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 Japanese cybersecurity policy was enacted in 2014. Based on the act, the Cybersecurity Strategic Headquarters was established under the Cabinet in 2015 to lead the cybersecurity measures of the government. Since then, a "Cybersecurity Strategy" has been formulated every three years to set goals and policies of measures considering changes in economic society and the increase in threats against cybersecurity. In September 2021, a new "Cybersecurity Strategy[1]" was decided by the Cabinet. The government has continued to promote cybersecurity policies based on this.

The "Action Plan on Information Security of Critical Infrastructure[2]" (decided by the Cybersecurity Strategic Headquarters in June 2022) established a basic framework for the protection of critical infrastructure and designates the information and communications field (telecommunications, broadcasting, and cable television) as one of the 14 critical infrastructure fields, suspension or unavailability of which would heavily affect people's lives and socioeconomic activities. As a government agency responsible for critical infrastructure, MIC must continue to promote efforts to ensure the safety and reliability of information and communications networks.

MIC has held meetings of the "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 the Tokyo Olympic and Paralympic games and the COVID-19 pandemic. In August 2022, it formulated "Comprehensive ICT Cybersecurity Measures 2022[3]," which includes measures to ensure the safety and reliability of information and communications networks and improve the ability to handle cyberattacks autonomously. In order to respond to situations where many cyberattacks target IoT devices, the "Subcommittee on Cybersecurity Measures in Information and Communications Networks" has been held under the task force since January 2023 to consider comprehensive measures required from both the terminal side (IoT devices) and the network side, based on the current status of efforts and issues. Based on this, various measures are now being taken to promote cybersecurity measures in the ICT field.

(2) Future challenges and directions

As the movement of people has been restricted to prevent the spread of COVID-19 and the use of remote work has progressed, the switching of all socioeconomic activities to digital (the promotion of digital transformation [DX] of society as a whole) is now recognized as an even more important policy issue.

In recent years, cyberspace has become a battleground between countries, reflecting the harsh security environment and geopolitical tensions. There have been many cyberattacks targeting government agencies and critical infrastructures. Amid widespread and rapid progress in the conversion of the economy and society to digital, an increase in cyberattacks including the disruption of information and communications networks and the leakage of information could cause serious damage to people's lives and to Japan's economic and social activities. In December 2022, Japan's National Security Strategy was revised to include the introduction of "active cyber defenses" to improve response capabilities in the cybersecurity field, marking a turning point in Japan's cybersecurity policy.

As cyberspace increasingly becomes a public space, information and communications technology (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.

Therefore, it is necessary to ensure the safety and reliability of information and communications networks, improve the ability to handle cyberattacks autonomously, promote international cooperation, and promote public awareness, as described below.

[1] Cybersecurity Strategy: https://www.nisc.go.jp/active/kihon/pdf/cs-senryaku2021.pdf
[2] Action Plan on Information Security of Critical Infrastructure: https://www.nisc.go.jp/pdf/policy/infra/cip_policy_2022.pdf
[3] Comprehensive ICT Cybersecurity Measures 2022: https://www.soumu.go.jp/main_content/000829941.pdf

2. Efforts to ensure safety and reliability of information and communications networks

(1) Initiatives related to IoT security

As IoT advances and various things supporting social and economic activities are connected to the Internet, IoT devices are often exposed to the threat of cyberattacks because they are difficult to manage, the performance of the devices is limited, and appropriate security measures cannot be taken. This calls for stronger countermeasures. In addition to cyberattacks that actually exploit IoT devices, communications related to cyberattacks observed by the NICTER cyberattack observation network operated by NICT in 2022 showed that IoT devices (especially DVR/NVR) were still the most frequently targeted.

Under these circumstances and in order to strengthen cybersecurity measures for IoT devices, the Act on the National Institute of Information and Communications Technology[4] was partially amended in 2018. Based on the amendment, MIC and NICT in collaboration with Internet service providers (ISPs) have been implementing the "National Operation Towards IoT Clean Environment (NOTICE)" initiative since February 2019. Under the current initiative, (1) NICT identifies IoT devices on the internet, which can be abused for cyberattacks by entering a password that can be easily derived such as "password" or "123456," (2) NICT sends information about 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 have been cooperating since June 2019 to implement a project where ISPs alert the users of IoT devices already infected with malware. In this project, devices performing communications caused by malware infection are detected by NICT based on the information obtained through NICTER above, and the ISPs identify the users of the devices.

In light of the fact that NOTICE efforts will end in March 2024, the Subcommittee on Cybersecurity Measures in Information and Communications Networks is now organizing the current status and issues with NOTICE and is examining the direction of NOTICE in the future. This includes enhancing observation capabilities and promoting effective countermeasures against the threat of cyberattacks that exploit IoT devices.

Figure (related data) Overview of NOTICE and NICTER alerts
URL: https://www.soumu.go.jp/johotsusintokei/whitepaper/eng/WP2023/data_collection.html#f00360
(Data collection)

(2) Initiatives related to active security measures by telecom carriers

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

Cyberattacks and other threats are becoming increasingly large, detailed, and complicated. In response, MIC has been taking measures so that telecom carriers can efficiently and actively deal with these threats, since fiscal 2022. In fiscal 2023, MIC will continue such efforts as (1) demonstrating C&C cyber detection technology, (2) demonstrating detection technologies and sharing methods for phishing sites and other malicious websites, and (3) demonstrating ways of introducing network security measures. MIC will also promote the sharing and use of detection information to improve the accuracy of C&C servers working with telecom carriers based on the discussions of the Subcommittee on Cybersecurity Measures in Information and Communications Networks, including visualizing IoT botnets.

The "Certified Association against Cyber Attacks on Telecommunications Facilities[6]" is a third party organization that shares information between ISPs and conducts research studies of sender information during DDoS and other cyberattacks, among other duties. 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 for signs of activity prior to attacks (port scanning), the Act Partially Amending the Telecommunications Business Act was enacted in June 2022 as an effort to promote collaboration among telecom operators handling DDoS and other cyberattacks.[7]

[4] Act on the National Institute of Information and Communications Technology (Act No. 162 of 1999)
[5] "Comprehensive ICT Cybersecurity Measures 2021" (formulated in 2021) states that "it is necessary to consider measures to realize advanced and flexible responses in information and communications networks managed by ISPs on the internet" through "implementing active measures by telecom operators against cyberattacks." (https://www.soumu.go.jp/menu_news/s-news/02cyber01_04000001_00192.html)
[6] 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.
[7] The Act Partially Amending the Telecommunications Business Act (Act No. 70 of 2022) came into effect on June 16, 2023.

(3) Initiatives related to supply chain risk policies

From fiscal 2019 to fiscal 2021, MIC conducted research and examination on ensuring the security of 5G networks. MIC organized a list of security issues and their countermeasures that operators should keep in mind by conducting technical verifications that take the entire 5G network into account (including virtualization infrastructures and management systems), and released some of the results in "5G Security Guidelines (First Edition)[8]" in April 2022. These guidelines were adopted as a new work item in ITU-T SG17 in September 2022, and MIC is currently promoting efforts toward international standardization in cooperation with specialized agencies.

In the communications field, the configuration of systems is becoming more complex as the functions required for systems become more sophisticated and diverse, and various commercial software products and open source software (OSS)[9] solutions are now being used as software components. These changes in software supply chains have resulted in cyberattacks that insert malicious code in software components or target vulnerabilities in software components. However, if the configuration of software components in a system is not understood, it becomes difficult to respond quickly to attacks.

In response, MIC has been conducting demonstration projects to introduce SBOM[10] in the communications field since fiscal 2023, in order to contribute to the enhancement of cybersecurity by gaining a clear understanding of software supply chains using SBOM.

Although smartphones are now widely used, there are only limited methods for checking the actual conditions of smartphone applications when there is a concern that they may be transmitting user information against the user's wishes. Since fiscal 2023, MIC has been conducting a demonstration project to gain a clear understanding of the actual conditions of application behavior through having third parties conduct technical analysis of applications.

(4) Initiatives related to trust services

Real space and cyberspace are highly integrated in Society 5.0, so exchanges conducted in physical spaces must also be able to be smoothly conducted in cyber space. In order to accomplish this, it is necessary to build infrastructures to safely and reliably distribute data. Trust services (**Figure 5-5-2-1**) are becoming increasingly important as systems to prevent data falsification and sender impersonation.

At the whole government level, the "Sub-working Group for Trust-Assured Digital Transformation" was established in November 2021 under the "Data Strategy Promotion Working Group" based on the Digital Society Promotion Council Order (Cabinet Order No. 193 of 2021), in order to study needs and the necessary assurance level of various procedures and transactions in the public and private sectors. The sub-working group published the "Report of the Sub-working Group for Trust-Assured Digital Transformation[11]" in July 2022.

Based on the final report[12] of the "Working Group on Trust Services" released in February 2020, MIC has been studying the development of necessary systems and guidelines for time-stamps and e-seals.

a Development of a national time-stamp authorization system

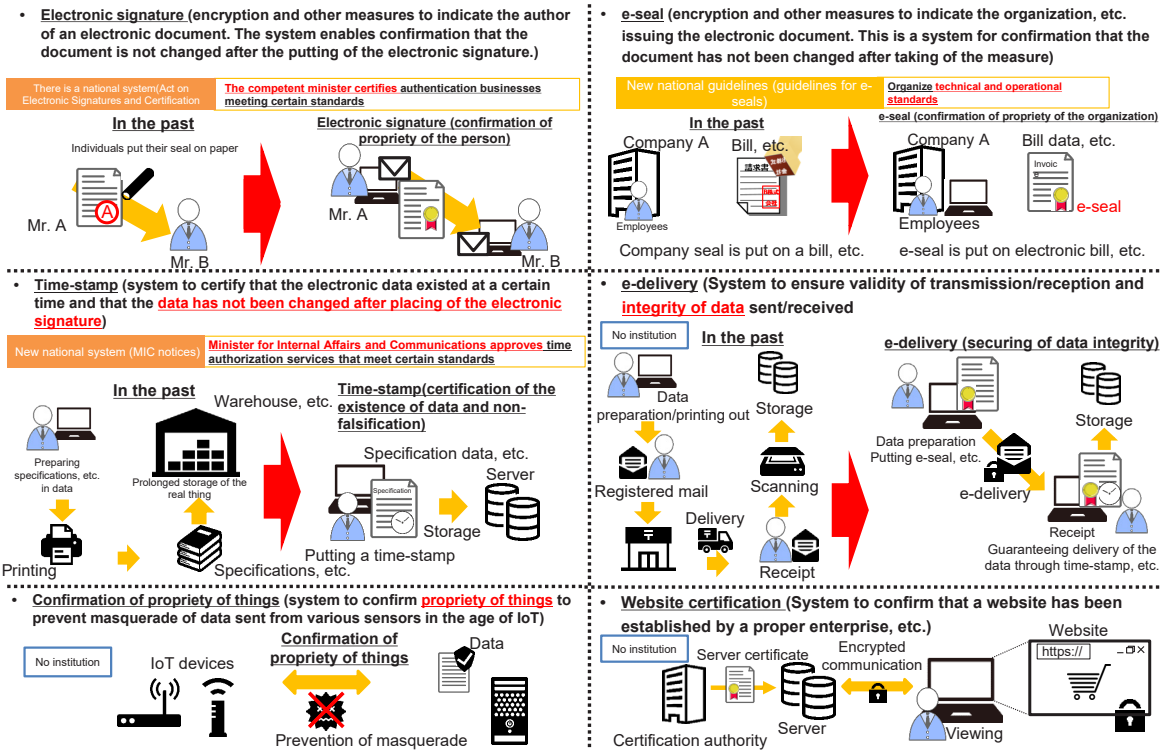
The "Study Group on the Time-Stamp Authorization System" established in March 2020 further reviewed time-stamps, and in April 2021 MIC established Rules Concerning Authorization of Time-Stamp Operations (MIC Notice No. 146 of 2021). The Japanese government (Minister for Internal Affairs and Communications) then established an authorization system. Due to the revision of the tax system in fiscal 2022, time-stamps based on the national authorization system will be adopted instead of time-stamps based on a private authorization system (Japan Data Communications Association), with regard to the digital data retention system for tax-related documents.[13] In February 2023, the Japanese government certified the time authorization service for the first time. MIC will continue to operate the state authorization system appropriately and reliably, while taking necessary measures to further expand the use of time-stamps.

b Formulation of "guidelines on e-seals"

The "Study Meeting on a System for Ensuring the Reliability of Data Issued by Organizations" established in April 2020 studied how ideal e-seals should be implemented in Japan. In June 2021, MIC released a report of the review committee and formulated "Guidelines on e-seals[14]" compiling technical/ operational standards required from reliable e-seal services and business operators in Japan.

[8] 5G Security Guidelines (First Edition): https://www.soumu.go.jp/main_content/000812253.pdf
[9] Software whose source code is freely available for anyone to use, improve, or redistribute.
[10] Software Bill of Materials.
[11] Report of the Sub-working Group for Trust-Assured Digital Transformation (https://www.digital.go.jp/councils/trust-dx-sub-wg/)
[12] Final Report of the Working Group on Trust Services https://www.soumu.go.jp/main_content/000668595.pdf
[13] A transitional measure was taken from April 1, 2022 to July 29, 2023 to allow the use of time-stamps pertaining to operations authorized by Japan Data Communications Association as before.
[14] Guidelines on e-seals (https://www.soumu.go.jp/main_content/000756907.pdf)

Figure 5-5-2-1 Trust services



(5) Initiatives related to ensuring the safety of cloud services

a Assessment of cloud service safety for government information systems

Under "Principle of the Cloud-by-Default," the government had the "Study Group on Safety Evaluation of Cloud Services" meeting to study the issue of safety assessment of cloud services. As a result, (1) the basic framework for a system, (2) the approach to cloud usage in government agencies, and (3) the 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 Cybersecurity Strategic Headquarters, January 30, 2020).

In response to the basic framework, the Information System Security Management and Assessment Program (ISMAP) was launched in June 2020 based on various rules and regulations decided by the ISMAP Management Committee, which consists of experts and government agencies with jurisdiction over the system (National Center of Incident Readiness and Strategy for Cybersecurity, Digital Agency, MIC, and METI). Cloud services that have been confirmed to have implemented security measures based on the standards set by this system began being registered in March 2021. As of May 11, 2023, a total of 44 services have been published on the ISMAP Cloud Service List.[15]

In November 2022, ISMAP for Low-Impact Use (ISMAP-LIU) was launched as a mechanism for SaaS solutions that deal mainly with confidentiality class 2 information and that are used for processing operations and information that pose a small security risk. ISMAP-LIU is designed to be looser than the current ISMAP for overall auditing of SaaS services that have very limited use or functionality, or that deal only with relatively unimportant information. It will work together with ISMAP to further expand cloud-by-default.

b Formulation of guidelines on cloud security

In order to promote the safe and secure use of cloud services, MIC formulates "Guidelines on Information Security Measures in Cloud Service Provision" summarizing information on 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. There have been recent cases where cloud service users failing to use services appropriately have resulted in the risk of information leaks. To address this issue, a broad range of entities including providers and users studied means for promoting the appropriate use of cloud services, and then formulated and released "Guidelines for Appropriate Settings for Cloud Service Usage and Provision" in October 2022.

[15] ISMAP Cloud Service List: https://www.ismap.go.jp/csm?id=cloud_service_list

3. Improvement of ability to handle cyberattacks autonomously

(1) Initiatives for the development of security personnel

While cyberattacks are becoming increasingly sophisticated and complicated, Japan is short of cybersecurity personnel both in quality and quantity. The development of human resources is an urgent issue. To address this issue, MIC is working with the NICT "National Cyber Training Center" on several initiatives (CYDER, CIDLE, and SecHack365) to actively promote the development of cybersecurity personnel.

a Practical cyber defense exercises for persons in charge of information systems (CYDER)

CYDER is a set of practical cyber defense exercises 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 exercises and experience actual machine operation for a series of actions from detection of incidents caused by cyberattacks, response, reporting, and restoration in a large-scale virtual LAN environment simulating the network environment of their organization (**Figure 5-5-3-1**).

In fiscal 2022, in addition to the conventional group exercise courses and online standard courses for beginners, intermediates, and semi-advanced students, a new online introductory course where students can learn the basics of incident response. In addition, the "Onsite CYDER" program was implemented, in which NICT travels to local governments to resolve issues with insufficient training due to geographical and temporal factors, and the "CYDER Satellite" program was implemented to improve the efficiency of instructors and staff by holding simultaneous meetings at multiple venues (**Figure 5-5-3-2**).

In total, more than 17,000 people have participated in CYDER group exercises since fiscal 2017.

Figure 5-5-3-1 Practical cyber defense exercises (CYDER: CYber Defense Exercise with Recurrence)

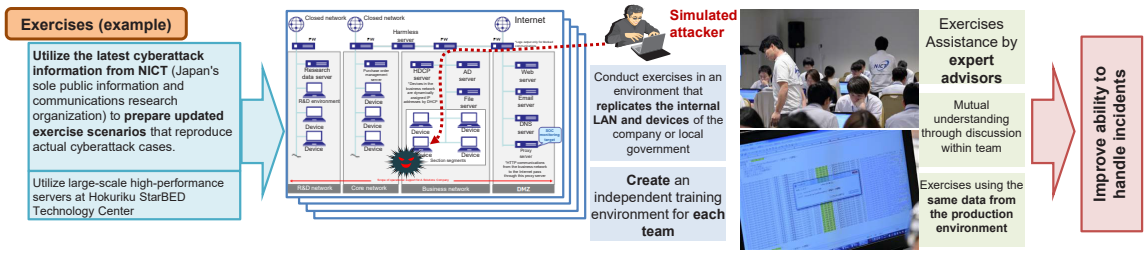


Figure 5-5-3-2 CYDER in fiscal 2022

Course	Type of exercise	Level	Intended audience (topics covered)	Intended organizations	Location	Frequency	Period
A	Group exercises	Beginner	Individuals just beginning to work with systems (Procedure for responding to incidents)	All organizations	All prefectures, etc. *On-site and satellite lessons are also being tried	72 times	From July, to Feb. of the following year
B-1		Intermediat	System administrators and operators (Autonomous incident response and security management)	Local governments	11 regions nationwide	20 times	From Oct., to Jan. of the following year
B-2				Organizations other than local governments	Tokyo, Osaka, Nagoya, Tsukuba	13 times	Jan. to Feb. of the following year
C		Semi-advanced	Security specialists (Advanced security technology)	All organizations	Tokyo	3 times	From Oct., to Feb. of the following year
Online Standard	Online exercises	Equivalent to beginner	Individuals just beginning to work with systems (Procedure for responding to incidents)	All organizations	(Participant workplaces, etc.)	As needed	5/24 to 7/19
Online Introduction		Introduction					1/17 to 2/24 of the following year

b Expo cyber defense training course (CIDLE)

CIDLE is a cyber defense training course for persons in charge of information systems of the Japan Association for the 2025 World Exposition, with the goal of ensuring a perfect security system for the 2025 World Exposition in Osaka. Leveraging what was learned during the Tokyo 2020 Olympic and Paralympic Games, a lecture and exercise program is scheduled to be offered during fiscal 2023.

c Training program for young security personnel (SecHack365)

A program for cultivating young security innovators, SecHack365 is for ICT personnel age 25 or younger and living in Japan to become cutting-edge security personnel (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 cyberattack-related data continuously and at full scale for one year. 40 enrollees completed the course in fiscal 2022, for a total of 252 since fiscal 2017.

(2) Establishment of an integrated cybersecurity knowledge/human resource development platform (CYNEX)

Domestic security business models are mostly based on the introduction and operation of overseas security products, and so cybersecurity measures in Japan heavily depend on overseas products and information, which leads to insufficient collection and analysis of cyberattack information and other data in Japan. In addition, through use of overseas security products, domestic data flows to overseas businesses, 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 cyberattacks, which include training of cybersecurity personnel, it is necessary to build an ecosystem that accelerates domestic generation of cybersecurity information and human resource development in Japan.

In collaboration with NICT, which conducts top-level research and development on cybersecurity in Japan, MIC began trial operation of the "integrated cybersecurity knowledge/human resource development platform" (commonly known as CYNEX) in fiscal 2022. CYNEX is an advanced platform that serves as a huge nexus for industry, academia, and government on cybersecurity, with the technology and knowledge cultivated by NICT at its core. In fiscal 2023, full-scale operation of information analysis, product verification, and human resource development projects is scheduled to start, while cooperation with universities and private companies is expanded.

Figure (related data) Integrated cybersecurity knowledge/human resource development platform (CYNEX)
URL: https://www.soumu.go.jp/johotsusintokei/whitepaper/eng/WP2023/data_collection.html#f00379
(Data collection)

Beginning in fiscal 2023, the introduction of domestic security software is planned for some ministries as one part of CYXROSS, a demonstration project for the collection and analysis of cybersecurity information using government device information. The strengthening of security measures in Japan is also planned by aggregating and analyzing obtained malware information in NICT's CYNEX.

Figure (related data): Demonstration project for the collection and analysis of cybersecurity information using government device information (CYXROSS)
URL: https://www.soumu.go.jp/johotsusintokei/whitepaper/eng/WP2023/data_collection.html#f00380
(Data collection)

This cutting-edge platform enables collection and analysis of a broad range of cybersecurity 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.

4. Promotion of international cooperation

Cyberspace spreads globally, and so collaboration with other countries is essential for establishing cybersecurity. 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.

Efforts to assist developing countries in building capacity in the field of cybersecurity are also important in order to reduce cybersecurity risks worldwide. MIC has been promoting human resource development projects in the ASEAN region through the ASEAN-Japan Cybersecurity Capacity Building Centre (AJCCBC), and has been engaged in efforts to contribute to the improvement of cybersecurity capabilities, particularly in the ASEAN region.[16]

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

5. Promotion of awareness raising

(1) Initiatives related to remote work security

Security was noted as the biggest challenge in a questionnaire survey[17] of enterprises introducing remote work. In order to dispel anxiety about security so that enterprises can implement remote work with security, MIC has been formulating and sharing "Telework Security Guidelines" since 2004.

The COVID-19 pandemic triggered drastic changes in the environment surrounding remote work and there are also changes in security trends, which include progress in use of the cloud and sophistication of cyberattacks. In response, MIC made a total guidelines revision of the security measures to be implemented, specific trouble cases, and other matters in May 2021.

At the same time, it is assumed that there may not be a dedicated person in charge of security or that the person in charge does not understand the specialized systems at small-to-medium-sized enterprises and other organizations. With this in mind, MIC formulated the "Telework Security Guide for SMEs (Checklists)" focusing on ensuring a minimum level of security. In May 2022, MIC revised the design and wording with universal design in mind to improve readability, and also prepared a new "Employee Handbook" as an appendix full of information that employees can actually use.

(2) Promotion of formulation of security communities rooted in the area (regional SECUNITY)

In order to ensure the safety and reliability of information and communications services and networks in Japan, it is necessary to ensure 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 local governments are facing various challenges, including information gaps on cybersecurity compared with enterprises running business in the Tokyo metropolitan area or nationwide, difficulties taking sufficient security measures independently due to lack of management resources, and failures 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 telecommunications) by fiscal 2022. In fiscal 2023, MIC will continue to support large-scale cross-regional events and the expansion of efforts to promote awareness among a wide range of people.[18]

Figure (related data) Regional security communities
URL: https://www.soumu.go.jp/johotsusintokei/whitepaper/eng/WP2023/data_collection.html#f00381
(Data collection)

[16] Refer to Chapter 5, Section 8 "Promotion of International Strategies for ICT" for more information on the efforts of the ASEAN-Japan Cybersecurity Capacity Building Centre.
[17] Survey on actual conditions of remote work security: https://www.soumu.go.jp/main_sosiki/cybersecurity/telework/
[18] Details on the latest events can be found at the following URL
https://www.soumu.go.jp/main_sosiki/cybersecurity/localsecunity/index.html

(3) Appropriate promotion of sharing and disclosure of information related to cyberattacks

As the threat of cyber attacks increases, it is beneficial for both the affected organization and society as a whole to share and disclose information related to cyberattacks with cybersecurity related organizations, in order to clarify the full extent of attacks and strengthen countermeasures. However, there are many cases where the affected organization is cautious about sharing and disclosing information due to concerns about its reputation.

In April 2022, the "Study Group on Sharing and Disclosing Information on Cyberattacks" was formed under the management committee of the "Cybersecurity Council," a consultative body consisting of a wide variety of public and private organizations. The study group discussed guidance on sharing and disclosing information on cyberattacks that would serve as a practical reference for organizations affected by cyberattacks. Following public comments, a document was compiled and published by the study group in March 2023.[19]

Relevant ministries and agencies will continue to work together to disseminate and raise awareness of this information, and will continue to consider whether to revise this information based on feedback from organizations affected by cyberattacks.

(4) Initiatives related to wireless LAN security

In addition to in homes and at workplaces, wireless LAN is now widely used while on the go through public wireless LAN services. However, without appropriate security measures, there is a danger of cyberattacks and information theft through wireless LAN devices. To address this issue, MIC has formulated separate guidelines on wireless LAN security measures for users and providers, and released revised versions of these documents adapted to new technologies and the latest security trends in May 2020.

The "Simplified Manual for Wi-Fi Users" is aimed at wireless LAN users, and presents three security measures to keep in mind: (1) carefully check access point to connect, (2) check whether the right URL is being used for HTTPS communication, and (3) check the settings of devices installed in the home. An explanation is provided for each of these points.

The "Guide on Security Measures for Wi-Fi Providers" is aimed at wireless LAN providers, and was compiled to help a broad range of people including restaurants and retail stores providing wireless LAN service to check what security risks are involved and what security measures to take.

In order to raise awareness about security measures for wireless LAN, a free online course is held every fiscal year in conjunction with Cyber Security Month (Feb. 1 to March 18) to provide information on the latest security measures for wireless LAN.[20] During fiscal 2022, an online course called "Learn About Wi-Fi Security Measures" was held from March 1, 2023 to March 26 of the same year.

[19] Guidance on sharing and disclosing information on cyberattacks that would serve as a practical reference for organizations affected by cyberattacks (formulated on March 8, 2023): https://www.soumu.go.jp/menu_news/s-news/01cyber01_02000001_00160.html

[20] Online course on security measures for wireless LAN (Wi-Fi): https://www.soumu.go.jp/main_sosiki/cybersecurity/wi-fi/index.html