Section 5 Developments in cybersecurity

1. Summary

(1) Past initiatives

In 2015, the Cybersecurity Strategic Headquarters was established under the Cabinet in accordance with The Basic Act on Cybersecurity (Act No. 104 of 2014), enacted against a background of rising cybersecurity threats becoming more serious on a global scale, setting forth the basic principles, etc., of Japan's cybersecurity policy. Since then, cybersecurity policies have been pursued in line with the "Cybersecurity Strategy[1]" approved by the Cabinet in September 2021, taking into account socioeconomic changes as well as increasing cybersecurity threats,

The "Cybersecurity Action Plan for Critical Infrastructure[2]" (approved by the Cybersecurity Strategic Headquarters in June 2022 and revised by the Headquarters in March 2024), which defines the basic framework for the protection of critical infrastructure, designates the information and telecommunications sector (telecommunications, broadcasting, and cable TV) as one of 15 areas of critical infrastructure that could have a significant impact on people's lives and socioeconomic activities if their functions were suspended or made unavailable. As the ministry responsible for critical infrastructure, MIC must continue its efforts to ensure the safety and reliability of information and telecommunications networks.

Furthermore, the Cabinet Secretariat convened an expert panel in June 2024 to discuss the legislation necessary to undertake new cybersecurity initiatives in order to improve response capabilities in the cybersecurity field to a level on par with major Western countries or better and thereby ensure the safety of the nation and critical infrastructure, etc., in keeping with the National Security Strategy approved by the Cabinet in December 2022. In November 2024, a "Proposal for Enhancing Response Capabilities in the Field of Cybersecurity" was compiled and, on this basis, "the Act on the Prevention of Damage from Unauthorized Acts Against Critical Computers" and "the Act Concerning Development of Laws Related to Enforcement of the Act on the Prevention of Damage from Unauthorized Acts Against Critical Computers" were both submitted to the 217th (regular) Diet session in 2025 and approved and passed in May 2025 after amendment, leading to the progress being made by the government in pursuing cybersecurity initiatives.

MIC has convened a Cybersecurity Task Force consisting of experts in the security field since 2017, and the Task Force has repeatedly compiled issues and measures to be addressed by MIC in light of changing circumstances, the Tokyo Olympic and Paralympic Games, the COVID-19 pandemic, etc. More recently, the ICT Cybersecurity Policy Subcommittee formed in February 2024 met to study the direction of cybersecurity policies that MIC should adopt over the medium to long term in light of the rapid spread of new technologies and services such as generative AI and the trends toward diversification and complexity in supply chains, and published its "Key Medium-term Strategies for ICT Cybersecurity Policy" in July 2024.

(2) Future issues and directions

The cybersecurity situation facing Japan is becoming more complex and sophisticated with each passing year. There have been ransomware attacks targeting the data centers of major businesses that disrupted their operations, and cases of persons without technical knowledge creating ransomware by using generative AI. The rising number of IoT devices stemming from rapid digitalization as well as the diversification of supply chains continue to expand the range of targets subject to attack, while accelerating changes in international relations are making the security situation more severe.

As cyberattacks become more complex and intricate, the security risks surrounding cyberspace are becoming more serious, since the targets of such attacks can include critical infrastructure, etc., that significantly impacts citizens' lives and economic activities.

With cyberspace transforming into a public space, it is becoming increasingly important to recognize the changing circumstances and ensure cybersecurity so that each and every citizen can use the information and communication technologies (ICT) forming the foundation of cyberspace with peace of mind.

Accordingly, MIC, in cooperation with relevant organizations and the private sector, will take the lead in Japan's cybersecurity policy, thereby helping ensure safety and security in cyberspace.

2. Cybersecurity in critical infrastructure, etc.

(1) Implementing comprehensive IoT botnet countermeasures

In seeking to ensure the safety and reliability of information and telecommunications networks that support cyberspace, the impact of large-scale cyberattacks such as DDoS attacks that could disrupt the functioning of information and telecommunications networks is of major concern. Typical DDoS attacks comprise two phases:

[1] Cybersecurity Strategy: https://www.nisc.go.jp/active/kihon/pdf/cs-senryaku2021.pdf
[2] Cybersecurity Action Plan for Critical Infrastructure: https://www.nisc.go.jp/pdf/policy/infra/cip_policy_2024.pdf

(1) infecting a large number of IoT devices with malware and bringing them under the attacker's control (expansion of attack infrastructure), and (2) using this attack infrastructure to carry out attacks through the network. In fact, as the number of IoT devices increases and their functions improve, the number and scale of cyberattacks that exploit IoT devices are also on the rise. NICTER, the cyberattack observation networks operated by NICT, showed in 2024 that cyberattack-related communications still targeted IoT devices most frequently.

Responding to such large-scale cyberattacks requires comprehensive countermeasures against IoT botnets, including both terminal-side (IoT device) countermeasures to prevent the expansion of the attack infrastructure and network-side countermeasures to deal with the command and control (C&C) servers that issue commands to the attack infrastructure.

MIC has been working with NICT and Internet service providers (ISPs) to investigate online IoT devices with easily guessable passwords such as "password" and "123456" and to alert users of such devices – with these terminal-side countermeasures showing some success – as part of "NOTICE (National Operation Towards IoT Clean Environment)".

However, the risk of cyberattacks exploiting IoT devices remains high, as seen in the recent increase in cyberattacks targeting software vulnerabilities in IoT devices, so cyber-attacks exploiting IoT devices remain an issue. Accordingly, responsibility for investigating IoT devices with software vulnerabilities or terminals already infected with malware as well as offering advice to device users and IoT device manufacturers was newly assigned to NICT as of FY2024 in addition to its existing tasks.

Furthermore, MIC will be implementing comprehensive countermeasures, in addition to previous notices provided to IoT device administrators, and these will include promoting security measures for IoT devices in cooperation with manufacturers and system vendors and raising awareness of security measures for IoT devices through video distribution and online advertising.

As a network-side measure, MIC began in FY2022 verifying the effectiveness of technology that allows telecommunications carriers to analyze flow information (IP addresses, port numbers, time stamps, etc.) related to communications traffic to detect C&C servers that are the source of cyberattack commands, and examining approaches to sharing and utilizing the detected C&C server list among carriers. MIC's efforts to date have confirmed the effectiveness of flow information analysis, including the successful detection of a number of C&C servers, and the goal from FY2025 will be to shrink the number of IoT botnets by visualizing overall structure of IoT botnets and implementing effective countermeasures tailored to the characteristics of each botnet, all the while coordinating these efforts with terminal-side countermeasures.

(2) Encouraging proactive cybersecurity measures by telecommunications carriers

To make security measures for IoT devices more effective, developing an environment that provides more agile measures on the network side through which communication traffic passes is considered a necessary complement to the comprehensive IoT botnet countermeasures mentioned above.[3]

A comprehensive demonstration of cybersecurity measures was conducted from FY2021 to enable telecommunications carriers to more efficiently and proactively deal with cyberattacks that are becoming larger, more sophisticated, and more complex. In the "Demonstration of Techniques for Detecting and Sharing Phishing Websites and Other Malicious Websites", a reference on practical phishing countermeasures was prepared for web service providers and awareness-raising activities were conducted for the general public; a reference outline was released in May 2024. In the "Demonstration of the Introduction of Network Security Countermeasure Techniques", a draft guideline for the introduction and operation of network security technologies such as RPKI[4], DNSSEC[5], and DMARC[6] was prepared using knowledge obtained through technical demonstrations of these technologies, which are not widely used in Japan despite the fact that their employment is becoming standard internationally. Based on this draft guideline, the Japan Network Information Center published the "Guidelines for Countermeasures against Unauthorized Internet Pathways Using RPKI ROA[7]" and the Japan Data Communications Association published "Guidelines for the Introduction of DMARC Transmission Domain Authentication Technology[8]" in FY2024. MIC continues in FY2025 to promote efforts to spread the use of these technologies.

[3] The "ICT Cybersecurity Comprehensive Countermeasures 2021" formulated in 2021 stipulate the need to consider means of developing advanced and flexible countermeasures for information and telecommunications networks managed by ISPs on the Internet as part of the efforts by telecommunications carriers to devise proactive countermeasures against cyberattacks.
https://www.soumu.go.jp/menu_news/s-news/02cyber01_04000001_00192.html

[4] RPKI (Resource Public-Key Infrastructure): A technology to verify the IP addresses and AS numbers of autonomous networks with digital certificates to prevent the hijacking of communication routes, etc.

[5] DNSSEC (DNS Security Extensions): A technology that prevents server spoofing by verifying the linkage between domain names and IP addresses with digital certificates

[6] DMARC (Domain-based Message Authentication Reporting and Conformance): A technology that verifies the authenticity of the domain from which an e-mail is sent and automatically handles instances of spoofing, etc.

[7] Guidelines for Countermeasures against Unauthorized Internet Pathways Using RPKI ROA
https://www.nic.ad.jp/doc/jpnic-01324.html

[8] Guidelines for the Introduction of DMARC Transmission Domain Authentication Technology
https://www.dekyo.or.jp/soudan/data/anti_spam/dmarc_guideline.pdf

(3) Initiatives involving supply chain risk countermeasures

MIC conducted technical verification over the entire 5G network, including virtualization infrastructure and management systems, from FY2019 to FY2021, and in April 2022 published the first edition of the 5G Security Guidelines[9] outlining security issues of which operators should be aware and measures to address them. The Guidelines were approved as an international standard by ITU-T SG17[10] in September 2024.

Telecommunications system configurations are becoming more complex as functions become more sophisticated, and OSS[11] is being used as a software component. Such changes in the software supply chain have resulted in the introduction of malicious code into software components, etc., and if the configuration of the software is not known, it is difficult to respond quickly to attacks.

In light of this situation, MIC carried out a demonstration project for introducing SBOM[12] in the telecommunications sector starting in FY2023 to help enhance cybersecurity through the use of SBOM, and prepared a draft set of points to keep in mind when creating and using SBOM.

Another demonstration project was conducted from FY2023 to ascertain the level of analysis capabilities and user information handling practices in Japan by having a third party carry out technical analyses of smartphone applications to determine the application behavior. With the "Act Concerning the Promotion of Competition in Relation to Specified Software Used in Smartphones" (Act No. 58 of 2024) coming into force as of FY2025, greater use of alternative distribution channels for apps other than the official stores operated by smartphone OS providers is anticipated in Japan. A survey is therefore being conducted to determine whether the operators of alternative distribution channels are taking measures to ensure security, etc., in compliance with the SPSI[13].

(4) Efforts to ensure the safety of cloud services

MIC has formulated the "Guidelines for Information Security Measures in the Provision of Cloud Services," which compiles information security measures for cloud service providers as an initiative to promote the safe and secure use of cloud services. A revised edition (the third edition) reflecting actual cloud service provision and use was published in September 2021.

Recent years have witnessed cases of cloud service users being unable to use cloud services appropriately, resulting in information leakage, so the "Guidelines for Appropriate Settings in the Use and Provision of Cloud Services" were formulated in October 2022 after discussions among a wide range of entities, including providers and users, on ways to ensure that users make appropriate use of cloud services. The "Guidebook of Countermeasures for Improper Cloud Settings" was published in April 2024 to explain the contents of the Guidelines to cloud service users in an easy-to-understand manner.

(5) Trust service initiatives

Real space and cyberspace will be highly integrated in Society 5.0, and various interactions in real space must be carried out smoothly in cyberspace as well. To achieve this, it will be essential to build infrastructure enabling the safe and secure distribution of data; trust services **(Figure 2-2-5-1)**, a mechanism to prevent data falsification and spoofing of transmission sources, are becoming increasingly important.

Based on the "Priority Plan for the Realization of a Digital Society" (approved by the Cabinet on June 21, 2024)[14], MIC is endeavoring to ensure proper implementation of time stamp systems and to formulate standards for evaluating the reliability of private-sector e-seal services,[15] as well as to put in place conformity assessments.

A Development of a government time stamp certification system

Time stamps were examined by the "Panel on Time Stamp Certification Systems" launched by MIC in March 2020, and the "Regulations on the Accreditation of Time Certification Services" (MIC Notification No. 146 of 2021) were set forth in April 2021 to establish a government accreditation system overseen by the Minister for Internal Affairs and Communications. Because of revisions made to the taxation system in FY2022, only those time stamps compliant with this accreditation system of the Minister for Internal Affairs and Communications are to be used for tax-related documents in the scanner preservation system under the Electronic Bookkeeping Act[16] (Act No. 25 of 1998). As of May 2025, four companies have been accredited as time stamp

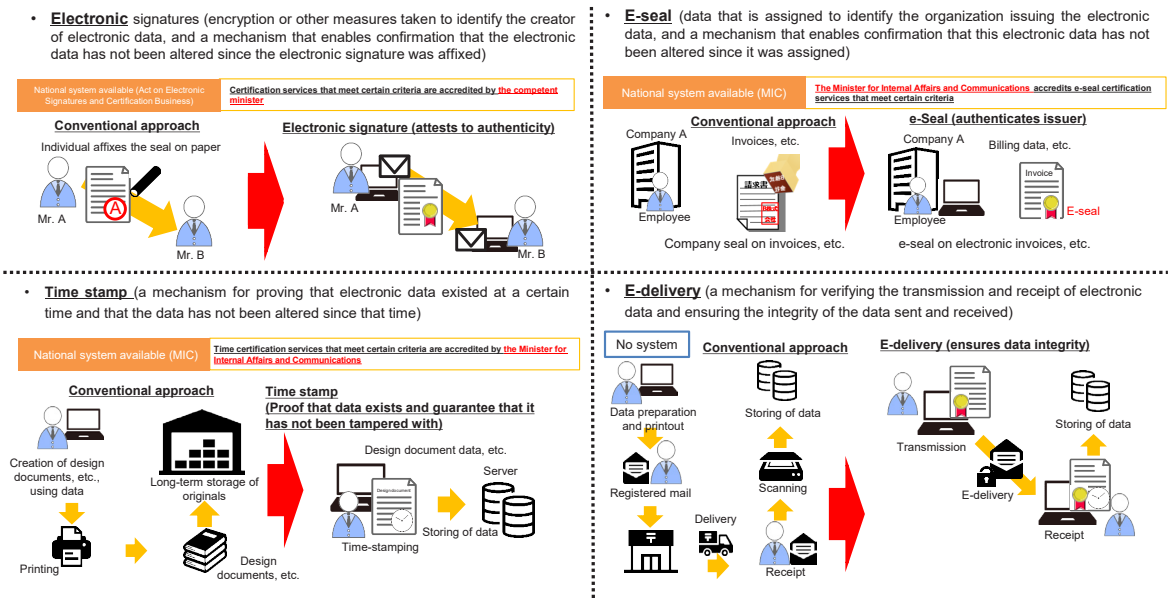
[9] 5G Security Guidelines Version 1
https://www.soumu.go.jp/main_content/000812253.pdf
[10] International Telecommunication Union Telecommunication Standardization Sector Study Group 17
[11] Refers to open source software, where the source code is released free of charge and can be used, improved, and redistributed by anyone
[12] Software Bill of Materials
[13] Smartphone Privacy Security Initiative (SPSI) (https://www.soumu.go.jp/main_content/000981875.pdf)
[14] Priority Plan for the Realization of a Digital Society
https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/5ecac8cc-50f1-4168-b989-2bcaabffe870/6329b727/20240621_policies_priority_outline_03.pdf
[15] An e-seal is electronic data that is attached to or logically associated with information recorded in an electromagnetic record and that meets the following two requirements: being used to indicate the source or origin of said information and being able to confirm whether or not said information has been altered.
[16] Act on Special Provisions for the Methods of Preserving Books and Documents Relevant to National Taxes Prepared by Use of a Computer (Act No. 25 of 1998)

businesses. MIC will continue to run the accreditation system appropriately and reliably, and will seek to further expand the use of time stamps.

B Efforts to institutionalize e-seals

In April 2020, MIC launched the "Panel on Systems to Ensure the Reliability of Data Issued by Organizations," which examined suitable approaches to the use of e-seals in Japan, and set out the "Guidelines for e-Seals" in June 2021 to provide certain standards regarding e-seal technologies and uses in Japan. In September 2023, the "Panel on e-Seals" was created to discuss the formulation of standards for evaluating the reliability of private-sector e-seal services and the establishment of conformity assessments[17], and the "Guidelines for e-Seals (2nd Edition)[18]" were published along with the Panel's final report in April 2024. The "Expert Committee for the Formulation of Relevant e-Seal Regulations" was convened in June 2024 for the purpose of helping formulate relevant regulations needed in preparation for an e-seal accreditation system, and in March 2025, the "Regulations for the Accreditation of e-Seal Certification Businesses" (MIC Notification No. 113 of 2025) established an accreditation system run by the national government (Minister for Internal Affairs and Communications). Going forward, MIC will work on designating an authorized investigative organization and related actions for full-scale operation.

Figure 2-2-5-1 Trust services



3. Improving cyberattack response capabilities and adapting to new technologies

(1) Efforts to develop security personnel

Cyberattacks are becoming more sophisticated and complex even as Japan's cybersecurity personnel remain inadequate both qualitatively and quantitatively, so developing human resources for cybersecurity is an urgent issue. To that end, MIC has been actively promoting cybersecurity human resource development initiatives (CYDER, CIDLE and SecHack365) through NICT's National Cyber Training Center.

A Practical cyber defense exercise for information system managers (CYDER)

CYDER (CYber Defense Exercise with Recurrence) is a practical cyber defense exercise for information system personnel from national government agencies, local governments, independent administrative agencies, and critical infrastructure providers. Participants experience a series of cyberattack response methods, from incident detection to response, reporting, and recovery, while operating actual equipment in a large-scale virtual LAN environment that simulates an organization's network environment (**Figure 2-2-5-2**).

In FY2024, the existing beginner, intermediate, and semi-advanced level group exercises were joined by the "Pre-CYDER" program **(Figure 2-2-5-3)**, in which participants can learn the basics of cyberattack mechanisms, trends, and incident handling.

4,225 people participated in the CYDER group exercise in FY2024, bringing the cumulative total to over 25,000 since FY2017.

[17] Final Report of the Panel on e-Seals (https://www.soumu.go.jp/main_content/000942601.pdf)
[18] Guidelines for e-Seals (2nd Edition) (https://www.soumu.go.jp/main_content/000942602.pdf)

Figure 2-2-5-2 CYber Defense Exercise with Recurrence (CYDER)

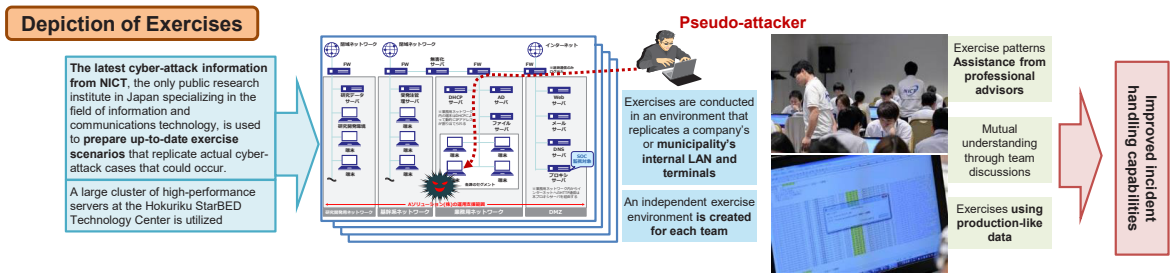


Figure 2-2-5-3 CYDER exercises in FY2024

Course name		Delivery method	Level	Target audience	Target organizations	Course venue	Course period
CYDER	A	Classroom instruction	Beginner	System novices (Incident response procedures)	For all organizations	All 47 prefectures	July - January of the following year
	B-1		Intermediate	System administrators and operators (proactive incident handling and security management)	Local governments	11 regions nationwide	October - January of the following year
	B-2				Organizations other than local governments	Tokyo, Osaka, Nagoya	January of the following year
	C		Pre-advanced	Security specialists (advanced security techniques)	For all organizations	Tokyo, Osaka	November - January of the following year
Pre-CYDER		Online	-	All information systems personnel (Acquisition and updating of minimum required knowledge)	For all organizations	(Participants' workplaces, etc.)	First half: May - July Second half: October - January

B Cyber Incident Defense Learning for EXPO (CIDLE)

CIDLE is a cyber defense training course for information system personnel from organizations connected with the Osaka-Kansai Expo, and it was designed to help ensure a complete security system for Expo 2025 (Osaka-Kansai Expo). Lectures and seminar programs were offered from FY2023 to FY2024, utilizing the legacy of the Tokyo 2020 Olympic and Paralympic Games.

C Training program for young security personnel (SecHack365)

SecHack365 is a program for young ICT professionals under the age of 25 residing in Japan that seeks to develop cutting-edge security personnel (security innovators) who can create new security countermeasure techniques. Utilizing NICT data from actual cyberattacks, leading researchers and engineers provide continuous and committed guidance on security technology R&D over the course of one year. In FY2024, 39 students completed the program, bringing the cumulative total since FY2017 to 328.

(2) Integrated platform for cybersecurity intellectual and human resource development (CYNEX)

Security providers in Japan mostly install and operate foreign security products. As a result, Japan's cybersecurity measures rely heavily on foreign products and foreign-derived information, and do not adequately collect and analyze domestic cyberattack information. In addition, the use of foreign security products continues to cause domestic data to flow to foreign operators and, with Japan's security-related information being analyzed overseas, the threat information obtained as a result of these analyses must be purchased from foreign operators.

Domestic security providers are consequently unable to accumulate core expertise and knowledge, and it is difficult for them to effectively contribute to information sharing at the global level and to train internationally competent engineers. User companies also lack the personnel needed to properly handle security products and security information. To enhance Japan's ability to autonomously cope with cyberattacks by developing cybersecurity personnel and adopting other approaches, it is necessary to establish an ecosystem that accelerates cybersecurity information generation and human resource development in Japan.

In cooperation with NICT, which conducts top-level cybersecurity R&D in Japan, MIC has since FY2021 been promoting CYNEX (CYbersecurity NEXus), an initiative to improve Japan's cybersecurity response capability by establishing and operating an integrated platform for cybersecurity intellectual and human resource development as cutting-edge infrastructure that will serve as a major hub for cybersecurity-related industry-academia-government collaboration. The CYNEX Alliance, consisting of organizations from industry, academia, and government participating in CYNEX, was launched in October 2023 to begin full-scale deployment of CYNEX. In FY2025, MIC will continue to collect and analyze a wide range of cybersecurity information in Japan and utilize such information to promote the development of domestic security products, while expanding cooperation with other ministries/agencies, private companies, educational institutions, etc. MIC will also seek to further improve Japan's

cybersecurity response capabilities by fostering high-level security personnel and supporting human resource development in government agencies, private companies, and educational institutions.

Figure (related data): Integrated platform for cybersecurity intellectual and human resource development (CYNEX)
URL:https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r07/html/datashu.html#f00393
(Data collection)

In FY2023, MIC launched an initiative to strengthen Japan's security measures by installing sensors that can verify security and transparency in some ministries and agencies, aggregating the collected cybersecurity information for analysis by NICT, and analyzing it by utilizing NICT's capabilities as part of the "Demonstration Project for the Collection and Analysis of Cybersecurity Information Using Government Terminal Information (CYXROSS)". In FY2025, MIC will continue to expand the aggregation and analysis of cybersecurity information, and to bolster Japan's unique cyberattack analysis capabilities by expanding the number of government ministries/agencies that have introduced sensors.

Figure (related data): Demonstration Project for the Collection and Analysis of Cybersecurity Information Using Government Terminal Information (CYXROSS)
URL:https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r07/html/datashu.html#f00394
(Data collection)

(3) Cybersecurity efforts connected with generative AI, etc.

While the employment of generative AI has been rapidly advancing in all fields in recent years, the risks associated with generative AI now include not only the spread of dis-/mis-information, privacy violations and infringements of intellectual property rights but also the exploitation of generative AI for cyberattacks. As cyberattacks become larger, more complex, and more sophisticated, the workload involved in implementing cybersecurity countermeasures is becoming an issue, and expectations are high that generative AI and other technologies will be utilized in cyberattack countermeasures as well.

Given this background, it is necessary to work on "Security for AI" to avoid or reduce security risks stemming from AI as much as possible while keeping abreast of the latest trends in generative AI and other AI technologies, and to tackle "AI for Security" to effectively utilize AI in security measures.

In addition to formulating security guidelines for the safe and effective development and provision of AI, MIC will join together with NICT and specialist organizations in the US and elsewhere to conduct research and develop on AI safety and to promote the safe and secure use of generative AI through the "Security for AI" approach.

As an "AI for Security" initiative, MIC will promote the active use of generative AI in cybersecurity measures by collecting and analyzing cyberthreat information and using generative AI, etc., to refine and accelerate the detection of attack infrastructures.

Figure (related data): Cybersecurity efforts connected with generative AI, etc.
URL:https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r07/html/datashu.html#f00395
(Data collection)

4. Efforts to strengthen cybersecurity across local communities and beyond

(1) Forming locally-rooted security communities (local SECUNITY)

Ensuring cybersecurity in communities is also an important issue from the perspective of ensuring a safe and secure cyberspace nationwide. Local companies and local governments may have difficulty in taking sufficient security measures on their own or fail to recognize the necessity of security measures due to the cybersecurity information gap between themselves and companies operating in the Tokyo metropolitan area or nationwide; they may also lack the required human and other management resources.

MIC promotes the formation of communities in the security field ("local SECUNITY") based on "mutual aid" relationships among interested local parties; by FY2022, such communities had been established in all 11 regions defined by the jurisdictions of the Regional Bureaus of Telecommunications and related offices. In FY2024, 20 seminars, 14 incident response exercises, and three Capture The Flag (CTF) competitions for young people were conducted, and additionally nationwide CTF events were held simultaneously at seven venues. In 2025, MIC will continue supporting the expansion of local SECUNITY initiatives by holding events and engaging in other activities.

Figure (related data): Security communities in various regions
MIC Support for Strengthening Local Security Communities (SECUNITY)
URL: https://www.soumu.go.jp/main_sosiki/cybersecurity/localsecunity/index.html

(2) Telework security initiatives

According to a survey of companies that have introduced telework[19], security has been the biggest issue in introducing telework. MIC has established and published "Telework Security Guidelines" since 2004 to dispel such security concerns and to enable companies to introduce and utilize telework with peace of mind.

Telework has spread in the wake of the COVID-19 pandemic and has taken center place in work style reform. In light of such changes in security as growing cloud utilization and more sophisticated cyberattacks, the Guidelines were revised in May 2021 in a complete overhaul of security measures to be implemented and the specific trouble cases to be considered.

Since it is assumed that small and medium-sized enterprises, etc., may not have a dedicated person in charge of security or that the person in charge of security measures may lack specialized knowledge, MIC has since 2020 formulated and published the "Telework Security Guide (Checklist) for Persons in Charge at Small and Medium Enterprises, etc." with a focus on maintaining at least a minimum level of security. MIC has also published an "Explanation of Settings" that describes how to configure products used for teleworking when implementing security measures according to the Checklist; the "Explanation of Settings" was updated in July 2024.

(3) Wireless LAN security initiatives

Wireless LANs are used widely at home and at work, and public wireless LAN services can even be accessed in town. If appropriate security measures are not taken, though, wireless LAN devices can be used as a stepping stone for attacks and information theft. For this reason, MIC has established guidelines for both users and providers regarding security measures for wireless LANs; these guidelines were revised in February 2025 to reflect the latest security and technology trends[20].

The "Simple Manual for Public Wi-Fi Users" for users of public wireless LAN services and the "Simple Manual for Home Wi-Fi Users" for those who install and use wireless LAN at home explain the security measures that users should keep in mind. The "Guide to Security Measures for Public Wi-Fi Providers" for restaurants, retail stores and other wireless LAN providers explains the required measures from two perspectives: that of users and that of the providers themselves.

To raise awareness of security measures for wireless LANs, free online courses on the latest security measures and related topics are also offered every year during Cybersecurity Month (February 1 - March 18). In FY2024, the online course "Learn Now: Wi-Fi Security Measures" was offered from February 5 to March 18, 2025.

(4) Cybersecurity Site for Citizens

MIC has created a "Cybersecurity Site for Citizens"[21]to promote widespread awareness and understanding of cybersecurity among the general public so that Internet users can protect themselves from cyberattacks and prevent others from unintentionally causing trouble.

In May 2024, the article content was updated in light of the latest security trends to systematically present examples of damage caused by cyberattacks, steps to take in the event of a cyberattack, and preventive measures.

[19] Fact-finding survey on telework security: https://www.soumu.go.jp/main_sosiki/cybersecurity/telework/
[20] Guidelines for Wireless LAN (Wi-Fi) Security: https://www.soumu.go.jp/main_sosiki/cybersecurity/wi-fi/
[21] Cybersecurity Site for Citizens: https://www.soumu.go.jp/main_sosiki/cybersecurity/kokumin/

5. Further promotion of international cooperation

Since cyberspace has a global reach, cooperation with other countries is essential for establishing cybersecurity. To this end, MIC is actively engaged in discussions, information dissemination, and information gathering at various international conferences and cyber dialogues with the aim of contributing to the formation of international consensus on cybersecurity.

Support for developing countries' capacity building efforts in the field of cybersecurity is also important to reduce cybersecurity risks worldwide. MIC is engaged in human resource development projects in the ASEAN region through the ASEAN-Japan Cybersecurity Capacity Building Centre (AJCCBC) and other related actions, thereby contributing to the improvement of cybersecurity capabilities in the ASEAN region and elsewhere[22]. Utilizing the know-how gained through AJCCBC activities, MIC has since FY2023 been expanding the scope of its activities to include, for example, new capacity-building support exercises for island countries and other locales in Oceania.

Additionally, for the sake of sharing information on international cybersecurity at the private-sector level with telecommunications carriers and others, MIC has hosted workshops attended by ISPs from ASEAN countries and has taken part in Japan-US and Japan-EU meetings via the Information Sharing and Analysis Center (ISAC).

[22] See also Part II, Chapter 2, Section 8, "Pursuing International ICT Strategies" for more information on MIC's efforts at the ASEAN-Japan Cybersecurity Capacity Building Centre.