Trusted Web white paper ver. 2.0 executive summary

1. Background (Overview slides p.1-2)

- Amid digitalization of social and economic activities, various pain points have arisen, including concerns over data reliability due to fake news and potential social division, the infringement of privacy, excessive dependence on certain services in the winner-takes-all situation, and siloed industrial data that is underutilized.
- When the society is transitioning to "digital society," the current communication protocols of 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.

2. The new trust framework that Trusted Web aims to build (Overview slides p.3-6)

- In the current trust framework, the verifiable areas in data exchanges 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.
- It is necessary, without excessively relying on certain services, to enable users to control the data; incorporate mechanisms for consensus building in data exchanges and tracing; and expand verifiable areas and thereby increase the level of trust.
- Trusted Web aims to overlay such a new trust framework on the Internet and the Web to enable various parties to create new values.
- Establishment of a trust framework for data exchanges through Trusted Web is essential for facilitating the collaboration among businesses, which is the foundation for digital transformation that requires various entities' value co-creation across sectors and organizational boundaries.

3. Architectural design of Trusted Web (Overview slides p.7-19 and 21)

- After releasing the white paper ver. 1.0 in March 2021, for the purpose of realizing its concept, we analyzed three use cases in which: 1) individuals (changing their jobs); 2) corporations (applying for subsidies); and 3) supply chain (exchanging data on chemical substance content). Also, based on the first use case for individuals, we developed a prototype to identify issues for realizing Trusted Web.

- Building on this, we propose the following new trust framework that Trusted Web aims at.
  - ✓ Entities can manage their own identity by using externally linked identity management systems.
  - ✓ The level of trust will be increased through the expansion of verifiable areas of both created data and the process of data exchanges.
  - ✓ Principally, digital signature technology is used to ensure the verifiability of data. 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[1]".
  - ✓ Verifiability of data exchange processes is ensured by modeling exchanges and combining it with digital signature technology. When data is exchanged with other parties, its process is mutually recorded to make it verifiable.
  - ✓ Architecture needs to have a high degree of flexibility to combine standards and protocols.

- Based on the design described above, we present in the white paper ver. 2.0 the architecture associated with this new trust framework for Trusted Web. The four functions presented in the ver. 1.0 were reorganized into six components – the four components from a data-focused perspective, Verifiable data, Identity, Message, and Transaction, and the two components from the perspective of computational resources and communication, Node and Transport.

[1] 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.

- To build up the Trusted Web as digital infrastructure, which is a common asset, we will further discuss what kind of governance structure should be in place, so that we can avoid excessive reliance on certain corporate activities in order to prevent the reoccurrence of pain points seen today.

4. Roadmap to realization (Overview slides p.20, 22 and 23)

- We expect that, as various services embodying the functions Trusted Web aims for are provided and their areas of use would expand, a kind of middleware would be formed, for example, between the transport and the layer of individual services. Then, we expect that, in the middleware, APIs, data models and protocols that should be compatible would be identified, and that such compatibility would ensure interoperability, leading to standardization, and facilitate the establishment of the Trusted Web as infrastructure.
- With this roadmap in mind, we have started to collect use cases from the private sector in various fields and will further identify challenges and accelerate the cooperation with related organizations with a view to international standardization.
- The trust framework and the architecture proposed in the white paper ver. 2.0 may change, as we will further obtain feedback from and discuss with a wide range of interested parties both in Japan and abroad.