Cyber Physical Security for IoT Society

Aiming to establish a resilient security infrastructure to support Society 5.0

Industrial systems and IoT devices installed in physical space, including living environments, are connected to cyberspace, such as a cloud, through a variety of networks. Thus, additional value is created through advanced knowledge processing and analysis, leading to enormous economic benefits for society. However, as IoT-based solutions proliferate, industrial activities are increasingly being threatened by the possibility of cyberattacks. Supply chains can also be exposed to the risk of falsification or infection by malicious programs during manufacturing and distribution processes. To avoid these risks, a project is being planned to develop a cyber-physical security infrastructure to protect a large-scale supply chain equipped with IoT systems and services, including small and medium-sized businesses. During this project, newly developed infrastructure will be incorporated into an actual supply chain with the aim to strengthen an IoT-based society against cyberattack threats.

Program Directorr

GOTO Atsuhiro

President, Institute of Information Security

Profile

GOTO Atsuhiro received his PhD from the University of Tokyo in 1984. Upon graduation, he joined NTT, working for nearly 27 years on information technologies. In 2007, he was named head of the NTT Information Sharing Platform Laboratories, and subsequently named head of the NTT Cyber Space Laboratories in 2010. He became a professor at the Institute of Information Security's Graduate School of Information Security in 2011, and has served in his present position since 2017. Dr. GOTO has various experiences in government-related work as well, serving as member or chair for various councils and committees for the Cabinet Secretariat, the Ministry of Internal Affairs and Communications, the Ministry of Education, Culture, Sports, Science and Technology, the Ministry of Economy, Trade and Industry, and the Ministry of Defense.

Research and Development Topics

To ensure the security of an entire supply chain together with IoT systems and services, a trustworthy chain validating each component of hardware and software needs to be established. To this end, testing will be carried out on the creation and confirmation of trustworthiness in IoT device security and the building blocks of supply chains, including organizations, products, and services.

(A) R&D on technology to create and confirm trustworthiness

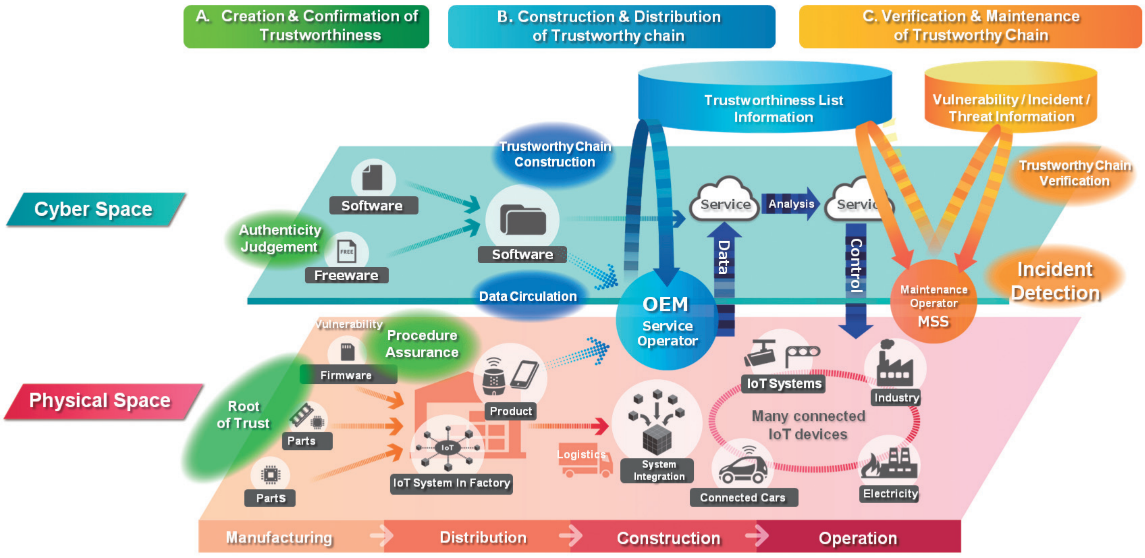
The security of individual IoT devices and services needs to be improved. R&D activities will be carried out on technology for creating and confirming trustworthiness to ensure the security of various IoT systems and services and an entire supply chain.

(B) R&D on technology to construct and distribute a trustworthy chain

R&D activities will be carried out on technology to construct a trustworthy chain for IoT systems, services, and supply chains. It will enable information to be distributed in a secure manner and ensure that security is maintained in various social infrastructures and services as well as wide-ranging supply chains.

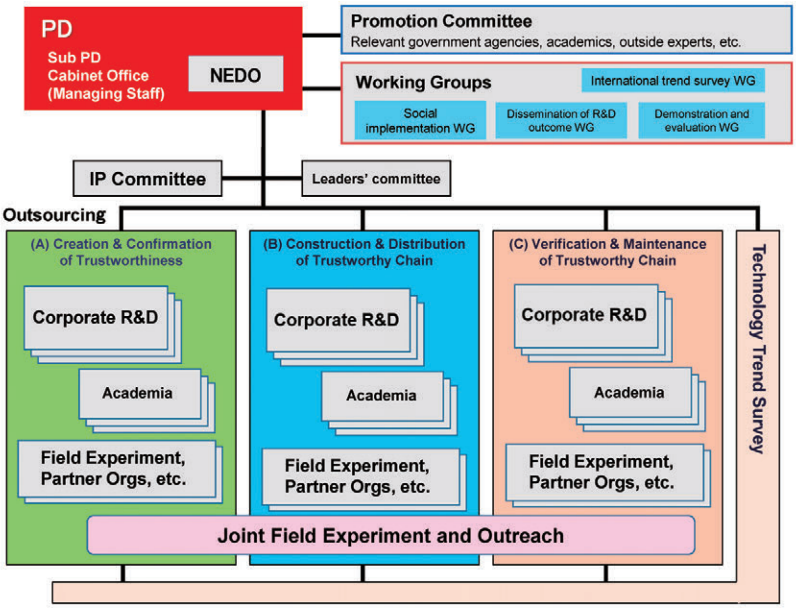
(C) R&D on technology to verify and maintain a trustworthy chain

R&D activities will be carried out on technology to verify that a trustworthy chain is safely operated and maintained. In addition, manuals will be prepared for the introduction and operation of a trustworthy chain, and human resources will be developed with a view toward applying developed technologies in society.



Implementation Structure

The project team will be led by a program director who works in cooperation with a steering committee composed of relevant government agencies, experts, and external specialists. This team will promote the project, while cross-sectional chakkenges, including demonstration and dissemination of R&D outcomes, will be addressed by working groups. Participating companies will play a key role in the project team, as they are expected to proactively commercialize R&D results. The project team will also include representatives of universities and other organizations which possess advanced tecnoologies. In addition, the project team structure will allow team members to share requirements raised from the perspective of realizing practical application. This will enable participating companies who have actual business experience and challenges to carry out demonstration tests in a proactive manner.


PD
Sub PD
Cabinet Office
(Managing Staff)
NEDO
Promotion Committee
Relevant government agencies, academics, outside experts, etc.
Working Groups
International trend survey WG
Social implementation WG
Dissemination of R&D outcome WG
Demonstration and evaluation WG
IP Committee
Leaders' committee
Outsourcing
(A) Creation & Confirmation of Trustworthiness
(B) Construction & Distribution of Trustworthy Chain
(C) Verification & Maintenance of Trustworthy Chain
Corporate R&D
Academia
Field Experiment, Partner Orgs, etc.
Corporate R&D
Academia
Field Experiment, Partner Orgs, etc.
Corporate R&D
Academia
Field Experiment, Partner Orgs, etc.
Joint Field Experiment and Outreach
Technology Trend Survey

Exit Strategies

☑ From demonstration testing to practical application

Demonstration testing of developed technologies will be carried out and test results will be fed back into R&D activities. In pursuit of early practical application in society, the cycle of testing and feedback will be repeated. At the same time, use of developed infrastructure will be promoted across supply chains, including small and medium-sized companies, with the aim of disseminating products, services, and systems having a high level of security ensured by Japanese technology.

☑ Commercialization led by participating companies

Participating companies will take the lead for the commercialization and introduction of developed technologies in industrial fields. Activities will include licensing of technology to relevant vendors with the aim of technology dissemination.

☑ Coordination with US and EU frameworks as well as the system established by Japanese government ministries

This project will be carried out in coordination with Japanese government measures regarding IoT devices and supply chains. It will contribute to the establishment of a system comparable to US and EU cybersecurity frameworks. In particular, it will be necessary to verify that project activities and achievements are in line with cybersecurity framework activities being accelerated in the US and Europe in order to ensure Japan's international competitiveness.

Past Milestones and Anticipated Outcomes

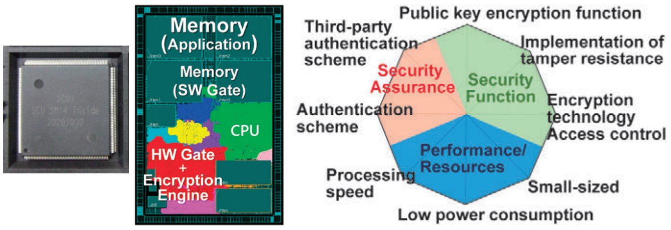
After completing basic technologies development in FY2020, project members have initiated demonstration experiment aiming at social implementation one by one using each prototype system.

In FY2021, demonstration experiment at social infrastructure services, building services and local governments, etc., will be accelerated under supervision of a "social implementation leader" in each team member organization.

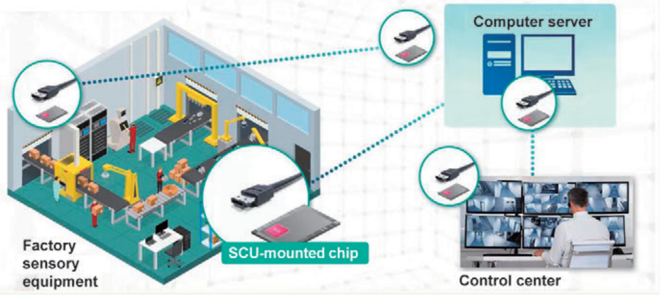
The management structure will include organizations responsible for verifying demonstration results, managing a trustworthiness list, and handling information about vulnerability, incidents, threats, or other issues related to infrastructure.

In this project, by realizing the "Cyber-Physical Security Infrastructure", the value creation brought about by the realization of Society 5.0 will be supported, and at the same time, the realization of the security assurance, that become a requirement for participating in the global supply chain, at an appropriate cost, will strengthen the international competitiveness of Japanese products and services.

Secure Cryptographic Unit (SCU), which forms the Root of Trust, and an illustration of its implementation



Application example of SCU-mounted chip to connector system


Computer server
Factory sensory equipment
SCU-mounted chip
Control center