Cross-Ministerial
Strategic Innovation Promotion Program (SIP)
Research and Development Plan for
Cyber Physical Security for IoT Society

July 19, 2018

(Revised July 11, 2019)

Director-General for Science,

Technology, and Innovation,

Cabinet Office

Overview of the Research and Development Plan

1. Significance and goals

IoT is the fundamental technology of Society 5.0[1], where IoT devices embedded in a physical space, such as social infrastructures, industrial systems, living environments, and natural environments, are expected to create various added values and services, and to bring significant benefits to the economy and society, which are also physical space, through connection with cyberspace, such as clouds via various networks, collaboration with advanced knowledge processing (represented by AI), and analysis processing as big data.

On the other hand, the scope of the targets of cyberattacks is rapidly expanding, and attack techniques are becoming more advanced. In particular, as a result of the spread and expansion of IoT which create new value within industrial society and family life, the threat of cyberattacks can be found in all industrial activities, not only in cyberspace, but also in physical space.

In addition, the risks of illegal programs being embedded, and programs being altered in an unauthorized manner during the processes of production and distribution of products and services, are becoming more prevalent within supply chains. Enhancement of cybersecurity measures is required within the global supply chains. As it is strongly feared that business operators, products, or services that fail to meet a certain level of security requirements may be excluded from global procurement projects in the future, it will be an important task to secure opportunities for the participation of the manufacturing sector, which accounts for the majority of exports from Japan.

That is why the "Cyber Physical Security Infrastructure" (hereinafter referred to as "*Infrastructure*"), which can be utilized to protect IoT systems, services and large-scale supply chains including SMEs, should be developed and verified for the purpose of protecting various IoT devices, and ensuring safety and security in society as a whole, towards the secure Society 5.0. After the effectiveness of the *Infrastructure* is confirmed through verification, the *Infrastructure* will be incorporated into supply chains that are actually operated, and put to practical use. Through promotion of implementation of this *Infrastructure* in society, IoT society will be made stronger against cyber threats, and a value of approximately 90 trillion yen, which Society 5.0 will bring[2], will be endorced.

---

1 Society 5.0 is a concept proposed in the 5th Science and Technology Basic Plan (Cabinet decision on January 22, 2016), which refers to a human-centered society where systems integrating cyberspace (virtual) and physical space (real) to a high degree will promote economic development, and solve social challenges.

2 From the "New Industrial Structure Vision" by New Industrial Structure Committee, Industrial Structure Council, the Ministry of Economy, Trade and Industry.
http://www.meti.go.jp/shingikai/sankoshin/shinsangyo_kozo /pdf/017_05_00.pdf

2. Content of the research

The research and development of the *Infrastructure*, which can handle the scale where a large-scale supply chain including SMEs becomes a multilayered structure (having 10,000 or more component organizations) and achieves the assurance of security for IoT systems/services (with thousands [or more] various IoT devices) and components (humans, organizations, products, systems, services, and data, etc.) of the supply chains, will be promoted. The *Infrastructure* is designed to achieve the security of the IoT systems/services and supply chains as a whole, by repeatedly performing the assurance of security (creation of trustworthiness) and confirmation thereof (confirmation of trustworthiness) on IoT devices and components of the supply chains, and by constructing a trustworthy chain. The three major items of research and development for the *Infrastructure* are as follows:

(A) "Creation & Confirmation of Trustworthiness" technology

Multidimensional research and development of the trustworthiness creation and confirmation technology necessary to enhance security of each IoT device and services, and to achieve assurance of security for various IoT systems/services and supply chains as a whole, will be conducted.

(B) "Construction & Distribution of a Trustworthy Chain" technology

Research and development of technologies for constructing a "trustworthy chain" in IoT systems/services and supply chains engaged in procurement and construction, and of ensuring the secure distribution of necessary information, will be conducted so that the security of various social infrastructures and services, as well as of a wide variety of supply chains, may be assured.

(C) "Verification & Maintenance of a Trustworthy Chain" technology

Research and development of technologies for verifying and maintaining the safe operations of a "trustworthy chain" will be conducted within the IoT systems/services, and supply chains where the "trustworthy chain" has been constructed.

3. Implementation structure

Program Director Atsuhiro GOTO[3] (hereinafter referred to as "PD") will be in charge of the establishment and promotion of the research and development plan. The Promotion Committee, which is chaired by the PD, and is composed of related ministries and agencies, specialists and experts, and for which the Cabinet Office serves as secretariat, will perform general coordination. Research and development will be promoted by research managers, who will be selected through open recruitment, through utilization of the National Research and Development Agency New Energy and Industrial Technology Development Organization (hereinafter referred to as "NEDO"). The progress of each research theme will be controlled

[3] President/Dean/Professor of the Institute of Information Security

under the management of NEDO. The PD may, if necessary, appoint sub-PDs to support the PD in managing the content and progress of the research and development. In addition, committees and working groups (WG) for planning and implementing efforts to widely publicize the activities and outcomes of activities for the project, and promote recognition and dissemination within industry, will be established as necessary.

4. Management of intellectual properties

The Intellectual Property Committee will be established in NEDO or an institution to which the selected research manager belongs (trustee), for the purpose of adjustment, so that the trend of intellectual properties applied by the trustee may be understood and managed, and such properties may be more conveniently used for industrial purposes.

5. Evaluation

Prior to the evaluation made by the Governing Board[4] at the end of each fiscal year, the research managers will conduct self-inspection, and the PD and management agency will also conduct self-inspections, referring as necessary to the opinions of outside experts.

6. Exit strategies

The research and development team will collaborate with user companies that are aware of challenges will be established from the start of the project, so that user requirements may be reflected in the technology development and verification experiments, and participating companies' proactive efforts for commercialization and establishment of business will be promoted. Introduction of the *Infrastructure* into supply chains (including SMEs) as a whole, and into the IoT systems/services of their constituent companies, will be promoted so that the outcomes of the projects may be adopted by 50% of the SMEs prior to 2030.

This project will be promoted through the SIP fund, and the participating companies' proactive contributions. The participating companies will play a central role in commercializing the outcomes of the research and development, and in promoting adoption thereof in various industrial areas. Some outcomes will be registered as IP (intellectual property rights), and licensed to related vendors for the purpose of dissemination. In order to disseminate the outcomes of this project more widely, the PD and the research and development team will have symposiums, seminars, and international conferences that may increase people's recognition and understanding of this project.

Projects related to this project are expected to include SIP automated driving (enhancement of systems and services), and SIP smart logistics services.

---

[4] The Governing Board is held to examine and consider important matters concerning SIP, thereby ensuring the smooth promotion of SIP.

Contents

1. Significance and goals

(1) Background, and situations inside and outside of Japan

Society 5.0 refers to a human-centered society where systems integrate cyberspace (virtual) and physical space (real) to a high degree (hereinafter referred to as "Cyber Physical Highly Integrated Systems"), to promote economic development and solve social challenges, and a society where all humans and things are connected through the use of advanced technologies such as IoT and AI, so that various knowledge and information may be shared, and new values may be created.

In addition, the development of networks, such as Connected Industries[5], enables construction of more flexible and dynamic supply chains that are different from those of the past, and increases opportunities to create new added values. On the other hand, in terms of cybersecurity, the number of target points of attack are increasing, and the range of necessary defenses must expand. One of the characteristics of cyberattacks is that attackers can break in if they can find even a single vulnerable point. From the attacker point of view, systems are becoming easier than ever to intrude into.

Moreover, the threat of cyberattacks is increasing day by day, and may significantly impact not only cyberspace, but also physical space, in Society 5.0, which is expected to develop along with the upcoming explosive dissemination and expansion of IoT devices[6]. There have actually been some cases of serious damage, such as a serious network fault caused by a large-scale DDoS attack via vulnerable IoT devices.

A certain security vendor's survey stated that cybercrimes in the entire world cause an economic loss of USD 600 billion (equivalent to 0.8% of the global GDP)[7].

Furthermore, the risks of illegal programs being embedded, or programs being altered in an unauthorized manner, during the processes of production and distribution of products and services, are becoming more prevalent within supply chains, such as in cases where the function of transmitting users' personal information overseas is embedded in the firmware of a smartphone.

To combat such supply chain risks, compliance with NIST SP800-171 is required for procurement by the Department of Defense, and other cybersecurity measures are being enhanced in the U.S. Similar cybersecurity measures are beginning to be required among supply chains in Japan, and fulfillment of certain standards may become a prerequisite for

---

[5] "Connected Industries" is a concept advocated in March 2017 by the Ministry of Economy, Trade and Industry as a model for future Japanese industries, referring to an industrial society in which various connections will create new added values.

[6] According to estimates by IHS Technology, the number of devices connected to the Internet was 17.3 billion as of 2016, and has been increasing at an average annual rate of 15.0% since then, so is expected to reach approximately 30 billion by 2020.

[7] From the report jointly published by McAfee LLC and CSIS, in February 2018.

business relationships in the future. It is feared that business operators, products, or services that don't satisfy security requirements may be gradually excluded in global supply chains.

In Society 5.0, the entire Cyber Physical Highly Integrated System composed of supply chains (including SMEs) and various IoT systems/services should be made highly resistant to cyberattacks from the formation phase of such societies. For that purpose, it is essential for assurance of security in the entire Cyber Physical Highly Integrated System to embed advanced security measures against unknown cyberattacks, on the assumption that such unknown cyberattacks may exist within the design, manufacturing, and operations phases, even after the elements (humans, organizations, products, systems, services, and data, etc.) constituting Society 5.0 are intricately interconnected to establish a diversified society.

(2) Significance and strategic importance

In order to promote Society 5.0 and Connected Industries, it is important to take adequate security measures to assure safety and security, but the security measures taken by a single company are far from sufficient in a society composed of various elements (humans, organizations, products, systems, services, and data, etc.) collaborating and merging with one another. In other words, even if each company separately considers cybersecurity measures for its products and services from the standpoint of "security by design" from the planning and design stages, it will not be sufficient. In addition to said measures, the entire IoT systems/services composed of a wide variety of IoT devices, and the entire supply chains including manufacturing and distribution (including related companies and business partners, etc.), should take security measures, taking into consideration the resilience of business activities, and cybersecurity should be established, including the security of data circulation, which would be difficult for a single player to strictly control (Figure 1-1).

If cybercrimes cause loss to the Japanese market at the same rate as that of the global economic loss found in the above-mentioned survey, the loss to the Japanese market may be approximately 3 trillion yen, which is 0.8% of Japan's current GDP. Thus, from the standpoint of Japan's economic development, cybersecurity measures for preventing cyberattacks are important.

On the other hand, in "Chapter 3 Cybersecurity Measures" of the "New Economic Policy Package", formulated by the Cabinet on December 8, 2017, the necessity of enhancement of IoT security and cybersecurity measures for SMEs is explained. This is an important project for promoting enhancement of the cybersecurity of IoT systems/services and the entire supply chain including SMEs in this IoT age.

In Society 5.0, which will be realized through a system that highly integrates cyberspace and physical space, it is essential for the advancement of the ICT industry, and the development of the society associated therewith, to establish a "Cyber Physical Security Infrastructure" (hereinafter referred to as "*Infrastructure*"), which can assure security for various IoT devices,

systems, and services from consumer equipment (such as smart home appliances) to industrial systems, as the most secure social infrastructure in the world.

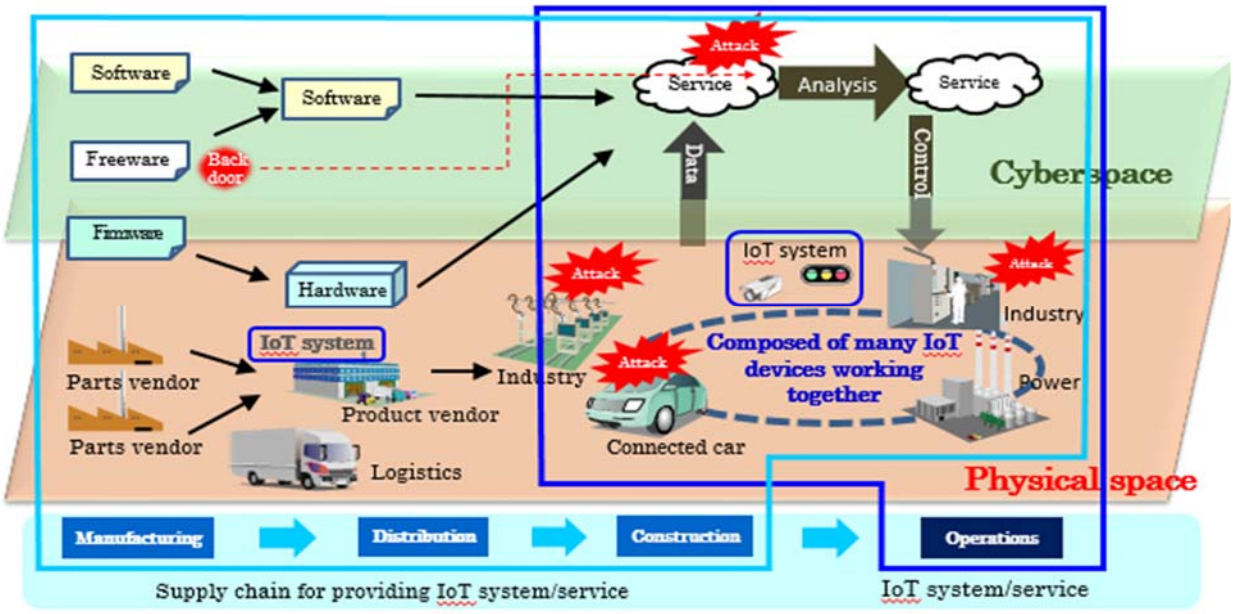

Figure 1-1. Challenges of the Cyber Physical Highly Integrated System toward Realization of Society 5.0

For that purpose, the most advanced core technologies in the world that will be necessary for realizing the *Infrastructure* will be developed, security will be assured for entire supply chains (including SMEs) engaged in the procurement and construction of IoT systems/services, and maintenance of security for various services will be realized. Verification of the effect of such developments within each industrial area[8] will contribute to an increase in the international competitiveness of industry, through reduction of the costs required for assurance of security of the entire life cycle of products and services, and improvement in the quality of security.

A value of approximately 90 trillion yen that Society 5.0 will bring, will be supported by establishment of the "Cyber Physical Security Infrastructure".

(3) Objective/Aim

(i) Toward realization of Society 5.0

- In Society 5.0, which will be realized by a system highly integrating cyberspace and physical space, this Project will assure the cybersecurity of the entire life cycle of the Society 5.0 services and systems, through the most secure social infrastructure in the world, "Cyber Physical Security Infrastructure" (Figure 1-2).
  - ➢ The purpose is to ensure complete security, without gaps even in situations where

[8] Areas where further economic development can be expected in Society 5.0 include automatic driving of vehicles, smart homes and buildings, new 5G-based communication services, the defense industry that supports Japan's defense capability, and medical devices.

the elements (humans, organizations, products, systems, services, and data, etc.) constituting Society 5.0 are diversified, and a large number of companies are involved in the supply chain in a multilayered manner.

- The evolution of cyberattacks will never cease, and the threat of such attacks may seriously affect not only cyberspace, but also physical space, in Society 5.0. With this situation in mind, we aim to make the entire Cyber Physical Highly Integrated System highly resistant to cyberattacks, by assuming that unprecedented cyberattacks may occur in the stages of operations, and in provision of products, systems, and services.

・ As Growth Strategy 2017[9] aims to improve labor productivity in the entire manufacturing industry by 2% or more every year through realization of Society 5.0, this Project will promote development and social implementation of technologies useful for the enhancement of the cybersecurity measures of entire supply chains including SMEs, which is essential for achievement of said aim.

・ It is assumed that the information necessary for the "Cyber Physical Security Infrastructure" will be in the merged and expanded databases of the "Trustworthiness Lists", which is the trustworthiness information of supply chains, and the original information to be used to determine the authenticity of components, in addition to traditional databases related to information security (vulnerability information, incident information, and threat information, etc.).

・ Effectiveness of the "Cyber Physical Security Infrastructure" will be confirmed through verification of the *Infrastructure*, and social implementation (that is, incorporation into live supply chains for practical use) of the *Infrastructure* will be promoted earlier than in any other countries, so that the IoT society may be made more resistant to cyberattacks, and realization of secure Society 5.0 in Japan may be promoted.

[9] Cabinet decision on June 9, 2017.
https://www.kantei.go.jp/jp/singi/keizaisaisei/pdf/miraitousi2017_t.pdf

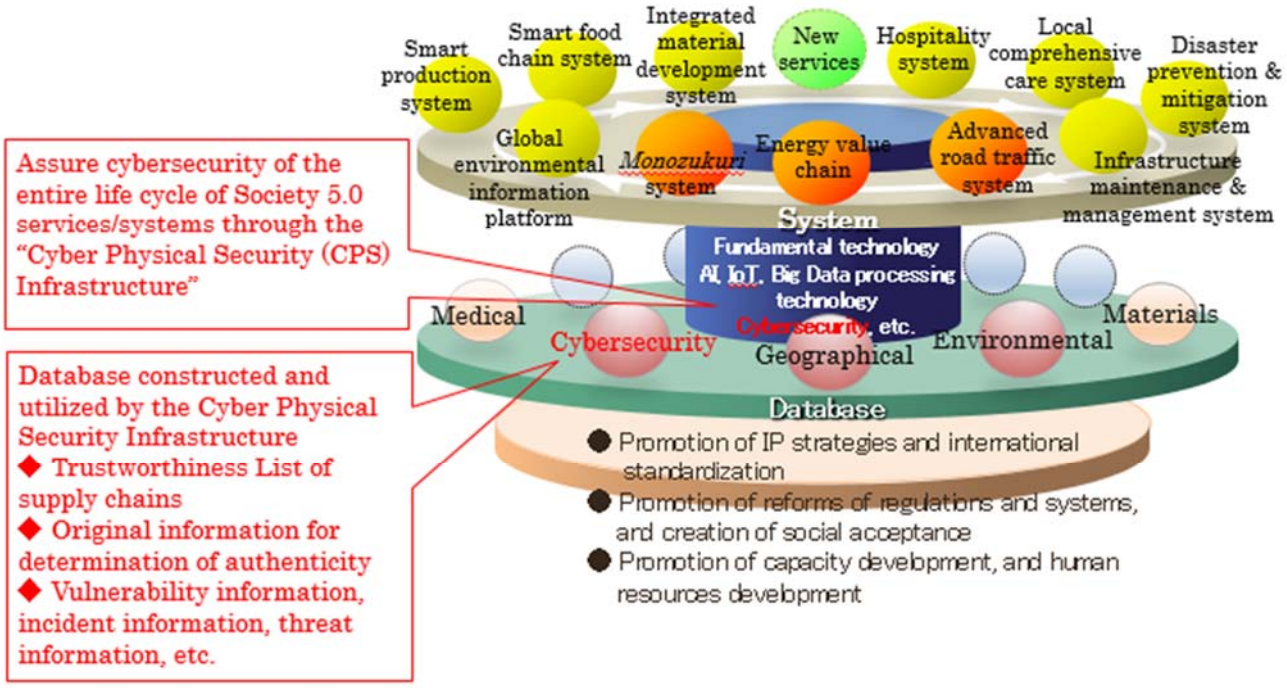

Figure 1-2. Roles of this Project in Society 5.0

(ii) Social objectives

- In a situation where the sources of cyberattacks are rapidly expanding, and attack techniques are becoming more sophisticated, this project will assure security of the entire supply chains (including SMEs) engaged in procurement and construction of IoT systems/services, and provide maintenance of security of the various IoT systems/services that are operated, thereby protecting IoT devices, systems, and services in the manufacturing/distribution areas, and smart buildings, etc., establishing the safety and security of all of society, and supporting a value of approximately 90 trillion yen that will be created by Society 5.0.

(iii) Industrial objectives

- The project will receive a good rating in the marketplace for the effectiveness of its technologies, by working on verification of the technologies in specific industrial areas constituting services that serve as social infrastructures or foundations, and large-scale supply chains, and by horizontally deploying the technologies in Japan and achieving satisfactory results after the technologies are established. As a result, international competitiveness will be enhanced in the areas of automated driving and smart life industries, new 5G-based communication services, the defense industry that supports Japan's defense capability, and medical devices, where further economic development can be anticipated due to the realization of Society 5.0.

- In order to avoid factors that may inhibit the international development of Japan's industries, consistency with cybersecurity measures taken in Europe and the U.S. will be ensured. Such measures will be introduced prior to 2030 in 50% of the SMEs that have high *monozukuri* quality in Japan, and responses to global supply chains will be promoted.
- Although Japan relies heavily on overseas business operators for security products for traditional IT devices, the leading technology development of security foundation products for IoT will be promoted through this research and development project, and efforts to standardize the technologies or to make them "de facto" will be made, so that a competitive advantage will be secured in overseas markets.

(iv) Technical objectives

- Multidimensional research and development will be conducted of (A) the "Creation & Confirmation of Trustworthiness" technology necessary to enhance the security of each IoT device and service, and to achieve assurance of security for various IoT systems/services, and entire supply chains, that is, the trustworthiness basic implementation (trustworthiness creation) technology applicable to a wide variety and large number of small-sized IoT devices in terms of both cost and performance, the IoT devices authenticity assessment (trustworthiness confirmation) technology, and the technology for eligibility assurance (trustworthiness confirmation) of the manufacturing process.
- Research and development will be conducted of (B) the "Construction & Distribution of Trustworthy Chain" technology for constructing a "trustworthy chain" in IoT systems/services, and of supply chains engaged in procurement and construction, and ensuring the secure distribution of necessary information so as to assure security in various social infrastructures and services, and a wide variety of supply chains, that is, the protocol technology and information distribution technology capable of constructing and utilizing the trustworthy chain.
- Research and development will be conducted of (C) the "Verification & Maintenance of Trustworthy Chain" technology to enable verification of safe operation, and maintenance of a "trustworthy chain" in IoT systems/services and supply chains where the "trustworthy chain" has been constructed.
- The (A) Creation & Confirmation of Trustworthiness, (B) Construction & Distribution of Trustworthy Chain, and (C) Verification & Maintenance of Trustworthy Chain above should not be developed simply as an elemental technology, but as a suite of technologies that can be consistently secured.
- As a concrete goal, "Creation & Confirmation of Trustworthiness" technology, "Construction & Distribution of Trustworthy Chain" technology, and "Verification &

Maintenance of Trustworthy Chain" technology will be established that can handle the scale where a large-scale supply chain including SMEs becomes a multilayered structure (having 10,000 or more component organizations), and achieve assurance of security for the IoT systems/services (with thousands [or more] of various IoT devices), and each component (humans, organizations, products, systems, services, and data, etc.) of the supply chains.

- As for the technology readiness level (hereinafter referred to as "TRL"), [10]the goal is TRL6 for the entire project, and TRL7 partially.

(v) Objectives pertaining to institutional systems

- Cyberattacks are performed across borders, so purely domestic efforts are not sufficient. Efforts that are always designed to secure international harmonization, such as enhanced collaboration with European countries and the U.S., and active promotion should be made of our efforts as international standards in an industry/academia/government collaboration. Specifically, with international trends in mind, collaboration should be pursued with ongoing activities for establishing security policies in the industrial areas of power, defense, automotive, smart homes/buildings, public transport, and telecommunications and broadcasting (Industry by Industry).
- In close collaboration with government measures by the Cyber Security Task Force (Ministry of Internal Affairs and Communications), the Study Group for Industrial Cybersecurity (Ministry of Economy, Trade and Industry), and the IoT Security Working Group (Ministry of Internal Affairs, Ministry of Economy, Trade, and Industry, and IoT Promotion Consortium)[hereinafter referred to as the "Three Major Government Measures[11]"]), contribution to establishment of systems for specific measures should be

---

10 Here, TRL as defined by the U.S. Department of Defense (DoD) will be used. TRL1: Level of proposal of basic principles/research and development papers TRL2: Level of confirmation and evaluation of basic principles/research and development papers TRL3: Analysis of basic principles and evaluation thereof in the laboratory TRL4: Level of evaluation of technical elements that are researched and developed, or of prototypes in the laboratory TRL5: Level at which technical elements that are researched and developed can be evaluated in the relevant environment TRL6: Level at which technical elements that are researched and developed can be demonstrated in the relevant environment TRL7: Level at which system prototypes can be demonstrated in the operational environment TRL8: Operation verification in linkage with the actual system TRL9: Level at which application to the actual/commercial system is possible.

11 In Japan, the Study Group for Industrial Cybersecurity was established in the Ministry of Economy, Trade and Industry in December 2017, and has just started considering cybersecurity measures in whole supply chains, with international trends in mind. Since December 12, 2017, the IoT Security Working Group under the control of the Ministry of Internal Affairs and Communications, the Ministry of Economy, Trade and Industry, and the IoT Promotion Consortium has considered measures for assuring the security of IoT devices, including authentication of IoT devices satisfying certain security requirements, while checking trends in the other countries mentioned above. In addition, the Cyber Security Task Force of the Ministry of Internal Affairs and

made, depending on individual needs in the industrial sector[12].

(vi) Global benchmarks

- In the United States, NIST SP800-171 is established as a standard for cybersecurity measures for controlling Controlled Unclassified Information (CUI)[13], and in connection with procurement for defense purposes, compliance with NIST SP800-171 by supply chains (including even subcontractors) is required (DFARS Clause 252.204-7012). In addition, the NIST Cybersecurity Framework, in which the government established the framework for risk evaluation of cybersecurity, states the policy of clearly positioning the evaluation of cyber supply chain risks.
- In Europe, the policy package published in September 2017 states that the EU Cybersecurity Certification Framework will be improved in the future. Cybersecurity measures that include supply chains are most likely to be sought in the future, with the characteristics of devices and certification methods both taken into consideration.
- This project will examine whether or not supply chains and IoT systems/services for which security is assured through the "Cyber Physical Security Infrastructure" can satisfy the overseas requirements mentioned above, as well as those in the Three Major Government Measures, thereby confirming their advantage in the world.

(vii) Collaboration with local government bodies

- IoT-related systems currently possessed by local government bodies, systems that are expected to be possessed in future, and their supply chains will be understood through information exchange with local government bodies, ministries, and industry associations, and the security requirements that are required for safe construction and operation will be clarified.

Communications announced "General Measures for IoT Security", including improvement of the systems for taking measures against vulnerability of IoT devices, in October 2017, promoting their measures.

[12] Japanese companies are significantly behind in responses to business partners, including contractors, compared with companies in European countries and the U.S.
http://www.meti.go.jp/committee/kenkyukai/shoujo/sangyo_cyber/pdf/001_05_00.pdf
For this reason, guidelines concerning comprehensive security measures have been established in collaboration with the "Cyber Physical Security Measures Framework", which the Ministry of Economy, Trade and Industry is trying to establish, in the hope that establishment of common guidelines concerning efforts through the detailed definition of security requirements in each area, and the social implementation of outcomes of the SIP, will double the understanding of security measures in IoT systems/services and supply chains, to a level comparable to European countries and the U.S.

[13] Although it is not highly confidential, it is regarded as "Controlled Unclassified Information", that is, information which should be controlled between only stakeholders having a need to share it.

2. Description of R&D activities

This Project will develop technologies for the "Cyber Physical Security Infrastructure" that will meet requirements such as (i) improved security of individual IoT devices, (ii) assurance of security in the entire supply chain (including SMEs) engaged in procurement and construction of IoT systems, and (iii) maintenance of security for various services, as well as for social infrastructures operated as IoT systems, thereby protecting IoT devices in such fields as production, logistics, and smart buildings, and establishing safety and security within all of society, with an aim to achieve secure Society 5.0.

o Assurance of security through the trustworthy chain

The basic idea of this research and development is to enhance security resistance by constructing and maintaining a trustworthy chain among components, both in the supply chain, and in IoT systems/services.

In the supply chain, the base of trustworthiness will be established on any of the components (humans, organizations, products, systems, services, and data, etc.) (that is, trustworthiness will be created), and a trustworthy chain starting from the base will create trustworthiness of each component, and enable confirmation thereof. By repeating this process, the "trustworthy chain" will be constructed throughout the supply chain, and the security of the supply chain will be assured through validation and maintenance of the trustworthy chain.

Similarly, in IoT systems and services, the base of trustworthiness will be established on IoT terminal equipment, etc., and the trustworthiness of each component (IoT equipment, IoT networks, clouds, etc.) will be created from the base and confirmed, thereby preventing tampering, etc., of the components. Construction, validation, and maintenance of such a "trustworthy chain" covering the components will achieve assurance of security over the entire IoT systems/services.

In addition, the supply chain and IoT systems/services are in a complementary relationship. For example, manufacturing plants and logistics systems, which are a part of the supply chain, are IoT systems, and products provided by the supply chain in the manufacturing and ICT industries are IoT systems (or equipment) or services. For this reason, in order to assure security for IoT systems/services, security for the supply chain engaged in procurement and manufacturing of said systems/services should be assured (e.g. a trustworthy chain should be constructed). Assurance of security for the supply chain will necessitate assurance of security for IoT systems/services that are components of the supply chain (e.g. production lines).

o Major R&D items

In this research and development of the "Cyber Physical Security Infrastructure", creation of trustworthiness, confirmation of trustworthiness, and construction and maintenance of the

trustworthy chain are important[14]. The three major R&D items are as follows:

(A) "Creation & Confirmation of Trustworthiness" technology

(B) "Construction & Distribution of Trustworthy Chain" technology

(C) "Verification & Maintenance of Trustworthy Chain" technology

In addition,

(D) Surveys of trends related to the "Cyber Physical Security Infrastructure",

which are required for research and development, will be conducted.

Figure 2-1 shows the complete picture of R&D items which are required for social implementation of security for the entire supply chain over the life cycle of products/services, through repeated assurance of security (creation of trustworthiness), and confirmation thereof (confirmation of trustworthiness) for each component of the supply chain, to construct a trustworthy chain.

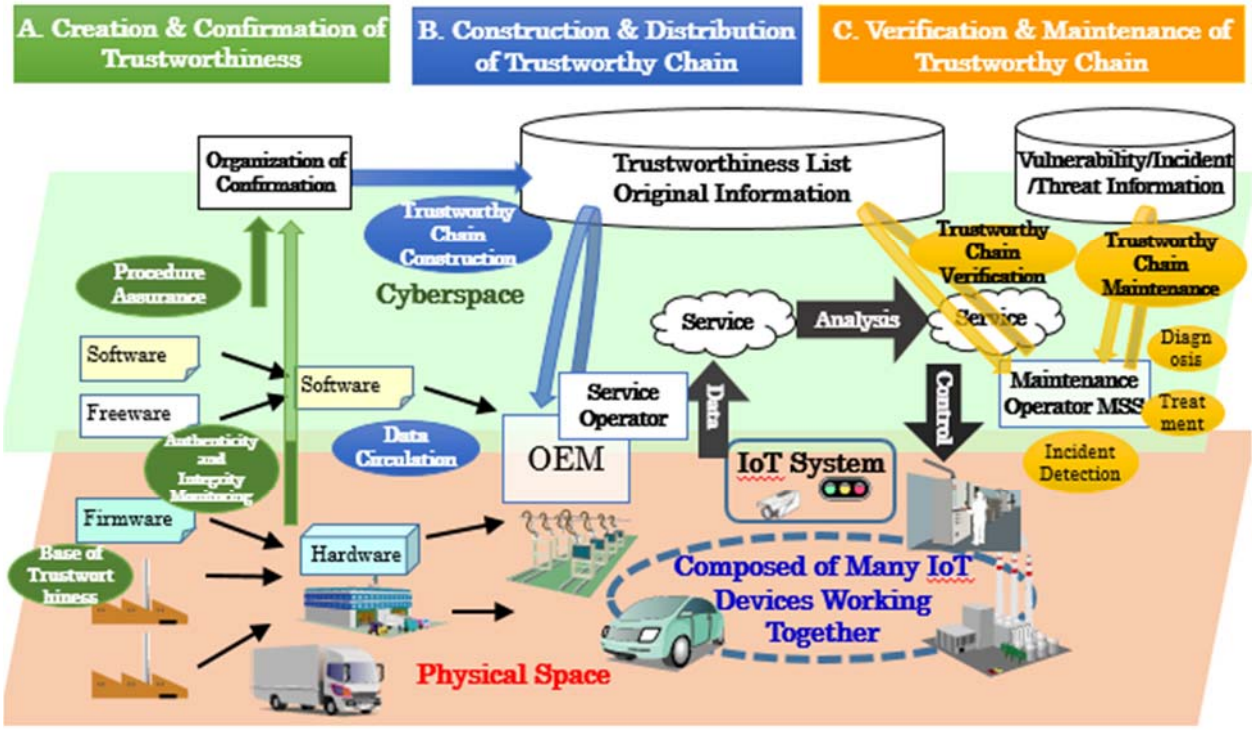

Figure 2-1. Image of the Cyber Physical Security Infrastructure Constructed with the Trustworthy Chain

In connection with (A), the "Creation & Confirmation of Trustworthiness" technology, multidimensional research and development will be conducted of the technology for creation

14 Also in the "Cyber Physical Security Framework", which the Ministry of Economy, Trade and Industry is trying to establish, assurance of security (creation of trustworthiness), and confirmation thereof (confirmation of trustworthiness), will be repeated for each component, and a trustworthy chain will be constructed and maintained, so that security for the entire value creation process will be achieved.

and confirmation of trustworthiness, which is necessary to enhance the security of each IoT device and service, and to achieve assurance of security for various IoT systems and services, and entire supply chains. In connection with (B), the "Construction & Distribution of Trustworthy Chain" technology, research and development will be conducted of the technology for constructing a "trustworthy chain" in IoT systems/services, and in supply chains engaged in procurement and construction, and for ensuring the secure distribution of necessary information so as to assure security in various social infrastructures and services, and a wide variety of supply chains. Further, in connection with (C), the "Verification & Maintenance of Trustworthy Chain" technology, research and development will be conducted of the technology to enable verification of safe operation, and maintenance of a "trustworthy chain" in IoT systems/services and supply chains where the "trustworthy chain" has been constructed. In addition, efforts will also be made to prepare the deployment and operation instructions necessary for social implementation of technical achievements, and to develop organizations and human resources.

During the research and development of the *Infrastructure*, experimental demonstrations on the development technology will be widely made, surveys for measuring the validity and effects of challenges will be conducted, and the results will be fed back to research and development. Dissemination activities, such as participation in international conferences where mutual evaluation with overseas initiatives is possible, will also be conducted.

In addition, (D) overseas trend surveys will be concurrently conducted, including surveys on R&D trends of related technologies and policy trends, and reflected in the research and development as appropriate, along with trend surveys on individual technologies to be conducted in (A), (B), and (C), respectively.

The three R&D items, and trend survey items, are described below.

(A) "Creation & Confirmation of Trustworthiness" technology

Assurance of security for various IoT systems/services, and entire supply chains, will start from a base on which the security for individual IoT devices and services can be enhanced, and on which their trustworthiness can be created. To that end,
(A1) research and development of the technologies for creating trustworthiness of IoT supply chains will be promoted.

In addition, in order to confirm the trustworthiness of the target devices, the manufacturing process thereof, and the provision process of the target services,
(A2) research and development of technologies for confirming trustworthiness through monitoring of authenticity and integrity of IoT devices, and
(A3) research and development of technologies for confirming trustworthiness through certification of the eligibility of procedures

will be conducted to realize frameworks for confirming that the target devices or services, have been generated while meeting requirements, both in terms of products and processes, or for confirming trustworthiness of the organizations or responsible individuals engaged in the process for generating the target devices or services.

Concurrent with this research and development, trend surveys related to technologies for creating and confirming trustworthiness will be conducted.

Based on the technologies mentioned above, the mechanism for certification concerning "things", hardware, software, services, and procedures will be prepared, and deployed in a system that is actually providing services, to verify the effects of the mechanism. In addition, it will be verified that (B) construction and distribution of the trustworthy chain, and (C) verification and maintenance of the trustworthy chain, which are the outcome of this research and development, constitute a consistent technology group. Experimental demonstrations will be conducted, including measurements of effectiveness, and dissemination activities will be conducted, based on their results.

(A1) Research and development of the technologies for creating trustworthiness of IoT supply chains

As the foundation of trustworthiness of large-scale IoT systems/services and IoT supply chains required in the age of Society 5.0, a set of functions for establishing the base of trustworthiness[15] (security assurance) on a IoT terminal device (terminal node), and enabling construction of a trustworthy chain through determination of authenticity of IoT devices and certification of the eligibility of procedures starting from the base is critical. To form such a set of functions, the following technologies will be researched and developed.

(i) Technologies for utilizing a cryptographic module which can be embedded in IoT devices, as the basis of trustworthiness.

(ii) Technologies for improving resistance to tampering, and for resisting malicious functions that may be embedded in hardware in any phase of the supply chain contrary to the supplier's intention, in order to respond to both cyberattacks and to physical attacks, on the base of trustworthiness.

(iii) Improvement/construction of the security assurance scheme for the base of trustworthiness. Specifically, patterns of attacks on the base of trustworthiness will be investigated, the technology for determining vulnerability of systems related to the base of trustworthiness will be established, standards for determining vulnerability will be established, and a framework will be constructed as an assurance scheme.

The technical challenge aspects of this theme are realization of the cutting-edge technology

[15] In the real world, based on a passport or driver's license (the base of trustworthiness), the identity of the holder of a bank account or mobile phone is assured (an example of construction of a trustworthy chain, starting from the base of trustworthiness).

for a base of trustworthiness which can be deployed in small-sized IoT devices, which is based on world-class cipher implementation techniques, and realization of resistance to tampering at low cost, which can be installed in various small-sized IoT device products.

Participating corporations and organizations :

Electronic Commerce Security Technology Research Association(Member: Yokohama National University, Kobe University, The University of Tokyo, Tohoku University, Nara Institute of Science and Technology,and Mitsubishi Electric Corporation), National Institute of Advanced Industrial Science and Technology

(A2) Research and development of technologies for confirming trustworthiness through monitoring of authenticity and integrity of IoT devices

As IoT devices cannot be properly monitored due to their characteristics, such as the large number, having no operator, and automatic operations, they tend to go unnoticed even if they are modified (tampered, or secretly switched), so damage may continue to occur for an extended period of time. In order to avoid damage, monitoring of the authenticity and integrity of each IoT device constituting the Cyber Physical Highly Integrated System, and immediate detection of contamination by malicious IoT devices, are required. To this end, the following technologies will be researched and developed.

(i) Technology for monitoring of authenticity and integrity that is so lightweight as to respond to IoT devices which otherwise would not accept security functions, and can respond to the very wide variety of architectures of IoT devices, and characteristics of the target devices.

(ii) Technology that can respond to the diversity of IoT devices, IoT systems, and supply chains, and enable reliable, efficient monitoring of the authenticity and integrity of the entire system, even if it is composed of an enormous number of IoT devices.

In spite of the diversification of IoT devices according to their usage and purposes, technologies that can monitor the authenticity and integrity of IoT systems while ensuring high resistance to cyberattacks and resilience will be realized, even if the IoT systems include an enormous number of IoT devices. In addition, lightness capable of responding to small-sized IoT devices, and flexibility capable of responding to IoT systems with various structures, are also technical challenges of this theme.

Participating corporations and organizations:

Nippon Telegraph and Telephone Corporation(Re-consignee:FFRI, Inc), NEC Corporation)

(A3) Research and development of technologies for confirming trustworthiness through

certification of the eligibility of procedures

In order to achieve secure Society 5.0, it is necessary to assure trustworthiness over entire supply chains. A procedure is a process in itself for creating values in a supply chain, so the technology for assuring eligibility that can certify trustworthiness of the procedure is necessary in order to construct a trustworthy chain. Thus, the following technologies will be researched and developed to assure the implementation of the procedures in the right order, without any addition or omission, as well as the trustworthiness of humans, organizations, products, systems, services, and data, etc., related to the procedure.

(i) Technology for making it possible to confirm that the procedure is implemented according to the predefined order, from events that can be observed from outside (such as human operation, the system log, network packets, etc.).
(ii) Technology for certifying the trustworthiness of an individual acting in a situation where several organizations act in linkage with one another, without using authority.
(iii) Technology for handling data according to a policy established by the creator (owner) of the data, and assuring that the data is not leaked or destroyed at the time of its delivery/receipt between organizations.
(iv) Technology for storing digital evidence so that the trustworthiness of humans, organizations, products, systems, services, data, and procedures, etc., can be confirmed at a later date.

The technical challenge aspects of this theme are realization of assurance of eligibility capable of integrating various kinds of element information existing in both physical space and cyberspace, to be presented to third parties, and assurance of traceability with digital evidence in an environment where many large-scale supply chains overlap with one another.

Participating corporations and organizations:

Hitachi, Ltd., NEC Corporation, KDDI Research, Inc.(Re-consignee: Advanced Telecommunications Research Institute International, Waseda University)

(B) "Construction & Distribution of Trustworthy Chain" technology

In large-scale plant and automotive industries, the number of OEM companies in supply chains is in the range of tens of thousands, and most of them are SMEs. IoT systems/services are provided by such supply chains, while part of these supply chains is composed of IoT systems. In this way, IoT systems/services and supply chains form a multilayer structure in Japanese industry as a whole.

In such IoT systems/services and large-scale supply chains, an environment will be necessary where a "trustworthy chain" is constructed through repetition of creation and confirmation of

trustworthiness and necessary information for operations is made to flow, and in such an environment, creation and management of a trustworthiness list that makes it possible to efficiently confirm that the target devices or services have been correctly generated, and development and realization of a secure distribution environment of work-related data, including information on trustworthiness, will be important. To that end,

(B1) research and development of the technology for constructing a trustworthy chain on the basis of characteristics of each area, and

(B2) research and development of the technology for safe distribution of information related to the trustworthy chain will be promoted.

Concurrent with this research and development, trend surveys will be conducted that are related to technologies for construction and distribution of trustworthy chains.

Based on the technologies mentioned above, a mechanism for construction and distribution of the trustworthy chain will be prepared, and deployed in a system that is actually providing services, to verify the effects of the mechanism.

In addition, the technology for construction and distribution of trustworthy chains will be established through repetition of verification in a demonstration field in several application areas, and it will be verified that (A) creation and confirmation of trustworthiness, and (C) verification and maintenance of trustworthy chains, which are the outcome of this research and development, constitute consistent group technologies. Experimental demonstrations will be conducted, including effectiveness measurement, and dissemination activities will be conducted based on their results.

(B1) Research and development of the technology for constructing a trustworthy chain on the basis of the characteristics of each area

The following technologies will be researched and developed, because in various business fields to which the outcomes of this research and development will be applied, different elements (such as humans, organizations, products, systems, services, data, procedures, etc.) are important for assurance of trustworthiness in the relevant supply chain.

(i) Development of requirements for achieving security for supply chains, depending on the characteristics of the application area ("area-specific profile") as security measures for each business area

(ii) Techniques for constructing a trustworthiness list according to the area-specific profile (techniques for configuring and managing the trustworthiness list)

(iii) A trustworthiness list technique for certifying that humans, organizations, products, systems, services, data, procedures, etc., involved in creating values can be trusted, and the techniques for utilizing the trustworthiness list by business operators that constitute a supply chain (techniques for registration, update and reference of the trustworthiness

list, the protocol technology, collaboration with the procurement system, and others.)

The technical challenge aspects of this theme are realization of techniques for construction and utilization of a trustworthiness list of which the compatibility with business operation of the actual operator can be confirmed through experimental demonstrations in an actual supply chain, and realization of both reduction of the operational costs, and robustness of the trustworthiness list corresponding to that actual business.

Participating corporations and organizations:

Hitachi, Ltd.(Re-consignee: National Institute of Advanced Industrial Science and Technology, Secom Co., Ltd.), NEC Corporation, KDDI Research, Inc.(Re-consignee: Advanced Telecommunications Research Institute International)

(B2) Research and development of technology for safe distribution of information related to the trustworthy chain

Data circulation technology, which provides safe distribution of work-related data (such as information related to trustworthiness) in order to form a trustworthy chain in the provision/operation of IoT systems/services and supply chains, will be realized. Specifically, technology (which satisfies the following) will be realized by monitoring and managing security in data circulation, and if any anomaly is detected, impacts on the system will be reduced in minimum, and then secure and scalable data circulation will be enabled.

(i) Technology for securing certification and traceability required for construction of a trustworthy relationship during data circulation.
(ii) Technology for visualizing the impact of cyberattacks related to data circulation.
(iii) Technology for minimizing any impact on the system by cyberattacks.
(iv) Technology for assuring resiliency related to safe data circulation through integrated implementation of (ii) and (iii) above.

The technical challenge aspects of this theme are realization of technologies having both scalability and traceability in an information distribution environment where a large number of wide-area, large-scale supply chains overlap with one another, and realization of an information distribution environment which is easy to deploy due to lightweight implementation, and reduction of operational costs.

Participating corporations and organizations:

Fujitsu Limited(Re-consignee: National Institute of Informatics, Nagoya University)

(C) "Verification & Maintenance of Trustworthy Chain" technology

It is important to verify and maintain safe operations of the "trustworthy chain" even after construction of a "trustworthy chain" is realized on a Cyber Physical Highly Integrated System. To that end,

(C1) research and development of the technology for verifying trustworthy chains, and

(C2) research and development of the technology for maintaining trustworthy chains

will be promoted. In addition, technology for ensuring and improving system recovery and resilience during operations, and technology for controlling data circulation, will be also considered as subjects of the research and development.

Concurrent with this research and development, trend surveys will be conducted that are related to technologies for verification and maintenance of trustworthy chains.

Based on the technologies mentioned above, the mechanism for verification and maintenance of trustworthy chains will be prepared, and deployed in a system that is actually providing services, to verify the effects of the mechanism. In addition, it will be verified that (A) creation and confirmation of trustworthiness, and (B) construction and distribution of the trustworthy chain, which are the outcome of this research and development, constitute a consistent technology group. Experimental demonstrations will be conducted, including effectiveness measurement, and dissemination activities will be conducted based on their results.

(C1) Research and development of the technology for verifying trustworthy chains

In order to secure the trustworthiness of an entire supply chain, it is necessary that business operators constituting the supply chain develop the technology for verifying a trustworthy chain that is constructed on the Cyber Physical Highly Integrated System. In particular, the following technologies will be developed, taking into consideration the difference between the business operators, difference of business areas, difference of configuration and operation, etc., of area-specific profiles and trustworthiness lists, and the need to conceal parts of the supply chain in some business areas.

(i) Technology for verifying trustworthy chains between different business operators, or different business areas, and the technology that enables coordinated verification among several different trustworthiness lists (such as protocol technologies, coordination with procurement systems, and others.)

(ii) Technology that enables verification of a trustworthy chain only by confirming that the chain is composed of trustworthy individuals, organizations, products, systems, services, data, and procedures, even if the specific names of the organizations, or specific structures of things, are not disclosed.

The technical challenge aspects of this theme are performance of evaluation of consistency and operational costs of activities related to the supply chain, through establishment of a verification protocol in an operational environment among several business operators, and

realization of technology that enables verification of trustworthiness, while keeping information hidden.

Participating corporations and organizations:

Hitachi, Ltd.(Re-consignee: National Institute of Advanced Industrial Science and Technology), NEC Corporation, KDDI Research, Inc. (Re-consignee: Advanced Telecommunications Research Institute,Inc.)

(C2) Research and development of technology for maintaining trustworthy chains

As coordinated operations by various devices that constitute cyberspace and physical space are promoted, the targets of cyberattacks are anticipated to expand from current relatively simple IoT devices performing IP communications to more diverse and specialized IoT devices. In addition, devices for which security countermeasures are insufficient, or devices on which it is difficult to implement security countermeasures, will continue to be used, due to the limited capabilities of the IoT devices themselves, or lack of operator skills.

In these surroundings, we will establish the three following technologies in order to maintain safe operation of trustworthy chains in a Cyber Physical Highly Integrated System. These technologies will support the entire security process, including detection, analysis, and mitigation of anomalies occurring on the system, and enable prompt responses to security incidents.

(i) Detection technology that enables accurate detection of anomalous events occurring across cyberspace and physical space, by efficiently and correctly collecting events in both cyberspace and physical space, and analyzing them in an integrated manner.

(ii) Technology for detecting and eliminating illegal data (physical data, control data, etc.) that flows between cyber/physical space.

(iii) Technology that enables, by using simulation, assessment of impacts and determination of countermeasures when cyberattacks take place on a Cyber Physical Highly Integrated System, and supports taking said countermeasures in the actual environment.

One technical challenge aspect of this theme is to remarkably shorten response time from the occurrence of an anomalous event until detection and response. In addition, this theme also aims to make it possible to decide swift and optimal countermeasures against the cyberattack while suppressing any impact on the actual system, by simulating and assessing in advance the direct impact of the attack, and the side effects of countermeasures.

Participating corporations and organizations:

Nippon Telegraph and Telephone Corporation（Re-consignee: Osaka University）, Mitsubishi Electric Corporation（Re-consignee: Kanazawa Institute of Technology）, Hitachi, Ltd., NEC Corporation

(D) Surveys of trends related to the "Cyber Physical Security Infrastructure"

To constantly update the exit strategies of this research and development, trend surveys will be conducted, mainly overseas, on the following four items, including trends of R&D, and policies related to the "Cyber Physical Security Infrastructure". For such surveys, all of the surveys, including ones that are individually conducted in connection with the research themes of (A), (B) and (C), will be coordinated. This surbeys was conducted only in 2018.

(i) Similar legal systems and civil activities in Asia, Europe, and the U.S.
(ii) Trends of evaluation technologies, taking into consideration the development of technologies related to IoT systems/services.
(iii) Trends of vendor evaluation as seen from the entire supplier chains, and related technologies.
(iv) Proposal on the direction of this research and development, based on results of the surveys.

Participating corporations and organizations：NEC Corporation

3. Implementation structure

(1) Utilization of National Research and Development Agency New Energy and Industrial Technology Development Organization

This Project will be implemented in the structure shown in Figure 3-1, using subsidies granted to NEDO. NEDO will support PD and the Promotion Committee and provide necessary cooperation in, for example, budget management and management of the progress of the research and development (including management of intellectual properties).

(2) Selection of research managers

This Project will construct a project implementation structure based on industry/academia cooperation, including universities and ventures that have advanced technologies, and among others, corporations that can independently make practical use of and commercialize the outcomes of the research and development. On the basis of this concept and this R&D Plan, NEDO will select research themes, as well as research entities and research managers that will pursue the research themes, through open recruitment. NEDO will, in consultation with PD and the Cabinet Office, determine the method of screening for the selection, such as standards for screening, and judges. In principle, PD and outside experts will participate in the screening. Stakeholders of researchers that have applied for a theme will not participate in the screening for the theme. The scope of "stakeholders" will be defined by NEDO. After research themes are determined through the selection, the research themes, as well as research entities and research participants thereof, will be specified in this Plan.

(3) Measures to optimize the research system

PD will consider changing or adding to research themes, or replacing or adding research entities, depending on the progress of the research themes, research results of technical surveys, conducted by related organizations, and changes of social circumstances. PD may, if necessary, appoint sub-PDs to support PD in managing the content and progress of the research and development.

For some research themes, adoption of the "stage gate method" may be considered, in which research entities will be narrowed after various proposals are selected and promoted for a fixed period, so that this Project may be promoted with an optimal structure.

A Leader Committee will be established, so that coordination amongst the research entities working on their own research themes can be promoted, and the objectives of this Project can be shared through regular information exchanges.

(4) Enhancement of the activities for dissemination and promotion of outcomes

Besides demonstration of the activities and outcomes of this Project by the participating

corporations and organizations, PD will take the initiative in appropriately establishing committees and working groups (WG) designed to more widely disseminate such activities and outcomes, to make them understood by the industrial world, and by announcing the content of efforts in symposiums, seminars, and business events, and by planning and providing international conferences.

WG planned are as follows. In fiscal 2019, in parallel with research and development ,we will start WG activities to resolve cross-theme issues.

(i) Demonstration and evaluation WG:

- In the demonstration test, investigate and consider methods to measure the practicality and effectiveness,and jointly with potential pilot partners and share among the themes for conducting pilot experiments.
- Consider demonstration experiments among the issues in this project, in cooperation with other national projects. (Role of external liaison)

(ii) Dissemination of R&D outcomes WG:

- Promote commercialization (productization) by participating companies and promote introduction to each industry field (collaboration with IP Committee)
- Launching an environment where small and medium-sized enterprises, such as shared verification centers (for voluntary evaluations), can easily utilize the R&D products and outcomes
- Plan and hold an international symposium to disseminate this initiative overseas

(iii) Internationl trend survey WG:

- Consolidate the status of relevant trends surveyed in Japan and abroad for each theme and share them across projects
- Organize advocacy activities actively to the United States NIST, European ENISA, and others. as international collaboration activities

(5) Coordination with government ministries and agencies

The "Cyber Physical Security Infrastructure", which is the goal of this Project, aims to assure security for supply chains of various social services and the manufacturing sector, and for their operational collaborations, and is a cross-sectional effort that requires coordination amongst a wide variety of government ministries and agencies, including the Ministry of Internal Affairs and Communications, the Ministry of Economy, Trade and Industry, NISC, the IT Comprehensive Strategy Office, the National Police Agency, the Ministry of Defense, and the Ministry of Health, Labor and Welfare. For this reason, this Project will be promoted in collaboration with the Promotion Committee and the three major ministries mentioned above to, among other things, establish the "Cyber Physical Security Infrastructure", which will be necessary to assure security for systems and services corresponding to IoT society and entire supply chains.

(6) Contribution from the industries

In this Project, practical use and commercialization is contemplated of the products and outcomes of the research and development, based on voluntary contribution by the participating corporations. In order to ensure that business operators and vendors who have actual fields and are aware of challenges may independently work on experimental demonstrations toward social implementation of technology outcomes, a structure in which they can closely collaborate with the research and development team from the start of this Project, and requirements from the standpoint of sharing social implementation, will be established. Each of the corporations engaged in the research and development, and the business operators participating in demonstration experiments, will be urged to invest human and business resources on their own initiative. Future contribution from the industrial world (including human and material contribution) is expected to account for 15% to 35% of the total research and development expenses (the total includes contributions from the national government, and the industrial world).

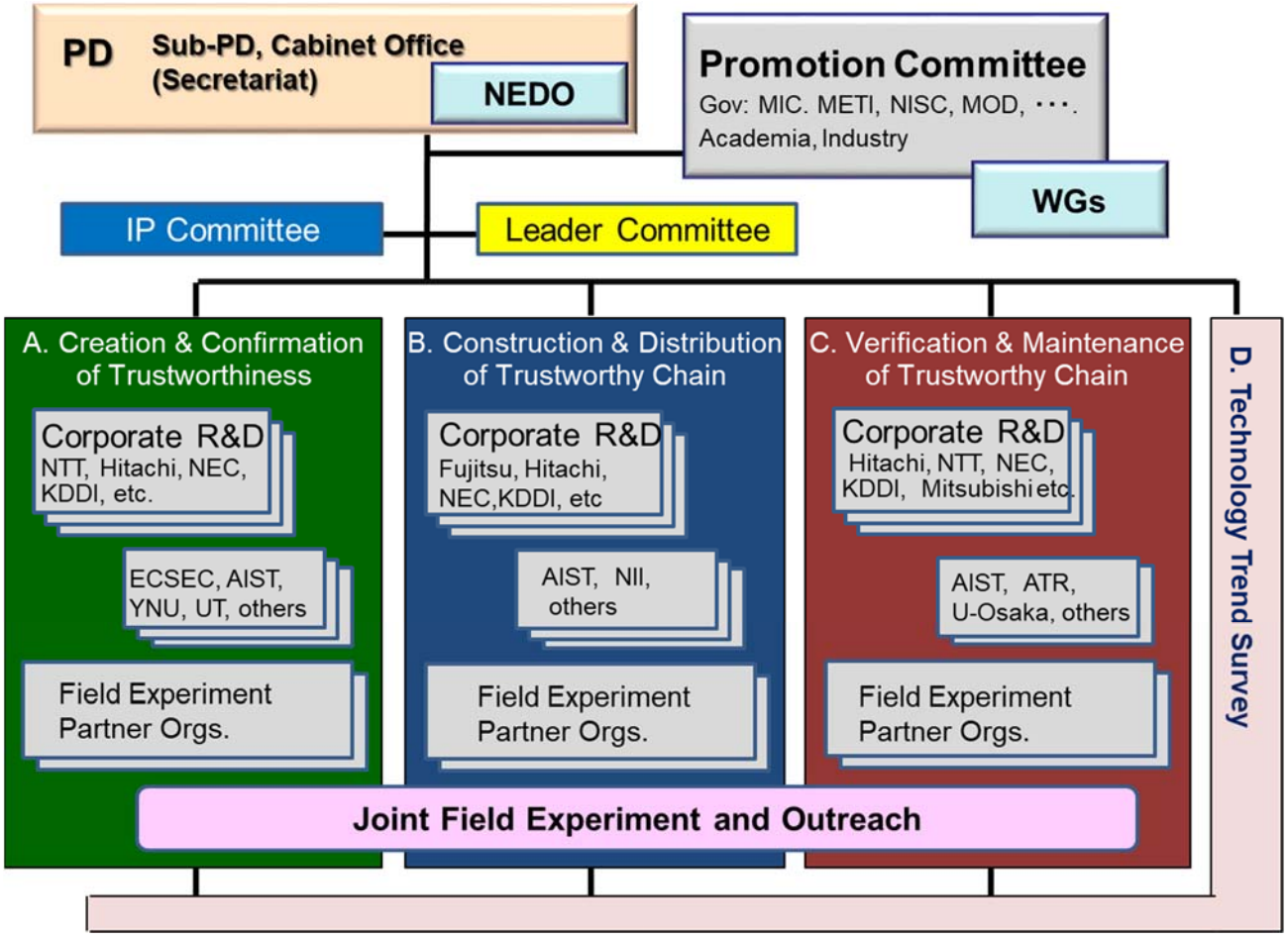

Figure 3-1. R&D Team by Leading Organizations

4. Matters related to intellectual properties

(1) Intellectual property committees

- For each research theme or research item constituting a research theme, an intellectual property committee will be established in the management agency, or an organization to which the selected Research Manager belongs (trustee).
- Intellectual property committees will determine policies for the publication of papers, and the application and maintenance of patents (hereinafter referred to as "IP rights"), concerning outcomes of the research and development, conducted by an organization which has established a relevant intellectual property committee, and perform adjustment, concerning licensing of IP rights, if necessary.
- Intellectual property committees will in principle be composed of PD or PD's agent, major stakeholders and experts.
- Details of operating methods of an intellectual property committee will be determined by an organization which has established an intellectual property committee.

(2) Arrangement concerning IP rights

- The management agency will determine in an agreement with the trustee in advance the handling of confidentiality, background IP rights (IP rights that research managers and the organizations to which they belong had possessed prior to participating in the program, or that they obtain without the use of the operating expenses of SIP after participating in the program), and foreground IP rights (IP rights generated through the use of the operating expenses of SIP during the program).

(3) Licensing of background IP rights

- The rights holder can grant a license for a background IP right to another program participant under terms and conditions determined by the rights holder (or "in accordance with the agreement with the program participant").
- In cases where IP rights holder responses, including said terms and conditions, may interfere with the promotion of SIP (including not only the research and development, but practical use and commercialization of the outcomes), the relevant intellectual property committee will make efforts for coordination and reasonable solutions.

(4) Handling of foreground IP rights

- In principle, the provision of Article 19, Paragraph 1 of the Industrial Technology Enhancement Act will apply to foreground IP rights, which will be vested in the organization to which the research manager who is the inventor belongs (trustee).
- In the event of an invention made by a re-trustee and others, IP rights may be vested in the

re-trustee and others, only with the approval of the relevant intellectual property committee. In such cases, the intellectual property committee may attach conditions to such an approval.

- If the rights holder of an IP right has little intention of commercializing it, the relevant intellectual property committee may promote possession of the IP rights by, or grant license for the IP rights to, an individual who is more committed to commercialization.
- For any individual withdrawing from the project during the participation period, the management agency and others, will have that individual assign free of charge, or grant a license for, all or part of the outcomes obtained with the use of the operational expenses of SIP during that individual's participation period (or all of the outcomes since that individual initially participated in the project, in the event of participation for several fiscal years) at the time of withdrawal.
- In principle, the rights holder will be responsible for the costs of application and maintenance of the IP rights. In the case of joint application, the percentages of ownership and cost burden will be determined through consultation between the joint applicants.

(5) Licensing of foreground IP rights

- The rights holder can grant a license for a foreground IP right to another program participant under terms and conditions determined by the rights holder (or "in accordance with the agreement with the program participant").
- The rights holder can grant a license for a foreground IP right to a third party under terms and conditions determined by the rights holder; provided, however, that such terms and conditions shall not be more advantageous than those for other program participants.
- In cases where IP rights holder responses, including said terms and conditions, may interfere with the promotion of SIP (including not only the research and development, but practical use and commercialization of outcomes), the relevant intellectual property committee will make efforts for coordination and reasonable solutions.

(6) Approval for transfer of, and establishment and transfer of an exclusive license for, foreground IP rights

- Under the provision of Article 19, Paragraph 1, Item 4 of the Industrial Technology Enhancement Act, any transfer of, or any establishment or transfer of an exclusive license for, foreground IP rights will require the approval of the management agency, except in cases of transfer due to a corporate merger or division, or transfer of IP rights to a subsidiary or parent company, or establishment or transfer of an exclusive license to a subsidiary or parent company (hereinafter collectively referred to as "cases of IP rights transfer due to mergers, etc.").
- Cases of IP rights transfer, etc., due to mergers, etc., will require the approval of the

management agency, etc., under contract with the management agency, etc.

- Even after IP rights transfer, etc., due to mergers, etc., the management agency, etc., may be able to possess a license for the IP rights, including the right for sub-licensing. Unless this condition is accepted, the transfer will not be permitted.

(7) Handling of intellectual property rights at the time of termination

- As for IP rights, etc., that no one wishes to possess when the research and development is terminated, the relevant intellectual property committee will discuss responses (abandonment or succession by the management agency, etc.).

(8) Participation by overseas organizations, etc. (such as foreign companies, universities, and researchers)

- If participation by an overseas organization, etc., is necessary for promotion of tasks, such participation will be permitted.
- In principle, from the perspective of appropriate executive management, only an overseas organization, etc., with a point of contact or an agent in Japan that can process paperwork related to acceptance of the research and development will be permitted to participate in the Project.
- In the case of an overseas organization, etc., IP rights will be shared by the management agency, etc., and the overseas organization, etc.

5. Matters related to assessment

(1) Assessing entities

Based on the self-inspection reports by PD and NEDO, the Governing Board will perform assessments by inviting external experts. The Governing Board may perform assessments separately for each area or issue.

(2) Timing of assessments

- Pre-assessments, assessments at the end of every fiscal year, and final assessments will be performed.
- After a lapse of a certain period after the termination (three years in principle), tracking assessments may be performed, if necessary.
- In addition to the above, assessments may be performed in the middle of a fiscal year, if necessary.

(3) Assessment items, and assessment standards

With the "General Guideline for the Evaluation of Government Research and Development (R&D) Activities" (established by the Prime Minister on December 21, 2016) taken into consideration, from the perspective of assessment of necessity, efficiency, and effectiveness, the assessment items and the assessment standards will be as follows. Assessments will not only determine whether or not the goals are attained, but also analyze the cause and factors of such (non-)attainment, and improvement measures will be proposed.

(1) The importance, and consistency with the purpose of the SIP system.

(2) The appropriateness of the goals (especially the technology outcomes), and the degree of achievement of the process table towards attainment of the goals.

(3) Whether or not proper management is being made. Particularly, how effective the coordination is with government ministries and agencies.

(4) The strategic relevance to, and degree of achievement of, practical use and commercialization.

(5) Expected outcomes, output, or ripple effects in the final assessment. Whether or not follow-up methods after the termination are appropriately and clearly specified.

(4) Methods for reflecting assessment outcomes

- Pre-assessments will be performed in connection with the Plan for the following fiscal year and thereafter, and will be reflected in the Plan, for the following fiscal year and thereafter.
- Assessments at the end of a fiscal year will be performed in connection with actual achievements up to the fiscal year and the Plan for the following fiscal year and thereafter, and will be reflected in the Plan, for the following fiscal year and thereafter.

- Final assessments will be performed in connection with actual outcomes up to the final fiscal year, and will be reflected in the follow-up, after termination.
- Tracking assessments will be performed in connection with the progress of practical use and commercialization of the outcomes of each task, and improvement measures will be proposed.

(5) Disclosure of outcomes

- In principle, assessment outcomes will be made available to the public.
- The Governing Board that performs assessments will be privately held, because it may include undisclosed research and development information.

(6) Self-inspection

(i) Self-inspection by research managers

Research managers will, in connection with the research theme that they are in charge of, inspect both the actual outcomes after the previous assessment, and the future plan according to the assessment items and assessment standards listed in 5(3), and will summarize not only determination of whether or not the goal was attained, but also analysis of the cause and factors of such (non-)attainment, and improvement measures will be proposed.

(ii) Self-inspection by PD

While seeing results of the self-inspection by research managers, and referring to the opinions of third parties and experts as necessary, PD will personally inspect the actual results of the PD, NEDO, and each research manager and the future plan, according to the assessment items and assessment standards listed in 5(3), and will summarize not only determination of whether or not the goal was attained, but also analysis of the cause and factors of such (non-)attainment, and improvement measures will be proposed. Based on the results of such an inspection, PD will determine whether or not each research entity should continue their research, and provide necessary advice to research managers. In this way, a structure will be established which can autonomously improve itself.

On the basis of these results, PD will prepare materials for the Governing Board, with the support of NEDO.

(iii) Self-inspection by the management agency

Self-inspection by NEDO will be performed only in connection with the proper processing of paperwork procedures related to budget execution.

6. Exit strategy

(1) Exit-oriented research promotion

To achieve social implementation of the research themes, it will be necessary not only to disseminate technologies demonstrated in each theme to private corporations, but also to build a structure designed to construct, verify, and maintain trustworthy chains in entire supply chains.

As for confirmation of whether each component of a supply chain truly satisfies security requirements or not (confirmation of trustworthiness), the content and standard of security requirements that are required differ according to industrial areas, and confirmation should be based on knowledge within each industry. Therefore, for example, industry groups and incorporated administrative agencies are expected to take the initiative in establishing the confirmation structure.

In addition, in order to build and manage a list or database for storing originals of certified trustworthiness information and making them available to inquiries by third parties, not only industry groups and incorporated administrative agencies, but also existing credit information databases that handle cross-industry information of companies may be utilized.

As for information on vulnerability, incidents and threats, to be utilized for maintenance of trustworthy chains, the examination will be continued on the assumption that coordination between the existing information sharing frameworks and public organizations is in place.

By around 2020, experimental demonstrations will be sequentially started, each one being on getting prepared for implementation, with the goal of social implementation of the "Cyber Physical Security Infrastructure" in IoT systems/services or supply chains, in experimental demonstration partner environments such as manufacturing/distribution sectors and building sectors, and other efforts will be made to apply or expand the *Infrastructure* to social infrastructure industries that possess large-scale supply chains.

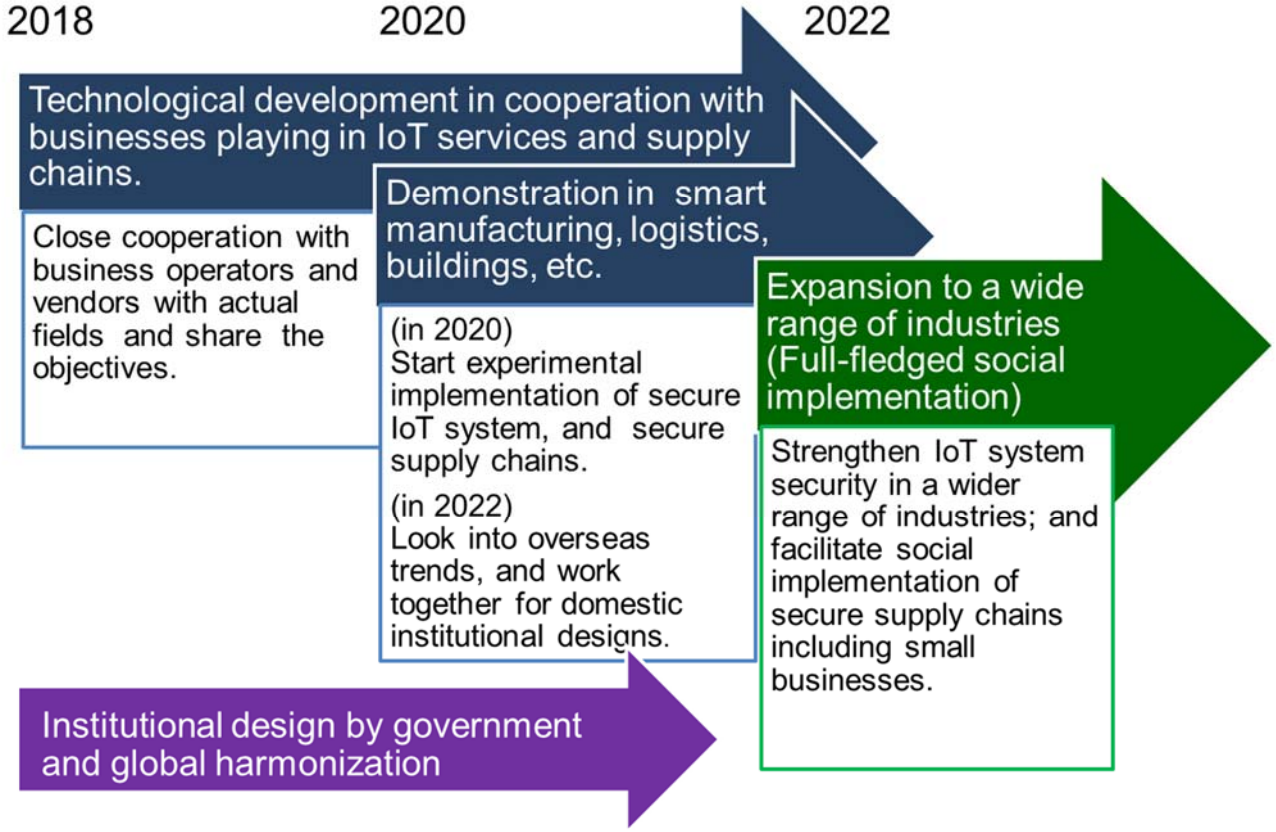

Figure 6-1. Project time Line for Social Implementation

By 2022, when this Project will terminate, for the industrial sectors where the demonstration experiments have been conducted, consideration of the structures of an organization for making confirmation, an organization for constructing and managing trustworthiness lists, and an organization for managing information on vulnerability, incidents and threats, etc., all based on outcomes of the experimental demonstrations, will be completed, and a structure capable of achieving assurance of security for entire supply chains will be established.

While this Project will work on experimental demonstrations in addition to technology developments, the participating companies will play a central role in commercializing outcomes of the research and development, and in promoting adoption thereof in various industrial areas. Some outcomes will be registered as IP (intellectual property rights), and licensed to related vendors for the purpose of dissemination.

Introduction of the *Infrastructure* into entire supply chains (including SMEs) and IoT systems/services of their constituent companies will be promoted, so that the outcomes of the *Infrastructure* may be adopted by 50% of the SMEs for which measures for supply chains are required prior to 2030.

(2) Measures for dissemination

Efforts will be made to disseminate the *Infrastructure*, which is the outcome of the research and development of security policies and trustworthy chains required in each area, that have been established with international trends taken into consideration, in areas such as automotive, smart buildings, communication and broadcasting, power supplies, public transportation, and defense, while demonstrating application of the *Infrastructure* in each of said areas. As a measure for promoting adoption of the *Infrastructure*, the national or local governments or IoT service providers will be encouraged to utilize the *Infrastructure* to confirm trustworthiness, and both suppliers and purchasers of IoT devices and services will be made aware of the benefits of the *Infrastructure*. As a means for raising such awareness, situations of efforts on their way to final achievement will be published at various events (such as presentations at symposiums, seminars and business events, and international conferences) to make them better understood by people engaged in IoT services in industry sectors both within and outside of Japan. Such events will also be utilized as opportunities for coordination to develop into efforts for international solutions, and as a result, the outcomes of the R&D efforts in Japan may lead to international contribution.

In addition, the *Infrastructure* will coordinate certification of IoT devices and assurance of security for IoT devices, which are being considered in the IoT Security WG established by the Ministry of Internal Affairs and Communications, the Ministry of Economy, Trade and Industry, and the IoT Promotion Consortium. This will contribute to establishing a system as effective as the status of the cybersecurity frameworks in the U.S. and Europe.

o Scenario of regulatory and institutional reforms

Efforts for early social implementation will be made through repetition of the demonstration of technologies that have been researched and developed, and the feedback thereof, and utilization of the *Infrastructure* by entire supply chains including SMEs will be promoted, so that products, services, and systems made in Japan that have high security quality may be disseminated.

For this reason, efforts will be made to contribute to establishment of security policies, certification of IoT devices, and measures for assuring security for IoT devices, which are required in various sectors such as automotive, smart homes and buildings, communication and broadcasting, power supplies, public transportation, and defense (Industry by Industry), in collaboration with the Three Major Government Measures mentioned above, with international trends taken into consideration.

o Scenario of international cooperation

As cyberattacks cross borders, taking only in-country measures may not be effective enough. In addition, in regards to overseas deployment of the IoT devices and services of Japan, it is

important to share policies with the U.S. and European countries, and efforts should be made, including enhanced collaboration with other countries, with international harmonization always taken into consideration.

Specifically, international symposiums will be utilized, in cooperation with various ministries and agencies, where opinions will be proactively exchanged with experts from various regions of the world, in an effort to make the activities of Japan/this Project understood, to understand activities in other regions, and compare them with those of Japan, so that international exchange may be promoted. In particular, it will be verified that the activities and outcomes of this Project are compatible with the trend of the cybersecurity framework accelerated in the U.S. and European countries (see below), and the research and development will be promoted, while ensuring that international competitiveness may be assured.

- U.S. NIST SP800-171: Standards for cybersecurity measures to control "Controlled Unclassified Information (CUI)". Compliance with NIST SP800-171 had already been required by supply chains for defense procurement (DFARS Clause 252.204-7012).
- European cybersecurity authentication framework: Development of the framework was announced in the policy package published in September 2017.

o Coordination amongst issues of SIP, or with other national projects

Mutual collaboration on core technologies will be formed with the fundamental technical issues in the 2nd term of SIP (cyberspace and physical space). In addition, mutual collaboration on joint implementation of experimental demonstrations will be formed with the applied issues of the Society 5.0 system (autonomous driving, logistics, etc.).

Through these efforts, the security quality in autonomous driving, smart buildings, 5G communication services, and defense industries, which are expected to lead to further economic development by Society 5.0, will be assured, thereby enhancing international competitiveness.

7. Other important matters

(1) Legal basis

This Project will be implemented in accordance with "3. Basic policy concerning the expense for creation and maintenance of science, technology and innovation" (May 23, 2014, Council for Science, Technology and Innovation) of Article 4, Paragraph 3, Item 7 of the Act for Establishment of the Cabinet Office (Act No.89 of 1999), the implementation policy for the 2nd term (funded by the supplementary budget for FY2017) of the Cross-Ministerial Strategic Innovation Promotion Program (SIP) (March 29, 2018, Council for Science, Technology and Innovation), the operational guideline for the Cross-Ministerial Strategic Innovation Promotion Program (May 23, 2014, Governing Board of Council for Science, Technology and Innovation) and Article 15, Item 2 of the Act on the New Energy and Industrial Technology Development Organization.

(2) Flexible changes of the project

This Project may be revised according to circumstances, from the perspective of the most early and maximal outcomes.

(3) History of PD and personnel responsible

(i) PD

Atsuhiro GOTO (since April 2018)

(ii) Sub PD

Makoto IMASE(since April 2019)
Kazuhisa URYU(since April 2019)

(iii) Responsible councilor (or director)

Takao NITTA, Councilor (since April 2018)
Reiko KONDO, Councilor (since July 2018)

Chie FUKUSHIMA, Director (April-July, 2018)

(iv) Personnel responsible

Akihiro OKAZAKI (since April 2018)

Appendix　Financial planning and accumulation

Fiscal year 2018　Total 2,500 million yen

(Accounting breakdown)

1. R & D budget[16]	2,350 million yen
(A) "Creation & Confirmation of Trustworthiness" technology	850 million yen
(B) "Construction & Distribution of Trustworthy Chain" technology	750 million yen
(C) "Verification & Maintenance of Trustworthy Chain" technology	670 million yen
(D) Surveys of trends related to the "Cyber Physical Security Infrastructure"	80 million yen
2. Project promotion expenses[17]	150 million yen

Fiscal year 2019　Total 2,200 million yen

(Accounting breakdown)

1. R & D budget	2,050 million yen
(A) "Creation & Confirmation of Trustworthiness" technology	750 million yen
(B) "Construction & Distribution of Trustworthy Chain" technology	600 million yen
(C) "Verification & Maintenance of Trustworthy Chain" technology	700 million yen
2. Project promotion expenses	150 million yen

[16] Include general and administrative expenses and overhead expenses
[17] Include personnel expenses, evaluation expenses, conference expenses, etc.