Trusted Web

Trusted Web White Paper ver. 3.0 Overview

Nov 2023

Secretariat of the Headquarters for Digital Market Competition,
the Cabinet Secretariat of Japan

Executive Summary

1 Background

- Amid digitalization of social and economic activities, various **pain points** have emerged, including concerns over data reliability due to fake news and disinformation generated by generative AI, the infringement of privacy, excessive dependence on specific services in the winner-takes-all situation, and siloed industrial data that is underutilized.
- When the society is transitioning to "digital society," the Internet and the Web do not ensure trust relationships and sense of security in social activities. Therefore, we must **rebuild trust** on the Internet and the Web.
- In the current trust framework, the portion where data transactions can be verified are limited, and which leaves us **no choice but to trust digital platform operators**, etc. without checking supporting facts. We also rely on them for identifier mechanisms to link data.
- The "Trusted Web" concept was proposed at the Digital Market Competition Council of the Cabinet Secretariat, and in October 2020, the "Trusted Web Promotion Council," consisting of experts from industry and academia, was established. Discussions have been conducted while repeatedly presenting and fleshing out the concept, receiving feedback from use cases, as well as taking international trends into consideration.

2 What is the Trusted Web?

- The Trusted Web is an **initiative to build a new trust framework that provides mechanisms without excessively relying on specific services, for enabling users (individuals and organizations) to keep control of the data related to themselves and to verify the exchanged data and the parties with whom the data is exchanged**.
- Through this, we aim to build a new **trust framework** for various social activities in digital society by **adding certain governance and operational mechanisms, and to realize the creation of new values by various parties**.
- In addition**, building the trust framework in data exchange** through the Trusted Web is extremely important for **facilitating "business-to-business collaboration,"** which is a prerequisite for promoting **digital transformation (DX)** that requires various entities to collaborate across industries and sectors. Furthermore, Trusted Web will ultimately contribute to the **realization of DFFT**.

3 Path toward realization

- Through pilot projects, etc., **various use cases will be created**, and shared and discussed with related parties inside and outside Japan, leading to **the creation of new businesses** through initiatives in line with the direction the Trusted Web should take, and promoting international collaboration.
- Various services that embody the mechanism that the Trusted Web aims are provided, and their areas of use are expanding. In the process, **APIs, data models, and protocols that should be compatible would be identified** while utilizing existing mechanisms to improve trust. The commonization of these will lead to **interoperability and standardization**, and is expected to materialize the Trusted Web.

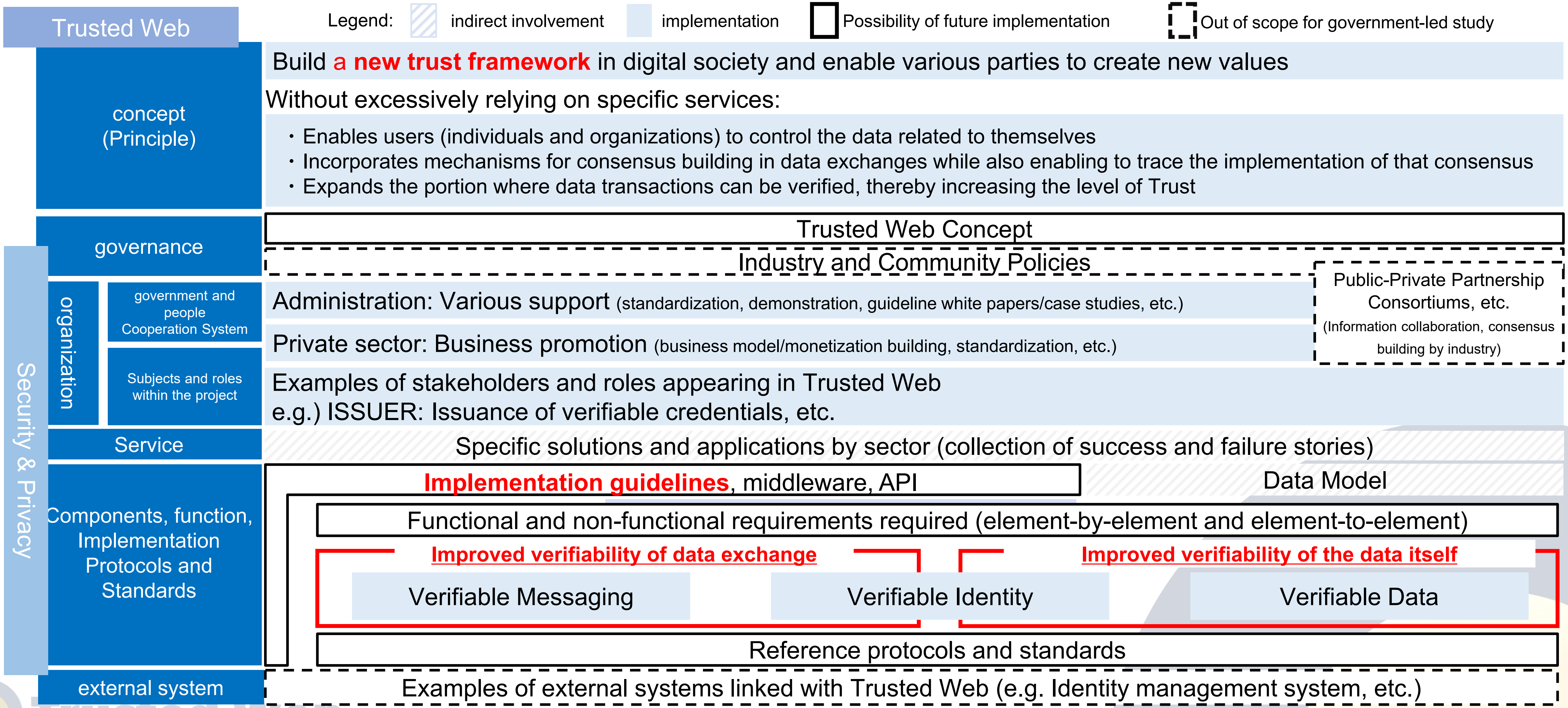
4 Progress since the White Paper ver. 2.0 (published August 2022)

- Through the "Pilot Project for Realization of Trusted Web" in FY2022 and other programs, the benefits and challenges of **various use cases being materialized by private companies and others** were shared, and **materials were provided to help companies find points of contact with their own business**, leading to the creation of new businesses.
- By organizing **the practices and implementation methods** necessary to implement the Trusted Web and **publishing on GitHub, engineers and others will be able to grasp concrete examples, discuss** and update them with each other for service development.
- Based on feedback from the pilot projects , **the architecture was restructured** and the governance supporting it as **the two wheels of the cart was presented.**

1. Overview / Concept

1-1. what is Trusted Web

The Trusted Web is an initiative to build a new trust framework that provides mechanisms without excessively relying on specific services, for enabling users (individuals and organizations) to keep control of the data related to themselves and to verify the exchanged data and the parties with whom the data is exchanged.



Trusted Web

Legend: ▨ indirect involvement 🟦 implementation ☐ Possibility of future implementation ⬚ Out of scope for government-led study

concept (Principle)

Build a **new trust framework** in digital society and enable various parties to create new values

Without excessively relying on specific services:

- Enables users (individuals and organizations) to control the data related to themselves
- Incorporates mechanisms for consensus building in data exchanges while also enabling to trace the implementation of that consensus
- Expands the portion where data transactions can be verified, thereby increasing the level of Trust

Security & Privacy

governance

Trusted Web Concept

Industry and Community Policies

organization

government and people Cooperation System

Administration: Various support (standardization, demonstration, guideline white papers/case studies, etc.)

Private sector: Business promotion (business model/monetization building, standardization, etc.)

Public-Private Partnership Consortiums, etc. (Information collaboration, consensus building by industry)

Subjects and roles within the project

Examples of stakeholders and roles appearing in Trusted Web
e.g.) ISSUER: Issuance of verifiable credentials, etc.

Service

Specific solutions and applications by sector (collection of success and failure stories)

Components, function, Implementation Protocols and Standards

Implementation guidelines, middleware, API

Data Model

Functional and non-functional requirements required (element-by-element and element-to-element)

Improved verifiability of data exchange

Verifiable Messaging

Verifiable Identity

Improved verifiability of the data itself

Verifiable Data

Reference protocols and standards

external system

Examples of external systems linked with Trusted Web (e.g. Identity management system, etc.)

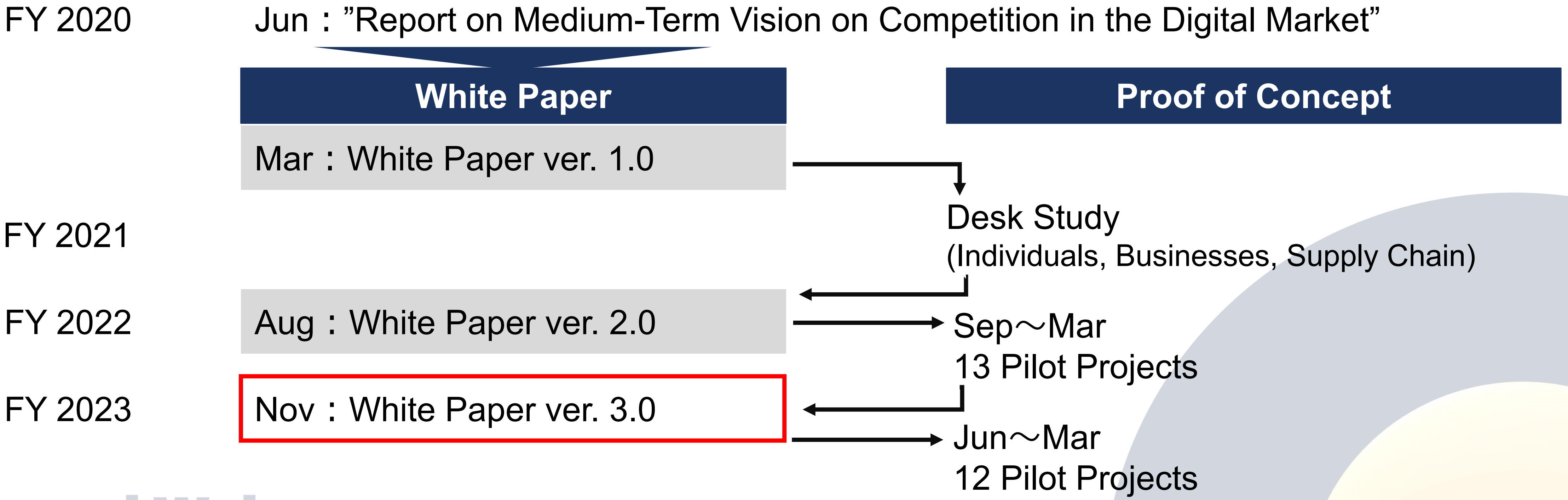
1-2. Background and History of Study

○The digital transformation (DX) of society as a whole is accelerating with the outbreak of COVID-19. **As the cyber and physical spaces are merging**, the society is **transitioning to “digital society”**.

○However, **various issues** have surfaced. It is necessary to search for the **third way** that leads to neither “**excessive dependence on a handful of giant companies**” nor a “**surveillance society**.”

○While the **Internet and the Web**, developed as the foundation of digital society, have data exchange protocols that are in place, much of the **data management, including identity management, depends on the services of platform operators**. As data is siloed, with little external verifiability, the situation allows no option but to believe in those platform operators.

○ In the context of these situations, **“Trusted Web”** was proposed, with the scope to realize Data Free Flow with Trust (DFFT).



FY 2020 — Jun：”Report on Medium-Term Vision on Competition in the Digital Market”

White Paper

Proof of Concept

Mar：White Paper ver. 1.0

Desk Study
(Individuals, Businesses, Supply Chain)

FY 2021

FY 2022 — Aug：White Paper ver. 2.0

Sep～Mar
13 Pilot Projects

FY 2023 — Nov：White Paper ver. 3.0

Jun～Mar
12 Pilot Projects

1-3. Current Issues and Their Causes

○ **The Internet and the Web** were developed as **globally common infrastructure** enabling to widely access information and **creating various services**.

○ However, there is **no adequate mechanism** to **ensure trust relationships and sense of security in various social activities** in the digital society. While **users rely on platform operators for most of their trust, this distortion has created pain points.**

Examples of pain points

○**Concerns about data being exchanged,** due to such as fake news and false data controlling devices
○**Privacy risk** due to aggregation and consolidation of personal data, including biometric information
○**Balance between privacy and public interest**
○**The siloed industrial data** that is underutilized
○Concerns about the sustainability of the ecosystem **due to the winner-takes-it-all situation** etc.
○**Dysfunction of governance** using societal norms

Causes of pain points

There are concerns about :
○**Whether the data being exchanged can be trusted**
○**Whether the party with whom the data is exchanged can be trusted**
○**Whether the other party's handling of the provided data can be trusted**

While leveraging the benefits gained from **the Internet and the Web**, it is necessary to **add certain governance and operational mechanisms as well as functions that enable these mechanisms on the top.**

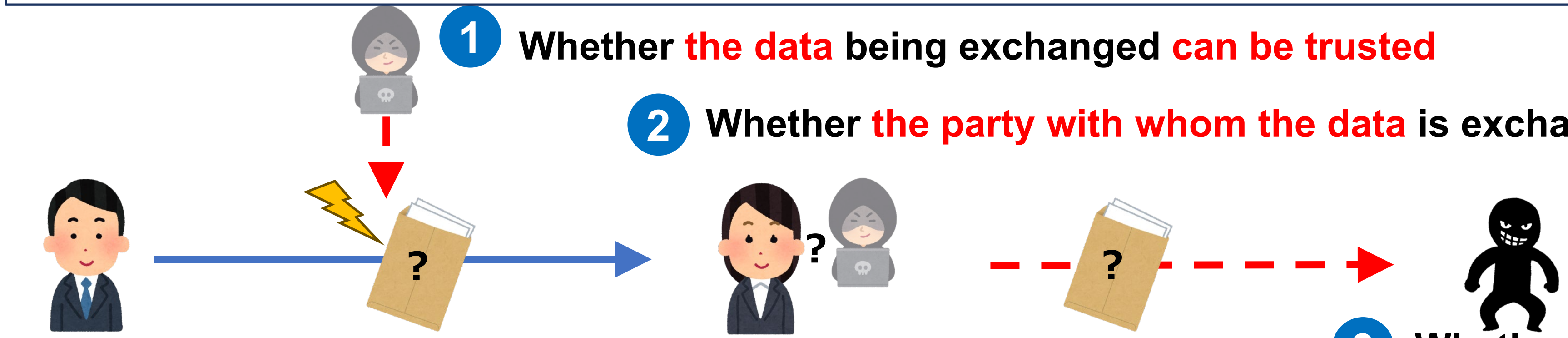
The key is "Trust"

Ref. Causes of pain points and potential needs

○ There are **concerns** with

1. **Whether the data being exchanged can be trusted**
2. **Whether the party with whom the data is exchanged can be trusted**
3. **Whether the other party's handling of the provided data can be trusted**

○ There is **no globally agreed standardized** means (either technical or governance-related).



① Whether the data being exchanged can be trusted

② Whether the party with whom the data is exchanged can be trusted

③ Whether the other party's handling of the provided data can be trusted

Needs of users

Users that present their data	Users as recipients
• Need to **control what to disclose to a recipient** e.g. Users have this need in particular when: - They can selectively disclose their data only when the recipient can reach out to the issuer of the presented data.	• Need to receive **unfalsified data** from **the intended issuer** of the data
• Need to **verify if the consent reflects the intentions of both the user and the recipient and how it is fulfilled afterwards** e.g. Users have this need in particular when:: - They have no idea if the consent and receipt of data are recorded.	• **If necessary,** are able to **verify** received data is not falsified and that the issuer is the intended one. e.g. Recipients have these needs in particular when: - They cannot make sure that received data are digitally proven to represent the intended attributes.

1-4. Goal of Trusted Web

○**Goal**: Build **a new trust framework for various social activities** in digital society and **enable various parties to create new values**

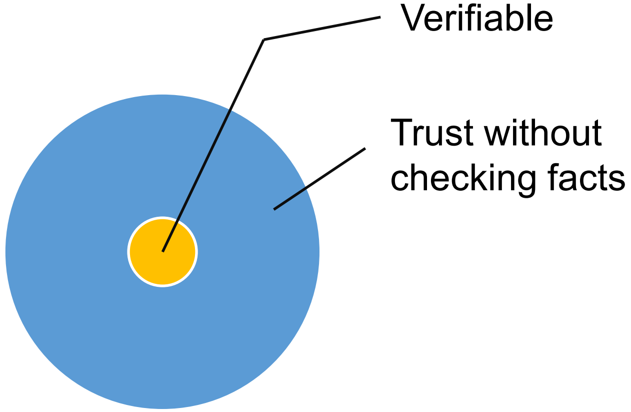
○**New Trust framework: Without excessively relying on specific services:**

- Enables **users (individuals and organizations) to control the data related to themselves**
- **Incorporates mechanisms for** consensus building in data exchanges while also enabling to **trace the implementation of that consensus**
- **Expands the portion where data transactions can be verified, thereby increasing the level of Trust**

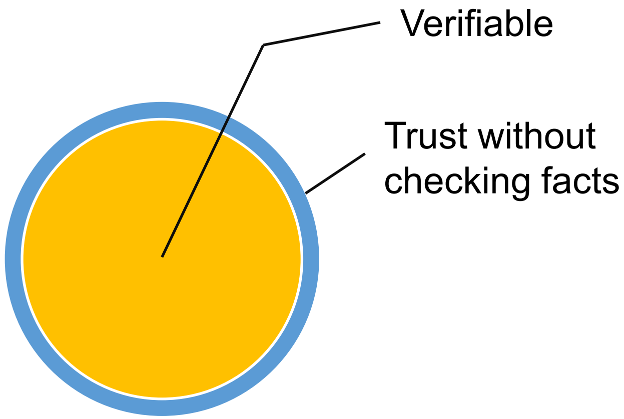
○**Approach: Overlay approach** where benefits of the Internet and the Web are leveraged and functions are added on the top

***Trust**: **The degree to which one believes that the other party behaves as expected without checking supporting facts to confirm the expectation**

The portion, where data transactions can be verified, changes depending on the mechanism applied

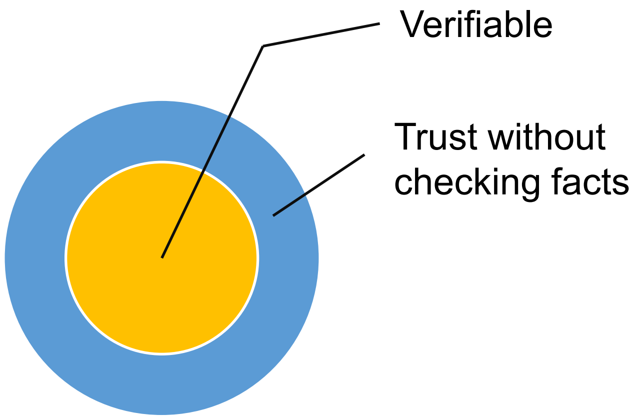


Current Internet:
As the verifiable portion is so small, decision making requires a great deal of trust in the other party.



Blockchain for all transactions, etc.

***Taking into account tradeoffs related to the issues such as scalability, energy consumption, and ease of upgrading without relying on a certain technology, the circle on the right is the goal of Trusted Web**



Goal of Trusted Web:
To expand the portion where data transactions can be verified, while satisfying continuity, interoperability and ease of upgrading
→ **Increase the level of "Trust"**

1-5 Benefits of the Trusted Web

○ **Through implementation in following with the Trusted Web concept, private sector can eliminate pain points to obstruct the realization of DX and DFFT. it will lead to the strengthening of competitiveness of companies and industries through the use of digital technology**.

○ Trusted Web will provide **end users** with benefit that **makes it easier and more secure**, and **the value created by the new services**.

Benefits to the company

- ✓ By improving trust in the handling of exchanged data and data at the other party, it is expected to lead to the **realization of "business-to-business collaboration," which is a prerequisite for advancing data distribution, DX, and DFFT.**
- ✓ By improving trust in the exchanged data and in the counterparties themselves, **the costs with data verification are reduced**.
- ✓ By improving the trust of data flow, it makes **more secure for users, and further promotion of service utilization**.
- ✓ Businesses can verify the values of their services that operate on a **newly built architecture**, and quick **scale-up** of their services on new digital infrastructure with interoperability.

Benefits to the end user

- ✓ **Enables users to control the data on free will.**
- ✓ With **users' data aggregated under their control points**, users can use and share their data **without involving platform operators**.
- ✓ **Sense of security from enhanced** verifiability of data being exchanged.
- ✓ **Users can benefit from a variety of services** created by service providers in the process of implementing the Trusted Web, **as well as from the value brought by these services.**

1-6. Use Case Verification and Prototype Implementation

Embodiment of benefits realized through prototype verification and planning in **3 theoretical studies conducted in FY2021 and 13 pilot projects demonstrations conducted in FY2022.**

Personal attribute(Academic and employment history, mutual aid service)

Certification of employment | Academic history | mutual aid services | Metaverse

○ While reskilling, etc. is required, a greater sense of security can be provided, and career development that better fits the applicant's needs in finding a job or changing jobs can be achieved, by controlling the attribute presented, agreeing on who the attribute will be used and for what purpose, and enabling the applicant to trace the employer who has accessed the attribute, etc.

○ To avoid mismatches during the hiring process, companies can increase the verifiability of their applications and reduce the cost of verification through third-party endorsements (e.g., certifications from learning institutions and past employers), as opposed to the cost of verifying that there are no falsehoods in resumes, job performance, work conditions, and other application details.

○ For mutual aid apps that match people to help each other in local community, there is a need to develop the indicators and items, etc. to be agreed upon in advance in order to enable verification of mutual aid achievements across apps. By building a trust framework to ensure governance across mutual aid apps, the scope of verification by users is expanded and trust can be formed across apps. Collaboration with other industry services can be made possible, such as promotion of digital service development by local governments.

Exchange of data between corporations and administrative agencies

application for subsidies | Industrial association certification

○ By utilizing digital credentials issued by different entities, such as manufacturers, industrial associations, and competent authorities, the verifiability of documents submitted to the government is improved. This will greatly reduce the man-hours required by the government to check credentials for tampering, validity, whether the credentials is from the intended issuer, etc., and speed up the process.

Exchange of data in the supply chain

Carbon emissions | Chemical substance content | IT system quality assurance | Machine product repair

○ A framework that ensures data reliability but limits the scope of disclosure of in consideration of trade secrets, etc., as data is processed and transmitted.

○ Establishment of a framework that user enables to confirm product reliability on IT systems (e.g., parts used in IT equipment, software vulnerability responses, etc.) provided by vendor, including uniform autonomous detection of software/hardware tampering and security operations coordination.

1-7. Use Case Verification and Prototype Implementation

Exchange of IoT attribute

Multifunction machine

- ○ While the maintenance of a telework environment is required, accounting departments and certain industries require authenticity of documents, there are still a lot of paper-based analog works. Prototype implementation enables to verify that the documents have not been tampered after the documents are scanned with specific multifunction devices, and were scanned with such multifunction devices.

Exchange of health care attribute

Clinical data

Health care data

- ○ Operational costs that important information and processes to handle highly sensitive information such as medical information are recorded on paper media are increased. The prototype implementation can ensure that files (including clinical trial data) have not been tampered with and only recipients who have confirmed that they are trusted parties verify not to be spoofing by sender. Transaction can be traced by checking the history (audit trails).
- ○ To enable medical and research to utilize of attributes from health checkups, health information at work, and a variety of other information at all times in daily.

Exchange of media attribute

Advertising

- ○ Originator Profile (OP) are discussing as a technology to improve the verifiability of the verification process for verifying the origin of media in news distribution. This is expected to be an effective countermeasure against "content falsification" and "spoofing”, which are the main methods of disinformation.
- ○ By impartial third-party certification organization issue OPs to "ad tech operators" and "website visitors" verify the OPs, the legitimacy of the ad tech operators can be confirmed and attributes of website visitors (consumers) can be prevented from being sent on to unauthorized ad tech operators.
- ○ By issuing non-bot credentials that subject that they are not bots behave as website visitors to make it look like the ads are effective, and by verifying that the "website operator" and "ad tech operator" are legitimate human accesses, it can be possible to confirm that it is not an advertising scam.

1-8. the Trusted Web and "Generative AI”

- The widespread awareness and rapid uptake of generative AI is expected to **accelerate innovation in a variety of fields** and **bring about dramatic changes in the world**.

- On the other hand, there are **also risks and issues that threaten the economy and society, such as deepfake and social disruption caused by disinformation**.

- At the April 2023 G7 Digital and Tech Ministers' Meeting, an agreement was reached regarding **"We plan to convene future G7 discussions on generative AI which could include topics such as governance, how to safeguard intellectual property rights including copyright, promote transparency, address disinformation, including foreign information manipulation, and how to responsibly utilise these technologies**” As a result of the G7 Hiroshima Summit in May, the Hiroshima AI Process was launched.

- Subsequently, international discussions have been underway, including the October 2023 presentation of the "Hiroshima Process International Guiding Principles for Organizations Developing Advanced AI System" and the "Hiroshima Process International Code of Conduct for Organizations Developing Advanced AI Systems.

- A report released by the OECD in September for discussion in the Hiroshima AI Process identified key areas of concern among G7 members, including **lack of transparency of generative AI both in the development stage and use, address disinformation, intellectual property rights, privacy and personal data governance, fairness, and security and robustness,** among others.

- In this context, the Trusted Web, which establishes a new trust framework enables verification of exchanged data and the other party, could **play an important role in securing trust for generative AI**.

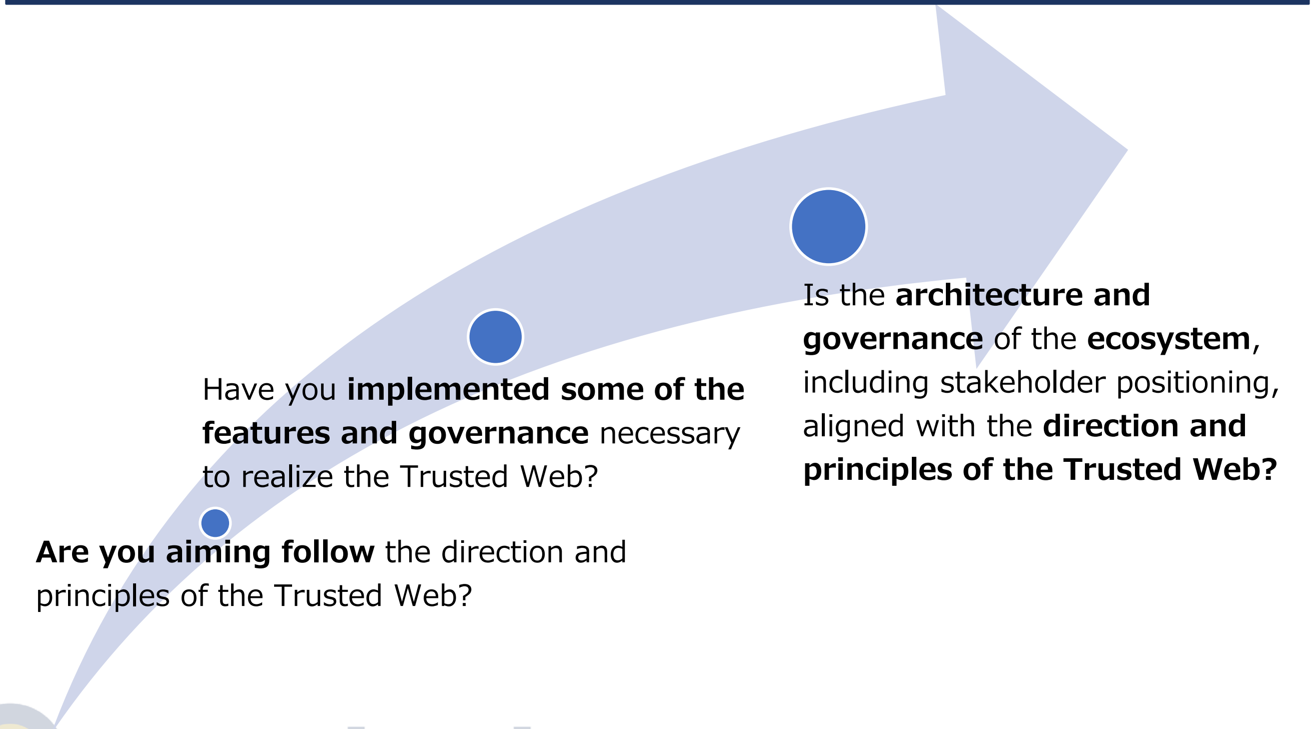
1-9. Measures for Concrete Participation of Companies

○ To achieve the Trusted Web concept, it is necessary for management, business divisions, engineers, and **other related parties of companies to understand and share the necessary action steps**, and to grasp the **status of the efforts as needed through self-assessment** while taking action. Therefore, **”Promotion Steps (tentative),"** which are referred as a **guide for reference** on what should be addressed, **will be studied further and released promptly after the release** of the white paper version 3.0.

○ The use of the “Promotion Steps (tentative)" is expected not only to promote the efforts of each company, but also to have the advantage of, for example, **disclosing the results of the self-assessment to external parties so that they can be referenced by each other in evaluating the company and its services and ensuring interoperability.**

○ In addition, we consider the **incentives for business** in order to promote widely with reference to similar cases.

Image of a referenceable guide(promotion steps)



Are you aiming follow the direction and principles of the Trusted Web?

Have you **implemented some of the features and governance** necessary to realize the Trusted Web?

Is the **architecture and governance** of the **ecosystem**, including stakeholder positioning, aligned with the **direction and principles of the Trusted Web?**

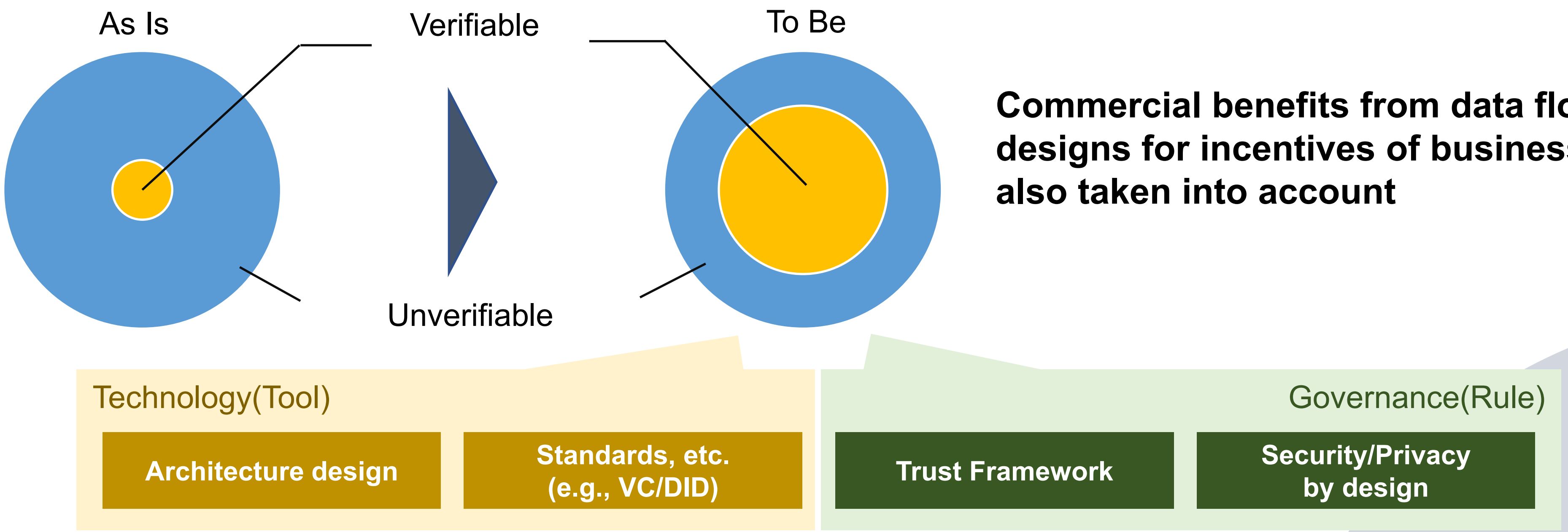
Image of items in self-assessment

- Identification status of areas to apply framework in accordance with the Trusted Web concept
- Identification status of pain points (e.g., non-tampering, anti-spoofing, selective disclosure, etc.)
- Direction of value creation based on the goal of Trusted Web (e.g., expansion of the portion where data transactions can be verified, consensus building framework, etc.)
- Status of following with principles (e.g., control by data subjects, interoperability, etc.)
- Other items related to architecture, governance, etc.

2 Axes Supporting the Trusted Web

○ In order to expand the portion where data transactions can be verified, it is necessary to take **not only technology approach, including architecture, but also governance approach**. These are **the two sides of a coin**.

○ **In order to maintain the neutrality of the technology**, a certain level of governance should be in effect. In addition, to maintain the concept of the Trusted Web over the medium to long term, a governance framework is necessary to prevent **excessive reliance on specific stakeholders.**


As Is
Verifiable
To Be
Unverifiable
Technology(Tool)
Architecture design
Standards, etc. (e.g., VC/DID)
Governance(Rule)
Trust Framework
Security/Privacy by design

Commercial benefits from data flows and designs for incentives of businesses are also taken into account

It aims to enhance verifiability and controllability in data exchange on the Internet and Web by facilitating the use of the functions that work on the existing Internet and Web.

1-11. Overlay approach and roadmap to realization

Through the overlay approach the initiative aims to implement Trusted Web.

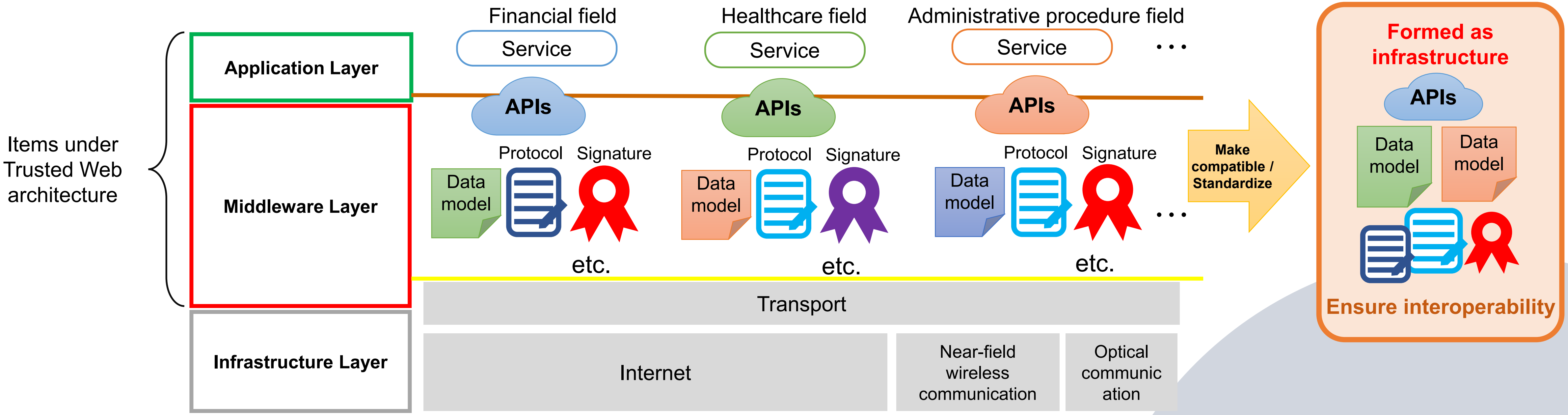
A potential scenario of the roadmap for the realization of Trusted Web

Various services that embody the functions Trusted Web aims at are provided, and their areas of use (fields) would expand

→ **A kind of middleware would be formed** and the layer of individual services

→ In the middleware, **APIs, data models, and protocols that should be compatible would be identified**, such compatibility ensures **interoperability**, leading to **standardization**

→ Trusted Web would be realized though obtaining feedbacks across various services.


Items under Trusted Web architecture
Application Layer
Middleware Layer
Infrastructure Layer
Financial field
Healthcare field
Administrative procedure field
Service
Service
Service
・・・
APIs
APIs
APIs
Protocol
Signature
Data model
etc.
Protocol
Signature
Data model
etc.
Protocol
Signature
Data model
etc.
・・・
Make compatible / Standardize
Formed as infrastructure
APIs
Data model
Data model
Ensure interoperability
Transport
Internet
Near-field wireless communication
Optical communication

Through the use case studies and implementation, we will present the benefits of Trusted Web to stakeholders in various fields and **obtain feedback on challenges and improvements to the architecture and governance, etc.**

2. Implementation / Guideline

2-1. Trust framework that Trusted Web aims to achieve

Based on the use case studies and the prototype implementation, we have organized **the picture of Trust framework that Trusted Web aims to achieve**. With this picture in mind, we propose the basic design of **verifiable data model and verifiable communication model with high interoperability** as the "**architecture**" of Trusted Web.

a. Identity management

- Entities manage their own identities by using an externally linked identity management system*

b. Trust and data verification

- The fundamental value of Trusted Web is “to increase the level of trust through the expansion of portion where data transactions can be verified”

c. Data covered by Trusted Web

- Created data and the process of data exchange are in scope
  - Created data: Verifiability is ensured by digital signature technology
  - Process of data exchange: Verifiability is ensured by modeling data exchanges and combining it with digital signature

d. Expansion of the portion where data transactions can be verified

- The entire data set, including the signature, can be verified by i) verifying “the signature itself”, ii) verifying “the signer”, and iii) clarifying “the intent of the signature”
  - Clarifying “the intent of the signature” refers to the state in which the function satisfied by the signature to achieve the purpose has been specified with data exchange framework agreed beforehand

Examples of the framework in which “the intent of the signature” is clarified:

Signatures are signed in accordance with the intent designed in the protocol (e.g., X.509 certificate, DNSSEC, etc.)

Signatures on data for digitized certification (e.g., Verifiable Credentials)

e. Modeling of data exchanges

- Data exchange is modelled in the form of messages and transactions
- The data exchange processes (orders, content, actually received or not, etc.) are mutually recorded
  → Ensures data transfer and enables to verify afterwards that the data exchange actually took place

f. Need to combine protocols

- An architecture with a high degree of flexibility to combine standards and protocols is essential

---

* Implementations can adopt OpenID and other standard-based systems, and technologies such as DID/VC.

2-2. ver.2.0 architecture reorganized

To expand the verifiable domain and improve trust in data exchange, the six components of the ver. 2.0 architecture are reorganized into **Verifiable Identity**, **Verifiable Data**, **Verifiable Messaging**, and **Verifiable Identity communities**

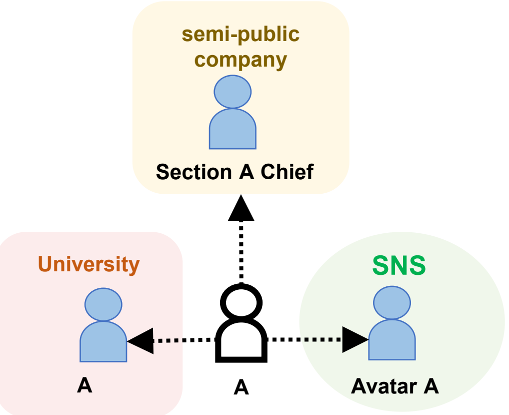
Component	Concept	Description
Verifiable Data	*Verifiable Data*	Data that can be verified by a verifier that the **subject data has been verified by the signer** through the use of **digital signature** technology.
Identity	*Verifiable Identity*	A digital identity consisting of **a minimum set of verifiable and context-specific attributes.** Verifiable Identity allows verifiers to confirm that the data in question has been verified by the signer (enabling Verifiable Data) and that the data exchange can be verified (enabling Verifiable Messaging).
Identity Graph	*Verifiable Identity Community*	A set of identities that support the establishment of Verifiable Identity by **sharing information, including the starting point of trust, under a certain governance.**
Node		As a given, not specified in the architecture
Message	*Verifiable Messaging* *Verifiable Message*	✓ **Reliable** delivery between multiple entities. } Confirmation can be made.
Transaction	*Verifiable Transaction*	✓ Including the ordering of messages sent and received } Confirmation can be made.
Transport		Not specified in the architecture in order to greedily utilize the available means of communication.

2-3. Overview of the architecture around Verifiable Identity and the relationship between the components of the Trusted Web

- ○ Present **a highly abstract architecture** around Verifiable Identity that **broadens the verifiable area**.
- ○ Verifiable Identity enables the implementation of Verifiable Data and Verifiable Messaging. Verifiable Identity communities anchor Verifiable Identity; Verifiable Identity aims to **broaden the verifiable domain and improve Trust in data exchange**.

Verifiable Identity Community (Verifiable Identity Community)

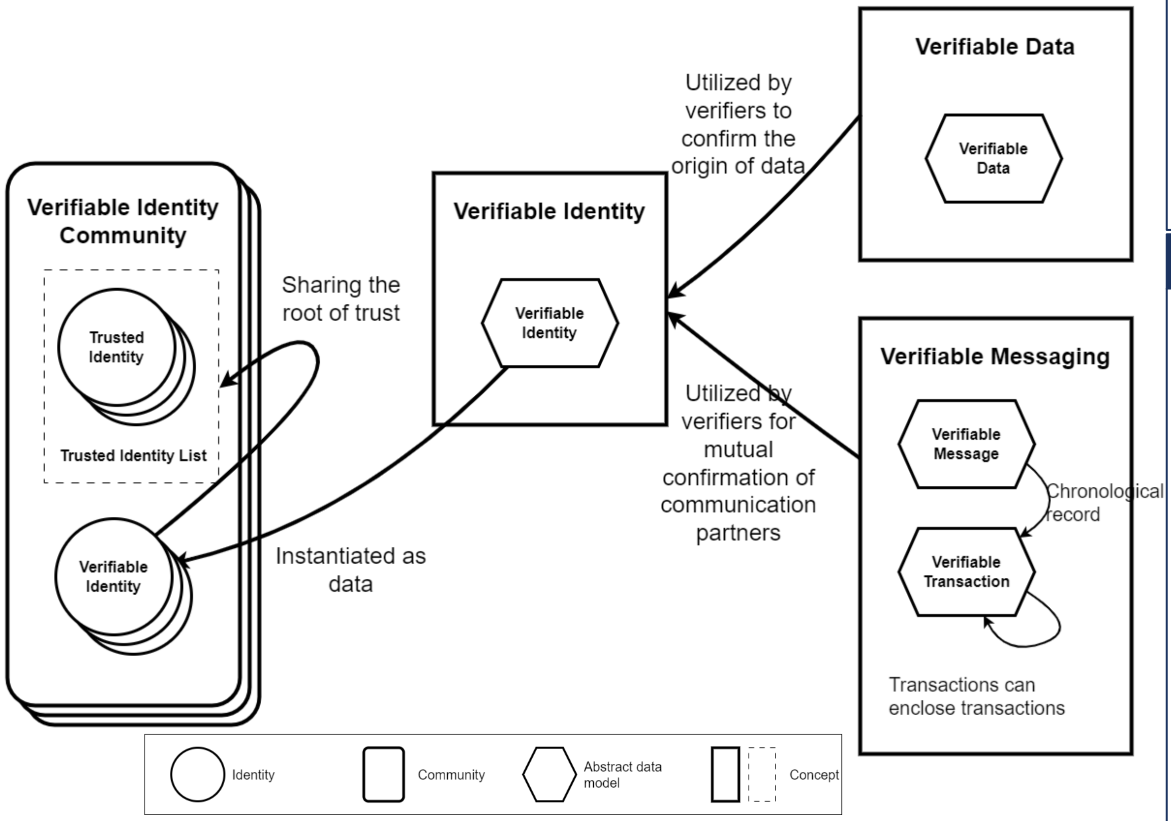
- If desired, build a chain of trust starting from an identity (Trusted Identity) operated by a trusted entity (Trusted Entity) with a high degree of certainty.
- Sharing Trusted Identity among ecosystem participants involved in data exchange simplifies building trust relationships.
- Verifiable Identity Community supports establishing Verifiable Identity by sharing information, including the starting point of trust, under governance.


semi-public company
Section A Chief
University
A
A
SNS
Avatar A

Identity is used for each community

Instances of Verifiable Identity

Overview of the architecture as revealed by the usecases to date


Verifiable Identity Community
Trusted Identity
Trusted Identity List
Verifiable Identity
Sharing the root of trust
Instantiated as data
Verifiable Identity
Verifiable Identity
Utilized by verifiers to confirm the origin of data
Utilized by verifiers for mutual confirmation of communication partners
Verifiable Data
Verifiable Data
Verifiable Messaging
Verifiable Message
Chronological record
Verifiable Transaction
Transactions can enclose transactions
Identity
Community
Abstract data model
Concept

Verifiable Identity

Digital identity consists of a minimum set of verifiable and context-sensitive attributes
To be verifiable, it consists of cryptographic key materials and an identifier.
*A single entity (natural person, legal entity, etc.) may use a single identity or multiple identities depending on the context (SNS, legal entity).
Example: Platform using WebPKI, OpenID Connect

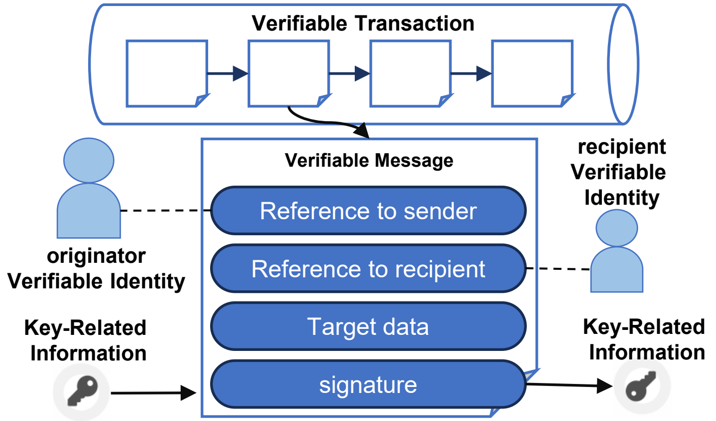
Verifiable Data

Verifiable Data consists of references to the target data, signature, and originating identity.

Signed and generated using a signature key (e.g., private key for public key cryptography) and verified using key-related information for verification (e.g., public key for public key cryptography) retrieved by referencing and verifying the Verifiable Identity.
Examples: X.509PKI certificates, vaccine certificates, signed PDFs

Verifiable Messaging

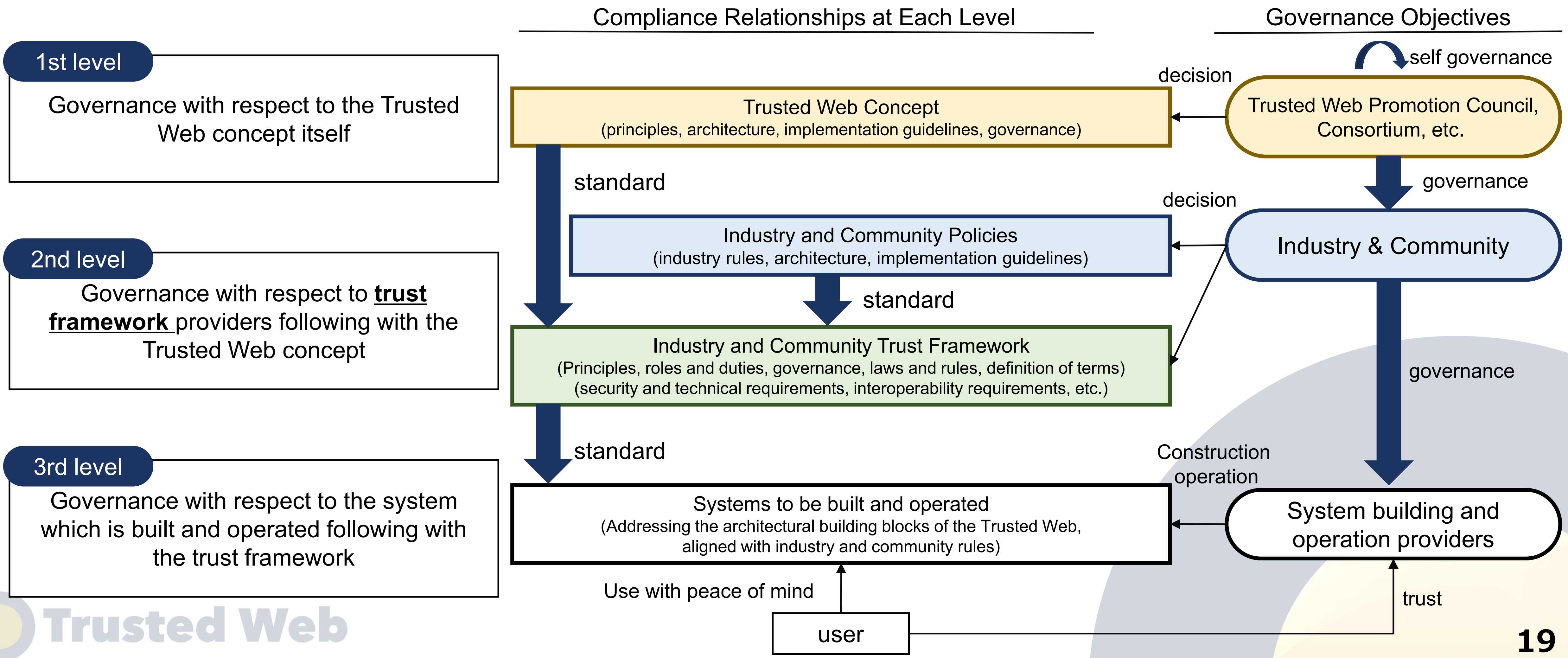
Record reliable delivery between multiple entities, including the sequence of messages sent and received.
Verifiable Message: Information to refer to the sender and receiver, the message itself, signature by the sender
Verifiable Transaction records multiple Transaction Records to enable verification of the order of their origination; Transaction Records contain either Verifiable Message or Verifiable Transaction (Transaction Records may recorded into Blockchain)


Verifiable Transaction
Verifiable Message
Reference to sender
Reference to recipient
Target data
signature
originator Verifiable Identity
recipient Verifiable Identity
Key-Related Information
Key-Related Information

2-4. governance (general view)

○ “Governance” is needed for the **principles of the Trusted Web itself** and that the **systems (industries) following with the principles are operated and utilized without losing their principles, according with technology develops and social systems change**.

○ Ver. 3.0 shows the hierarchy of governance, how to organize the governance, and the outline of the trust framework as **a basis for future study.**



Compliance Relationships at Each Level

Governance Objectives

1st level

Governance with respect to the Trusted Web concept itself

2nd level

Governance with respect to **trust framework** providers following with the Trusted Web concept

3rd level

Governance with respect to the system which is built and operated following with the trust framework

self governance
decision
Trusted Web Concept
(principles, architecture, implementation guidelines, governance)
Trusted Web Promotion Council, Consortium, etc.
standard
governance
decision
Industry and Community Policies
(industry rules, architecture, implementation guidelines)
Industry & Community
standard
Industry and Community Trust Framework
(Principles, roles and duties, governance, laws and rules, definition of terms)
(security and technical requirements, interoperability requirements, etc.)
governance
standard
Construction operation
Systems to be built and operated
(Addressing the architectural building blocks of the Trusted Web, aligned with industry and community rules)
System building and operation providers
Use with peace of mind
trust
user

2-5. governance (future consideration)

- ○ The governance of trust framework will be fleshed out in the future, with reference to the guidelines[*1] released by OIX[*2] in 2022.
- ○ In particular, it is **necessary to consider the** governance of trust framework **the DIACC in Canada, which is a non-profit coalition under public-private leadership, as a neutral and sustainable organizational form, keeping in mind concretely**.

* 1 Open Identity Exchange
* 2 A Guide to Trust Framework for Smart Digital ID

Examples of how the governance operating structure should be

- **Independent Governing Entity**
  Example: A non-profit coalition of public and private sector leaders such as the Digital Identity and Authentication Council of Canada (DIACC)

- **Consortium of Participating Entities**
  Example: the CA/Browser Forum, which consists of a group of browser vendors and certification authorities that jointly agrees upon the trust framework

- **Single Participant Governing Entity**
  Example: A single existing organization, such as those operated by the US government login.gov program

- **Non-Governing Standards or Certification Organization**
  e.g., an independent entity, non-governmental standards/certification bodies such as the Kantara Initiative

- **Mutual Agreement Among All Participants**

OIX - A Guide to Trust Frameworks for Smart Digital ID (openidentityexchange.org)

2-6. governance (future considerations)

The governance of trust framework will be fleshed out in the future, with reference to the guidelines*1 released by OIX*2 in 2022.

*1 Open Identity Exchange
*2 A Guide to Trust Framework for Smart Digital ID

Trust Framework Outline

Component	What is required of the Trusted Web (example)
Glossary	-
Principles	To follow with Trusted Web principles
Trust Mark	To consider the requirements for monitoring compliance with the Principles, when you are making a statement to users or others that your trust framework is Trusted Web compliant.
Roles and Obligations	To define compliance with Trusted Web principles as an obligation
Governance	To follow Trusted Web governance concepts (e.g., multi-stakeholder)
Trust Rules	To trust entities structured in accordance with Trusted Web principles
User Services	To ~~B~~be structured in accordance with Trusted Web principles (verifiability, transparency, etc.)
Relying Party Services	
General and Legal Rules	-
Security and Technical Requirements	To adopt technologies that can ensure verifiability. To adopt technologies that are widely accepted as standards, rather than technologies that have been established only by specific operators.
interoperability requirements	To adoption of widely accepted technologies as standards, allowing for easy expansion of the ecosystem as needed

2-7. Principles in design and operation

1 Sustainable ecosystem

There is an incentive for stakeholders to share their responsibilities and fulfill them.

2 Governance by multiple stakeholders

Multiple stakeholders are involved in governance, stakeholder responsibilities are clearly defined, and the root cause can be investigated whenever a problem occurs.

3 Openness and transparency

Architecture design, implementation and its process are open, highly transparent and mutually verifiable.

4 Control by data entity

Control of access to data belongs to the data entity (individual / company).

5 Universality

Do not eliminate anyone and do not leave vulnerable people behind. Anyone can participate freely.

6 User viewpoint

It is lock-in free and users have choices. It is easy to understand and safe to use for users.

7 Continuity

With the existing Internet architecture as the basis, it is built on the top of it and it will be added to the current Web in a transitional manner. Also consider the federation with the existing trust.

8 Flexibility

The components are loosely coupled and the system has a scalable architecture.

9 Interoperability

It should be possible to link different systems not only for technology but also for the entire social system such as legal system, governance, and organization.

10 Ease of upgrade, scalability

It should not depend too much on a specific technology. It should be scalable and it should be easy to continuously enhance its functions considering medium-to-long term use.

Trusted Web

Supporting mechanism

Users' standpoint

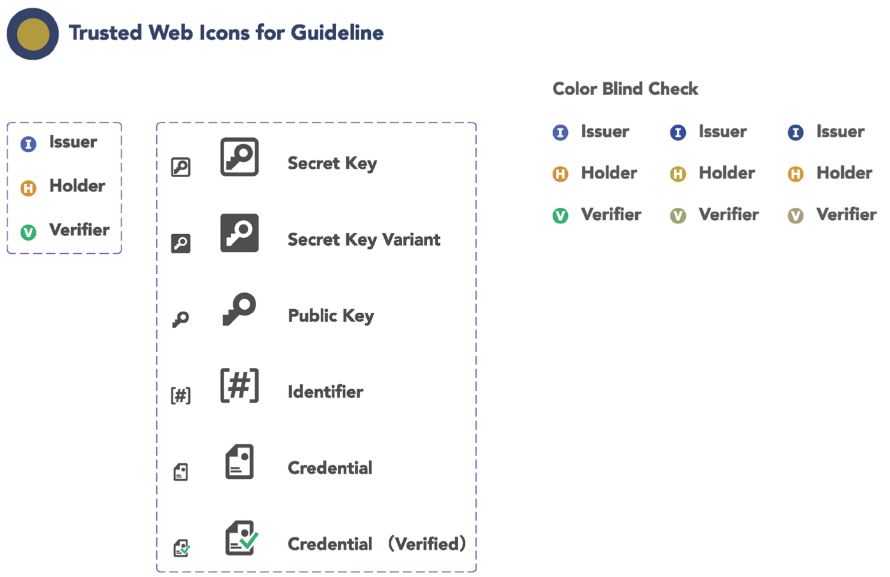
System's standpoint

2-8. Implementation Guidelines

- ○ **Implementation Guidelines is positioned as a practice that can be used as a reference for private sector to implement** based on the Trusted Web design philosophy. Specifically, the following are presented.
  - ➢ **Variation of implementation methods for** functional requirements extracted for use cases
  - ➢ **Notes, samples, and component diagram**, etc on implementation in use cases.
- ○ We will publish on **GitHub** and invite people to participate in the discussion on the Trusted Web website. It is expected that engineers and other stakeholders involved will be able to adopt rapidly advancing technological trends and **grasp concrete examples of implementation** and **use them in service development through mutual discussion and updating.**

https://github.com/TrustedWebPromotionCouncil/trusted-web-implementation-guideline

License-free icon set (using the color palette of the Digital Agency Design System)



Trusted Web Icons for Guideline

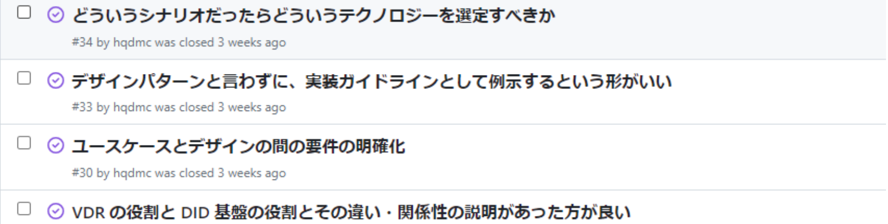
Issuer
Holder
Verifier

Secret Key
Secret Key Variant
Public Key
Identifier
Credential
Credential （Verified）

Color Blind Check

Issuer	Issuer	Issuer
Holder	Holder	Holder
Verifier	Verifier	Verifier

Updates by issue/pull requests

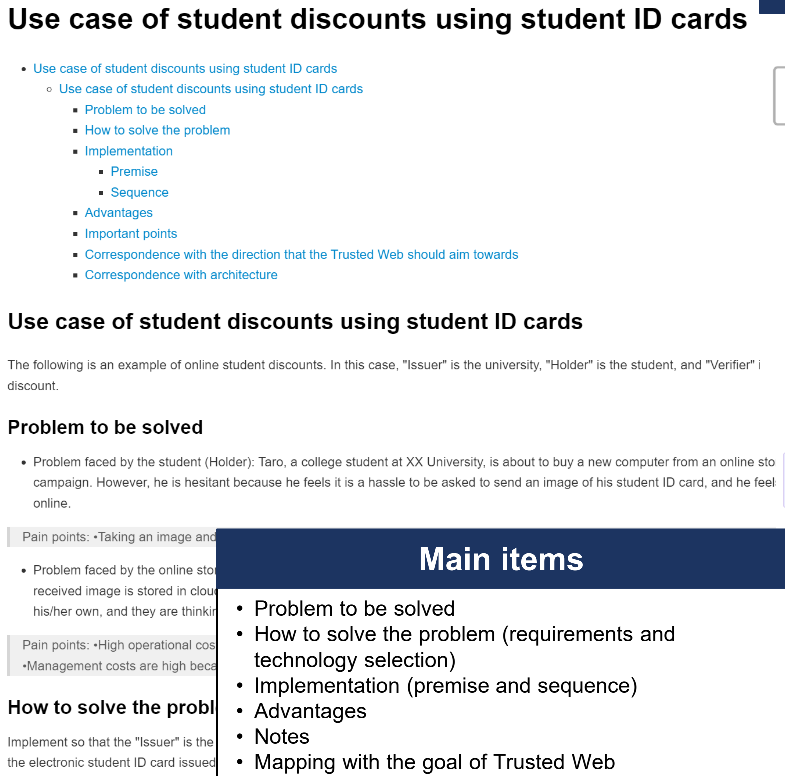


☐ どういうシナリオだったらどういうテクノロジーを選定すべきか
#34 by hqdmc was closed 3 weeks ago

☐ デザインパターンと言わずに、実装ガイドラインとして例示するという形がいい
#33 by hqdmc was closed 3 weeks ago

☐ ユースケースとデザインの間の要件の明確化
#30 by hqdmc was closed 3 weeks ago

☐ VDR の役割と DID 基盤の役割とその違い・関係性の説明があった方が良い



Use case of student discounts using student ID cards

- Use case of student discounts using student ID cards
  - Use case of student discounts using student ID cards
    - Problem to be solved
    - How to solve the problem
    - Implementation
      - Premise
      - Sequence
    - Advantages
    - Important points
    - Correspondence with the direction that the Trusted Web should aim towards
    - Correspondence with architecture

Use case of student discounts using student ID cards

The following is an example of online student discounts. In this case, "Issuer" is the university, "Holder" is the student, and "Verifier" i
discount.

Problem to be solved

- Problem faced by the student (Holder): Taro, a college student at XX University, is about to buy a new computer from an online sto
campaign. However, he is hesitant because he feels it is a hassle to be asked to send an image of his student ID card, and he feel
online.

> Pain points: •Taking an image and

- Problem faced by the online sto
received image is stored in clou
his/her own, and they are thinki

> Pain points: •High operational cos
> •Management costs are high beca

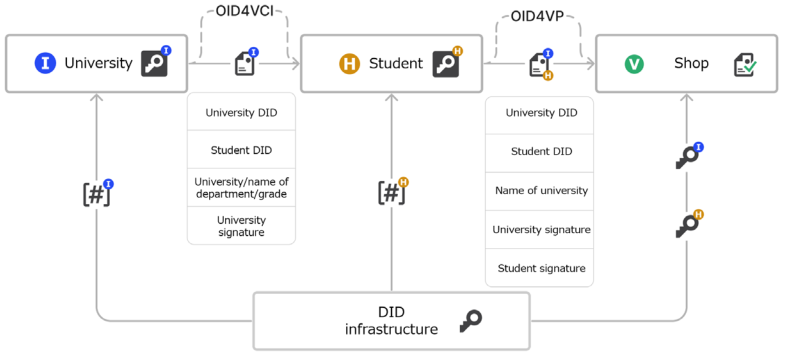
How to solve the probl

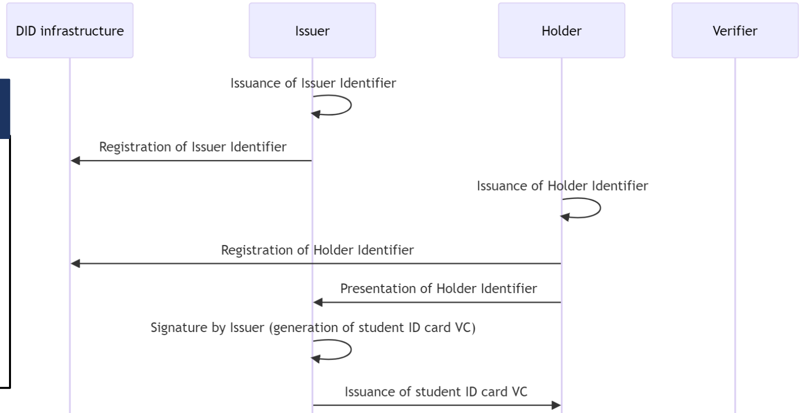
Implement so that the "Issuer" is the
the electronic student ID card issued

Main items

- Problem to be solved
- How to solve the problem (requirements and technology selection)
- Implementation (premise and sequence)
- Advantages
- Notes
- Mapping with the goal of Trusted Web Correspondence with the goal of the Trusted Web
- Correspondence with architecture

System configuration diagrams and sequences diagrams


OID4VCI
OID4VP
University
Student
Shop
University DID
Student DID
University/name of department/grade
University signature
University DID
Student DID
Name of university
University signature
Student signature
[#]
[#]
DID infrastructure


DID infrastructure
Issuer
Holder
Verifier
Issuance of Issuer Identifier
Registration of Issuer Identifier
Issuance of Holder Identifier
Registration of Holder Identifier
Presentation of Holder Identifier
Signature by Issuer (generation of student ID card VC)
Issuance of student ID card VC

We will expand the implementation variations and provide updates so that engineers know what technologies should be selected for what scenarios.

3 . International Cooperation

2-9. Related Events and Ministerial Declarations at the G7 Digital and Tech Ministers' Meeting in Takasaki, Gunma

At the G7 Digital and Tech Ministers' Meeting in Takasaki, Gunma on April 29-30, the G7 agreed to share best practices on digital identity and digital credentials. As a related event of this meeting, policy initiatives and use cases for the Trusted Web were discussed at the "Stakeholders' Conference on Digital Technologies for Trust".

Emerging and Disruptive Technologies in Innovating Society and Economy

Ministerial Declaration

We share the importance of developing policy discussions on digital identity systems and other means to build trust and security in data sharing. **We will share and accelerate best practices on digital identity and credentials and support discussions on the ongoing development of the OECD draft recommendation on the governance of digital identity**.
We take note of the discussions at the G7 Stakeholder Conference on Digital Technologies for Trust on 29 March 2023 on compatible policy approaches and technologies for data exchange in a trusted way, including enhanced traceability and controllability of data as well as verification of data sharing partners.

Annex on G7 Vision for Operationalising DFFT and its Priorities

Ministerial Declaration

The COVID-19 crisis and current global situation has demonstrated the value and need for like-minded partners to find consensus on approaches to data sharing in priority sectors such as healthcare, green/climate, and mobility (e.g., geospatial information platform for autonomous mobilities) to foster innovation and economic growth. **We uphold the role of technology and use cases thereof such as digital credentials and identities in facilitating data sharing as a part of our efforts to operationalise DFFT**. Improved data use is also a major strategic opportunity for economic growth.

Stakeholders' Conference on Digital Technologies for Trust

The event was attended by the government officials from G7 countries, invited countries, invited institutions, companies and academic groups involved in trust services, and featured presentations and discussions on the efforts to ensure trust for the operationalization of the Data Free Flow with Trust (DFFT). Mr. KUROSAKA presented the basic concept and initiatives of the "Trusted Web," and ORPHE and DNP introduced use cases. A discussion among panelists by the government officials from G7 countries were held.

The G7 Digital and Tech Ministers' Meeting
Stakeholders' Conference on Digital Technologies for Trust
29 March 2023, Tokyo, Japan

olders' Conference on Digital Technologies for Trust
29 March 2023, Tokyo, Japan
DNP

ORPHE CORE 2.0
Stakeho

Stakeholders' Conference on

2-10. overseas cases

EU: EU Digital Identity Wallet

- Regulation in 2021 to issue a Digital Identity Wallet that store and provide attributes linked to her/his identity in electronic ledger enabling decentralized governance models was proposed.
- Ideas similar to the Trusted Web, including the use of endorsed attributes for authentication (with the goal of wide deployment by 2030)
- Architecture and Reference Framework (ARF) published (2023/2), which defines technical specifications

Canada: PCTF (The Pan-Canadian Trust Framework)

- A framework that sets out high-level requirements for the secure use of digital identities was released from DIACC*1 (a Canadian non-profit coalition of public-private).
- Promoting use case using VC (Verifiable Credentials) for academic digital credentials that is intended to be cross-border.
- In British Columbia, there is a service to use attributes verified by the bank for other services with the consent of the individual.

1 Digital ID & Authentication Council of Canada

Trusted Web

UK: The UK digital identity and attributes trust framework

- A framework aims to make it easier and more secure for people to use services that enable them to prove who they are or information about themselves.
- Demonstrating to collect credentials for medical staff's identity skills and experience with using VC (verifiable credentials) and DID (decentralized identifiers). This reduces the time the staff are waiting for administration check.

→ We share **information and collaborate** use-case-based **interoperability** with these countries and others.

4． Future Activities

2-11. future activities

Creation of use cases

- Use case demonstration of concrete implementation to create practical examples (12 demonstration projects for FY2023)
- Identify further challenges through feedback and reviews as the use case development progresses
- Discussion on how the Trusted Web can contribute to generative AI that leverages data on the Internet

Further promotion of efforts by companies and engineers

- Realization of "Promotion Steps (tentative)" for further promotion of corporation
- Utilizing implementation guidelines on GitHub, constantly update technical revisions (assuming active involvement of engineers and other)
- Encourage entities to come up with ideas actively through workshops based on the use cases developed

Accelerate social implementation

- Realization of the governance itself, how to organize the governance, and the trust framework, etc.
- The opportunities for the public and private sectors to collaborate on information and deepen discussions on an business to business to realize the Trusted Web.

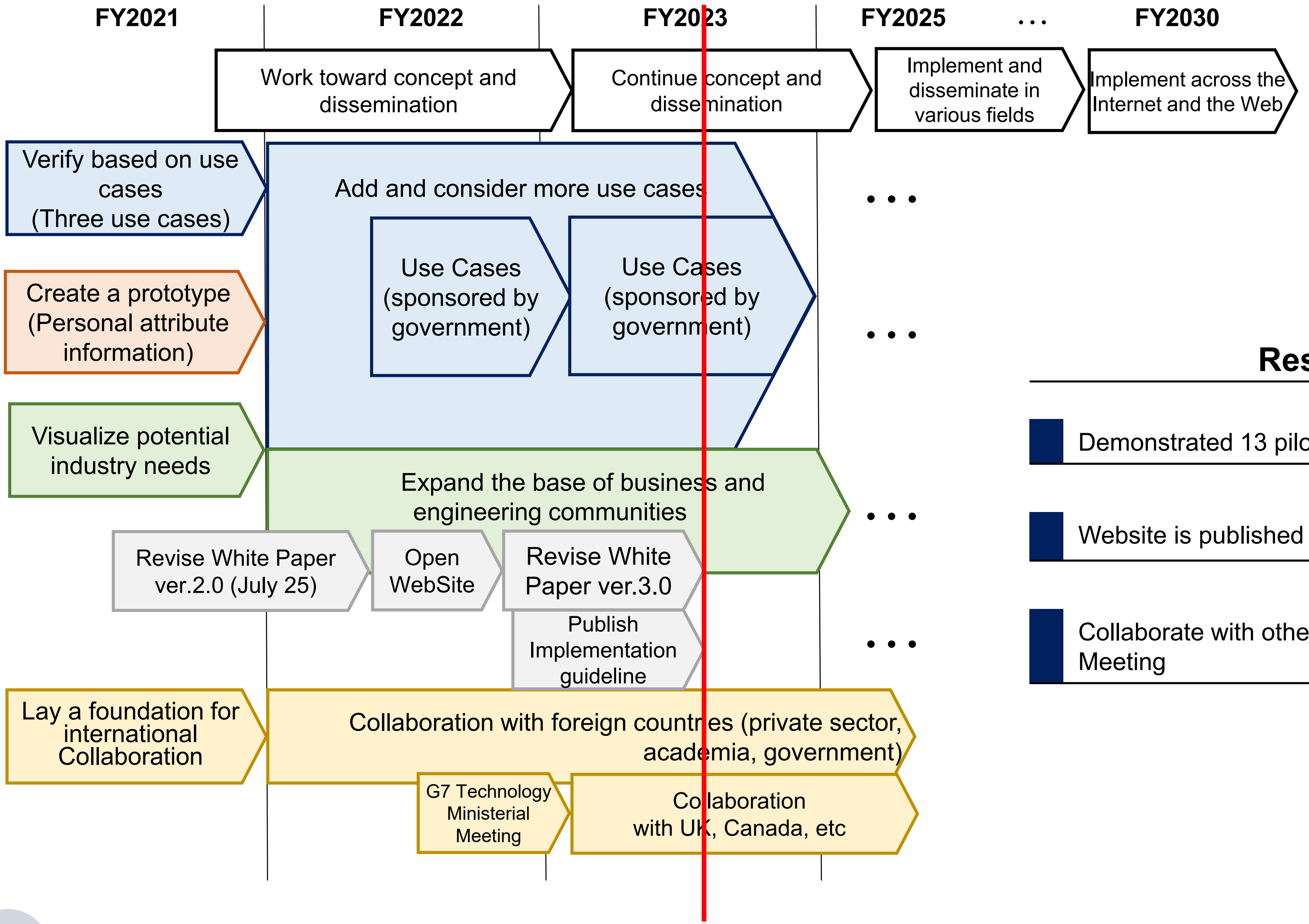
International Cooperation

- Promote discussions on sharing best practices and ensuring interoperability with other countries and related organizations on the occasion of the G7

Overall

- Promote collaboration between the Trusted Web and initiatives that have already been designed and led by the government (e.g., Ouranos Ecosystem).
- Deployment of the Trusted Web, including transition in user behavior.
  (Establishment of a "ceremony" in which everyone goes through the same actions and processes to achieve the same results, the experiences become predictable and unambiguous and archive very high levelsf of reliability in the communication between the system and its human users)
- Discussion of the transition process from the existing systems, its notes, and the future roadmap.

2-12. Mid-term Strategy Toward 2030 (conceptual diagram)



FY2021

FY2022

FY2023

FY2025 …

FY2030

Work toward concept and dissemination

Continue concept and dissemination

Implement and disseminate in various fields

Implement across the Internet and the Web

Verify based on use cases (Three use cases)

Add and consider more use cases

Use Cases (sponsored by government)

Use Cases (sponsored by government)

…

Create a prototype (Personal attribute information)

…

Visualize potential industry needs

Expand the base of business and engineering communities

…

Revise White Paper ver.2.0 (July 25)

Open WebSite

Revise White Paper ver.3.0

Publish Implementation guideline

…

Lay a foundation for international Collaboration

Collaboration with foreign countries (private sector, academia, government)

G7 Technology Ministerial Meeting

Collaboration with UK, Canada, etc

Result of FY2022 activities

- Demonstrated 13 pilot projects,
- Website is published to dissemination-Trusted Web
- Collaborate with other countries, agreement G7 Technology Ministerial Meeting

List of selected pilot projects (FY2022)

	Name of pilot projects	Business Name/ Representative Organization Name	Category
1	Personal data distribution in online marketing	DataSign Inc.	Personal
2	Trust verification of service eligibility and provided data in virtual reality space	NRI Digital, Ltd.	Personal（Metaverse）
3	Promotion of Human-Resource Mobility through Personal Management of Academic Records	The University of Tokyo	Personal（Personal Skills）
4	Trusted data exchange system of learning information for human resource development	Fujitsu Japan Limited	Personal（Personal Skills）
5	Information distribution system with high reliability and applicability in clinical trials and medical sites	CMIC Co. Ltd.	Healthcare
6	Trusted gait data distribution system between patients with lower limb musculoskeletal disorders, physicians, and researchers	ORPHE Inc.	Healthcare
7	Carbon emissions tracing system with decentralized ID (DID/VC)	Datagateway Pte. Ltd.	Supply chain（CO2）
8	Traceability Management for Machine Product Supply Chain	YANMAR HOLDINGS CO., LTD	Supply chain（Manufacturing）
9	Innovating trust paradigm of critical social IT infrastructure by Trusted Network Ecosystem	Alaxala Networks Corporation	Supply chain（economic security）
10	Trusted digital document data Platform for Workplace	Toshiba Tec Corporation	Documents（IoT）
11	Development and demonstration a Trusted Web related prototype system for the proof of identity and existence in the case of an online subsidy application for Solo proprietorship and Small and Medium-Sized Company	DENTSU.INC	Government
12	Industrial Association Certificate in the Corporate tax system	Japan Information Technology Services Industry Association	Government
13	Sharing user trust across platforms in mutual aid services	Dai Nippon Printing Co., Ltd.	Personal

List of selected pilot projects (FY2023)

	Name of pilot projects	Business Name/ Representative Organization Name	Category
1	Wallet-based identity management and online communication	DataSign Inc.	Personal
2	Trust ecosystem across mutual aid mutual aid services	Dai Nippon Printing Co.,Ltd.	Personal
3	Building a Network of Trust to Expand International Education and Increase Labor Market Mobility ～Creating a world where people can learn and expand their own potential without financial issues～	Institution for a Global Society Corporation	Personal（Personal Skills）
4	Skill Visualization for the Active Participation of University Technical Staffs: Challenge to Assurance of Skill Quality and Self-determination on Information Disclosure.	Fujitsu Japan Limited	Personal（Personal Skills）
5	Cross-Border Personal Information Management Platform in the Return Flow of Overseas Human Resources	PitPa, Inc.	Personal（Personal Skills）
6	The Chemical Management Platform (CMP) for reliable communication of information on chemicals in products in the manufacturing supply chain	Mizuho Research & Technologies, Ltd.	Supply chain
7	Business Unit Identity and its Digital Certification Platform	SBI Holdings, Inc.	Supply chain
8	Information distribution system with high reliability and applicability in clinical trials and medical sites	CMIC Co., Ltd.	Healthcare
9	Trustworthy gait data authentication and distribution system connecting doctors, researchers and patients with lower limb musculoskeletal diseases	ORPHE Inc.	Healthcare
10	a new model to accelerate “trusted transactions based on KYC/KYB”	Information Services International-Dentsu, Ltd.	Corporation, Financial
11	Preliminary Study on Establishing a Government Administrative Procedures DX Society Infrastructure for Corporations with a Focus on Subsidy Programs.	Japan Information Technology Services Industry Association	Government
12	Trusted Web Advertising System with OP	Originator Profile Collaborative Innovation Partnership (OPCIP)	Media

Trusted Web Promotion Council – List of Members

（As of May, 2024）

Shinichi Urakawa	Chair, Planning Sub-Committee, Committee on Digital Econom, Keidanren（Japan Business Federation）Advisor, Sompo Japan Insurance Inc.
Yuichi Ota	Founder and CEO of DataSign Inc.
Tatsuya Kurosaka	President and CEO, Kuwadate Incorporated
Nat Sakimura	Executive Fellow, Tokyo Digital Ideas, Co., Ltd.
Seiko Shirasaka	Dean/Professor, Graduate School of System Design and Management, Keio University
Haruo Takeda	Science Advisor, Hitachi, Ltd.
Hiroshi Tsuda	Fellow, SVP, Fujitsu Research, Fujitsu Limited
Yusuke Tomimoto	Senior Vice President, Toyota Financial Services Corporation
Koiti HASIDA	Professor, Graduate School of Information Science and Technology, The University of Tokyo
Takanori Fujita	Senior Fellow, The Tokyo Foundation for Policy Research
Masakazu Masujima	Partner, Mori Hamada & Matsumoto
Shin'ichiro Matsuo	Research Professor, Georgetown University, Virginia Tech
Kazuyoshi Mishima	Co-Founder & COO, Keychain
○Jun Murai	Distinguished Professor,Keio University
Kristina Yasuda	Federal Agency of Disruptive Innovation

（○: Chairperson）

Observers: Digital Agency, Ministry of Internal Affairs and Communication, Ministry of Economy, Trade, and Industry, National Institute of Information and Communications Technology (NICT), Information-technology Promotion Agency (IPA)

Trusted Web Promotion Council Task Force – List of Members

（As of May, 2024）

Tomoya Asai	Chief Technology Officer, WebDINO Japan
Hirochika Asai	Preferred Networks, Inc. VP of Infrastructure Strategy, Senior Researcher
Ryosuke Abe	Project Research Associate, Graduate School of Media and Governance, Keio University
Daichi Iwata	DGDF Business Unit / Senior Executive Professional
○Tatsuya Kurosaka	President and CEO, Kuwadate Incorporated
Kazue Sako	Professor, Department of Computer Science and Engineering, Waseda University
Shigeya Suzuki	Project Professor, Graduate School of Media and Governance, Keio University
Naohiro Fujie	Chairman, OpenID Foundation Japan
Shin'ichiro Matsuo	Research Professor, Georgetown University, Virginia Tech

（○: Chairperson）