資料３

ウラノス・エコシステムの拡大及び相互運用性確保に向けたトラスト研究会報告書（案）

2025 年 3 月

経済産業省

目次

1. はじめに

1.1 産業データ連携及びウラノス・エコシステムに係る経緯

経済産業省では、DFFT（Data Free Flow with Trust：信頼性のある自由なデータ流通）の実現に向け、複数のシステムを連携させ、企業・業界を横断したデータの利活用を促進することで、データ・システム・ビジネス連携を具体的に推進し、官民協調で企業・産業競争力強化を目指す取組を、「ウラノス・エコシステム」として推進している。ウラノス・エコシステムは、「新しい資本主義のグランドデザイン及び実行計画」や「骨太の方針」、「デジタル社会の実現に向けた重点計画」といった主要な閣議決定文書（いずれも 2024 年 6 月閣議決定）にも関連する記載があり、政府一体として推進すべき重要施策として位置付けられている。

現在、ウラノス・エコシステムでは、経済活動に必要なあらゆるデータ連携、サービス連携、ビジネス連携を可能とするための協調領域を組成すべく、ユースケースの創出・拡大が進められている。その中でも、先行ユースケースとして位置付けられているのは、自動車・蓄電池業界横断でのトレーサビリティ管理である。このユースケースについては、2023 年 5 月に独立行政法人情報処理推進機構（IPA）デジタルアーキテクチャ・デザインセンター（DADC）より、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（蓄電池 CFP・DD 関係）α版が公開[1]され、データ連携基盤の開発が開始されると、2024 年 5 月に、一般社団法人自動車・蓄電池トレーサビリティ推進センター（ABtC）が主体となってトレーサビリティサービスの提供を開始した。同年 9 月には、データ連携システム運営事業者のトラストを外形的に担保すべく創設された経済産業省による「公益デジタルプラットフォーム（DPF）運営事業者認定制度」の認定を初めて取得している[2]。

1.2 本研究会開催の目的

1.1 でみたように、ウラノス・エコシステムでは現在、ユースケースの創出・拡大が推進されているところであるが、一方でデータ連携に参加する事業者やユースケースの拡大は、不正な事業者の参入や不正確なデータの混入リスク等の増大等、不確定な要素やリスクの増大を招く。そこで、データの共有・利活用を、安全で信頼できる形で実現するために求められるのが、データそのものやデータに関するステークホルダーの信頼性確保のための「トラスト」である。ここでいうトラストとは「相手が期待を裏切らないと思える状態」を指す。トラストの確保は不確定要素を受容可能なリスクへ落とし込む一つのアプローチであり、データ連携の拡大にも資することになる。

---

[1] IPA 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（蓄電池 CFP ・DD 関係）
https://www.ipa.go.jp/digital/architecture/guidelines/scdata guidline.html

[2] 公益 DPF 運営事業者認定制度 HP
https://www.ipa.go.jp/digital/dx/dpf-nintei.html

しかしながら、トラストの担保の要素や水準はユースケースやデータの性質によって異なり、様々な局面において実際にデータの共同利用・利活用を行うユーザー企業が求めるニーズ等とのバランスを重視することが重要であることから、ユースケースやニーズ、コスト等に即したトラストの考え方を整理することが必要である。

以上の考え方の下、安全で信頼できる形で、ユースケースドリブンで産業データ連携を推進するために、ニーズとのバランスを考慮したトラスト要求を整理することを目的として、研究会を開催することとした。

なお、産業界においては、産業データ連携やデータガバナンスに関する議論が高まっている。直近の代表的な動向をみると、2024 年 10 月 15 日には、一般社団法人日本経済団体連合会が事務局となり、産業データスペースの構築に関する検討がなされ、「産業データスペースの構築に向けて」が公表されている[3]。また、同月 17 日には、デジタル政策フォーラム（DPFJ）、デジタル社会推進協議会（DSA）、デジタルトラスト協議会（JDTF）の連名で、「データガバナンス戦略の推進」が公表されている[4]。

[3] 一般社団法人日本経済団体連合会産業データスペースの構築に向けて
https://www.keidanren.or.jp/policy/2024/073.html

[4] 一般社団法人デジタル政策財団提言「データガバナンス戦略の推進」
https://prtimes.jp/main/html/rd/p/000000009.000131931.html

2. ユースケースに基づくトラスト要求の整理方法

2.1 トラストの整理に当たっての基本的な方針

前述のとおり、本研究会では、ユースケースドリブンで産業データ連携を推進するために、ニーズとのバランスを考慮したトラスト要求を整理することを目的としている。各業界におけるユースケースドリブンでトラストを整理するに当たり、データ連携の対象となるデータやデータの取扱いに係る規律や規約を整理し、トラストによって対応する不確実性（リスク）要素を明確化することが必要である。整理・明確化に当たっては、データマネジメントのモデル化やリスク分析のアプローチ手法である DMF（データマネジメント・フレームワーク）を参考にした。

2.2 DMF の概要

2.2.1 DMF 策定の経緯

我が国では、サイバー空間とフィジカル空間を高度に融合させることにより、多様なニーズにきめ細かに対応したモノやサービスを提供し、経済的発展と社会的課題の解決を両立する超スマート社会「Society5.0」の実現を提唱している。「Society5.0」では、価値創造過程（バリュークリエイションプロセス）がより柔軟で動的なものに変化することが期待されているものの、サイバー空間とフィジカル空間の融合により、サイバー攻撃の脅威が増大することが指摘されている。

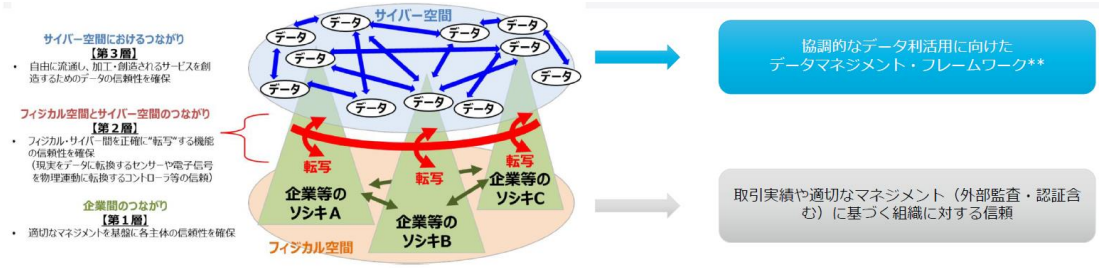
そこで、経済産業省では、「Society5.0」におけるセキュリティ対策の全体像を整理し、産業界が自らの対策に活用できるセキュリティ対策例をまとめた「サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）」を 2019 年４月に策定した[5]。CPSF では、三層構造モデルを導入し、「Society5.0」におけるバリュークリエイションプロセスの信頼性の基点を明確化するために、産業社会を３つの層で整理している。このうち、産業データ連携が行われる第３層（サイバー空間におけるつながり）では、データ自体に信頼性の基点を置いて包括的なセキュリティ対策を実施するために、データのライフサイクル全体にわたってリスクを洗い出し、ステークホルダー間での強調した信頼性確保・リスク低減が必要となる。

そのため、経済産業省において、データを軸に置き、データのライフサイクルを通じて、その置かれている状態を可視化してリスクを洗い出し、そのセキュリティを確保するために必要な措置を適切なデータマネジメントによって実現することを可能とする DMF を 2022 年 4 月に策定[6]した。

---

[5]経済産業省 サイバー・フィジカル・セキュリティ対策フレームワーク
https://www.meti.go.jp/policy/netsecurity/wg1/cpsf.html

[6]経済産業省 協調的なデータ利活用に向けたデータマネジメント・フレームワーク
～データによる価値創造の信頼性確保に向けた新たなアプローチ
https://www.meti.go.jp/policy/netsecurity/wg1/DataManagement Framework_1_1.pdf



図●CPSF の三層構造モデル

2.2.2　データマネジメントのモデル化

DMF では、データマネジメントを「データの属性が場におけるイベントによる変化する過程を、ライフサイクルを踏まえて管理すること」と定義し、「イベント」、「場」、「属性」という３つのそれぞれ影響し合う関係にある３つの要素から構成されるモデルとして整理されている。３つの要素のそれぞれの定義は次のとおりである。

- イベント：データの生成・取得から破棄に至るまでのフロー
- 場：データの取扱いにかかる規律や規約
  例）各種法令（個人情報、越境移転規制、知財、輸出管理）、プラットフォームの利用規約
- 属性：各データに対する「場」からの要件、データ所有者や開示先など、データが持つ性質の集合

このモデル化により、データの状態が可視化され、ステークホルダーの間で認識を共有しやすくなり、ステークホルダー全体での適切なデータマネジメントの実施につながることが期待される。

2.2.3　リスク分析手順

DMF においては、下記の４つのステップに沿ってバリュークリエイションプロセスにおけるデータの状態を可視化する[7]。

STEP１　データ処理フロー（「イベント」）の可視化

- データの生成・取得から廃棄に至るまで、想定されるデータ利活用プロセスにおける大まかなデータフロー及び「イベント」を可視化する

STEP２　必要な制度的保護措置（「場」）の整理

- データ保護に資する「場」を検討し、法律・契約の観点から適切なものを設定する。その際、一つのデータに対して複数の「場」が重なり合う、つまり、データに対して様々な観点からの要求がなされることが考えられる

[7] 経済産業省　協調的なデータ利活用に向けたデータマネジメント・フレームワークを策定しました
https://www.meti.go.jp/press/2022/04/20220408005/20220408005.html

STEP３　「属性」の具体化

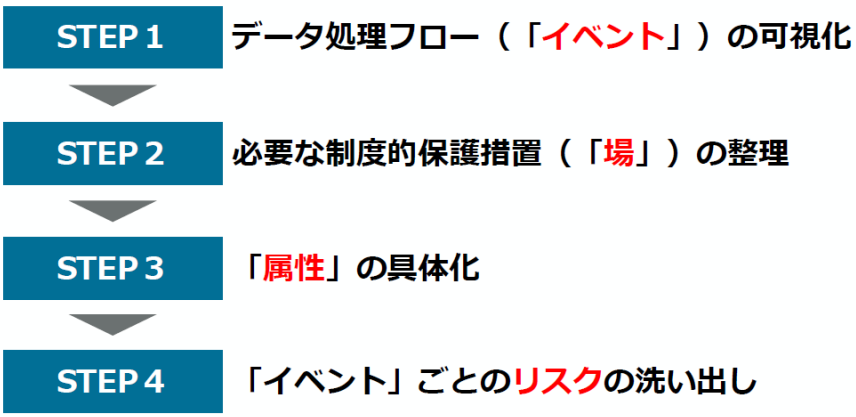
・　設定されたデータや「イベント」、「場」に基づいて、管理上あるべき「属性」を特定する

・　データの「属性」を整理していく中で、本データが取り扱われるべき「場」や実施されるべき「イベント」に漏れがあった場合、適宜追加等を実施する

STEP４　「イベント」ごとのリスクの洗い出し

・　設定された「場」という観点から、「イベント」ごとに想定されるリスクを抽出し、設定した「属性」をレビューする

・　その際、機密性・完全性・可用性といったサイバーセキュリティに係る観点のほか、各法制度等に係るコンプライアンスの観点でのリスクについても洗い出す



図●DMF におけるリスク分析手順

2.3 DMF STEP に沿ったトラストの整理の方法

本研究会では各ユースケースにおけるトラストの整理に当たって、上記の DMF に沿ったリスク分析とそれに対する対応策を整理するべく、下記の Q1～Q4 の４つの要素に分けて、データ連携の対象となるデータや場を整理し、トラストによって対応する不確実性（リスク）要素及び対処方法を収集、分析した。1.2 の繰り返しになるが、本研究会において、トラストとは「相手が期待を裏切らないと思える状態」を指し、トラストを確保することは、不確定要素を需要可能なリスクへ落とし込むことにつながる。

Q.１　連携対象となるデータ（DMF STEP１に該当）

・　連携の対象となるデータの種類

・　各データの生成・取得から破棄までのフロー　等

Q.２　データ連携の場（DMF STEP２に該当）

・　データ連携の場を構成する事業者の種類や数

・　事業者やデータに対する規律・規制や事業者間での規約　等

Q.３　データに関わるリスク・不確実性（DMF STEP３・４に該当）

・　データごとの属性と属性に対し想定されるリスク

・　リスクを生じさせる不確実要素は何か　等

Q.４　リスクに対する対応策

・　トラストが必要な項目・対象

・　項目・対象ごとに備えるべきアシュアランスレベル

・　トラストアンカーは誰が担うか　等

図●産業データ連携におけるトラストの整理の方法

3. 各分野におけるユースケース

本章では、第２章で記載した整理方法に基づき、国内のデータ連携のユースケース７事例について整理する。

3.1 自動車・蓄電池のユースケース①：蓄電池 CFP/DD[8,9]

一般社団法人自動車・蓄電池トレーサビリティ推進センターによる、蓄電池 CFP データや DD データのデータ連携ユースケースを紹介する。

3.1.1 連携対象となるデータ

連携対象となるデータとしては、蓄電池のサプライチェーンにおける Carbon Footprint of Products（CFP）情報と Due Diligence（DD）情報である。CFP は、原材料の調達から製造工程、さらには輸送や販売に至るまでの各段階で生成される CO2 排出量を含む。また、多種多様な情報が含まれる。また、DD は、原材料の採掘・調達における人権・環境リスクの評価及び改善活動状況を含む。

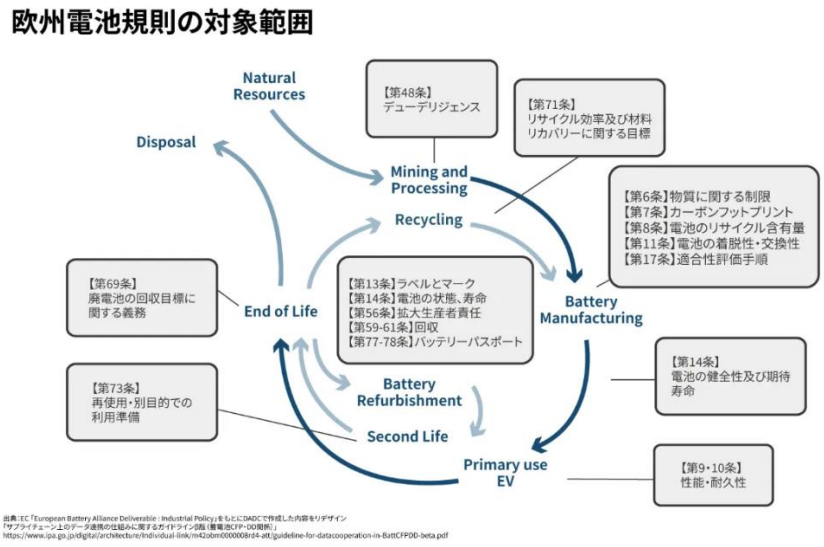
3.1.2 データ連携の場

蓄電池データのサプライチェーン上での共有については、特に欧州電池規則で求められている。直近としては欧州電池規則の第 7 条の電池の CFP 及び第 48 条のサプライチェーンの DD への対応が求められている。さらに、将来的には第 8 条のリサイクル含有量や第 77 条の電池パスポートの規定への対応が必要になる。

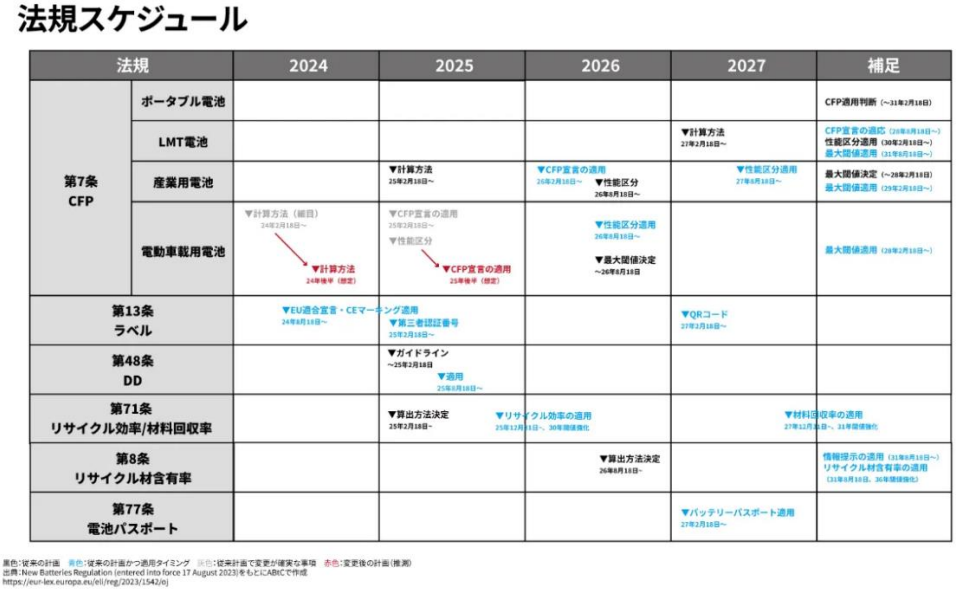
---

[8] 経済産業省 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 β 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

[9] IPA DADC データ連携基盤を活用した 蓄電池・自動車の カーボンフットプリント（CFP） 運用ガイドブック β 版
https://www.ipa.go.jp/digital/architecture/Individual-link/jod03a000000a3d1-att/cfp-guidebook.pdf



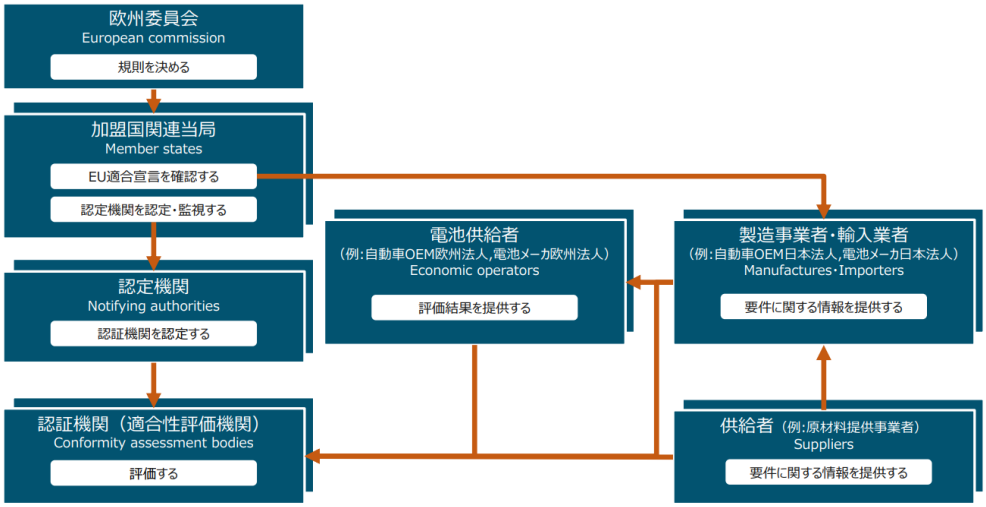
図●欧州電池規則の対象範囲[10]



図●欧州電池規則の法規スケジュール [10]

欧州電池規則に定義されているサプライチェーン上の事業者の種類としては、供給者（例：原材料提供事業者）、製造事業者・輸入事業者（例：自動車 OEM 日本法人、電池メーカー日本法人）、電池供給者（例：自動車 OEM 欧州法人、電池メーカー欧州法人）が挙げられる。

[10] ABtC 欧州電池規則 -概要編-
https://abtc.or.jp/column/240815-1#index_n8X65XBm



図●欧州電池規則案に定義されているステークホルダー[8]

3.1.3　データに関わるリスク・不確実性

データに関わるリスク・不確実性としては、データ改ざんや成りすましが発生するリスク、データ漏えい・プライバシーのリスク、国際間データ連携の不確実性の３つが挙げられる。

1. データ改ざんや成りすましが発生するリスク

   悪意ある第三者がシステムに侵入し、電池の環境データを書き換えたり、他企業に成りすまして虚偽のデータを入力するおそれが挙げられる。また、中間者攻撃などにより送受信中のデータが改ざんされる可能性も存在する。

2. データ漏えい・プライバシーのリスク

   蓄電池のデータには企業の機密情報（製造ノウハウや原材料のサプライヤ情報など）が含まれることがある。そのため、不適切なアクセス制御やサイバー攻撃によってデータが漏えいするリスク、共有先の企業が意図と異なる目的でデータを再利用してしまうリスクが存在する。

3. 国際間データ連携の不確実性

   蓄電池サプライチェーンはグローバルに広がっているため、国や地域ごとの規制の違いなどがデータ連携の障壁となり得る。

3.1.4　リスクに対する対応策

上記のリスクに対する対応策としては、機密保護・アクセス制御の強化、データの透明性確保、相互運用性の確保の３つが挙げられる。

1. 機密保護・アクセス制御の強化

   ユーザー認証システムを導入し、参加企業ごとに ID を発行して権限に応じたアクセス制限を

行っている。これにより、許可された関係者のみが必要なデータにアクセスでき、不正な成りすましアクセスを遮断する。また、正しい接続情報であることを確認し、通信の機密性と完全性を満たすセキュアな通信を実現している。

2. データの透明性確保

   具体的には、第三者機関認証の仕組みの構築である。算出された CFP 値や提出された DD 報告について独立した第三者機関による検証・認証を必要とするプロセスを設けられている。第三者の関与によって、データの信憑性が客観的に担保され、関係企業間だけでなく消費者に対しても説明責任を果たしやすくなる。

3. 相互運用性の確保

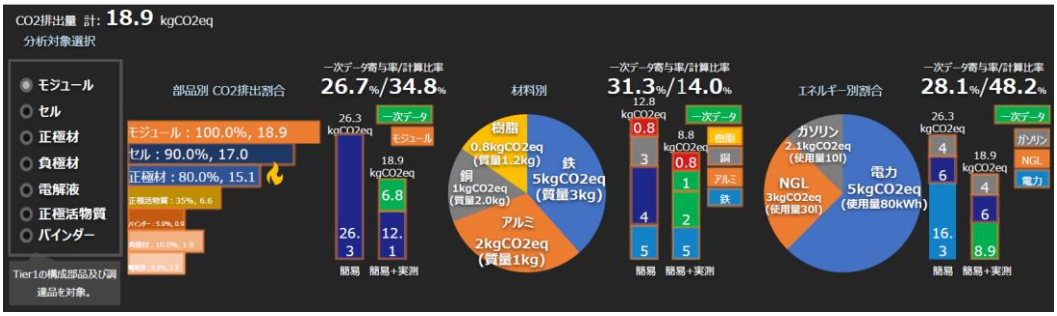
   蓄電池サプライチェーンはグローバルに広がっているため、海外のデータ連携基盤との相互運用性の確保が不可欠である。将来的には、欧州の Catena-X 等との相互運用の実現を目指している。

3.2 自動車・蓄電池のユースケース②：自動車 LCA

ここでは、一般社団法人自動車・蓄電池トレーサビリティ推進センターによる、自動車 Life Cycle Assessment（LCA）のデータ連携ユースケースを紹介する。

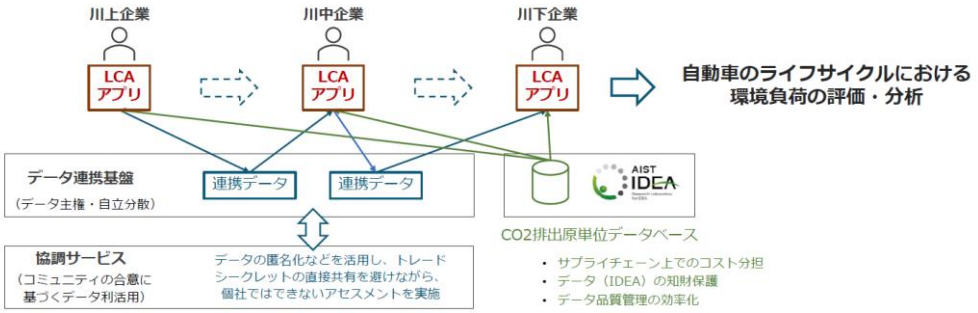
3.2.1 連携対象となるデータ

連携対象となるデータは２つある。１つ目は、原材料調達から廃棄に至るまでのサプライチェーン上の各社による CO_2排出データである。自動車メーカー（OEM）、部品メーカー（Tier1）、材料メーカー（Tier2）など、多様なステークホルダーが関与し、各工程における CO_2排出データを収集し、業界全体でのデータ連携を実現することで、サプライチェーン全体での環境負荷の可視化と排出削減の方策を検討する。LCA の目的は単に CO_2排出量の数値を算定するだけでなく、どこでどのように排出が発生しているかを明確にし、問題点を特定して改善策を講じることにある。そのため、素材別、部品別、エネルギー別といった詳細な分析を行い、排出削減のための施策をサプライチェーン全体で展開することが求められる。



図●アセスメントのイメージ図（数字はダミー）

２つ目は、CO_2排出原単位データである。例えば、AIST（産業技術総合研究所）が開発した環境負荷評価のためのデータベースである IDEA（Inventory Database for Environmental Analysis）を用いる場合、IDEA のデータはライセンス管理されており、サプライチェーン全体での利用や共有には、知的財産の権利や個人情報の適切な管理が求められる。



図●自動車 LCA におけるデータ連携のイメージ図

3.2.2　データ連携の場

LCA の実施に際しては、自動車サプライチェーンにおける企業間取引を前提としながら、データ連携を推進する。今後の LCA の広がりによっては、数万社規模の企業が関与する可能性がある。

また、LCA の国際標準化については、国連 WP29（自動車基準調和世界フォーラム）で議論中であり、将来的にはグローバルサプライチェーンがデータ連携の場となる可能性がある。

3.2.3　データに関わるリスク・不確実性

LCA におけるデータ連携には、外部からの攻撃等によるデータの漏えいリスクが伴うほか、データ提供者が本来想定していない用途で、データ利用者によって情報が目的外利用される懸念がある。IDEA データの利用に関しては、ライセンスが個人単位で管理されており、国内外の個人情報保護ルールへの適応が必要である。また、グローバルなデータ連携においては、国や地域の法令の差異により、

連携が途絶する可能性がある。

将来的には、各社・各団体等による自主活動や、規制化等の同行を見据えつつ、第三者認証等によるデータ品質管理の導入を検討する必要性がある。

3.2.4 リスクに対する対応策

データ連携に先立ってモノの取引契約があるため、ビジネス要件として新たなデジタルトラストは不要である。一方で、今後のLCAの広がりによっては、参加者の裾野が広がることから、事業者の本人性確認には安価でスケーラブルな仕組みへのニーズがあると思われる。

また、IDEA データについては、知財保護・課金・個人情報管理の観点から適切な取扱いが求められる。データ提供と利活用の在り方について関係者間で合意を形成し、データの匿名化などを活用してトレードシークレットの保護とデータ活用を両立する仕組みの構築が進められている。

表●自動車 LCA のユースケースにおける Q1～Q4 のまとめ

Q. 1　連携対象となるデータ
✓ サプライチェーン上の各社による CO_2 排出データ。これらは取引関係に沿って集約され、分析の対象となる。 ✓ CO_2 排出原単位データ（IDEA）。IDEA はサプライチェーンの各企業によって用いられるが、取扱条件に知財の伝播や個人情報管理を含む。
Q. 2　データ連携の場
✓ 自動車サプライチェーンにおける企業間取引。今後の LCA の広がりによるが、場の規模は自動車サプライチェーンの企業数は数万社の規模となる。 ✓ 自動車 LCA の国際標準を国連 WP29 で議論中。将来的には、グローバルサプライチェーンがデータ連携の場となる可能性がある。
Q. 3　データに関わるリスク・不確実性
✓ 外部からの攻撃等によるデータの漏えい ✓ データ利用者による、データ提供者が意図しない利活用（CO_2 排出に関する情報、IDEA） ✓ IDEA 利用者の個人情報管理。IDEA はライセンスが個人単位で管理され、国内外の個人情報保護ルールへの対応が必要。 ✓ データ越境の差止め等による連携の途絶（グローバル対応時） ✓ 第三者認証等によるデータ品質管理（自主活動、規制化等の同行を見据えて検討要）
Q. 4　リスクに対する対応策

- ✓ 価値情報のサプライチェーン上での取扱い（知財保護・課金・個人情報管理）について IDEA を題材として議論中。
- ✓ その他については、蓄電池 CFP と同様。

3.3 自動車・蓄電池のユースケース③：電池パスポート

3.3.1 連携対象となるデータ

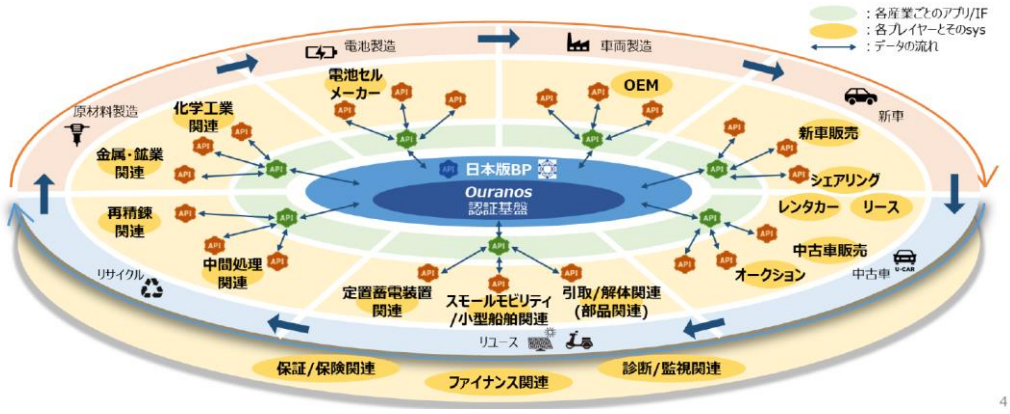
電池パスポートの導入は、電池のライフサイクル全体を通じたトレーサビリティの確保を目的とし、製造からリサイクルに至るまでの各段階で必要な情報を一元的に管理することを目指している。本ユースケースでは、OEM、電池メーカー、リサイクル業者など、多様なステークホルダーが関与し、国際的な電池パスポート規制（2027 年施行予定）にも対応できる仕組みの構築を進めている。連携対象となるデータは、以下の３つである。

1. 個体識別情報（製造者情報、電池寸法、資源量など）
2. 価値情報（性能・寿命に関わるデータ、履歴情報など）
3. 環境対応情報（カーボンフットプリント（CFP）、デューデリジェンス（DD）データなど）

3.3.2 データ連携の場

電池パスポートのデータ連携は、段階的に拡張される計画であり、まず国内市場でのデータ連携を確立し（Step1）、その後、グローバルへと拡張する（Step2）。

Step1 として、国内では、電池のライフサイクル全体で価値を創出し、電池の資源循環を促進するためのエコシステムの構築が進められている。エコシステム全体においては、多様なステークホルダーとビジネスプロセスが存在するとともに、競争サービスと協調サービスが生むデータが複雑に連携し合う関係になる。このため、単一の中央管理システムではなく、「System of Systems」として、さまざまな基盤やプラットフォームが相互に連携する形で構築されることが必要とされている。また、エコシステムを横断して共有するコア部分（日本版バッテリーパスポート）では、①様々な基盤・サービスを連携させる共通窓口（API）、②データ提供者に経済的に報いるための公平かつ安全な課金の仕組みと取引台帳、③コミュニティで共有すべき最低限保持すべき情報を備える必要がある。国内市場では、中古車の性能保証、小型モビリティのモジュール単位でのリユース、定置蓄電池のリユース・リサイクルなどのユースケースが先行している。



図●電池のエコシステム

Step 2 では、海外との連携を目指す。このときの場は、欧州の電池パスポート規制（2027 年施行予定）をはじめとする国際的な規制である。各国の電池パスポート規制との相互運用性を確保しながら、国際的な電池パスポートの枠組みと統合することが求められている。

3.3.3 データに関わるリスク・不確実性

電池パスポートにおけるデータ連携には、以下のようなリスクが考えられる。

- データのなりすましや改ざん等によるデータの不適切な利用
- 外部からの攻撃等によるデータの漏えい
- 汎用性のないシステムによる他国との相互接続困難
- 地域間ルールの総意に伴うデータ連携の途絶（蓄電池に関するルール、資源循環に関するルール、データ越境や DPP サービスプロバイダー要件に関するルール等）

3.3.4 リスクに対する対応策

多用なステークホルダーとビジネスプロセスが存在する中で、電池のライフサイクルで生じる様々な情報を取り扱うため、単一のリスク・トラストを想定することが困難である。そのため、ユースケースごと（産業ごと）に検討・実証を行い、必要十分なリスク対応とトラスト設計が必要である。特に以下の３つの点に留意しながら、国内の電池市場を起点とした価値創造、及び海外の電池パスポート規制への対応という両軸で進める必要がある。

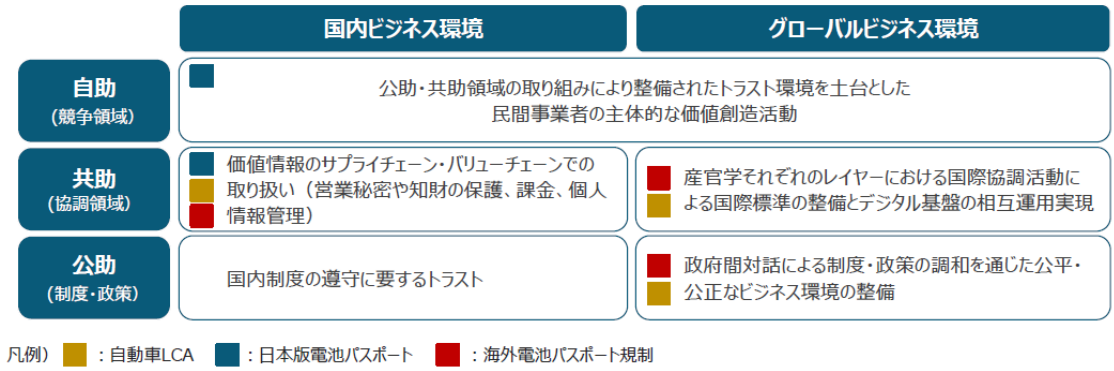
1. 業界やユースケースごとに必要十分なトラスト設計
2. 海外、業界やユースケースごとに必要十分な堅牢性確保
3. API を用いた他国との相互接続に向けた柔軟なシステム構成

表●電池パスポートのユースケースにおける Q1～Q4 のまとめ

Q. 1　連携対象となるデータ
✓　製造、使用、二次使用（中古）、リサイクル等の電池のライフサイクルで生じる様々な情報 ・　個体識別情報（製造者情報、電池寸法、資源量など） ・　価値情報 ✓　性能・寿命に関わるデータ（履歴情報など） ✓　環境対応に関わるデータ（CFP、DD※など） ※CFP:カーボンフットプリント、DD:デューデリジェンス
Q. 2　データ連携の場
✓　製造、使用、二次使用（中古）、リサイクル等の国内市場における蓄電池の様々なライフサイクルステージの参加者 ・　Step1　国内ユースケースごと（産業ごと）に連携の場を構築 ✓　中古車の性能保証（実施中） ✓　小型モビリティへのモジュール単位でのリユース（実施中） ✓　定置蓄電池へのリユース、リサイクル（今後展開） ・　Step2　海外連携し、グローバルに場を拡大
Q. 3　データに関わるリスク・不確実性
✓　なりすましや改ざん等によるデータの不適切な利用 ✓　外部からの攻撃等によるデータの漏えい ✓　汎用性のないシステムによる他国との相互接続困難 ✓　地域間ルールの相違に伴うデータ連携の途絶 （蓄電池に関するルール、資源循環に関するルール、データ越境や DPP サービスプロバイダー要件に関するルール等）
Q. 4　リスクに対する対応策
✓　業界やユースケースごとに必要十分なトラスト設計 ✓　海外、業界やユースケースごとに必要十分な堅牢性確保 ✓　API を用いた他国との相互接続に向けた柔軟なシステム構成

3.1 で述べた自動車 LCA のユースケースと、電池パスポートのトラストの検討領域は、異なるステークホルダー間を含む複数の領域にまたがる（図●）。したがって、特定のデジタル技術が全ての領域に適用可能であるとは限らない。それぞれの領域において、当事者による法規制、商慣習、ビジネ

ス構造、既存のデジタル資産等の総合的な考慮・検討と、具体的な実証をしながら、要求されるトラストの内容・レベルに関する合意形成と実装を進める必要がある。



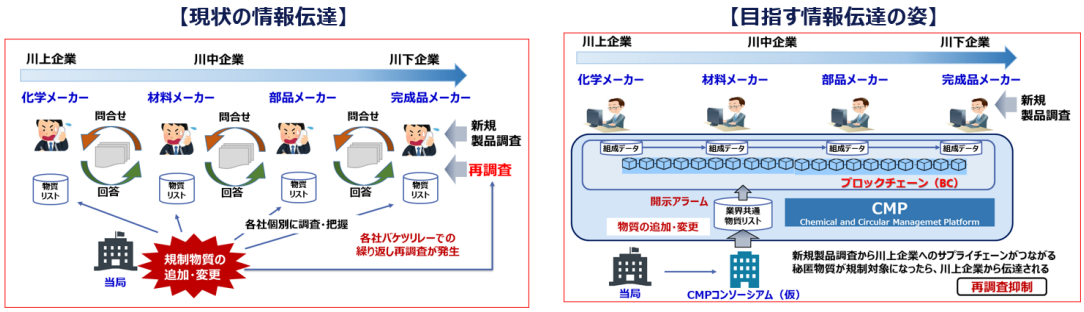
図●自動車分野におけるトラストの検討領域

3.4 化学物質管理のユースケース

ここでは、CMP タスクフォースによる、製品含有化学物質及び資源循環情報の連携に係るユースケースを紹介する。

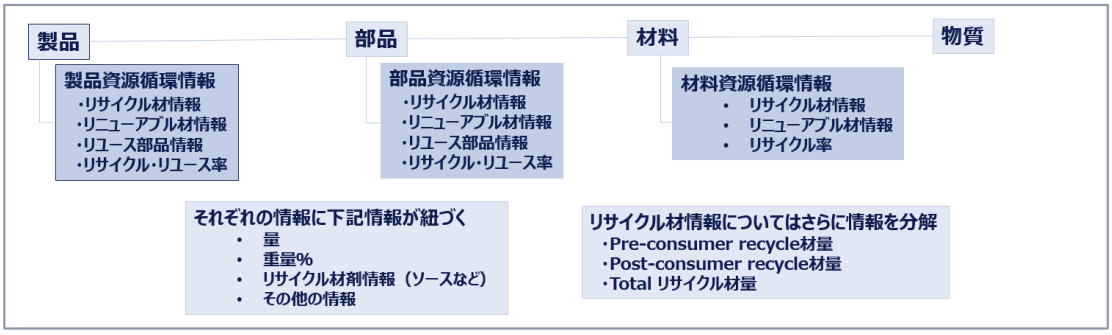
3.4.1 連携対象となるデータ

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）ため、川上の事業者（化学品メーカー）から川下の事業者（セットメーカー）へ、製品含有化学物質情報が連携される。また、欧州 ESPR 規制を睨み、DPP を意識したバリューチェーンでの資源循環情報として、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）も連携対象とされている。



図●CMP における製品含有化学物質の連携イメージ

ここでは、CMP が持つ製品・部品・材料・化学物質のヒエラルキー情報に、資源循環情報を加味することで効率的に情報共有を図る検討がなされている。



図●CMP のデータ構造と資源循環情報の関係

3.4.2　データ連携の場

先述のとおり、川上の事業者（化学品メーカー）から川下の事業者（セットメーカー）へのサプライチェーンを通じて製品含有化学物質情報、資源循環情報が連携され、参加者数は 1 万を超えることが想定されている。

ただ、CMP における製品含有化学物質の連携は、既に取引基本契約が締結されている直接の取引先同士の間で行われる（B2B）ため、法人、人、モノのトラストは、当該取引基本契約を基礎として既に成立している。したがって、例えばモノのトラストに関しては、モノの特定は依頼者品番と提供者品番の紐付けによって実施され、各社提供者の責任において情物一致が行われることになる。

また、データ連携に関してもこれを規律する契約が取引先同士の間で存在しており、この中で品質保証や瑕疵責任、秘密保持、製品含有化学物質情報の提供義務等が定められている。

3.4.3　データに関わるリスク・不確実性

製品含有化学物質情報や、リサイクル材・リユース部品情報については、各種の法規制への対応を目的として連携されるものであるため、データの信頼性が必要とされる。

なお、先述のとおり、CMP での製品含有化学物質情報の連携は、既に取引基本契約のある事業者間において B2B で行われる。そのため、例えば参加者の実在性・本人性に関しても、データを交換する相手としての法人認可については、契約に基づき行われるため、トラストを確保するための手段が新しく必要とされることはない。

一方で、不特定多数の事業者とのデータ連携が想定されるシーンも存在するため、その場合には、更なるトラストが必要となる局面が考えられる。例えば、資源循環情報の連携に際しては、オープンループリサイクルという観点から不特定多数の企業が関与することも考えられるほか、マーケットプレイスのような場における情報交換が行われる可能性もある。

また、自動車分野における IMDS（International Material Data System）との連携や、東南アジアでのシステム展開等、海外への展開を想定した場合には、海外プラットフォームとの相互認証が必要になることが考えられる。

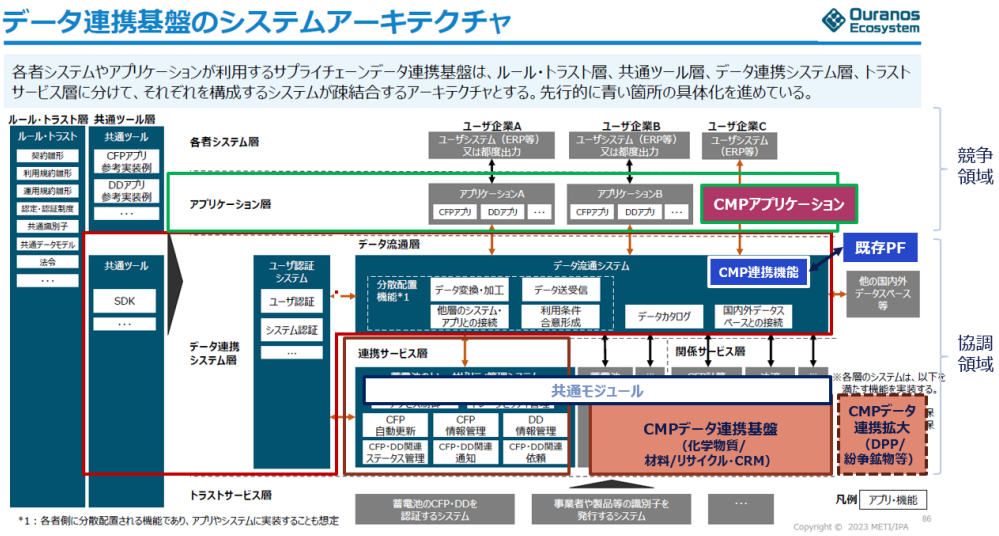
3.4.4 リスクに対する対応策

データの信頼性については、IEC63000 の国際標準により実施される。これは、物の化学物質規制の遵法判断は、企業が持つ製造プロセスのマネジメントシステム、分析データ並びに、これらのデータを基にしたサプライチェーンからの情報伝達（IEC/ISO82474、IEC62474）ルールに基づく情報伝達により確保することとされているところ、多くの国、地域の化学物質規制への遵法判断には IEC63000 が指定されていることによるものである（欧州においては、EN63000 として域内で活用されている）。

法人の特定と認証に関しては、サービス加入時に、公的な認証コード（国内においては法人番号、帝国 DB など、グローバルには DUNS など）を使い、サービス約款などとともに法人認証と認可を行う。なお、法人配下の組織及び利用者（個人）については、法人に任され、プラットフォームとしては認証・認可を必要としない（情報としては、アプリケーション層で管理される）。

CMP では、各国の化学物質規制への遵法判断を可能すると同時に、サーキュラーエコノミーに対応した情報連携基盤を構築すること、及び各社の海外にも展開されるサプライチェーンに対応するため、海外との連携、活用を視野に入れたシステムを構築することが企図されている。

基盤の構築に際しては、ウラノス・エコシステムのユースケースとして先行するサプライチェーン情報伝達（蓄電池 CFP・DD）ガイドラインに則ることで、公益 DPF 間の整合を図ると同時に、効率的かつ迅速な基盤構築を図っている。そのため、CMP としては、効率性の観点から、ウラノス・エコシステム上に複数のユースケースが運用された場合、そこで共通化されたトラスト認証システムが実装されることが望まれるとしている。



図●CMP におけるウラノス・エコシステムとの連携イメージ

表●化学物質管理のユースケースにおける Q1～Q4 のまとめ

Q. 1　連携対象となるデータ	
	✓　製品含有化学物質情報 ✓　活用されるリサイクル材、リユース部品情報
Q. 2　データ連携の場	
	✓　川上産業から川下産業に至るサプライチェーン。自動車・電機電子業界で国内 1 万社、海外数千を超える企業の参加が見込まれる。 ✓　海外システムとの連携、海外への CMP 展開
Q. 3　データに関わるリスク・不確実性	
	✓　化学物質、リサイクル材、リユース部品情報の信頼性。法規制対応となるためデータの信頼性が必要 ✓　海外システムとの連携 ✓　不特定多数の企業、データの扱い（将来課題）
Q. 4　リスクに対する対応策	
	✓　契約並びに IEC/ISO82474、IEC63000 準拠にて対応（現状） ✓　海外（特に東南アジア）へのシステム展開

3.5 鉄道のユースケース

ここでは、東日本旅客鉄道株式会社による、列車の遅れや在線位置などのリアルタイムデータの連携に係るユースケースを紹介する。

3.5.1 連携対象となるデータ

リアルタイムな列車の遅れを加味した列車の遅れ時間や在線位置などが連携対象となるデータである。

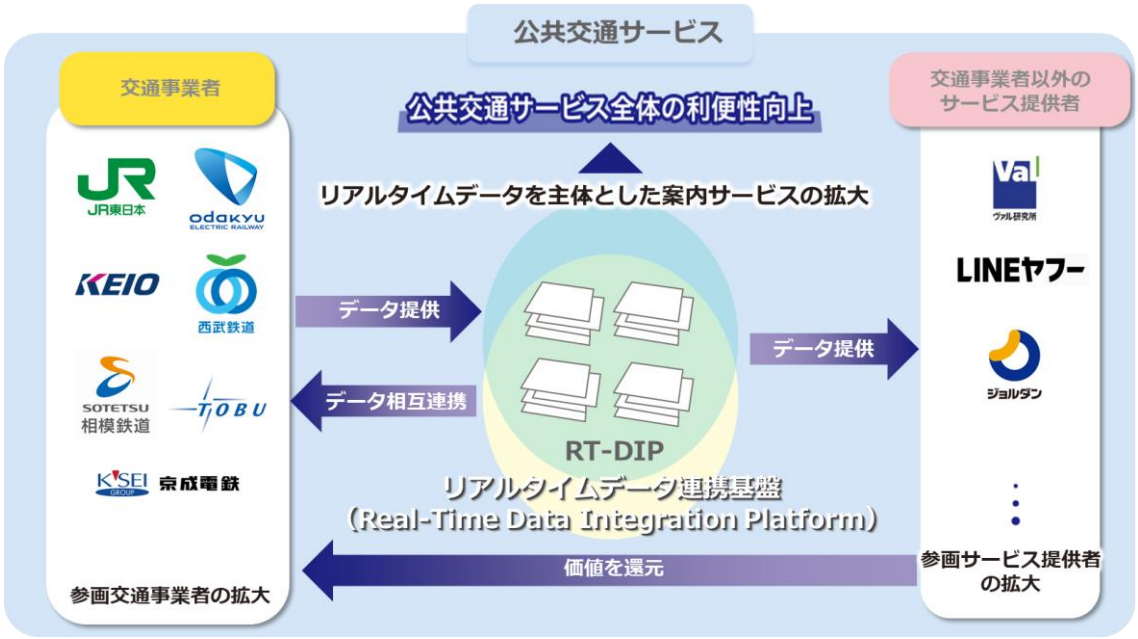
日本国内の移動の際、様々な交通手段、交通事業者を利用するため、様々な会社の交通事業者のデータが連携されている必要がある。各交通事業者からリアルタイムデータを各社フォーマットで受領し、統一フォーマットに生成している。

3.5.2 データ連携の場

RT-DIP（Real-Time Data Integration Platform）は、リアルタイムでデータをやり取りするための基盤であり、JR 東日本と各交通会社が規約を締結し、共同で運用している。2024 年 9 月時点で、JR 東日本を含む 8 つの鉄道事業者が参画している。

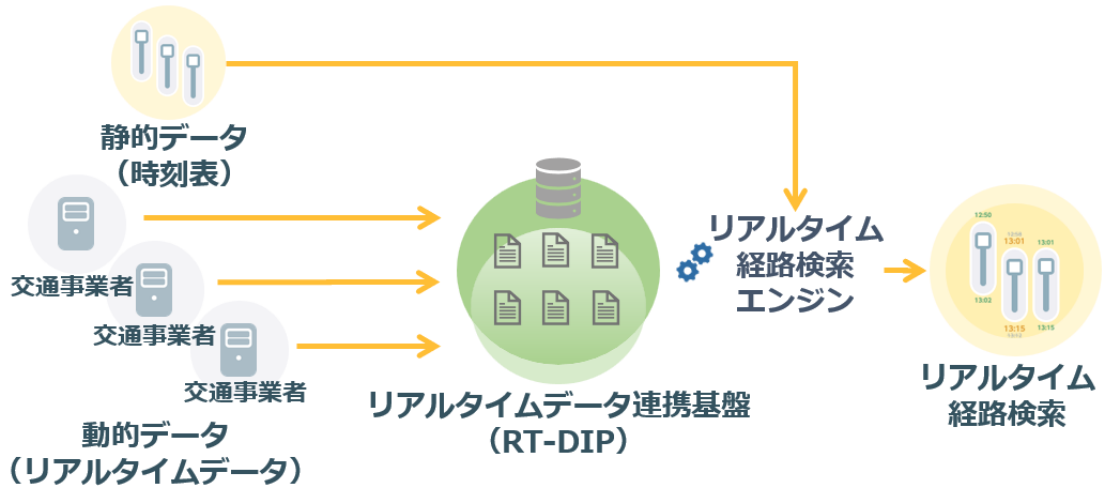
鉄道事業者は RT-DIP を通じて、自社のウェブサイトやアプリに乗換案内を掲載するほか、外部の乗換案内サービスへデータを提供することが可能となる。前者は無償、後者は有償の契約形態となっている。

これにより、サービス利用者は複数の鉄道事業者やバス事業者の運行状況を考慮した経路検索が可能となり、より正確で利便性の高い移動手段の選択ができるようになる。



図●RT-DIP の全体像

また、リアルタイム経路検索は静的データ（時刻表など通常のダイヤデータ）と動的データ（遅延情報などリアルタイムデータ）を組み合わせることで実現している。



図●リアルタイム経路検索を成立させるシステム構成

3.5.3　データに関わるリスク・不確実性

主に 2 つのリスクが存在する。

まず、データを提供する各社が相互に項目や形式を正しく理解せず、適切に活用できない可能性がある（リスク①）。データの統一性や互換性が確保されなければ、連携の効果が十分に発揮されない。

次に、ダイヤ改正などの変化に適切に対応できず、データ品質が低下するリスクがある（リスク②）。特に後者は、利用者に与える影響が大きく、誤ったデータが提供されることで電車の乗り遅れなどの不便が発生する可能性がある。

3.5.4　リスクに対する対応策

リスク①については、各社が提供する独自フォーマットのデータを適切に理解し、統一フォーマットへ変換した上で共通基盤に収容することで対応している。また、国際的なデータ標準である GTFS 形式も推奨されている。

リスク②については、移動関連データがデータ提供者などに共有される際、データ品質の担保に細心の注意を払うことでリスクを低減している。

表●鉄道のユースケースにおける Q1～Q4 のまとめ

Q. 1　連携対象となるデータ
✓　リアルタイムな列車の遅れ時間、在線位置など ✓　各交通事業者からリアルタイムデータを各社フォーマットで受領し、統一フォーマットに生成
Q. 2　データ連携の場
✓　鉄道事業社 8 社（2024 年 9 月時点）がデータ基盤を利用 ✓　各交通事業者と JR 東日本が規約を締結して運用
Q. 3　データに関わるリスク・不確実性
✓　提供する会社が相互にデータの項目、形式等を理解して活用できることが必要 ✓　ダイヤ改正などに伴う変化に対応し、データ品質が維持されることが重要
Q. 4　リスクに対する対応策
✓　各社独自フォーマットによるデータを理解して共通基盤に収容している。また、国際的なデータ標準である GTFS 形式も推奨されている ✓　移動関連データがデータ提供者などに共有される場合は適切なデータ扱いに配慮する

3.6 電力データのユースケース

ここでは、一般社団法人電力データ管理協会による、スマートメーターから得られる電力データの共有に係るユースケースを紹介する。

3.6.1 連携対象となるデータ

全国 8,000 万台のスマートメーターにおいて、30 分ごとに生成される電力使用・売電実績、電力取引の基礎となる電力データが連携対象となる。なお、データレイクの保存期間は 3 年となっている。

提供される電力データのうち、同意を得た個データは、実績把握や CO_2 排出量の算定（これらをサポートする事業者を含む）、省エネ診断、発電設備等の稼働把握や見守りなどに利用されている。また、統計は地域の経済動向把握や個データとの比較のために用いることができる。さらに、オーダーメイド統計は任意の母集団の設定や偏差の算出など自由度の高い調査が可能となっている。

利用会員名	提供サービス（報道・プレス等）
中部電力株式会社	電力データを分析してフレイルリスクの高い方を検知する自治体向けサービス
株式会社リバスタ	建設工事会社向けに、全国の工事現場のCO2排出量の算出を支援するサービス
ＥＮＥＣＨＡＮＧＥ株式会社	比較サイトにおいて正確な料金シミュレーションを提供するサービス
ヒラソル・エナジー株式会社	・太陽光発電所の買取・リパワリング、オンサイトPPA型太陽光発電所の設計、発電所の運営を効率化するためのDXツール開発、自社の電力データを希望するフォーマットで取得可能な「プレミアム電力データ提供サービス」
中部電力ミライズコネクト株式会社	・高齢者の住宅難民化の解消や賃貸物件の空室率の低減に向け、電力データを活用して入居者を見守るサービス ・太陽光発電状況と電力使用量のモニタリングサービスをローソンに提供
株式会社ビーマップ	・シニアや単身家族の健康を見守る３つ（電力データ、ベッドデバイス、Wi-Fi）の見守りサービス
東芝エネルギーシステムズ株式会社	・工場等の電力データを分析し、生産のピークシフトや節電の余地があるかを見極める電気の需給調整サービス
株式会社エナーバンク	・電力や脱炭素に関するデジタルコンシェルジュサービス　エネルギー調達や脱炭素支援サービスと連動
株式会社エネット	・AI分析を活用し三菱UFJ銀行全国約200施設でエネットのEnneteye®を活用した省エネアクションを推進
三井不動産レジデンシャル株式会社	・毎月のCO2削減量に応じてポイントを付与し、省エネ行動を推進する入居者向けアプリ
大和ハウス・アセットマネジメント株式会社	・運用委託を受けている賃貸物件一棟あたりの電気使用量からCO2排出量を測定、数値をもとに将来的に省エネ設備改修も検討
早稲田大学	・カーボンニュートラルなスマートシティの実現に向けた総合的なエネルギーマネジメントシステムの研究

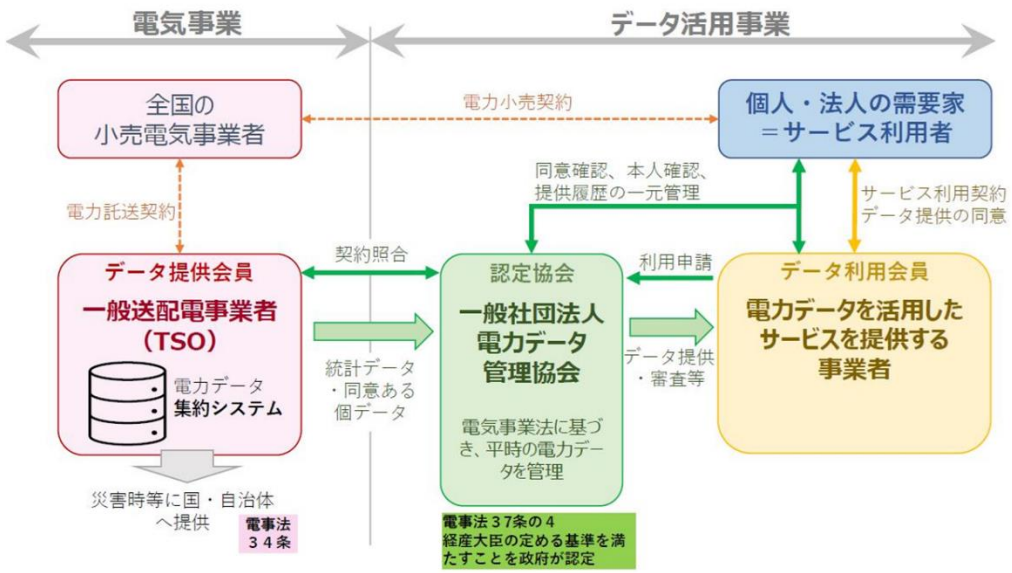
図●電力データの活用事例

3.6.2 データ連携の場

電気事業法では公正競争の観点から、一般送配電事業者（TSO）に電力データの目的外利用を禁止しているが、2020 年 6 月に電気事業法が改正され、個人情報の保護や適正な競争の確保を前提とした「認定協会制度」の下、電気事業者以外の事業者も含め、電力データの活用が可能となった。認定協会制度は、電気事業法第 37 条の 4 の規定に基づき、「個人情報保護（個人情報保護法）」及び「適正な競争関係の確保（電気事業法）」を前提としながら、安全に、適切な同意手続をもって電力データの第三者提供を担う専門機関を政府が認定するスキームである。

これを受け、データ利用者 7 社と TSO10 社により「一般社団法人電力データ管理協会」（以下「電管協」という。）が設置され、2022 年 6 月 30 日、同条に基づき、経済産業大臣より「認定電

気使用者情報利用者等協会」としての認定を取得した。具体的には、以下のようなスキームの下でデータの提供・利用が行われる。



図●認定協会制度に基づくデータの提供・利用スキーム

認定に当たっては、「電気事業法第 37 条の４の規定による認定電気使用者情報利用者等協会の認定の基準」を満たすことが要求されており、適正な同意手続やトレーサビリティ、データ取扱者のセキュリティ確保（ISMS・P マークの第三者認証）などの具体的な要求事項が定められている。

（電気事業法（昭和 39 年法律第 170 号）第 37 条の４）

（認定電気使用者情報利用者等協会の認定）

第三十七条の四　経済産業大臣は、経済産業省令で定めるところにより、電気使用者情報を利用しようとする者並びに前条第一項の規定により電気使用者情報を提供しようとする一般送配電事業者及び配電事業者（第二号において「電気使用者情報利用者等」という。）が設立した一般社団法人であつて、次に掲げる基準に適合すると認められるものを、その申請により、次条に規定する業務（以下この章において「情報利用等適正化業務」という。）を行う者として認定することができる。

一　社員（以下この章において「会員」という。）による電気使用者情報の利用及び提供の適正化を図ることにより電気供給事業者間の適正な競争関係の確保に資することを目的とすること。

二　電気使用者情報利用者等を会員に含む旨の定款の定めがあること。

三　情報利用等適正化業務の適確な実施のために必要な業務の方法を定めているものであること。

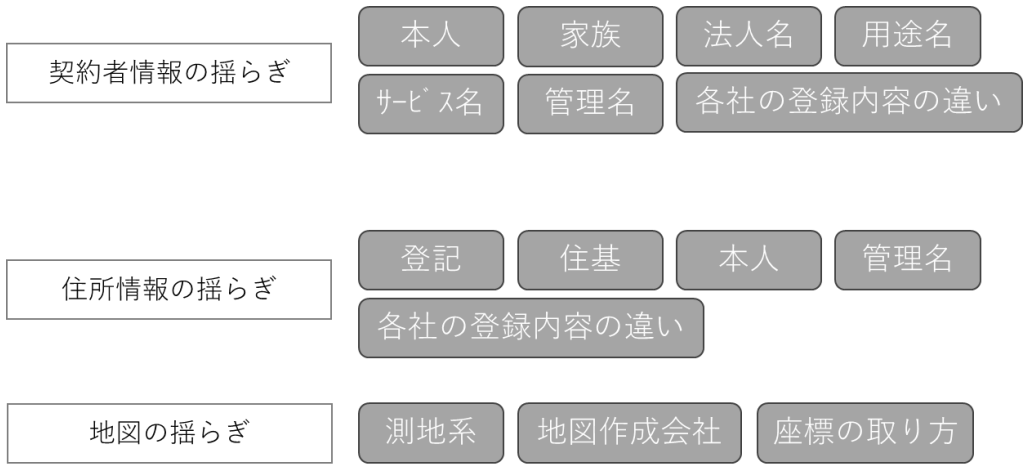
四　情報利用等適正化業務を適確に行うに足りる知識及び能力並びに財産的基礎を有するものであること。

3.6.3　データに関わるリスク・不確実性

先に述べたとおり、個データの提供に際しては同意取得が必要とされており、電管協から連携された同意申請者の情報と、一般送配電事業者において管理している契約者情報の同一性の確認は、一般送配電事業者において実施される。この確認に際して、主に情報の揺らぎや紐付けの困難性といった、供給・料金計算に直接関係がない部分での課題が存在している。

（情報の揺らぎに関する課題認識）

- 電気の場合、「供給地点特定番号」が分かっていれば、契約を一意に特定可能であるが、同意申請者と電力会社の台帳とで契約名義人が完全一致することは少ない
- 申請者と契約の突合に当たっては、名義、住所等の情報から判断するが、いずれも揺らぎや更新がなされていない情報が含まれており、同意申請者と契約者の同一性の確認には手間とコストを要している
- データ活用に際し位置情報を活用したい場合、管理者によって住所情報が異なっていたり、地図の違いや位置情報の設定の考え方が異なっていたりする点にも留意が必要

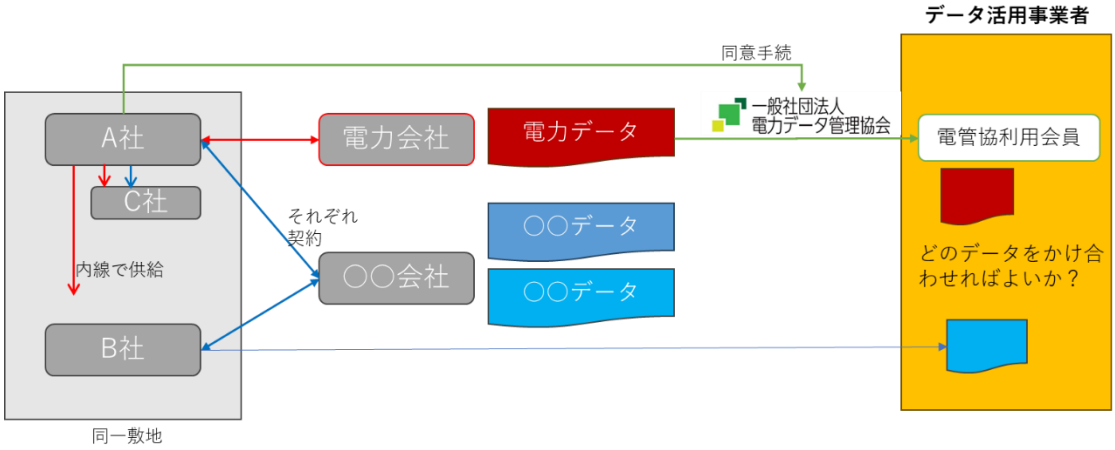


図●情報の揺らぎに係る内訳

（複数の契約情報の紐付けの難しさに係る課題認識）

- 同一の敷地や建物に複数の法人が入居していたり、契約者と実際の利用者が異なっていたり、電気とガスと水道と通信とで契約先が異なっていたり、管理会社が間に入っていたり、様々な契約形態がある
- また、外部との契約や供給に直接関係のない内線情報は当事者以外には流通し得ない（この場合ではＢやＣがＡから入手するしかない）ことについても、問合せが多い（内線の計量値を知

りたい等）



図●情報の紐づけの難しさの背景にある事業者間の関係性

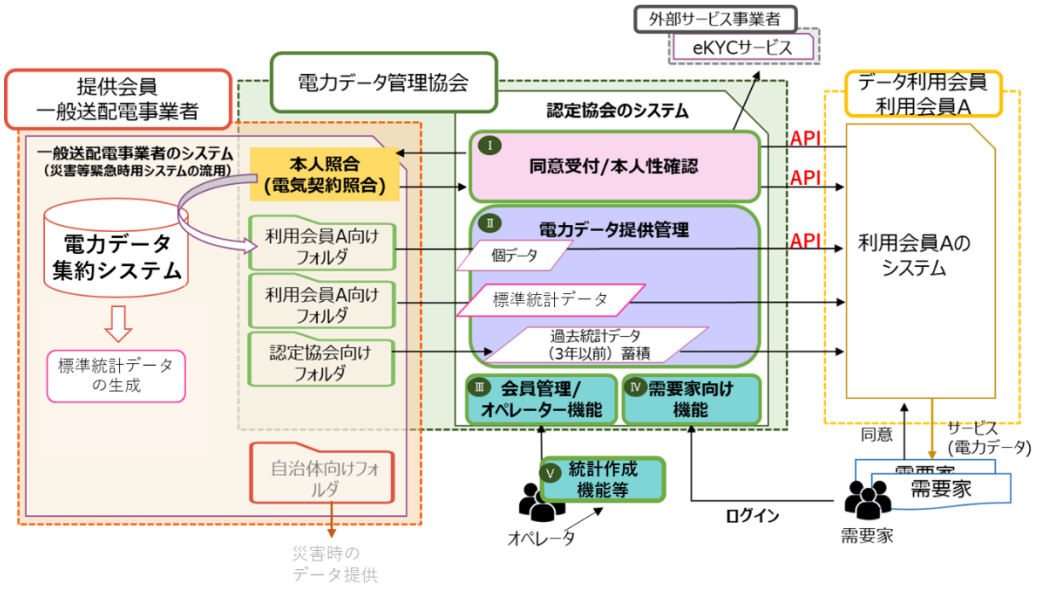
また、データの漏えい防止の観点から、外部からの攻撃に対するセキュリティの確保が課題として認識されている。

3.6.4　リスクに対する対応策

電力データを提供するシステムとしては、主に次のような機能を備えている。

（電力データを提供するシステムの主な機能）

- 個データを利用する場合は、同意申請手続及び個データの取得について、API を用いたシステム連携が必須（利用会員側での開発、又は構築済の他社システム）
- 標準統計データを利用する場合は原則 API、オーダーメイド統計の場合はストレージサービスによる提供となる
- システムの IF 定義や仕様は入会後に開示



図●電力データを提供するシステムの主な機能

データの漏えい防止の観点からは、電管協がトークンを停止すると利用会員はデータ取得できなくなるシステム構成としている。

また、個データの提供に際して取得が必要とされる同意に関しては、同意申請書類の正当性の目検確認（代表印、電子署名、委任状、代理権限表明書等）が行われており、同意申請者の本人性の確認は、電管協のシステムにおいて外部 eKYC サービスによって実施している。

表●電力データのユースケースにおける Q1～Q4 のまとめ

Q. 1　連携対象となるデータ
✓　全国 8000 万台のスマートメーターにおいて 30 分ごとに生成される電力使用・売電実績、電力取引の基礎となる電力データ ✓　データレイクの保存期間は 3 年
Q. 2　データ連携の場
✓　国の認定を受けた専門機関（電管協）を通じて、同協会の利用会員に対して、統計及び同意を得た個データを第三者提供可能、当該利用会員から契約者自身への開示も可能 ✓　なお、災害復旧等に必要な場合、全国の自治体は、同意なしに電力データを利用可能
Q. 3　データに関わるリスク・不確実性

	✓ 供給・料金計算に直接関係がない部分等のデータ精度に課題 ✓ 全国のデータを一括保存・提供する新たなシステムであり、当初想定できなかった課題の解消に数年を要す ✓ 申請側・電力会社の台帳いずれにも、契約情報の不備や揺らぎがあるため、対象の紐付けに手間とコストを要す ✓ 外部からの攻撃等のセキュリティリスク
Q.４ リスクに対する対応策	
	✓ 電力各社・電管協・利用会員のセキュリティが担保されたシステム間の API 連携で同意手続・電力データを授受 ✓ 利用目的ごと・地点ごと・提供先ごとの同意手続 ✓ 同意申請書類の正当性の目検確認（代表印、電子署名、委任状、代理権限表明書等） ✓ 電管協がトークンを停止すると利用会員はデータ取得できなくなるシステム構成

3.7 人流データのユースケース

ここでは、ソフトバンク株式会社による、携帯電話基地局から得られる位置情報を活用した人流統計データの共有に係るユースケース（商用化サービス事例）を紹介する。

3.7.1 連携対象となるデータ

携帯電話基地局から得られる位置情報等の自社人流データ（指定メッシュ区間での発着人数・滞在人口、交通施設の移動人数など）のほか、気象庁、国勢調査、道路交通量などの外部データが連携対象となる。

これらのデータの提供を内容とするサービスとして、例えば、基地局から得られる位置情報を利用し、人の移動・滞在情報を統計加工した上で、様々な分野・業界に提供するサービス「全国うごき統計」が既に商用化されている。

（「全国うごき統計」のデータの性質及びデータの提供先・用途）

- データの性質：提供データの価値として、次の３つの性質が位置付けられている
  - 網羅性：地理的範囲としては基地局が立地する範囲（日本全国）を、時間的範囲としては 24 時間 365 日を網羅したデータである
  - 機能性：人の移動・滞在情報について、移動経路及び交通手段まで分かるようなデータである

- 信頼性：高サンプルかつ統計データ補正がなされており、信頼性の確保されたデータである

・ データの提供先・用途：

- 商業・不動産：競合施設の商圏分析や交通量に応じた駐車場設営計画の策定、新規出店エリアの検討等の用途に用いられている
- 観光：観光地の周遊促進や渋滞対策、地域交通網の整備等の用途に用いられている
- 交通：新交通サービスの導入検討や道路の整備計画の策定、空港への二次交通改善等の用途に用いられている
- 防災・減災：災害時の避難ルート設計や防災備蓄計画への反映、帰宅困難者数の予測等の用途に用いられている

3.7.2 データ連携の場

携帯電話基地局から得られる位置情報等の自社人流データについては、秘匿処理／統計加工の上、契約先における特定のシステムに対してのみに限って提供され、当該特定のシステム間においてのみデータ連携が行われる。ただし、災害等の状況において公益性のある場合には、例外的に対価なしでデータの提供が行われている。

また、個人情報保護の観点から、プライバシーポリシー／携帯電話会社の顧客の同意にのっとった対応が行われている。

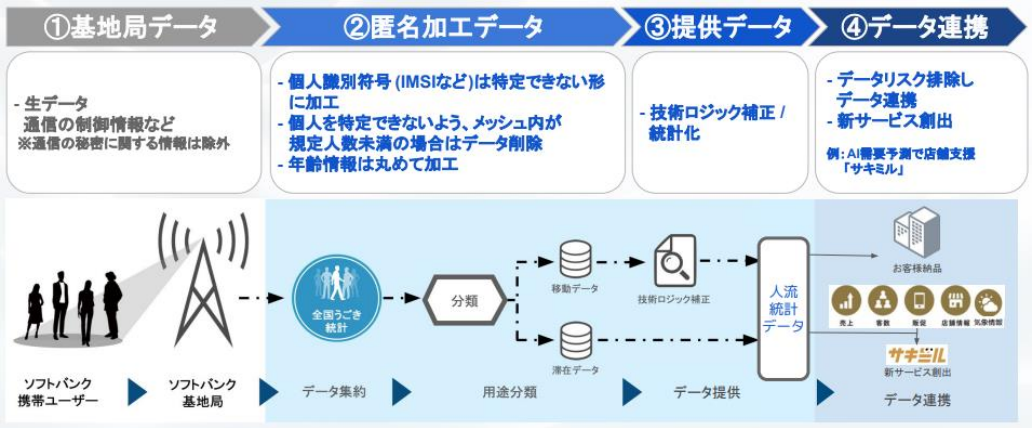
3.7.3 データに関わるリスク・不確実性

携帯電話基地局から得られる生データは個人を特定することができるデータであることから、そのデータのままでは個人が特定されるリスクが残ることとなる。

また、データの品質／信頼性についても、課題として認識されている。提供されるデータにはリードタイムが必要となっている。

3.7.4 リスクに対する対応策

先述のとおり、携帯電話基地局から得られる生データについては、秘匿処理／統計加工が行われる。個人識別符号等は、個人を特定できない形に加工するほか、個人を特定できないよう、メッシュ内が規定人数未満の場合にはデータを削除するという対応をとっている。具体的には、携帯電話基地局からデータの提供先までの間において、以下に示すようなプロセスでデータの秘匿処理／統計加工が行われる。



図●データの秘匿処理／統計加工プロセス

また、データの品質／信頼性に関しては、信頼性の高い他データとの掛け合わせにより統計補正を行うことで、統計加工の精度の向上を図っている。

表●人流データのユースケースにおける Q1～Q4 のまとめ

Q. 1　連携対象となるデータ	
	✓　携帯電話基地局から得られる自社人流データ ✓　気象庁、国勢調査、道路交通量などの外部データ
Q. 2　データ連携の場	
	✓　秘匿処理/統計加工の上、特定システム間で連携 ✓　個人情報保護、プライバシーポリシー/お客様同意にのっとった対応
Q. 3　データに関わるリスク・不確実性	
	(1)個人が特定されるリスク (2)データ品質/信頼性
Q. 4　リスクに対する対応策	
	(1)-1.個人識別符号など特定できない形に加工 (1)-2.個人を特定できないよう、メッシュ内が規定人数未満の場合はデータ削除 (2)　信頼性の高いデータとの掛け合わせにより統計加工の精度向上

3.8 スマートビルのユースケース

ここでは、ソフトバンク株式会社による、施設から得られるデータの共有・アジャイル・ガバナンスプラットフォームに係るユースケース（研究開発事例）を紹介する。

3.8.1 連携対象となるデータ

国や自治体等において管理されているシステムやインフラ等に設置されている監視カメラやセンサー等が収集したデータのほか、ロボット事業者やビル事業者の管理する、ロボット・ドローンの運航データ、LiDAR データ、ビル OS 等から提供されるエレベータ運行データ等が連携対象とされている。

これらのデータが、例えば大学の施設において、同じ基盤を用いて、ロボ運用や飲料の配送、施設警備、災害時個別支援、混雑予測等、様々なサービスを提供する事業者に対して提供される。

3.8.2 データ連携の場

マルチステークホルダーのデータを同じ基盤上で共有／連携するものであるため、データの共有／連携は、事業者及び自治体・私有地・ビル等でのルール／規約といったソフトローにのっとって行われる。ルール／規約の内容は、データの取扱いや共有範囲・粒度に関して定めるものである。

また、データの提供先となる事業者は、基盤の運営者（実証事業においては大学法人）が認可した事業者・サービスに限定される。

3.8.3 データに関わるリスク・不確実性

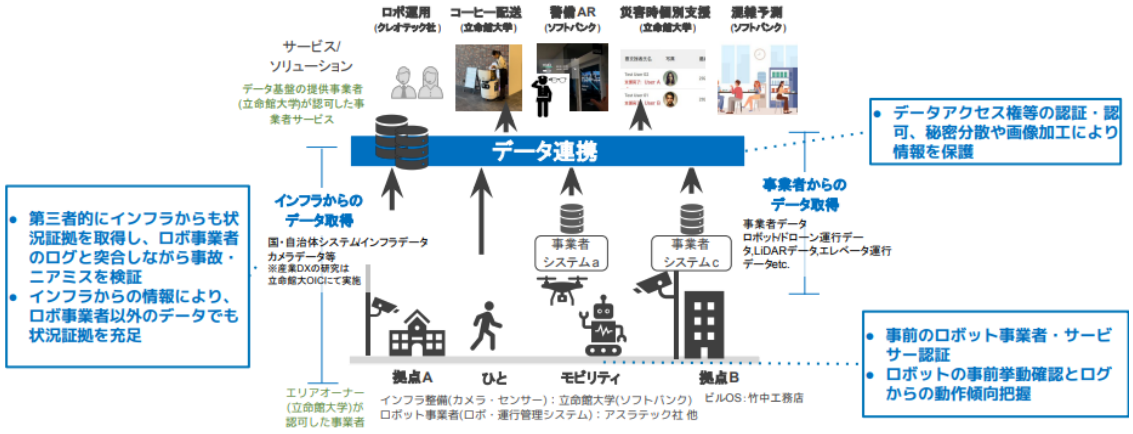
事業者から正しいデータが提供されない／できない可能性があるという点において、データの真正性の確保に対するリスクが存在している。

データの機密性の確保に対するリスクも課題として認識されている。

3.8.4 リスクに対する対応策

事業者から正しいデータが提供されない／できない可能性があるという点に関しては、第三者的にインフラからも状況証拠を取得し、ロボット事業者のログと突合しながら事故・ニアミスを検証したり、あるいは、ロボットの事前挙動確認を行い、ログから動作傾向を把握したりすることで対応を試みている。また制度的な対応として、事前のロボット事業者・サービサーの認証を行うことにより、事業者による正しいデータの提供を担保することも試みている。データの保持者がデータを提供しない場合には、インフラからの情報により、ロボット事業者以外のデータでも状況証拠を充足することで対応を試みている。

データの機密性の確保に関しては、データアクセス権等の認証・認可を行うほか、秘密分散や画像加工によって情報を保護することで対応を試みている。



図●データの真正性・機密性の確保に向けた対応策

表●スマートビルのユースケースにおける Q1～Q4 のまとめ

Q. 1　連携対象となるデータ	
	✓　監視カメラ等（←国/自治体システム/インフラ） ✓　ロボット/ドローン運行データ,LiDAR データ,エレベータ運行データ等 （←ロボット事業者,ビルシステム事業者 etc.）
Q. 2　データ連携の場	
	✓　事業者及び自治体・私有地・ビル等でのルール規約に基づきマルチステークホルダーのデータを PF 上で共有/連携
Q. 3　データに関わるリスク・不確実性	
	(1)データの真正性 – 事業者から正しいデータが提供されない/できない可能性 (2)データの機密性
Q. 4　リスクに対する対応策	
	(1)-1.事前のロボット事業者・サービサー認証 (1)-2.ロボットの事前挙動確認とログからの動作傾向把握 (1)-3.第三者的にインフラからも状況証拠を取得し、ロボ事業者のログと突合しながら事故・ニアミスを検証 (2)　データアクセス権等の認証・認可、秘密分散や画像加工により情報を保護

4. 諸外国における産業データ連携事例とトラスト

第 3 章では、国内の取組を中心に各分野のデータ連携のユースケースについて、トラストに対するニーズ等を整理した。他方で国際的な企業間のデータ連携も想定されるため、国際的な相互運用性確保等の観点から、本章では、産業データ連携の代表的な事例として Catena-X における取組を紹介する。また、トラストフレームワークを整備している代表的な諸外国として、シンガポール、カナダ、英国における事例を紹介する。

4.1 Catena-X における取組

欧州における産業データ連携に関して、現在すでに商用運用されている代表的なデータスペースが Catena-X データスペースである。本研究会の第 2 回において、Catena-X e.V.の Kraemer 氏、土屋氏より、「欧州における自動車業界向け産業横断データ連携事例」と題して、Catena-X における取組に関してご発表をいただいた。本節では、主に両名の御発表内容を基にしつつ、Catena-X におけるガバナンス（中でも、両名の発表において言及のあったアプリケーションの認定制度と Gaia-X トラストフレームワークに関する内容）およびアーキテクチャの両側面から、トラスト確保のために実施されている取組を紹介する。

4.1.1 ガバナンス

Catena-X データスペースにおいては、Catena-X Association が、共通の運用ルールや通信方式、各ユースケースごとのデータモデルの標準仕様などを Catena-X Standard として定めており、HP にて公開している[11]。また、Eclipse Foundation において Catena-X データスペースに実装される様々な機能が Tractus-X と呼ばれるオープンソースソフトウェア群として開発されている。Catena-X Standard に準拠したデータスペースの運用は、欧州だけでなく世界各国に運営事業者を設立して運用できるルールになっており、現時点では、2023 年に設立された Confinity-X 社が運用している。Catena-X が目指すビジョンを実現するためのアプリケーションは、T-Systems、Siemens、SAP などの企業から Catena-X Standard に準拠したソフトウェアサービスとして提供されている。

Catena-X データスペースで各種のサービスを提供するためには、Catena-X Association が定める Standard に準拠してデータ主権や相互運用性、セキュリティの基準を満たすソフトウェアを準備し、認定（Certificate）を取得する必要がある。認定にあたっては、中立的な認定機関による審査を行う制度が整備されており、認定プロセスの中では、データの構造の適合性やトラスト確保のための仕組みが実装されていることが確認されることになっている。運用サービスを行う Cofinity-X が契約ユー

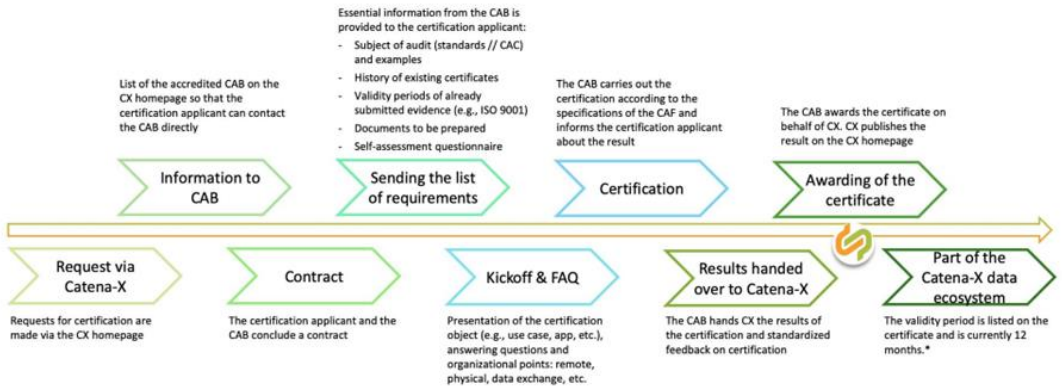
[11] https://catena-x.academy/librarian/

ザー向けにマーケットプレイスでビジネスアプリケーションやイネーブルメントサービスのソフトウェアを紹介するのは、認定を受けたソフトウェアのみである。

ビジネスアプリケーション等の認定プロセスは「Request via Catena-X」、「Information to CAB」、「Contract」、「Sending the list of requirements」、「Kickoff & FAQ」、「Certification」、「Results handed over to Catena-X」、「Awarding of the certificate」、「Part of the Catena-X data ecosystem」の 9 段階に分かれている。各プロセスの内容は以下の通り。

（Catena-X におけるビジネスアプリケーション等の認定プロセス）

- **Request via Catena-X**：Catena-X の HP を通じて認証の申請を行う
- **Information to CAB**：認証機関である CAB に連絡を行う。CAB リストは Catena-X の HP に掲載されている
- **Contract**：CAB と申請者が契約を締結する
- **Sending the list of requirements**：CAB から認証審査における情報が提供される。提供される情報としては、監査対象（基準など）と例、既存証明書の履歴、既に提出された証憑の有効期限（ISO 9001 など）、準備すべき書類、自己評価アンケート、がある
- **Kickoff & FOQ**：認証対象（ユースケースやアプリケーションなど）の紹介等を行う
- **Certification**： CAB が CAF の仕様に従って審査を実施し、結果を申請者に通知する
- **Results handed over to Catena-X**：CAB が審査結果を Catena-X に提出する
- **Awarding of the certificate**： CAB が Catena-X の代理で証明書を授与し、Catena-X が結果を HP に掲載する
- **Part of the Catena-X data ecosystem**：Catena-X に参加する。証明書の有効期限は 12 か月



図●Catena-X におけるアプリケーションの認定プロセス

4.1.2 アーキテクチャ

（1）基本的な設計思想とその背景

Catena-X の構想が立ち上がった当初から、「特定の支配的なプレーヤーにあらゆる情報が集中するという事態を避けること」「データが安全・セキュアに扱われること、企業秘密が適切に保護されることを担保すること」「データの所有者がデータに対するコントロールを適切に及ぼし続けることができるようにすること（データ主権）」が、基本的な思想として重視されてきた。

また、Catena-X データスペースの国際的な展開にあたっては、国・地域に応じて適用される法律や用いられる標準、登記等の ID に係るシステムが異なるため、そのような国・地域ごとに異なるものを許容・吸収しつつ、その一つ上の層は国際標準に則って、トラスト（相手の本人性やデータの真正性を確認し、改ざん・ねつ造を防ぐこと）およびデータ主権（データをいつ、誰が利用できるかをデータ提供者が自らコントロールすること）を確保した運営を行うことを目指している。実際に、NTTCom、富士通や T-Systems などが、上記のような運営を実現するための技術実証を 2024 年に開始しているほか、2024 年 4 月 22 日に IPA-Catena-X 間で締結された MOU に基づいて、自動車業界向けデータ共有における相互運用に向けた取組を進めてきた。

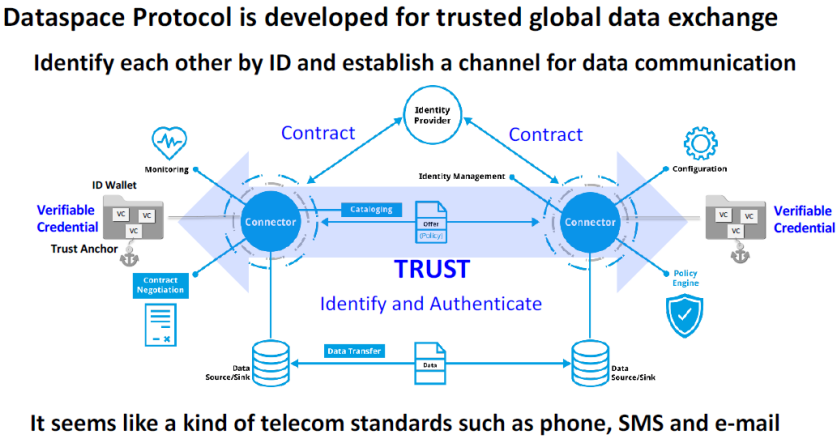
特に、Catena-X が、一つのデータプラットフォームにデータが保管されることなく、データの提供者以外の者がデータに勝手にアクセスすることができない分散型アーキテクチャを採用する背景としては、データ連携基盤が目指す目的の達成（例えば地球規模でのサーキュラーエコノミーの達成等）のためには、データの利用や越境に関するルールの異なる国にいる企業同士が法律と契約にもとづいて安心安全にデータ交換できるようにすること、広く世界中の事業者が参加できること、特定の 1 社のベンダに依存しないような仕組みにすることで、様々な事業者が参加できるようにするという狙いもある。

（2）データ連携の仕組み

Catena-X データスペースでは、Gaia-X のトラストフレームワークに則ってデータ連携に際してのトラスト確保を図っている。なお、2024 年段階で Catena-X におけるトラスト確保の仕組みの中で、最初にトラストアンカーを担ったのは（独 T-Systems[12]）であった。

分散型データスペースにおける実際のデータ連携は、以下の図のような仕組みで行われている。

[12] https://www.t-systems.com/de/en/insights/newsroom/expert-blogs/catena-x-anchors-trust-on-t-systems-668920



図●分散型データスペースにおける実際のデータ連携の仕組み[13]

ここでは、コネクタ（Connecter）が、データスペースを構成する主要なデータ交換の出入口となる。コネクタは、企業の ID を提供する機関（アイデンティティプロバイダ）より ID 交付を受け、その上で、コネクタ同士において相手先がどのような企業であるのか交渉・確認し、その後に実際のデータ交換に入ることになる。

また、実際のデータ交換は上記のコネクタ同士のやり取りとは別のところ（Data Plane と呼ばれる通信ルート）で行われ、他の者を介することなく、データ連携の相手方との間で直接行われる。Catena-X データスペースでは、参加者はウォレットを持ち、ウォレットに Verifiable Credential（VC）を格納して、データ連携時にはこれを提示することにより、属性情報に係る検証が行われることになる。

Catena-X では、今後普及していくことが見込まれる新しい分散型トラスト技術を、産業データ流通の領域でも採用し運用開始している。実際に、先に述べた属性情報の検証に際して用いられる VC は、発行・検証が分散型で行われる新しいトラスト技術である。

4.2 諸外国におけるトラストフレームワークの事例

本研究会の第２回において、濱口構成員より、「諸外国におけるデータ連携と求められるトラスト」と題して、諸外国における取組に関してご発表いただいた。本節では、濱口構成員の御発表内容を基にしつつ、シンガポール、カナダ、英国での主要なトラストフレームワークとして、Trusted Data Sharing Framework 、Pan-Canadian Trust Framework 、Digital Identity and Attribute

[13] IDSA の Web サイトより（第３回トラスト研究会資料３p. 15）

Framework の概要を紹介する。また、トラストフレームワークのほかに、英国におけるデータスペースの設計・運営を行う組織である Icebreaker One の取り組みも併せて紹介する。

4.2.1 シンガポールにおける取組（Trusted Data Sharing Framework）

（1）概要

シンガポールは、2019 年に Trusted Data Sharing Framework（TDSF）を策定し、デジタル経済の促進及び「スマートネーション」構想の支援を目的として導入した。TDSF は、政府が発行するガイドラインの位置付けであり、法的拘束力を持つ規制や制度ではなく、データ共有を円滑に進めるための指針を示すものである。本フレームワークは、Info-communications Media Development Authority（IMDA）が策定し、Personal Data Protection Commission（PDPC）と共同で発表された。

（2）目的

TDSF の目的は以下の 4 点である。

1. 組織間のデータ共有促進
2. データ共有の課題解決
3. 新製品・サービス開発の促進
4. 消費者の信頼構築

（3）フレームワークの構成要素

TDSF は以下の 4 つのパートで構成されている。このフレームワークにより一連のトラストテクノロジとベースラインの「共通データ共有言語」を確立し、信頼できるデータ共有パートナーシップを確立するための幅広い考慮事項を理解するための体系的なアプローチを確立することで、企業を支援することを想定している[14]。

表●TDSF の全体像

パート	概要	推奨読者

[14] IMDA TRUSTED, DATA SHARING FRAMEWORK
https://www.imda.gov.sg/-/media/imda/files/programme/data-collaborative-programme/trusted-data-sharing-framework.pdf

Data Sharing Strategy データ共有戦略	組織が、どのようなデータを共有するのが有益か、データをどのように評価できるか、データの共有に使用できる様々な取決めやモデルを理解することを意図	・ データ共有プロセスに関わる全ての主要な意思決定者、利害関係者 ・ 社内ユニット/ユーザー
Legal and Regulatory Considerations 法的、規制上の考慮事項	組織が、データ共有に関するコンプライアンス要件及び当事者間で信頼できるデータ共有を可能にする法的関係の構築方法を理解することを意図	・ プロジェクトを推進するユーザー ・ データを収集・管理・利用する事業部門 ・ 技術/リスク/コンプライアンスに関するアドバイザリーチーム
Technical and Organisation Considerations 技術的、組織的考慮事項	組織が、データを他の組織に移動するための技術的な考慮事項とメカニズムを理解することを意図	・ プロジェクトを推進するユーザー ・ データを収集・管理・利用する事業部門 ・ 技術/リスク/コンプライアンスに関するアドバイザリーチーム
Operationalising Data Sharing データ共有の運用化	組織が、データ共有が行われた後の追加の検討事項を理解することを意図	・ プロジェクトを推進するユーザー ・ 技術/リスク/コンプライアンスに関するアドバイザリーチーム

また、TDSF では、「データ」は個人データとビジネスデータの両方を対象としており、特に商業部門及び非政府部門での使用を意図した産業界向けのガイドラインとして設計されている。データ共有はデータ資産の移動を伴うことが多いため、各当事者が責任を持ってデータ資産を取り扱い、管理できることを確立することが重要であるとして、TDSF には 6 つのトラスト原則が導入されている。

（６つのトラスト原則）

- 透明性
  - データ共有に関わる全ての関係者が、データ共有パートナーシップを成功させるために必要な全ての情報を利用できるようにすること
- アクセス可能性
  - 当事者が必要なときに必要なデータにアクセスできること
- 標準化
  - データ共有パートナーシップに一貫した法的、技術的、その他の手段を適用すること
- 公平性と倫理性

- 個人データ保護や技術的・セキュリティ的な基準、あるいは規制上の要件を満たすことにとどまらないこと
- 最初の設計段階から、データ共有システムとフレームワークの作成と使用に倫理基準を適用すること

・ 説明責任

- データ保護法及びデータ共有パートナーシップに固有のその他の規則を遵守し、各当事者が強固なガバナンス構造を有し、従業員がデータの取扱いに責任を持つことを推進する企業文化を持っていることを示すこと

・ セキュリティとデータの完全性

- データ共有のための安全な環境を可能にするために、情報とデータを安全に保護し、保護するように設計された対策と仕組みを実施すること

（4）**認証の仕組み**

上記（３）で照会したフレームワークへの適合性への評価の枠組みや認証制度は存在しない。

4.2.2 カナダにおける取組（Pan-Canadian Trust Framework）

（1）**概要**

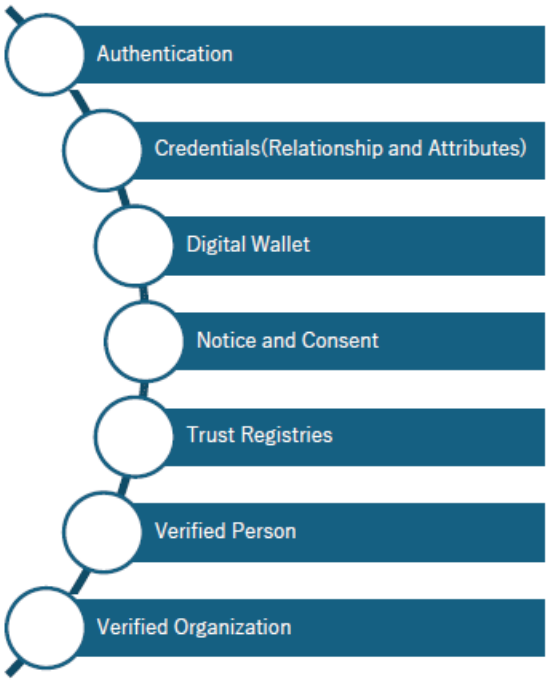
Pan-Canadian Trust Framework は、官民で構成される非営利組織である Digital ID & Authentication Council of Canada（DIACC）により開発された。PCTF は、デジタルアイデンティティエコシステムの信頼性を確保するために、2016 年に概要が発表され、2019 年に最初のバージョンがリリースされた。

（2）**目的**

PCTF は、カナダのデジタルアイデンティティ管理における原則や基準、デジタル ID の作成、管理、提供に係る一連のプロセスなどを定義しており、デジタル ID に関係する公共・民間のステークホルダー、研究者などに参照されることを目的としている。

（3）**フレームワークの構成要素**

PCTF は、７つのトラステッドコンポーネントで構成されており、それぞれに対して４段階（LoA１～４）のレベルに応じた要件が定められている。



図●PCTF の 7 つのコンポーネント

特にデータ連携に関連すると想定されるコンポーネントの要件は次のとおりである。

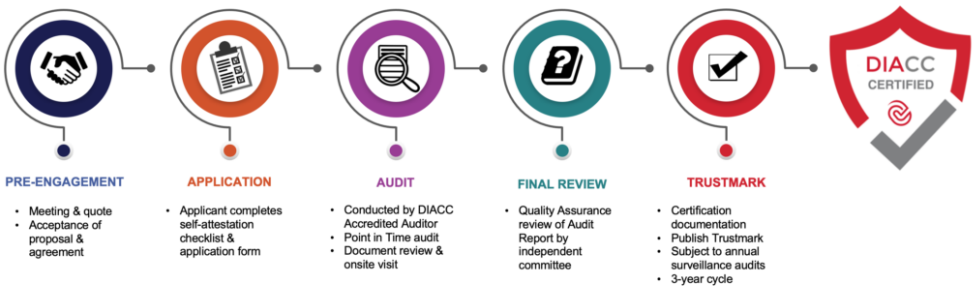
表●データ連携に関連するコンポーネントとその要件

コンポーネント	概要	要件
Authentication	デジタル ID の検証	信頼されるプロセス（クレデンシャル発行、認証、セッション開始/終了、クレデンシャルの一時停止/回復/保守/失効）、役割（認証及びクレデンシャル・サービス・プロバイダ）、リスク及び提案される保護手段、ユースケース（Digital Wallet における VC、バイオメトリクス認証など）、及び特定のトラストレベルに対する適合要件を定義
Credentials	認証に用いる情報全般	信頼される関係プロセス（定義、宣言、支持、検証、否認）及び信頼される属性プロセス （定義、バインド、維持、失効）、及びリスク評価を含む、決定された保証レベルでのクレデンシャルのライフサイクル管理の適合性に関する要件

Digital Wallet	デジタルIDと関連資産を格納するデジタルウォレット	信頼関係（申請者-発行者-保有者-検証者-リポジトリ）、信頼されたプロセス（ウォレットのインスタンス化とセキュリティ、クレデンシャルの管理と使用、同意の管理）、役割、リスクリポジトリと軽減戦略、及びコンフォーマンス要件を規定
Trust Registries	デジタル ID エコシステムの参加者が、他のエコシステム参加者が信頼できることを検証する手段	トラスト・レジストリに登録される参加者には、発行者、検証者、ウォレットプロバイダが含まれる。トラスト・レジストリのガバナンス、運用、登録、及び認証管理に関する適合性要件を規定
Verified Organization	組織の身元確認	組織の身元を確立及び検証するためのプロセスを定義し、適合性基準を規定。組織が適切に検証されていることを保証するプロセスや、組織の信頼できるデジタル表現を作成するプロセスなどを含む

（4）認証の仕組み

ISO/IEC 17065 に基づいて、PCTF の基準への適合性を認証するスキームが整備され、2022 年より運用が開始された[15]。認証に係る組織として、認定準備アドバイザー、DIACC 認定監査人、独立レビュー委員会が存在する。現時点で認証を受けているサービスは 2 つである。



図●PCTF への適合性の認証フロー

（認証に係る組織）

- 認定準備アドバイザー

[15] https://diacc.ca/certification-program/

- 認証を希望する組織が準備を進める際に支援を提供する専門家
- 利益相反となるため、DIACC 認定監査人はアドバイザーになれない

・ DIACC 認定監査人
- ISO/IEC 17020 要件に基づくプロセスを経て認定された専門家
- PCTF に対する監査を実施する能力、経験、資格を有す

・ 独立レビュー委員会
- 国際的なアイデンティティ、監査、コンプライアンス、情報セキュリティの専門家で構成されるボランティア組織
- DIACC 認定監査人の監査結果の品質レビューを実施する

4.2.3 英国における取組

4.2.3.1 Digital Identity and Attribute Framework

（1）**概要**

Digital Identity and Attribute Framework（DIAF）は、新技術を使用して人々がより迅速かつ容易に本人確認できるようにすることを目的に Department for Digital, Culture, Media & Sport（DCMS）が策定を進めているフレームワークである。2021 年 8 月に α 版が公開され、その後継続的に更新が図られ、2022 年 6 月以降は β 版として作業が進められている。直近では、2024 年 11 月にβ版の v0.4 がリリースされ、技術的な要素として Wallet と VC が制度的に取り込まれた。今後、2025 年から v0.4 の認証プロセスが開始され、年次レビューと更新が実施される。2025 年以降、データ保護及びデジタル情報法案（ECHR Memorandum）によって、法的根拠が確立される予定である。

（2）**目的**

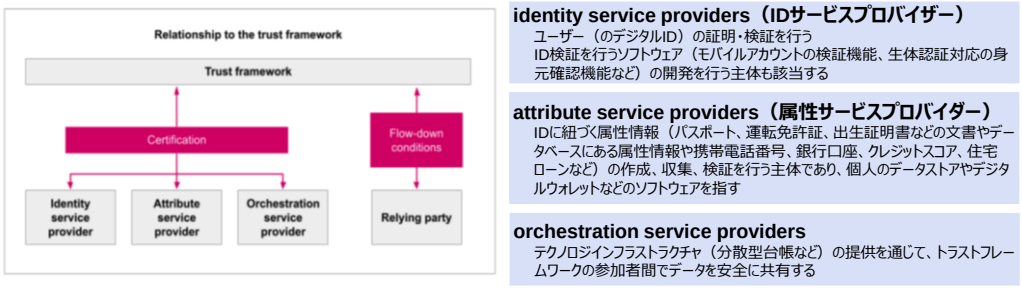
DIAF の目的は以下の 3 点である。

1. デジタル ID サービスの信頼性の向上
2. イノベーションと投資の促進
3. 安全なサービス開発と展開の保証

（3）**フレームワークの構成要素**

デジタル ID と属性情報のプロバイダ及びトラストフレームワークの参加者でデータが安全に共有することを保証するテクノロジーインフラストラクチャを提供する Orchestration service provider を定義し、それぞれトラストフレームに対して認定を取得する必要が示されている。また、ユーザーからデ

ジタル ID、属性情報を受け取り、検証結果を基にサービス提供を行う Relying Party については、トラストフレームに対して認定される必要はないものの、市場のセキュリティを確保するために、トラストフレームワークの関係組織からのフローダウン条件に従う必要が示されている。



図●トラストフレームワークと各ステークホルダーの関係

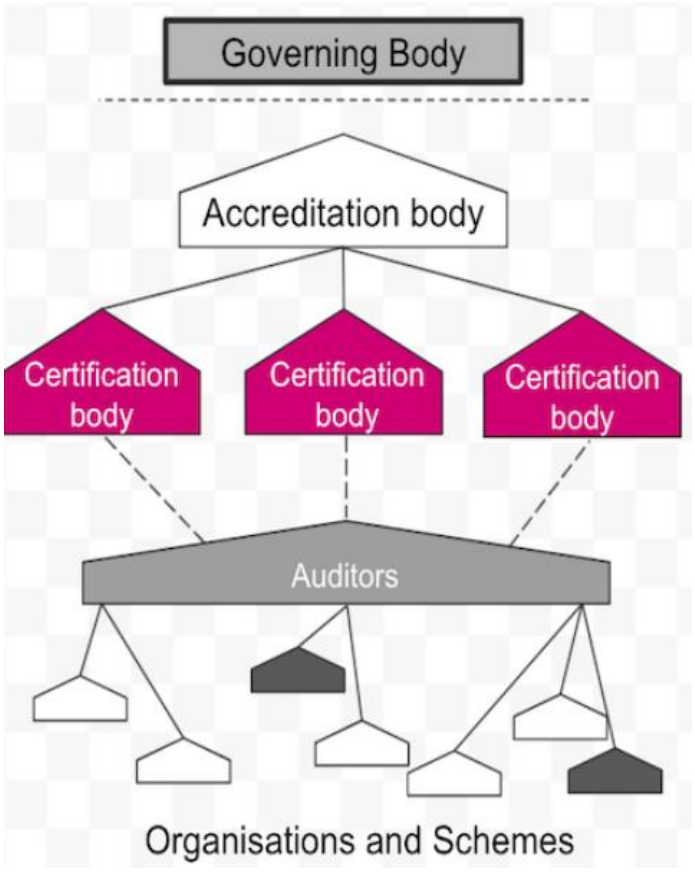
（4）認証の仕組み

組織がフレームワークのルールと基準を遵守していることを証明するための厳格な認証プロセスが設けられている。これは、利用者がデジタル ID サービスを信頼できるようにするために不可欠であり、ISO/IEC 17065 等の国際的な認証プロセスに準拠した Accredited Certification の仕組みを導入している。この認証プロセスにより、組織は第三者機関による独立した評価を受け、フレームワークの要件を満たしていることが確認される。その結果、適格と判断された組織には Trust Mark が付与され、信頼性の証明となる。認証プロセスは以下の 5 つのステップで構成される。

1. Governing Body（統括機関）による基準の設定
   - DIAF の運営を担う Governing Body である DCMS が、デジタル ID 及び属性管理の基準、ルール、認証の範囲を定める
   - この基準に準拠することで、組織が信頼できるサービスを提供していることが保証される
2. Accreditation Body（認定機関）による認証機関の認定
   - UKAS（United Kingdom Accreditation Service）が、政府により指定された Accreditation Body として、Certification Body を認定する
   - これにより、認証機関はフレームワークの基準に基づいて組織を評価・認証する権限を得る
3. Certification Body（認証機関）による組織の評価と認証
   - フレームワークに準拠した組織やスキーム（デジタル ID プロバイダーなど）は、認定された Certification Body によって審査される
   - これにより、各組織がフレームワークの要件を満たしていることが確認される
4. Auditors（監査人）による適合性評価

- 資格を持つ Auditors が、企業や認証機関に対して監査を行い、全ての要件が満たされていることを確認する
- 監査結果は、企業と認証機関にフィードバックされ、必要な改善点が指摘される

5. Trust Mark の付与
   - 認証を取得した組織には、Governing Body が Trust Mark を付与する
   - Trust Mark を持つ組織は、公式に DIAF の基準を満たしていると認められ、利用者からの信頼性が向上する



図●DIAF の認証プロセス[16]

4.2.3.2 **Icebreaker One**

（1）**概要**

Icebreaker One（IB1）は、2020 年の世界経済フォーラム（ダボス会議）で発表された非

[16] https://www.gov.uk/government/consultations/digital-identity-and-attributes-consultation/digital-identity-and-attributes-consultation

営利組織であり、気候変動対策の意思決定を支えるデータ連携基盤の構築をミッションとしている。エネルギー、金融、水管理、輸送、建築環境、農業など複数のセクターにおいて、分散する産業データや環境データを統合し、企業や政府などのユーザーに活用可能な形で提供することを目指す。

IB1 は、オープンソース技術とオープンデータの活用を重視し、データ共有のオープン標準やフレームワークを開発することで、組織間の安全かつ円滑なデータ共有を促進する。これにより、セクター間を横断したデータ連携を強化し、「ネットゼロのためのデータ基盤」の構築を進めている。

（2）組織構造[17,18]

IB1 は、独立した非営利団体として運営されている。収入源はプロジェクトごとの助成金や企業・団体からのメンバーシップ費用、寄付金などであり、メンバーシップ制度により活動資金を調達しつつ、中立性を保つため営利を目的としない運用を徹底している。70 以上の政府・公共機関、民間企業、学術機関、非営利団体・シンクタンク等の多様なセクターのメンバーが参加している。

表●IB1 のメンバーシップ料金

組織の規模（年間売上）	月額会費
大企業（3,600 万£～）	5,000£
中規模企業（1,000 万£～3,600 万£）	3,000£
小規模企業（200 万£～1,000 万£）	500£
マイクロ企業/スタートアップ（～200 万£）	250£
公共部門（例：地方公共団体）	250£
エコシステムサポーター（例：業界団体）	0
政策パートナー（例：政府、規制当局）	要相談

（3）主要な活動

IB1 の主要な取組として、Icebreaking Process と Core Trust Framework の提供に２つについて紹介する。

1）Icebreaking Process[19]

IB1 が提唱するデータ共有ルール共創のためのプロセスである。Icebreaking プロセスでは、まず

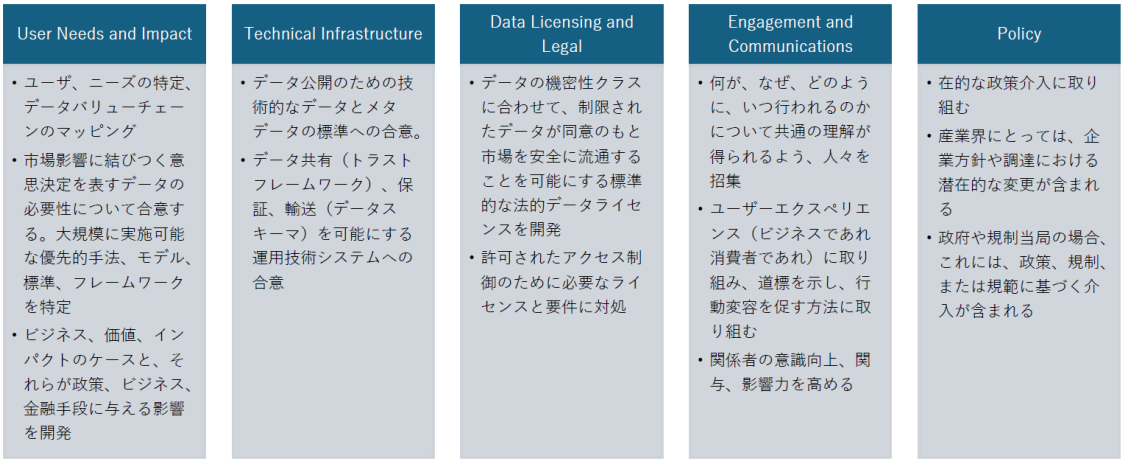
[17] https://ib1.org/2019/09/24/opening-icebreaker-one-at-un-hq/#:~:text=We%20are%20delighted%20to%20announce,cases%29%20over%20the%20coming%20months

[18] https://energy.icebreakerone.org/join/#:~:text=Following%20extensive%20industry%20consultation%2C%20via, Pricing%20is%20as%20detailed%20below

[19] https://ib1.org/icebreaking/#:~:text=IB1%20helps%20you%20implement%20data,specific%20needs

関係者を集めて重要なユースケースを特定し、その価値や影響を検討する。具体的には、以下のプロセスに沿って検討する。

1. ユーザーニーズと影響の特定
   - ➢ どのようなデータが必要かを明確にし、そのデータが持つ市場価値を評価する
2. 技術インフラの確立
   - ➢ データ共有に必要な技術的標準やシステム要件を定義する
3. データライセンシングと法的整備
   - ➢ データ共有を法的に適切な形で進めるためのルールを策定する
4. コミュニケーションとエンゲージメント
   - ➢ データ提供者、ユーザー、規制当局との調整を行い、関係者の意識向上を図る
5. 政策や規制への適合
   - ➢ 政府や規制当局と連携し、適切な政策を提案・導入する
   - ➢ このプロセスにより、組織は安全かつ効率的なデータ共有を実現できる



図●Icebreaking Process[20]

このプロセスにおいて、IB1 は中立的なファシリテーター兼事務局として機能し、産官学からなるステアリンググループ（運営委員会）及び最大五つのアドバイザリーグループ（技術・法務・ポリシー等の専門分野別）を組成してプロジェクトを推進する。強固なガバナンスの下、関係者全員が参加したコーデザイン（共同設計）により、データ共有のためのルールブックとなる「スキーム」を作成する。スキームには、特定のユースケースの定義や、実装に必要な法的・技術的・ポリシー的取決め、コミュニケーション方策などが盛り込まれる。Icebreaking Process は、技術（API やデータ標準）と

[20] https://www.meti.go.jp/policy/mono_info_service/digital_architecture/ouranos/ouranos_trust/241217/siryo4.pdf

非技術（契約やポリシー）の両面から課題を洗い出し、合意形成されたルールを文書化する一連の手順と言える。このようにして策定された「スキーム」は、後述の Trust Framework を通じて実社会で機能するルールへと実装される。

2）**Core Trust Framework**[21]

IB1 が提供するデータ共有のトラスト基盤となる枠組みである。上記の Icebreaking Process で策定された「スキーム」を実際に運用可能にするため、組織間の信頼関係と共通ルールを技術的・契約的に担保する仕組みが Trust Framework である。中でも Core Trust Framework は全ての参加組織に共通する基本的な約束事やサービスを定めた基盤となっており、個別のデータ共有スキームに参加するためのエントリーポイントとして機能する。CTF を土台に、エネルギーや水道など各セクターに特化した Trust Framework が構築される。CTF に参加する組織は、IB1 のメンバーシップに加入した上で CTF の利用規約に同意する必要があり、これによって一度の契約で複数のスキームへの参加資格を得られるよう工夫されている。CTF の主なサービス内容は以下のとおりである。

（CTF の主なサービス内容）

- 認定組織の登録簿
  - Trust Framework に参加している組織のリストを公開したレジストリ。これによりデータ共有相手の組織が信頼できる（身元確認済み・規約順守）ことを確認できる
- 共通のデータインフラ定義
  - データ共有に必要な保証プロセス（Assurance）やデータ機密性クラス（Data Sensitivity Classes）といった共通の原則・基準を策定・維持する
  - CTF はまた、「オープンデータ公開のベストプラクティス」等の原則も提示し、参加組織が機械可読かつ信頼できる形でデータを公開することを促す
- オープンネットゼロ (Open Net Zero)カタログ
  - 公開データの検索カタログとして、気候・環境に関連するデータセットの索引を提供する
  - 例えば OpenNetZero.org では、ネットゼロ実現に役立つ様々なデータ（エネルギー効率や炭素排出データ等）を検索可能にしており、データの存在と所在を可視化することで活用を促進する

4.3 総括

本章では、産業データ連携におけるトラスト確保の国際的な動向について、欧州における Catena-X

[21] https://ib1.org/tf/ctf/#:~:text=%26%20Conditions%20%28using%20this%20form%29,org

の取組及び諸外国のトラストフレームワークの事例（シンガポール、カナダ、英国）を整理した。

各国のトラスト確保のアプローチは一様ではなく、それぞれの制度や産業構造に応じた異なる枠組みが構築されていることが明らかになった。特に、Catena-X の事例は、産業データ連携におけるトラストの確保に関する欧州のアプローチを示しており、分散型アーキテクチャを採用しつつ、業界標準の整備とガバナンスの強化を進めることで、サプライチェーン全体の透明性と相互運用性を確保する仕組みを構築している。

一方、トラストフレームワークの作成主体や制度化の有無や運用方法には違いを確認できた。例えば、シンガポールの TDSF については、政府がデータ共有のガイドラインとして整備しており、制度化には至っていないが、業界におけるデータ共有の指針として活用されている。他方で、カナダの PCTF については、官民で構成される非営利組織がデジタルアイデンティティの相互運用性を確保するためのフレームワークとして整備しており、認証制度を通じた具体的な適用が進められている。

英国では、政府主導の DIAF と、業界主導の IB1 という異なるアプローチが併存している。DIAF は政府が運営するデジタルアイデンティティの枠組みとして、認証プロセスの整備が進められており、法制度と連携する形で運用が進められている。一方、IB1 は、エネルギーなどの特定分野におけるデータ共有のためのトラストフレームワークとして機能しており、業界主導の信頼確保の仕組みを提供している。

これらの事例を比較すると、トラストの確保に向けた取組は、一律に決まった形があるわけではなく、各国の制度や産業環境に応じた異なるアプローチが存在することが確認できる。今後、産業データ連携の国際的な相互運用性を確保するためには、各国のトラストに対する考え方やアプローチの違いを理解し、トラストを確立する上で必要な要素を整理することが重要である。

5. 産業データ連携におけるトラスト確保に向けた分析と進め方

本章では、第 3 章及び第 4 章の内容を基に、産業データ連携におけるトラスト確保に向けた分析方法の結果の整理方法とウラノス・エコシステムにおける取組の方向性について記載する。

5.1 データ連携の「場」に関する分析（Q1、Q2 関係）

本節では、第 3 章において紹介した事例全体に関して、連携対象とされるデータや適用される場の性質について整理する。

まず、Q1 及び Q2 に沿って、データ連携が生じる「場」の分析を行った。まずは、連携対象とされるデータに関する分析が必要だが、本研究会で対象とした事例については、自動車サプライチェーンにおけるデータ連携（3.1, 3.2）や電力データの連携（3.6 ）、人流データの連携（3.7 ）のように、個人を特定することができるデータ、あるいはこれを基にして作成されるデータを取り扱うユースケースがみられた。また、連携されるデータの営業秘密等への該当性を意識している事例もみられた。

そして、適用される場の分析に当たっては、法令等、官による場の設計の存否による、官民の役割分担に留意する必要がある。具体的には、上述のようなデータの性質によって遵守が要求される、個人情報保護・営業秘密保護に係る法令のほか、データ連携のための基盤利用のために参加者と基盤の間で締結する契約、さらにはデータ連携の当事者間における契約等を想定しているユースケースがみられた。また、製品含有化学物質情報の連携（3.4 ）のように、連携されるデータの品質について、既に業界内で通用している法令や国際標準等に準拠することが求められているユースケースもみられた。さらには、電池パスポート（3.2）や製品含有化学物質情報の連携（3.4 ）、電力データの連携（3.6 ）のように、情報の連携そのものの許否・要否が、法令によって規定されているといったユースケースもみられた。

5.2 データに対するリスクと対処に関する分析（Q3、Q4 関係）

本節では、第 3 章において紹介したユースケース全体に対して、データに関わるリスク・不確実性及びそれに対して検討・実施している方策について、整理する。

5.1 で分析した、各ユースケースにおいて連携対象とされるデータや適用される場の性質を考慮し想定され得る一般的なリスク及び対応策のうち、トラストに関係するものは以下にまとめられた。

- 参加者の実在性・本人性に係るリスク
  - 権限のない者のデータ連携への参加やなりすましのリスク。対応策としては、例えば参加者の識別・認証のための仕組み・ルールの実装が想定される。
- データの真正性や改ざんに係るリスク

- 内容に誤りのあるデータが流通するリスク。対応策としては、例えば電子署名やブロックチェーン・スマートコントラクト等の技術実装による改ざん防止等が想定される。

・ 個人情報保護に係るリスク
  - 国内外における個人情報保護法制上要求される同意取得等への対応ができず、基盤やその参加者が法令遵守できないリスク。対応策としては、例えば同意の取得状況等の追跡が可能な仕組みの実装等が想定される。

・ 営業秘密等保護に係るリスク
  - 営業秘密等、データ提供者において一部ないし全部の開示を希望しないデータが開示されてしまうリスク。対応策としては、例えばデータ提供者において開示を希望しないデータの秘匿処理や統計加工の適用、開示先及び開示範囲を制御できる仕組みの実装等が想定される。

・ 目的外利用に係るリスク
  - データ提供者が認めていない目的・用途によってデータが利用されてしまうリスク。対応策としては、例えばデータ利用規約による統制等が想定される。

5.3 各事例から得られた内容とその整理

5.2 における分析を踏まえ、トラストを必要とする要素として、大きく「事業者」「データそのもの」「その他（連携基盤等）」の３つに区分した。

5.3.1 事業者（主体の真正性・実在性）に関するリスク

・ 事業者（主体の真正性・実在性）に関するリスクは、様々なユースケースにおいて、共通して存在するリスクであり、海外連携を視野にした場合、事業者認証や身元確認は対外的にも求められ得るものである。本研究会で紹介されたユースケースにおいては、人手による確認によって対処している事例があった。

5.3.2 データそのものに関するリスク

・ データそのものに関するリスクは、データの精度や品質は分野問わず課題とされるが、求められる精度や品質の尺度は分野に依存する傾向がある。また、事業者以外の主体（例：製品）を識別するIDも主体に関するデータとして、信頼性の確保が課題とされる。

5.3.3 連携基盤等に関するリスク

・ その他のリスクとして、データ共有先での取扱い等が課題となる場合もある。

5.4 ウラノス・エコシステムにおけるトラストの考え方、あり方

本節では、5.3 で分析したリスクに対して、ウラノス・エコシステムにおけるユースケース拡大等を行う際のトラストに対する基本的な考え方を示す。

まず、以下の点を考慮しながら、「場」の分析及びそれに基づくリスクの明確化を行う。

- 「場」に作用する法令等のルール、官民の役割分担（データ連携基盤における法令の適用範囲、官による場の設計存否等）
- 「場」の参加者間の合意形成を担う主体やその形成手法（プラットフォーム主体の有無、エンドユーザーの視点、参加者が結ぶ契約や合意の状況等）、国際標準の有無
- 「場」の範囲（１つのデータ連携基盤内で議論を完結するのか、それともデータ連携基盤間の接続やデータスペースをまたいだ連携が行われるのか、国外との連携を想定するか等）
- 「場」の拡大（参加者数の増加や連携範囲の拡大等の規模）

そして、明確化されたリスクに対して、トラストの確保を含めた手段での解決策を検討する。データそのものに関するリスクや、連携基盤等に関するリスクへの対応については、各事例に応じて、それぞれに適用される場が要求する水準が存在しているため、これに応えるための手段は、各事例の設計・運用において議論・対処することが必要となる。

他方で、事業者（主体の真正性・実在性）に関するリスクへの対応としては、5.3.1 で述べたように様々なユースケースに共通して存在するリスクであることを踏まえると、官の情報を基にしたトラスト確保が分野横断的に有効となる可能性があると考えられる。官の情報を元に確認がなされた事業者認証サービスの事例としてデジタル庁 G ビズ ID[22]が挙げられる。なお、それぞれの「場」において事業者に関するリスクやその対応に対して、これを上回る要求がある場合は、追加的な対処が必要となる。

[22] G ビズ ID は、デジタル庁が運用する法人・個人事業主向け共通認証サービスである。事業者は G ビズ ID を取得することで複数の行政手続システムに１つの ID・パスワードでログイン可能となる。G ビズ ID プライムは、事業者の代表者情報の確認が行われた上で発行される。

6. 終わりに

企業・業界を横断したデータの利活用の促進を通じ、官民協調で企業・産業競争力強化を目指す「ウラノス・エコシステム」でのデータ連携におけるトラストについて、本研究会ではユースケースや国外の取組事例の収集・分析に基づいてトラストの考え方・在り方を整理した。データ連携の「場」の分析を通じてリスクや求められる対応を明らかにした上で、それぞれの「場」で求められる要素や水準に応じて必要な取組を推進するべきであると整理した。また、今回分析した事例において共通的な要求が存在するものとして、データ連携を行う主体（事業者）の真正性・実在性が挙げられ、官の情報を基にしたトラスト確保が分野横断的に有効となる可能性があることが示された。

各ユースケースの創出が今後蓄積されていく中で、データ連携におけるトラストについての将来的論点としては、ユースケース間連携におけるトラストの確立、相互運用性の確保やスケーラビリティのある拡大に有用なアーキテクチャ・共通コンポーネント等の整備、複数の海外データスペースとの連携等が考えられる。また、データ連携のトラスト確立の推進に向けては、上述したリスクやその対処において、既存のトラストに関する取組や制度も含めた様々な手段や技術が存在する中で、官民それぞれの取組が求められると考えられる。

信頼できるデータ連携やエコシステムによって、より多くの事業者が産業データ連携の活用、それを通じた産業競争力の向上に貢献できるよう、今後も「ウラノス・エコシステム」の取組を推進していく。

構成員名簿

座長	江崎 浩	東京大学 情報理工学系研究科 教授
構成員	伊藤 健一	東日本旅客鉄道株式会社 マーケティング本部 戦略・プラットフォーム部門 MaaS ユニット ユニットリーダー
	入江 直彦	ロボット革命・産業 IoT イニシアティブ協議会 WG1 共同主査
	工藤 郁子	大阪大学 社会技術共創研究センター 特任准教授
	境野 哲	一般社団法人日本経済団体連合会 産業データスペ―ス検討会 委員
	丹波 廣寅	ソフトバンク株式会社 テクノロジーユニット統括 データ基盤戦略本部 執行役員本部長
	手塚 悟	慶應義塾大学 グローバルリサーチインスティテュート 特任教授
	濵口 総志	株式会社 Maximax 代表
	藤井 達人	株式会社みずほフィナンシャルグループ 執行役員 デジタル企画部 部長
	藤原 輝嘉	一般社団法人自動車・蓄電池トレーサビリティ推進センター 代表理事
	古田 清人	ＣＭＰタスクフォース リーダー
	松本 泰	日本ネットワークセキュリティ協会 フェロー
	眞野 浩	一般社団法人データ社会推進協議会 専務理事／事務局長
	満塩 尚史	順天堂大学 健康データサイエンス学部 准教授
	安井 威人	一般社団法人電力データ管理協会 業務執行理事　事務局長
	吉田 理重	一般社団法人デジタルトラスト協議会 理事兼事務局長

オブザーバー名簿

内閣官房内閣サイバーセキュリティセンター総括戦略ユニット

デジタル庁国民向けサービスグループデータ戦略・企業間取引班

デジタル庁デジタル社会共通機能グループトラスト政策班

総務省サイバーセキュリティ統括官室

総務省情報流通行政局地域通信振興課デジタル経済推進室

経済産業省製造産業局総務課ＤＸチーム

経済産業省製造産業局自動車課

経済産業省イノベーション・環境局基準認証政策課

経済産業省イノベーション・環境局ＧＸグループ資源循環経済課

経済産業省商務情報政策局サイバーセキュリティ課

経済産業省商務情報政策局電池産業課

経済産業省通商政策局通商戦略課

経済産業省通商政策局貿易振興課

経済産業省資源エネルギー庁電力・ガス事業部電力産業・市場室

国土交通省鉄道局総務課企画室

国立研究開発法人新エネルギー・産業技術総合開発機構

独立行政法人情報処理推進機構

一般社団法人電子情報技術産業協会

一般社団法人日本情報システムユーザー協会

一般財団法人日本情報経済社会推進協会

日本認定機関協議会

本研究会の開催実績

第 1 回（2024 年 11 月 20 日）

議事

1. 開会
2. 事務局資料説明
3. 藤原構成員説明（欧州における自動車業界向け産業横断データ連携事例）
4. 事務局からの論点提起
5. 自由討議
6. 総括、今後の予定

第 2 回（2024 年 12 月 17 日）

議題

1. 開会
2. 事務局資料説明
3. Kraemer 様・土屋様説明（欧州における自動車業界向け産業横断データ連携事例）
4. 濱口構成員（諸外国におけるデータ連携と求められるトラスト）
5. 事務局からの論点提起
6. 自由討議
7. 総括、今後の予定

第 3 回（2025 年 1 月 31 日）

議題

1. 開会
2. 事務局資料説明
3. 藤原構成員説明（自動車・蓄電池分野における今後のユースケースを想定したトラスト検討）
4. 古田構成員説明（CMP 構想ならびにトラストの考え方について）
5. 伊藤構成員説明（JR 東日本におけるデータ連携のユースケース）
6. 安井構成員説明（電力データの第三者提供スキームについて）
7. 丹波構成員代理折原様説明（ソフトバンクの取り組みご紹介）
8. デジタル庁説明（法人共通認証基盤（G ビズ ID）について）
9. 事務局からの論点提起
10. 各構成員発言
11. 総括、今後の予定

第 4 回（2025 年 3 月 5 日）

議題

・ 報告書（案）の議論