Section 5 Trends in cybersecurity policy

1. Summary

(1) Initiatives so far

In response to the increasing global threat of cybersecurity, the Basic Act on Cybersecurity (Act No. 104 of 2014), which outlines the fundamental principles of Japan's cybersecurity policy, was enacted. Consequently, in 2015, the Cybersecurity Strategic Headquarters was established under the Cabinet. Since then, taking into account changes in the economic and social landscape as well as the growing cybersecurity threats, the "Cybersecurity Strategy[1]," which sets forth the goals and implementation policies of various measures, has been revised every three years. Currently, cybersecurity policies are being promoted based on the "Cybersecurity Strategy" approved by the Cabinet in September 2021.

Additionally, the "Cybersecurity Policy for Critical Infrastructure Protection[2]" (approved by the Cybersecurity Strategic Headquarters in June 2022 and revised in March 2024), which outlines the basic framework for protecting critical infrastructure, designates the information and communication sector (telecommunications, broadcasting, and cable television) as one of the 15 critical infrastructure sectors. This designation is due to the significant impact on national life and socio-economic activities if these functions are halted or become unavailable. As one of the ministries responsible for critical infrastructure, the MIC is required to continue promoting efforts to ensure the safety and reliability of information and communication networks.

Furthermore, the National Security Strategy, approved by the Cabinet in December 2022, emphasizes the need to "enhance the response capabilities in the field of cyber security to a level comparable to or exceeding that of major Western countries to ensure the safety of the nation and critical infrastructure." The government is collectively advancing discussions to realize the initiatives based on this strategy.

Since 2017, the MIC has convened the "Cyber Security Task Force," composed of experts in the security field. This task force has periodically compiled issues and measures that the MIC should address, considering various changes in circumstances, the Tokyo Olympic and Paralympic Games, and responses to the COVID-19 pandemic. Most recently, to address the frequent cyberattacks targeting IoT devices, the "Subcommittee on Cybersecurity Measures in Information and Communication Networks" was held under the task force starting in January 2023. Based on these discussions, the "Comprehensive ICT Cybersecurity Measures 2023[3]," which includes measures to ensure the safety and reliability of information and communication networks and to enhance autonomous response capabilities to cyberattacks, such as a comprehensive measures to deal with IoT botnets, was formulated in August 2023. Moreover, anticipating significant changes in the cybersecurity environment due to the rapid spread of new technologies and services such as generative AI and the increasing diversity and complexity of supply chains, the "ICT Cybersecurity Policy Subcommittee" has been convened since February 2024. This subcommittee is examining the direction of cybersecurity policies that the MIC should pursue in the medium to long term.

(2) Future challenges and directions

With the promotion of DX across society, cyberspace has become a part of everyday life for everyone. However, the risks surrounding cyberspace have evolved with the times and environment, as evidenced by the increasing reports of phishing scams and ransomware attacks.

In recent years, cyberspace has become a battleground for international conflicts, reflecting severe security environments and geopolitical tensions. Many countries have experienced cyberattacks targeting government agencies and critical infrastructure. Japan has also faced serious cyber incidents targeting ports, medical institutions, and government agencies. Moreover, while new technologies such as generative AI have increased convenience, they have also raised concerns about the expansion of risks due to their misuse.

As cyberspace becomes a public space, it is increasingly important to ensure cybersecurity so that every citizen can safely utilize ICT (Information and Communication Technology), including IoT and 5G, which form the foundation of this space.

In light of these considerations, it is necessary to ensure the safety and reliability of information and communication networks, enhance autonomous response capabilities to cyberattacks, promote international cooperation, and advance public awareness and education, as outlined below.

[1] Cybersecurity Strategy: https://www.nisc.go.jp/active/kihon/pdf/cs-senryaku2021.pdf
[2] The Cybersecurity Policy for Critical Infrastructure Protection: https://www.nisc.go.jp/pdf/policy/infra/cip_policy_2024.pdf
[3] Comprehensive ICT Cybersecurity Measures 2023: https://www.soumu.go.jp/main_content/000895981.pdf

2. Ensuring safety and reliability of information and communications networks

(1) Promotion of comprehensive IoT botnet countermeasures

In order to ensure the safety and reliability of the information and communication networks that support the cyber space, concerns are also raised about the impact of large-scale cyberattacks that disrupt the functionality of the information and communication networks, such as DDoS attacks. In the case of a typical large-scale cyberattack like a DDoS attack, there are two stages: (1) the expansion of the attack infrastructure by infecting a large number of IoT devices with malware (expansion of the attack infrastructure); and (2) the execution of attacks through the network using this attack infrastructure. In fact, with the increase in the number and functionality of IoT devices, cyberattacks exploiting IoT devices have been on the rise, and the NICTER, which is the cyberattack observation network operated by NICT, observed that attacks targeting IoT devices (especially DVR/NVR) remained the most common type of cyberattacks in the cyberattack-related communications observed in 2023.

To address these large-scale cyberattacks, it is necessary to promote comprehensive IoT botnet countermeasures from both the terminal side (IoT devices) to prevent the expansion of the attack infrastructure, and the network side to deal with the Command and Control (C&C) servers that issue instructions to the attack infrastructure.

On the terminal side, the MIC and the NICT have been implementing an initiative called "NOTICE (National Operation Towards IoT Clean Environment)" in collaboration with Internet Service Providers (ISPs) since February 2019. Under this initiative, based on the Act on the National Institute of Information and Communications Technology (hereinafter referred as to "NICT Act"), the NICT has been conducting investigations into IoT devices on the Internet that have easily guessable passwords such as "password" or "123456," as well as devices conducting communications due to malware infections, and has been promoting measures such as alerting device users to prevent these devices from being exploited for cyberattacks, achieving certain results.

However, the risk of cyberattacks exploiting IoT devices remains high, with an increase in cyberattacks targeting vulnerabilities in IoT device software. In response to this, in the 212th session of the National Diet in 2023, a revision of the NICT Act was carried out to continue the investigation of IoT devices with vulnerabilities in ID and password settings beyond FY2024, and to expand the scope of investigation to include IoT devices with software vulnerabilities or those already infected with malware. In addition to alerting IoT device administrators, efforts are being made to promote security measures for IoT devices in collaboration with manufacturers and system vendors, as well as to raise awareness of IoT device security measures through video distribution and online advertising.

On the network side, since FY2022, telecommunications service providers have been analyzing flow information related to communication traffic (IP addresses, port numbers, timestamps, etc.) to verify the effectiveness of technology for detecting Command and Control (C&C) servers that are the source of cyberattacks, as well as to study the sharing and utilization of information about detected C&C servers among operators. The effectiveness of flow information analysis has been confirmed, with successful detection of a certain number of C&C servers, and efforts will continue in FY2024 to further improve detection accuracy through the expansion of telecommunications service providers conducting flow information analysis and the active analysis of detected C&C servers.

Figure (related data) Awareness raising of IoT security countermeasures with the use of video distribution
URL: https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r06/html/datashu.html#f00399
(Data collection)

(2) Promotion of proactive cybersecurity measures by telecommunications operators

To make the security measures for IoT devices more effective, it is considered necessary to establish an environment that allows for more agile responses on the network side, where communication traffic passes through, in addition to the comprehensive IoT botnet measures mentioned earlier[4].

In FY2023, following FY2022, comprehensive demonstrations of cybersecurity measures were conducted to enable telecommunications operators to respond more efficiently and proactively to increasingly large-scale, sophisticated, and complex cyberattacks. In the "Demonstration of Detection Technologies and Sharing Methods for Malicious Websites such as Phishing Sites," a phishing response practical reference for web service providers was created, and awareness-raising activities for the general public were carried out. In the "Demonstration of Network Security Measures," guidelines for the introduction and operation of network security tech-

[4] "Comprehensive ICT Cybersecurity Measures 2021" (formulated in 2021) stated 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

nologies such as RPKI[5], DNSSEC[6], and DMARC[7], which are being implemented internationally but have not yet been widely adopted in Japan, were drafted based on the knowledge gained through technical demonstrations[8]. Efforts to promote their widespread adoption will continue in FY2024.

(3) Initiatives for supply chain risk measures

The MIC conducted technical verifications considering the entire 5G network, including virtualization infrastructure and management systems, from FY2019 to FY2021. In April 2022, the "5G Security Guidelines Version 1[9]" was published, summarizing the security issues and countermeasures that operators should be aware of. These guidelines were approved as a new work item for standardization at ITU-T SG17 in September 2022, and efforts are currently underway to promote international standardization in collaboration with specialized agencies.

In the field of communications, the system configurations are becoming more complex due to the increasing sophistication and diversification of required functions. Various commercial software and open-source software (OSS)[10] are being used as software components. With these changes in the software supply chain, cyberattacks targeting vulnerabilities in software components or the insertion of malicious code into software components have occurred. However, if the composition of software components within a system is not understood, it becomes difficult to respond quickly to attacks.

In light of this situation, the MIC has been conducting demonstration projects to introduce SBOM[11] in telecom sector since FY2023 to strengthen cybersecurity by understanding the software supply chain using SBOM.

Furthermore, from FY2023, considering the widespread use of smartphones and the limited methods available to verify whether smartphone apps are transmitting user information against the user's intent when concerned, demonstration projects are being conducted to understand the actual behavior of apps through technical analysis by third parties.

(4) Initiatives to ensure the safety of cloud services

A Evaluation of the safety of cloud services in government information systems

Under the principle of cloud by default, the government deliberated on the evaluation of the safety of cloud services in the "Study Group on the Safety Evaluation of Cloud Services" and established the "Basic Framework for the Security Evaluation System for Cloud Services in Government Information Systems" (the Cybersecurity Strategic Headquarters Decision of January 30, 2020). This decision included the basic framework of the system, the approach to usage by each government agency, and the administrative and operational structure.

Based on the basic framework, various regulations were determined by the ISMAP Operating Committee, consisting of experts and the ministries and agencies responsible for the system (the NISC, the Digital Agency, the MIC, and the METI), and the "Information system Security Management and Assessment Program (ISMAP)" was launched. From March 2021, the registration of cloud services that have been confirmed to have implemented security measures based on the criteria set by this system began, and as of May 1, 2024, a total of 68 services have been published as the ISMAP cloud service list[12].

In November 2022, the operation of "ISMAP for Low-Impact Use (ISMAP-LIU)" began, which is a system for SaaS that handles mainly confidential level 2 information and is used for processing tasks and information with low security risks. ISMAP-LIU is designed to be more lenient than the current ISMAP in terms of the overall audit for services that are extremely limited in their usage and functionality or handle relatively low-importance information.

Furthermore, with the maintenance of the reliability and stability of ISMAP as a premise, efforts to rationalize and clarify the system operation have been ongoing through the "ISMAP System Improvement Initiatives" since October 2022. As part of this, a full-scale operation of the improved framework, which includes "reducing the burden of external audits" and "streamlining and enhancing the efficiency of reviews", began in October 2023. Going forward, the promotion of further expansion of cloud by default will be pursued through system improvement initiatives and other efforts.

---

[5] Resource Public-Key Infrastructure (RPKI). A technology that verifies the IP addresses and AS numbers of autonomous networks using digital certificates, preventing issues such as route hijacking.
[6] DNS Security Extensions (DNSSEC): A technology that verifies the association between domain names and IP addresses using digital certificates to prevent server impersonation and other related threats.
[7] Domain-based Message Authentication, Reporting & Conformance (DMARC): A technology that verifies the authenticity of the sender's domain in emails and automatically handles cases of impersonation and other similar threats.
[8] The 5th ICT Cybersecurity Policy Subcommittee Reference Materials 2-4 include: (1) Guidelines for Countermeasures against Illegitimate Routes on the Internet Using RPKI's ROA; (2) Guidelines for DNS Response Authentication Technology Using DNSSEC; and (3) Guidelines for Email Spoofing Countermeasures and Anti-Spam Technologies, including DMARC (including SPF and DKIM) Email Authentication Technology. https://www.soumu.go.jp/main_sosiki/kenkyu/cybersecurity_taskforce/02cyber01_04000001_00286.html
[9] 5G Security Guidelines Version 1: https://www.soumu.go.jp/main_content/000812253.pdf
[10] Software whose source code is freely available to the public, allowing anyone to use, modify, and redistribute it.
[11] Software Bill of Materials
[12] ISMAP Cloud Service List: https://www.ismap.go.jp/csm?id=cloud_service_list

B Development of guidelines for cloud security

The MIC has formulated the "Guidelines for Information Security Measures in Cloud Service Provision" as part of its efforts to promote the use of safe and secure cloud services. In September 2021, a revised version (3rd edition) was published, taking into account the actual provision and usage of cloud services. Moreover, due to cases where inappropriate use of cloud services by users has led to potential information leaks, a guideline for promotion of appropriate configuration in cloud service usage was formulated in October 2022 with the examination by wide range of stakeholders such as providers and users. In April 2024, a "Cloud Misconfiguration Prevention Guidebook" was published to provide a clear explanation of the content of the guidelines for cloud service users.

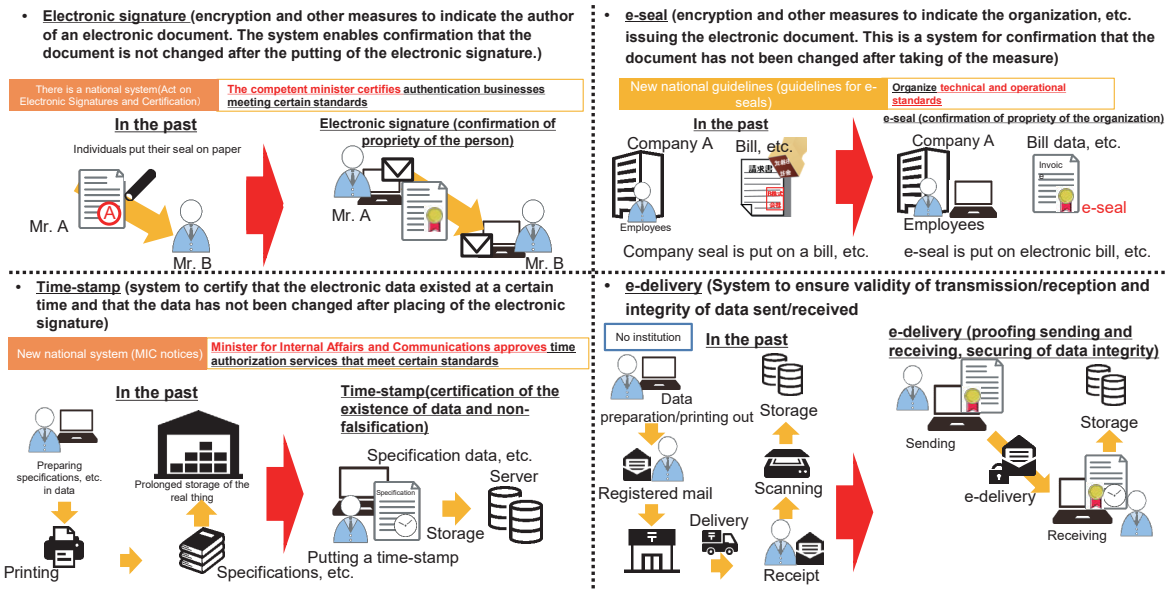
(5) Initiatives related to trust services

In Society 5.0, where the physical and cyber spaces are highly integrated, it is essential to seamlessly facilitate various interactions in the cyber space as well. To achieve this, it is crucial to establish a foundation that allows data to circulate safely and securely. The importance of trust services, which are mechanisms to prevent data tampering and spoofing of the sender **(Figure 2-2-5-1)**, is increasing.

As a government-wide effort, 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). This sub-working group examines the digitalization needs and required assurance levels for various public and private procedures and transactions. In July 2022, the "Report of the Sub-working Group for Trust-Assured Digital Transformation[13]" was published.

The MIC is advancing discussions on the appropriate operation of the electronic time stamps certification system and the establishment of standards and conformity assessments to evaluate the reliability of private electronic seals (e-Seals) services, based on the "Priority Plan for Realization of a Digital Society" (Cabinet decision on June 9, 2023)[14].

Figure 2-2-5-1 Image of trust service



A Establishment of a national certification system on electronic time stamps

Regarding time stamps, further discussions were held in the "Study Meeting on the Time Stamp Certification System," which was launched in March 2020. In April 2021, the "Rules Concerning the Certification of Time-stamping Services (MIC Notice No. 146 of 2021)" were established, creating a certification system by the national government (Minister of Internal Affairs and Communications). Additionally, due to the tax reform in FY2022, the electronic time stamps based on the national certification system was positioned to replace the electronic time stamps based on the certification system by the private sector (Japan Data Communications Association) for the scanner storage system related to tax documents. In February 2023, the first national certification for time authentication services was granted. Moving forward, the national certification system will continue to be operated appropriately and reliably, and necessary efforts will be made to further expand the use of electronic time stamps.

[13] Report of the Sub-working Group for Trust-Assured Digital Transformation: https://www.digital.go.jp/councils/trust-dx-sub-wg/
[14] Priority Plan for Realization of a Digital Society: https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/5ecac8cc-50f1-4168-b989-2bcaabffe870/b24ac613/20230609_policies_priority_outline_05.pdf

B Initiatives for institutionalizing e-Seals

Regarding e-Seals, the "Study Meeting on a System for Ensuring the Reliability of Data Issued by Organizations" was launched in April 2020 to discuss the ideal state of e-Seals in Japan. In June 2021, the "Guidelines on e-Seals" were formulated, indicating certain standards for the technology and operation of e-Seals in Japan. Furthermore, in September 2023, the "Study Group on e-Seals" was established to discuss the establishment of standards and conformity assessments to evaluate the reliability of private e-Seals services. In April 2024, the final report of the study group[15] and the "Guidelines on e-Seals (2nd Edition) [16]" were published. Based on these study results, efforts will be made to start the operation of a national certification system for e-Seals.

3. Improvement of ability to handle cyberattacks autonomously

(1) Initiatives for developing security personnel

As cyberattacks become more sophisticated and complex, Japan faces a significant shortage of cybersecurity personnel both in terms of quality and quantity. Addressing this issue is an urgent priority. To this end, the MIC is actively promoting initiatives for cybersecurity personnel development through the National Cyber Training Center of the NICT, including programs such as CYDER, CIDLE, and SecHack365.

A Practical cyber defense exercises for information system personnel (CYDER)

CYDER is a practical cyber defense exercise targeting information system personnel from national agencies, local governments, independent administrative agencies, and critical infrastructure operators. Participants join the exercise in teams and experience a series of responses to cyberattacks, from detection to response, reporting, and recovery, in a large-scale virtual LAN environment that simulates an organization's network environment **(Figure 2-2-5-2)**. In FY2023, in addition to the existing beginner, intermediate, and pre-advanced group exercise courses and the online introductory course, a trial implementation of "Pre-CYDER" was conducted, which allows participants to learn the basics of cyberattack mechanisms, trends, and incident handling **(Figure 2-2-5-3)**.

The number of participants in CYDER group exercises in FY2023 was 3,742, bringing the total number of participants since FY2017 to over 20,000.

Figure 2-2-5-2: Practical cyber defense exercises (CYDER Cyber Defense Exercise with Recurrence)

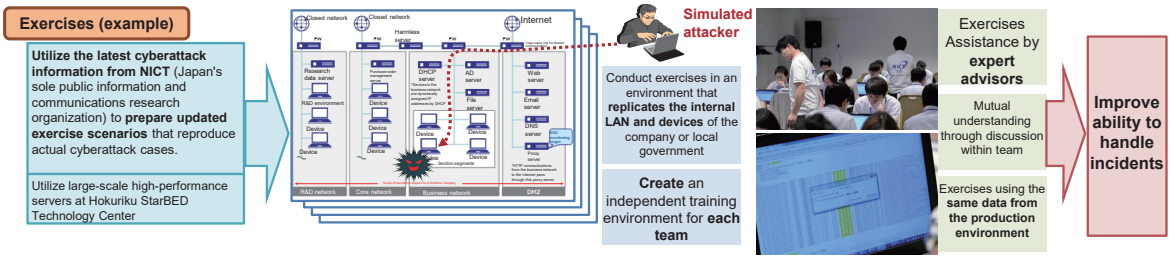


Figure 2-2-5-3 Implementation status of CYDER in FY2023

Course	Type of exercise	Level	Intended audience (topics covered)	Intended organizations	Location	Frequency	Period
A	Group exercises	Beginner	Individuals beginning to work with systems (Procedure for responding to incidents)	All organizations	47 prefectures	68 times	From Jul. to Jan. of the following year
B-1		Intermediate	System administrators and operators (Autonomous incident response and security management)	Local governments	11 regions nationwide	21 times	From Oct., to Jan. of the following year
B-2				Organizations other than local governments	Tokyo, Osaka, Nagoya	13 times	Jan. of the following year
C		Semi-advanced	Security specialists (Advanced security technology)	All organizations	Tokyo	4 times	From Nov., to Jan. of the following year
Online Standard	Online exercises	Equivalent to beginner	Individuals beginning to work with systems (Procedure for responding to incidents)	All organizations	(Participant workplaces, etc.)	As needed	From Mar. to Jul.
Pre CYDER		—	Individuals just beginning to work with systems (Prerequisite knowledge, basic matters)	National agencies etc., local government			From Dec., to Jan. of the following year

[15] Final Report of Study Group on e-Seal: https://www.soumu.go.jp/main_content/000942601.pdf
[16] Guidelines on e-Seals (2nd Edition): https://www.soumu.go.jp/main_content/000942602.pdf

B Cyber defense training for the Expo (CIDLE)

CIDLE is a cyber defense training program aimed at ensuring a robust security posture for the 2025 World Exposition (Osaka-Kansai Expo). It targets information system personnel from organizations related to the Osaka-Kansai Expo. Utilizing the legacy of the Tokyo 2020 Olympic and Paralympic Games, lecture and exercise programs have been provided since FY2023.

C Young security talent development program (SecHack365)

SecHack365 is a program aimed at developing cutting-edge security personnel (security innovators) who can create new security countermeasure technologies. It targets young ICT talents under the age of 25 residing in Japan. Utilizing actual cyberattack-related data held by the NICT, researchers and engineers at the forefront of the field provide continuous and intensive guidance on security technology research and development over the course of a year. In FY2023, 38 participants completed the program, bringing the total number of graduates since FY2017 to 289.

(2) Building an integrated cybersecurity intelligence and human resource development platform (CYNEX)

In Japan, security businesses primarily adopt and operate overseas security products. Consequently, the country's cybersecurity measures heavily rely on foreign products and information, leading to insufficient collection and analysis of domestic cyberattack information. The continued use of overseas security products results in domestic data being transferred to foreign businesses, leading to the analysis of Japan's security-related information abroad. Meanwhile, Japan continues to purchase threat information obtained from these analyses from foreign businesses.

This situation also results in a lack of accumulation of core knowledge and insights within domestic security businesses, making it difficult to effectively contribute to global-level information sharing and develop internationally recognized engineers. Furthermore, user companies also face a shortage of personnel capable of handling security products and information appropriately. To enhance Japan's autonomous response capability to cyberattacks, it is essential to accelerate the establishment of an ecosystem for accelerating the generation of domestic cyber security information and personnel development.

The MIC, in collaboration with the NICT, which conducts top-level research and development in cybersecurity, is promoting the CYNEX initiative. This initiative aims to enhance Japan's cybersecurity response capabilities by constructing and operating an advanced platform, the "Integrated Cybersecurity Intelligence and Human Resource Development Platform," which serves as a major nexus for industry-academia-government collaboration in cybersecurity, leveraging the technology and know-how accumulated by the NICT. In October 2023, the "CYNEX Alliance," composed of organizations from industry, academia, and government participating in CYNEX, was launched, marking the full-scale deployment of CYNEX. In the FY2024, the MIC will continue to expand collaboration with private companies and educational institutions, broadly collect and analyze Japan's cybersecurity information, promote the development of domestic security products using this information, and support the development of advanced security personnel and human resource development in private companies and educational institutions, aiming to further strengthen Japan's cybersecurity response capabilities.

Figure (related data) Building an integrated cybersecurity intelligence and human resource development platform (CYNEX)
URL: https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r06/html/datashu.html#f00403
(Data collection)

Additionally, from FY2023, the "Project to Involves the Verification of Sensors Capable of Ensuring Safety and Transparency in Collecting and Analyzing Cybersecurity Information from Government Terminals (CYXROSS)", was initiated to aggregate and analyze the obtained information in the NICT's CYNEX, strengthening Japan's security measures. In FY2024, efforts will continue to expand the aggregation and analysis of cyber security information and increase the adoption of sensors in government agencies to enhance Japan's unique cyberattack analysis capability.

Figure (related data) Project to Involves the Verification of Sensors Capable of Ensuring Safety and Transparency in Collecting and Analyzing Cybersecurity Information from Government Terminals (CYXROSS)
URL: https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r06/html/datashu.html#f00404
(Data collection)

4. Promotion of international collaboration

Given the global nature of cyberspace, collaboration with other countries is essential for establishing robust cybersecurity measures. To this end, the MIC actively engages in discussions, information dissemination, and information gathering at various international conferences and cyber consultations to contribute to the formation of international consensus on cybersecurity.

Additionally, supporting capacity building in the field of cybersecurity for developing countries is crucial to reducing global cybersecurity risks. MIC promotes initiatives to enhance cybersecurity capabilities, particularly in the ASEAN region, through projects such as the ASEAN-Japan Cybersecurity Capacity Building Centre (AJCCBC)[17]. In FY2023, leveraging the expertise and know-how accumulated through AJCCBC activities, MIC has expanded its capacity-building support activities to include trial exercises for island nations in the Pacific region.

Furthermore, to promote international information sharing on cybersecurity at the private sector level, MIC organizes workshops involving ISPs from ASEAN countries and holds opinion exchange meetings with ISACs (Information Sharing and Analysis Centers) between Japan and the U.S. as well as between Japan and the EU.

5. Promotion of awareness raising

(1) Initiatives for telework security

According to a survey conducted on companies that have introduced telework[18], security assurance is considered the biggest challenge when implementing telework. In response to these security concerns, the MIC has been formulating and publishing the "Telework Security Guidelines" since 2004.

With the expansion of telework, which becomes prevalent due to the spread of COVID19 and is positioned as the central focus of workstyle reform, and considering the advancement of cloud utilization and the increasing sophistication of cyber-attacks, the guidelines were revised in May 2021 to comprehensively review the necessary security measures and specific trouble cases.

Additionally, for small and medium-sized enterprises where there may not be dedicated security personnel or where the responsible individuals may not have a deep understanding of security measures, a "Telework Security Guide for Small and Medium-sized Enterprises and Others (Checklist)" was formulated and published in 2020, focusing on ensuring the minimum level of security. In May 2022, the checklist was revised to ensure readable design and words with a view of universal design, and an "Employee Handbook" that employees can actually use was newly created as an appendix. Furthermore, to assist in implementing security measures according to the checklist, a "Configuration Explanation Document" was published to explain how products used in telework should be configured. In October 2023, the range of products covered by the "Configuration Explanation Document" was expanded, and updates were made to the content of the already published products.

(2) Formation and promotion of locally rooted security communities (Regional SECUNITY)

From the perspective of ensuring a safe and secure cyber space in Japan, ensuring cybersecurity at the local level is also an important issue. On the other hand, in local businesses and municipalities, there is an information disparity regarding cybersecurity compared to companies operating on a metropolitan or national scale. Additionally, due to reasons such as a lack of management resources such as personnel, it may be difficult for them to take sufficient security measures on their own or they may not recognize the necessity of security measures.

The MIC is promoting the formation of security communities ("Regional SECUNITY") based on a "mutual assistance" relationship among stakeholders in the security field. By the end of FY2022, the establishment of Regional SECUNITY had been completed in 11 regions based on the jurisdiction of the Regional Bureau of Telecommunications etc. In FY2023, 16 seminars, 10 incident response exercises, and 7 CTF (Capture The Flag) events for young people were conducted, and large-scale cross-regional events were also held. To further expand the activities of Regional SECUNITY, support for events will continue to be provided in FY2024[19].

Figure (related data) Security communities in each region
URL: https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r06/html/datashu.html#f00405
(Data collection)

[17] Regarding the AJCCBC, refer to Section 8 "Promotion of ICT International Strategy" in Chapter 2, Part 2.
[18] Survey on actual conditions of remote work security: https://www.soumu.go.jp/main_sosiki/cybersecurity/telework/
[19] 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 cyberattack damages

As the threat of cyberattacks increases, it is beneficial for both the affected organizations and society as a whole for organizations that have suffered from cyberattacks to share and disclose information related to the damage with cybersecurity-related organizations. This helps in fully understanding the attack and strengthening countermeasures. However, due to concerns about their own reputation, affected organizations are often cautious about sharing and disclosing such information.

In response, in April 2022, the "Guidance Review Committee on Sharing and Disclosure of Information Related to Cyber Attack Damages" was established under the steering committee of the "Cybersecurity Council," a collaborative body involving various public and private entities. This committee compiled and published the "Guidance on Sharing and Disclosure of Information Related to Cyber Attack Damages" in March 2023, which serves as a practical reference for organizations that have suffered from cyberattacks[20].

Moving forward, relevant government agencies will work together to promote and raise awareness of this guidance. Additionally, based on feedback from organizations that utilize the guidance after suffering from cyberattacks, the necessity of revising the guidance will be considered.

(4) Initiatives related to wireless LAN security

Wireless LAN is widely used not only at home and workplaces but also in public wireless LAN services in urban areas. However, if appropriate security measures are not taken, there is a risk of attacks using wireless LAN devices as stepping stones or information theft. Therefore, the MIC has formulated guidelines for both users and providers of Wi-Fi to ensure security[21].

In March 2024, the content of the "Simple Manual for Wireless LAN Users" was updated and subdivided into two separate manuals: the "Simple Manual for Public Wireless LAN Users" and the "Simple Manual for Home Wireless LAN Users." This allows users to check appropriate content according to their wireless LAN usage situation.

The "Security Measures Guide for Wireless LAN Providers," aimed at a wide range of wireless LAN providers including restaurants and retail stores, was also updated, and the revised version was published in March 2024.

Additionally, to raise awareness and promote understanding of wireless LAN security measures, a free online course is held annually during the Cybersecurity Month (from February 1 to March 18). In FY2023, the online course "Learn Wireless LAN Security Measures Now" was held from March 1 to March 24, 2024.

[20] Guidance on sharing and disclosing information on damages by cyberattacks (formulated March 8, 2023): https://www.soumu.go.jp/menu_news/s-news/01cyber01_02000001_00160.html
[21] Guidelines on Wireless LAN (Wi-Fi) security: https://www.soumu.go.jp/main_sosiki/cybersecurity/wi-fi/index.html