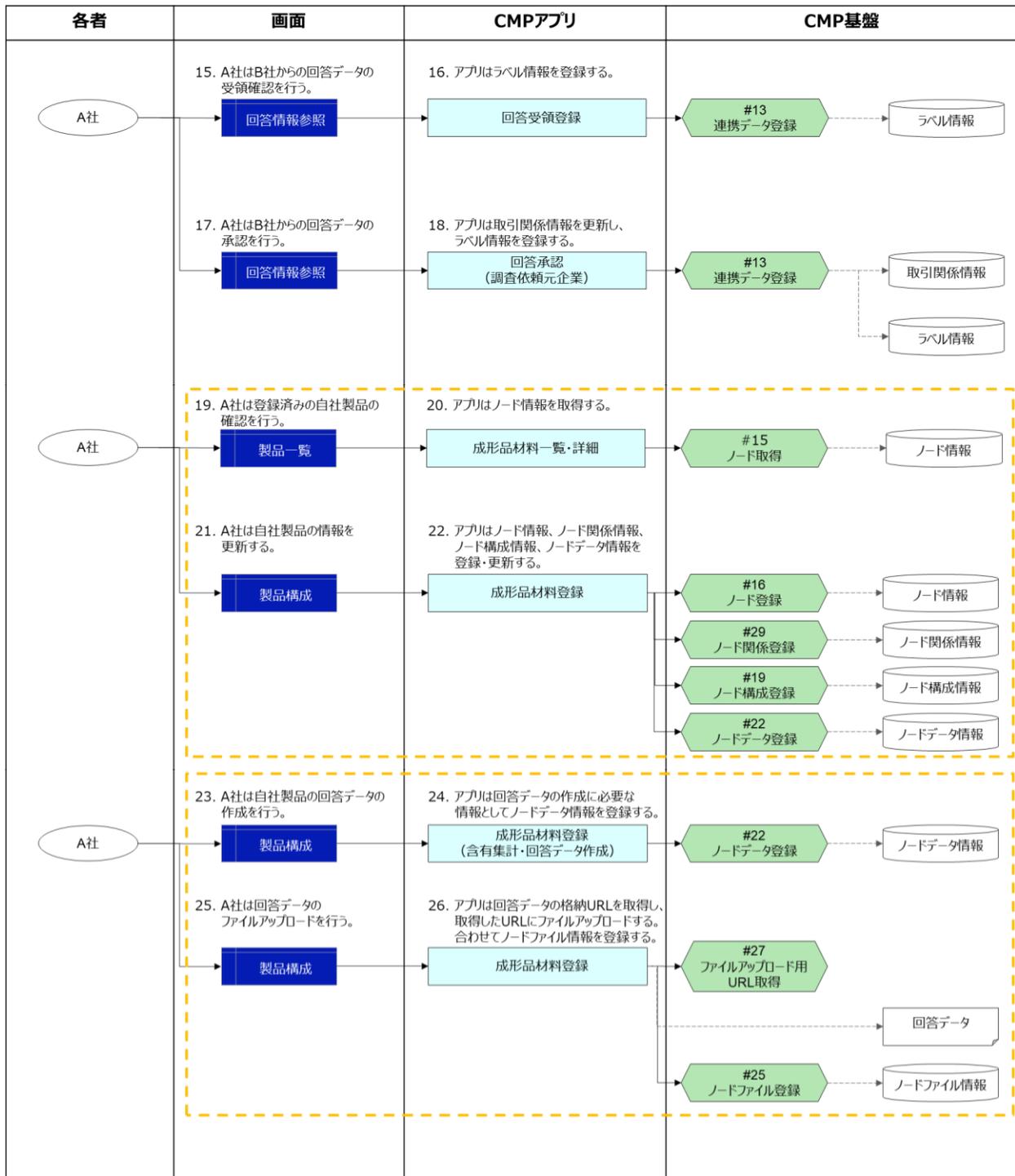
③回答登録 (C社→B社)





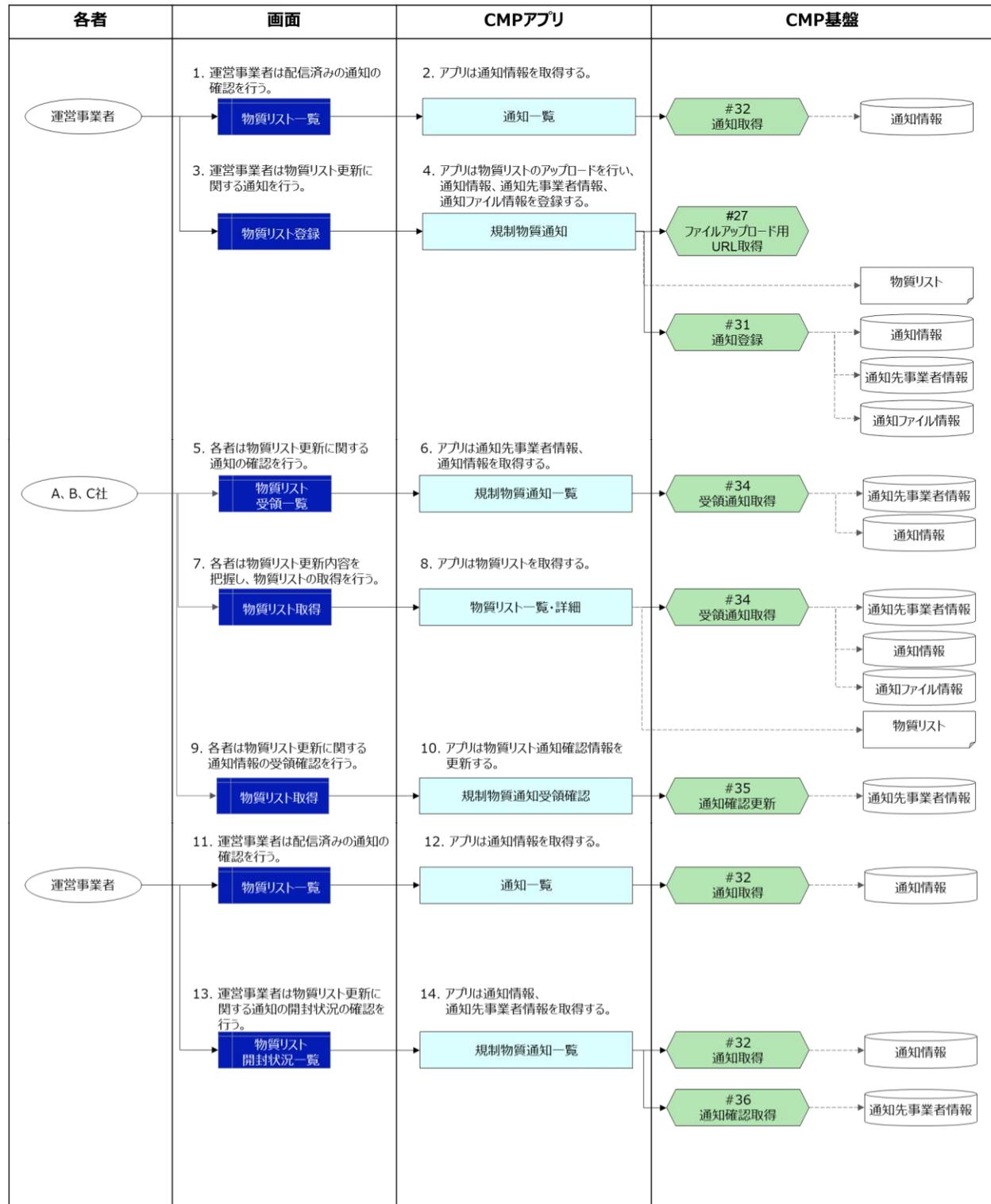
④回答登録 (B社→A社)



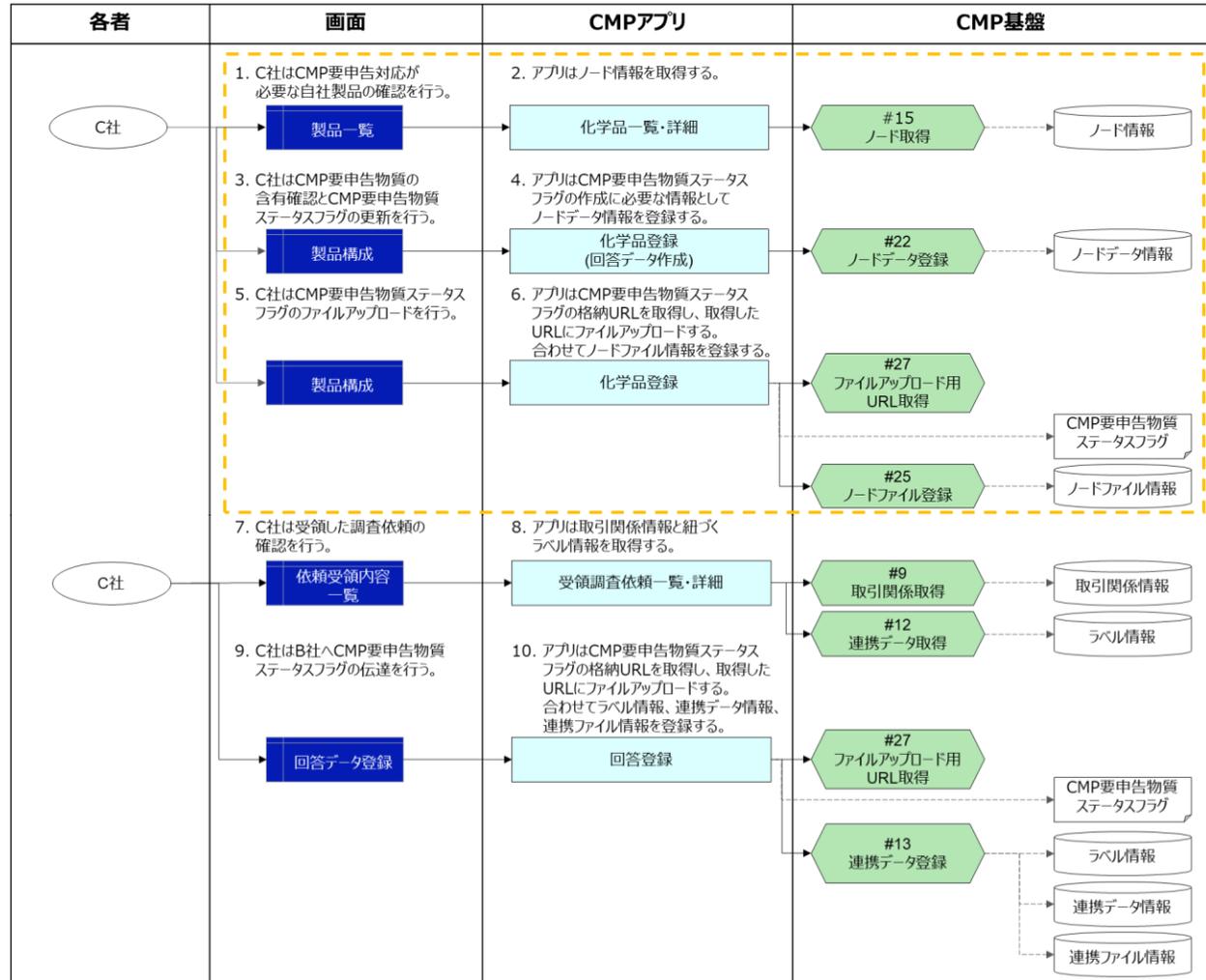


2.2.2.2.2 標準データモデル#2: 規制変更に伴い CMP 要申告物質ステータスフラグを伝達

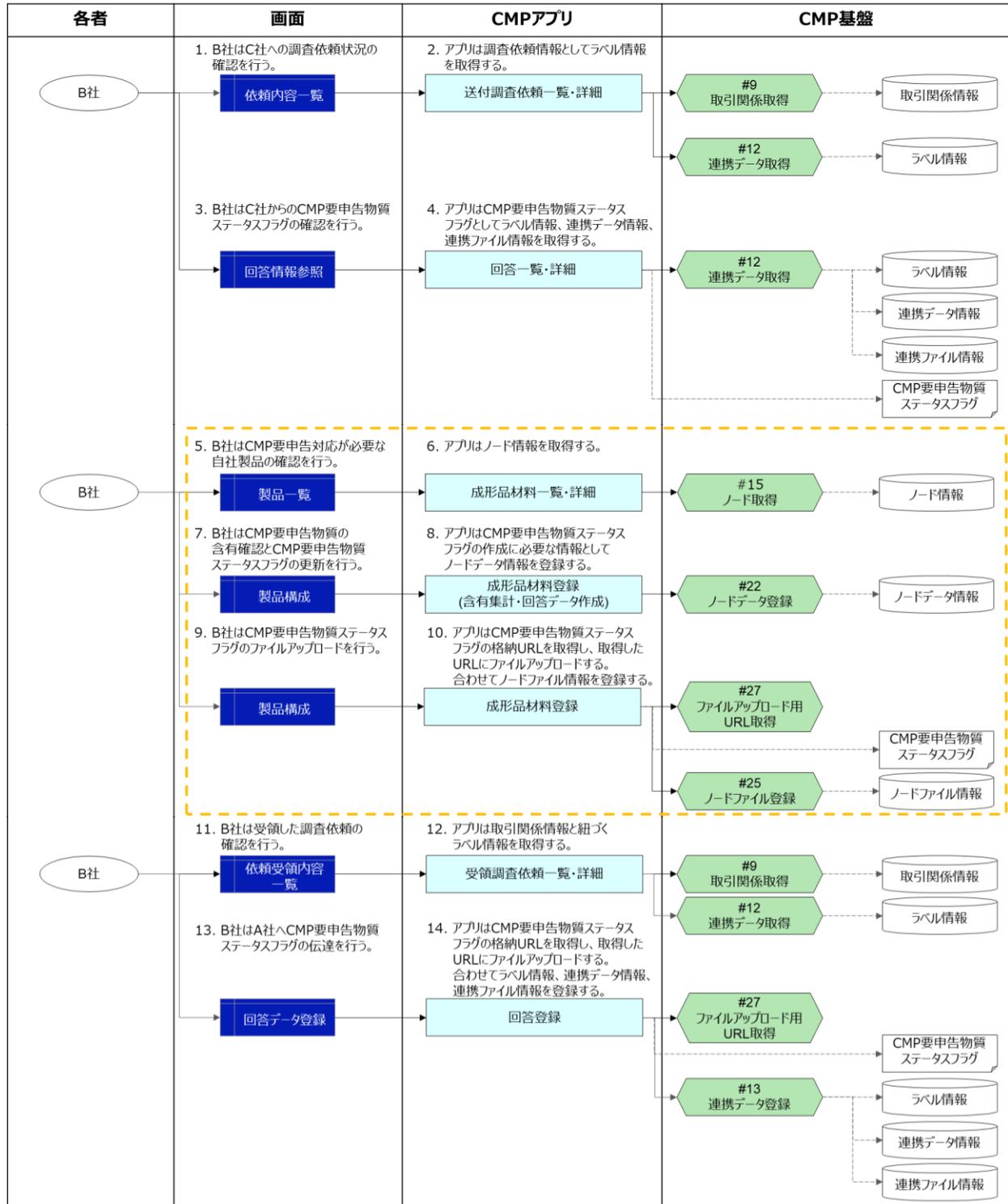
①物質リスト更新及び通知受領確認

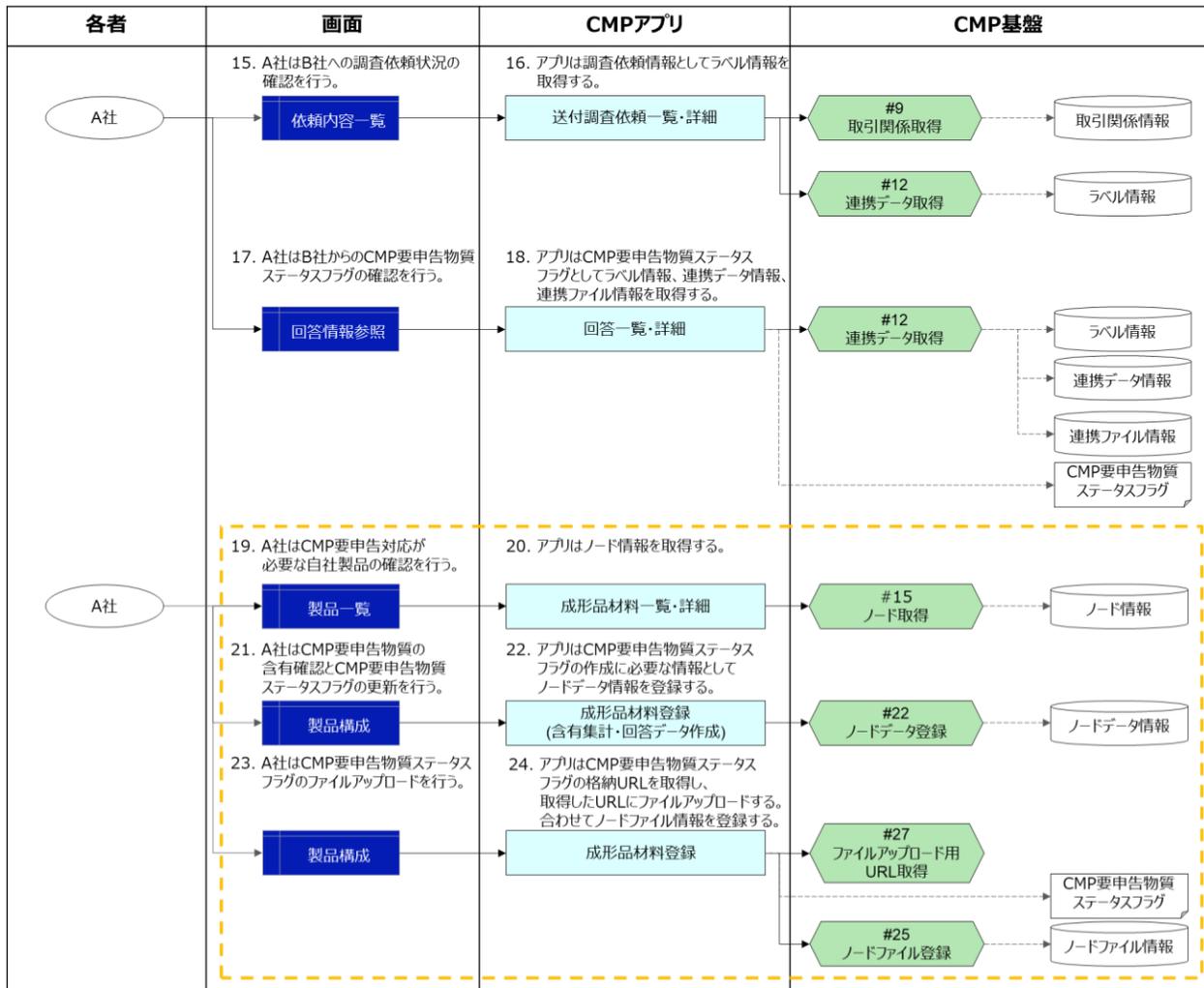


②CMP 要申告物質ステータスフラグの伝達 (C社→B社)



③CMP 要申告物質ステータスフラグの伝達 (B社→A社)





④CMP 要申告物質を踏まえた回答更新 (C 社→B 社)

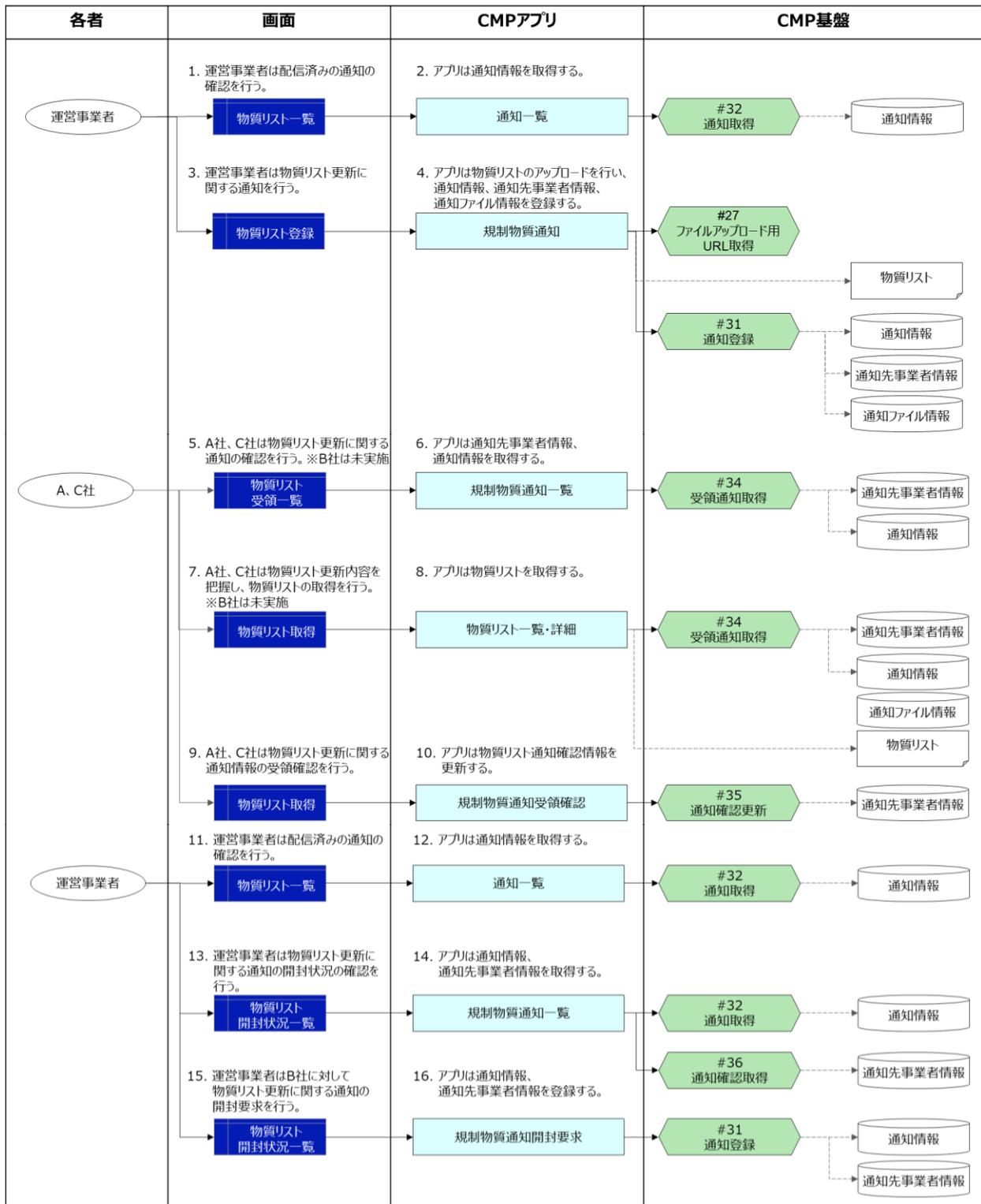
各者	画面	CMPアプリ	CMP基盤
「モデル#1: 川下事業者から調査依頼」のプロセス③と同様のため省略			

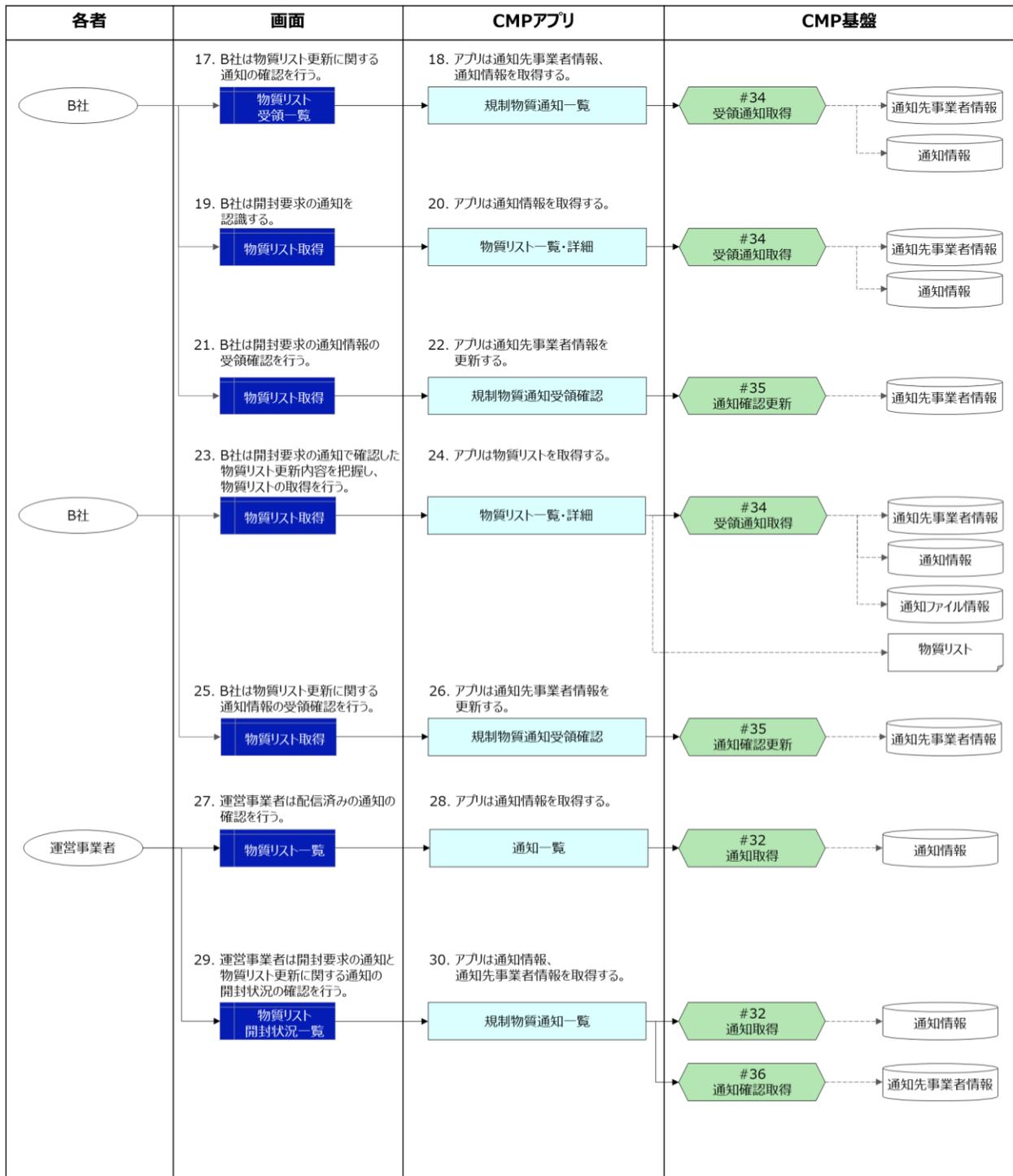
⑤CMP 要申告物質を踏まえた回答更新 (B 社→A 社)

各者	画面	CMPアプリ	CMP基盤
「モデル#1: 川下事業者から調査依頼」のプロセス④と同様のため省略			

2.2.2.2.3 標準データモデル#3: 規制変更に伴い CMP 要申告候補物質ステータスフラグを伝達

①物質リスト更新及び通知受領確認





②CMP 要申告候補物質ステータスフラグの伝達 (C 社→B 社)

各者	画面	CMPアプリ	CMP基盤
<p>「モデル#2:規制変更に伴うCMP要申告物質ステータスフラグの伝達」 のプロセス②と同様のため省略</p>			

③CMP 要申告候補物質ステータスフラグの伝達 (B 社→A 社)

各者	画面	CMPアプリ	CMP基盤
<p>「モデル#2:規制変更に伴うCMP要申告物質ステータスフラグの伝達」 のプロセス③と同様のため省略</p>			

3.2 データ一覧

CMP 基盤、トラストレイヤで保持するデータを以下に定義する。配置する基準はデータ配置基準に従う。

CMP アプリで保持するデータおよび構成は、アプリケーション内の機能構成に合わせて設計することとする。

データ分類	データ分類	配置レイヤ/システム	概要
法人・組織情報	事業者情報	トラストレイヤ	利用者(企業・部門)の情報を管理する。
	事業所情報	トラストレイヤ	事業者識別子(内部)に紐づいた事業所情報を管理する。
トレーサビリティ情報	取引関係情報	CMP 基盤	利用事業者間で連携したデータを識別するための情報を管理する。
	ノード関係情報	CMP 基盤	トレーサビリティ確保のための製品と購入品のつながりを管理する。
連携データ情報	ラベル情報	CMP 基盤	利用事業者間で連携した情報を管理する。
	連携データ情報	CMP 基盤	利用事業者間で連携したデータを管理する。
	連携ファイル情報	CMP 基盤	利用事業者間で連携したファイルを管理する。
ノード情報	ノード情報	CMP 基盤	製品、部品等の情報を管理する。
	ノード構成情報	CMP 基盤	製品、部品等の構成情報を管理する。
	ノードデータ情報	CMP 基盤	製品、部品等の付加情報を管理する。
	ノードファイル情報	CMP 基盤	製品、部品等に関するファイル情報を管理する。
通知情報	通知情報	CMP 基盤	通知情報を管理する。
	通知先事業者情報	CMP 基盤	通知に関連する事業者情報を管理する。
	通知ファイル情報	CMP 基盤	通知に関連するファイル情報を管理する。

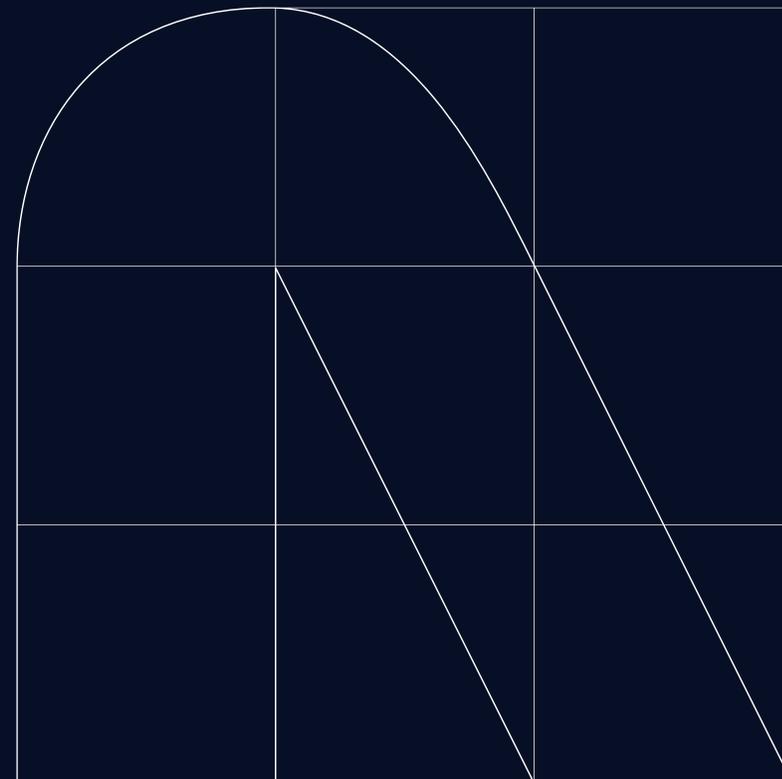
データに対する項目一覧は以下の通り。

データ分類	データ名	配置レイヤ/システム	概要	PKEY	項目名
法人・組織 情報	事業者情報	トラストレイヤ	利用者(企業・部門)の情報を管理する。	○	事業者識別子 (内部)
					事業者名
					事業者所在地
					事業者識別子 (グローバル)
					事業者識別子 (ローカル)
	事業所情報	トラストレイヤ	事業者識別子 (内部) に紐づいた事業所情報を管理する。	○	事業所識別子 (内部)
					事業者識別子 (内部)
					事業所名
					事業所所在地
					事業所識別子 (グローバル)
トレーサビリティ 情報	取引関係情報	CMP 基盤	利用事業者間で連携したデータを識別するための情報を管理する。	○	取引関係情報識別子
					納品先事業者識別子 (内部)
					仕入先事業者識別子 (内部)
					納品先トレース識別子
					仕入先トレース識別子
					項番
	ステータス				
	ノード関係情報	CMP 基盤	トレーサビリティ確保のための製品と購入品のつながりを管理する。	○	ノード関係情報識別子
					最上位トレース識別子
					最下位トレース識別子
連携データ 情報	ラベル情報	CMP 基盤	利用事業者間で連携したデータを識別するための情報を管理する。	○	ラベル識別子
					取引関係情報識別子
					事業者識別子 (発) (内部)
					事業者識別子 (着) (内部)
					ラベル登録日時
	データ種別				
	連携データ情報	CMP 基盤	利用事業者間で連携したデータを管理する。	○	連携データ識別子
					ラベル識別子
					トレース識別子
					項番
					データ項目名
	データ値				
	連携ファイル情報	CMP 基盤	利用事業者間で連携したファイルを管理する。	○	連携ファイル識別子
					ラベル識別子
					トレース識別子
項番					
ファイル名					
ファイル説明					

データ分類	データ名	配置レイヤ/システム	概要	PKEY	項目名
ノード情報	ノード情報	CMP 基盤	製品、部品等の情報を管理する。	○	トレース識別子
					事業者識別子 (内部)
					事業所識別子 (内部)
					ノード項目
					ノード補助項目
					ノード名称
	ノード構成情報	CMP 基盤	製品、部品等の構成情報を管理する。	○	ノード構成情報識別子
					親トレース識別子
					子トレース識別子
	ノードデータ情報	CMP 基盤	製品、部品等の付加情報を管理する。	○	ノードデータ識別子
					トレース識別子
					項番
					データ項目名
	ノードファイル情報	CMP 基盤	製品、部品等に関するファイル情報を管理する。	○	ノードファイル識別子
					トレース識別子
					項番
ファイル名					
通知情報	通知情報	CMP 基盤	通知情報を管理する。	○	通知識別子
					通知種別
					通知タイトル
					通知内容
					通知登録日時
					通知元事業者識別子(内部)
	通知先事業者情報	CMP 基盤	通知に関連する事業者情報を管理する。	○	通知確認識別子
					通知識別子
					通知確認ステータス
					通知登録更新日時
					通知確認日時
					通知元事業者識別子(内部)
	通知ファイル情報	CMP 基盤	通知に関連するファイル情報を管理する。	○	通知ファイル識別子
					通知識別子
					ファイル名
					ファイル説明

Appendix

CMP基盤/CMPアプリ 標準仕様書別紙 非機能要件一覧



非機能要件の検討（全体方針）

CMPの要求項目としての総論を示します。この考え方にに基づき、以降のページにて記載する非機能要求詳細を定義します。

- －優先度高：他の項目と比べ手厚く対応する（コストをかけてでも優先して対応する）項目
- －優先度低：最低限の対応でよい項目

分類	概要	CMPにおける優先度		優先度の主な判断根拠
		アプリ	基盤	
可用性	システムを継続的に利用可能とするための要求。 「継続性」、「耐障害性」、「災害対策」、「回復性」などで構成される。	低	低	■ アプリ・基盤共通 システム停止により直ちに影響が出るシステムではないため、最低限の対応とする。
性能	システムの性能に関する要求。 「業務処理量」、「性能目標値」などで構成される。	高	低	■ アプリ 処理待ち時の処理中表示などユーザへの配慮は必要であるため、手厚く対応する。 ■ 基盤 応答性能を求めるシステムではないため、最低限の対応とする。多量性能については、拡張性で対応する。
拡張性	将来のシステム拡張に関する要求。 「リソース拡張性」などで構成される。	低	高	■ アプリ 利用者の増加とアプリの機能拡張次第であり、最低限の対応とする。 ■ 基盤 参加企業の増加、逐次発生する参加・退会へ柔軟に対応する必要があるため、手厚く対応する。
運用・保守性	システムの運用と保守のサービスに関する要求。 「通常運用」、「保守運用」、「障害時運用」の運用パターンと「運用環境」、「サポート体制」、「運用管理方針」などで構成される。	高	高	■ アプリ・基盤共通 障害やシステムアップデートなどが生じた際に、効率的で安定性のある対応が求められるため、手厚く対応する。
移行性	現行システム資産の移行に関する要求。 「移行方式」、「移行対象」、「移行計画」などで構成される。	低	低	■ アプリ・基盤共通 CMPは新規システムであり、システム移行は想定されないため、最低限の対応とする。 ■ アプリ chemSHERPAなど、現行業務アプリからのデータ移行を支援する機能があると望ましい。
セキュリティ	情報システムの安全性の確保に関する要求。 「セキュリティ診断」、「アクセス制御」、「データの秘匿」、「不正監視」、「ネットワーク対策」、「マルウェア対策」、「セキュリティインシデント対応」などで構成される。	高	高	■ アプリ・基盤共通 秘匿性の高いデータを取り扱うため、手厚く対応する。

重要度高要件の考え方 # 1 (セキュリティ、性能・拡張性等)

IPAの非機能要求グレード2018に基づいた、重要度高要件 (セキュリティ) の考え方の素案です。

大項目	中項目	小項目	小項目説明	メトリクス	【ご参考】 トレサビシステム	CMP案	
						アプリ	基盤
セキュリティ	前提条件・制約条件	情報セキュリティに関するコンプライアンス	<p>順守すべき情報セキュリティに関する組織規程やルール、法令、ガイドライン等が存在するかどうかを確認するための項目。</p> <p>なお、順守すべき規程等が存在する場合は、規定されている内容と矛盾が生じないよう対策を検討する。 例)</p> <ul style="list-style-type: none"> ・国内/海外の法律 ・資格認証 ・ガイドライン ・その他ルール 	<p>順守すべき社内規程、ルール、法令、ガイドライン等の有無</p> <p>0:無し 1:有り</p>	1: 自工会/部工会ガイドラインを参照	【推奨】 ISO/IEC27001:2013に定められた情報セキュリティ基準への準拠	ISO/IEC27001:2013に定められた情報セキュリティ基準への準拠
	セキュリティリスク分析	セキュリティリスク分析	<p>システム開発を実施する中で、どの範囲で対象システムの脅威を洗い出し、影響の分析を実施するかの方針を確認するための項目。</p> <p>なお、適切な範囲を設定するためには、資産の洗い出しやデータのライフサイクルの確認等を行う必要がある。また、洗い出した脅威に対して、対策する範囲を検討する。</p>	<p>リスク分析範囲</p> <p>0:分析無し 1:重要度が高い資産を扱う範囲、あるいは、外接部分 2:開発範囲</p>	1: 社会的影響が限定されるシステムでの基準をもとに、「重要度が高い資産を扱う範囲、あるいは、外接部分」に対してセキュリティリスク分析を実施	【必須】 1:重要度が高い資産を扱う範囲、あるいは、外接部分	1:重要度が高い資産を扱う範囲、あるいは、外接部分

重要度高要件の考え方 # 1 (セキュリティ、性能・拡張性等)

IPAの非機能要求グレード2018に基づいた、重要度高要件 (セキュリティ) の考え方の素案です。

大項目	中項目	小項目	小項目説明	メトリクス	【ご参考】 トレサビシステム	CMP案	
						アプリ	基盤
セキュリティ	セキュリティ診断	セキュリティ診断	対象システムや、各種ドキュメント (設計書や環境定義書、実装済みソフトウェアのソースコードなど) に対して、セキュリティに特化した各種試験や検査の実施の有無を確認するための項目。	ネットワーク診断実施の有無 0:無し 1:有り	1: 情報セキュリティサービス事業者/組織が提供するセキュリティ診断(ペネトレーションテスト等)を実施	【必須】 1:有り	1:有り
				Web診断実施の有無 0:無し 1:有り	1: 情報セキュリティサービス事業者/組織が提供するセキュリティ診断(Webアプリケーション診断等)を実施	【必須】 1:有り	1:有り

重要度高要件の考え方 # 1 (セキュリティ、性能・拡張性等)

IPAの非機能要求グレード2018に基づいた、重要度高要件 (セキュリティ) の考え方の素案です。

大項目	中項目	小項目	小項目説明	メトリクス	【ご参考】 トレサビシステム	CMP案	
						アプリ	基盤
セキュリティ	アクセス・利用制限	認証機能	資産を利用する主体 (利用者や機器等) を識別するための認証を実施するか、また、どの程度実施するのかを確認するための項目。 複数回の認証を実施することにより、抑止効果を高めることができる。 なお、認証するための方式としては、ID/パスワードによる認証や、ICカード等を用いた認証等がある。	主体の認証 0:実施しない 1:1回 2:複数回の認証 3:複数回、異なる方式による認証	2: アプリ、基盤共に複数回の認証を実施 ・アプリ ユーザ認証システムを利用して、ID・PASS + 証明書 + API KEY ・基盤 クラウドサービス (AWS) の多要素認証 + 踏み台認証	【必須】 2:複数回の認証	2:複数回の認証
		利用制限	認証された主体 (利用者や機器など) に対して、資産の利用等を、ソフトウェアやハードウェアにより制限するか確認するための項目。 例) ドアや保管庫の施錠、USBやCD-RWやキーボードなどの入出力デバイスの制限、コマンド実行制限など。	システム上の対策における操作制限度 0:無し 1:必要最小限のプログラムの実行、コマンドの操作、ファイルへのアクセスのみを許可	1: アプリケーションおよびシステム基盤の利用者において、役割に応じた適切な権限付与を設計/設定	【必須】 1:必要最小限のプログラムの実行、コマンドの操作、ファイルへのアクセスのみを許可	1:必要最小限のプログラムの実行、コマンドの操作、ファイルへのアクセスのみを許可

重要度高要件の考え方 # 1 (セキュリティ、性能・拡張性等)

IPAの非機能要求グレード2018に基づいた、重要度高要件 (セキュリティ) の考え方の素案です。

大項目	中項目	小項目	小項目説明	メトリクス	【ご参考】 トレサビシステム	CMP案	
						アプリ	基盤
セキュリティ	データの 秘匿	データ暗 号化	機密性のあるデータを、伝送時や蓄積時に秘匿するための暗号化を実施するかを確認するための項目。	伝送データの暗号化の有無 0:無し 1:認証情報のみ暗号化 2:重要情報を暗号化	2: Internetを経由する伝送データについては暗号化を実施	【必須】 2:重要情報を暗号化	2:重要情報を暗号化
				蓄積データの暗号化の有無 0:無し 1:認証情報のみ暗号化 2:重要情報を暗号化	2: 蓄積データの重要情報を暗号化	【必須】 2:重要情報を暗号化	2:重要情報を暗号化

重要度高要件の考え方 # 1 (セキュリティ、性能・拡張性等)

IPAの非機能要求グレード2018に基づいた、重要度高要件 (セキュリティ) の考え方の素案です。

大項目	中項目	小項目	小項目説明	メトリクス	【ご参考】 トレサビシステム	CMP案	
						アプリ	基盤
セキュリティ	不正追跡・監視	不正監視	不正行為を検知するために、それらの不正について監視する範囲や、監視の記録を保存する量や期間を確認するための項目。 なお、どのようなログを取得する必要があるかは、実現するシステムやサービスに応じて決定する必要がある。 また、ログを取得する場合には、不正監視対象と併せて、取得したログの内、確認する範囲を定める必要がある。	ログの取得 0:実施しない 1:実施する	1: データの変更を伴う処理、操作に係るログ (アクセスログ、操作ログ等) に関してはログ取得を実施	【必須】 1:実施する	1:実施する
				ログ保管期間 0:6ヶ月 1:1年 2:3年 3:5年 4:10年以上有期 5:永久保管	2: 原則CFPのログは3年保管、DDは10年保管となる見込み	【推奨】 2:3年	2:3年

重要度高要件の考え方 # 1（セキュリティ、性能・拡張性等）

IPAの非機能要求グレード2018に基づいた、重要度高要件（セキュリティ）の考え方の素案です。

大項目	中項目	小項目	小項目説明	メトリクス	【ご参考】 トレサビシステム	CMP案	
						アプリ	基盤
セキュリティ	不正追跡・監視	不正監視	不正行為を検知するために、それらの不正について監視する範囲や、監視の記録を保存する量や期間を確認するための項目。 なお、どのようなログを取得する必要があるかは、実現するシステムやサービスに応じて決定する必要がある。また、ログを取得する場合には、不正監視対象と併せて、取得したログの内、確認する範囲を定める必要がある。	不正監視対象（装置、ネットワーク、侵入者・不正操作等） 0:無し 1:重要度が高い資産を扱う範囲、あるいは、外接部分 2:システム全体	1: 「重要な情報資産」と定義した範囲において、システムへの侵入痕跡や不正操作等の不正な挙動を監視	【必須】 1:重要度が高い資産を扱う範囲、あるいは、外接部分	1:重要度が高い資産を扱う範囲、あるいは、外接部分

重要度高要件の考え方 # 1（セキュリティ、性能・拡張性等）

IPAの非機能要求グレード2018に基づいた、重要度高要件（セキュリティ）の考え方の素案です。

大項目	中項目	小項目	小項目説明	メトリクス	【ご参考】 トレサビシステム	CMP案	
						アプリ	基盤
セキュリティ	ネットワーク対策	ネットワーク制御	不正な通信を遮断するための制御を実施するかを確認するための項目。	通信制御 0:無し 1:有り	1: WAF/FW等、不正な通信を遮断するための制御を実施	【必須】 1:有り	1:有り
		不正検知	ネットワーク上において、不正追跡・監視を実施し、システム内の不正行為や、不正通信を検知する範囲を確認するための項目。	不正通信の検知範囲 0:無し 1:重要度が高い資産を扱う範囲、あるいは、外接部分 2:システム全体	1: 「重要な情報資産」と定義した範囲において、不正通信を検知	【必須】 1:重要度が高い資産を扱う範囲、あるいは、外接部分	1:重要度が高い資産を扱う範囲、あるいは、外接部分
		サービス停止攻撃の回避	ネットワークへの攻撃による輻輳についての対策を実施するかを確認するための項目。	ネットワークの輻輳対策 0:無し 1:有り	1: DDoS等、サービス停止攻撃への対策を実施	【必須】 1:有り	1:有り

重要度高要件の考え方 # 1 (セキュリティ、性能・拡張性等)

IPAの非機能要求グレード2018に基づいた、重要度高要件 (セキュリティ) の考え方の素案です。

大項目	中項目	小項目	小項目説明	メトリクス	【ご参考】 トレサビシステム	CMP案	
						アプリ	基盤
セキュリティ	マルウェア対策	マルウェア対策	マルウェア (ウイルス、ワーム、ボット等) の感染を防止する、マルウェア対策の実施範囲やチェックタイミングを確認するための項目。 対策を実施する場合には、ウイルス定義ファイルの更新方法やタイミングについても検討し、常に最新の状態となるようにする必要がある。	マルウェア対策実施範囲 0:無し 1:重要度が高い資産を扱う範囲、あるいは、外接部分 2:システム全体	1: 「重要な情報資産」と定義した範囲において、マルウェア対策を実施	【必須】 1:重要度が高い資産を扱う範囲、あるいは、外接部分	1:重要度が高い資産を扱う範囲、あるいは、外接部分
	Web対策	Web実装対策	Webアプリケーション特有の脅威、脆弱性に関する対策を実施するかを確認するための項目。	セキュアコーディング、Webサーバの設定等による対策の強化 0:無し 1:対策の強化	1: Internetからの接続を受け付けるWebアプリケーションにおいて、セキュアコーディング等の対策の強化を実施	【必須】 1:対策の強化	1:対策の強化
				WAFの導入の有無 0:無し 1:有り	1: Internetからの接続を受け付けるWebアプリケーションにおいて、WAFの導入を実施	【必須】 1:有り	1:有り

重要度高要件の考え方 # 1 (セキュリティ、性能・拡張性等)

IPAの非機能要求グレード2018に基づいた、重要度高要件 (性能・拡張性) の考え方の素案です。

大項目	中項目	小項目	小項目説明	メトリクス	【ご参考】 トレサビシステム	CMP案	
						アプリ	基盤
性能・ 拡張性	業務処 理量	通常時 の業務 量	性能・拡張性に影響を与える業務 量。 該当システムの稼働時を想定し、合 意する。 それぞれのメトリクスにおいて、単一 の値だけでなく、前提となる時間帯 や季節の特性なども考慮する。	ユーザ数 0:特定ユーザの み 1:上限が決まって いる 2:不特定多数の ユーザが利用	1: ・参加企業者数200 =事業者数	【推奨】 1:上限が決まって いる ※ユーザがストレ スなく利用できる ことが望ましい	1:上限が決まって いる 企業数：1,000 社 (最大 10,000社)
				同時アクセス数 0:特定利用者の 限られたアクセス のみ 1:同時アクセスの 上限が決まってい る 2:不特定多数の アクセス有り	1: ・同時アクセス数 10TPS	【推奨】 1:同時アクセスの 上限が決まってい る ※ユーザがストレ スなく利用できる ことが望ましい	1:同時アクセスの 上限が決まってい る 通常時1000社が同 時に1分間に1操作 を行う (≒17TPS) ピーク時10,000社が 1分間に1操作を行 う (≒170TPS)

重要度高要件の考え方 # 1 (セキュリティ、性能・拡張性等)

IPAの非機能要求グレード2018に基づいた、重要度高要件（性能・拡張性）の考え方の素案です。

大項目	中項目	小項目	小項目説明	メトリクス	【ご参考】 トレサビシステム	CMP案	
						アプリ	基盤
性能・ 拡張性	業務処 理量	通常時 の業務 量	性能・拡張性に影響を与える業務量。 該当システムの稼働時を想定し、合意する。 それぞれのメトリクスにおいて、単一の値だけでなく、前提となる時間帯や季節の特性なども考慮する。	データ量 0:全てのデータ量が明確である 1:主要なデータ量のみが明確である	1: 以下の基礎数値をベースに試算 ①主要テーブルの一覧 ②テーブル毎の最大レコードサイズ ③最大レコード件数	【推奨】 1:主要なデータ量のみが明確である ※ユーザがストレスなく利用できることが望ましい	1:主要なデータ量のみが明確である
				オンラインリクエスト件数 0:処理毎にリクエスト件数が明確である 1:主な処理のリクエスト件数のみが明確である	1: 以下の基礎数値をベースに試算 主なオンライン処理とリクエスト件数/h(最繁忙時)の一覧	【推奨】 1:主な処理のリクエスト件数のみが明確である ※ユーザがストレスなく利用できることが望ましい	1:主な処理のリクエスト件数のみが明確である

重要度高要件の考え方 # 1 (セキュリティ、性能・拡張性等)

IPAの非機能要求グレード2018に基づいた、重要度高要件（性能・拡張性）の考え方の素案です。

大項目	中項目	小項目	小項目説明	メトリクス	【ご参考】 トレサビシステム	CMP案	
						アプリ	基盤
性能・ 拡張性	業務処 理量	業務量 増大度	システム稼働開始からライフサイクル 終了までの間で、開始時点と業務 量が最大になる時点の業務量の倍 率。 必要に応じ、開始日の平均値や、 開始後の定常状態との比較を行う 場合もある。	ユーザ数増大率 0:1倍 1:1.2倍 2:1.5倍 3:2倍 4:3倍 5:10倍以上	5: 初期利用時10社 参加企業者数200 →20倍 増大に柔軟に対応で きるようクラウドサービ スを利用する	【推奨】 1:1.2倍 ※ユーザの増加 に応じて拡張でき ることが望ましい <small>※非機能要求グレードの社会 的影響が限定されるシステムの 値を設定した</small>	5:10倍以上
				同時アクセス数 増大率 0:1倍 1:1.2倍 2:1.5倍 3:2倍 4:3倍 5:10倍以上	5: 初期利用時10社 参加企業者数200 →20倍 増大に柔軟に対応で きるようクラウドサービ スを利用する	【推奨】 1:1.2倍 ※ユーザの増加 に応じて拡張でき ることが望ましい <small>※非機能要求グレードの社会 的影響が限定されるシステムの 値を設定した</small>	5:10倍以上

重要度高要件の考え方 # 1 (セキュリティ、性能・拡張性等)

IPAの非機能要求グレード2018に基づいた、重要度高要件 (性能・拡張性) の考え方の素案です。

大項目	中項目	小項目	小項目説明	メトリクス	【ご参考】 トレサビシステム	CMP案	
						アプリ	基盤
性能・ 拡張性	業務処 理量	業務量 増大度	システム稼働開始からライフサイクル 終了までの間で、開始時点と業務 量が最大になる時点の業務量の倍 率。 必要に応じ、開始日の平均値や、 開始後の定常状態との比較を行う 場合もある。	データ量増大率 0:1倍 1:1.2倍 2:1.5倍 3:2倍 4:3倍 5:10倍以上	5: 初期利用時10社 参加企業者数200 →20倍 増大に柔軟に対応で きるようクラウドサービ スを利用する	【推奨】 1:1.2倍 ※ユーザの増加 に応じて拡張でき ることが望ましい <small>※非機能要求グレードの社会 的影響が限定されるシステムの 値を設定した</small>	5:10倍以上
				オンラインクエス ト件数増大率 0:1倍 1:1.2倍 2:1.5倍 3:2倍 4:3倍 5:10倍以上	5: 初期利用時10社 参加企業者数200 →20倍 増大に柔軟に対応で きるようクラウドサービ スを利用する	【推奨】 1:1.2倍 ※ユーザの増加 に応じて拡張でき ることが望ましい <small>※非機能要求グレードの社会 的影響が限定されるシステムの 値を設定した</small>	5:10倍以上

重要度高要件の考え方 # 1 (セキュリティ、性能・拡張性等)

IPAの非機能要求グレード2018に基づいた、重要度高要件 (性能・拡張性) の考え方の素案です。

大項目	中項目	小項目	小項目説明	メトリクス	【ご参考】 トレサビシステム	CMP案	
						アプリ	基盤
性能・ 拡張性	業務処 理量	保管期 間	システムが参照するデータの内、OS やミドルウェアのログなどのシステム基 盤が利用するデータに対する保管が 必要な期間。 必要に応じて、データの種別毎に定め る。 保管対象のデータを選択する際に は、対象範囲についても決めておく。	保管期間 0:6ヶ月 1:1年 2:3年 3:5年 4:10年以上有期 5:永久保管	2: 原則ログを含むCFP データは3年保管、 DDは10年保管となる 見込み	【必須】 4:10年以上有期 業務データについ ては、REACH規 則より対象製品 が最終出荷され てから10年保管 が必要	5:永久保管 業務データについ ては、REACH規 則より対象製品 が最終出荷され てから10年保管 が必要であるが、 基盤としてはそれ 以上の長期保管 が求められる。
	性能目 標値	オンライ ンレスポ ンス	オンラインシステム利用時に要求され るレスポンス。 システム化する対象業務の特性を ふまえ、どの程度のレスポンスが必要 かについて確認する。ピーク特性や、 障害時の運用を考慮し、通常時・ ピーク時・縮退運転時毎に順守率 を決める。具体的な数値は特定の 機能またはシステム分類毎に決めて おくことが望ましい。(例: Webシス テムの参照系/更新系/一覧系な ど)	通常時レスポンス 順守率 0:順守率を定め ない 1:60% 2:80% 3:90% 4:95% 5:99%以上	0: 性能目標は定義しな い。ただし、事前に測 定を行い、利用者・ 関連団体と結果につ いて合意すること。	【推奨】 3:90% 基盤接続処理を 除き、処理待ち 時の処理中表示 などを含め、通常 時のトランザクシ ョン数の内90%が 目標値を達成す るよう設計する	0:順守率を定め ない SLA/SLOは定め ないが、高トラ フィック時にもデー タ損失が発生し ないこと

重要度高要件の考え方 # 1 (セキュリティ、性能・拡張性等)

IPAの非機能要求グレード2018に基づいた、重要度高要件（性能・拡張性）の考え方の素案です。

大項目	中項目	小項目	小項目説明	メトリクス	【ご参考】 トレサビシステム	CMP案	
						アプリ	基盤
性能・ 拡張性	性能目 標値	オンライ ンレスポ ンス	オンラインシステム利用時に要求されるレスポンス。 システム化する対象業務の特性をふまえ、どの程度のレスポンスが必要かについて確認する。ピーク特性や、障害時の運用を考慮し、通常時・ピーク時・縮退運転時毎に順守率を決める。具体的な数値は特定の機能またはシステム分類毎に決めておくことが望ましい。（例：Webシステムの参照系/更新系/一覧系など）	ピーク時レスポンス順守率 0:順守率を定めない 1:60% 2:80% 3:90% 4:95% 5:99%以上	0: 性能目標は定義しない。ただし、事前に測定を行い、利用者・関連団体と結果について合意すること。	【推奨】 2:80% ※ユーザがストレスなく利用できることが望ましい <small>※非機能要求グレードの社会的影響が限定されるシステムの値を設定した</small>	0:順守率を定めない SLA/SLOは定めないが高トラフィック時にもデータ損失が発生しないこと

重要度高要件の考え方 # 1（セキュリティ、性能・拡張性等）

IPAの非機能要求グレード2018に基づいた、重要度高要件（性能・拡張性）の考え方の素案です。

大項目	中項目	小項目	小項目説明	メトリクス	【ご参考】 トレサビシステム	CMP案	
						アプリ	基盤
性能・ 拡張性	リソース 拡張性	CPU拡張性	CPUの拡張性を確認するための項目。 CPU利用率は、将来の業務量の増加に備え、どれだけCPUに余裕をもたせておくかを確認するための項目。 CPU拡張性は、物理的もしくは仮想的に、どれだけCPUを拡張できるようにしておくかを確認するための項目。	CPU利用率 0:80%以上 1:50%以上80%未満 2:20%以上50%未満 3:20%未満	1: 社会的影響が限定されるシステムでの基準をもとに50%以上、80%未満の範囲の利用率に収まるようサイジングを実施	【推奨】 1:50%以上80%未満 ※ユーザがストレスなく利用できることが望ましい <small>※非機能要求グレードの社会的影響が限定されるシステムの値を設定した</small>	1:50%以上80%未満
				CPU拡張性 0:1倍（拡張要求無し） 1:1.5倍 2:2倍 3:4倍 4:8倍以上	1: 1.5倍以上の拡張性を最低限としているが、クラウドサービスを利用するため、クラウドサービスの上限値まで（8倍以上）拡張可能	【推奨】 1:1.5倍 ※ユーザの増加に応じて拡張できることが望ましい <small>※非機能要求グレードの社会的影響が限定されるシステムの値を設定した</small>	4:8倍以上 将来的な参加企業の増加に対応するため、柔軟なスケールアウト/スケールアップが可能であること

重要度高要件の考え方 # 1 (セキュリティ、性能・拡張性等)

IPAの非機能要求グレード2018に基づいた、重要度高要件 (性能・拡張性) の考え方の素案です。

大項目	中項目	小項目	小項目説明	メトリクス	【ご参考】 トレサビシステム	CMP案	
						アプリ	基盤
性能・ 拡張性	リソース 拡張性	メモリ拡張性	メモリの拡張性を確認するための項目。 メモリ利用率は、将来の業務量の増加に備え、どれだけメモリに余裕をもたせておくかを確認するための項目。 メモリ拡張性は、物理的もしくは仮想的に、どれだけメモリを拡張できるようにしておくかを確認するための項目。	メモリ利用率 0:80%以上 1:50%以上80%未満 2:20%以上50%未満 3:20%未満	1: 社会的影響が限定されるシステムでの基準をもとに50%以上、80%未満の範囲の利用率に収まるようサイジングを実施	【推奨】 1:50%以上80%未満 ※ユーザがストレスなく利用できることが望ましい <small>※非機能要求グレードの社会的影響が限定されるシステムの値を設定した</small>	1:50%以上80%未満
				メモリ拡張性 0:1倍 (拡張要求無し) 1:1.5倍 2:2倍 3:4倍 4:8倍以上	1: 1.5倍以上の拡張性を最低限としているが、クラウドサービスを利用するため、クラウドサービスの上限値まで (8倍以上) 拡張可能	【推奨】 1:1.5倍 ※ユーザの増加に応じて拡張できることが望ましい <small>※非機能要求グレードの社会的影響が限定されるシステムの値を設定した</small>	4:8倍以上 将来的な参加企業の増加に対応するため、柔軟なスケールアウト/スケールアップが可能であること

重要度高要件の考え方 # 2 (運用・保守性)

IPAの非機能要求グレード2018に基づいた、重要度高要件 (運用・保守性) の考え方の素案です。

大項目	中項目	小項目	小項目説明	メトリクス	【ご参考】 トレサビシステム	CMP案	
						アプリ	基盤
運用・保守性	通常運用	運用時間	システム運用を行う時間。利用者やシステム管理者に対してサービスを提供するために、システムを稼働させ、オンライン処理やバッチ処理を実行している時間帯のこと。	運用時間 (通常/特定日) 0:規定無し 1:定時内 (9時～17時) 2:夜間のみ停止 (9時～21時) 3:1時間程度の停止有り (9時～翌朝8時) 4:若干の停止有り (9時～翌朝8時55分) 5:24時間無停止	5: 計画停止を除き24時間無停止 (計画停止は月1回実施)	【推奨】 5:24時間無停止 計画停止を除き24時間無停止	5:24時間無停止 計画停止を除き24時間無停止 (計画停止は月1回実施)

重要度高要件の考え方 # 2（運用・保守性）

IPAの非機能要求グレード2018に基づいた、重要度高要件（運用・保守性）の考え方の素案です。

大項目	中項目	小項目	小項目説明	メトリクス	【ご参考】 トレサビシステム	CMP案	
						アプリ	基盤
運用・保守性	通常運用	バックアップ	システムが利用するデータのバックアップに関する項目。	外部データの利用可否 0:全データの復旧に利用できる 1:一部のデータ復旧に利用できる 2:外部データは利用できない	2: 障害を理由にした外部システムからのデータ利用は原則として想定しない。万が一データが消失した場合には、ユーザへの再登録を依頼する。（バックアップデータはシステム外に出さない）	【推奨】 2:外部データは利用できない	2:外部データは利用できない
				バックアップ利用範囲 0:バックアップを取得しない 1:障害発生時のデータ損失防止 2:ユーザエラーからの回復 3:データの長期保存（アーカイブ）	1: 定められたRPOへのデータ回復に利用する。 システム管理者の作業ミスによる復旧は管理者が作業前に個別にデータ保全作業を実施することで担保することとし、バックアップによる回復はしない	【必須】 1:障害発生時のデータ損失防止	1:障害発生時のデータ損失防止

重要度高要件の考え方 # 2 (運用・保守性)

IPAの非機能要求グレード2018に基づいた、重要度高要件 (運用・保守性) の考え方の素案です。

大項目	中項目	小項目	小項目説明	メトリクス	【ご参考】 トレサビシステム	CMP案	
						アプリ	基盤
運用・保守性	通常運用	バックアップ	システムが利用するデータのバックアップに関する項目。	バックアップ自動化の範囲 0:全ステップを手動で行う 1:一部のステップを手動で行う 2:全ステップを自動で行う	1: バックアップに関するオペレーションは自動化するが、クラウドサービスの制約上一部の作業 (バックアップ対象外としている重要度の低いログデータ等) は必要に応じて手動で行う必要がある	【推奨】 1:一部のステップを手動で行う	1:一部のステップを手動で行う
				バックアップ取得間隔 0:バックアップを取得しない 1:システム構成の変更時など、任意のタイミング 2:月次で取得 3:週次で取得 4:日次で取得 5:同期バックアップ	4. 1日1回スナップショット & 1日分のシステムトランザクションログを取得。限りなく障害直前までは戻せる想定。	【必須】 4.日次で取得	4.日次で取得

重要度高要件の考え方 # 2 (運用・保守性)

IPAの非機能要求グレード2018に基づいた、重要度高要件 (運用・保守性) の考え方の素案です。

大項目	中項目	小項目	小項目説明	メトリクス	【ご参考】 トレサビシステム	CMP案	
						アプリ	基盤
運用・保守性	通常運用	バックアップ	システムが利用するデータのバックアップに関する項目。	バックアップ保存期間 0:バックアップを取得しない 1:1年未満 2:3年 3:5年 4:10年以上有期 5:永久保存	1: 定期的にバックアップを取得する。そのバックアップは何年も保存しない。 業務データは指定期間腹持ちする。(併せてデータの改ざん防止対策を実施する)	【必須】 1:1年未満	1:1年未満

重要度高要件の考え方 # 2 (運用・保守性)

IPAの非機能要求グレード2018に基づいた、重要度高要件 (運用・保守性) の考え方の素案です。

大項目	中項目	小項目	小項目説明	メトリクス	【ご参考】 トレサビシステム	CMP案	
						アプリ	基盤
運用・保守性	通常運用	運用監視	<p>システム全体、あるいはそれを構成するハードウェア・ソフトウェア（業務アプリケーションを含む）に対する監視に関する項目。</p> <p>セキュリティ監視については本項目には含めない。「不正監視」の項目で別途検討すること。</p>	<p>監視情報</p> <p>0:監視を行わない</p> <p>1:死活監視を行う</p> <p>2:エラー監視を行う</p> <p>3:エラー監視（トレース情報を含む）を行う</p> <p>4:リソース監視を行う</p> <p>5:パフォーマンス監視を行う</p>	<p>4: CPU使用率やスワップの発生状況等に対して閾値を設定し、サービスレベル低下の予兆を監視した上でシステムの拡張計画や運用スケジュールの検討を行う</p>	<p>【推奨】 4:リソース監視を行う</p>	<p>4:リソース監視を行う</p>

重要度高要件の考え方 # 2（運用・保守性）

IPAの非機能要求グレード2018に基づいた、重要度高要件（運用・保守性）の考え方の素案です。

大項目	中項目	小項目	小項目説明	メトリクス	【ご参考】 トレサビシステム	CMP案	
						アプリ	基盤
運用・保守性	通常運用	運用監視	<p>システム全体、あるいはそれを構成するハードウェア・ソフトウェア（業務アプリケーションを含む）に対する監視に関する項目。</p> <p>セキュリティ監視については本項目には含めない。「不正監視」の項目で別途検討すること。</p>	<p>監視間隔</p> <p>0:監視を行わない</p> <p>1:不定期監視（手動監視）</p> <p>2:定期監視（1日間隔）</p> <p>3:定期監視（数時間間隔）</p> <p>4:リアルタイム監視（分間隔）</p> <p>5:リアルタイム監視（秒間隔）</p>	<p>4:</p> <p>サービス提供に影響がある範囲は冗長化されており、障害が直ちにサービス提供に影響しないことから、分間隔での監視を許容する。</p>	<p>【推奨】</p> <p>4:リアルタイム監視（分間隔）</p>	<p>4:リアルタイム監視（分間隔）</p>

重要度高要件の考え方 # 2 (運用・保守性)

IPAの非機能要求グレード2018に基づいた、重要度高要件 (運用・保守性) の考え方の素案です。

大項目	中項目	小項目	小項目説明	メトリクス	【ご参考】 トレサビシステム	CMP案	
						アプリ	基盤
運用・保守性	保守運用	計画停止	点検作業や領域拡張、デフラグ、マスターデータのメンテナンス等、システムの保守作業の実施を目的とした、事前計画済みのサービス停止に関する項目。	計画停止の有無 0:計画停止有り (運用スケジュールの変更可) 1:計画停止有り (運用スケジュールの変更不可) 2:計画停止無し	0: 計画的な停止は許容する。また運用スケジュールの変更も可とする。	【必須】 0:計画停止有り (運用スケジュールの変更可)	0:計画停止有り (運用スケジュールの変更可)
		運用負荷削減	保守運用に関する作業負荷を削減するための設計に関する項目。	保守作業自動化の範囲 0:保守作業は全て手動で実施する 1:一部の保守作業を自動で実行する 2:全ての保守作業を自動で実行する	1: 業務機能の起動・停止など定期的に行う処理は自動化するが、パッチ適用など非定期に実行する処理は管理者が一部手動で実施する。また、バックアップからのリカバリ等は手動となる。	【推奨】 1:一部の保守作業を自動で実行する	1:一部の保守作業を自動で実行する

重要度高要件の考え方 # 2 (運用・保守性)

IPAの非機能要求グレード2018に基づいた、重要度高要件 (運用・保守性) の考え方の素案です。

大項目	中項目	小項目	小項目説明	メトリクス	【ご参考】 トレサビシステム	CMP案	
						アプリ	基盤
運用・保守性	運用環境	開発用環境の設置	ユーザがシステムに対する開発作業を実施する目的で導入する環境についての項目。	<p>開発用環境の設置有無</p> <p>0:システムの開発環境を設置しない</p> <p>1:運用環境の一部に限定した開発環境を設置する</p> <p>2:運用環境と同一の開発環境を設置する</p>	<p>2: サービス開始後の維持と開発用途を兼ねた環境とすることを許容する</p> <p>【ご参考】 トレサビシステムの環境</p> <ul style="list-style-type: none"> ・本番環境 ・検証環境 (★本項でいう開発用環境に該当) ・開発環境 (基盤開発事業者が機能追加・改変の開発を先行して行う環境) ・オンボーディング環境 (アプリ開発事業者向けの基盤接続テスト向け環境) 	<p>【推奨】 2:運用環境と同一の開発環境を設置する</p>	<p>2:運用環境と同一の開発環境を設置する</p>

重要度高要件の考え方 # 2 (運用・保守性)

IPAの非機能要求グレード2018に基づいた、重要度高要件 (運用・保守性) の考え方の素案です。

大項目	中項目	小項目	小項目説明	メトリクス	【ご参考】 トレサビシステム	CMP案	
						アプリ	基盤
運用・保守性	運用環境	試験用環境の設置	ユーザがシステムの動作を試験する目的で導入する環境についての項目。	試験用環境の設置有無 0:システムの試験環境を設置しない 1:システムの開発用環境と併用する 2:専用の試験用環境を設置する	2: 専用の試験用環境を用意する。 ただし、サービス開始後の維持と開発用途を兼ねた環境とすることを許容する 【ご参考】 トレサビシステムの環境 ・本番環境 ・検証環境 ・開発環境 (★本項の試験用環境に該当) ・オンボーディング環境 (★本項の試験用環境に該当)	【推奨】 2:専用の試験用環境を設置する	2:専用の試験用環境を設置する

重要度高要件の考え方 # 2 (運用・保守性)

IPAの非機能要求グレード2018に基づいた、重要度高要件 (運用・保守性) の考え方の素案です。

大項目	中項目	小項目	小項目説明	メトリクス	【ご参考】 トレサビシステム	CMP案	
						アプリ	基盤
運用・保守性	運用環境	マニュアル準備レベル	運用のためのマニュアルの準備のレベル。	マニュアル準備レベル 0:各製品標準のマニュアルを利用する 1:システムの通常運用のマニュアルを提供する 2:システムの通常運用と保守運用のマニュアルを提供する 3:ユーザのシステム運用ルールに基づくカスタマイズされたマニュアルを提供する	2: 通常運用は、マニュアルを整備する。また、緊急時に迅速に対応を行うために、保守運用マニュアルを整備する。	【必須】 2:システムの通常運用と保守運用のマニュアルを提供する	2:システムの通常運用と保守運用のマニュアルを提供する

重要度高要件の考え方 # 2（運用・保守性）

IPAの非機能要求グレード2018に基づいた、重要度高要件（運用・保守性）の考え方の素案です。

大項目	中項目	小項目	小項目説明	メトリクス	【ご参考】 トレサビシステム	CMP案	
						アプリ	基盤
運用・保守性	運用環境	リモートオペレーション	システムの設置環境とは離れた環境からのネットワークを介した監視や操作の可否を定義する項目。	リモート監視地点	2: パブリッククラウドを採用するため、システムを構成する機器/サービスについてはリモート監視する。	【必須】 2:遠隔地でリモート監視を行う	2:遠隔地でリモート監視を行う
				0:リモート監視を行わない 1:構内LANを介してリモート監視を行う 2:遠隔地でリモート監視を行う			
				リモート操作の範囲	2: パブリッククラウドを採用するため、システムを構成する機器/サービスについてはリモートで操作を行う。そのため、リモート操作内容の制限は行わない。 (セキュリティ要件である利用制限と不正監視を守る前提)	【必須】 2:任意のリモート操作を行う (セキュリティ要件である利用制限と不正監視を守る前提)	2:任意のリモート操作を行う (セキュリティ要件である利用制限と不正監視を守る前提)
				0:リモート操作を行わない 1:定型処理のみリモート操作を行う 2:任意のリモート操作を行う			

重要度高要件の考え方 # 2 (運用・保守性)

IPAの非機能要求グレード2018に基づいた、重要度高要件 (運用・保守性) の考え方の素案です。

大項目	中項目	小項目	小項目説明	メトリクス	【ご参考】 トレサビシステム	CMP案	
						アプリ	基盤
運用・保守性	運用環境	外部システム接続	システムの運用に影響する外部システムとの接続の有無に関する項目。	外部システムとの接続有無 0:外部システムと接続しない 1:社内の外部システムと接続する 2:社外の外部システムと接続する	2: 本システム特性上、アプリや各社システムからの接続が存在する。その他、海外接続 (Catena-X等) も将来予定される。	【必須】 2:社外の外部システムと接続する	2:社外の外部システムと接続する

重要度高要件の考え方 # 2 (運用・保守性)

IPAの非機能要求グレード2018に基づいた、重要度高要件 (運用・保守性) の考え方の素案です。

大項目	中項目	小項目	小項目説明	メトリクス	【ご参考】 トレサビシステム	CMP案	
						アプリ	基盤
運用・保守性	サポート体制	保守契約 (ハードウェア)	保守が必要な対象ハードウェアの範囲。	保守契約 (ハードウェア) の範囲 0:保守契約を行わない 1:ベンダの自社製品 (ハードウェア) に対してのみ保守契約を行う 2:マルチベンダのサポート契約を行う (一部対象外を許容) 3:マルチベンダのサポート契約を行う (システムを構成する全製品を対象)	対象外 HWの持ち込み無しのため、対象外。	【推奨】 2:マルチベンダのサポート契約を行う (一部対象外を許容) ただし、HWを利用する場合のみ <small>※非機能要求グレードの社会的影響が限定されるシステムの値を設定した</small>	対象外 HWの持ち込み無しのため、対象外。

重要度高要件の考え方 # 2 (運用・保守性)

IPAの非機能要求グレード2018に基づいた、重要度高要件 (運用・保守性) の考え方の素案です。

大項目	中項目	小項目	小項目説明	メトリクス	【ご参考】 トレサビシステム	CMP案	
						アプリ	基盤
運用・保守性	サポート体制	保守契約 (ソフトウェア)	保守が必要な対象ソフトウェアの範囲。	保守契約 (ソフトウェア) の範囲 0:保守契約を行わない 1:ベンダの自社製品 (ソフトウェア) に対してのみ保守契約を行う 2:マルチベンダのサポート契約を行う (一部対象外を許容) 3:マルチベンダのサポート契約を行う (システムを構成する全製品を対象)	1: ベンダのソフトウェア製品個別に保守契約を結ぶ。 ※ここでいうベンダは、ソフトウェアのベンダ (RedHat, Microsoft等) を指す	【推奨】 1:ベンダの自社製品 (ソフトウェア) に対してのみ保守契約を行う	1:ベンダの自社製品 (ソフトウェア) に対してのみ保守契約を行う

重要度高要件の考え方 # 2 (運用・保守性)

IPAの非機能要求グレード2018に基づいた、重要度高要件 (運用・保守性) の考え方の素案です。

大項目	中項目	小項目	小項目説明	メトリクス	【ご参考】 トレサビシステム	CMP案	
						アプリ	基盤
運用・保守性	サポート体制	ライフサイクル期間	運用保守の対応期間および、実際にシステムが稼働するライフサイクルの期間。	ライフサイクル期間 0:3年 1:5年 2:7年 3:10年	1: HW保守はクラウドサービス (AWS) 側で実施しているため、特に意識する必要は無し。 OSは5年間であれば耐えうると想定。	【必須】 1:5年	1:5年

重要度高要件の考え方 # 2 (運用・保守性)

IPAの非機能要求グレード2018に基づいた、重要度高要件 (運用・保守性) の考え方の素案です。

大項目	中項目	小項目	小項目説明	メトリクス	【ご参考】 トレサビシステム	CMP案	
						アプリ	基盤
	その他の運用管理方針	内部統制対応	IT運用プロセスの内部統制対応を行うかどうかに関する項目。	内部統制対応の実施有無 0:内部統制対応について規定しない 1:既存の社内規定に従って、内部統制対応を実施する 2:新規に規定を制定し、内部統制対応を実施する	1: 既存の社内規定に従って、内部統制対応を実施する	【推奨】 1:既存の社内規定に従って、内部統制対応を実施する ISO 9001 (品質)、ISO/IEC 27001 (情報セキュリティ)、ISO 31000 (リスク管理)、ISO 22301 (事業継続)、ISO 37001 (贈収賄防止) に定められた内部統制関連規格への準拠	1:既存の社内規定に従って、内部統制対応を実施する

重要度高要件の考え方 # 2（運用・保守性）

IPAの非機能要求グレード2018に基づいた、重要度高要件（運用・保守性）の考え方の素案です。

大項目	中項目	小項目	小項目説明	メトリクス	【ご参考】 トレサビシステム	CMP案	
						アプリ	基盤
運用・保守性	その他の運用管理方針	サービスデスク	ユーザの問合せに対して単一の窓口機能を提供するかどうかに関する項目。	サービスデスクの設置有無 0:サービスデスクの設置について規定しない 1:既存のサービスデスクを利用する 2:新規にサービスデスクを設置する	2: 新規システムのため、新規にサービスデスクを立ち上げる方針とする。	【推奨】 2:新規にサービスデスクを設置する	2:新規にサービスデスクを設置する ただし、CMPの運用団体様との議論によっては、トレサビシステムのサービスデスクの共用はあり得るものとする。

重要度低要件の確認

以降のページは重要度低要件である、可用性についての考え方を記載したものとなります。

分類	概要	CMPにおける優先度		優先度の主な判断根拠
		アプリ	基盤	
可用性	システムを継続的に利用可能とするための要求。 「継続性」、「耐障害性」、「災害対策」、「回復性」などで構成される。	低	低	■ アプリ・基盤共通 システム停止により直ちに影響が出るシステムではないため、最低限の対応とする。
性能	システムの性能に関する要求。 「業務処理量」、「性能目標値」などで構成される。	高	低	■ アプリ 処理待ち時の処理中表示などユーザへの配慮は必要であるため、手厚く対応する。 ■ 基盤 応答性能を求めるシステムではないため、最低限の対応とする。多量性能については、拡張性で対応する。
拡張性	将来のシステム拡張に関する要求。 「リソース拡張性」などで構成される。	低	高	■ アプリ 利用者の増加とアプリの機能拡張次第であり、最低限の対応とする。 ■ 基盤 参加企業の増加、逐次発生する参加・退会へ柔軟に対応する必要があるため、手厚く対応する。
運用・保守性	システムの運用と保守のサービスに関する要求。 「通常運用」、「保守運用」、「障害時運用」の運用パターンと「運用環境」、「サポート体制」、「運用管理方針」などで構成される。	高	高	■ アプリ・基盤共通 障害やシステムアップデートなどが生じた際に、効率的で安定性のある対応が求められるため、手厚く対応する。
移行性	現行システム資産の移行に関する要求。 「移行方式」、「移行対象」、「移行計画」などで構成される。	低	低	■ アプリ・基盤共通 CMPは新規システムであり、システム移行は想定されないため、最低限の対応とする。ただし、chemSHERPAなど、現行業務アプリからのデータ移行が発生する場合は、優先度を上げて対応する。
セキュリティ	情報システムの安全性の確保に関する要求。 「セキュリティ診断」、「アクセス制御」、「データの秘匿」、「不正監視」、「ネットワーク対策」、「マルウェア対策」、「セキュリティインシデント対応」などで構成される。	高	高	■ アプリ・基盤共通 秘匿性の高いデータを取り扱うため、手厚く対応する。

【ご参考】重要度低要件の確認

IPAの非機能要求グレード2018に基づいた、重要度低要件（可用性）の考え方の素案です。

大項目	中項目	小項目	小項目説明	メトリクス	【ご参考】 トレサビシステム	CMP案	
						アプリ	基盤
可用性	継続性	業務継続性	可用性を保証するにあたり、要求される業務の範囲とその条件。	対象業務範囲 0:内部向けバッチ系業務 1:内部向けオンライン系業務 2:内部向け全業務 3:外部向けバッチ系業務 4:外部向けオンライン系業務 5:全ての業務	4: オンラインでのデータ連携（共有）が本システムの主要業務であるため、「外部向けオンライン系業務」を保証範囲とする。	【推奨】 4:外部向けオンライン系業務	4:外部向けオンライン系業務
				サービス切替時間 0:24時間以上 1:24時間未満 2:2時間未満 3:60分未満 4:10分未満 5:60秒未満	3: CFP・DDデータの共有は、法令順守や規制対応を目的としており、ビジネス上の即時性が求められるものではない。	【推奨】 3:60分未満	3:60分未満

【ご参考】重要度低要件の確認

IPAの非機能要求グレード2018に基づいた、重要度低要件（可用性）の考え方の素案です。

大項目	中項目	小項目	小項目説明	メトリクス	【ご参考】 トレサビシステム	CMP案	
						アプリ	基盤
可用性	継続性	業務継続性	可用性を保証するにあたり、要求される業務の範囲とその条件。	業務継続の要求度 0:障害時の業務停止を許容する 1:単一障害時は業務停止を許容せず、処理を継続させる 2:二重障害時でもサービス切替時間の規定内で継続する	1: CFP・DDデータの共有は、法令順守や規制対応を目的としており、ビジネス上の即時性が求められるものではない。上記理由から、単一障害には対応するが、二重障害に耐える構成は必須としない。 ※Hyperledger fabricの参照業務のみにおいては、今回の構成上、単一障害時に業務継続は不可となる。(単一企業の障害は全体の障害とは捉えない)	【推奨】 1:単一障害時は業務停止を許容せず、処理を継続させる	1:単一障害時は業務停止を許容せず、処理を継続させる

【ご参考】重要度低要件の確認

IPAの非機能要求グレード2018に基づいた、重要度低要件（可用性）の考え方の素案です。

大項目	中項目	小項目	小項目説明	メトリクス	【ご参考】 トレサビシステム	CMP案	
						アプリ	基盤
可用性	継続性	目標復旧水準 (業務停止時)	業務停止を伴う障害が発生した際、何をどこまで、どれ位で復旧させるかの目標。	RPO（目標復旧地点） 0:復旧不要 1:5営業日前の時点（週次バックアップからの復旧） 2:1営業日前の時点（日次バックアップからの復旧） 3:障害発生時点（日次バックアップ+アーカイブからの復旧）	3: データベースについては、障害発生時点を復旧目標とする。同期もしくは日次バックアップを利用して復旧を行い、アーカイブを用いて、障害復旧時点まで復旧を行う。 データベース以外のファイルシステムについては、障害復旧時点までの復旧を必須とせず、日次バックアップからの復旧を行う。	【推奨】 3:障害発生時点（日次バックアップ+アーカイブからの復旧）	3:障害発生時点（日次バックアップ+アーカイブからの復旧）

【ご参考】重要度低要件の確認

IPAの非機能要求グレード2018に基づいた、重要度低要件（可用性）の考え方の素案です。

大項目	中項目	小項目	小項目説明	メトリクス	【ご参考】 トレサビシステム	CMP案	
						アプリ	基盤
可用性	継続性	目標復旧水準 (業務停止時)	業務停止を伴う障害が発生した際、何をどこまで、どれ位で復旧させるかの目標。	RTO（目標復旧時間） 0:1営業日以上 1:1営業日以内 2:12時間以内 3:6時間以内 4:2時間以内	2: CFP・DDデータの共有は、法令順守や規制対応を目的としており、ビジネス上の即時性が求められるものではない。上記理由から、非機能要件グレード表の「社会的影響が限定されるシステム」を参考に12時間以内のRTOを設定する。	【推奨】 2:12時間以内	2:12時間以内

【ご参考】重要度低要件の確認

IPAの非機能要求グレード2018に基づいた、重要度低要件（可用性）の考え方の素案です。

大項目	中項目	小項目	小項目説明	メトリクス	【ご参考】 トレサビシステム	CMP案	
						アプリ	基盤
可用性	継続性	目標復旧水準（業務停止時）	業務停止を伴う障害が発生した際、何をどこまで、どれ位で復旧させるかの目標。	RLO（目標復旧レベル） 0:システムの復旧 1:特定業務のみ 2:全ての業務	1: エンドユーザ系業務： 全て システム運用系業務： 復旧対象は一部	【推奨】 1:特定業務のみ	1:特定業務のみ
		目標復旧水準（大規模災害時）	大規模災害が発生した際、どれ位で復旧させるかの目標。 大規模災害とは、火災や地震などの異常な自然現象、あるいは人為的な原因による大きな事故、破壊行為により生ずる被害のことを指し、システムに甚大な被害が発生するか、電力などのライフラインの停止により、システムをそのまま現状に修復するのが困難な状態となる災害をいう。	システム再開目標 0:再開不要 1:数ヶ月以内に再開 2:一ヶ月以内に再開 3:一週間以内に再開 4:3日以内に再開 5:1日以内に再開	3: システム再開目標として、大規模災害が発生した場合には、構築可能（人、リソース含む）な状態になってから、一週間以内の再開を設定する。	【推奨】 3:一週間以内に再開	3:一週間以内に再開 システム再開目標として、大規模災害が発生した場合には、構築可能（人、リソース含む）な状態になってから、一週間以内の再開を設定する。

【ご参考】重要度低要件の確認

IPAの非機能要求グレード2018に基づいた、重要度低要件（可用性）の考え方の素案です。

大項目	中項目	小項目	小項目説明	メトリクス	【ご参考】 トレサビシステム	CMP案	
						アプリ	基盤
可用性	継続性	稼働率	<p>明示された利用条件の下で、システムが要求されたサービスを提供できる割合。</p> <p>明示された利用条件とは、運用スケジュールや、目標復旧水準により定義された業務が稼働している条件を指す。その稼働時間の中で、サービス中断が発生した時間により稼働率を求める。</p>	<p>稼働率</p> <p>0:95%以下 1:95% 2:99% 3:99.9% 4:99.99% 5:100%</p>	<p>2. CFP・DDデータの共有は、法令順守や規制対応を目的としており、ビジネス上の即時性が求められるものではない。</p> <p>上記特性を考慮した上で、99%（年間87.6時間※）の停止時間は許容できると判断し、コストバランスを図る。</p> <p>※計画停止時間は稼働率計算に含めない</p>	<p>【推奨】 2:99%</p>	<p>2:99%</p>

【ご参考】重要度低要件の確認

IPAの非機能要求グレード2018に基づいた、重要度低要件（可用性）の考え方の素案です。

大項目	中項目	小項目	小項目説明	メトリクス	【ご参考】 トレサビシステム	CMP案	
						アプリ	基盤
可用性	回復性	可用性 確認	可用性として要求された項目をどこまで確認するかの範囲。	確認範囲 0:実施しない。または単純な障害の範囲 1:業務を継続できる障害の範囲 2:業務停止となる障害の内一部の範囲 3:業務停止となる障害の全ての範囲	2: 業務停止となるリスクの高い範囲を確認する。	【推奨】 2:業務停止となる障害の内一部の範囲	2:業務停止となる障害の内一部の範囲

【ご参考】重要度低要件の確認

以降のページは重要度低要件である、移行性についての考え方を記載したものとなります。

移行性につきましては、同一システムの更改を意識した観点となっておりますため、全項目、ご参考として提示いたします。

分類	概要	CMPにおける優先度		優先度の主な判断根拠
		アプリ	基盤	
可用性	システムを継続的に利用可能とするための要求。 「継続性」、「耐障害性」、「災害対策」、「回復性」などで構成される。	低	低	■ アプリ・基盤共通 システム停止により直ちに影響が出るシステムではないため、最低限の対応とする。
性能	システムの性能に関する要求。 「業務処理量」、「性能目標値」などで構成される。	高	低	■ アプリ 処理待ち時の処理中表示などユーザへの配慮は必要であるため、手厚く対応する。 ■ 基盤 応答性能を求めるシステムではないため、最低限の対応とする。多量性能については、拡張性で対応する。
拡張性	将来のシステム拡張に関する要求。 「リソース拡張性」などで構成される。	低	高	■ アプリ 利用者の増加とアプリの機能拡張次第であり、最低限の対応とする。 ■ 基盤 参加企業の増加、逐次発生する参加・退会へ柔軟に対応する必要があるため、手厚く対応する。
運用・保守性	システムの運用と保守のサービスに関する要求。 「通常運用」、「保守運用」、「障害時運用」の運用パターンと「運用環境」、「サポート体制」、「運用管理方針」などで構成される。	高	高	■ アプリ・基盤共通 障害やシステムアップデートなどが生じた際に、効率的で安定性のある対応が求められるため、手厚く対応する。
移行性	現行システム資産の移行に関する要求。 「移行方式」、「移行対象」、「移行計画」などで構成される。	低	低	■ アプリ・基盤共通 CMPは新規システムであり、システム移行は想定されないため、最低限の対応とする。ただし、chemSHERPAなど、現行業務アプリからのデータ移行が発生する場合は、優先度を上げて対応する。
セキュリティ	情報システムの安全性の確保に関する要求。 「セキュリティ診断」、「アクセス制御」、「データの秘匿」、「不正監視」、「ネットワーク対策」、「マルウェア対策」、「セキュリティインシデント対応」などで構成される。	高	高	■ アプリ・基盤共通 秘匿性の高いデータを取り扱うため、手厚く対応する。

【ご参考】重要度低要件の確認

IPAの非機能要求グレード2018に基づいた、重要度低要件（移行性）の考え方の素案です。

大項目	中項目	小項目	小項目説明	メトリクス	【ご参考】 トレサビシステム	CMP案	
						アプリ	基盤
移行性	移行時期	移行のスケジュール	移行作業計画から本稼働までのシステム移行期間、システム停止可能日時、並行稼働の有無。（例外発生時の切り戻し時間や事前バックアップの時間等も含むこと。）	システム移行期間 0:システム移行無し 1:3ヶ月未満 2:半年未満 3:1年未満 4:2年未満 5:2年以上	新規システムであるため移行は無し （対象外）	【推奨】 4:2年未満 <small>※非機能要求グレードの社会的影響が限定されるシステムの値を設定した</small>	新規システムであるため移行は無し （対象外）

【ご参考】重要度低要件の確認

IPAの非機能要求グレード2018に基づいた、重要度低要件（移行性）の考え方の素案です。

大項目	中項目	小項目	小項目説明	メトリクス	【ご参考】 トレサビシステム	CMP案	
						アプリ	基盤
移行性	移行時期	移行のスケジュール	移行作業計画から本稼働までのシステム移行期間、システム停止可能日時、並行稼働の有無。（例外発生時の切り戻し時間や事前バックアップの時間等も含むこと。）	システム停止可能日時 0:制約無し（必要な期間の停止が可能） 1:5日以上 2:5日未満 3:1日（計画停止日を利用） 4:利用の少ない時間帯（夜間など） 5:移行のためのシステム停止不可	新規システムであるため移行は無し（対象外）	【推奨】 4:利用の少ない時間帯（夜間など） <small>※非機能要求グレードの社会的影響が限定されるシステムの値を設定した</small>	新規システムであるため移行は無し（対象外）
				並行稼働の有無 0:無し 1:有り		新規システムであるため移行は無し（対象外）	

【ご参考】重要度低要件の確認

IPAの非機能要求グレード2018に基づいた、重要度低要件（移行性）の考え方の素案です。

大項目	中項目	小項目	小項目説明	メトリクス	【ご参考】 トレサビシステム	CMP案	
						アプリ	基盤
移行性	移行方式	システム展開方式	システムの移行および新規展開時に多段階による展開方式をどの程度採用するかの程度。	拠点展開ステップ数 0:単一拠点のため規定無し 1:一斉展開 2:5段階未満 3:10段階未満 4:20段階未満 5:20段階以上	新規システムであるため移行は無し (対象外)	【推奨】 1:一斉展開 <small>※非機能要求グレードの社会的影響が限定されるシステムの値を設定した</small>	新規システムであるため移行は無し (対象外)
				業務展開ステップ数 0:単一業務のため規定無し 1:全業務一斉切り替え 2:4段階未満 3:6段階未満 4:10段階未満 5:10段階以上			

【ご参考】重要度低要件の確認

IPAの非機能要求グレード2018に基づいた、重要度低要件（移行性）の考え方の素案です。

大項目	中項目	小項目	小項目説明	メトリクス	【ご参考】 トレサビシステム	CMP案	
						アプリ	基盤
移行性	移行対象（機器）	移行設備	移行前のシステムで使用していた設備において、新システムで新たな設備に入れ替え対象となる移行対象設備の内容。	設備・機器の移行内容 0:移行対象無し 1:移行対象設備・機器のハードウェアを入れ替える 2:移行対象設備・機器のハードウェア、OS、ミドルウェアを入れ替える 3:移行対象設備・機器のシステム全部を入れ替える 4:移行対象設備・機器のシステム全部を入れ替えて、さらに統合化する	新規システムであるため移行は無し（対象外）	【推奨】 3:移行対象設備・機器のシステム全部を入れ替える <small>※非機能要求グレードの社会的影響が限定されるシステムの値を設定した</small>	新規システムであるため移行は無し（対象外）

【ご参考】重要度低要件の確認

IPAの非機能要求グレード2018に基づいた、重要度低要件（移行性）の考え方の素案です。

大項目	中項目	小項目	小項目説明	メトリクス	【ご参考】 トレサビシステム	CMP案	
						アプリ	基盤
移行性	移行対象 (データ)	移行 データ量	旧システム上で移行の必要がある 業務データの量（プログラムを含む）。	移行データ量 0:移行対象無し 1:1TB未満 2:1PB未満 3:1PB以上	新規システムであるため 移行は無し (対象外)	【推奨】 2:1PB未満 <small>※非機能要求グレードの社会的影響が限定されるシステムの値を設定した</small>	新規システムであるため 移行は無し (対象外)
				移行データ形式 0:移行対象無し 1:移行先と形式が同一 2:移行先と形式が異なる	新規システムであるため 移行は無し (対象外)	【推奨】 2:移行先と形式が異なる <small>※非機能要求グレードの社会的影響が限定されるシステムの値を設定した</small>	新規システムであるため 移行は無し (対象外)

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。



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律経済戦略」において、資源循環に必要な製品・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。

製造業3類型で市場規模が一番大きい加工組立型産業をモデルケースとする。		ニーズ特性				
		動脈産業		静脈産業		
		・商品設計・コスト低減に関わる情報ニーズ高		・ビジネスに関わる情報ニーズ高		
情報特性	動脈産業	情報保有	マテリアル製造	製品製造	小売リコマース	リサイクルリソーシング
		マテリアル製造		<ul style="list-style-type: none"> 素材のCO2原単位 リサイクル材の利用率 	<ul style="list-style-type: none"> 修繕や適正処分のための原材料情報 	<ul style="list-style-type: none"> リサイクルの品質を左右する成分情報（忌避物質、添加剤等）
	製品製造	<ul style="list-style-type: none"> 素材性能の最低要求水準（オーバースペック回避） 		<ul style="list-style-type: none"> 製品のCFP・MFP 製品性能・仕様 修理可能性・方法 	<ul style="list-style-type: none"> 主な循環資源の所在（部品等） 容易な解体方法 部品の性能 	
	小売リコマース	<ul style="list-style-type: none"> 循環資源の流通・リーク実態把握 	<ul style="list-style-type: none"> 流通履歴 修理・変更履歴 部品の流通履歴 		<ul style="list-style-type: none"> 循環資源の流通・リーク実態把握 	
	リサイクルリソーシング	<ul style="list-style-type: none"> 再生材の品質 再生材のCFP 	<ul style="list-style-type: none"> 再生材のCO2原単位 再生材の品質 	<ul style="list-style-type: none"> 適切なリサイクルのための分別方法 		
静脈産業	<ul style="list-style-type: none"> 型式、仕様、設計値等の静的情報を中心に保有 量産情報が主で、情報更新頻度低 静脈と比べて情報量が多いが、情報所有者はある程度固定 					
	<ul style="list-style-type: none"> 流通時、流通後の動的情報を中心に保有 所有者移転、用途変更が多く、情報更新頻度高 情報量は動脈に比べて多くないが、他の情報との連結や情報の切離しが発生 					

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

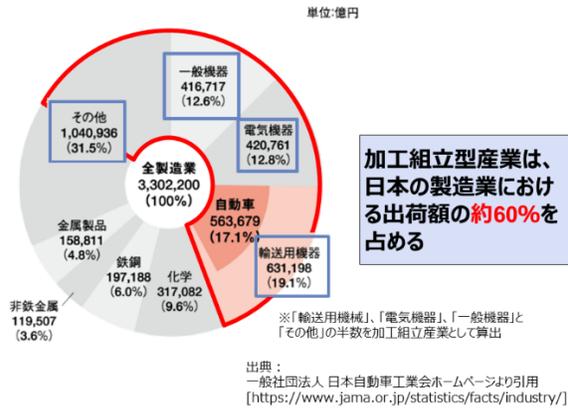
日本の製造業における加工組立型産業は、三大類型の中で出荷額の60%を占めているため、他の類型や産業のベースとして考えられる。他産業への展開も見据えられるため、今回は加工組立型産業をモデル化の対象として選定する。また、基礎素材型産業からの材料供給も行われるため、製造業全体のカバー範囲は広いと想定している。

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

2021年の主要製造業の製造品出荷額等



検討フロー

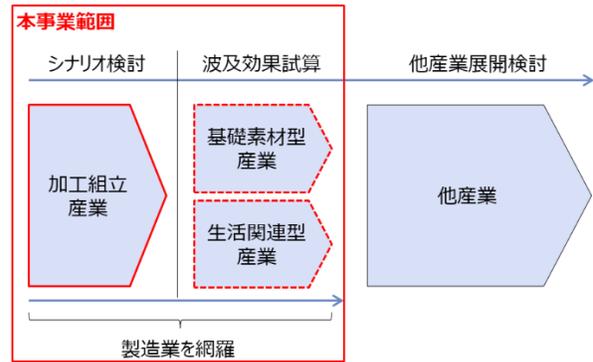


図 1-3

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。

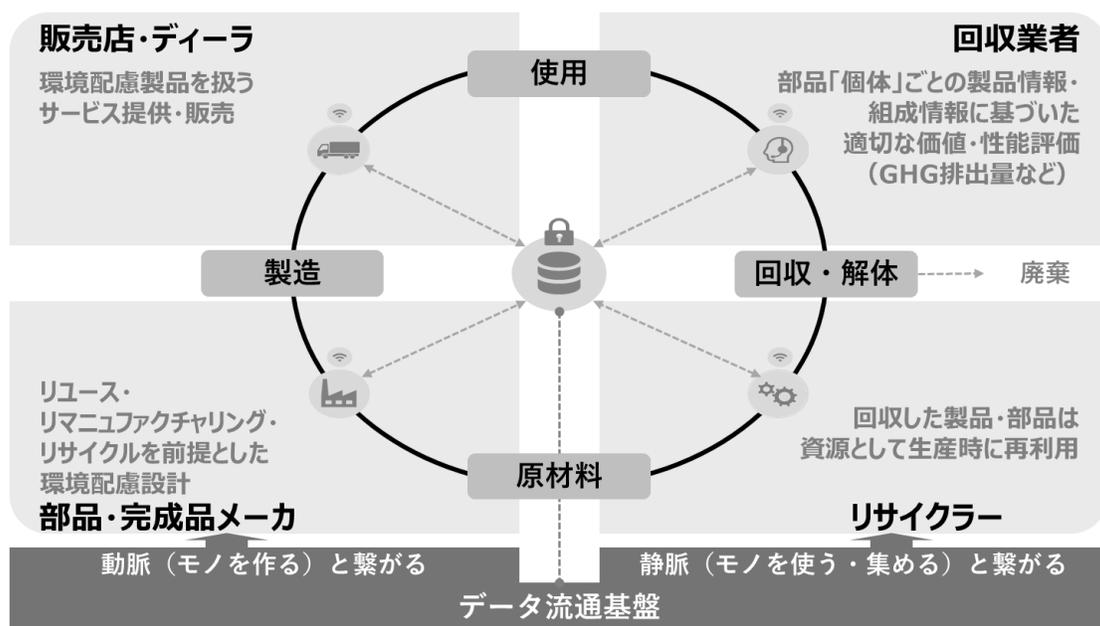


図 1-4

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

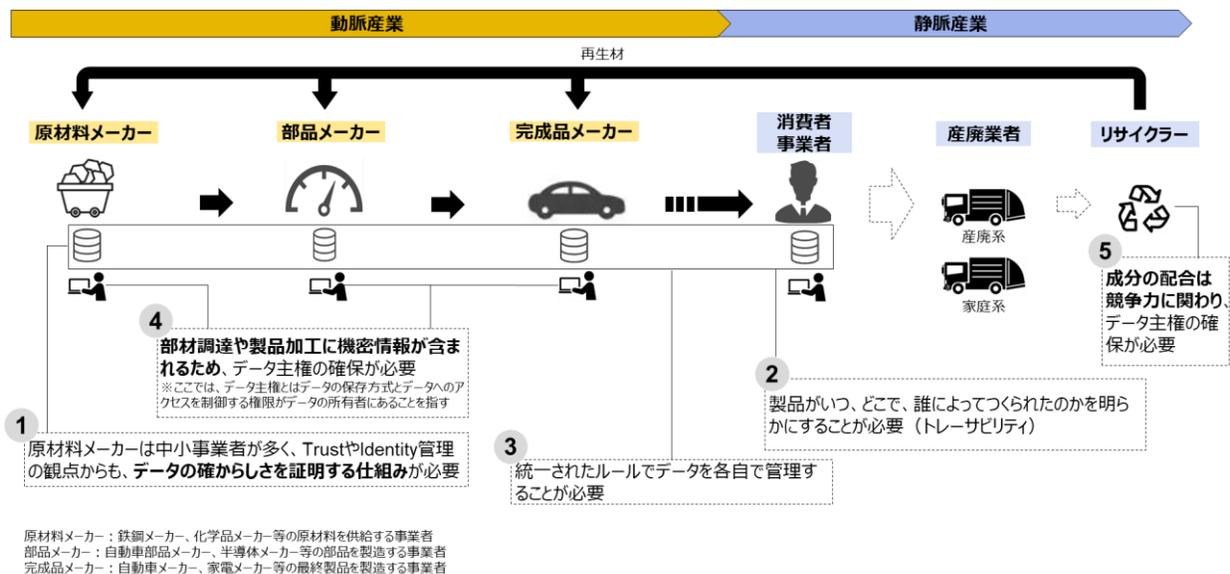


図 1-5

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／材料を組み合わせることで最終完成品を製造するため、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。

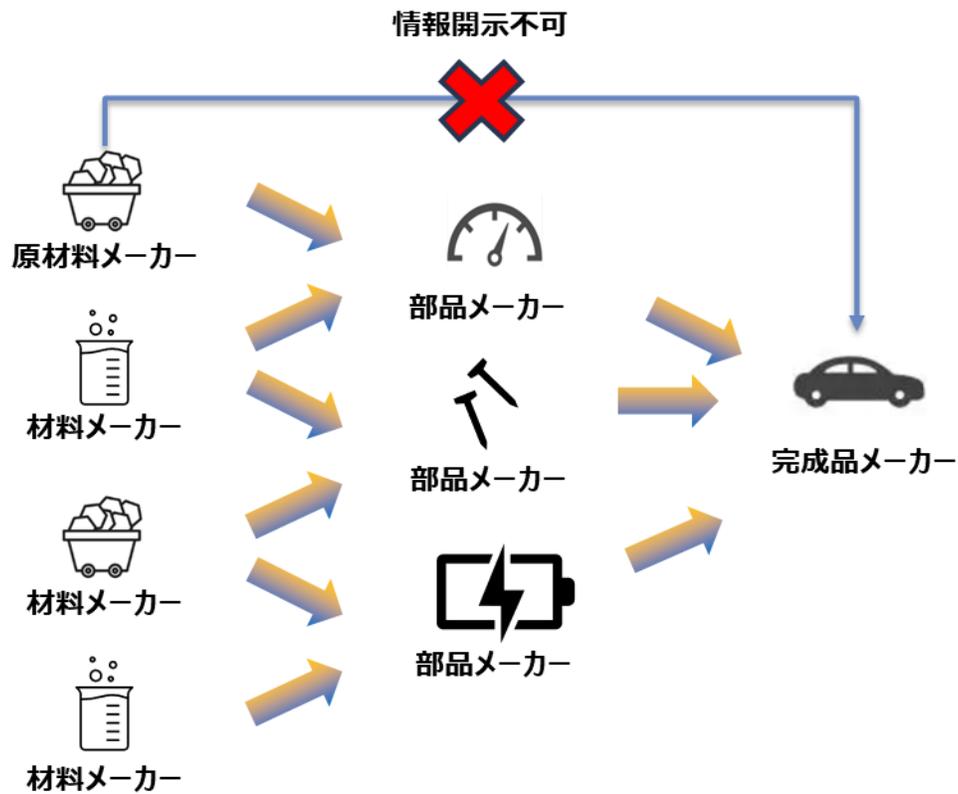


図 1-7

- 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」→「リサイクラー」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。

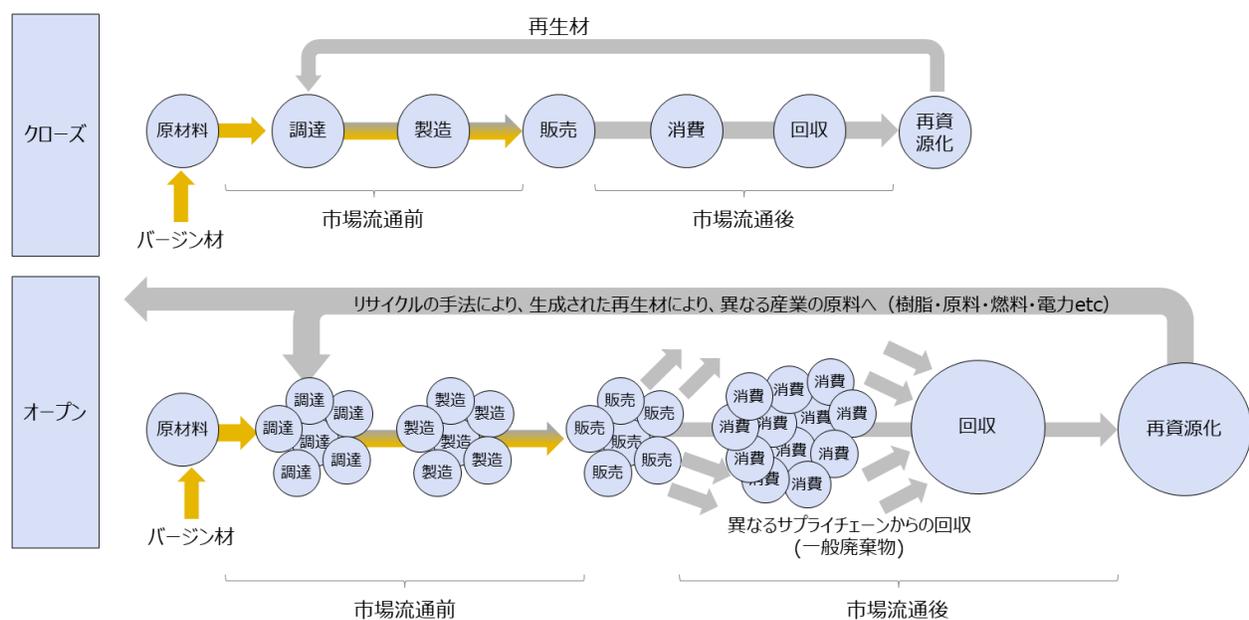


図 1-9

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、リサイクラー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、リサイクラー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。

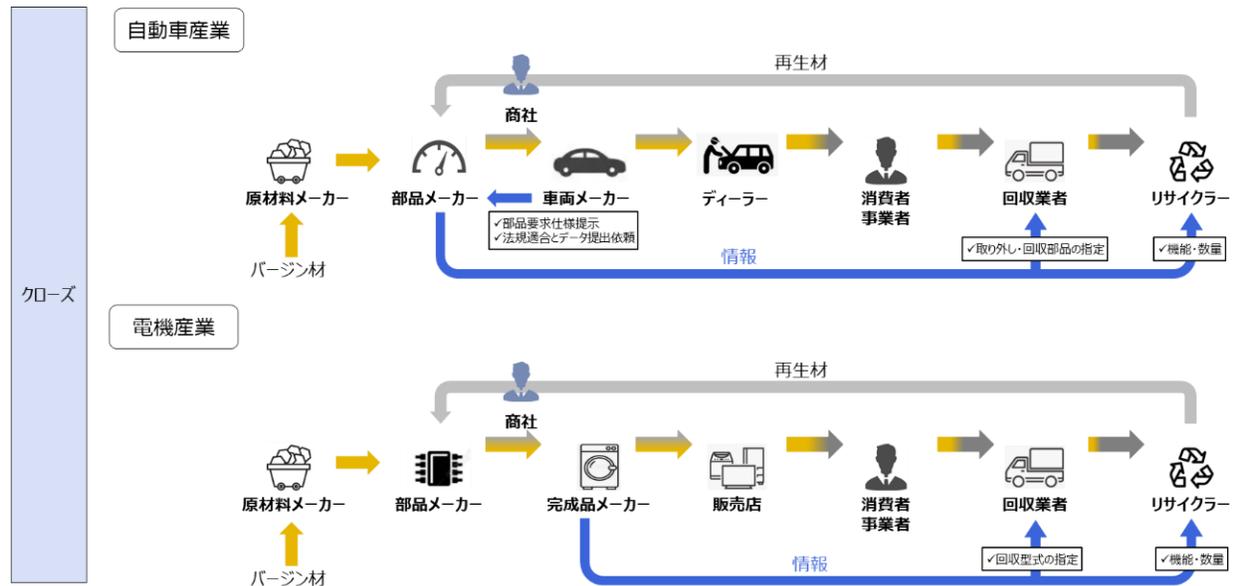


図 1-10

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へ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。

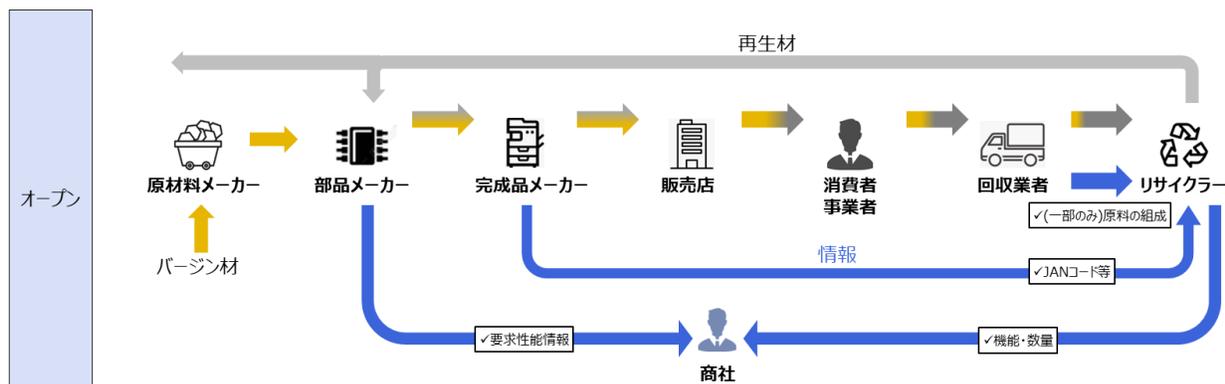


図 1-11

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とって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する。

1.7.1 規制・標準化類

これまで、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ーは、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	$(1 - R_1)E_V + R_1 \times (A \times E_{recycled} + (1 - A)E_V \times \frac{Q_{Sin}}{Q_P}) + (1 - A)R_2 \times (E_{recyclingEoL} - E_V^* \times \frac{Q_{Sout}}{Q_P})$ <div style="display: flex; justify-content: space-between; margin-top: 10px;"> <div style="border-top: 1px dashed green; width: 30%; padding-top: 5px;"> <p style="color: green; font-weight: bold;">バージン資源 の投入による 排出</p> </div> <div style="border-top: 1px dashed blue; width: 30%; padding-top: 5px;"> <p style="color: blue; font-weight: bold;">リサイクル材の投入による排出</p> </div> <div style="border-top: 1px dashed red; width: 30%; padding-top: 5px;"> <p style="color: red; font-weight: bold;">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</p> </div> </div>

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。
Q _P		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}		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 _{SE,elec}		
E _D		
X _{ER,heat}		エネルギー回収プロセスの効率(熱、電力)。
X _{ER,elec}		
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（CIF¹）＋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

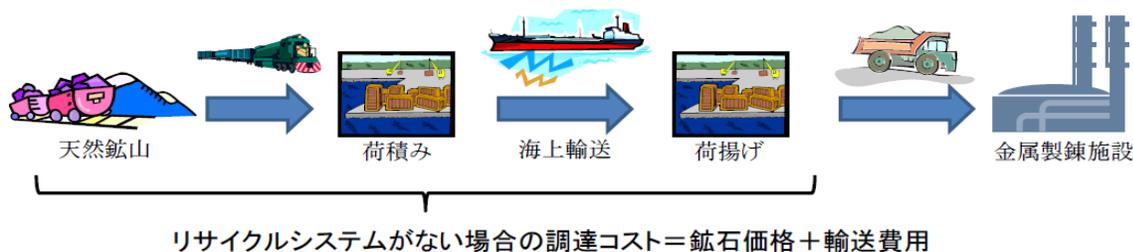


図 1-13

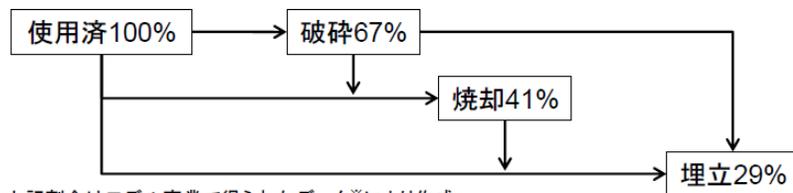
¹ CIF：輸出業者が貨物を荷揚げ地の港（輸入港）で荷揚げするまでの費用（輸出梱包費、輸出通関費、運賃、船荷保険料等）を負担し、荷揚げ以降の費用は輸入業者が負担するという取引条件。



図 1-14

(参考) 最終処分コスト

$$\text{最終処分コスト削減便益} = \text{埋立処分コスト等削減便益} + \text{薬剤処理コスト削減便益}$$



上記割合はモデル事業で得られたデータ※により作成
 ※ 平成21年度使用済小型家電からのレアメタルの回収及び適正処理に関する研究会とりまとめP.3-17

破碎処理コスト削減 = 破碎処理量 (67%) × 破碎処理単価36円/kg 焼却処理コスト削減 = 焼却処理量 (41%) × 焼却処理単価23円/kg 埋立処分コスト削減 = 埋立処分量 (29%) × 埋立処分単価22円/kg	}	合計が埋立処分コスト等削減便益
※処理・処分単価は処理・処分単価を公表しているモデル事業実施自治体の平均値を採用		8.4億円
		※20品目、回収率30%の場合

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、特に鉍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靱化実証事業（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靱化支援事業（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・強靱化を実現するため、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、大型铸造品は、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。

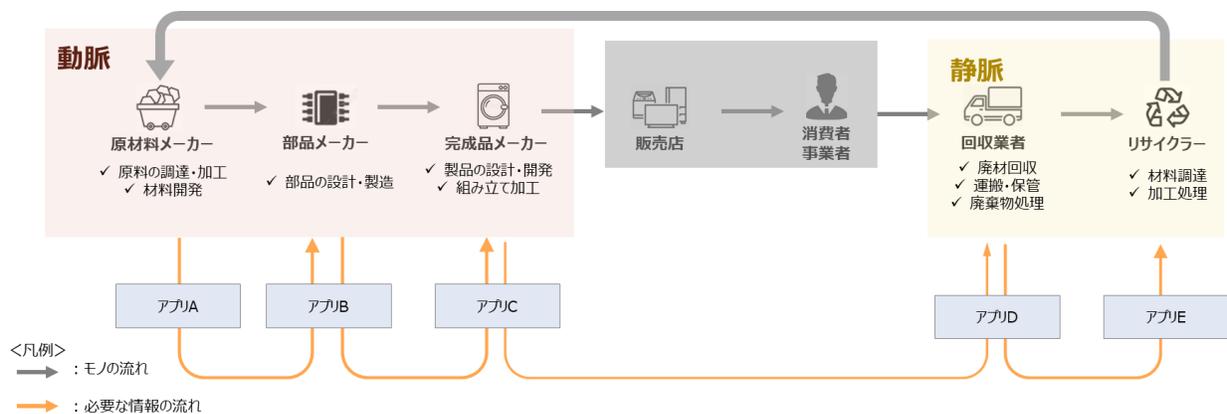


図 1-16

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	動静脈産業には様々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	<ul style="list-style-type: none"> ・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
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、再利用時にも活用できる状態とする	<ul style="list-style-type: none"> ・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
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	<ul style="list-style-type: none"> ・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

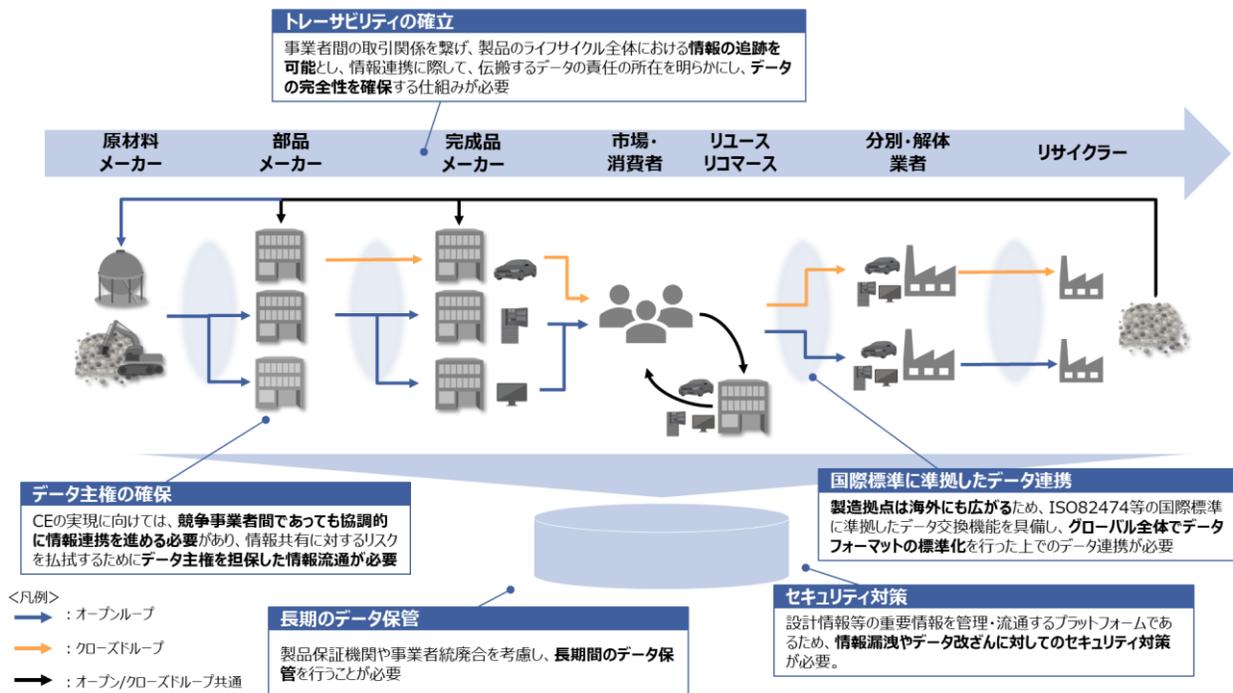


図 1-17

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證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 のような用途がある。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。

B. 産業競争力の強化に向けたユースケースと経済的インパクト
B1. ブロックチェーンの特性と用途 及び その期待効果

B1

ブロックチェーンには、その特性を活かした、7つの主要な用途がある

ブロックチェーンの特性

- システムの耐障害性が高い
- 記録の透明性・信頼性が高い (改ざん耐性が高い)
- トランザクションのコスト・時間が節約できる
- システムの持続性が高い

ブロックチェーンの主要な用途 (出来ること)

誰でも参加しやすく安定・持続性があり低コストな決済

- 例) 価格が安定的な暗号資産(ステーブルコイン)による低手数料の決済

企業横断で利用可能な低コストで信頼性が高い本人確認 (eKYC)

- 例) 複数の金融機関による顧客の本人情報確認 (反社チェックなどのeKYC) 情報の安全な共有

国・地域を問わず真正性の担保が可能な書類の電子化

- 例) 原本性が必要な貿易書類の電子化

透明・安定・低コストで簡単なデジタル/リアル資産の取引

- 例) デジタルアートの保有を証明しての取引
- 例) 不動産の証券化商品の簡易で低コストな取引

透明・安定・低コストなライセンス等の権利の取引

- 例) コンテンツの知的財産権の証明と少ない手間でのライセンスの付与

改ざんによる不正を防ぎ信頼性・真正性が高い記録

- 例) 治験データの転記ミスやデータ改ざんの防止
- 例) 工場や建設現場の検査データの転記ミスや改ざんの防止

透明で信頼性の高いトレーサビリティの確保・証明

- 例) 食品の産地等のサプライチェーン横断での改ざん不可能な記録
- 例) 電池やプラスチックなどの素材のリサイクルの改ざん不可能な記録 等

Copyright © 2024 by Boston Consulting Group. All rights reserved.

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。

B. 産業競争力の強化に向けたユースケースと経済的インパクト
B1. ブロックチェーンの特性と用途 及び その期待効果

B1

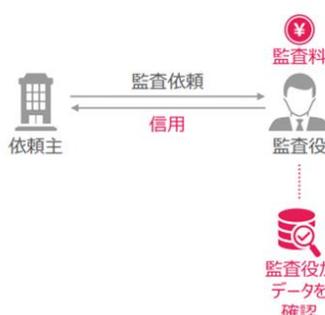
ネットワーク上の全参加者によって検証され、不変の公開台帳にデータが保存されことにより、データの改ざんなど不正に対する手動での確認が不要になる

改ざんによる不正を防ぎ信頼性・真正性が高い記録

従来とブロックチェーン活用時の違い

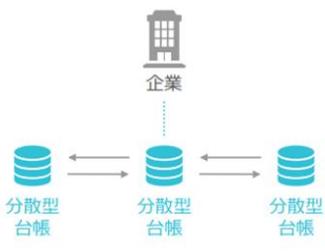
中央集権型システム (従来型)

監査役が、登録データの不正・改ざんがないか確認し、信頼性・安全性を担保



分散型システム (ブロックチェーン技術活用)

分散型で記録されたデータ・プログラムがデータの不变性を担保



ポイント

享受できるメリット

- なぜ信頼性があるのか?
 - 企業、仲介者 (中央管理者) が存在せず、その1点がシステムの急所になることがないため
- なぜ真正性が高いのか?
 - ネットワーク上の全参加者によってトランザクションが検証され、承認されたあとに不変の分散型台帳に記録されるため

制約・リスク

- 分散合意メカニズムには、51%攻撃などの脆弱性がある
- また前提となるブロックチェーン自体のスマートコントラクトや、データの信頼性の確認は必要になる

Copyright © 2024 by Boston Consulting Group. All rights reserved.

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。

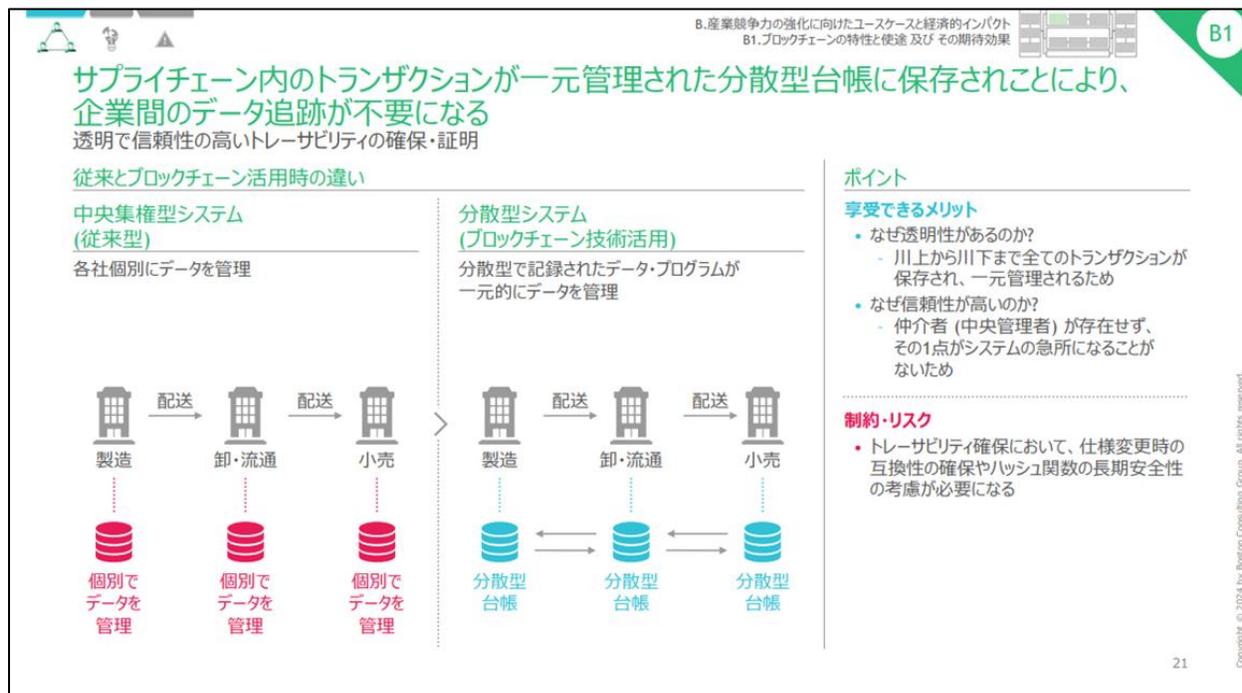


図 2-3

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。

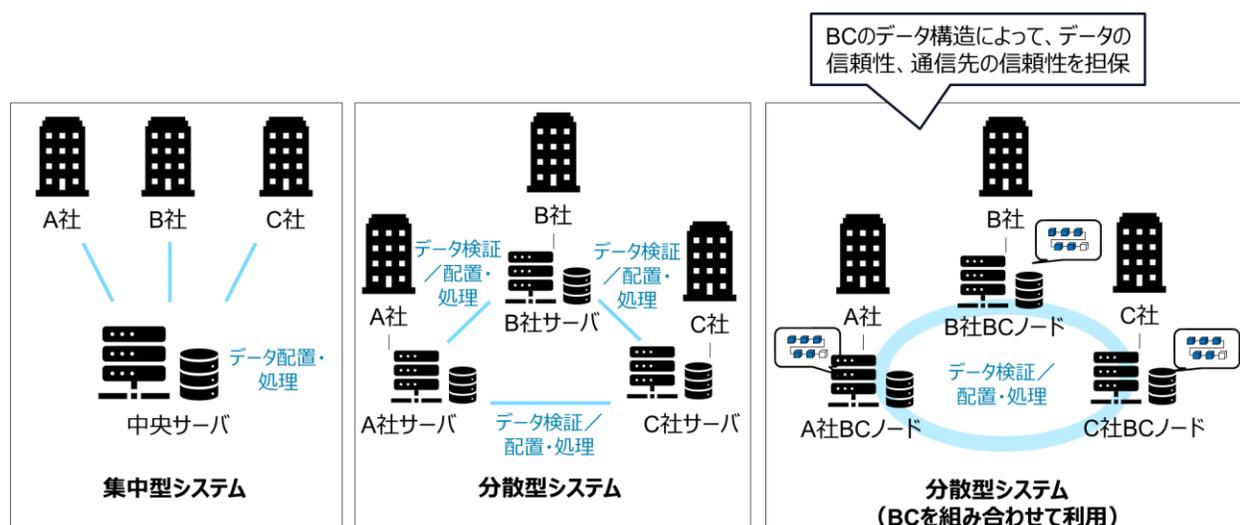


図 2-4

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。

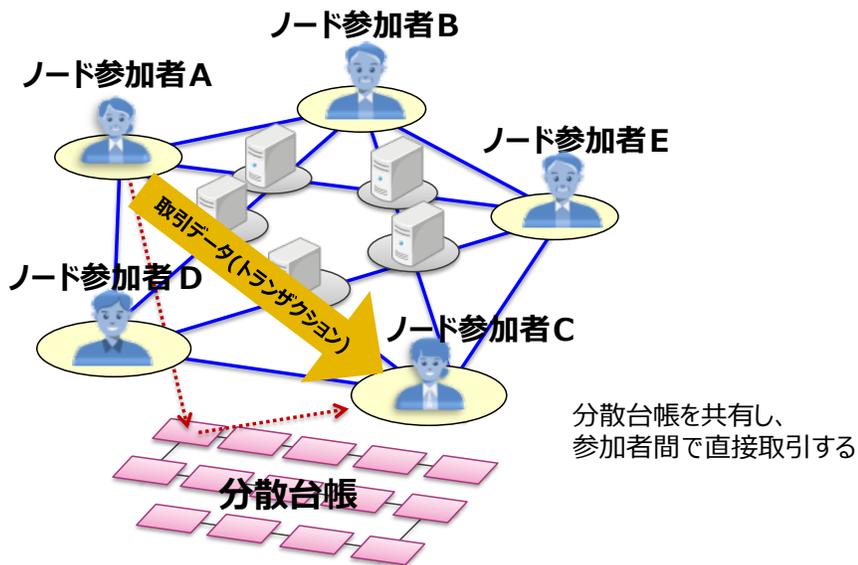


図 2-5

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 BC⁴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 BC⁴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

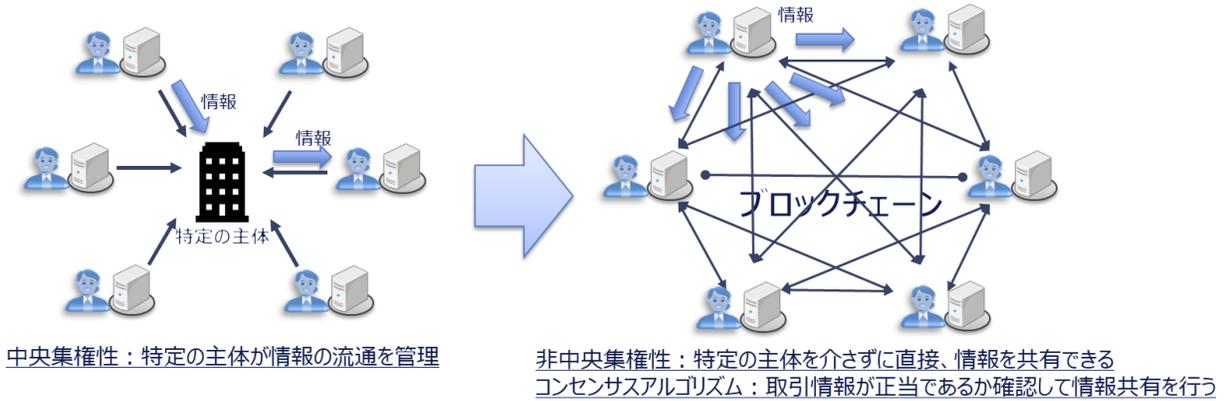
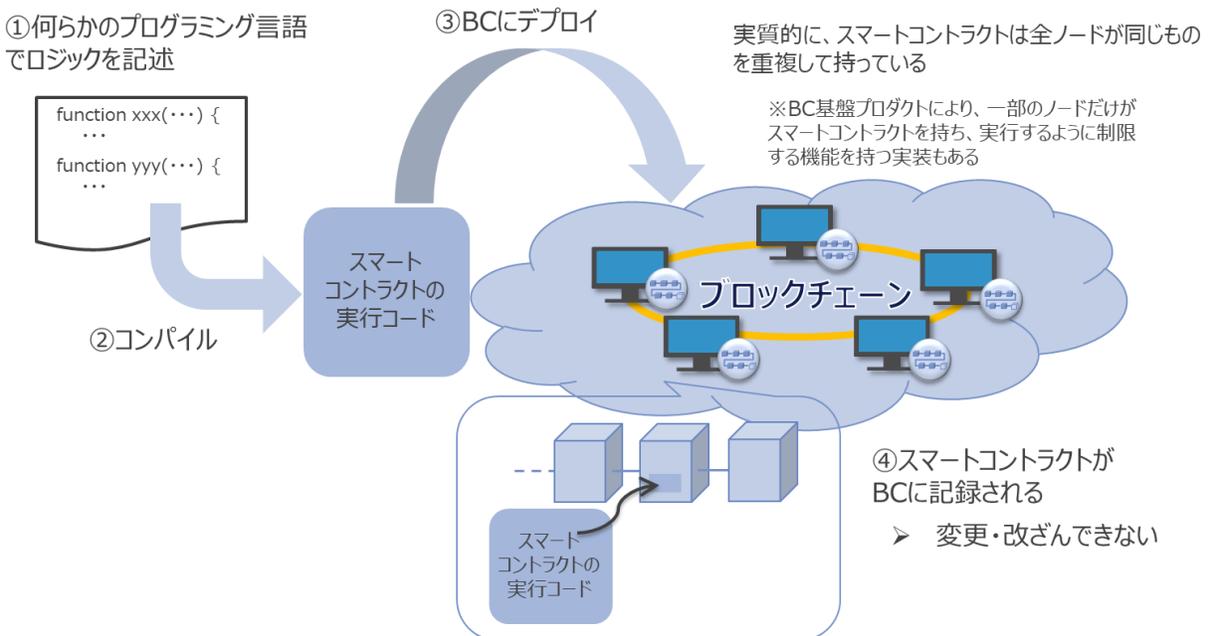


図 2-6

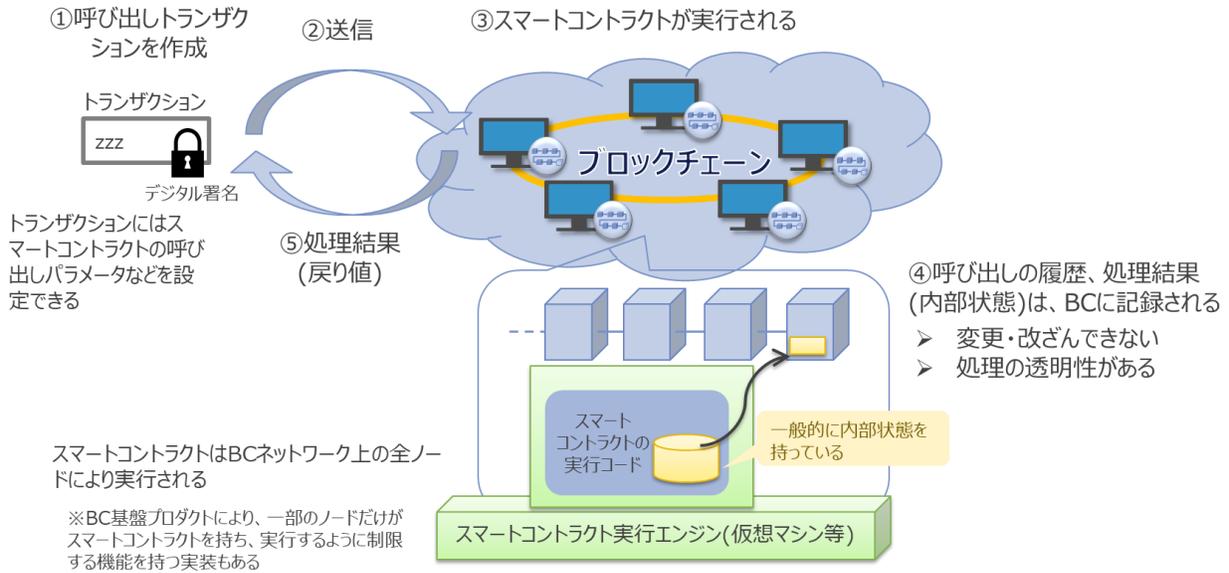
2.3.3 スマートコントラクト（自動執行）

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

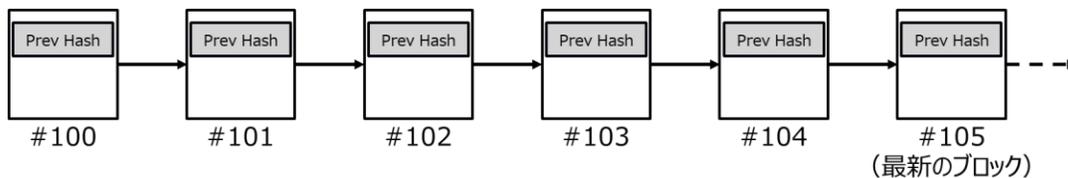


スマートコントラクトの実行の例：呼び出しの履歴・処理結果がBC上で共有されるので透明性がある

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。



※Prev Hash=前のブロックとハッシュ値

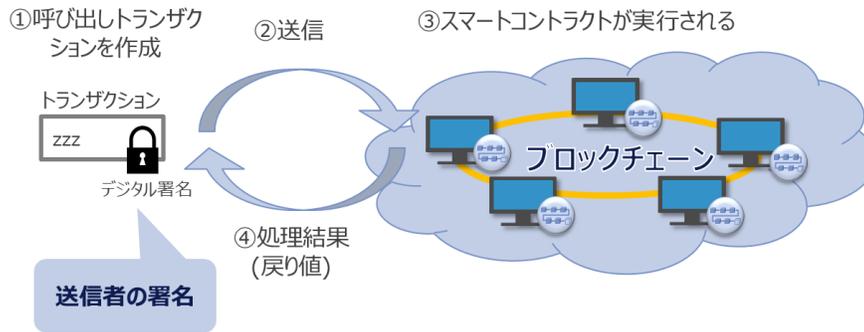
図 2-9

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。

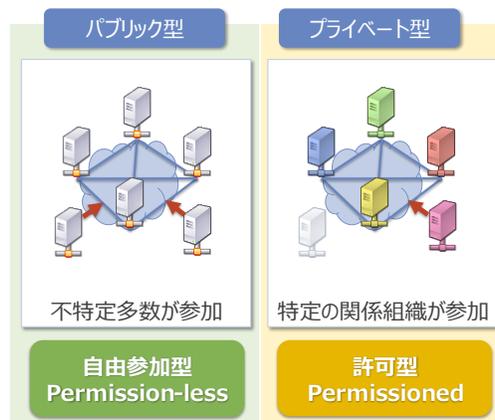


図 2-11

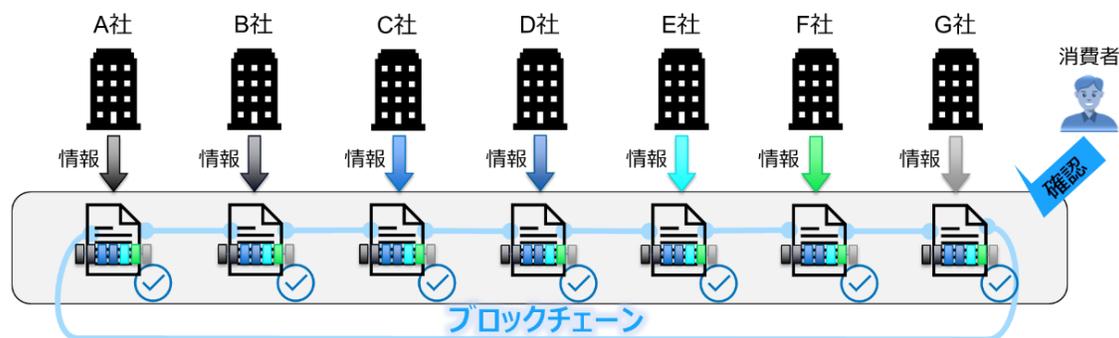
2.4 機能面における利点と課題

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

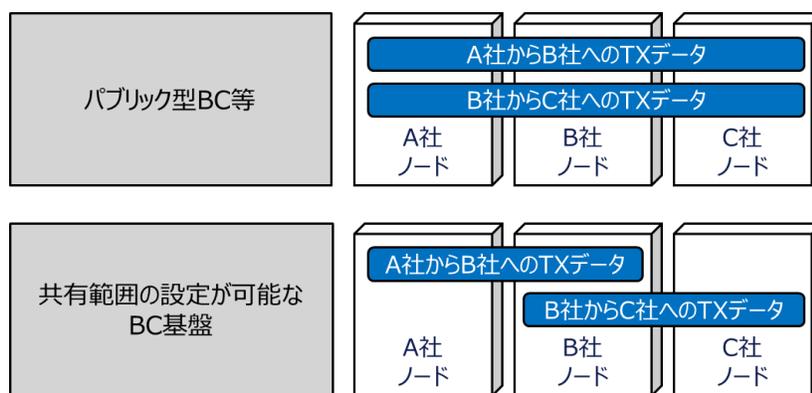
「2.3.3 スマートコントラクト（自動執行）」の技術特性により、BC 上では処理ロジックを自動執行させることができる。これにより、業務自体の効率化に加え、BC の透明性の利点から、第三者による確認、監査といった業務の効率化を図れる。

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。



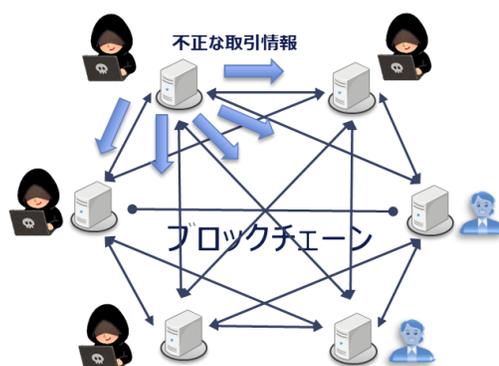
※TX=トランザクションの略

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。



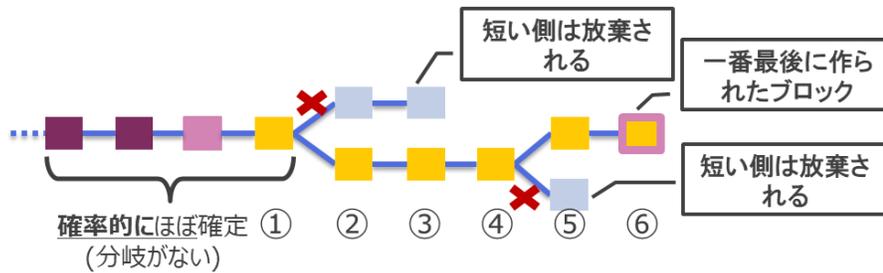
ネットワーク支配の例：悪意のある主体が十分な数のノードを乗っ取ると不正な取引が可能になる

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的な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、合意形成で一意的な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。

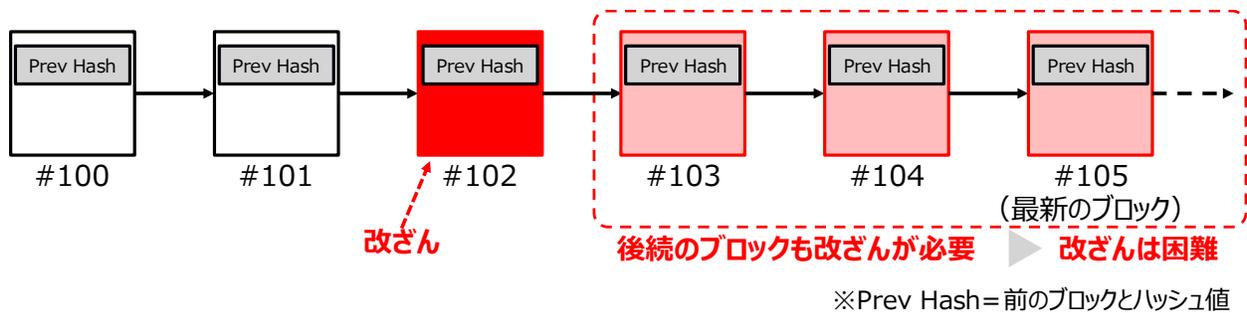


図 2-16

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。

トランザクション例：Aさんが持っている仮想通貨を10コインをBさんに送金

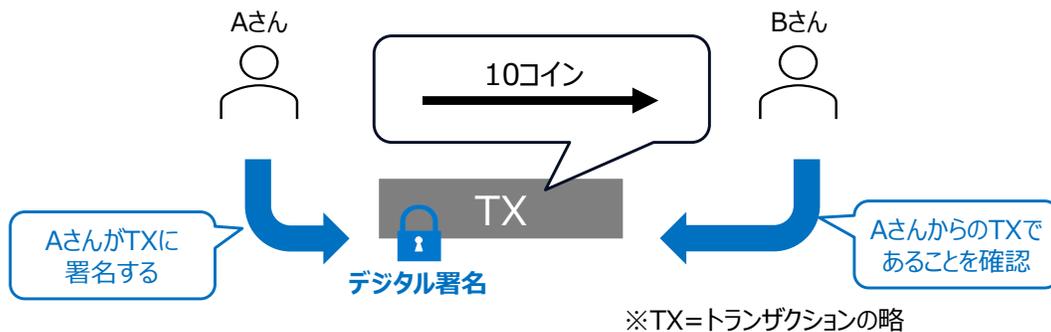


図 2-17

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。

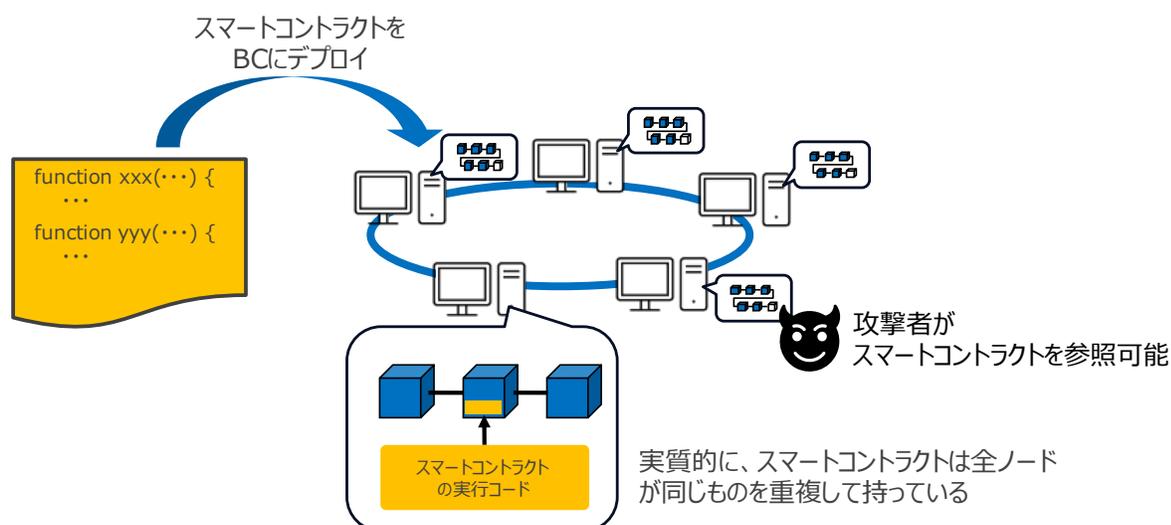


図 2-18

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、間違っただけの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に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あたりに 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ルリングおよびサイドチェーンスケール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継続される。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。

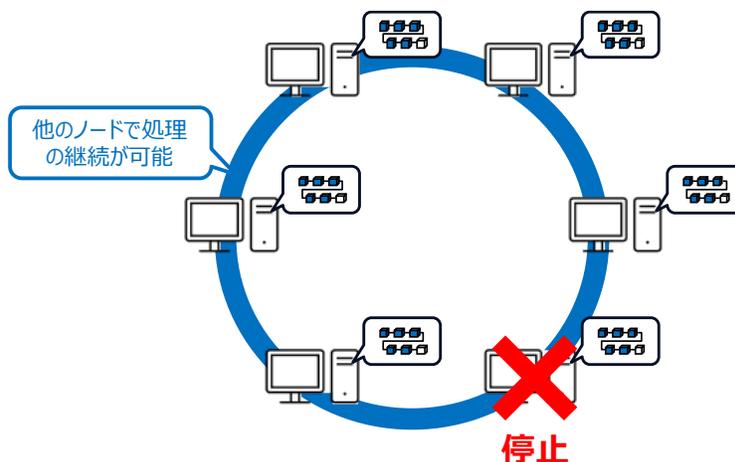


図 2-19

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。

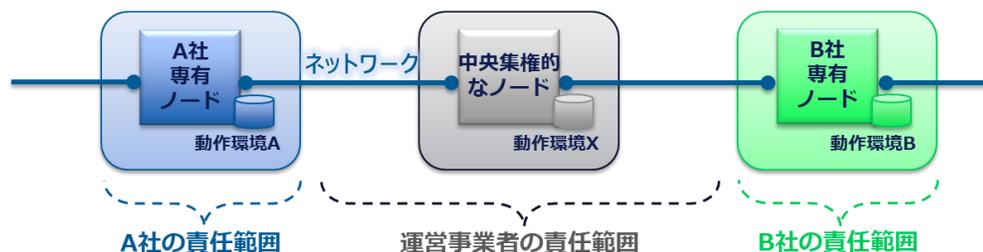
2.5.4.2 課題

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ふ可能性がある。

- 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ふ可能性がある。

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はある。

- 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、

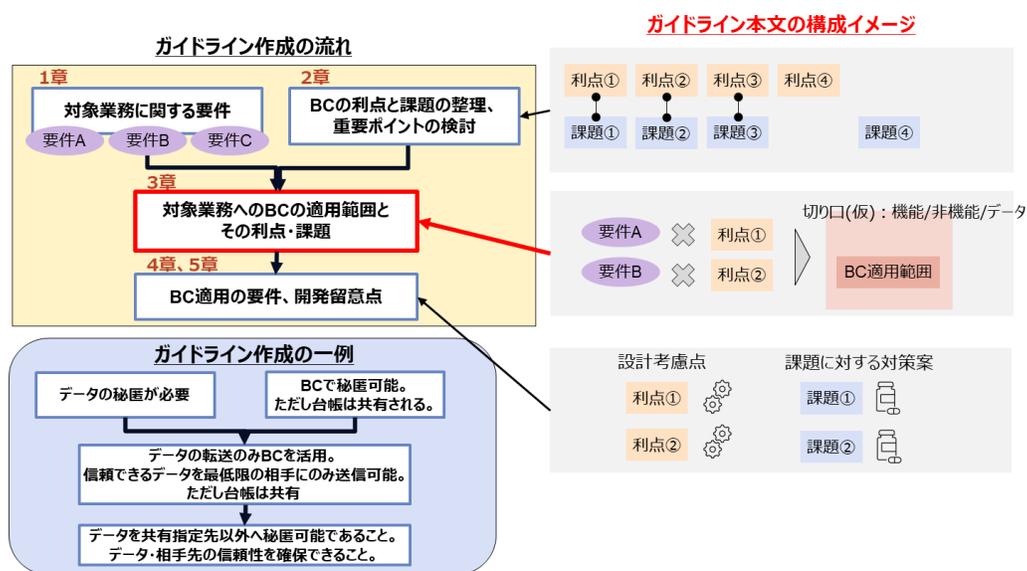


図 3-1

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・エコシステム」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。

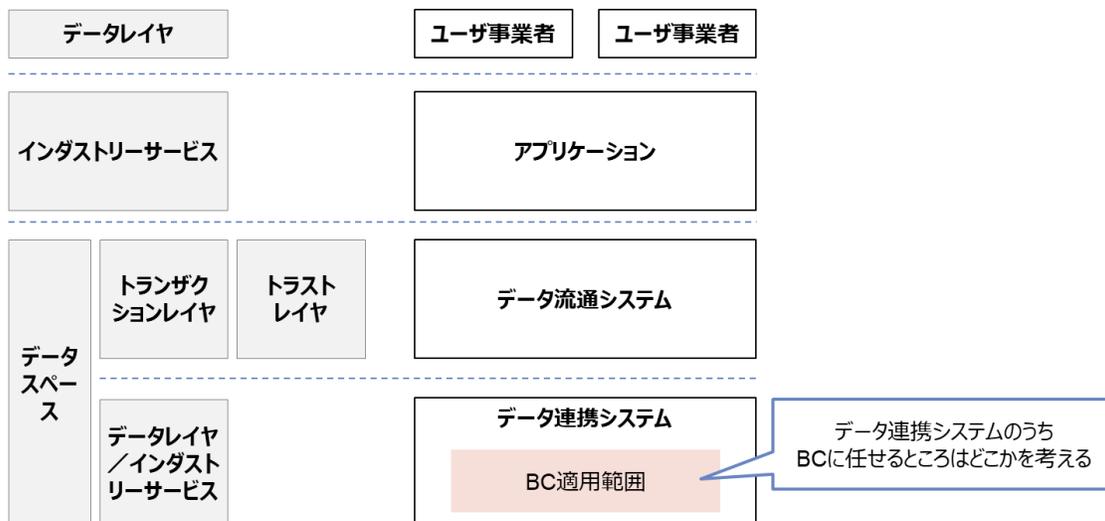


図 3-2

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。 篡改ざん性 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
 ・分散台帳という特性から「情報共有」の機能的利点が生じる
 ・一方、共有データの秘匿化という課題が同時に生じる

課題	機能的利点				非機能的利点				
	情報の共有 (透明性)	公平性 (分権)	不正防止 (二重支払い)	業務 効率性	セキュリティ	性能・拡張性	可用性	運用保守	移行性
分散台帳	✓ データ秘匿化	✓			・責任追跡性	・スループット ・レイテンシ	・継続性/耐障害性	・運用負荷軽減	
非中央集権性 (コンセンサスアルゴリズム)		✓ ネットワーク支配		整理イメージ(抜粋)				・責任分解 ・運用オペレーション煩雑	
スマートコントラクト (自動執行)			✓	✓					
データ構造 (ハッシュチェーン)			✓		・完全性 (耐改ざん性)				
デジタル署名 (トランザクション)		✓			・否認防止性 ・信頼性 秘密鍵流出				

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

2章：BCの利点と課題の整理										
	情報の共有 (透明性)	公平性 (分権)	効率性	不正防止 (二重支払い 防止)	セキュリティ				可用性 継続性/ 耐障害性	運用保守性 運用負荷 軽減
					完全性 (耐改ざん性)	責任追跡性	否認防止性	信頼性		
1章：業務観点のシステム要件	データ共有	✓								
	データの信頼性	✓			✓	✓	✓	✓		
	処理ロジックの透明性と確実性	✓		✓		✓	✓		✓	
	通信先の信頼性							✓	✓	
	データ主権		✓				✓	✓		
	システムの持続可能性		✓			✓	✓			✓
	大量データ処理性能の確保									
	拡張処理性能の確保									
	利点と対をなす課題	データ秘匿化	NW支配				秘密鍵流出			責任分解

赤字部分：BC活用の利点が得られる部分

利点が活かされない課題
 性能リスク
 性能リスク

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	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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（透視性）	<ul style="list-style-type: none"> 事業者間で組成データ等を共有する
4		公平性（分権）	<ul style="list-style-type: none"> 事業者間でBC書き込みデータを合意する
5		業務効率性	<ul style="list-style-type: none"> 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）	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 参加事業者追加などの非機能的な要件
9		可用性	<ul style="list-style-type: none"> 耐障害性などの非機能的な要件
10		運用保守	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 移行性に関する要件
12		データ	非共有データ
13	共有データ		<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 国内からCE情報流通PFへアクセスするユーザ
15		海外	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> データ連携システムの本番運用環境
21		開発環境	<ul style="list-style-type: none"> 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^o 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のあるものを対象「○」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。

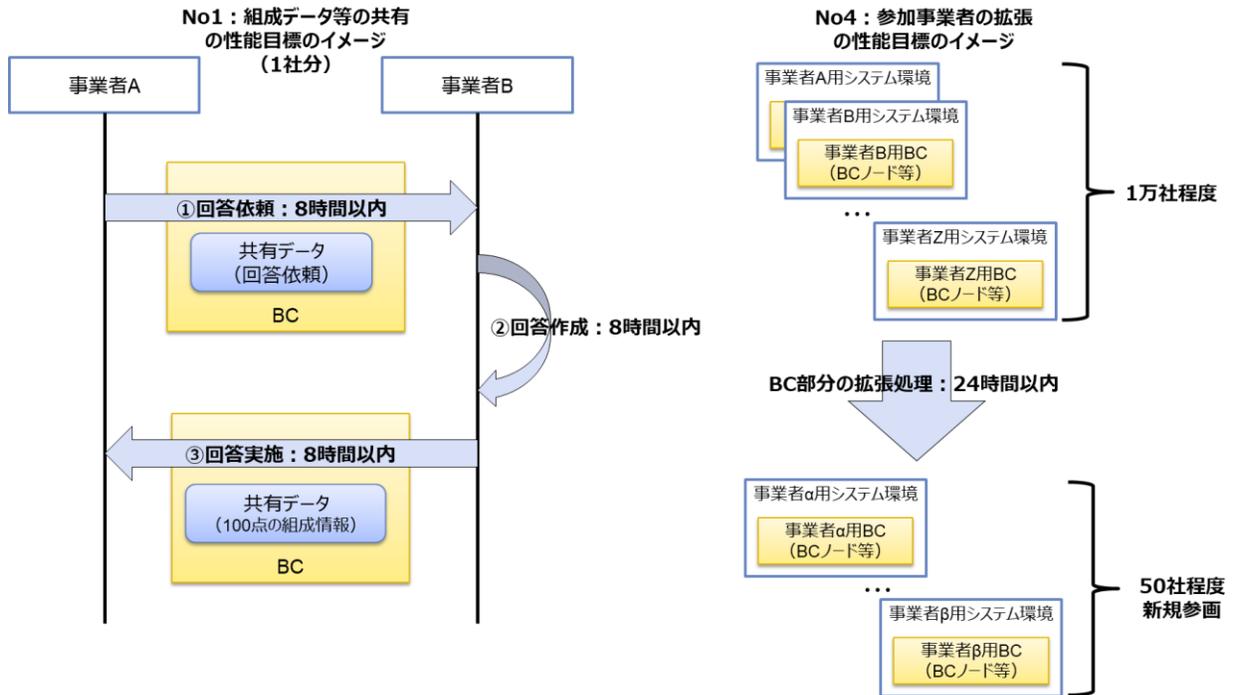


図 4-1

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。

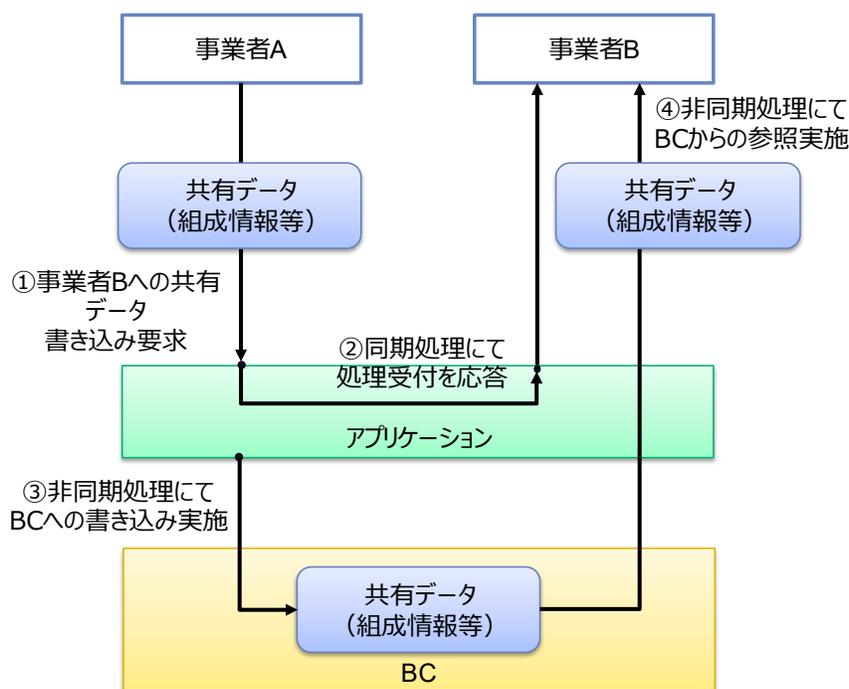


図 4-2

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りすぎ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逼迫のリスクがある。

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

<p>秘匿対象 (何を秘匿するか)</p>	<p>取引先としてどこが存在するのかわ、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。</p>
<p>共有範囲 (誰に共有/秘匿するか)</p>	<p>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。</p>
<p>秘匿期間 (いつまで秘匿するか)</p>	<p>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。</p>
<p>秘匿変更 (秘匿先の追加・削除)</p>	<p>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。</p>

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

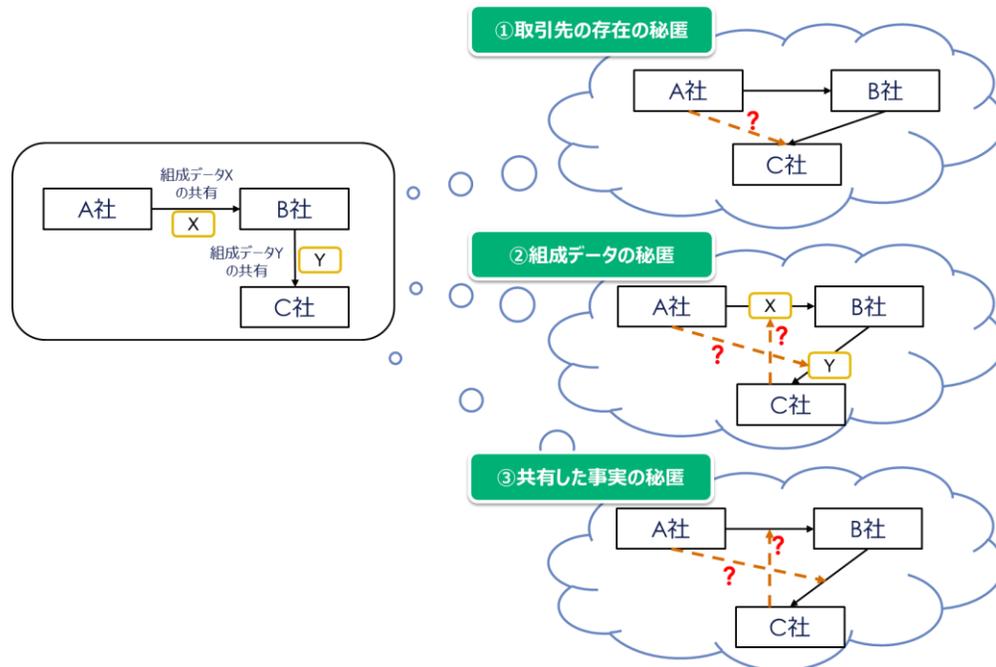


図 4-3

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。

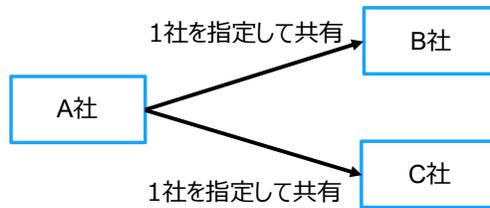


図 4-4

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。

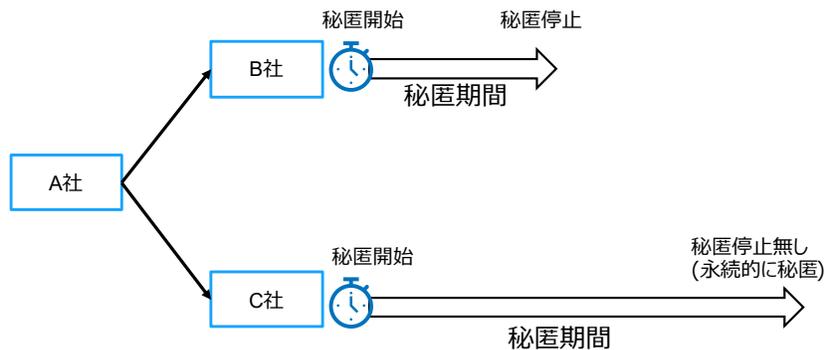


図 4-5

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

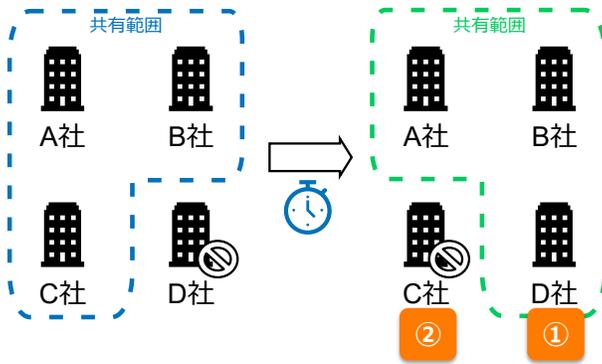


図 4-6

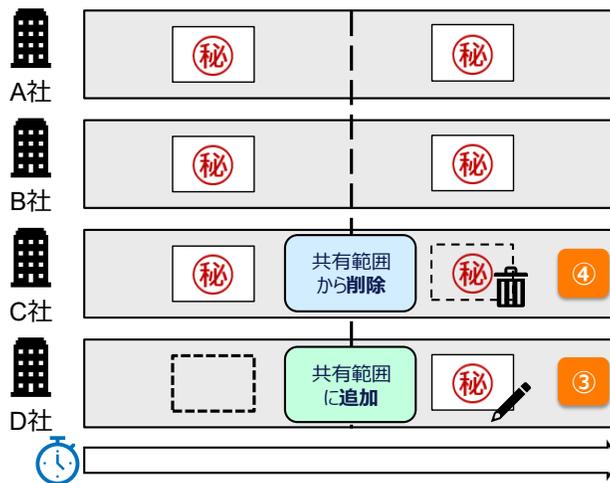


図 4-7

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。

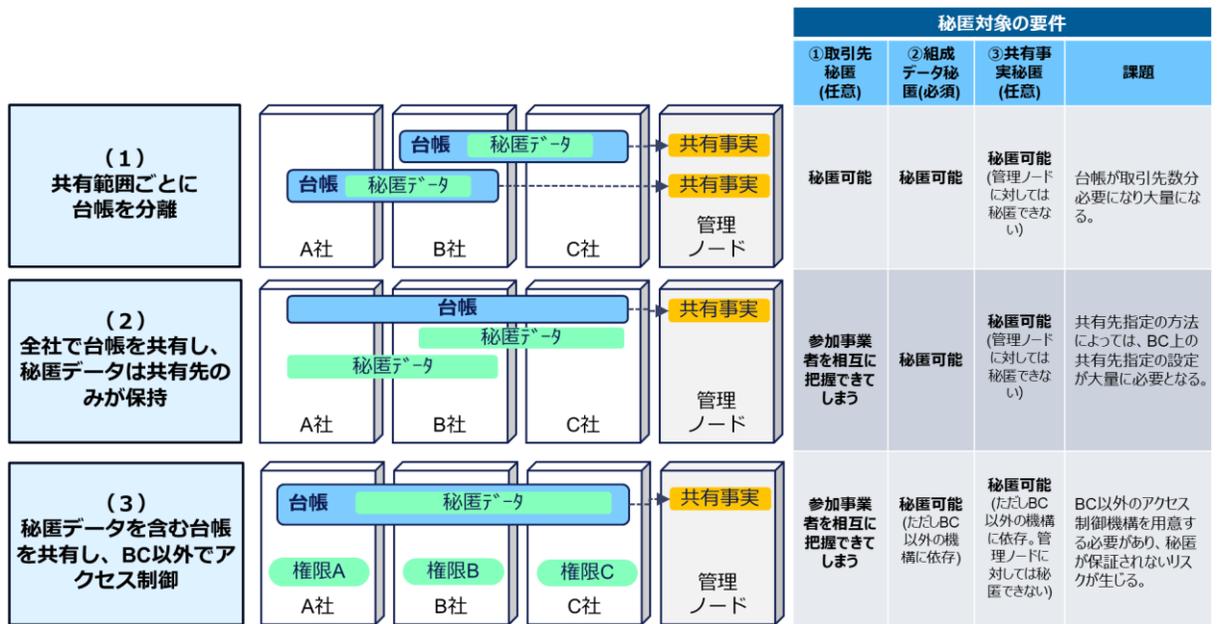


図 4-8

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が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

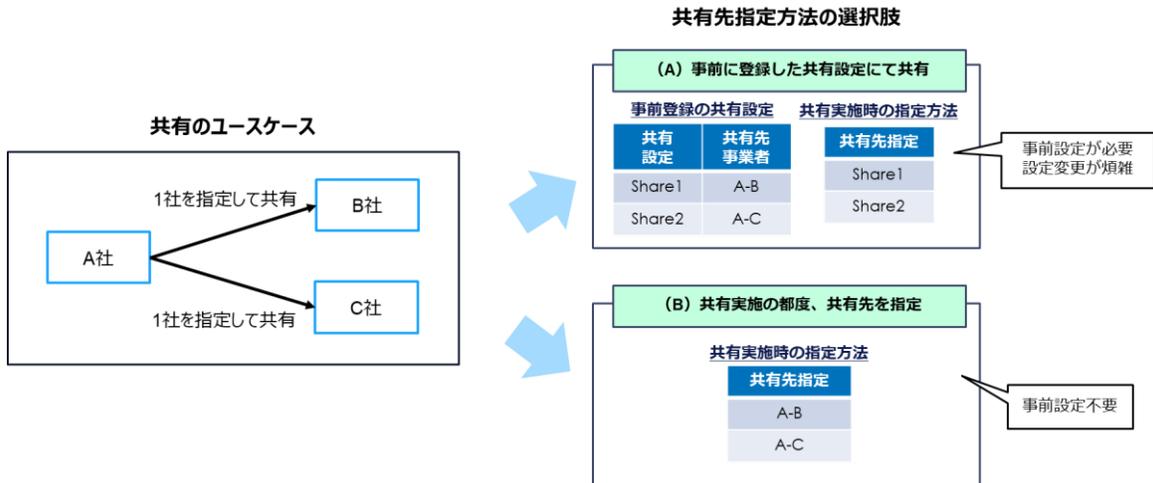


図 4-9

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。

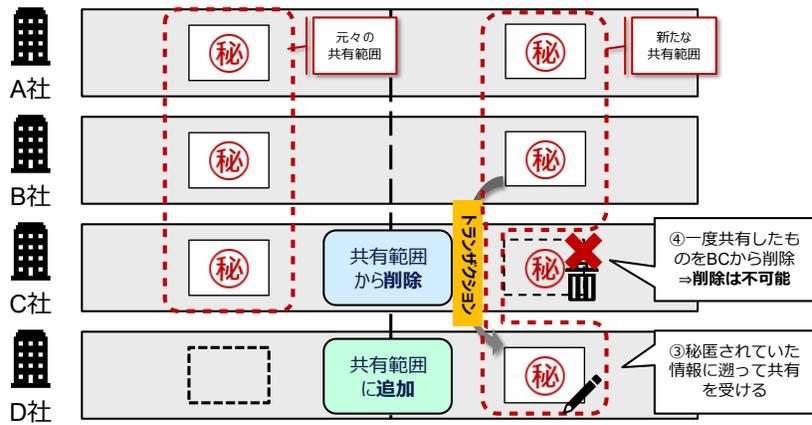
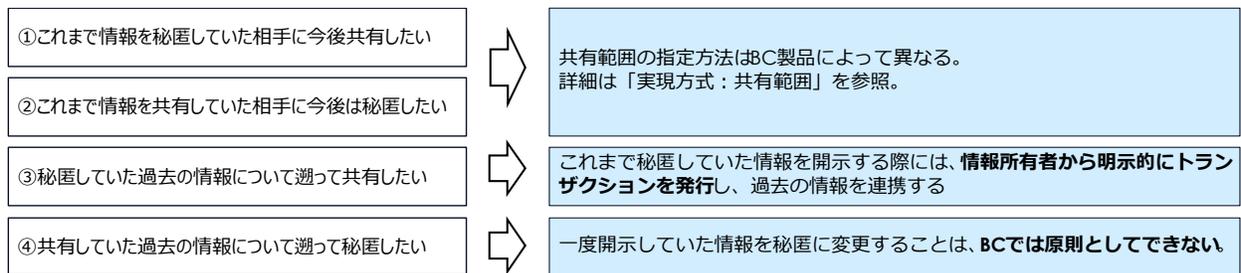


図 4-10

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。

<問題の状態>

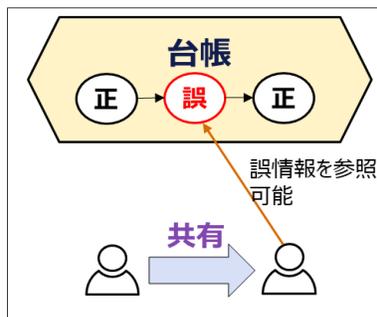
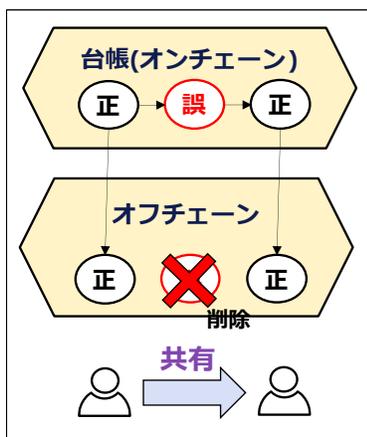
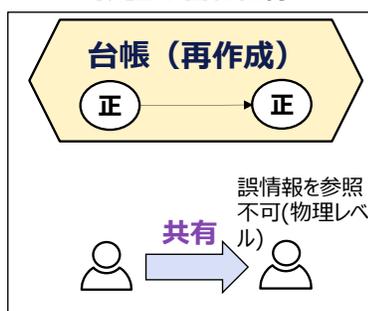


図 4-11

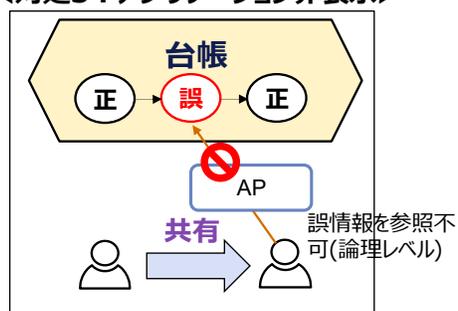
<対処1：オフチェーン・ハッシュ値の利用>



<対処2：台帳削除>



<対処3：アプリケーション非表示>



※AP=アプリケーションの略

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。

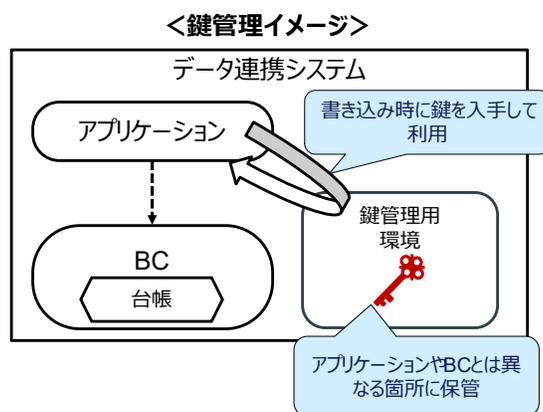


図 4-13

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。	—

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、意図的な入力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」を指すものではない点に注意する。

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。

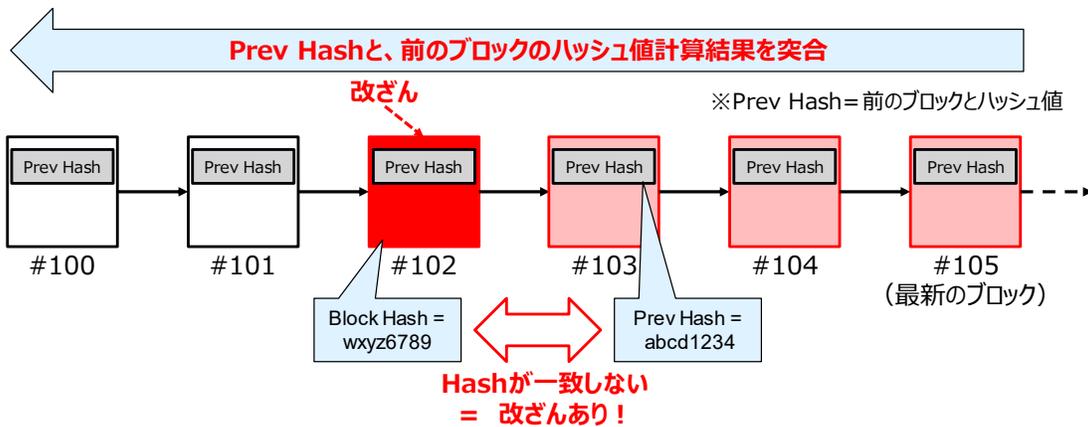


図 4-14

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の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。

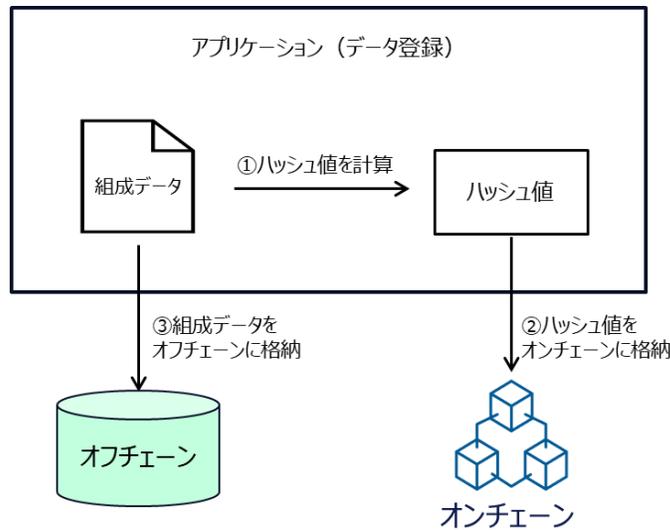


図 4-15

- 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。

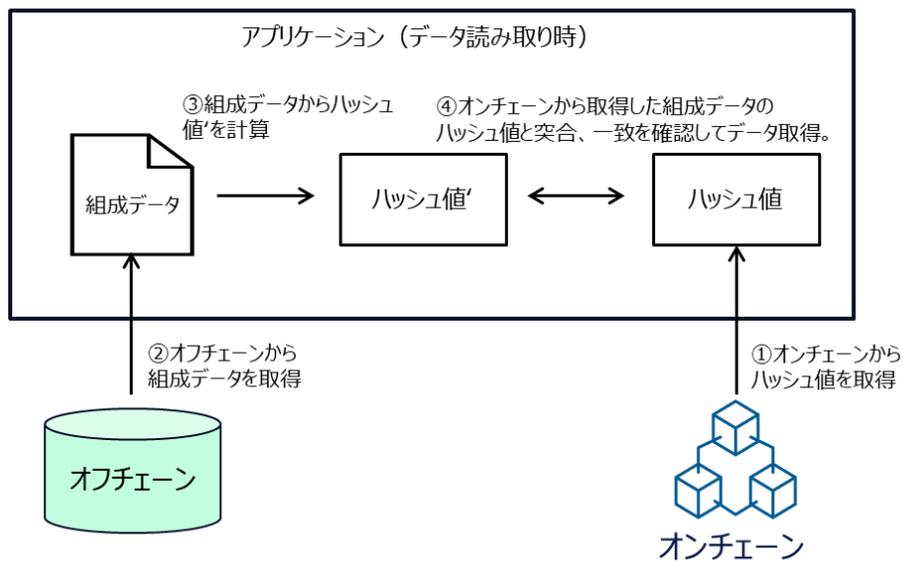


図 4-16

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。

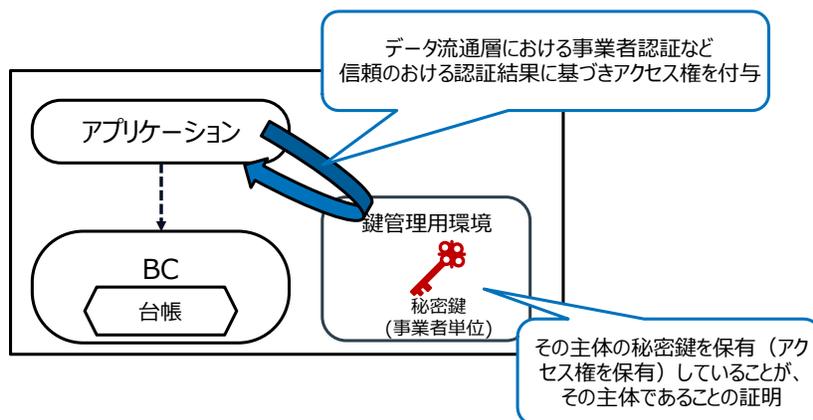


図 4-17

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に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、システム的设计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、ノードを地理的に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。

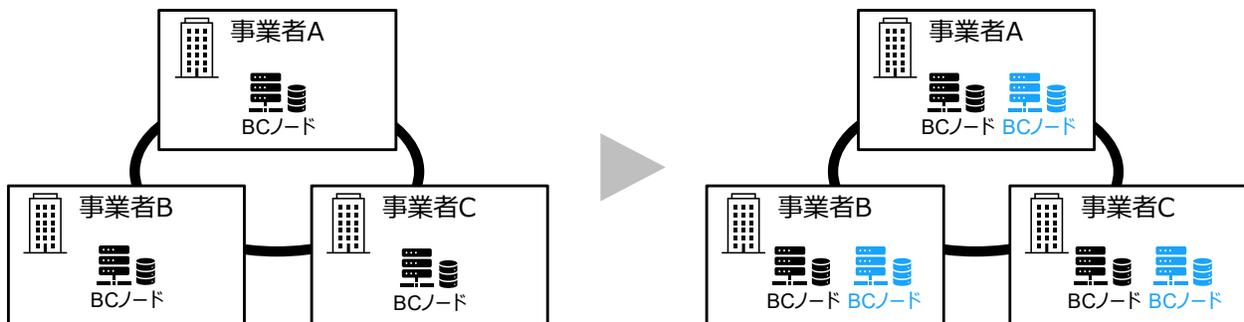


図 4-18

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。

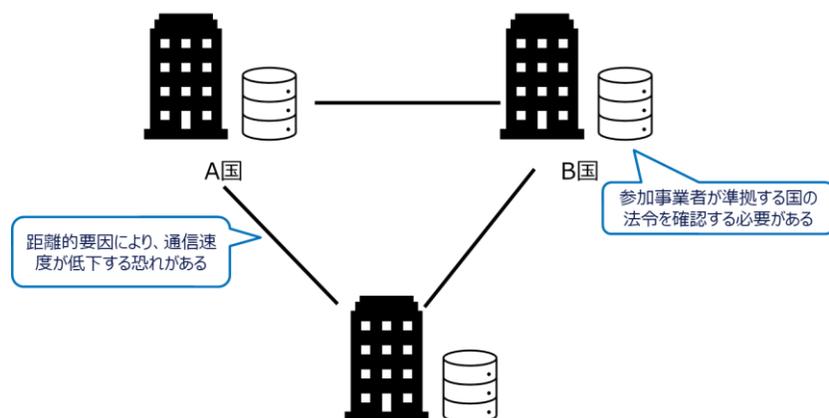


図 5-1

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。

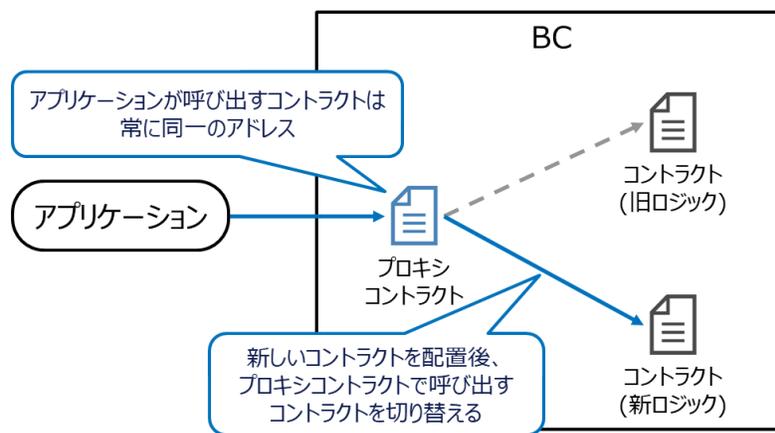


図 5-2

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 を使ってもらお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。

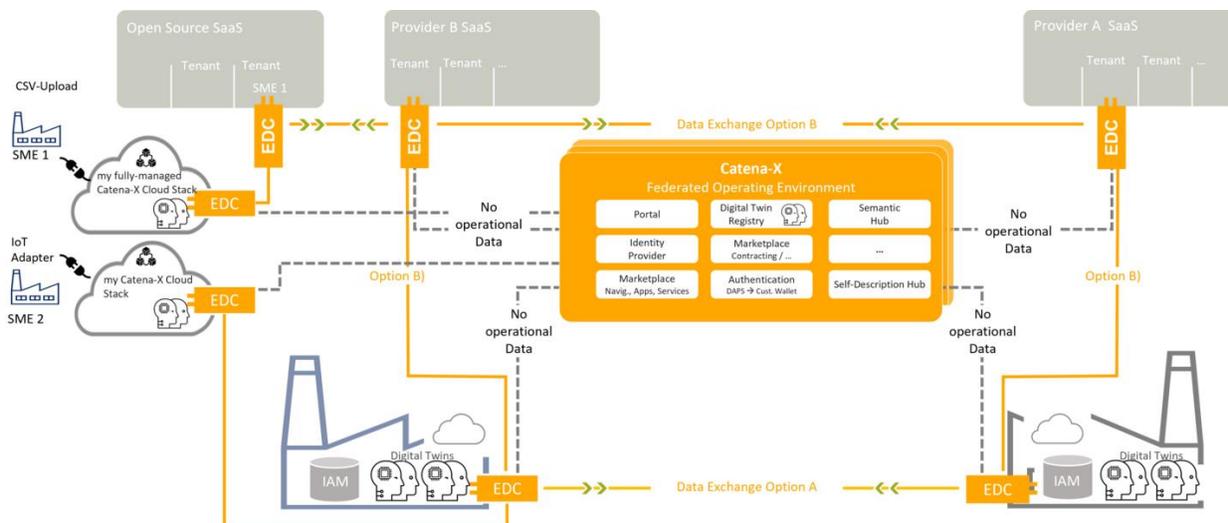


図 5-3

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ー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。

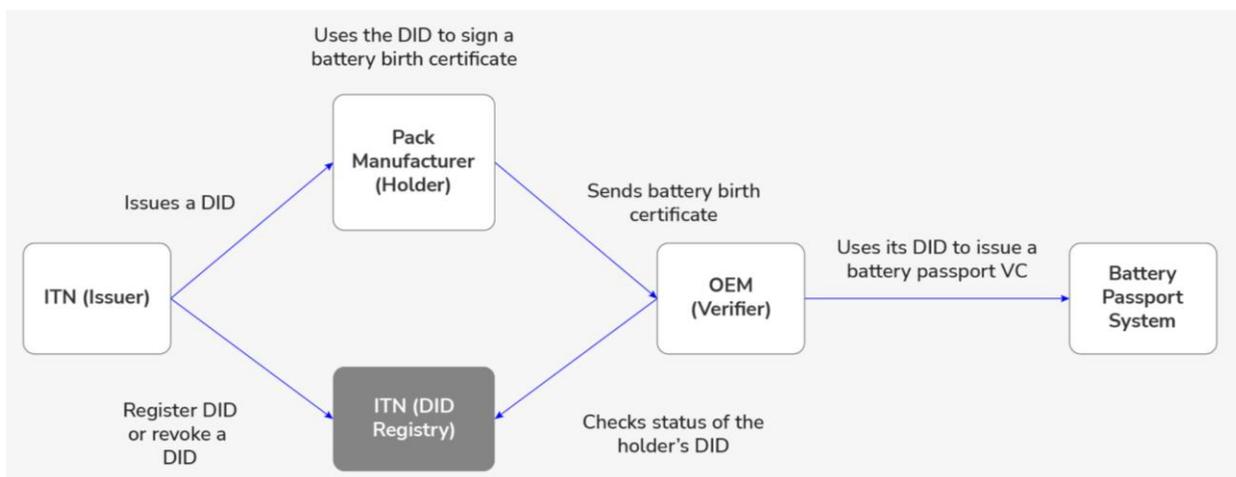


図 5-4

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参加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、プライバシー保護、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。

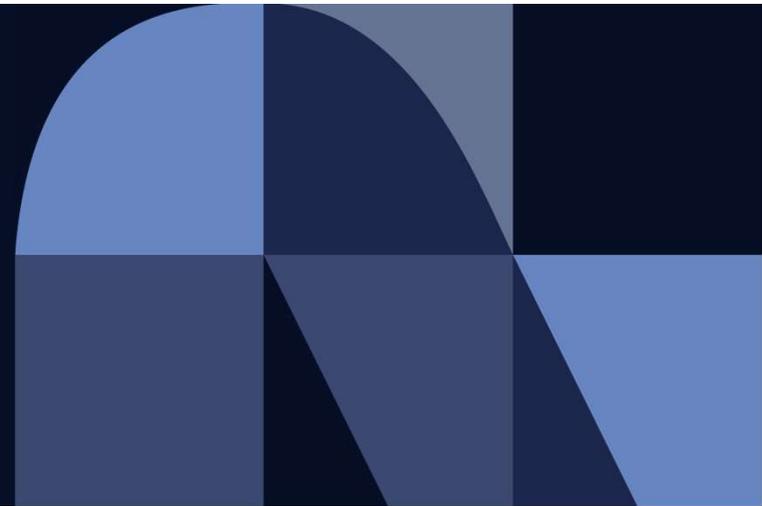
6 まとめ

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。

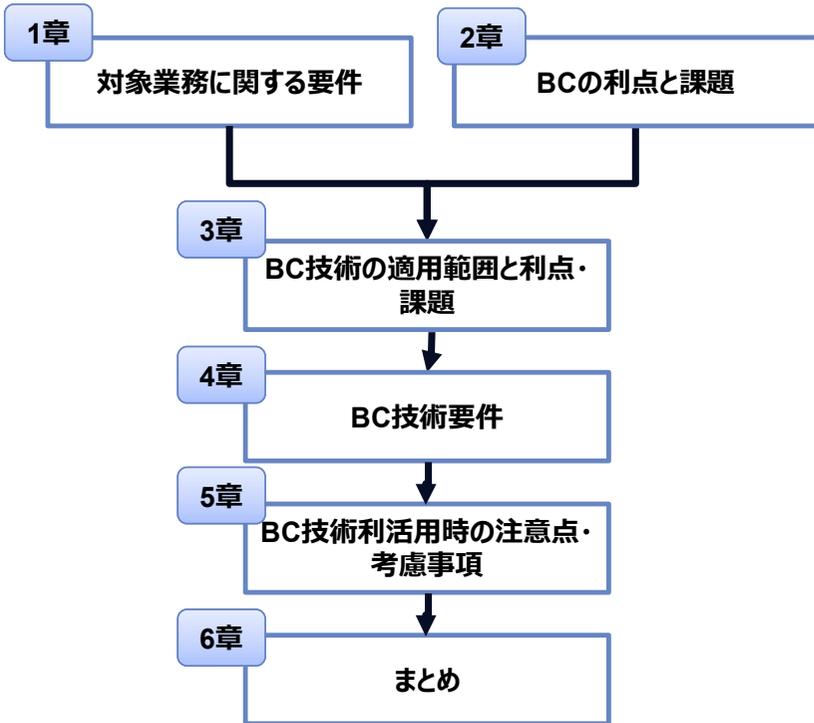
なお、本ガイドライン別紙の「ブロックチェーン技術ガイドライン別紙 チェックリスト」に、本ガイドラインにて示した検討ポイントをチェックリストの形で用意しており、検討漏れ防止のために活用いただきたい。



ブロックチェーン技術活用ガイドライン別紙 エグゼクティブサマリ

2025年2月
株式会社NTTデータ

ブロックチェーン技術活用ガイドラインの全体構成



章	記載内容
1章	本ガイドラインのモデル対象における課題を解決するためのプラットフォームに求められる業務要件を示した。 「トレーサビリティの確立」「データ主権の確保」「長期のデータ保管」「セキュリティ対策」「国際標準に準拠したデータ連携」が業務要件として求められる。
2章	BCの特性を踏まえた上で、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した。 データ主権の観点から分散型、また信頼性の観点からBCを利用することが最適である。
3章	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を整理して示した。 「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。
4章	BCをCE情報流通PFへ適用するにあたり、課題やBC技術を適切に用いるための考慮点があるため、それらを踏まえてBCを活用することが重要である。 「性能リスクへの対策」「情報漏洩・改ざん防止」「BCに掲載する情報」「認証方式」「可用性」「運用・保守性」に関して検討すべき点を示した
5章	BC技術を利用する際の注意点を示した。 「BCを利用・開発する上での注意点」「普及展開に関する課題への対応策」「海外関連システムとの連携」の三点が注意すべき点である。
6章	ガイドライン全体のまとめを示す。

1章 本書において前提とする資源循環モデル

CE情報流通PFへのBC技術の適用範囲を検討するため、日本の製造業において主要な位置を占める組立加工産業の資源循環をモデルケースとして、資源循環モデルを定義し、その課題とその解決方法（CE情報流通PFに求められる業務要件）を整理した。

図 資源循環モデルの課題

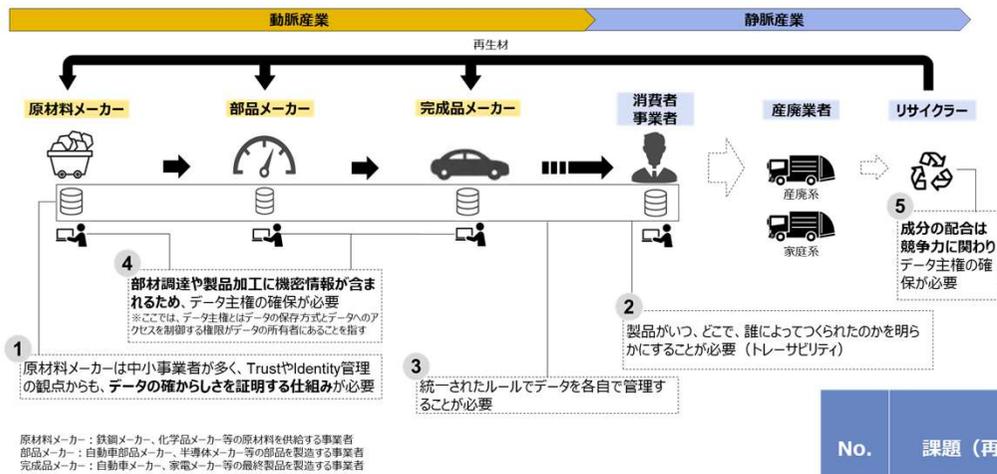


表 資源循環モデルの課題と解決方法

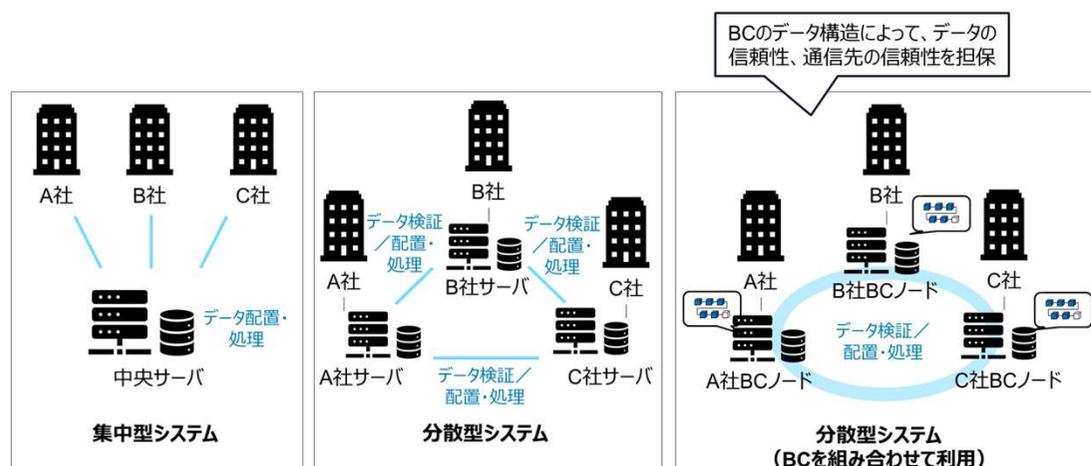
No.	課題（再掲）	内容	解決方法（業務要件）
1	データの信頼性確保	動静脈産業には様々な事業者が参加することから、データの確からしさの証明が必要	・法規要件を満たす国際標準に準拠したデータフォーマットにて標準化を行う
2		証拠能力の確保を目的に、トレーサビリティ管理を実現することが必要	・事業者間でデータ交換を行う際に法規要件を考慮した証拠能力を具備するトレーサビリティデータを記録する機能を具備する
3	データの保管	統一されたルールで保管し、再利用時にも活用できる状態とする	・長期間でのデータ保管や法規要件への遵法性を保証する
4		製品保証期間を大きく超えた長期間でのデータの保管が必要	
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
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	・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

2章 ブロックチェーンの必要性

BCの特性を踏まえた上で、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した。

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）として下記があり、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した。

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



結論としては、**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。

データ主権の要件について、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り、データの信頼性や通信先の信頼性などはBC活用により、より確実に実現できるため。

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

3章 ブロックチェーンの適用範囲

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と課題を整理して示した。

データの活用範囲の観点において、データの共有範囲の特性により分類すると、「**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。**

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下記表のように存在する。

No.	システム要件	BC活用の利点が得られる部分	事業者間・全事業者で利用（共有データ）	
			一つの事業者内でのみ利用（個社データ）	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	-	○	○

「BC活用の利点が得られる部分」と一致する点が多い

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章 ブロックチェーン技術要件

BCをCE情報流通PFへ適用するにあたり、課題やBC技術を適切に用いるための考慮点があるため、これらを踏まえてBCを活用することが重要である。

No.	課題	内容	対策方法・検討ポイントの概要
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。 具体的なリスクとしては、「BCの特性としての性能リスク」、「利用者増に伴う性能劣化」、「利用者追加の性能劣化」、「データ蓄積に伴う性能劣化」などが考えられる。	各性能リスクに対して、「非同期アーキテクチャの検討」、「コンセンサスアルゴリズムの選択」、「共有先指定方法の選択」、「BC拡張方法の選択」、「履歴データの容量の削減」などの対策方法が考えられる。
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。	データ秘匿の実現方式としては「全社で台帳を共有し、秘匿データは共有先のみが保持」の方式が最適である。 長期的な秘匿のためには暗号やハッシュ関数のアルゴリズム危殆化への対策も必要である。また、情報漏洩時の対処、鍵管理といった点も重要な検討ポイントとなる。
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。	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が重要。 ハッシュ値・オフチェーンを活用することで、耐改ざん性を保証しつつデータ削除なども実現可能となる。

4章 ブロックチェーン技術要件

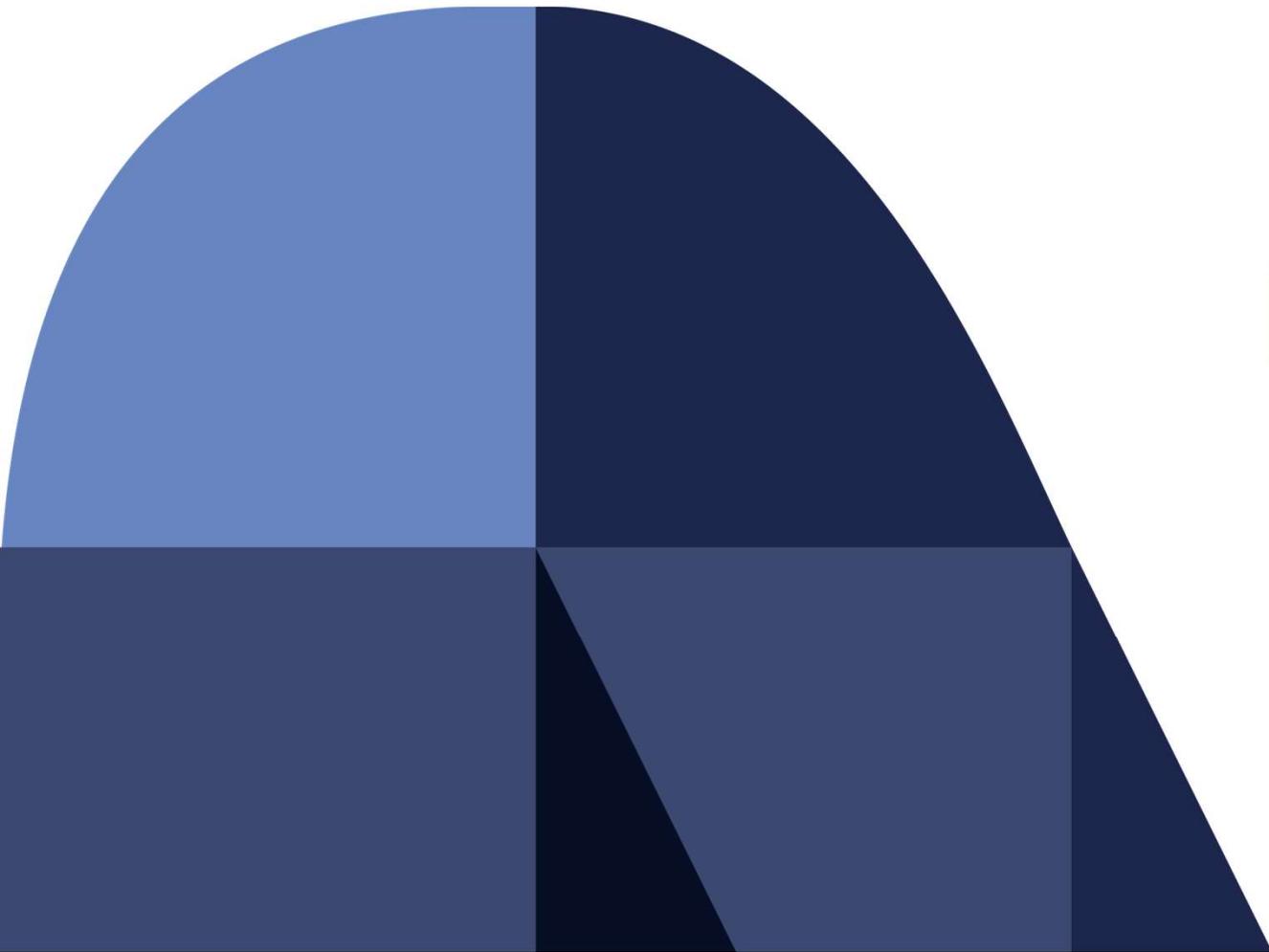
BCをCE情報流通PFへ適用するにあたり、課題やBC技術を適切に用いるための考慮点があるため、これらを踏まえてBCを活用することが重要である。

No.	課題	内容	対策方法・検討ポイントの概要
4	認証方式に関する実現方法の検討	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。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。	「データの信頼性」については、BCのハッシュチェーンの構造にて保証することができる。「相手先の信頼性」については、BCの電子署名により保証することができる。
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。	BCでは、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ため、「複数ノード構成」や「コンテナ利用」などによりノードの可用性の検討も必要となる。
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。	各事業者において、BCならではの運用監視やシステム更新などの運用・保守が必要となる。また、運営事業者においては、BCのシステム全体の運用・保守が必要となる。

5章 ブロックチェーン活用時の注意点・考慮事項

BCをCE情報流通PFへ適用するにあたり、注意すべき点・考慮すべき点があり、これらを踏まえてBCを活用することが重要である。

No.	注意点	概要
1	BCを利用・開発する上での注意点	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。また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。 海外の拠点にBCを配置する際の注意点や、ノード管理、スマートコントラクト開発時の注意点もあり、これらの注意点へ配慮することが必要である。
2	普及展開に関する課題への対応策	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いような注意が必要である。 また、BCを外部システムと接続するケースを想定することや、システム改善や機能拡充の継続性についても検討が必要である。
3	海外関連システムとの連携	Catena-XやMOBIなどの海外動向に注視する必要がある。



NTT DATA
Trusted Global Innovator