# The Ouranos Ecosystem Trust Study Group Report

## March 2025
## Ministry of Economy, Trade and Industry

**(This English translation is provided for reference purposes only.
The Japanese version is the original and shall prevail in case of any discrepancy.)**

# Contents

## Executive Summary

Background and Purpose

This report outlines the concept and approach of 'trust' that is essential for promoting data sharing in a secure and trustworthy manner within Ouranos Ecosystem, which is being promoted by the Ministry of Economy, Trade and Industry (METI). The primary intended readers are a wide range of stakeholders involved in industrial data sharing.

Analysis Method and Target Use Cases

In this study group, we defined 'trust'[1] as 'the state in which one believes that the other party will not betray expectations,' in response to risks such as the entry of fraudulent businesses (e.g., non-qualified entities, spoofing) and the inclusion of inaccurate data (e.g., lacking or low quality data, data tampering), arising from the expansion of industrial data sharing. We then analyzed the required trust and other factors using the Data Management Framework (DMF) for eight domestic use cases (batteries, automotive LCA, battery passports, chemical substance management, railways, electricity, people flow data, and smart buildings). Additionally, we examined international business data sharing, reviewing leading examples from Europe, Singapore, Canada, and the UK.

Analysis Results

As a result of the analysis, the main risks associated with data sharing were organized into the following three categories:

1. Risks Related to Entities (Authenticity and Identity Verification)
2. Risks Related to Data Itself
3. Risks Related to Data Integration Platform and Other Factors

The risk related to entities is a common risk across all use cases, and it was suggested that establishing trust based on government information could be effective across various fields. On the other hand, the risks related to 'data itself' and 'sharing platforms and other factors.' should be addressed individually based on the requirements and levels requested by each domain[2] and should be discussed and dealt with within each use case and its design.

Future Challenges and Issues

Based on the above, future issues regarding trust in data sharing include the establishment of

[1] Refer to Section 5.2 for the difference between ‘trust’ and ‘trustworthiness’.

[2] For details, refer to Sections 2.2.2 and 5.1 .

trust in cross-use case sharing, the development of useful architectures and common components that ensure interoperability and scalability, and sharing with multiple overseas data spaces.

# 1. Introduction

## 1.1 Background of Industrial Data Sharing and Ouranos Ecosystem

METI is promoting the realization of DFFT (Data Free Flow with Trust) by integrating multiple systems to facilitate the use of data across businesses and industries, thereby advancing data, system, and business sharing. This initiative aims to enhance the competitiveness of companies and industries through public-private collaboration, and it is being promoted under the name "Ouranos Ecosystem". Ouranos Ecosystem is linked to key cabinet decisions, such as the "Grand Design and Action Plan for a New Form of Capitalism", the "Basic Policy on Economic and Fiscal Management and Reform", and the "Priority Plan for the Realization of a Digital Society" (all of which were approved in June 2024), positioning it as a critical policy to be advanced as part of the government's unified approach.

Currently, Ouranos Ecosystem is expanding and creating use cases in order to establish areas of sharing that enable the integration of all necessary data, services, and business activities for economic activities. Among these, one of the leading use cases is the management of traceability across the automotive and battery industries. In May 2023, the Digital Architecture and Design Center (DADC) of the Information-technology Promotion Agency (IPA) published the “Guidelines on Data Integration Mechanisms in Supply Chains[3] Version alpha (for Battery CFP/DD)”. Following the start of the development of the data integration platform, in May 2024, the Automotive and Battery Traceability Center (ABtC), an incorporated association, began providing traceability services. In September of the same year, ABtC obtained the first certification under METI’s newly established "Certification of Interoperable Data Infrastructure Management Entity (CIDIME)[4]" which externally assesses the operator’s trustworthiness.

## 1.2 Purpose of the Study Group

As seen in Section 1.1, the creation and expansion of use cases within Ouranos Ecosystem are currently being promoted. However, increase in the number of businesses participating in data sharing and the expansion of use cases also introduce uncertain elements and risks, such as the entry of fraudulent businesses and the risk of inaccurate data being mixed in. To achieve secure and trustworthy data sharing and utilization, it is essential to establish ‘trust,’ which ensures the

[3] IPA, "Guidelines on Data Integration Mechanisms in Supply Chains (Battery CFP/DD)," accessed February 3, 2025, https://www.ipa.go.jp/en/digital/architecture-guidelines/scdata-guidline-en.html

[4] METI, "Certification of Interoperable Data Infrastructure Management Entity," accessed February 3, 2025, https://www.ipa.go.jp/digital/dx/dpf-nintei.html

trustworthiness of both the data itself and the stakeholders involved. In this context, ‘trust’ refers to the belief that the other party will not betray expectations. Ensuring trustworthiness is one approach to converting uncertain elements into acceptable risks and will also contribute to the expansion of data sharing.

However, the elements and levels of trustworthiness required differ depending on the use case and the nature of the data. It is important to consider the balance with the needs of the user companies that will actually engage in joint data use and utilization in various situations. Therefore, it is necessary to organize the concept of trustworthiness in a way that is aligned with use cases, needs, and costs.

From this perspective, this study group was convened to organize the requirements of trustworthiness while considering the balance with user needs, in order to promote industrial data sharing in a secure and trustworthy manner, driven by use cases.

In the industry, discussions about industrial data sharing and data governance are gaining momentum. Looking at recent developments, on October 15, 2024, the Japan Business Federation (Keidanren) served as the secretariat for discussions on the construction of industrial data spaces, and "Towards the Construction of Industrial Data Spaces[5]" was published. Additionally, on October 17 of the same month, the Digital Policy Forum Japan (DPFJ), the Digital Society Alliance (DSA), and the Japan Digital Trust Forum (JDTF) jointly published "Policy Proposal for Promoting the Data Governance Strategy[6]".

This report outlines the content and discussions from the ” The Ouranos Ecosystem Trust Study Group”, which was held in four sessions between November 2024 and March 2025, as well as the concept and approach to trust within Ouranos Ecosystem at the time of this study group. The content of this report is intended for a wide range of stakeholders involved in industrial data sharing, including businesses engaged in establishing data sharing, system developers supporting these efforts, and businesses that provide or utilize data. It is intended to serve as a reference when considering trust and related risks in industrial data sharing.

---

5 Keidanren, " Towards the Construction of Industrial Data Spaces " accessed February 3, 2025, https://www.keidanren.or.jp/en/policy/2024/073.html

6 Digital Policy Forum Japan (DPFJ), "Policy Proposal for Promoting the Data Governance Strategy," accessed February 3, 2025, https://prtimes.jp/main/html/rd/p/000000009.000131931.html

## 2. Method for Organizing Requirements of Trustworthiness Based on Use Cases

### 2.1 Framework for Analyzing Trust in this study groups

As mentioned earlier, the purpose of this study group is to organize requirements of trustworthiness, while balancing needs to promote industrial data sharing driven by use cases. When organizing trust driven by use cases in each industry, it is necessary to arrange the data subject to data sharing and the regulations or terms related to the handling of that data, and to clarify the uncertainties (risks) that will be addressed by trust. In this process, we referenced the DMF (Data Management Framework), which involves modeling data management and risk analysis.

### 2.2 Overview of DMF

#### 2.2.1 Background of DMF Formulation

In Japan, the realization of a super-smart society, known as "Society 5.0," which aims to balance economic development with the social issue resolution, is being proposed by highly integrating cyberspace and physical space. This society aims to provide products and services that precisely meet diverse needs. In "Society 5.0," it is expected that the value creation process will become more flexible and dynamic. However, it has also been pointed out that the integration of cyberspace and physical space will increase the threat of cyberattacks.

To address this, METI organized the overall security measures for "Society 5.0" and compiled examples of security measures that industries can utilize. In April 2019, METI established the "Cyber-Physical Security Framework (CPSF).[7]" CPSF adopts a three-layer structure to clarify the foundation of trust in the value creation process within "Society 5.0.", organizing the industrial society into these three layers. In the third layer (connections in cyberspace), where industrial data sharing occurs, the focus is placed on the reliability of the data itself. To implement comprehensive security measures, risks must be identified throughout the entire data lifecycle, emphasizing the establishment of trust and risk reduction among stakeholders.

Therefore, in April 2022, METI established DMF to visualize the status of data throughout its lifecycle, identify risks, and implement appropriate measures to secure data security

[7] METI, "Cyber-Physical Security Framework," accessed February 3, 2025, https://www.meti.go.jp/policy/netsecurity/wg1/cpsf.html

through proper data management, which makes it possible to ensure the necessary actions to secure that data[8].

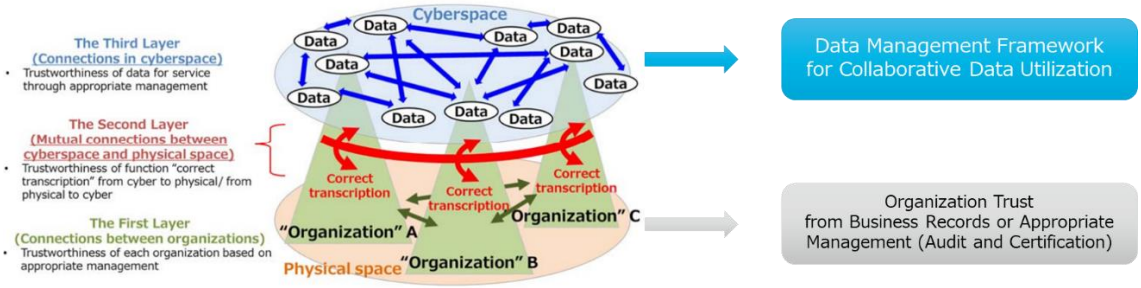



Figure 2-1 CPSF Three-Layer Structure Model

### 2.2.2 Modeling of Data Management

In DMF, data management is defined as "managing the processes during which data properties change due to events in the domains throughout the life cycle". It is organized as a model consisting of three mutually influencing elements: "events", "domains" and "properties". The definitions of these three elements are as follows:

- Events: The flow from the generation and acquisition of data to its disposal.
- Domains: The rules and regulations governing the handling of data.
  Examples include various laws (e.g., personal information, cross-border transfer regulations, intellectual property, export controls) and platform usage terms.
- Properties: The set of characteristics of data, including requirements from the "domains" data rights holders, and recipients of disclosures, among others.

Through this modeling, the state of the data becomes visualized, making it easier for stakeholders to share understanding. This is expected to lead to the implementation of appropriate data management across all stakeholders.

### 2.2.3 Risk Analysis Procedure

In the DMF, the state of data in the value creation process is visualized through the following four steps[9]:

[8] METI, "Data Management Framework for Collaborative Data Utilization," accessed February 3, 2025, https://www.meti.go.jp/policy/netsecurity/wg1/DataManagementFramework_20250203.pdf

[9] METI, "Formulation of the Data Management Framework for Collaborative Data Utilization," accessed February 3, 2025, https://www.meti.go.jp/press/2022/04/20220408005/20220408005.html

STEP 1: Visualize the Data Processing Workflow ("Events")

- Visualize the rough data flow and "events" in the assumed data utilization process from data generation/acquisition to disposal.

STEP 2: Organize the Necessary Institutional Conditions and Measures ("Domains")

- Examine "domains" that should be managed based on the set data, “events”, and “domains”. At that time, it is conceivable that several “domains” overlap for one data, namely, requires are made for the data from various viewpoints.

STEP 3: Specify the "Properties"

- Identify the “properties” that should be managed based on the set data, “events”, and “domains”.
- In some cases, additions will be made as appropriate while organizing the “properties” of data, if there are any omissions in the “domains” where this data should be handled or “events” that must be implemented.

STEP 4: Identify the Risks of Each "Events"

- The risk assumed for each “events” is expected and the set “properties” are reviewed from the viewpoint of the “domains” set.
- Risks must not only be identified from the perspectives of cybersecurity (i.e., confidentiality, integrity, availability), but also from the point of view of compliance (i.e., laws, regulations).

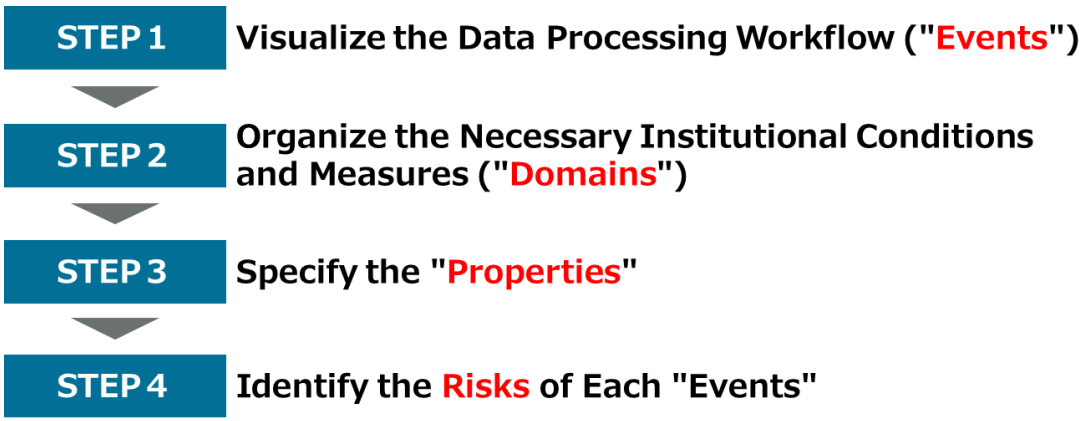



Figure 2-2 The Risk Analysis Procedure in DMF

### 2.3 Method for Organizing Trust Based on the DMF STEP

In this study group, when organizing trust for each use case, we followed the DMF framework to organize the risks and corresponding countermeasures. The data and domains for data sharing were sorted into the four elements, Q1 to Q4, to collect and analyze the uncertainty (risk) elements and the countermeasures to address them. As reiterated in Section 1.2, in this study group, trust refers to the state where "one believes that the other party will not betray expectations," and ensuring trustworthiness leads to transforming uncertain elements into acceptable risks.

Q1: Data to be Shared (Corresponding to DMF STEP 1)

- Types of data to be shared.
- The flow of data from generation/acquisition to disposal.

Q2: Domains of Data Sharing (Corresponding to DMF STEP 2)

- The types and number of businesses included in domains of data sharing.
- The rules, regulations, and agreements between businesses and regarding the data.

Q3: Risks and Uncertainties Related to Data (Corresponding to DMF STEP 3 and 4)

- Properties of each data and the risks anticipated for those properties.
- What are the uncertain elements that create risks?

Q4: Countermeasures for Risks

- Items and targets requiring trustworthiness.
- The assurance level that should be prepared for each item or target.
- Who should be the trust anchors?

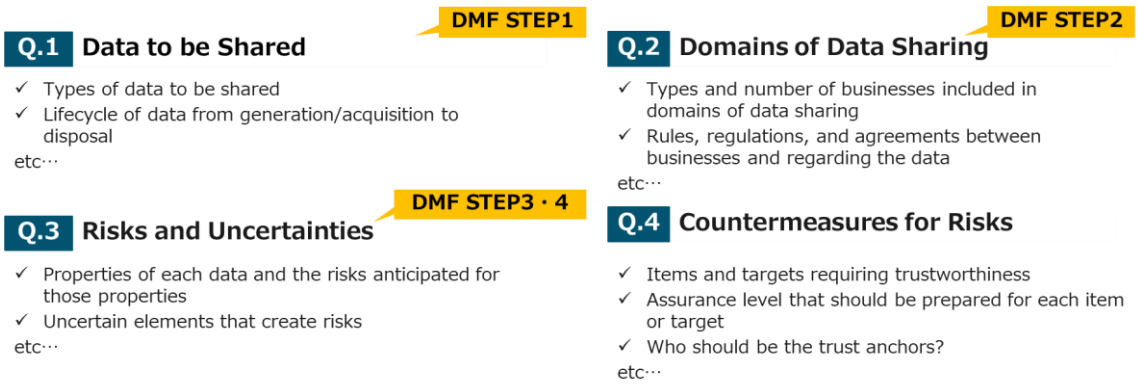



Figure 2-3 Method for Organizing Trust in Industrial Data Sharing

## 3. Use Cases in Some Industries

In this chapter, we will organize and analyze seven use cases of domestic industrial data sharing, based on the organizational method outlined in Chapter 2.

### 3.1 Automotive and Battery Use Case 1: Battery CFP/DD[10,11]

We will introduce the data sharing use cases of battery CFP data and DD data, led by ABtC.

#### 3.1.1 Data to be Shared

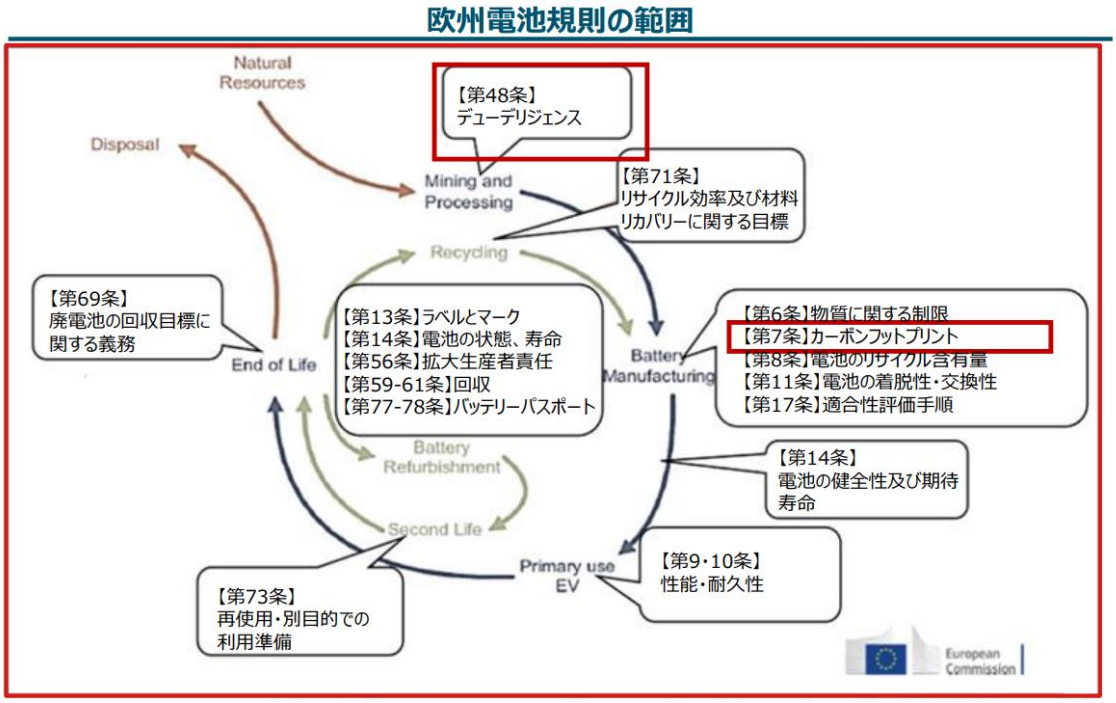
The data to be shared include the Carbon Footprint of Products (CFP) information and Due Diligence (DD) information within the supply chain of batteries. The CFP includes $CO_2$ emissions generated at each stage, from raw material procurement to manufacturing processes, and even through transportation and usage. It also contains a wide range of other information. On the other hand, the DD involves the evaluation of human rights and environmental risks in raw material extraction and procurement, as well as the status of improvement activities related to these risks.

#### 3.1.2 Domains of Data Sharing

The sharing of battery data along the supply chain is particularly required by the EU Battery Regulation. In a year or two, Article 7 of the EU Battery Regulation mandates the CFP for batteries, while Article 48 requires compliance with the DD in the supply chain. Furthermore, in the future, compliance with Article 8 on recycled content and Article 77 regarding the battery passport will be necessary.

[10] METI and DADC, "Guidelines on Data Integration Mechanisms in Supply Chains (Battery CFP/DD)," accessed February 3, 2025, https://www.ipa.go.jp/en/digital/architecture-guidelines/scdata-guidline-en.html

[11] DADC, and IPA, "Carbon Footprint (CFP) Operational Guidebook for Batteries and Vehicles Using Interoperable Data Infrastructures," accessed February 3, 2025, https://www.ipa.go.jp/en/digital/architecture-guidelines/individual-link/c0epbp000000tjma-att/cfp-guidebook-en.pdf




出典：EC「European Battery Alliance Deliverable：Industrial Policy」をもとにDADCで作成

Figure 3-1 The Scope of the EU Battery Regulation[12]

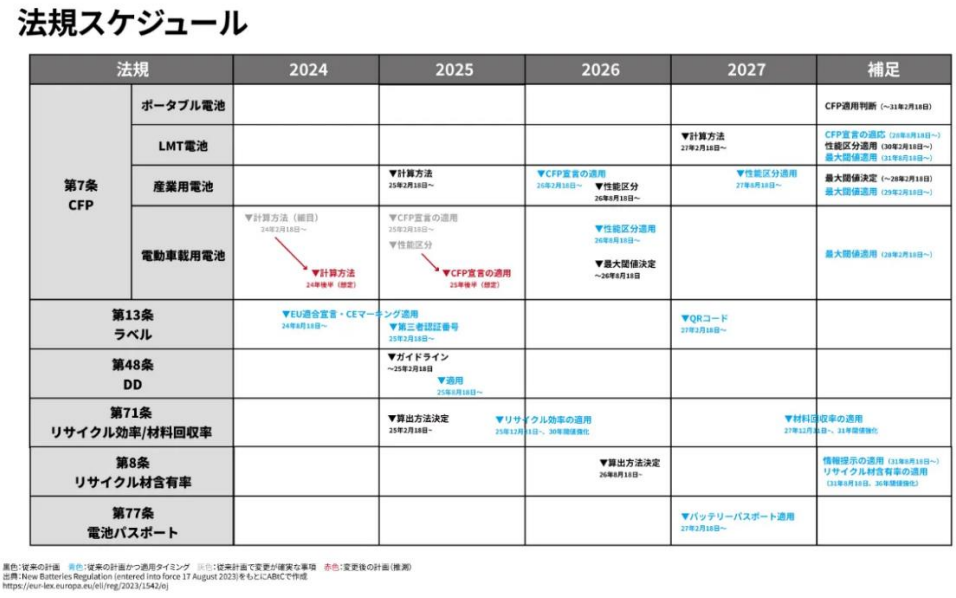



Figure 3-2 The Regulatory Schedule of the EU Battery Regulation[13]

[12] METI and DADC, Guidelines for Data Cooperation Mechanisms in Supply Chains (Battery CFP/DD-related) (Beta version), accessed March 17, 2025, https://www.ipa.go.jp/digital/architecture/Individual-link/m42obm0000008rd4-att/guideline-for-datacooperation-in-BattCFPDD-beta.pdf.

[13] ABtC, "EU Battery Regulation: Overview and Implications," accessed February 21, 2025, https://abtc.or.jp/column/240815-1#index_n8X65XBm

The types of businesses defined in the EU Battery Regulation along the supply chain include suppliers (e.g., raw material providers), manufacturers (e.g., Japanese subsidiaries of automotive OEMs, Japanese subsidiaries of battery manufacturers), importers and battery suppliers (e.g., European subsidiaries of automotive OEMs, European subsidiaries of battery manufacturers).

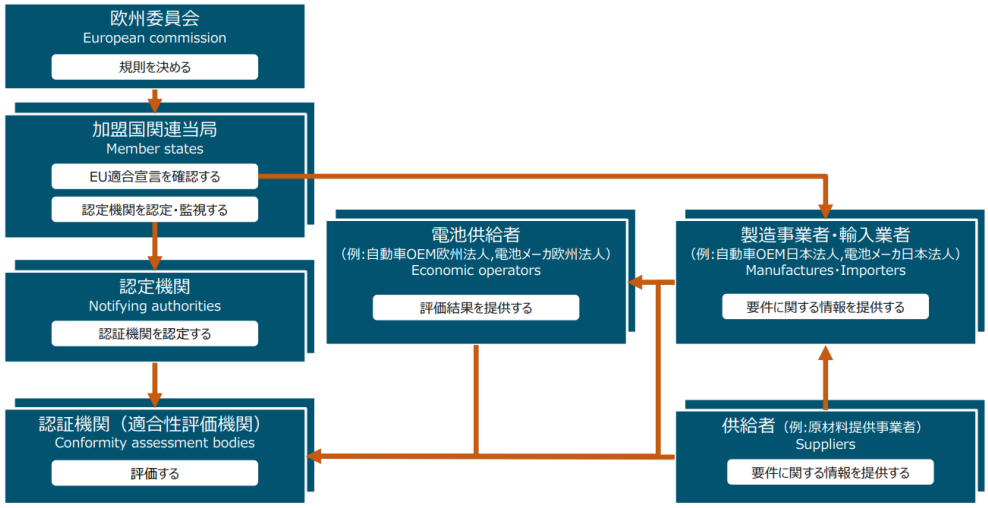



Figure 3-3 Stakeholders Defined in the Draft EU Battery Regulation [10]

### 3.1.3 Risks and Uncertainties Related to Data

The risks and uncertainties associated with the data include three main concerns: the risk of data tampering and impersonation, the risk of data leakage and privacy violations, and the uncertainties surrounding international data sharing.

1. Risk of data tampering and impersonation

   There is a risk that malicious third parties could infiltrate the system and alter battery environmental data or input false data by impersonating other companies. Additionally, there is a possibility that data could be tampered with during transmission, such as in a man-in-the-middle attack.

2. Risk of data leakage and privacy violations

   Battery data may contain confidential business information, such as manufacturing know-how or raw material supplier information. As a result, there is a risk of data leakage due to inadequate access controls or cyberattacks. Additionally, there is a risk that shared data may be reused by receiving companies for purposes other than originally intended.

3. Uncertainty of international data sharing

As the battery supply chain is globally distributed, differences in regulations between countries or regions may create barriers to seamless data sharing.

### 3.1.4 Countermeasures for Risks

The following countermeasures are proposed for the above risks:

1. Enhancing confidentiality protection and access control
   A user authentication system has been implemented, issuing unique IDs to participating companies and enforcing access restrictions based on roles and permissions. This ensures that only authorized individuals can access the necessary data, effectively blocking unauthorized impersonation attempts. Additionally, secure communication is established by verifying the correct connection information and ensuring the confidentiality and integrity of data transmission.
2. Ensuring data transparency
   Specifically, a system for third-party certification has been established. The calculated CFP values and submitted DD reports are required to undergo verification and certification by an independent third-party organization. Involving a third party ensures that the credibility of the data is objectively guaranteed, making it easier to fulfill accountability not only to the participating companies but also to consumers.
3. Ensuring interoperability
   Since the battery supply chain is globally distributed, ensuring interoperability with overseas data sharing platforms is crucial. In the future, interoperability with European systems, such as Catena-X, is being pursued to ensure seamless international data sharing.

## 3.2 Automotive and Battery Use Case 2: Automotive LCA[14]

Here, we will introduce the data sharing use case for the Automotive Life Cycle Assessment (LCA) led by ABtC.

### 3.2.1 Data to be Shared

There are two types of data involved in the sharing. The first type is $CO_2$ emission data from various companies along the supply chain, from raw material procurement to disposal.

[14] METI, "Materials No.3, 3rd Meeting of the Ouranos Ecosystem Trust Study Group" accessed February 21, 2025, https://www.meti.go.jp/policy/mono_info_service/digital_architecture/ouranos/ouranos_trust/250131/siryo3.pdf

Diverse stakeholders, such as automotive manufacturers (OEMs), parts manufacturers, and materials suppliers (Tier 1, 2 and more), are involved. By collecting $CO_2$ emission data at each stage and enabling data sharing across the entire industry, the aim is to visualize the environmental impact across the entire supply chain and explore strategies for emission reduction. The goal of the LCA is not only to calculate $CO_2$ emissions but also to clearly identify where and how emissions occur, pinpoint problems, and implement improvements. Therefore, detailed analyses by material, parts, and energy are required, and strategies for emission reductions must be deployed throughout the entire supply chain.

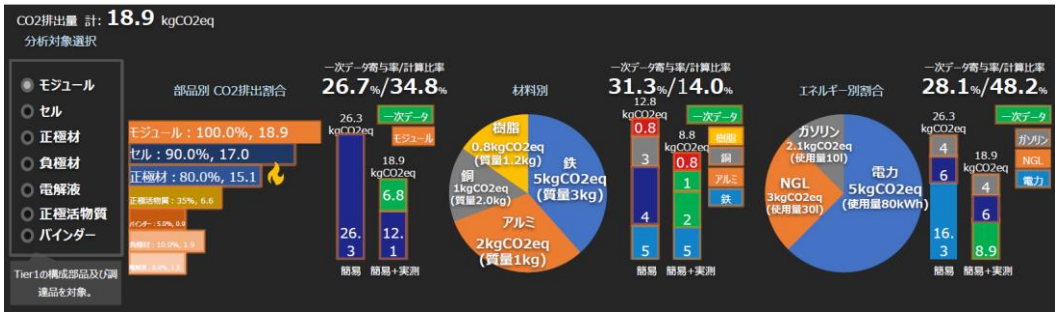



Figure 3-4 Assessment Image Diagram (numbers are placeholders)

The second type of data is the $CO_2$ emission factor data. For example, when using the IDEA (Inventory Database for Environmental Analysis) database developed by AIST (National Institute of Advanced Industrial Science and Technology) for environmental impact assessment, the IDEA data is subject to license management. Therefore, proper management of intellectual property rights and personal information is required for its use and sharing across the entire supply chain.

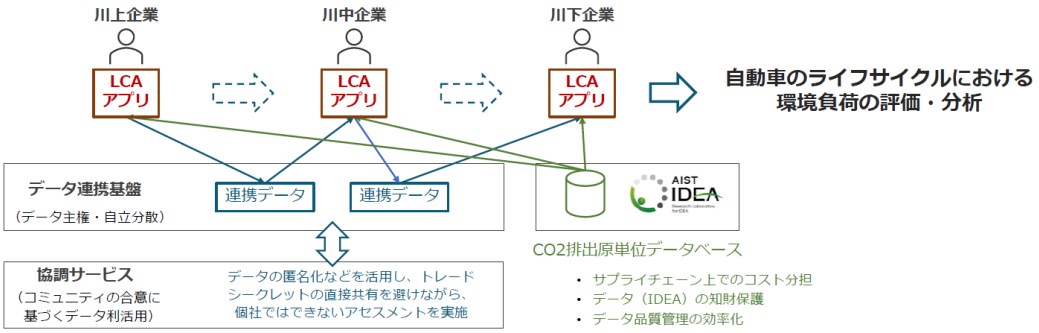



Figure 3-5 Image Diagram of Data Sharing in Automotive LCA

### 3.2.2 Domains of Data Sharing

In implementing the LCA, data sharing will be promoted based on inter-company transactions within the automotive supply chain. As the scope of LCA expands in the future, it is possible that tens of thousands of companies could become involved.

Regarding the international standardization of LCA, discussions are ongoing within the United Nations WP29 (World Forum for Harmonization of Vehicle Regulations). In the future, it is possible that global supply chains will serve as platforms for data sharing.

### 3.2.3 Risks and Uncertainties Related to Data

Data sharing in LCA involves risks such as data leakage from external attacks, as well as concerns that data users might use the information for unintended purposes, outside of the scope initially intended by the data providers. Regarding the use of IDEA data, licenses are managed on an individual basis, and compliance with domestic and international personal information protection regulations is necessary. Furthermore, in global data sharing, there is a risk that sharing could break down due to differences in laws and regulations across countries and regions.

In the future, it will be necessary to consider the introduction of data quality management through third-party certification, taking into account self-regulatory activities by companies and organizations, as well as potential regulatory actions.

### 3.2.4 Countermeasures for Risks

In terms of data sharing, there is no immediate need for new digital trust mechanisms due to the existing business agreements that govern the transactions of goods. However, as the scope of LCA expands, the number of participants is likely to grow, which will create a demand for scalable, cost-effective solutions to verify the identity of businesses involved.

Additionally, with respect to the IDEA data, it is essential to handle it appropriately, considering intellectual property protection, billing, and personal information management. Stakeholders are working to establish agreements on how data is provided and used, while also building systems that balance the protection of trade secrets with the ability to leverage the data. Techniques such as anonymization are being utilized to facilitate this balance and

ensure the protection of sensitive information.

Table 3-1 Summary of Q1–Q4: Automotive LCA Use Case

| |
|---|
| Q.1 Data to be Shared |
| ✓ $CO_2$ emission data from each company in the supply chain. These are aggregated based on business relationships and become the subject of analysis.<br>✓ $CO_2$ emission inventory data (IDEA). IDEA is used by each company in the supply chain, but its handling conditions include intellectual property dissemination and personal information management. |
| Q.2 Domains of Data Sharing |
| ✓ Inter-company transactions in the automotive supply chain. Due to the future expansion of LCA, the scale of the field will grow, and the number of companies in the automotive supply chain could reach tens of thousands.<br>✓ The international standard for automotive LCA is currently being discussed at the UN WP29. In the future, the global supply chain may become a platform for data sharing. |
| Q.3 Risks and Uncertainties Related to Data |
| ✓ Data leakage due to external attacks.<br>✓ Misuse of data-by-data users for purposes not intended by the data provider (e.g., $CO_2$ emission information, IDEA).<br>✓ Management of personal information for IDEA users. IDEA is licensed on an individual basis, and it is necessary to comply with domestic and international personal information protection rules.<br>✓ Interruption of sharing due to data cross-border restrictions (when dealing globally).<br>✓ Data quality management through third-party certification (needs to be considered with an eye on self-regulation, regulatory trends, etc.). |
| Q.4 Countermeasures for Risks |
| ✓ The handling of value information along the supply chain (intellectual property protection, billing, personal information management) is being discussed using IDEA as a subject.<br>✓ Other matters are similar to those of the battery CFP. |

## 3.3 Automotive and Battery Use Case 3：Battery Passport[14]

### 3.3.1 Data to be Shared

The introduction of the battery passport aims to ensure traceability throughout the entire battery lifecycle, from manufacturing to recycling, and to centrally manage the necessary information at each stage. In this use case, various stakeholders, including OEMs, battery manufacturers, and recyclers, are involved in the development of a system that can comply with international battery passport regulations (scheduled to be enforced in 2027). The following three types of data are subject to shared:

1. Identification information (manufacturer information, battery specifications, resource amounts, etc.)
2. Value information (data related to performance and lifespan, historical information, etc.)
3. Environmental information (the CFP), the DD data, etc.)

### 3.3.2 Domains of Data Sharing

The data sharing for the battery passport is planned to expand gradually, starting with establishing data sharing in the domestic market (Step 1) and then expanding globally (Step 2).

As Step 1, in the domestic market, efforts are being made to build an ecosystem that creates value throughout the entire battery lifecycle and promotes resource circulation for batteries. Within this ecosystem, there are various stakeholders and business processes, and the data generated from competitive and collaborative services will be intricately interconnected. Therefore, it is necessary to build the system not as a single centralized management system, but as a "System of Systems," where various foundations and platforms interconnect with each other. Furthermore, the core components to be shared across the ecosystem (the Japanese version of the battery passport) must include: 1) a common interface (API) to link various platforms and services, 2) a fair and secure charging mechanism and transaction ledger to economically reward data providers, and 3) essential information that should be maintained for sharing within the community. In the domestic market, use cases such as performance guarantees for used cars, reuse of small mobility units, and reuse and recycling of stationary batteries are taking the lead.

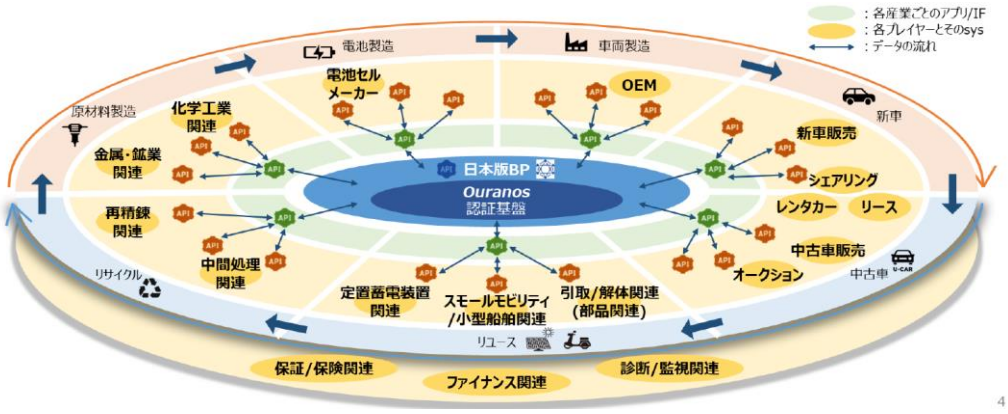



Figure 3-6 Battery Ecosystem

In Step 2, the goal is to establish sharing with overseas markets. The framework for this sharing will be international regulations, including the EU battery passport regulation (scheduled to be enforced in 2027). While ensuring interoperability with the battery passport regulations of each country, it is essential to integrate into the international battery passport framework.

### 3.3.3 Risks and Uncertainties Related to Data

The data sharing in the battery passport may involve the following risks:

- Improper use of data due to data impersonation, tampering, etc.
- Data leakage due to external attacks or other security breaches.
- Difficulty in interconnecting with other countries due to the lack of a universal system.
- Disruption of data sharing due to regional consensus on rules (rules related to batteries, resource circulation, data cross-border issues, DPP service provider requirements, etc.).

### 3.3.4 Countermeasures for Risks

Given the diverse stakeholders and business processes, it is difficult to assume a single risk and trust framework because of handling various types of information generated throughout the battery lifecycle. Therefore, it is necessary to conduct case-by-case (or industry-specific) studies and verifications to ensure that appropriate risk responses and trust designs are in place. In particular, attention should be paid to the following three points, advancing both value creation starting from the domestic battery market and responding to international battery passport regulations:

1. Sufficient and appropriate trust design tailored to each industry and use case.

2. Ensuring sufficient robustness specific to each country, industry, or use case.
3. A flexible system configuration aimed at interconnecting with other countries using APIs.

Table 3-2 Summary of Q1–Q4: Battery Passport Use Case

| |
|---|
| Q.1 Data to be Shared |
| ✓ Various information generated throughout the battery lifecycle, including manufacturing, usage, second-use (used), recycling, etc.<br>・ Identification Information (Manufacturer details, battery specifications, resource quantities, etc.)<br>・ Value Information<br>✓ Data related to performance and lifespan (such as historical information, etc.)<br>✓ Data related to environmental considerations (CFP, DD, etc.) |
| Q.2 Domains of Data Sharing |
| ✓ Participants in various lifecycle stages of batteries in the domestic market, including manufacturing, usage, second-use (used), recycling, etc.<br>・ Step 1: Establish sharing platforms for each domestic use case (by industry).<br>✓ Performance warranty for used cars (currently being implemented)<br>✓ Module-based reuse for small mobility (currently being implemented)<br>✓ Reuse and recycling for stationary batteries (to be expanded in the future)<br>・ Step 2: Expand the platform globally through international sharing. |
| Q.3 Risks and Uncertainties Related to Data |
| ✓ Improper use of data due to impersonation or tampering<br>✓ Data leakage due to external attacks or other security breaches<br>✓ Difficulty in interconnecting with other countries due to the lack of a universal system<br>✓ Interruption of data sharing due to differences in regional rules (rules related to batteries, resource circulation, data cross-border transfer, and requirements for DPP service providers, etc.) |
| Q.4 Countermeasures for Risks |
| ✓ Designing sufficient and necessary trust for each industry and use case<br>✓ Ensuring sufficient robustness for each industry and use case, both domestically and internationally<br>✓ Flexible system architecture for interconnection with other countries using APIs |

The use case for automotive LCA discussed in Section 3.1 and the trust considerations for the battery passport span multiple areas, including different stakeholders (Figure 3-7). Therefore, it cannot be assumed that a specific digital technology is applicable across all areas. In each area, comprehensive consideration of factors such as regulations, business

practices, business structures, and existing digital assets, along with specific demonstrations, is required. It is essential to advance the formation of agreements and implementation regarding the required trust content and levels.

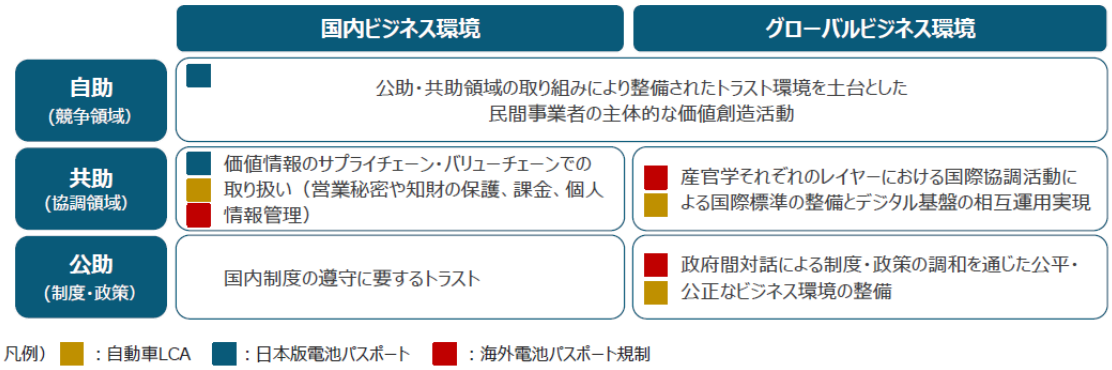



Figure 3-7 The Areas of Trust Consideration in the Automotive Field

## 3.4 Chemical Substance Management Use Case[15]

This section introduces the use cases related to the data sharing of chemical substances contained in products and resource circulation information by the CMP (Chemical and Circular Management Platform) Task Force.

### 3.4.1 Data to be Shared

Information on chemical substances contained in products will be linked from upstream industries (chemical manufacturers) to downstream industries (final products manufacturers) in order to promptly respond to the REACH regulations and other chemical substance regulations that are becoming stricter year by year (improvement of reinvestigation efficiency). Additionally, with an eye on the EU ESPR regulation, resource circulation information in the value chain, such as parts reuse information and recycled material information (including content ratio, purity, source, etc.), is also a target for data sharing, focusing on DPP (Digital Product Passport).

[15] METI, "Materials No.4, 3rd Meeting of the Ouranos Ecosystem Trust Study Group" accessed February 21, 2025, https://www.meti.go.jp/policy/mono_info_service/digital_architecture/ouranos/ouranos_trust/250131/siryo4.pdf

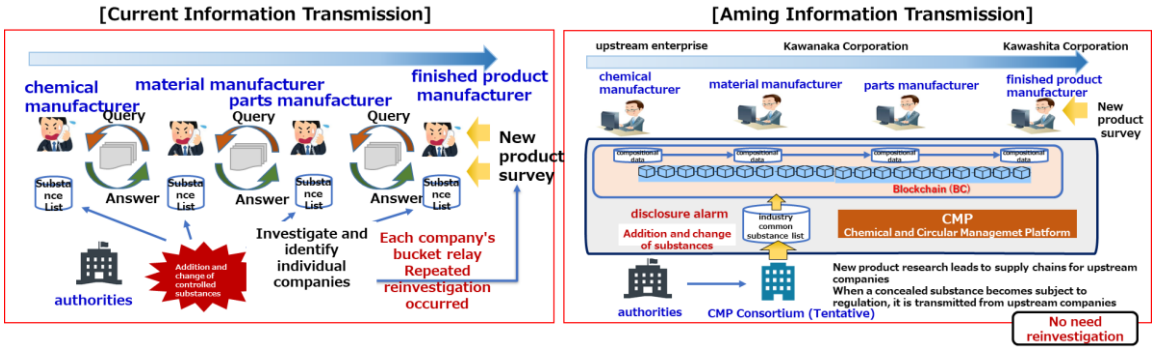
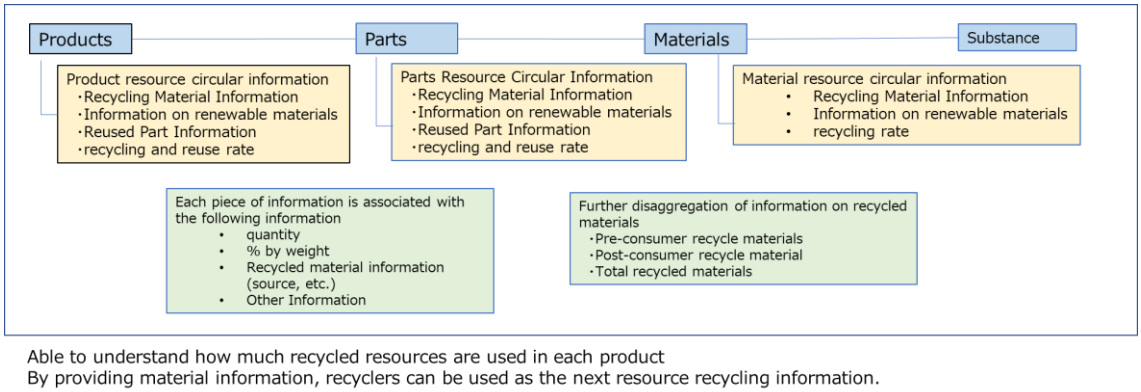



Figure 3-8 Overview of Sharing on Chemical Substances in Products (CMP)

Discussions are being held on how to efficiently share information by incorporating resource circulation data into the hierarchy information of products, parts, materials, and chemicals held by CMP.




Able to understand how much recycled resources are used in each product
By providing material information, recyclers can be used as the next resource recycling information.

Figure 3-9 Relationship between CMP Data Structure and Resource Circulation Information

### 3.4.2 Domains of Data Sharing

As mentioned earlier, information of chemical substances contained in products and resource circulation data will be shared through the supply chain from upstream manufactures (chemical manufacturers) to downstream manufactures (final products manufacturers), and it is expected that the number of participants will exceed 10,000.

However, in the CMP, the sharing of information of chemical substances contained in products occurs between direct business partners (B2B) who have already concluded basic transaction agreements, so trust in entities, individuals, and products is already established based on these agreements. Therefore, for example, in terms of product trust, product identification is carried out by linking the customer part number and the supplier part

number, and the responsibility for matching the information falls on each supplier.

Additionally, there are contracts governing data sharing between the business partners, which define aspects such as quality assurance, liability for defects, confidentiality, and the obligation to provide information of chemical substances contained in products.

### 3.4.3 Risks and Uncertainties Related to Data

Information of chemical substances contained in products, recycled material and reused parts information, are linked for the purpose of complying with various regulations, and therefore, data reliability is required.

As mentioned earlier, in the CMP, the sharing of information of chemical substances contained in products occurs through B2B exchanges between businesses that already have basic transaction agreements. Therefore, for example, regarding the authenticity and identity of participants, corporate authorization as the counterparty for data exchange is carried out based on the contract, and there is no need for new means to ensure trust.

However, there are scenarios where data sharing with an unspecified number of businesses is anticipated, and in such cases, additional trust may be required. For example, in the case of sharing resource circulation information, there may be involvement from many companies in open-loop recycling. Furthermore, information exchange could take place in platforms such as marketplaces.

Additionally, if expansion to overseas markets is considered, such as system deployment in Southeast Asia, mutual authentication with overseas platforms may be required.

### 3.4.4 Countermeasures for Risks

The trustworthiness of data will be ensured by the international standard IEC 63000. This standard dictates that compliance with chemical substances regulations for goods is ensured through a company’s manufacturing process management system, analysis data, and information transmission based on these data according to rules such as IEC/ISO 82474 and IEC 62474. IEC 63000 has been designated for compliance assessments by many countries and regions' chemical substances regulations (in Europe, it is used as EN63000 within the

region).

Regarding the identification and certification of corporations, when joining the service, a public certification code (in Japan, this could be the corporate number, or the Teikoku DB; globally, it could be DUNS, etc.) is used along with service terms and conditions to carry out corporate certification and authorization. As for the organizations and users (individuals) under the corporation, this is managed by the corporation, and the platform does not require certification and authorization (the information is managed at the application layer).

In CMP, while enabling compliance with various countries' chemical substances regulations, the aim is to build an information-sharing infrastructure supporting the circular economy. It also envisions systems for global supply chains, as the system will need to be expanded for use by companies overseas.

In constructing the infrastructure, by following the guidelines for supply chain information transmission (battery CFP/DD) as an existing use case of Ouranos Ecosystem, CMP aims to ensure alignment between public DPFs and efficiently and swiftly develop the platform. Therefore, from an efficiency perspective, CMP hopes that a unified trust certification system will be implemented on Ouranos Ecosystem when multiple use cases are deployed there.

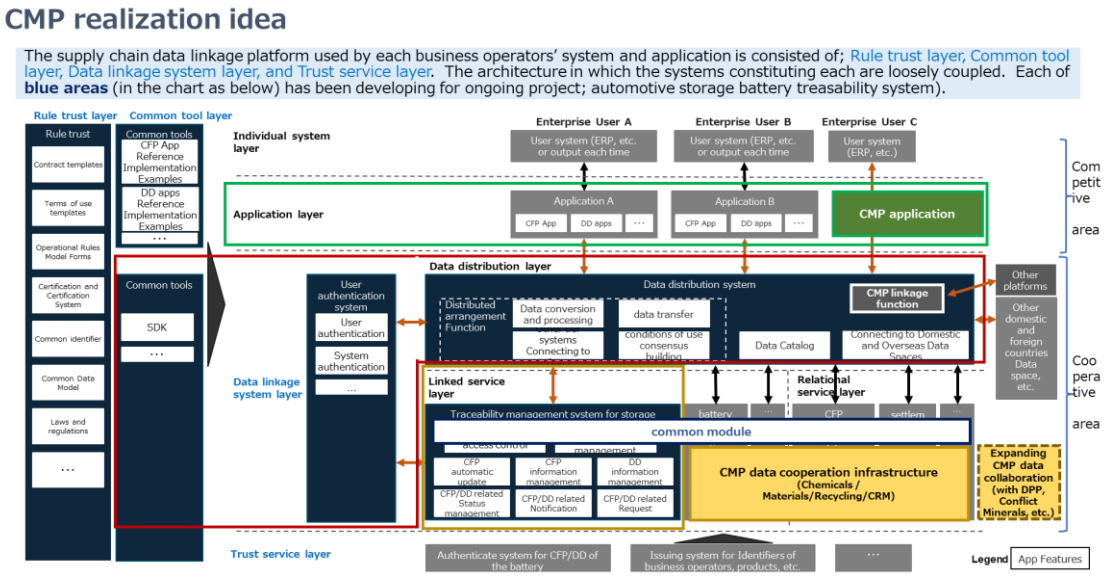



Figure 3-10 Concept of Integration between CMP and Ouranos Ecosystem

Table 3-3 Summary of Q1–Q4: Chemical Substance Management Use Case

| | |
|---|---|
| Q.1 Data to be Shared | |
| | ✓ Information of chemical substances contained in products<br>✓ Information on utilized recycled materials and reused components |
| Q.2 Domains of Data Sharing | |
| | ✓ The supply chain from upstream industries to downstream industries. It is expected that 10,000 domestic companies and several thousand overseas companies from the automotive and electronics industries will participate.<br>✓ Integration with overseas systems and expansion of CMP to overseas markets. |
| Q.3 Risks and Uncertainties Related to Data | |
| | ✓ The trustworthiness of chemical substances, recycled materials, and reused parts information. Data reliability is necessary as it pertains to regulatory compliance.<br>✓ Integration with overseas systems.<br>✓ Handling of data by an unspecified number of companies (future challenge). |
| Q.4 Countermeasures for Risks | |
| | ✓ Compliance with contracts and IEC/ISO 82474, IEC 63000 (current status).<br>✓ System expansion to overseas markets (particularly Southeast Asia). |

## 3.5 Railway Use Case[16]

Here, we introduce a use case related to the real-time data sharing of train delays and online positions by East Japan Railway Company (JR East).

### 3.5.1 Data to be Shared

Real-time data such as train delay times and online positions, taking into account delays, are the data to be shared. When traveling within Japan, various modes of transportation and transportation operators are used, so it is necessary to share data from various transportation companies. Real-time data is received from each transportation operator in their respective formats and is then converted into a unified format.

### 3.5.2 Domains of Data Sharing

RT-DIP (Real-Time Data Integration Platform) is a platform for exchanging real-time data,

[16] METI, "Materials No.5, 3rd Meeting of the Ouranos Ecosystem Trust Study Group" accessed February 21, 2025, https://www.meti.go.jp/policy/mono_info_service/digital_architecture/ouranos/ouranos_trust/250131/siryo5.pdf

operated jointly by JR East and various transportation companies under an agreement. As of September 2024, eight railway operators, including JR East, are participating.

Through RT-DIP, railway operators can post route information on their websites and apps, and also provide data to external route navigation services. The former is offered free of charge, while the latter is based on a paid contract.

This enables service users to search for routes while considering the operational status of multiple railway and bus operators, allowing them to choose more accurate and convenient modes of transportation.

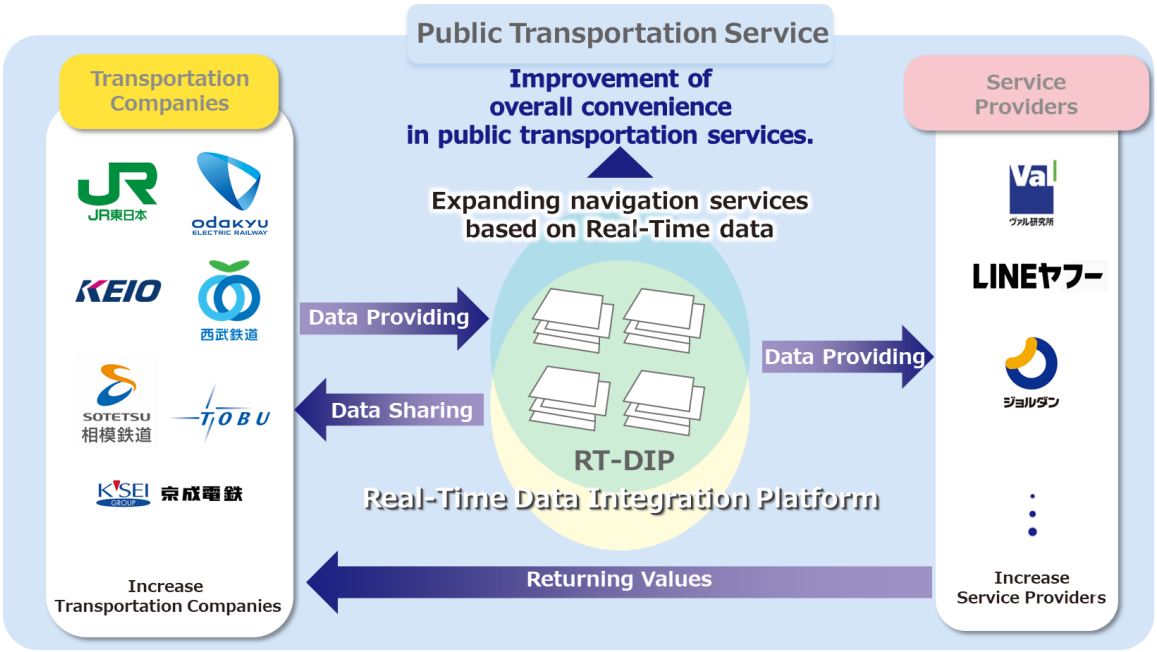



Figure 3-11 The Overall Picture of RT-DIP

The real-time route search is achieved by combining static data (such as timetables and regular schedule data) with dynamic data (such as delay information and other real-time data).

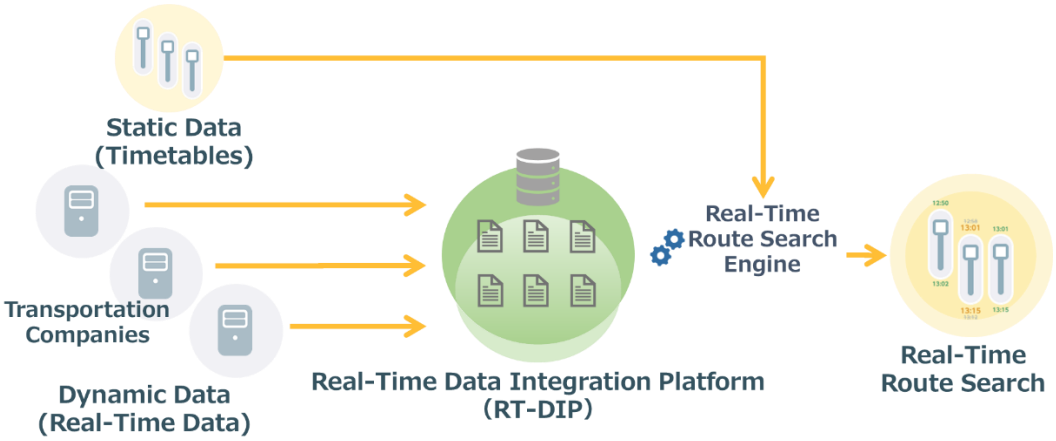



Figure 3-12 System Configuration to Enable Real-Time Route Search

### 3.5.3 Risks and Uncertainties Related to Data

There are mainly two risks.

First, there is the risk that the companies providing data may not correctly understand the items and formats, which could prevent them from being used appropriately (Risk 1). Without ensuring data consistency and compatibility, the benefits of integration may not be fully realized.

Second, there is the risk of data quality deteriorating due to failure to adequately respond to changes such as timetable revisions (Risk 2). Particularly, the latter poses a significant impact on users, as providing incorrect data could lead to inconveniences such as missing trains.

### 3.5.4 Countermeasures for Risks

To address Risk 1, each company understands the proprietary formats of the data they provide, converts it into a unified format, and stores it in a common platform. Additionally, the use of the international data standard, GTFS (General Transit Feed Specification), is recommended.

For Risk 2, when movement-related data is shared with data providers and others, careful attention is paid to ensure data quality, which helps reduce the risk of errors.

Table 3-4 Summary of Q1–Q4: Railway Use Case

| Q.1 Data to be Shared |
|---|
| ✓ Real-time train delay times, online positions, etc.<br>✓ Receiving real-time data from each transportation operator in their respective formats and converting it into a unified format. |
| Q.2 Domains of Data Sharing |
| ✓ 8 railway operators (as of September 2024) are using the data platform.<br>✓ Each transportation operator has entered into agreements with JR East to operate the platform. |
| Q.3 Risks and Uncertainties Related to Data |
| ✓ It is necessary for the providing companies to understand and utilize the data items and formats correctly.<br>✓ It is important to respond to changes such as timetable revisions and ensure that data quality is maintained. |
| Q.4 Countermeasures for Risks |
| ✓ Data provided by each company in their own formats is understood and stored in a common platform. Additionally, the international data standard GTFS format is also recommended.<br>✓ When sharing transportation-related data with data providers, careful attention is given to proper data handling. |

## 3.6 Electric Power Data Use Case[17]

Here, we will introduce use cases related to the sharing of power data obtained from smart meters, as presented by the Secured Meter Data Sharing Association.

### 3.6.1 Data to be Shared

The power usage and power generation achievements, as well as the power transaction data generated every 30 minutes from 80 million smart meters nationwide, will be shared as part of the target data. The data will be stored in a data lake for a period of three years.

Among the power data provided, individual data for which consent has been obtained is used for purposes such as tracking actual usage, calculating CO2 emissions (including services that support these activities), energy efficiency assessments, monitoring and understanding the operation of power generation facilities, and other related activities. Additionally, statistics can be used to analyze local economic trends and compare with individual data.

[17] METI, "Materials No.6, 3rd Meeting of the Ouranos Ecosystem Trust Study Group" accessed February 21, 2025, https://www.meti.go.jp/policy/mono_info_service/digital_architecture/ouranos/ouranos_trust/250131/siryo6.pdf

Moreover, custom statistics allow for flexible investigations, including the ability to set specific populations and calculate deviations.

| 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<br>・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 |

Figure 3-13 Use Cases of Electric Power Data

### 3.6.2 Domains of Data Sharing

Under the Electricity Business Act, from the perspective of fair competition, the use of power data for purposes other than its intended use is prohibited for Transmission System Operators (TSOs). However, with the revision of the Electricity Business Act in June 2020, under the "Certified Association System" designed to protect personal information and ensure fair competition, businesses other than electricity suppliers are now allowed to utilize power data. The Certified Association System, based on the provisions of Article 37-4 of the Electricity Business Act, is a scheme where the government certifies specialized organizations that are responsible for safely and appropriately providing power data to third parties, following proper consent procedures, while ensuring the protection of personal information (as per the Personal Information Protection Act) and the maintenance of fair competition (under the Electricity Business Act).

In response to this, the "Secured Meter Data Sharing Association" was established by seven data users and ten TSOs. On June 30, 2022, based on the relevant provisions, the Secured Meter Data Sharing Association was certified by the Minister of Economy, Trade, and Industry as the "Certified Electricity User Information Utilization Association." Specifically, the provision and utilization of data will be carried out under the following scheme.

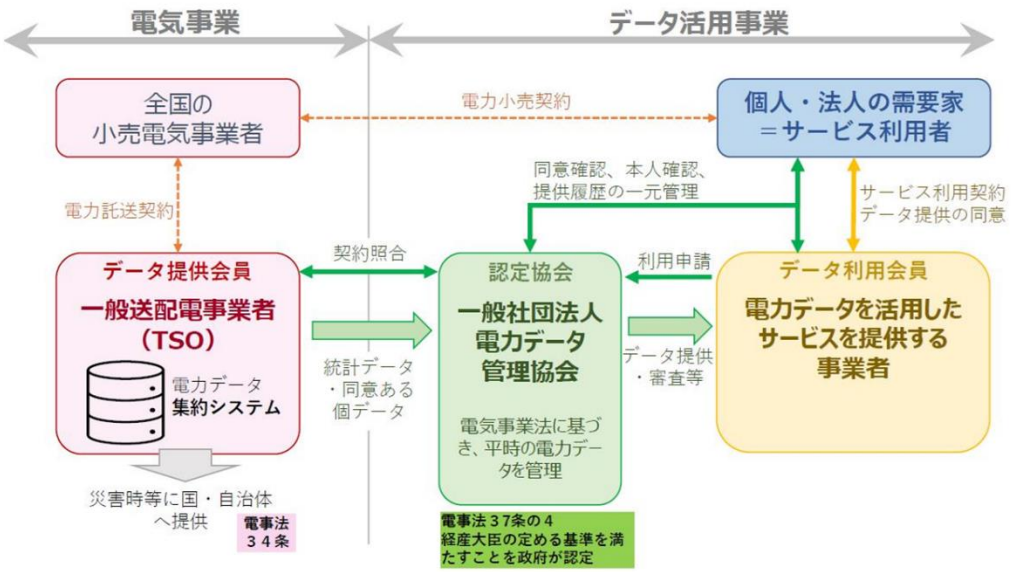



Figure 3-14 Data Provision and Utilization Scheme Based on the Certification Association System

In order to obtain certification, it is required to meet the "Certification Standards for Certified Electricity User Information Utilization Associations under Article 37-4 of the Electricity Business Act." Specific requirements are set out, including proper consent procedures, traceability, and ensuring the security of data handlers (such as third-party certifications for ISMS and P-Mark).

(Article 37-4 of the Electricity Business Act (Act No. 170 of 1964))
(Certification of Certified Association for Electricity Consumer Information Users)

Article 37-4. The Minister of Economy, Trade and Industry may certify, pursuant to an application and as specified by Ordinance of the Ministry of Economy, Trade and Industry, a general incorporated association established by persons intending to utilize electricity user information and general electricity transmission and distribution business operators and electricity distribution business operators intending to provide electricity user information as prescribed in paragraph (1) of the preceding article (collectively referred to as "Electricity User Information Users" in item (ii)), provided the association meets the following standards. Such associations may perform duties stipulated in the following article (hereinafter referred to as "duties for ensuring proper use of information" in this chapter):

(i) The purpose of the association must be to contribute to ensuring fair competition among

electricity suppliers by ensuring proper use and provision of electricity user information by its members (hereinafter referred to as "members" in this chapter).

(ii) Its articles of incorporation must stipulate inclusion of Electricity User Information Users as members.

(iii) It must have defined necessary methods for appropriately performing duties for ensuring proper use of information.

(iv) It must possess sufficient knowledge, capabilities, and financial foundations necessary to appropriately perform duties for ensuring proper use of information.

### 3.6.3 Risks and Uncertainties Related to Data

As mentioned earlier, consent must be obtained when providing individual data. The verification of the identity of consent applicants, linked through the Secured Meter Data Sharing Association, with the customer information managed by general transmission and distribution operators, is carried out by the general transmission and distribution operators. During this verification process, challenges mainly arise in areas that are not directly related to supply or billing calculations, such as inconsistencies in the information and the difficulty of linking data.

（Challenges Related to Information Inconsistencies）

- In the case of electricity, if the "supply point identification number" is known, the contract can be uniquely identified. However, it is rare for the contract holder's name to match exactly between the consent applicant and the power company's register.
- When matching the applicant with the contract, information such as name and address is used to make the determination. However, these details often include inconsistencies or outdated information, which makes verifying the identity of the consent applicant and the contract holder time-consuming and costly.
- When utilizing data, especially if location information is to be used, attention is needed as the address information may differ across administrators, and there may be discrepancies in maps or differences in how location data is set up

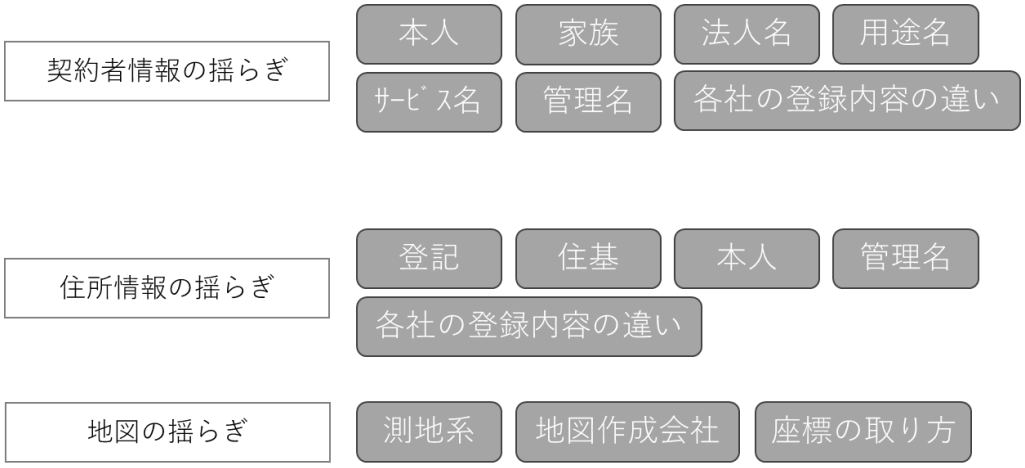



Figure 3-15 Breakdown of Data Fluctuations

（Challenges Related to Linking Multiple Contract Information）

- In some cases, multiple corporations may occupy the same premises or building, the contract holder and the actual user may differ, or there may be different contract parties for electricity, gas, water, and telecommunications. Additionally, property management companies might be involved, resulting in various contract structures.
- Furthermore, internal network information that is not directly related to external contracts or supply cannot be shared with parties other than the involved entities (in this case, B or C can only obtain it from A). There are frequent inquiries regarding this, such as requests to access internal network measurement data.

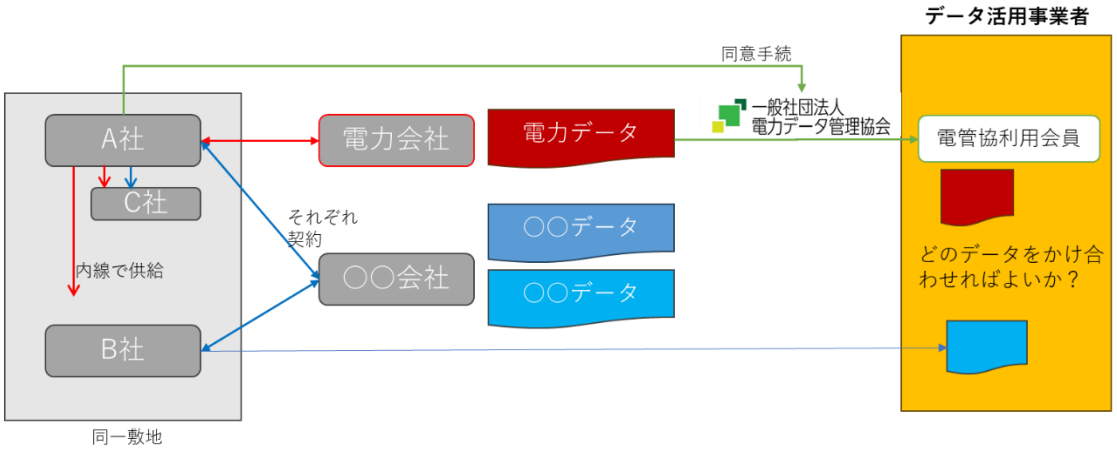



Figure 3-16 The Background of the Difficulty in Data Linkage: Inter-Business Relationships

Additionally, from the perspective of preventing data leakage, ensuring security against external attacks is recognized as a key challenge.

### 3.6.4 Countermeasures for Risks

The system for providing power data mainly includes the following functions:

（Main Functions of the System for Providing Power Data）

- When utilizing individual data, system integration via API is essential for the consent application process and the acquisition of individual data (either developed by the user members or through third-party systems already built).
- When using standard statistical data, API is generally used, whereas for custom statistics, data is provided through a storage service.
- The system's interface definitions and specifications will be disclosed after membership registration.

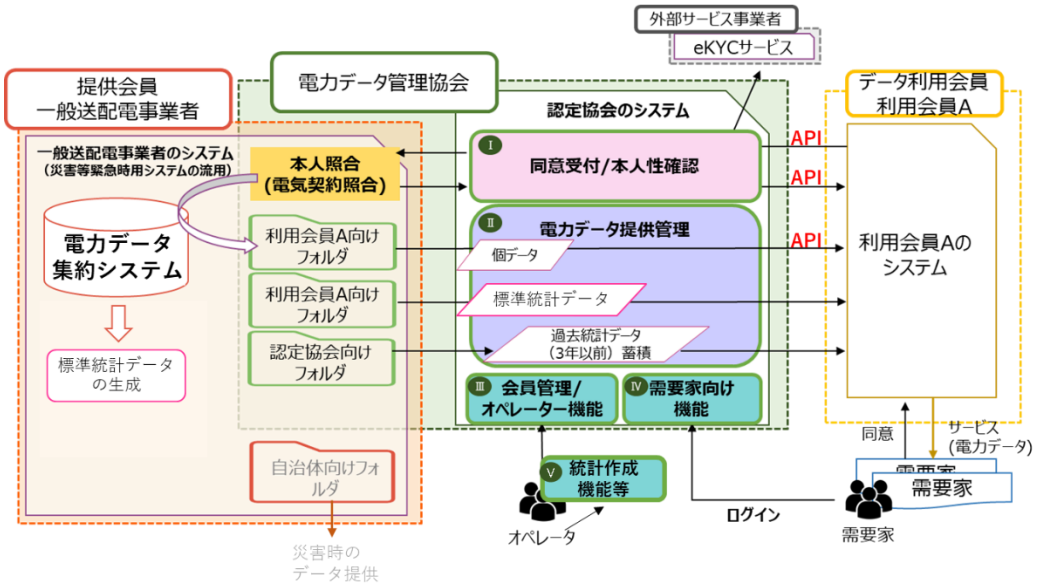



Figure 3-17 Main Functions of the System for Providing Electric Power Data

From the perspective of preventing data leakage, the system is designed such that if the Secured Meter Data Sharing Association halts the token, the user members will no longer be able to access the data.

Additionally, regarding the consent required for providing individual data, the validity of the consent application documents (such as the official seal, electronic signature, power of attorney, and authority declaration) is manually verified. The identity verification of the consent applicant is conducted using an external eKYC service integrated into the Secured Meter Data Sharing Association's system.

Table 3-5 Summary of Q1–Q4: Electric Power Data Use Case

| |
|---|
| Q.1 Data to be Shared |
| ✓ Power usage and power generation achievements, as well as the foundational power transaction data, are generated every 30 minutes from 80 million smart meters nationwide.<br>✓ The data is stored in a data lake for a period of 3 years. |
| Q.2 Domains of Data Sharing |
| ✓ Through a government-certified specialized organization (the Secured Meter Data Sharing Association), statistical data and individual data with obtained consent can be provided to third parties, as well as disclosed to the contract holder themselves from the user members of the association.<br>✓ In cases where necessary for disaster recovery or similar situations, local governments across the country are allowed to use power data without consent. |
| Q.3 Risks and Uncertainties Related to Data |
| ✓ There are issues with data accuracy, particularly in areas not directly related to supply or billing calculations.<br>✓ The new system, which stores and provides nationwide data in bulk, will require several years to resolve challenges that were not initially anticipated.<br>✓ Due to inconsistencies and inaccuracies in contract information on both the applicant's side and the power company's register, linking the relevant data requires considerable time and cost.<br>✓ Security risks, such as attacks from external sources, are a concern. |
| Q.4 Countermeasures for Risks |
| ✓ The consent process and exchange of power data occur through API integration between the power companies, the Secured Meter Data Sharing Association, and the user members, ensuring security across the systems.<br>✓ Consent procedures are conducted for each use case, location, and recipient.<br>✓ The validity of consent application documents (such as official seals, electronic signatures, powers of attorney, and authority declarations) is manually verified.<br>✓ If the Secured Meter Data Sharing Association halts the token, the user members will no longer be able to access the data, as part of the system design. |

## 3.7 People Flow Data Use Case[18]

Here, we will introduce a use case related to the sharing of people flow statistical data utilizing location information obtained from mobile phone base stations, provided by SoftBank Corp. (a commercialization service example).

### 3.7.1 Data to be Shared

In addition to the in-house people flow data obtained from mobile phone base stations (such as the number of arrivals and departures, population density in specified mesh areas, and the number of people moving through transportation facilities), external data such as census data is also integrated.

As a service based on the provision of these data, an example is the already commercialized service "National Movement Statistics," which utilizes location information from base stations to process and provide statistical data on human movement and stay information. This service is offered to various fields and industries.

（Nature of "National Movement Statistics" Data and Its Recipients and Uses）

- Nature of the Data: The value of the provided data is characterized by the following three qualities:
  - Comprehensiveness: The data covers the entire geographical range where base stations are located (nationwide in Japan) and spans a temporal range of 24 hours, 365 days
  - Functionality: The data provides detailed information about people's movements and stays, including travel routes and modes of transportation.
  - Trustworthiness: The data is derived from high sample sizes and statistical adjustments, ensuring its trustworthiness.
- Recipients and Uses of the Data:
  - Commercial and Real Estate: The data is used for market analysis of competing facilities, planning parking lots based on traffic volume, and examining new store locations.
  - Tourism: It is used to promote visits to tourist destinations, address traffic congestion, and improve regional transportation networks.
  - Transportation: The data is utilized in considerations for introducing new

[18] METI, "Materials No.7, 3rd Meeting of the Ouranos Ecosystem Trust Study Group" accessed February 21, 2025, https://www.meti.go.jp/policy/mono_info_service/digital_architecture/ouranos/ouranos_trust/250131/siryo7.pdf

transportation services, planning road improvements, and enhancing secondary transportation to airports.

- Disaster Prevention and Mitigation: It supports the design of evacuation routes during disasters, integrates into disaster preparedness plans, and forecasts the number of people unable to return home.

### 3.7.2 Domains of Data Sharing

The people flow data obtained from mobile phone base stations, including location information, is provided only after anonymization and statistical processing. It is shared exclusively with specific systems at the contracted organizations, and data exchange occurs only between these particular systems. However, in the case of public interest, such as during disasters, data may be provided without compensation as an exception.

Furthermore, from the perspective of personal data protection, the data handling follows privacy policies and is conducted in accordance with the consent of the mobile phone company's customers.

### 3.7.3 Risks and Uncertainties Related to Data

Since the raw data obtained from mobile phone base stations can potentially identify individuals, there remains a risk of personal identification if the data is used as is.

Additionally, there are challenges related to the quality and trustworthiness of the data. The provided data requires a lead time before it can be delivered.

### 3.7.4 Countermeasures for Risks

As mentioned earlier, the raw data obtained from mobile phone base stations undergoes anonymization and statistical processing. Personal identification codes and other identifiers are processed in a way that prevents individuals from being identified. Additionally, data within a mesh area is deleted if the number of individuals in the area is below a specified threshold, to further protect privacy. Specifically, the data undergoes the following anonymization and statistical processing steps between the mobile phone base stations and the recipients of the data.

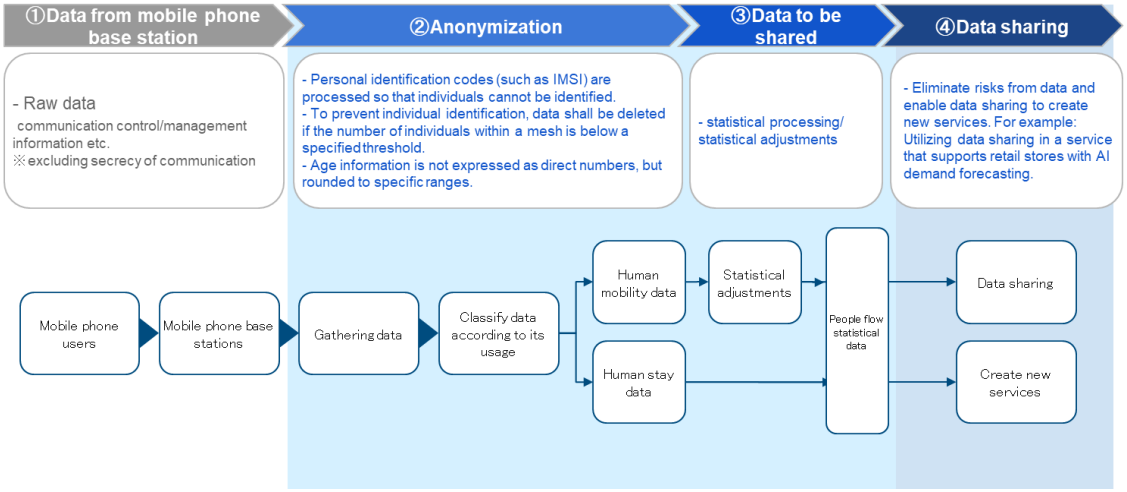



Figure 3-18 Process of Data Anonymization and Statistical Processing

Additionally, regarding the quality and trustworthiness of the data, statistical adjustments are made by combining the data with other reliable sources. This helps to improve the accuracy of the statistical processing and enhance the overall trustworthiness of the data provided.

Table 3-6 Summary of Q1–Q4: People Flow Data Use Case

| | |
|---|---|
| Q.1 Data to be Shared | |
| | ✓ People flow data obtained from mobile phone base stations<br>✓ External data such as census data |
| Q.2 Domains of Data Sharing | |
| | ✓ Anonymization and statistical processing are performed, and data is exchanged only between specific systems<br>✓ Compliance with personal data protection, privacy policies, and customer consent procedures |
| Q.3 Risks and Uncertainties Related to Data | |
| | ✓ Risk of identifying individuals<br>✓ Data quality/trustworthiness |
| Q.4 Countermeasures for Risks | |
| | (1)-1. Anonymization of personal identifiers<br>(1)-2. Data deletion for small mesh areas<br>(2) Improvement of statistical processing accuracy through the combination with reliable data |

## 3.8 Smart Buildings Use Case[18]

Here, we will introduce a use case related to the sharing of data obtained from facilities and an agile governance platform, provided by SoftBank Corp. (a research and development example).

### 3.8.1 Data to be Shared

In addition to the data collected by surveillance cameras and sensors installed in systems and infrastructure managed by the government or local municipalities, other data from robot operators, building operators, and various systems are integrated. This includes operational data from robots and drones, LiDAR data, elevator operation data from building OS, and more.

For example, at a university facility, these data are used on the same platform to provide a range of services to various operators, such as robot operation, beverage delivery, facility security, individualized support during disasters, and congestion forecasting.

### 3.8.2 Domains of Data Sharing

Since the data from multiple stakeholders is shared and integrated on the same platform, the sharing and integration of data are conducted in accordance with soft laws, such as rules and regulations set by businesses, local governments, private properties, and buildings. These rules and regulations define the handling, scope, and granularity of data sharing.

Additionally, the businesses receiving the data are limited to those approved by the platform operator (in the case of the demonstration project, the university corporation) and the authorized businesses or services.

### 3.8.3 Risks and Uncertainties Related to Data

There is a risk regarding the authenticity of the data, as there is a possibility that businesses may not provide accurate data or may be unable to do so.

Additionally, the risk of ensuring the confidentiality of the data is also recognized as a challenge.

### 3.8.4 Countermeasures for Risks

Regarding the potential issue of businesses not providing accurate data or being unable to do so, efforts are being made to address this by obtaining circumstantial evidence from infrastructure independently and cross-referencing it with robot operators' logs to verify accidents or near-misses. Additionally, pre-operation behavior checks of robots are performed to understand their operational tendencies from the logs. From a procedural standpoint, certification of robot operators and service providers is conducted in advance to ensure the correct provision of data by businesses. If the data holder fails to provide data, the system attempts to address the issue by filling in circumstantial evidence from other data sources outside of the robot operator, using information from the infrastructure.

Regarding the protection of data confidentiality, measures are being taken to address the issue through authentication and authorization of data access rights, as well as protecting the information using techniques such as secret sharing and image processing.

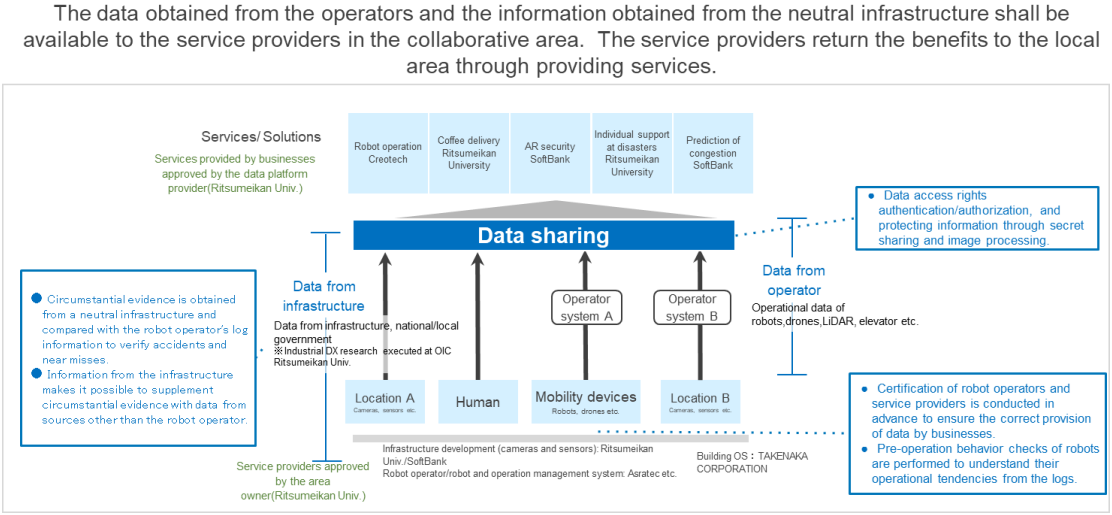



Figure 3-19 Measures to ensure data authenticity and confidentiality

Table 3-7 Summary of Q1–Q4: Smart Buildings Use Case

| | |
|---|---|
| Q.1 | Data to be Shared |
| | ✓ Surveillance cameras, etc. (← Government/municipality systems/infrastructure)<br>✓ Robot/drone operation data, LiDAR data, elevator operation data, etc. (← Robot operators, building system operators, etc.) |
| Q.2 | Domains of Data Sharing |
| | ✓ Sharing and integrating multi-stakeholder data on the platform based on rules and regulations set by businesses, local governments, private properties, and buildings. |

| Q.3 Risks and Uncertainties Related to Data |
| --- |
| ✓ Data authenticity – The possibility that businesses may not provide or be able to provide accurate data.<br>✓ Data confidentiality – Ensuring the protection of the data's confidentiality. |
| Q.4 Countermeasures for Risks |
| (1)-1. Pre-certification of robot operators and service providers<br>(1)-2. Pre-operation behavior checks of robots and understanding operational tendencies from logs<br>(1)-3. Obtaining circumstantial evidence from infrastructure independently and cross-referencing it with robot operators' logs to verify accidents or near-misses<br>(2) Data access rights authentication/authorization, and protecting information through secret sharing and image processing |

# 4. International Examples of Industrial Data Sharing and Trust

In Chapter 3, we outlined various domestic use cases and summarized their specific trust-related requirements, primarily focusing on current initiatives within Japan. However, as industrial data sharing extends internationally, it becomes necessary to consider cross-border interoperability and associated trust frameworks. This chapter, therefore, presents an overview of international examples, focusing particularly on initiatives in Singapore, Canada, and the United Kingdom as representative examples of trust frameworks, as well as the Catena-X data sharing initiative in Europe.

## 4.1 Initiatives of Catena-X

Catena-X represents a significant example of industrial data sharing in Europe and is already commercially operational as an industrial data space. In the second meeting of this study group, Mr. Kraemer and Mr. Tsuchiya from Catena-X e.V. presented on "Cross-Industry Data Sharing in the European Automotive Industry." This section outlines Catena-X's efforts to establish trust within its industrial data sharing ecosystem, primarily based on the contents presented by both speakers. Specifically, it describes Catena-X's initiatives from two perspectives—governance (with a particular focus on the certification system for applications and the Gaia-X trust framework) and system architecture.

### 4.1.1 Governance

Within the Catena-X data space, common operational rules, communication protocols, and standardized data models for each use case are established by the Catena-X Association as the "Catena-X Standard," which is publicly available on their website[19]. Additionally, various functionalities implemented within the Catena-X data space are being developed as open-source software collectively known as "Tractus-X" under the Eclipse Foundation. Operations of data spaces aligned with the Catena-X Standard are governed by rules that allow not only European organizations but also global entities to operate such data spaces. Currently, Cofinity-X, established in 2023, manages these data space operations. Software services compliant with the Catena-X Standard, intended to realize Catena-X's vision, are provided by companies such as T-Systems, Siemens, and SAP.

[19] Catena-X, "Librarian," accessed February 3, 2025, https://catena-x.academy/librarian/.

To offer various services within the Catena-X data space, organizations must prepare software compliant with the standards set by the Catena-X Association, particularly concerning data sovereignty, interoperability, and security, and then obtain certification. A system for independent third-party assessment has been established to verify the structural conformity of data as well as the implementation of mechanisms to ensure trust during the certification process. Only certified software is presented by the operating service provider, Cofinity-X, to contracted users on its marketplace for business applications and enablement services.

The certification process for business applications and similar services consists of nine steps: "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," and "Part of the Catena-X data ecosystem."

（The certification process for business applications comprises nine steps:）

- Request via Catena-X：Submit an application for certification through the Catena-X website.
- Information to CAB：Contact a Certification Assessment Body (CAB). A list of CABs is available on the Catena-X website.
- Contract：Formal agreement is concluded between the CAB and the applicant.
- Sending the list of requirements：The CAB provides the applicant with necessary information for the certification audit, including audit criteria, relevant examples, history of existing certifications (e.g., ISO 9001), required documentation, and a self-assessment questionnaire.
- Kickoff & FAQ：An initial briefing is conducted, introducing the scope of certification (use cases, applications, etc.) and addressing frequently asked questions.
- Certification：The CAB conducts the audit based on CAF specifications and informs the applicant of the audit results.
- Results handed over to Catena-X：The CAB submits the certification results to Catena-X.
- Awarding of the certificate： The CAB awards the certificate on behalf of Catena-X, and Catena-X publishes the certification results on their official website.
- Part of the Catena-X data ecosystem：The certified entity formally joins the Catena-

X data ecosystem. The certificate remains valid for a period of 12 months.

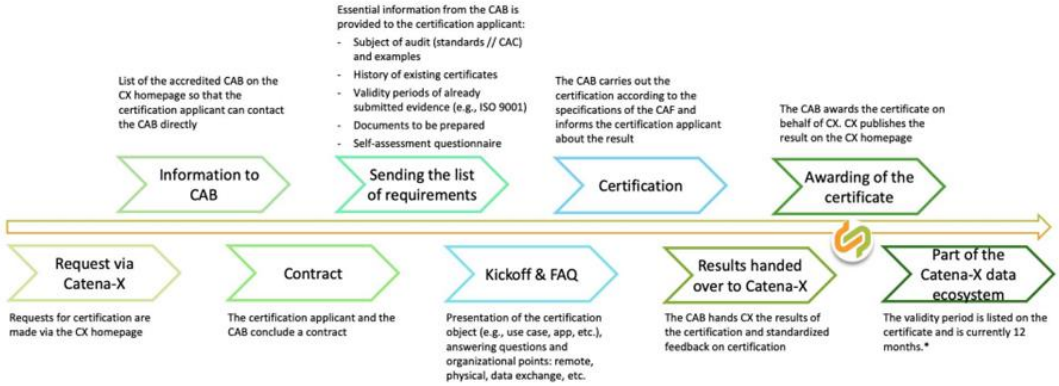



Figure 4-1 Certification Process for Applications in Catena-X

### 4.1.2 Architecture

#### （1）Fundamental Design Principles and Background

From the outset, the Catena-X initiative has emphasized the following core design principles:

- Avoidance of data centralization, preventing any single dominant player from centralizing control over data.
- Secure and confidential handling of data, ensuring robust protection of trade secrets and proprietary information.
- Ensuring data sovereignty, defined as data rights holders retain continuous and appropriate control over their data.

In terms of architecture, Catena-X accommodates regional differences by permitting variations at the local or national level—such as diverse regulatory frameworks, standards, and identification systems—while maintaining a globally unified upper layer aligned with international standards. This approach guarantees trust (verifying identity authenticity, data authenticity, and protection against data manipulation or falsification) and secures data sovereignty at a global scale. To realize this model, technology demonstrations involving companies such as NTT Communications, Fujitsu, and T-Systems commenced in 2024. Additionally, an MoU was signed between IPA and Catena-X on April 22, 2024, specifically targeting interoperability for data sharing within the automotive industry.

Furthermore, Catena-X adopts a decentralized architecture where data remains distributed among participants without central aggregation. Under this design, unauthorized parties

cannot freely access data, thus preserving privacy and security. This approach was chosen not only to achieve ambitious global goals (e.g., establishing a global circular economy), but also to enable safe and secure data sharing across regions with differing rules governing data utilization and cross-border transfers. By avoiding dependence on a single vendor or provider, this approach seeks broad inclusivity, allowing diverse organizations worldwide to participate actively in the data-sharing ecosystem.

### （2）Data Sharing Mechanism

In the Catena-X data space, data sharing mechanisms are established in accordance with the Gaia-X Trust Framework to ensure trustworthiness during data exchanges. As of 2024, T-Systems (Germany) was the first organization to serve as a trust anchor within the Catena-X framework[20].

The following diagram illustrates the mechanism of actual data sharing within a decentralized data space.

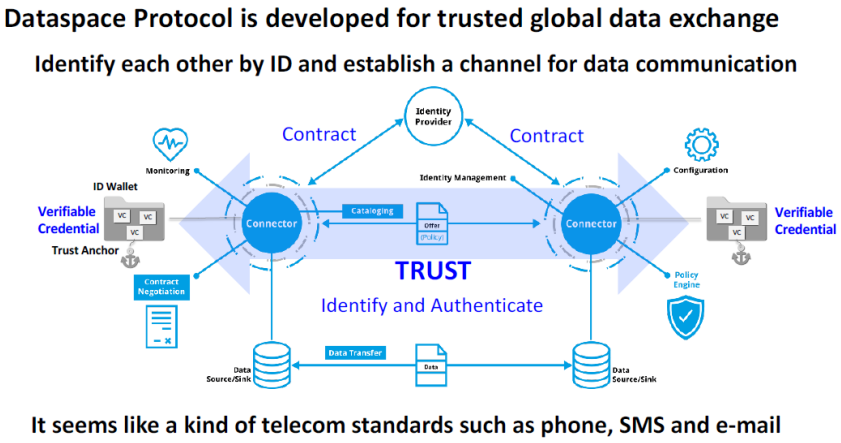



Figure 4-2 Data Sharing Mechanism in a Decentralized Data Space[21]

In this architecture, "Connectors" serve as the primary data exchange gateways within the decentralized data space. Each Connector obtains a corporate ID from an Identity Provider, which supplies the identifiers for participating organizations. Connectors then mutually negotiate and verify the identity and attributes of their counterpart organizations before initiating actual data exchanges.

[20] T-Systems, "Catena-X Anchors Trust on T-Systems," accessed February 3, 2025, https://catena-x.academy/librarian/.

[21] International Data Spaces Association (IDSA), "Dataspace Protocol," accessed February 3, 2025, https://docs.internationaldataspaces.org/ids-knowledgebase/dataspace-protocol.

The actual data exchange occurs independently of the Connector-to-Connector negotiation described above, through a separate communication route known as the "Data Plane." This ensures direct and secure data transfers between collaborating parties without involving any intermediaries. Participants in the Catena-X data space manage their own digital wallets, where Verifiable Credentials (VCs) are stored. These VCs are presented during data exchange processes to verify attribute information, ensuring trusted and authenticated interactions.

Catena-X has adopted emerging decentralized trust technologies that are expected to become increasingly prevalent in industrial data ecosystems. The aforementioned VCs represent one such decentralized trust technology, enabling distributed issuance and verification of digital credentials to authenticate attributes securely and reliably.

## 4.2 Examples of Trust Frameworks in Other Countries[22]

During the second meeting of this study group, Mr. Hamaguchi presented a report titled "Data Sharing and Required Trust in Other Countries," introducing international initiatives related to data sharing and trust frameworks. Based primarily on the content of this presentation, this section provides an overview of major trust frameworks adopted by Singapore, Canada, and the United Kingdom, specifically:

- Trusted Data Sharing Framework (TDSF) (Singapore)
- Pan-Canadian Trust Framework (PCTF) (Canada)
- Digital Identity and Attributes Trust Framework (DIAF) (United Kingdom)

In addition to these trust frameworks, this section also introduces the activities of Icebreaker One (IB1), an organization responsible for designing and operating data spaces in the United Kingdom.

### 4.2.1 Initiatives in Singapore（TDSF）

#### （1）Overview

Singapore developed the Trusted Data Sharing Framework (TDSF) in 2019 to facilitate the growth of its digital economy and support its broader "Smart Nation" initiative.

[22] METI, "Materials No.4, 2nd Meeting of the Ouranos Ecosystem Trust Study Group" accessed February 3, 2025, https://www.meti.go.jp/policy/mono_info_service/digital_architecture/ouranos/ouranos_trust/241217/siryo4.pdf

TDSF, developed by the Info-communications Media Development Authority (IMDA) in sharing with the Personal Data Protection Commission (PDPC), is positioned as a set of government-issued guidelines. Rather than legally binding regulations or systems, it provides guidance aimed at enabling smoother data sharing practices.

### （2）Objectives

The primary objectives of TDSF are as follows:

1. Promote inter-organizational data sharing
2. Address challenges associated with data sharing
3. Encourage the development of new products and services
4. Foster consumer trust

### （3）Components of the Framework

TDSF comprises the following four parts. By establishing a series of trust technologies and a baseline "common data sharing language," this framework intends to help organizations adopt a systematic approach to understanding a broad range of considerations necessary for establishing trustworthy data-sharing partnerships[23].

Table 4-1 Overview of TDSF

| Part | Description | Recommended Readers |
|---|---|---|
| Data Sharing Strategy | Organizations can understand what types of data are beneficial to share, how to evaluate their value, and various arrangements or models that can facilitate data sharing. | · Key decision-makers and stakeholders involved in data sharing processes<br>· Internal business units/users |

[23] IMDA, "Trusted Data Sharing Framework," accessed February 3, 2025, https://www.imda.gov.sg/-/media/imda/files/programme/collaboration/trusted-data-sharing-framework.pdf.

| | | |
|---|---|---|
| Legal and Regulatory | Organizations can understand compliance requirements related to data sharing and how to establish legal relationships between involved parties to enable trustworthy data sharing. | · Users leading data-sharing projects<br>· Business units responsible for data collection, management, and utilization<br>· Advisory teams related to technology, risk, and compliance |
| Technical and Organisation | Organizations can understand the technical considerations and mechanisms involved in transferring data to other organizations. | · Users leading data-sharing projects<br>· Business units responsible for data collection, management, and utilization<br>· Advisory teams related to technology, risk, and compliance |
| Operationalising Data Sharing | Organizations can understand additional considerations necessary after data sharing has commenced. | · Users leading data-sharing projects<br>· Advisory teams related to technology, risk, and compliance |

Additionally, TDSF is designed as a set of industry-oriented guidelines intended primarily for use within the commercial and non-government sectors. It covers both personal data and business data. Since data sharing typically involves the transfer of data assets, it is critical that each party involved manages data assets responsibly and accountably. To facilitate this, TDSF introduces six trust principles to guide responsible data sharing among stakeholders.

**（Six Trust Principles）**

· Transparency
  - ➢ Ensuring that all stakeholders involved in data sharing have access to all necessary information for the success of the data-sharing partnership.

- Accessibility
  - Ensuring that involved parties have access to the required data when it is needed.
- Standardization
  - Applying consistent legal, technical, and other measures to data-sharing partnerships.
- Fairness and Ethics
  - Going beyond merely meeting personal data protection, technical and security standards, or regulatory requirements.
  - Ethical standards must be incorporated from the initial design stages in the creation and use of data-sharing systems and frameworks.
- Accountability
  - Ensuring compliance with data protection laws and other specific rules related to data-sharing partnerships. Each party should have robust governance structures and foster a corporate culture where employees take responsibility for handling data.
- Security and Data Integrity
  - Implementing measures and mechanisms designed to securely protect and safeguard information and data, thereby providing a secure environment for data sharing.

#### （4）Certification Mechanism

Currently, TDSF does not include a formal certification or conformity assessment mechanism.

### 4.2.2 Initiatives in Other Countries: Pan-Canadian Trust Framework (PCTF)

#### （1）Overview

PCTF was developed by the Digital ID & Authentication Council of Canada (DIACC), a public-private nonprofit organization. An overview of PCTF was first published in 2016, and its initial version was released in 2019 to establish trustworthiness within Canada's digital identity ecosystem.

#### （2）Objectives

PCTF defines principles and standards for managing digital identities in Canada, as well as a series of processes associated with creating, managing, and providing digital IDs. It aims

to serve as a reference for both public and private stakeholders, researchers, and other parties involved in the field of digital identity.

### （3）Components of the Framework

PCTF consists of seven trusted components, each specifying requirements according to four defined Levels of Assurance (LoA 1–4).

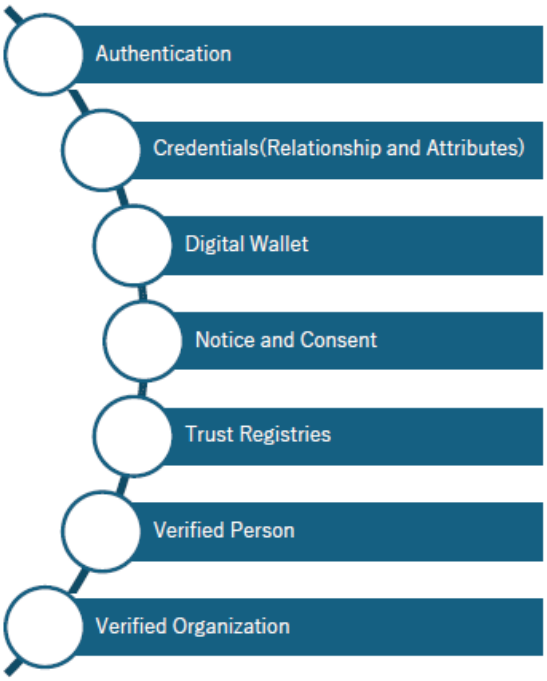



Figure 4-3 Seven Components of PCTF

In particular, the requirements for components most directly related to data sharing are as follows:

Table 4-2 Components Related to Data Sharing and Their Requirements

| Component | Description | Requirements |
|---|---|---|
| Authentication | Verification of digital identities | Defines trusted processes (credential issuance, authentication, session initiation/termination, credential suspension/recovery/maintenance/revocation), roles (authentication and credential service providers), risks and recommended mitigation measures, specific use cases (e.g., verifiable credentials in digital wallets, biometric authentication), and conformity requirements corresponding to specified trust levels. |
| Credentials | All information used for authentication | Specifies conformity requirements regarding lifecycle management of credentials at defined assurance levels, including trusted relationship processes (definition, declaration, endorsement, verification, and denial), trusted attribute processes (definition, binding, maintenance, revocation), and associated risk assessment. |
| Digital Wallet | Digital wallet that stores digital IDs and related assets | Defines trust relationships (applicant–issuer–holder–verifier–repository), trusted processes (wallet instantiation and security, credential management and usage, consent management), roles, risk repository and mitigation strategies, and conformity requirements. |
| Trust Registries | Mechanisms by which digital ID ecosystem participants verify the trustworthiness of other ecosystem participants | Sets conformity requirements related to governance, operations, registration, and credential management for trust registries. Participants registered in trust registries include issuers, verifiers, and wallet providers. |

| | | |
|---|---|---|
| Verified Organization | Identity verification of organizations | Defines processes and conformity criteria for establishing and verifying organizational identity, ensuring proper validation of organizations, and creating reliable digital representations of organizations. |

### （4）Certification Mechanism

A certification scheme to assess conformity with PCTF requirements, based on ISO/IEC 17065, was developed and became operational in 2022[24]. Organizations involved in the certification process include Recognized Readiness Advisors, DIACC Auditors, and Independent Review Committee. As of the present, two services have successfully obtained certification.

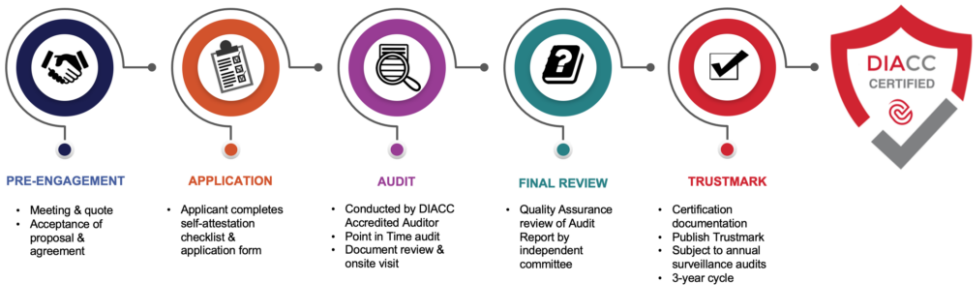



Figure 4-4 The Certification Journey

[24] DIACC, "Certification Program," accessed February 3, 2025, https://diacc.ca/trust-framework/certification-program/

**（Organizations Involved in Certification）**

- Recognized Readiness Advisors
  - Experts who provide guidance and assistance to organizations preparing for certification.
  - DIACC Auditors cannot act as Recognized Readiness Advisors due to conflicts of interest.
- DIACC Auditors
  - Professionals accredited through a process based on ISO/IEC 17020 requirements.
  - Possess the competence, experience, and qualifications necessary to perform audits against PCTF.
- Independent Review Committee
  - A volunteer body composed of international experts in digital identity, auditing, compliance, and information security.
  - Responsible for conducting quality reviews of audit results provided by DIACC Auditors.

### 4.2.3 Initiatives in the United Kingdom

#### 4.2.3.1 Digital Identity and Attribute Framework

**（1）Overview**

DIAF is being developed by the UK government's Department for Digital, Culture, Media & Sport (DCMS) to enable people to verify their identities more quickly and easily using emerging technologies. The framework has been continuously evolving, with the latest version (v0.4) released in 2024, formally incorporating technical components such as digital wallets and VCs. Starting in 2025, the certification process for version 0.4 will be initiated, followed by annual reviews and updates. From 2025 onwards, the framework is expected to have its legal basis established through the Data Protection and Digital Information Bill (ECHR Memorandum).

**（2）Objectives**

DIAF has three primary objectives:

1. Enhance the trustworthiness of digital identity services
2. Stimulate innovation and investment
3. Ensure the development and deployment of secure digital identity services

### （3）Components of the Framework

DIAF defines Orchestration Service Providers, which deliver the technological infrastructure necessary to ensure secure data sharing among digital identity and attribute providers as well as participants within the trust framework. Each of these providers is required to obtain certification under the trust framework. On the other hand, entities identified as Relying Parties, which receive digital identities and attribute information from users to deliver services based on verification outcomes, are not mandated to obtain certification. However, to maintain market security, these Relying Parties must adhere to flow-down conditions imposed by certified organizations within the trust framework.

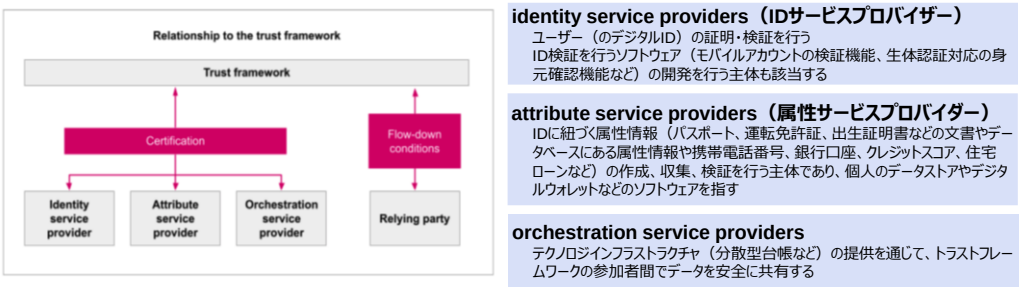



Figure 4-5 Relationship Between Trust Framework and Stakeholders

### （4）Certification Mechanism

A rigorous certification process is established to ensure organizations comply with the rules and standards set forth by DIAF. This process, referred to as Accredited Certification, aligns with international certification standards such as ISO/IEC 17065 and is essential for enabling users to trust digital identity services. Through this certification process, organizations undergo independent assessment by third-party entities to verify compliance with DIAF requirements. Organizations deemed compliant are awarded a Trust Mark, officially recognizing their trustworthiness. The certification process consists of the following five steps:

1. Standards established by the Governing Body
   - DCMS, serving as the governing body of DIAF, establishes standards, rules, and the scope of certification for digital identity and attribute management.
   - Compliance with these standards ensures that organizations provide trustworthy services.
2. Accreditation of Certification Bodies by an Accreditation Body
   - The United Kingdom Accreditation Service (UKAS), as the government-appointed

accreditation body, accredits Certification Bodies.

- Accredited Certification Bodies are thereby authorized to evaluate and certify organizations against the framework's standards.

3. Assessment and Certification of Organizations by Certification Bodies
   - Organizations and schemes (e.g., digital identity providers) claiming compliance with DIAF standards are audited by accredited Certification Bodies.
   - Certification confirms organizational adherence to framework requirements.
4. A Conformity Assessment by Auditors
   - Qualified auditors perform audits on organizations and Certification Bodies to ensure all requirements have been fulfilled.
   - Audit findings are reported back to both organizations and Certification Bodies, along with feedback and recommendations for improvement as necessary.
5. Awarding of the Trust Mark
   - The Governing Body awards the Trust Mark to certified organizations.
   - Organizations holding the Trust Mark are officially recognized as compliant with DIAF standards, thereby enhancing user trust.

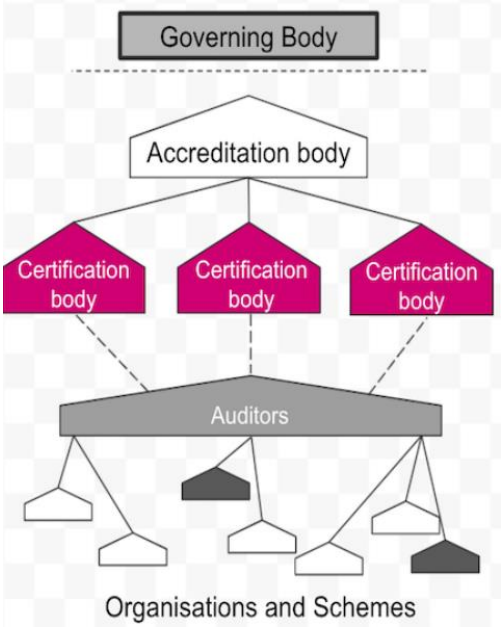



Figure 4-6 Organisations and Schemes[25]

[25] Department for Digital, Culture, Media & Sport (DCMS), "Digital Identity and Attributes Consultation," accessed February 3, 2025, https://www.gov.uk/government/consultations/digital-identity-and-attributes-consultation.

#### 4.2.3.2 Icebreaker One

**（1）Overview**

IB1 is a non-profit organization launched at the 2020 World Economic Forum (Davos). Its mission is to build data sharing infrastructure to support decision-making for climate action. IB1 aims to aggregate distributed industrial and environmental data from multiple sectors—including energy, finance, water management, transport, the built environment, and agriculture—and provide these data in a usable format to users such as businesses and governments.

IB1 emphasizes open-source technologies and open data, developing open standards and frameworks to facilitate secure and seamless data sharing between organizations. Through these efforts, IB1 is enhancing cross-sectoral data sharing and advancing the creation of a robust "Data Infrastructure for Net Zero."

**（2）Organizational Structure[26,27]**

IB1 operates as an independent non-profit organization, with funding primarily derived from project-specific grants, membership fees from corporations and organizations, and donations. Through its membership model, IB1 maintains neutrality by strictly adhering to non-profit operations. Currently, IB1 comprises more than 70 member organizations representing diverse sectors, including government and public institutions, private enterprises, academic institutions, non-profits, and think tanks.

Table 4-3 IB1 Membership Fees

| Organization Size (Annual Revenue) | Monthly Fee (£) |
|---|---|
| Large Companies (£36 million and above) | 5,000£ |
| Medium-sized Companies (£10m – £36m) | 3,000£ |
| Small-sized Companies (£2m – £10m) | 500£ |
| Micro-enterprises / Startups (up to £2m) | 250£ |
| Public Sector (e.g. Local Authorities) | 250£ |
| Ecosystem Supporters (e.g. Trade bodies) | 0 |

[26] Icebreaker One, "Opening Icebreaker One at UN HQ," accessed February 21, 2025, https://ib1.org/2019/09/24/opening-icebreaker-one-at-un-hq/.

[27] Icebreaker One, "Open Energy Membership," accessed February 21, 2025, https://energy.icebreakerone.org/join/.

| | |
|---|---|
| Policy partner (e.g. Government, Regulators) | to be confirmed |

### （3）Key Activities

This section highlights two main initiatives of IB1: the Icebreaking Process and the Core Trust Framework (CTF).

#### 1）Icebreaking Process[28]

The Icebreaking Process is a collaborative approach proposed by IB1 to co-create rules for data sharing. In this process, stakeholders initially come together to identify key use cases and evaluate their potential value and impacts. Specifically, the process involves the following steps:

1. Identifying User Needs and Impacts
   - Clarify which data is necessary and evaluate its market value.
2. Establishing Technical Infrastructure
   - Define technical standards and system requirements essential for data sharing.
3. Data Licensing and Legal Preparation
   - Develop appropriate rules and legal frameworks to enable legally compliant data sharing.
4. Communication and Engagement
   - Coordinate with data providers, users, and regulators to raise awareness among stakeholders and facilitate sharing.
5. Policy and Regulatory Alignment
   - Work closely with governments and regulators to propose and implement suitable policies and regulatory frameworks.
   - This process enables organizations to achieve safe and efficient data sharing.

[28] Icebreaker One, "Icebreaking," accessed February 21, 2025, https://ib1.org/icebreaking/.

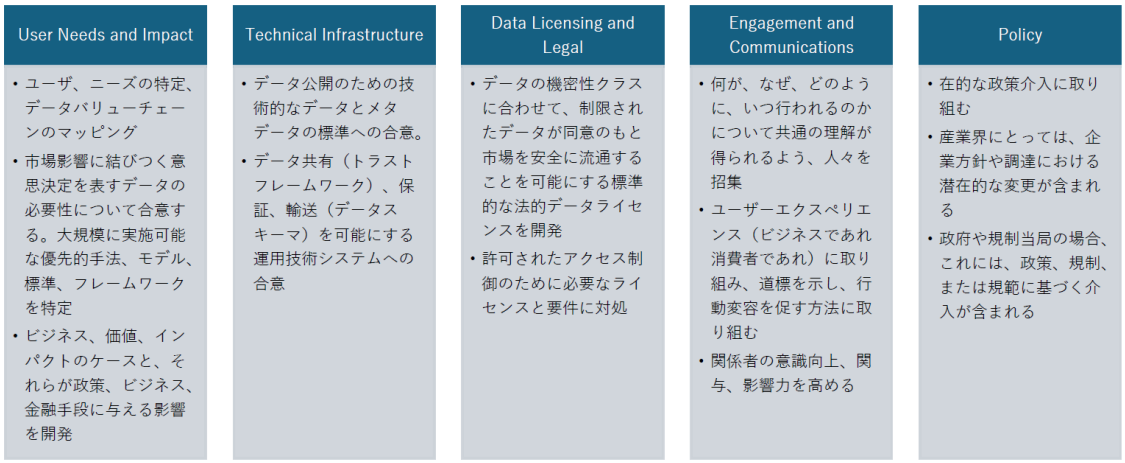



Figure 4-7 Icebreaking Process

In this process, IB1 operates as a neutral facilitator and secretariat, forming a Steering Group (operational committee) comprising representatives from industry, government, and academia, as well as up to five advisory groups specializing in areas such as technology, legal, and policy. Under strong governance, IB1 leads a co-design effort involving all stakeholders to develop a “Scheme,” which serves as a rulebook for data sharing. This Scheme includes the definition of specific use cases, the necessary legal, technical, and policy arrangements for implementation, and strategies for stakeholder communication. The Icebreaking Process systematically identifies challenges from both technical perspectives (such as APIs and data standards) and non-technical perspectives (including contracts and policies), documenting consensus-based rules. The resulting Scheme is then implemented as practical, real-world rules through the Core Trust Framework (described in the following section).

### 2）**Core Trust Framework**[29]

The Trust Framework provided by IB1 serves as a foundational structure for trusted data sharing among organizations. To operationalize the "Schemes" developed through the Icebreaking Process mentioned above, the Trust Framework ensures technical and contractual trust among organizations, underpinned by shared rules and common standards. The Core Trust Framework (CTF), in particular, establishes fundamental obligations and services applicable to all participating organizations, functioning as an entry point for involvement in individual data-sharing Schemes. Built upon the foundation of the CTF,

[29] Icebreaker One, "Core Trust Framework (CTF)," accessed February 21, 2025, https://ib1.org/tf/ctf/.

sector-specific Trust Frameworks—such as those tailored for energy, water, and other sectors—are developed. Organizations joining CTF are required to become IB1 members and agree to CTF's terms and conditions. This structure is designed to streamline the participation process, allowing organizations to qualify for multiple Schemes with a single agreement. The primary services provided by CTF are detailed below:

**（Main Services Provided by CTF）**

- Accredited Organization Registry
  - A publicly accessible registry listing all organizations participating in the Trust Framework. This registry allows stakeholders to verify the trustworthiness (including identity verification and compliance status) of partner organizations involved in data sharing.
- Common Data Infrastructure Definitions
  - Establishes and maintains shared principles and standards necessary for data sharing, including assurance processes and data sensitivity classifications.
  - CTF also provides guidance on best practices for open data publication, encouraging participating organizations to publish their data in a machine-readable and trustworthy format.
- Open Net Zero Catalog
  - A searchable catalog indexing publicly available datasets related to climate and environmental issues.
  - For example, OpenNetZero.org enables the discovery of various datasets beneficial to achieving net-zero targets, such as energy efficiency and carbon emissions data, thus facilitating the use of data by making its existence and location more visible.

### 4.3 Summary

In this chapter, we reviewed international trends related to ensuring trust in industrial data sharing, specifically examining the European initiative Catena-X and selected examples of national trust frameworks from Singapore, Canada, and the United Kingdom.

Our analysis revealed that approaches to establishing trust vary significantly across countries, reflecting different institutional structures and industry dynamics. In particular, the Catena-X initiative represents Europe's approach toward securing trust in industrial data sharing. It utilizes a decentralized architecture, while simultaneously developing industry standards and enhancing governance, aiming to ensure transparency and interoperability across the supply chain.

On the other hand, we observed notable differences in the entities responsible for creating trust frameworks, their institutionalization, and operational methods. For instance, Singapore's TDSF serves as government-issued guidelines rather than a legally institutionalized system, yet it effectively guides industry practices on data sharing. In contrast, Canada's PCTF, developed by a public-private non-profit organization, has implemented a formal certification system to ensure trust within the digital identity ecosystem.

In the United Kingdom, two different approaches coexist: the government-led DIAF and the industry-driven IB1. DIAF, managed by the government, is developing formal certification processes integrated with the legal system to support digital identity services. Conversely, IB1 adopts an industry-led approach, providing a trust framework specifically designed to facilitate secure cross-sector data sharing in support of climate action, particularly through industry-specific initiatives such as energy, finance, transportation, and environmental sectors.

Comparing these cases highlights that no single uniform approach exists for ensuring trust in industrial data sharing. Instead, each country adopts an approach tailored to its regulatory environment and industrial context. To effectively secure trust, it will be critical to understand these diverse approaches and clarify essential trust-related elements, adapted to each country's specific circumstances.

# 5. Analysis and Approaches for Establishing Trust in Industrial Data Sharing

In this chapter, based on the discussions presented in Chapters 3 and 4, we summarize our analytical approach to establishing trust in industrial data sharing and outline the direction for related initiatives within Ouranos Ecosystem.

## 5.1 Analysis of the "Domains" of Data Sharing (Related to Q1 and Q2)

This section categorizes the nature of the data being shared and the contextual characteristics of data sharing, as introduced in Chapter 3.

We first conducted an analysis of the "Domains" of data sharing, following the framework provided by questions Q1 and Q2. Initially, it was necessary to analyze the characteristics of the data being shared. Within the use cases examined by this study group, some involved data capable of identifying individuals or data derived from such personal data, including use cases related to automotive and battery data sharing (Sections 3.1 and 3.2), electric power data sharing (Section 3.6), and people flow data sharing (Section 3.7). Furthermore, some cases exhibited a clearly awareness of issues pertaining to business secrets and the confidentiality of shared data.

When analyzing the domain of application, it is crucial to consider the roles of both public and private sectors, particularly regarding whether the data-sharing contexts have been established or mandated by public laws or regulations. Specifically, several use cases involved compliance requirements arising from the nature of data, such as laws for the protection of personal information and trade secrets. Other cases anticipated contracts between platform operators and participants, or agreements among data-sharing parties. Furthermore, in some instances, such as chemical substance management (Section 3.4), the quality of the shared data is required to adhere to existing industry regulations or international standards.

Moreover, certain use cases demonstrated explicit regulatory control over the permissibility or necessity of data sharing, such as the battery passport (Section 3.3), chemical substance management (Section 3.4), and electric power data sharing (Section 3.6).

## 5.2 Analysis of Risks and Countermeasures Related to Data (Q3 and Q4)

This section provides a summary the data-related risks and uncertainties identified across the use cases discussed in Chapter 3, along with the measures considered or implemented to address them.

Taking into account the characteristics of data shared, and the domain of each use case analyzed in Section 5.1, the following general trust-related risks and countermeasures have been identified. It is essential to distinguish between "Trust" and "Trustworthiness." "Trustworthiness" refers to the quality characteristics demonstrated by the trusted entity, whereas "Trust" represents the subjective judgment or action performed by the trustor based on the presented trustworthiness[30].

- Risks related to participant identity and authenticity
  - Risk of unauthorized participation or identity fraud in data sharing.
  - Countermeasures include implementing identification and authentication mechanisms and rules for participants.
- Risks related to data authenticity and integrity
  - Risk of incorrect or tampered data being circulated.
  - Countermeasures include the implementation of technologies such as electronic signatures and e-Seals[31], blockchain, or smart contracts to prevent data tampering.
- Risks related to personal data protection
  - Risk of non-compliance with domestic and international personal data protection laws, such as failure to obtain necessary consent.
  - Countermeasures include implementing mechanisms capable of tracking the status of consent acquisition and compliance.
- Risks related to protection of business secrets and confidential data
  - Risk of unintentionally disclosing data that providers intend to keep fully or partially confidential, such as trade secrets.
  - Countermeasures include anonymizing or statistically processing confidential data before disclosure and implementing mechanisms to control the scope and recipients of

[30] The concepts of Trust and Trustworthiness are elaborated in the strategic proposal titled "Formation of New Trust in the Digital Society" (original Japanese title:『New Trust Formation in the Digital Society』), published by the Center for Research and Development Strategy (CRDS) of the Japan Science and Technology Agency (JST) (see p.9). Please refer to this document as appropriate.
Available at: https://www.jst.go.jp/crds/pdf/2022/SP/CRDS-FY2022-SP-03.pdf

[31] In Japan, the Ministry of Internal Affairs and Communications published the "Guidelines on e-Seals (Second Edition)" in April 2024. The term “e-Seal” as used in the guidelines means electronic data that is assigned to or logically associated with information that can be recorded in an electronic or magnetic record (a record prepared in an electronic form, a magnetic form or any other forms not perceivable by human senses and used for information processing by computers; hereinafter referred to in the same way throughout the guidelines). It must meet both of the following requirements:
(i) data that indicates the source or origin of the relevant information; and
(ii) data that confirms whether the relevant information has been altered.

data disclosure.

- Risks related to unauthorized or unintended data usage
  - Risk of data being used for purposes not approved by data providers.
  - Countermeasures include control measures enforced through data usage agreements or terms of use.

## 5.3 Insights and Findings from Case Studies

Based on the analysis provided in Section 5.2, we categorized the key elements requiring trust in industrial data sharing into three main groups: "Entities (business operators)," "Data itself," and "Other factors (data integration platforms, etc.)."

### 5.3.1 Risks Related to Entities (Authenticity and Identity Verification)

Risks concerning the authenticity and identity verification of participating entities are common across various use cases. In particular, when considering international sharing, entity authentication and identity verification may also be required externally. Among the use cases examined in this study, some addressed this risk through manual verification processes.

### 5.3.2 Risks Related to Data Itself

Risks regarding the data itself, such as data accuracy and quality, are common issues regardless of the sector. However, the standards required for data accuracy and quality tend to vary depending on the specific sector involved. Moreover, ensuring the trustworthiness of identifiers (IDs) for entities other than business operators (e.g., products) is also recognized as an important challenge in trusted data sharing.

### 5.3.3 Risks Related to Data Integration Platforms and Other Factors

Additional risks identified include the handling and management of data at the recipient end, presenting further challenges to secure data sharing.

## 5.4 Conceptual Approach to Establishing Trust in Ouranos Ecosystem

In this section, based on the analysis presented in Section 5.2, we outline our basic approach to establishing trust within Ouranos Ecosystem for industrial data sharing.

First, the analysis of data-sharing "domains" and associated risks should be conducted by

considering the following points:

- Rules and regulations governing the domain, including applicable laws and the respective roles of the public and private sectors (e.g., whether the domain's data-sharing environment is designed or mandated by public authorities).
- Mechanisms of stakeholder consensus-building within the domain, including whether a central platform entity exists, how end-user perspectives are considered, the status of contracts or agreements among participants, and the existence or absence of international standards.
- Scope of the domain, including whether discussions are limited within a single data sharing infrastructure, extend across connections between multiple data sharing infrastructures or data spaces, or involve international sharing.
- Expansion of the domain, including the scale of growth such as an increase in the number of participants and the extension of the data sharing scope.

Subsequently, solutions, including methods for establishing trust, should be considered to address the clarified risks. For risks related to the data itself, risks associated with data integration platforms and any other risks, appropriate measures depend on the specific requirements defined within each domain. Therefore, methods for addressing these risks must be discussed and managed according to the design and operation of each individual use case.

On the other hand, regarding risks related to the authenticity and existence of entities (business operators), as discussed in Section 5.3.1, such risks commonly exist across various use cases. Consequently, cross-sectoral solutions leveraging government-verified information could potentially serve as an effective approach for establishing trust. A practical example of entity authentication and identity verification based on governmental information is the "gBizID"[32] provided by Digital Agency of Japan. However, if a given domain has requirements exceeding the assurances provided by such general solutions, additional measures will be necessary.

[32] gBizID is an identity provider operated by the Digital Agency of Japan for business entities, including corporations and sole proprietorships. By obtaining a gBizID, business operators can use a single ID and password to access multiple government administrative systems. gBizID Prime is issued after verifying the identity of the business entity's representative.

## 6. Conclusion

Through promoting cross-enterprise and cross-industry data utilization, Ouranos Ecosystem aims to strengthen corporate and industrial competitiveness through public-private collaboration. In this study, we reviewed and analyzed domestic use cases as well as international examples to clarify the concept and approach for establishing trust in data sharing within Ouranos Ecosystem. By examining the "domains" of data sharing, we identified risks and requirements, concluding that initiatives should be advanced based on the specific elements and standards required by each domain. Furthermore, our analysis highlighted a common requirement across multiple cases—the authenticity and identity of entities (business operators) engaged in data sharing. This indicates that cross-sectoral use of government-verified information could be an effective way of establishing trust.

Along with enlargement use cases, future topics related to trust in data sharing may include establishing trust across multiple use cases, developing architectures and common components beneficial for interoperability and scalable expansion, and promoting collaboration with various international data spaces. Additionally, to advance trust establishment in data sharing, it will be essential for both public and private sectors to proactively make actions with utilizing existing practices regarding trust, technological solutions and efforts to address identified risks.

Going forward, Ouranos Ecosystem will continue efforts to establish trustworthy data sharing frameworks, enabling a greater number of businesses to effectively utilize industrial data sharing and contributing to enhanced industrial competitiveness.

## List of Members

### Chairperson

- **Hiroshi Esaki**, **PhD**, Professor, Graduate School of Information Science and Technology, The University of Tokyo

### Members

- **Kenichi Ito**, Division Senior Manager, MaaS Division / Strategies & Business Platform Department, Marketing Headquarters, East Japan Railway Company
- **Naohiko Irie**, Co-chair, Working Group 1, Robot Revolution & Industrial IoT Initiative (RRI)
- **Fumiko Kudo**, Specially Appointed Associate Professor, Research Center on Ethical, Legal and Social Issues, Osaka University
- **Akira Sakaino**, Member, Industrial Data Space Study Group, Japan Business Federation (Keidanren)
- **Hironobu Tamba**, Vice President, Technology Unit, Data Platform Strategy Division Head & Digital Infrastructure Architect Office Head, SoftBank Corp.
- **Satoru Tezuka**, Project Professor, Keio University Global Research Institute
- **Soshi Hamaguchi**, CEO, Maximax Corporation
- **Tatsuto Fujii**, Executive Officer, General Manager, Digital Planning Department, Mizuho Financial Group, Inc.
- **Teruyoshi Fujiwara**, Chairperson, Automotive and Battery Traceability Center Association, Inc. (ABtC)
- **Kiyoto Furuta**, Leader, CMP Task Force
- **Yasushi Matsumoto**, Fellow, Japan Network Security Association (JNSA)
- **Hiroshi Mano**, Executive Director / General Secretary, Data Society Alliance
- **Hisafumi Mitsushio**, Associate Professor, Faculty of Health Data Science, Juntendo University
- **Taketo Yasui**, Executive Director and Secretary General, Secured Meter Data Sharing Association
- **Toshikazu Yoshida**, Director, Chief of Secretariat, Japan Digital Trust Forum

## List of Observers

- General Management and Strategy Planning Unit, National Center of Incident Readiness and Strategy for Cybersecurity (NISC), Cabinet Secretariat
- Data Strategy and Inter-Enterprise Transactions Team, Citizen Services Group, Digital Agency
- Trust Policy Team, Digital Society Infrastructure Group, Digital Agency
- Office of the Director-General for Cybersecurity, Ministry of Internal Affairs and Communications
- Digital Economy Promotion Office, Regional Communications Promotion Division, Information and Communications Bureau, Ministry of Internal Affairs and Communications
- DX Team, Policy Planning and Coordination Division, Manufacturing Industries Bureau, Ministry of Economy, Trade and Industry
- Automobile Division, Manufacturing Industries Bureau, Ministry of Economy, Trade and Industry
- Technical Regulations, Standards and Conformity Assessment Policy Division, Innovation and Environment Policy Bureau, Ministry of Economy, Trade and Industry
- Resource Efficiency and Circular Economy Division, GX Policy Group, Innovation and Environment Policy Bureau, Ministry of Economy, Trade and Industry
- Cybersecurity Division, Commerce and Information Policy Bureau, Ministry of Economy, Trade and Industry
- Battery Industry Division, Commerce and Information Policy Bureau, Ministry of Economy, Trade and Industry
- Strategic Policy Planning Division, Trade Policy Bureau, Ministry of Economy, Trade and Industry
- Trade Promotion Division, Trade Policy Bureau, Ministry of Economy, Trade and Industry
- Electricity Industry and Market Office, Electricity and Gas Industry Department, Agency for Natural Resources and Energy, Ministry of Economy, Trade and Industry
- Planning Office, General Affairs Division, Railway Bureau, Ministry of Land, Infrastructure, Transport and Tourism
- New Energy and Industrial Technology Development Organization
- Information-technology Promotion Agency, Japan
- Japan Electronics and Information Technology Industries Association
- Japan Users Association of Information Systems
- Japan Institute for Promotion of Digital Economy and Community (JIPDEC)
- Japan Accreditation Council

## Record of Meetings of This Study Group

**1st Meeting (November 20, 2024)**

Agenda

1. Opening
2. Explanation of materials by the Secretariat
3. Explanation by Member Fujiwara (Cross-industry data collaboration for the automotive sector in Europe)
4. Key points raised by the Secretariat
5. Open discussion
6. Summary and next steps

**2nd Meeting (December 17, 2024)**

Agenda

1. Opening
2. Explanation of materials by the Secretariat
3. Explanation by Mr. Kraemer and Mr. Tsuchiya (Cross-industry data sharing for the automotive sector in Europe)
4. Explanation by Member Hamaguchi (Data sharing and required trust in other countries)
5. Key points raised by the Secretariat
6. Open discussion
7. Summary and next steps

**3rd Meeting (January 31, 2025)**

Agenda

1. Opening
2. Explanation of materials by the Secretariat
3. Explanation by Member Fujiwara (Trust considerations assuming future use cases in the automotive and battery sectors)
4. Explanation by Member Furuta (Overview of the CMP concept and approach to trust)
5. Explanation by Member Ito (Use cases of data sharing at JR East)
6. Explanation by Member Yasui (Third-party provision scheme for electric power data)
7. Explanation by Mr. Orihara on behalf of Member Tamba (Introduction to SoftBank's initiatives)
8. Explanation by the Digital Agency (Identity Provider of government system for Business Entity, gBizID)
9. Key points raised by the Secretariat
10. Comments from members
11. Summary and next steps

**4th Meeting (March 5, 2025)**

Agenda

1. Opening
2. Explanation of Secretariat materials and the draft report
3. Summary by Chairperson Esaki
4. Comments from members
5. Summary and next steps