Section 5 Trends in Cybersecurity Policy

1. Summary

(1) Initiatives so far

Under intensifying threats to cybersecurity on a worldwide scale, the Basic Act on Cybersecurity (Act No. 104 of 2014) stipulating basic principles of national cybersecurity policy was enacted in 2014. Based on the act, the Cybersecurity Strategic Headquarters was established under the Cabinet in 2015 to lead cybersecurity measures of the government. Since then, a Cybersecurity Strategy has been formulated every three years setting goals and policies of measures considering changes in economic society and the increase in threats against cybersecurity. In September 2021, a new "Cybersecurity Strategy"[23] was decided by the Cabinet and cybersecurity policies have been promoted based on the strategy.

"The 4th Action Plan on Information Security of Critical Infrastructure"[24] (decided by the Cybersecurity Strategic Headquarters in April 2017) establishing basic framework for protection of critical infrastructure designates the information and communication sector (telecommunication, broadcasting and cable television) as one of the 14 critical infrastructure sectors, suspension or unavailability of which would heavily affect people's lives and socioeconomic activities. The next action plan is scheduled to include clarification of the responsibilities of related entities and enhancement of the troubleshooting system. Holding jurisdiction over critical infrastructure, MIC needs to take measures to secure safety and reliability of the information and communication networks.

MIC has held a Cyber Security Task Force consisting of security experts since 2017. The task force has successively compiled a list of challenges and measures to be tackled by MIC with consideration to various changes in the situation, including Tokyo Olympic and Paralympic games and the COVID-19 pandemic. In July 2021, the task force formulated the "Comprehensive ICT Cybersecurity Measures 2021"[25], which includes measures regarding ICT infrastructure/services. Based on the above, MIC has been implementing measures to promote cybersecurity in the ICT sector.

(2) Future challenges and direction

When movement of persons is restricted to prevent the spread of COVID-19 and use of telework is progressing, promotion of digitalization of overall socioeconomic activities by the people, or promotion of digital transformation across society is recognized as an increasingly important policy issue.

ICT infrastructure and services including IoT and 5G provide the basis for digital transformation. In order to promote digital reform and transformation across society, it is a critical prerequisite to ensure cybersecurity so that each citizen can use ICT safely.

As described in Chapter 3 Section 7, a large number of cyber-attack-related communications are still observed. Because the ratio of the attacks targeting IoT equipment remains the highest, it is necessary to continue to strengthen security measures for IoT equipment.

For introduction of telework and wireless LAN which are necessary for digitalization across society, ensuring security and dealing with anxiety concerning security remain the largest and urgent issues.

Domestic security business models are mostly based on introduction and operation of overseas security products. As a result, domestic security companies cannot collect domestic cyberattack information, etc., and conduct R&D based on real data to develop domestic security technologies, which leads to the failure of such domestic technologies to spread. In order to avoid or grow out of the excessive dependence on security technologies provided by overseas players, and to enhance the ability to independently handle cyber-attacks including development of the cybersecurity human resources, it is necessary to create an ecosystem that will accelerate domestic generation of cybersecurity information and human resource development.

2. Securing safety and reliability of information and communications networks

(1) Initiatives pertaining to IoT

While IoT is progressing as social infrastructure, IoT devices are often exposed to cyber-attacks because it is difficult to manage them completely, and appropriate security measures cannot be taken due to their limited performance and other reasons. The need to strengthen the countermeasures has been pointed out. Cyber-attacks abusing IoT devices are actually made and the ratio of the attacks targeting IoT equipment is the highest among the cyber-attack-related communications observed in 2021 by the Network Incident Analysis Center for Tactical Emergency Response (NICTER) operated by NICT.

Under these circumstances, in order to strengthen cybersecurity measures for IoT devices, the Act on the National Institute of Information and Communications Technology, Independent Administrative Agency[26] was partially amended in 2018. Based on the amendment, MIC and NICT in collaboration with internet service providers (ISPs) have been implementing an initiative named "National Operation Towards IoT Clean Environ-

[23] Cybersecurity Strategy: https://www.nisc.go.jp/active/kihon/pdf/cs-senryaku2021.pdf
[24] The 4th Action Plan on Information Security of Critical Infrastructure (revised): https://www.nisc.go.jp/active/infra/pdf/infra_rt4_r2.pdf
[25] Comprehensive ICT Cybersecurity Measures 2021: https://www.soumu.go.jp/main_content/000761893.pdf
[26] Act on the National Institute of Information and Communications Technology, Independent Administrative Agency (Act No. 162 of 1999)

ment (NOTICE)" since February 2019. NOTICE is a series of projects: (1) NICT identifies devices on the internet, which can be abused for cyber-attacks by entering a password that can be easily derived such as "password" or "123456"; (2) NICT notifies the information of the identified devices to the relevant ISP, and (3) the notified ISP identifies the users of the devices and alerts them.

Concurrently with NOTICE, MIC, NICT, ICT-ISAC and ISPs cooperate to implement a project where ISPs alert the users of IoT device already infected with malware. In this project, devices performing communications caused by malware infection are detected based on the information obtained through NICTER above, and the ISPs identify the users of the devices.

(2) Initiatives related to active measures taken by telecommunications carriers

With the progress of 5G, it is expected that use of IoT devices will further expand in various industries. In order to improve the effectiveness of security measures for IoT devices, it seems necessary to improve the environment for more flexible responses on the network side where traffic is passing in addition to the existing measures on the terminal side.[27]

In this context, in November 2021 MIC at "the Study Group for Proper Dealing with Telecommunications Business Cyber-attacks" found that it is possible for telecommunication carriers to detect C&C servers (servers giving directions to terminals infected with malware) by collecting, accumulating and analyzing flow of information at normal times and share the information on the detected C&C servers under certain conditions considering secrecy of communication.[28] The study group plans to start validity verification of the technology to detect C&C servers by telecommunication carriers through analyzing flow of information and a demonstration project to sort out operational challenges for sharing among carriers in fiscal 2022.

Certified Association against Cyber Attacks on Telecommunications Facilities[29] is a third party organization to conduct operations including sharing, survey and research of senders' information of DDoS and other cyber-attacks. In the past, information sharing and analysis at the association was limited to cases where the senders are identified after attacks. In order to allow information sharing and analysis before attack, a bill for partial amendment of the Telecommunications Business Act was submitted to the Diet in March 2022 and enacted in June of the same year, as an effort to promote collaboration among telecommunication carriers in handling DDoS and other cyber-attacks.

3. Initiatives related to Telework Security

Security was the biggest challenge in a questionnaire survey of enterprises introducing telework.[30] In order to dispel anxiety about security so that enterprises can implement telework with security, MIC has formulated a "telework security guideline"[31] since 2004. The COVID-19 pandemic triggered drastic changes in the environment surrounding telework and there are also changes in security trends, which include progress in use of the cloud and sophistication of cyber-attacks. In response, MIC made a total revision of the security measures to be implemented, specific trouble cases and other matters in May 2021.

Some SMEs may not have dedicated security staff, or their persons in charge may not understand technical schemes. In response, MIC formulated "Telework Security Guide for SMEs (Checklists)" focusing on reliable securing of minimum security and revised the guide along with the guidelines in May 2021.

4. Initiatives related to Trust Services

In Society5.0, integration of real space and cyberspace will further progress and every activity in the real space will be placed in cyberspace. In this process, construction of infrastructure for data distribution with confidence is essential, and trust services (**Figure 4-5-4-1**) that are a system to prevent data falsification and sender masquerade are increasingly important.

(1) Study by the Working Group on Trust Services

MIC set up "Working Group on Trust Services" under the "Study Group on Platform Services" in January 2019. The working group studied the ideal state of trust services in Japan and presented the following directions for time-stamp and e-seal initiatives in its final report in February 2020.

Regarding time-stamps certifying that electric data existed at a certain time and has not been altered after that time, a private authorization system has been operated. However, without state support for its reliability, there is a concern about international applicability. Therefore, it is appropriate for the state to establish a system to authorize reliable time-stamp services and business operators.

Regarding e-seal that enables simple confirmation of

[27] "Comprehensive ICT Cybersecurity Measures 2021" formulated in 2021 states: "it is necessary to consider measures to realize advanced and flexible responses in information and communication networks managed by ISP on the internet" in the section of "Active measures by telecommunication carriers against cyber-attacks" (https://www.soumu.go.jp/menu_news/s-news/02cyber01_04000001_00192.html)
[28] The Fourth Report of the Study Group for Proper Dealing with Telecommunications Business Cyber-attacks: https://www.soumu.go.jp/main_content/000779208.pdf
[29] Based on Article 116-2 (1) of the Telecommunications Business Act, ICT-ISAC was certified as a Certified Association against Cyber Attacks on Telecommunications Facilities in January 2019.
[30] Survey on actual conditions of telework security (2nd survey in fiscal 2020): https://www.soumu.go.jp/main_sosiki/cybersecurity/telework/
[31] Ensuring security in telework: https://www.soumu.go.jp/main_sosiki/cybersecurity/telework/

the organization sending electronic data, this is a new service and its content and technologies for its provision have not been established. Therefore, it is appropriate to formulate technical and operational guidelines for reliable services and business operators with involvement of the state, and establish a private authorization system based on the guidelines.

(2) Establishment of time-stamp authorization system by the state

Based on the recommendations of the working group, the "Study Group on the Time Stamp Certification System" conducted further study, and MIC established a state certification system by instituting the Provisions Concerning Approval of Time-stamp Authentication Operations (Ministry of Internal Affairs and Communications Notice No. 146 of 2021) in April 2021. Further through the tax reform in fiscal 2022, time-stamps based on a private certification system (Japan Data Communications Association) are replaced by time-stamps based on the state certification system in scanner archiving of taxation-related documents and other systems.[32] In the future, MIC will operate the state certification system appropriately and reliably, while taking necessary measures for further expansion of the use of time-stamps.

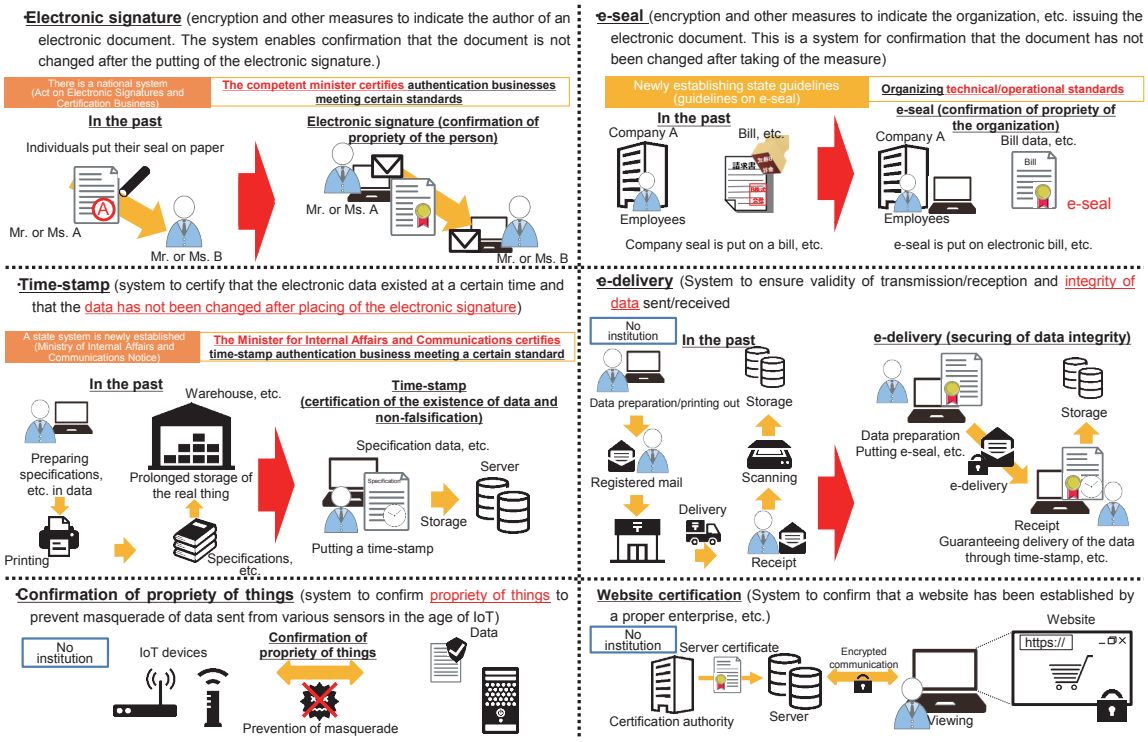
(3) Formulation of the guidelines on e-seals

Based on the recommendations of the working group, the "Study Meeting on a System for Ensuring the Reliability of Data Issued by Organizations" set up in April 2020 studied the ideal e-seals in Japan. Later in June 2021, MIC released a report of the study meeting and formulated "Guidelines on e-seal"[33] compiling technical/operational standards required from reliable e-seal services/business operators in Japan.

(4) Study at the Digital Agency

It was found effective that the Digital Agency would handle dissemination of electronic signatures and system planning integrally based on the Act on Electronic Signatures and Certification Business (Act No. 102 of 2000[34]). As a result, affairs regarding this Act were relegated from MIC and METI to the Digital Agency[35], and the Agency is leading efforts to expand use of electronic signature and improvement of its convenience. At the whole government level, under the Data Strategy Promotion Working Group based on the Digital Society Promotion Council Order (Cabinet Order No.193 of 2021), the Sub-working Group for Trust-Assured Digital Transformation was established to study digitalization needs and the necessary assurance level of various procedures and transactions in the public and private sectors in November 2021. The sub working group discusses the framework of trust services based on the MIC's initiatives regarding time-stamps and e-seal.

Figure 4-5-4-1 Image of trust service



[32] For the period from April 1, 2022 to July 29, 2023, a transitional measure is taken to allow use of time-stamps pertaining to operations authorized by Japan Data Communications Association as before.
[33] Guidelines on e-seal (https://www.soumu.go.jp/main_content/000756907.pdf)
[34] Report of the Working Group on Digital Reform Related Bills Task Force: (https://www.kantei.go.jp/jp/singi/it2/dgov/houan_wg/dai4/siryou2.pdf)
[35] Provisions regarding legal effects of electronic signature (e.g., presumption of authentic establishment of private documents) remain under the jurisdiction of the Ministry of Justice.

5. Initiatives related to wireless LAN security

Wireless LAN is widely used in homes, workplaces and while on the go through a public wireless LAN service, for example. However, without an appropriate security measure, there is a danger of cyber attacks and information theft through wireless LAN devices. To address this issue, MIC has formulated guidelines on wireless LAN security measures separately for users and providers and released revised versions of them both adapted to new technologies and the latest security trends in May 2020.[36]

"Simplified manual for Wi-Fi users" for wireless LAN users presents three points of security measures: (1) carefully check the access point to connect; (2) check whether right URL is used for HTTPS communication; and (3) check the setting of the device installed in the home, which are followed by commentary on each point.

"Guide on security measures for Wi-Fi providers" for wireless LAN providers is compiled to help a broad range of people including restaurants and retail stores providing wireless LAN service to check what security risks are involved in the provision and what security measures to take.

6. Initiatives related to ensuring safety of cloud services

(1) Assessment of safety of cloud services for government information systems

Under "Principle of the Cloud-by-Default", the government at the "Study Group on Safety Evaluation of Cloud Services" studied safety assessment of cloud services. As a result, (1) the basic framework for a system, (2) the approach to cloud usage in each government ministry and agency, and (3) jurisdiction and operation of the system have been determined as per "The Basic Framework for the Security Evaluation System of Cloud Services in the Government Information System" (established by the Cyber Security Strategy Headquarters, January 30, 2020).

In response, based on the rules decided by the ISMAP Management Committee consisting of experts and competent authorities (National center of Incident readiness and Strategy for Cybersecurity, Digital Agency, MIC and METI), the Information system Security Management and Assessment Program (ISMAP) system was established in June 2020. Registration of cloud services that are confirmed to be implementing security measures specified in the system started in March 2021. As of June 1, 2022, 34 services are open to the public in the ISMAP Cloud Service List[37].

(2) Formulation of guidelines on information security measures in cloud service provision

In order to promote safe and secure use of cloud services, MIC formulates "guidelines on information security measures in cloud service provision" compiling information security measures to be taken by cloud service providers. In September 2021, MIC released a revised edition (the 3rd edition) based on the actual state of cloud service provision and use.[38] Recently, there are cases where failure of cloud service users to use the service appropriately resulted in risk of information leak. To address this issue, a broad range of entities including providers and users are studying means for promotion of appropriate use of cloud services and plan to formulate and release guidelines for appropriate settings for cloud service provision and use.

7. Initiatives for development of security human resources

While cyber-attacks are increasingly sophisticated and complicated, Japan is short of cyber-security human resources both in quality and quantity. To address this issue, MIC with the National Cyber Training Center of NICT is actively promoting training of cybersecurity human resources (CYDER and SecHack365).

(1) Cyber Defense Exercise with Recurrence (CYDER)

CYDER is a practical cyber defense exercise for persons in charge of information systems at various organizations including state organs, local governments, independent administrative agencies and critical infrastructure operators. Teams of trainees participate in the exercise and experience actual machine operation for a series of actions from detection of incidents caused by cyber-attacks, response, reporting and restoration in a large-scale virtual LAN environment simulating the network environment of their organization. Since fiscal 2017, 13,867 trainees in total have taken the course. Since fiscal 2021, in addition to the existing basic and intermediate-level exercise courses, CYDER includes: upper-intermediate courses to learn more advanced security skills taking advantage of the knowledge of Cyber Colosseo[39] and an online exercise course for people who cannot take CYDER due to geographical/time constraints or other reasons to learn minimum handling.

---

[36] For safe use of wireless LAN: https://www.soumu.go.jp/main_sosiki/cybersecurity/wi-fi/
[37] ISMAP Cloud Service List: https://www.ismap.go.jp/csm?id=cloud_service_list
[38] Guidelines on information security measures in cloud service provision (the 3rd edition): https://www.soumu.go.jp/main_content/000771515.pdf
[39] Cyber Colosseo: practical cyber exercise program that was held prior to the Tokyo Olympic and Paralympic Games for persons in charge of security at organizations related to the games. Colosseo consisted of: Colosseo Exercise to learn methods to deal with attacks through offence and defense exercise using real machines, where cyber-attacks were simulated in a virtual network environment faithfully reproducing the systems involved in the games, and: Colosseo College to learn security knowledge and skills through lectures and seminars. Colosseo was held in close cooperation with The Tokyo Organizing Committee of the Olympic and Paralympic Games for the period from fiscal 2017 to 2020. 571 enrollees were trained through the Exercise and 1,717 enrollees in College in total.

(2) Program for cultivating young security innovators (SecHack365)

SecHack365 is a program for ICT talents age 25 or younger and living in Japan to become cutting-edge security innovators who can create new security technologies. Front-line researchers and engineers teach research and development of security technologies by using NICT's actual cyber-attack-related data continuously and at full scale for one year. 41 enrollees completed the course in fiscal 2021, 212 in total since fiscal 2017.

8. Constructing the integrated cybersecurity knowledge/human resource development foundation (CYNEX)

Because domestic security business models are mostly based on introduction and operation of overseas security products, security measures in Japan heavily depend on overseas products and information, which leads to insufficient collection and analysis of cyberattack information, etc. in Japan. In addition, through use of overseas security products, domestic data flows to overseas businesses, the security-related information of Japan is analyzed overseas, and domestic businesses purchase threat information based on the analytical results from foreign businesses.

As a result, domestic security businesses cannot accumulate core knowhow and knowledge, and it is difficult for them to contribute to global information sharing or to train engineers who can work internationally. User companies also have a shortage of personnel who can appropriately handle security products and information. In order to enhance Japan's independent skills to cope with cyber-attacks, which include training of cyber-security talents, it is necessary to build an ecosystem that accelerates domestic generation of cybersecurity information and human resource development in Japan.

In collaboration with NICT implementing Japan's top-level R&D on cybersecurity, MIC has built a cutting-edge "integrated cybersecurity knowledge/human resource development platform (popularly named CYNEX)," a huge industry-academia-government node regarding cybersecurity around the technologies/knowhow of NICT, since 2021 and started trial operation in 2022.

This cutting-edge platform enables collection and analysis of a broad range of cyber security information in Japan, and further promotes development of domestic security products taking advantage of such information, while at the same time training highly skilled security personnel and supporting human resource development in private and educational institutions. Through this project, MIC aims to further reinforce cybersecurity measures in Japan.

9. Promoting formulation of security communities rooted in the area (regional SECUNITY)

In order to ensure safety and reliability of information and communication services/networks in Japan, it is an important issue to secure cybersecurity not only at business operators providing national or metropolitan-area services but also at business operators providing information communication services in local areas. However, local enterprises and governments have challenges including: information gap compared with enterprises running business in Tokyo metropolitan area or nationwide; difficulty of taking sufficient security measures independently due to lack of management resources, or failure to recognize the need for security measures.

MIC established regional SECUNITY - communities that have built "mutual help" relationships regarding security among involved parties - in 11 regions (mostly districts of Regional Bureaus of Communications) by fiscal 2021. In fiscal 2022, MIC continues support by holding events and other initiatives in addition to seminars to deploy activities across regions and expand awareness-raising activities to a wide range of people.

10. Initiatives related to international cooperation

Because cyberspace spreads globally, collaboration with other countries is essential for establishment of cybersecurity. For this purpose, MIC actively engages in discussions, disseminating and collecting information at various international conferences and cyber consultations with the aim of contributing to building international consensus on cybersecurity.

Furthermore, in order to promote information sharing on international cybersecurity among private entities including information communication operators, MIC holds workshops with participation of ISP of ASEAN countries as well as Japan-US and Japan-EU opinion exchange sessions at the Information Sharing and Analysis Center (ISAC).

In ASEAN region, the ASEAN Japan Cybersecurity Capacity Building Center (AJCCBC) is leading initiatives to improve cybersecurity skills in the region.[40] At the same time, MIC regularly holds ASEAN-Japan Cyber Security Workshop for ISP businesses of ASEAN countries in order to promote information sharing and to build and enhance collaboration systems.

[40] See Chapter 4 Section 8