Tentative translation

1. Background of the whitepaper

- The digital transformation (DX) of society as a whole is accelerating with the outbreak of COVID-19. As the cyber and the physical spaces are converting, the society is moving to the **"Digital Society" where various activities are carried out.**
- However, **various issues have surfaced**. It is necessary to **search for a 3rd way** that is neither "Dependence on a handful of giant companies", nor "Surveillance society".
- Under these circumstances, on **Internet and the Web** that has developed as an infrastructure of the digital society, **most data management, including identity management, depends on the respective service such as platform operators. Data is siloed and it is difficult to verify from outside how data is used.** "There is no option but to rely on platform operators" is the situation.
- In response to the proposal of the "Report on the Medium-Term Vision on Competition in the Digital Market" released in June 2020, with a view to realizing **DFFT**, **the "Trusted Web Promotion Council" was launched** in October 2020. Based on the results of the examination conducted so far, this whitepaper has been compiled as the **starting point for cooperating and collaborating with various parties inside and outside the country** in the future.

2. Current issues and their causes

- **The Internet and the Web** have developed as a **globally common infrastructure, making it possible to widely access information and various services have been created** on the top.
- However, **there is no adequate mechanism for ensuring trust relationship and safeness required in various social activities** carried out in the digital society. **While users rely on platform operators for most of their trust, this distortion** has created **several pain points**.

Examples of pain points

- ✓ **Concerns about data being exchange** such as fake news and false data controlling devices
- ✓ **Privacy risk** due to aggregation and consolidation of data including biological information
- ✓ **Balance between privacy and public interest** that is discussed due to the outbreak of COVID-19 etc.

- ✓ **The siloed industrial data** is not fully utilized
- ✓ Concerns about sustainability of the ecosystem **due to the winner-take-it-all** approach etc.
- ✓ **Dysfunction of governance** by social norms which should be applicable when conducting social activities

Underlying causes

- There is no adequate mechanism in place **that would allow users to effectively control access to their data**.
- **There is no mechanism of consensus building that would reflect the intentions of both sides** when they exchange data, and **there is no mechanism to verify the subsequent fulfillment status**.
- There is no mechanism to **verify the reliability of information (data)**.
- **Governance by multiple stakeholders** is not functioning.
- While there are **existing mechanism** like electronic signature **for increasing reliability, they have limitations when it comes to ensuring trust between unknown parties and avoiding the risk of a single point of failure.**

While leveraging the benefits afforded by **the Internet and the Web**, it is necessary **to add a certain governance and operational mechanism and the functions that enable such mechanism on the top.** → **The key is "Trust"**

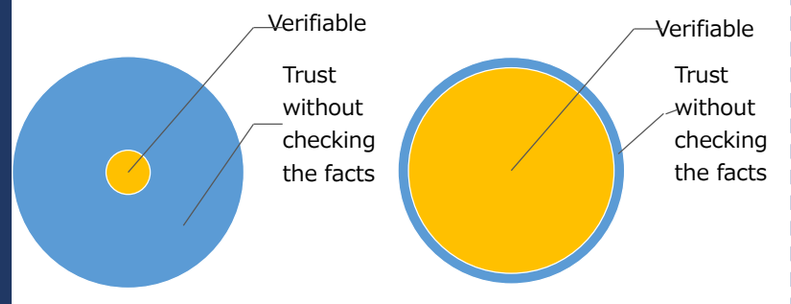
3. Goal of Trusted Web

Goal of Trusted Web

- **Goal**: Build **the new trust framework** for various social activities in the digital society **to enable various parties to create new value**.
- **New Trust Framework**: **Without replying on a specific service**,
  - **While making it possible to control the data disclosed to the other party**,
  - **and incorporating the mechanism of consensus building** in data exchange,
  - **expand the areas that can be verified**, and **reducing the areas that had to be trusted without checking the facts**, thereby **increasing the level of Trust** (the degree to which one believes that the other party behaves as expected).
- **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 confirming facts**

The verifiable areas change depending on the mechanism



The current internet :
Because of the small portion of the area that can be verified, decision making requires a great deal of trust in the other party.

Use of blockchain and other technologies :
There is a large portion of verification and a small element of trust in the other party.

***However, this method cannot be used for all use cases because of trade-offs in processing performance and other factors.**

Don't trust, Verify

Goal of Trusted Web :
A system that ensures a certain degree of verifiability, while satisfying Continuity, Interoperability and Ease of upgrade.
→ **Increase the level of "Trust"**

Direction

1.Sender of data: Individuals and companies can **check the receiver of the data**, **control the data disclosed on the basis of agreement**, and manage the values created by using the data

2.Receiver of data: Receivers can check the **sender** of the data and **data to be exchanged**, and value conversion is done **on the basis of the agreement**

3.Scheme of exchanging data: Based on verifiable data, it is possible **to build consensus** between the sender and the receiver **that reflect their mutual intentions** and **make changes according to the subsequent situation,** and it is possible to **verify this process and its outcomes.**

*Exchange: Includes processes within a single system, transactions between networked systems, and interfaces between systems and humans

4.Stakeholders involved: **Clearly define the roles of stakeholders** involved, where **each stakeholder plays its own role** to maintain and manage the functions related to Trust as a whole system.

Principles in design and operation

<Supporting mechanism>

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.

<Users' standpoint>

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.

<System's standpoint>

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.

4. Four main functions and governance that form the Trusted Web architecture

Management and verification of digital identity

① Identifier Management function

✓ *Management of Identifiers*

Users can issue identifiers by themselves and link them to various attributes.

→ So far, users were **locked in with an identifier issued by each service provider**, and **their attributes** (age, contract details, etc.) **were linked to the identifier and managed by the service provider**. **However, users should be able to control the scope of disclosure of attributes by themselves** and **avoid being identified**.

② Trustable Communication function

✓ *Reliable management and verification of identities*

Users can manage their attributes (Graduation certificate, test results, reliability, etc.) **endorsed or reviewed by a third party**, and **disclose them to the other party to the extent necessary**, and **the other party can verify the attributes without inquiring with the issuers** etc. **each time**.

→ **Judging by the trustworthiness of the data sender,** it is possible to **estimate the correctness of the contents of the message**.

Reflection and verification of intentions digitally

③ Dynamic Consent function

✓ *Dynamic consensus building*

For exchanging data, both sides can **go through the process of arriving at agreement after setting various conditions** and **manage the results of the agreement**.

→ This allows users to **control the conditions when exchanging data.** It is not a uniform rule, but **reflects the intentions of both parties**, and **if there is a discrepancy, it can be dynamically corrected.**

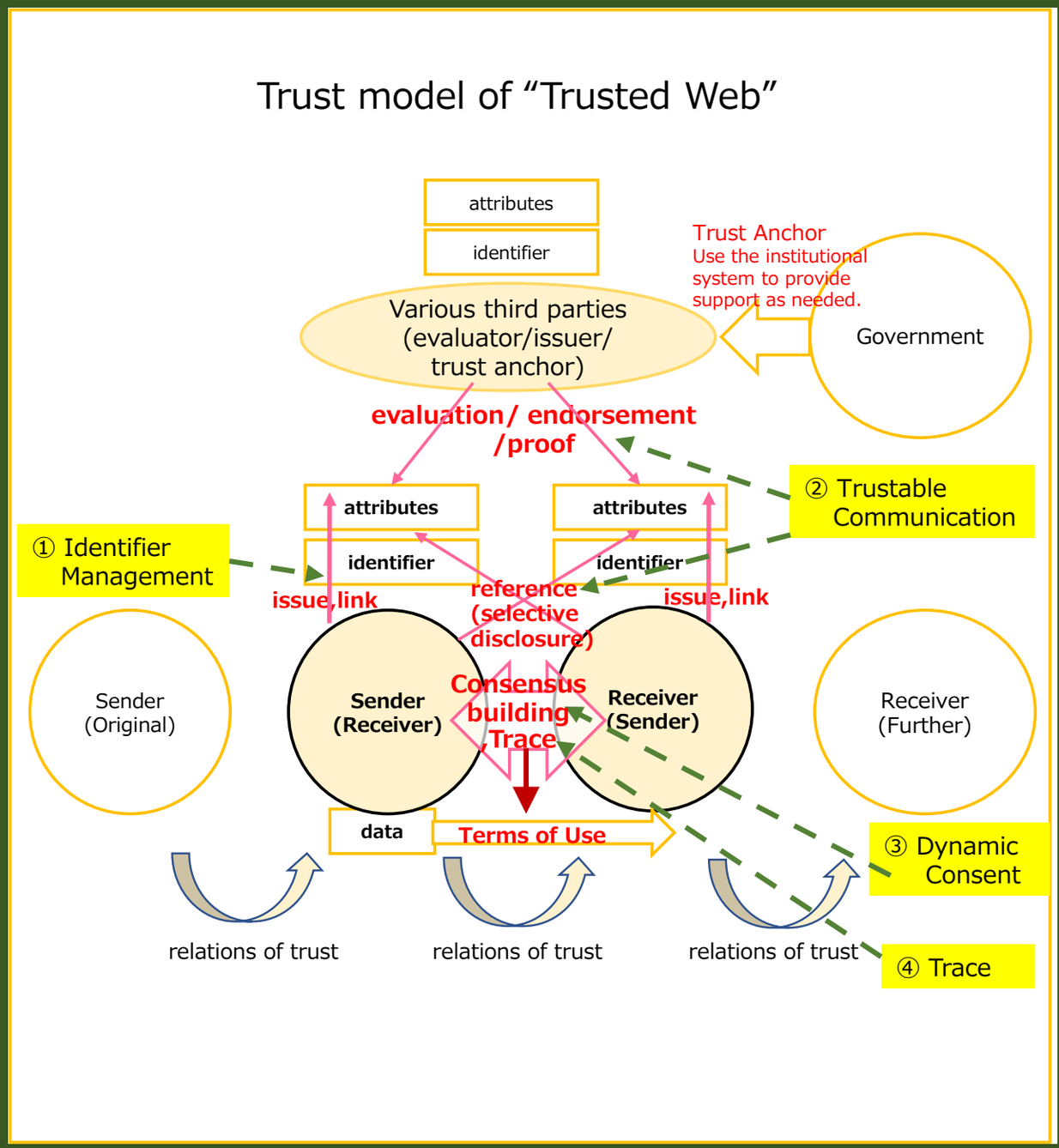
④ Trace function

✓ *Verification of fulfillment of conditions*

By setting conditions at the time of agreement, it is possible **to monitor the process of agreement formation and fulfillment of agreement**, and verify whether they are **appropriate or not**.

→ **Removing the concerns that once data is transferred, use of data becomes a complete black box**.

Technically, **when assuming P2P** (Peer to Peer. Computers communicate with each other on the equal basis), it is a frame for conducting "**Authentication**" in terms of authentication of entities, authentication of contents, and authentication of attributes**.**



Governance

- **Governance by multiple stakeholders** (Support the **chains underlying the Trust** in a decentralized collaboration. **Consensus building** on rules and operations)
- **Role of the government** (Function as a **trust anchor.** Development and operation of **supporting institutional system**)
- **Ensuring transparency** (Various stakeholders will verify and put checks and balances)
- **Incentive design** for making the ecosystem sustainable (**Design for public roles** such as contributing engineers and institutions that support the Trust)

5. Economic values expected to be created by Trusted Web

(1) Economic values expected to be created by Trusted Web

"Application layer"

- **Reliable data becomes more valuable** (Example: news contents)
- Once it becomes possible to verify the attributes of the other party, **it facilitates data sharing without even knowing each other**, **enabling collaboration that was previously difficult**
  (Example: Data sharing in the supply chain and value creation through it)
- **Value creation in synchronization with data flow and value flow**
  (Example: Precisely tracing the environmental load in the supply chain digitally and converting contribution made to social issues for SDGs into value)

"Middle layer"

- **Digital value creation by participating in a chain of trust as an institution giving "endorsement"**
  (Examples: Financial institutions, testing/auditing institutions, human resources education institutions, etc.)

"Infrastructure layer"

- **Provision of services through companies including startups for unbundled four functions** of Trusted Web
  (Identifier Management function, Trustable Communication function, Dynamic Consent function, Trace function)

(2) Examples of use case analysis

Distribution of content media, Proof of test results when traveling during the outbreak of infectious diseases, Proof of human resources qualifications, Understanding the value in the life cycle of vehicles

6. Road to implementation

(1) Future issues to be examined

- Such as specific mechanism of functions, interoperable framework, specific architecture based on use case and verification of its implementation, implementation options on the Internet, governance, concrete incentives etc. **We will conduct examination in collaboration with domestic and foreign communities by using the white paper as a starting point**.

(2) Road (image)

2021-22 Starting period
Dissemination and collection of feedback from the global community → Building a collaborative system with the Internet community → Whitepaper 2.0 preparation
Sandbox environment such as prototype and sample code
Coordinating with business-based initiatives, and identifying the requirements.
(Organizing ideathons, hackathons, etc.)

2023-24 Creation of functions and services
Provision of various services with excellent UI / UX such as Identifier management function, consensus building function, etc. by companies
→ Service deployment in human resources, PHR, contents, supply chain, etc.

2025- Implementation and dissemination in each field

2030 Internet-wide implementation

(3) Roles expected from each stakeholder

- Engineers (reference models, etc.), universities (prototypes), industry (new business models), users (active participation), international standard organizations (collaboration)
- The council will form a community in which engineers, universities, industry, etc. participate, revitalize the activities of related parties, collect feedback on various efforts made, and facilitate the entire initiative.

Trusted Web Promotion Council – List of Members

(As of March 12, 2021)

Koki Uchiyama	Chairman and CEO,Hotto Link Inc.
Urakawa	Chair, Sub-committee on Digital Economy, Keidanren / Director, Senior Managing
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	Professor, Graduate School of System Design and Management Keio University
Haruo Takeda, Dr.	Corporate Chief Engineer, Hitachi, Ltd.
Hiroshi Tsuda, Ph.D	Head of Security Laboratory,Fujitsu
Yusuke Tomimoto	Deputy Chief Officer, Innovation Division, TOYOTA FINANCIAL SERVICES CORPORATION
HASIDA Koiti	Professor, Graduate School of Information Science and Technology, The University of Tokyo
Takanori Fujita	Project Lead for Healthcare Data Policy World Economic Forum, Centre for the Fourth Industrial Revolution Japan
Masakazu Masujima	Partner, Mori Hamada & Matsumoto
Shin'ichiro Matsuo	Research Professor, Computer Science Department, Georgetown University / Head of blockchain research, NTT Research Inc.
Kazuyoshi Mishima	Co-Founder & COO, Keychain
○Jun Murai	Distinguished Professor,Keio University
Kristina Yasuda	Microsoft Corp. Identity Standards Architect

(○: Chairperson)

Observers: Cabinet Secretariat IT General Strategy Office, 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 March 12, 2021)

Tomoya Asai	Chief Technology Officer, WebDINO Japan
Hirochika Asai	Researcher, Preferred Networks, Inc.
Daichi Iwata	Director, Digital Integration Division, NEC Corporation
Koki Uchiyama	Chairman and CEO,Hotto Link Inc.
Masakazu Kikuchi	Secured Finance Co-founder & CEO
○Tatsuya Kurosaka	President and CEO, Kuwadate Incorporated
Kazue Sako	Waseda University
Shigeya Suzuki	Project Professor, Graduate School of Media and Governance, Keio University
Shigeru Fujimura	NTT Service Evolution Laboratories, NTT Corporation Senior Research Engineer
Shin'ichiro Matsuo	Research Professor, Computer Science Department, Georgetown University / Head of blockchain research, NTT Research Inc.
Sota Watanabe	CEO, Stake Technologies, Inc.

(○: Chairperson)