NISC National center of Incident readiness and Strategy for Cybersecurity

# Overview of Cybersecurity 2024

**July 10, 2024**

**National center of Incident readiness and Strategy for Cybersecurity (NISC)**

# Cybersecurity 2024 (annual report / plan) Overview (Part 1: Executive Summary)

## 1. Recent changes and circumstances surrounding cyberspace

- Cyberattacks are becoming increasingly refined and sophisticated, including an increasing number of state-sponsored attacks and zero-day attacks that exploit unknown vulnerabilities. New risks are also increasing with the spread of new technologies, such as generative AI.

⇒ It is important that competent entities, such as government agencies, critical infrastructure operators, and technology companies providing services to users, fulfill wider roles and responsibilities. It is necessary to strengthen measures and improve their response capabilities regularly, including from the perspective of ensuring cybersecurity, implement measures based on principles for Security by Design and Default, and coordinate and collaborate with relevant countries, including leading Western countries.

## 2. Measures to be taken especially strongly(*)

(*) The "FY 2025 Budget Prioritization Policy" also plans to emphasize these measures.

✓ **In order to strengthen the response capabilities in the field of cybersecurity equal to or surpassing the level of leading Western countries, the government will draft legislation for the implementation of active cyber defense as soon as possible.** In addition, it will pursue the following measures with special emphasis..

### (1) Realizing a Digital Society where the People can Live with a Sense of Safety and Security ~ Improvement in Response Capabilities of Government Agencies and Critical Infrastructures, etc. ~

✓ Fundamentally Strengthen the Government's Cybersecurity System
- Identification of vulnerabilities through attack surface management, information gathering through protective DNS, and promotion of CYXROSS

✓ Strengthen Critical Infrastructure Exercises and Improve Resilience in Individual Sectors
- [Various sectors and cross-sectoral] New exercises with emphasis on public-private partnerships, [Medical] Verification and inspection of the security of connections of hospitals to external networks, [Administration] Measures based on the Amendment of Local Autonomy Act

✓ Raising the Level of Cybersecurity Measures by Strengthening the Functions of IPA and Initiatives of NICT
- [IPA] Establishment of AISI, development of a system to analyze cyber-attack trends and geopolitical information, [NICT] Development of new exercise programs specialized for each sector

### (2) Enhancing Socio-Economic Vitality and Sustainable Development ~ Strengthening of Response to Supply Chain Risks and Reinforcement of Initiatives for Advancing and Supporting DX ~

✓ Strengthening of Cybersecurity Measures for IoT Devices and Software Products Based on principles for Security by Design and Default
- Creation of guidelines on software development methods, promotion of the use of SBOM, the establishment of "IoT Product Security Conformity Assessment Scheme," and expansion of devices covered under the "NOTICE" survey

✓ Promote Cybersecurity Measures of Small and Medium Enterprises (SMEs)
- Dissemination and development of "Cybersecurity Supporters Services," including new service types, promotion of matching and sharing of security person with SMEs

### (3) Contribution to the Peace and Stability of the International Community and Japan's National Security ~ Further Strengthening of Collaboration with Relevant Countries Including leading Western countries ~

✓ Promote Coordination and Collaboration with Overseas Cybersecurity-Related Organizations and Support of Capacity Building in the Indo-Pacific Region
- Sharing of policy trends, etc., through multilateral frameworks (such as G7) or bilateral meetings, participation in signing joint statements, etc., and support capacity building to Pacific Island Countries

✓ Promotion of Initiatives by the Police to Ensure the Safety and Security of Cyberspace
- Participation in joint investigations with foreign investigative authorities, strengthening of collaboration with various Japanese and foreign entities, information gathering on cases and cross-case analysis

# [1] Fundamentally Strengthen the Government's Cybersecurity System



## 1. Background and Issues

- **To cope with the sudden increase in IT assets and services**, which can be the potential starting point of cyber-attack intrusions and **dramatic sophistication of cyber-attack methods**, such as the rise of Living Off the Land attacks, there is a crucial need for **strategic implementation of cybersecurity measures across all government agencies** more than before.
- To address issues such as variations in the level of operation monitoring by each PJMO and prompt information sharing in the event of incidents, the Digital Agency will work **on improvement of the level of operational monitoring** by the Digital Agency and **development a framework for comprehensive operational monitoring** that checks all Digital Agency systems across the board **to prevent, detect and recover from incidents as early as possible.**
- Amid increasingly sophisticated and complex cyber-attacks and expansion of unknown threats, **there is no adequate collection of attack scenarios specific to Japan**. It is also **difficult to accumulate the know-how and expertise necessary to develop Japanese products and services**. Therefore, **it is a pressing issue to establish a system that enables Japan to collect and analyze information on cybersecurity on its own**.

## 2. Overview of Initiatives

### 1) Method

- ✓ Promote measures to **strengthen the effectiveness of standards and rules such as the "Government Standards for Government Agencies" and the "IT Procurement Agreement"** and **to consider initiatives to evaluate measures and responses of government agencies from multiple perspectives, including organizational, system, and personnel aspects, such as the utilization and the strengthening of development of government human resources specializing in cybersecurity and the Red Team Test.**
- ✓ Steadily develop and operate the existing security operations framework (GSOC) and **systematically implement "threat hunting" that actively searches for threats**. (In this process, NISC will actively work on new measures such as **identifying vulnerabilities through attack surface management** and **identifying TTPs through protective DNS**.)
- ✓ The Digital Agency plans to **design and develop a comprehensive operation monitoring system and start operation monitoring** within FY2024.
- ✓ **Sensors manufactured in Japan** that can be verified for safety and transparency will be **installed on government devices**, and the information obtained from them will be **consolidated on CYNEX** (*) by NICT **and analyzed**. By cross-sectionally analyzing the government device data aggregated in CYNEX and the cybersecurity information collected by NICT over the years, **generate data on cybersecurity independently in Japan**. The information generated **is shared across the government**.

(*) Cybersecurity Nexus

### 2) Expected Results and Effects

- ✓ **Realize a robust government-wide cybersecurity system** through **autonomous enhancements of both policy and operation segments , etc.**
- ✓ **Prevention, early detection, and early recovery from incidents** will be possible by ensuring IT governance through operation monitoring across all government entities and by improving the level of operation monitoring.
- ✓ Further enhancement of cybersecurity measures through the **generation of Japan's cybersecurity-related information and the sharing of analysis results, across the government.**

## 3. Key feedback from the Expert Members at the Cybersecurity Strategic Headquarters

- It is paramount important to strengthen Japan's system.
- Cybersecurity attack techniques are constantly evolving, becoming noticeably more sophisticated and secretive, and cannot be easily discovered and prevented using conventional detection and defense methods. To address this, discovery (sensing) of an attack, real-time information sharing, and dynamic defense are important, and government agencies must introduce and operate these with all their efforts.
- It needs to strongly promote to establish a unified system for sharing cyber-related information among ministries and agencies and for appropriate and effective response.
- It is important to conduct comprehensive operation monitoring of government information systems and sharing Japan's cybersecurity-related information.
- It needs to fundamentally strengthen the system that protects the government and the defense system of Japan as a whole, including critical infrastructure companies and private companies.

## 1. Background and Issues

- The Cabinet Secretariat **conducts "Cross-sectoral exercises" every fiscal year** in collaboration with the competent ministries and agencies to verify the effectiveness of the incident response capability of critical infrastructure operators, etc. Although efforts have been made to ensure the resilience of critical infrastructure through exercises, it is **a challenge to respond when incident occurs at multiple organizations and to implement and confirm information sharing between the public and private sectors**.
- **Regarding security measures at medical institutions**, each institution has taken initiatives voluntarily up to now; however, since there have been incidents of long-term suspension of medical services due to cyber-attacks, **voluntary efforts alone are considered insufficient**. It is necessary to promote cybersecurity measures at medical institutions aggressively.
- Amid the **further development of the interconnection of national and local governments through networks**, it is necessary to ensure the effectiveness of cybersecurity measures of local governments.

## 2. Overview of Initiatives

1) Method

- ✓ Conduct **new public-private collaboration exercises focusing on the implementation of public-private collaboration**, along with the current cross-sectoral exercises. Include situations such as two-way communication between the Cabinet Secretariat, competent ministries and agencies, critical infrastructure operators, etc., and scenarios such as the interruption in critical infrastructure services and the occurrence of incidents in external critical infrastructure services in the exercises.
- ✓ Provide **initial response support to medical institutions** where a cybersecurity incident has occurred, and **consultation and advice to medical institutions on taking cybersecurity measures**. In addition, **create and post contents, etc., that can be used for training of employees**, on the "Security Education Support Portal Site for Medical Institutions."
- ✓ Conduct training and raise public awareness on the "Guidelines for the Safe Management of Medical Information Systems" Ver. 6.0 at medical institutions. In addition, promote daily security measures at the institutions based on the "Checklist of Cybersecurity Measures for Medical Institutions" and conduct onsite inspections using the checklist.
- ✓ Under a project commissioned by the Ministry of Health, Labour and Welfare, **verify and inspect the security of hospital network connections to external networks** and **provide support for the development of offline backup systems.**
- ✓ **Revise the Local Autonomy Act** to mandate **local governments to formulate policies and implement measures necessary for the proper use of information systems based on the guidelines prepared by the Minister of Internal Affairs and Communications.**

2) Expected Results and Effects

- ✓ These initiatives can be expected to encourage critical infrastructure operators, etc., to improve their own incident response capability and to **improve their ability to respond to incidents affecting multiple organizations which happened in other critical infrastructure sectors** and **strengthen the information sharing system between the public and private sectors**, which in turn will improve the resilience of all critical infrastructure sectors.
- ✓ **Secure the local healthcare structure** by **raising the level of cybersecurity measures of medical institutions as a whole** and preventing the occurrence of cases that cause long-term outages of medical services.
- ✓ **Promote efforts related to "Responsibility of Local Governments" as prescribed in the Basic Act on Cybersecurity and raise the level of cybersecurity at all local governments.**

## 3. Key feedback from the Expert Members at the Cybersecurity Strategic Headquarters

- Improving the security level across all critical infrastructures is exactly the kind of measure that the government should undertake.
- The impact of cyber damage on critical infrastructures is significant, and experiencing the reality of such damage through exercises is important. Considering the recent international situations, the public and private sectors should aim for "highly skilled" and highly "realistic" exercises through closer collaboration.
- Public-private collaboration cannot be achieved without engaging in specific practices. The significance of conducting exercises to deal with damage through collaboration and cooperation across all ministries and agencies is immeasurable. Continuing such efforts and inviting broad participation across the public and private sectors is important. Verifying whether there are any inadequacies in organizational and institutional responses through the exercises is important.
- Reinforcing exercises specific to individual sectors, including medical institutions, is also important.
- In cross-sectoral exercises, clearly defining the purpose of an exercise and the role of the government and selecting realistic scenarios and participants is essential. Utilizing existing exercise such as Locked Shields is also necessary.

# [3] Raising the Level of Cybersecurity Measures by Strengthening the Functions of IPA and Initiatives of NICT



## 1. Background and Issues

- While **opportunities and possibilities for AI technology are expanding, risks are diversifying and increasing**. The "**AI Safety Institute**" (AISI) **was established within the IPA**, and **the "Guidelines for AI Businesses" was published** to promote the safe and secure use of AI.
- IPA implements various initiatives, including **developing measures standards such as various guidelines**, and **support for initial response** against cyber-attacks by the **Cyber Rescue Team**.
- There have been a **series of incidents where** critical infrastructure operators **such as medical institutions ceased to function due to cyber-attacks**, partly due to the **shortage of human resources specializing in cybersecurity** in this sector. The government needs to provide support and **promptly train human resources** based on the actual situation in the concerned sector.

## 2. Overview of Initiatives

### 1) Method

- ✓ **Promote studies on how to ensure the implementation of the Guidelines for AI Businesses, considering international conformity, etc.**, and **establish safety evaluation methods for AI** in cooperation with Japanese and overseas AI experts, **mainly AISI**, **while collaborating with equivalent organizations in partner countries and regions**, including the United Kingdom and the United States.
- ✓ IPA will **manage and centralize the function to create the guidelines** and enhance their effectiveness in **collaboration with** the newly established **"IoT Product Security Conformity Assessment Scheme," etc.**
- ✓ In addition to analyzing cyber-attack trends, **develop a system for analyzing** underlying **geopolitical information, etc.,** and **strengthen the capability** to deal with cyber-attacks and **collect and analyze information**.
- ✓ **Develop new exercise programs specialized for each sector** in collaboration with the Ministry of Health, Labour and Welfare, etc., utilizing NICT's experience and knowledge in training human resources and cybersecurity research, and establish a system to provide such programs to private companies and organizations. Train instructors in conjunction with the above.

### 2) Expected Results and Effects

- ✓ **Businesses** can **check guidelines on actions for the safe and secure use of AI** from the Guidelines for AI Businesses.
- ✓ Cybersecurity is expected to be enhanced by establishing **benchmarks for necessary measures and visualizing the status of measures based on the actual conditions of the supply chain**, including the type of industry and size of each company. This can contribute to ensuring the national and economic security.
- ✓ The initiatives can be expected to **improve the response capabilities of the medical and cybersecurity sectors**. In addition, **opportunities to participate in practical cybersecurity exercises utilizing human resources from the private sector will expand**.

## 3. Key feedback from the Expert Members at the Cybersecurity Strategic Headquarters

- Intensive enhancement of IPA and NICT is likely to boost efficient initiatives.
- IPA and NICT, public organizations that widely utilize human resources from the private sector, are expected to foster trust and facilitate the bidirectional exchange of information between the public and private sectors. Expert groups such as J-CSIP/J-CRAT are expected to participate more actively, especially in areas such as economic security.
- The use of AI also plays an important role in the field of cybersecurity measures. In this context, enhancing the functions of IPA is of great significance.
- Securing human resources is a pressing issue, especially in critical infrastructure sectors. It is important to contribute to cybersecurity reinforcement in critical infrastructure sectors by utilizing NICT's knowledge and experience in practical measures for training human resources specializing in cybersecurity for sectors where such measures are needed.
- To raise the level of security across Japan, continuous efforts across organizations are necessary, and human resources who can lead such efforts are indispensable.

# [4] Strengthen Cybersecurity Measures for Software Products and IoT Devices Based on Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Security by Design and Default



## 1. Background and Issues

- **Discussions on strengthening security measures for software and IoT products are being expedited**, mainly in the United States and Europe. To ensure the effectiveness of these measures, **promoting the utilization of SBOM** (Software Bill of Materials) and **building a mechanism to evaluate the conformity of IoT devices with security requirements** is necessary.
- While the number of attacks that expand botnets by hijacking IoT devices is increasing and the risk of attacks further increases, **taking measures for vulnerable IoT devices and IoT devices already infected with malware is a pressing issue.** At the same time, **initiatives to detect and share C&C server** activities by analyzing the flow of information are also necessary.

## 2. Overview of Initiatives

### 1) Method

✓ Promote the following initiatives **based on principles for Security by Design and Default.**

- **Prepare guidelines on development methods** for software developers, **promote the use of SBOM**, and study the **mechanism for self-declaration of conformity** for safe **software**.
- **Establish "IoT Product Security Conformity Assessment Scheme,"** coordinate and negotiate for cooperation on certified products and government procurement, etc., and mutual recognition with the schemes of other countries.
- **Expand the devices covered under the "NOTICE (*)" survey**, enhance the publicity of safety management measures for users, **strengthen the collaboration among IoT device manufacturers, etc.**, and other initiatives.
- Take initiatives to **improve and validate a series of mechanisms to detect, evaluate, share, and manage C&C server** activities, with a focus on dealing with actual IoT botnets, and **improve the capability to monitor C&C server** activities by expanding ISPs that analyze the flow of information, etc. In addition, aggregate and analyze data obtained during countermeasures to facilitate visualization of the overall picture of IoT botnets.

(*) Initiatives by NICT to investigate IoT devices that may be exploited for cyber-attacks and issue alert users of such devices.

### 2) Expected Results and Effects

✓ By organizing knowledge on SBOM and developing tools such as transaction models for software, **an environment will be created that will enable users to use software with a sense of safety and security**, and as a result, **increased added value such as increased productivity and the creation of new services** can be expected in all industries.

✓ **Establishing an internationally harmonized conformity assessment scheme** for IoT devices will ensure the **distribution of safe devices within Japan** and **enhance competitiveness** by **reducing the cost of additional support to comply with foreign schemes** when companies expand their sales channels of IoT devices overseas.

✓ Continued activities to reduce (Curb the increase) vulnerable IoT devices will lead to **a safer use environment for IoT devices**.

## 3. Key feedback from the Expert Members at the Cybersecurity Strategic Headquarters

- Discussions on security measures for software and IoT devices are being expedited, mainly in the United States and European countries, and initiatives to ensure the effectiveness of these measures are important.
- The concepts of "Security by Design" and "Security by Default" will soon become fundamental in the ICT industry. More specific measures are necessary moving forward.
- Key issues to be addressed in the medium to long term. It is also important to think from the aspect of global coordination.
- Continued efforts should be made to address security issues in software and IoT while further strengthening the collaboration among developing firms, etc.
- It is important to establish an evaluation scheme for IoT devices. In this system, attention must be paid to "maintaining collaboration with other countries" and "setting a threshold (difficulty level) that is not excessively high."
- Regarding NOTICE, more information is expected to be exchanged in both directions in the future, which will be useful in reinforcing security.

# [5] Cybersecurity Measures of Small and Medium Enterprises (SMEs)



## 1. Background and Issues

- Cyber-attacks targeting SMEs that are relatively lagging in countermeasures against such attacks in the entire supply chain **are causing apparent damage to the SMEs themselves and their customers, including large companies**. On the other hand, **SMEs do not perceive the risk as their affairs** or **do not understand how to deal with the risks**.
- It is necessary to **create an environment that will enable SMEs with insufficient budgets and human resources to assess the level of security measures that are most effective for them** given their size, type of industry, business circumstances, etc., and **implement such measures. It is also necessary to disseminate and promote security services that are easy to use** for SMEs.

## 2. Overview of Initiatives

1) Method

- ✓ **Promote and deploy the Cybersecurity Supporters Services at SMEs, etc., including new service types** launched in FY 2023.
- ✓ **Present cost-effective methods, etc.,** while establishing linkage with guidelines **following the size of the companies and nature of their IT assets.**
- ✓ Create opportunities facilitating **matching between SMEs and human resources specializing in security,** and **reduce costs incurred by SMEs for searching human resources** through **promoting sharing of human resources specializing in security, etc.**

2) Expected Results and Effects

- ✓ These initiatives will **promote public awareness** of **Cybersecurity Supporters Services** including among medium-sized and larger SMEs.
- ✓ By presenting methods for cost-effective security measures, **the level of security measures of the entire supply chain in industry will improve**.
- ✓ By reducing the cost incurred by SMEs for searching human resources, **the number of human resources implementing cybersecurity measures at companies will increase**.

## 3. Key feedback from the Expert Members at the Cybersecurity Strategic Headquarters

- SMEs often support supply chains. Therefore, it is important to ensure their security.
- SMEs have become easy targets for criminals. In Japanese industry, the “Cornerstone” of security defense lies with SMEs.
- The government should take the lead in actively promoting support for security measures for SMEs. In particular, the focus should be on human resources, information sharing, and subsidy support activities.
- Ensuring resilience is a vital issue for SMEs. The role of the “Cybersecurity Supporters Services” is important in providing and disseminating appropriate response methods in response to feedback and needs of companies needing help, and in training human resources who will be responsible for such support.
- We also expect to implement support measures for securing human resources, such as matching and sharing of human resources specializing in security.

# [6] Promote Coordination and Collaboration with Overseas Cybersecurity-Related Organizations and Support of Capacity Building in the Indo-Pacific Region



## 1. Background and Issues

- Since National Security Strategy of Japan stipulates, "**the response capabilities in the field of cybersecurity should be strengthened equal to or surpassing the level of leading Western countries,**" **strengthening cooperation and collaboration with ally and like-minded countries** is becoming increasingly important. There is a need to promote **international collaboration further considering the technical aspects** while ensuring conformity with foreign and security policies.
- For securing the lives of Japanese nationals residing in foreign countries and ensuring the stability of activities of Japanese companies, which depend on critical infrastructures of the target countries, and providing **support of capacity building in the field of cybersecurity**, which is directly linked to ensuring the safety of the cyberspace as a whole, **it is necessary** for relevant ministries and agencies, and the public and private sectors to closely collaborate and **provide support in a manner that leverages Japan's strengths**, based on the "Basic Policy on Cybersecurity Capacity Building Support for Developing Countries," after identifying new threats in cyberspace and needs of each country.

## 2. Overview of Initiatives

(1) Method

- ✓ **Information exchange and policy coordination with ally and like-minded countries, participation in and contribution to multilateral frameworks** related to cybersecurity (such as G7, IWWN, CRI, QUAD, and FIRST), and dissemination of Japan's policies at international think tanks and forums.
- ✓ **Support of capacity building in the field of cyberspace for developing countries, including the Indo-Pacific region** through ASEAN-Japan Cybersecurity Policy Meeting, cybersecurity exercises for the industrial control systems in the Indo-Pacific region, implementation of various exercises and CTFs at AJCCBC, Cybersecurity Capacity Building Support Project for Pacific Island Countries, and contribution to the World Bank's Cybersecurity Multi-Donor Trust Fund, etc.

(2) Expected Results and Effects

- ✓ Collaboration with other countries will make it possible to **effectively promote cybersecurity policies** and **mitigate damage after an incident occurs**.
- ✓ **The level of cybersecurity-related capacity** of government officials and critical infrastructure operators **will improve**, mainly those in **the Indo-Pacific region, including ASEAN.**

## 3. Key feedback from the Expert Members at the Cybersecurity Strategic Headquarters

- Essential Initiatives from a global perspective.
- Agreed that there is a need to strengthen coordination and collaboration with overseas cybersecurity-related organizations. The kind of contribution Japan can make within the international framework is also an essential perspective in building, fostering, and strengthening relationships of trust with relevant organizations in other countries.
- Due to the recent increase in geopolitical tensions, there is a need to strengthen collaboration and cooperation with ally and like-minded countries, considering the improvement of technical capabilities, skills, etc.
- It is extremely important to build a strong relation of cooperation between Japan and neighboring countries in the Indo-Pacific region.
- Such outreach is important because the Indo-Pacific region has become a critical area of strategic competition.

## 1. Background and Issues

- **While cyberspace is transforming into a public domain** where all citizens participate **and important socioeconomic activities are carried out**, irrespective of region, age, or gender, the **threats to cyberspace and the impact of major cyber incidents on the functioning of society continue to be extremely serious**, including the spread of ransomware, a sharp increase in unauthorized use of credit cards and unauthorized remittances through online banking, believed to be caused by phishing, and the emergence of cyber incidents targeting cryptocurrency asset-related businesses and academic institutions.
- Further promotion of the following initiatives is required in response to this situation
  - ✓ **Promote reporting to and consultation with the police, raise public awareness, and alert the public** on measures to prevent damage from cyber incidents
  - ✓ **Enhance cross-sectoral and bird's-eye analysis of cyber incidents** and **collaborate with foreign investigative authorities**

## 2. Overview of Initiatives

1) Method

- ✓ The Cyber Affairs Bureau of the National Police Agency, **in cooperation with various domestic and foreign entities**, will effectively promote measures to prevent damage from cyber incidents, such as alerting the public and making various requests to related organizations based on the threat situation in cyberspace. The National Cyber Department, which was formed after a much-needed reorganization of the Kanto Regional Police Bureau's National Cyber Unit, will also enhance its system to collect, organize, and analyze information and will **actively participate in international joint investigations** through high-level coordination with foreign investigative authorities.

2) Expected Results and Effects

- ✓ Working with various entities in Japan and overseas is expected to **improve the safety and security of cyberspace** through timely and accurate damage prevention measures based on the threat situation in cyberspace, and investigation and clarification of cyber incidents in collaboration with foreign investigative authorities.

## 3. Key feedback from the Members at the Cybersecurity Strategic Headquarters

- In recent years, serious cyber incidents like ransomware and phishing attacks have intensified. There is an expectation for further strengthening of cooperation between the public and private sectors, cooperation between government agencies and collaboration with foreign investigative authorities.
- This year, an even stronger system of investigative cooperation is expected, including with the FBI and Europol. Promote sharing of crime information through media such as TV and social media.
- To deal with cybercrimes, which are evolving and becoming more sophisticated daily, law enforcement agencies must develop better organizational structures and measures to improve their capabilities.
- Collaboration with foreign authorities is also expected.

**Increasing severity and sophistication of cyber-attacks**

- Cyberattacks are becoming increasingly refined and sophisticated, including an increasing number of state-sponsored attacks and zero-day attacks that exploit unknown vulnerabilities. New risks are also increasing with the spread of new technologies, such as generative AI.

⇒ It is important that competent entities, such as government agencies, critical infrastructure operators, and technology companies providing services to users, fulfill wider roles and responsibilities. It is necessary to strengthen measures and improve their response capabilities regularly, including from the perspective of ensuring cybersecurity, implement measures based on principles for Security by Design and Default, and coordinate and collaborate with relevant countries, including leading Western countries.

## Enhancing Socio-Economic Vitality and Sustainable Development

### Economic and social situation

- Rise in threats associated with increased use of IT in corporate activities.
- In addition to direct cyber-attacks on large enterprises, there have also been instances of their business partners being used as springboards for attacks.
- Damage could extend beyond the targeted organization to the entire supply chain
- Approximately half of ransomware victims are SMEs.

### SMEs and supply chain measures

- Measures to address supply chain risks for organizations are essential, and the private sector requires enhanced support services and functions, particularly for SMEs.

### Promotion of initiatives to ensure the security of IoT products

- Measures such as security evaluation for IoT devices that may be misused are necessary.

## Realizing a Digital Society where the People can Live with a Sense of Safety and Security

### Situation at each entity supporting economic and social infrastructure

**(1) Government agencies, etc.**

- The number of cyber incidents remains high.
  (207 in FY 2021, 266 in FY 2022, 233 in FY 2023)
- The provision of vulnerability information, etc., by the GSOC to government agencies, etc., has also increased.
  (598 in FY 2021, 630 in FY 2022, 861 in FY 2023)
- Close cooperation between the first and second GSOCs is necessary.
- Introduction of a mechanism (ASM) to encourage correction of vulnerabilities, etc., and protective DNS to detect and store IP addresses of malicious sites.

**(2) Critical infrastructure**

- Numerous cases of system failures and information leaks have occurred in the critical infrastructure field, both in Japan and overseas.
  (Example: Suspension of operations at a port facility after a ransomware cyber-attack)
- System design and operation based on the concept of multi-layered defense built on the premise of hacking, and business continuity formulation and inspection based on the assumption of damage due to cyber incidents are necessary.

**(3) Universities, educational/research institutions, etc.**

- Proactive maintenance and improvement of security standards based on the characteristics of universities and other institutions is necessary.

**(4) Utilization of knowledge gained from the initiatives for the Tokyo Olympic and Paralympic Games**

- Utilization of this knowledge for the Expo 2025 Osaka, Kansai, etc., is important.

## Contribution to the Peace and Stability of the International Community and Japan's National Security

### Overseas developments (international trends in other countries)

**United States**

- Department of Defense released the summary of the "2023 Department of Defense Cyber Strategy" (September 2023)
- Updated the International Guidance regarding "Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Security by Design and Default" (Co-sealed by 13 countries and organizations including Japan) (October 2023)

**United Kingdom**

- Created "Guidelines for secure AI system development" (Joint statement of 8 countries and organizations including Japan) (November 2023)

**Australia**

- The Australian Government released the "2023-2030 Australian Cyber Security Strategy" and "Action Plan" (November 2023)
- "Engaging with Artificial Intelligence (AI) Guidelines" prepared (Co-sealed by 11 countries and organizations including Japan) (January 2024)

**EU**

- European Parliament approved the "Cyber Resilience Act"; Political agreement on the "EU Cyber Solidarity Act" (March 2024)

**ASEAN**

- The Commemorative Summit for the 50th Year of ASEAN-Japan Friendship and Cooperation was held, and the "Joint Vision Statement" and "Implementation Plan" were released (December 2023)

International cooperation is essential. Work on strengthening international cooperation based on trends in each country.

## Cross-Cutting Approaches to Cybersecurity

### Research and development in the cybersecurity sector

- As the scope of security further expands into the field of cyberspace because of the spread of generative AI, advances in cutting-edge technologies such as quantum technology, and the recent complexity of the international situation, the importance of R&D, which forms the basis of safety and security in cyberspace, continues to increase.
- The government is establishing a system to build an industry-academia-government ecosystem from the perspective of expanding the scope of research and examining practical R&D concepts.

### Human resources specializing in IT and cybersecurity

- In addition to the growing demand for securing cybersecurity human resources, demand for reskilling human resources who lack knowledge and work experience will continue to increase as DX advances.
- Under the "Comprehensive Strategy for the Vision for a Digital Garden City Nation" the government aims to develop 2.3 million digital promotion human resources, including cybersecurity human resources, by the end of FY 2026.
- Create an environment where skills can be acquired, change the awareness of management, such as "Plus Security," and strengthen initiatives at universities, KOSEN (National Institute of Technology, Japan), etc.

### Public awareness and behavior

- While digitization is making steady progress, the number of victims and cost of damages caused by fraudulent phishing transfers is at an all-time high.
- Regarding the need for cybersecurity measures, it is essential for all entities to cooperate and collaborate and conduct more detailed public awareness raising activities that are tailored to their target audience.
- Continued efforts should be made to engage in public awareness activities based on the "Cybersecurity Awareness and Action Enhancement Program."

# 1. Enhancing Socio-Economic Vitality and Sustainable Development

## Examples of efforts last year

### Awareness of Management

- Created videos on topics such as response to supply chain risks and fostering corporate culture with awareness of security, with the aim of supplementing knowledge on "Plus Security" for the management level
- Supported initiatives to investigate and disclose information disclosure status of private companies
- Raised awareness of the "Cybersecurity Management Guideline" and improved the usability of visualization tools

### Cybersecurity Measures for Local Communities and SMEs

- Conducted training and incident exercises with industry-government-academia collaboration through regional SECURITY
- Conducted empirical research to develop IoT security human resources within local communities
- Revised the "Cybersecurity Supporters Services Standards," promoted the "SECURITY ACTION" program, and expanded the number of regional security leaders

### Ensure Reliability of Supply Chain, etc.

- Promoted the Software Bill of Materials (SBOM) and implemented initiatives to strengthen security measures for IoT products
  - ✓ Formulated the "Handbook for Implementation of SBOM for Software Management"
  - ✓ Decided to begin partial operation of the IoT Product Security Conformity Assessment Scheme
- Organized issues arising when introducing SBOM, a software component configuration table, in the communications field

## Evaluation

- With the expansion of supply chain risks, there is concern that the risk of further damage from attacks will increase in the future, so additional initiatives are needed to raise awareness of the importance of cybersecurity from a corporate governance perspective
- It is essential to encourage the spread of initiatives in regions and through supply chains, address the risk of unintended leakage of information assets due to inadequate security settings, etc.
- It is necessary to continue to develop various initiatives, such as the horizontal deployment of industry-specific practices, the development of infrastructure that serves as a hub between industry, academia, and government, and the creation of standards and specifications based on a framework that addresses the security requirements of the cyber and physical world

## Examples of efforts this year

- Dissemination of model curricula and public awareness content to supplement knowledge on "Plus Security" for the management level
- Continue to support private sector initiatives based on the "Cybersecurity Measures Information Disclosure Guidance"
- Raise further public awareness of cybersecurity management through the "Cybersecurity Management Guideline" and related tools

- Support efforts for voluntary management of regional SECURITY, such as seminars and incident exercises
- Raise public awareness about the "Guidelines for Appropriate Settings for Using and Providing Cloud Services"
- Hold discussions on how to promote and raise public awareness of the "Cybersecurity Supporters Services Standards" and how to spread knowledge about and utilize the system to promote "SECURITY ACTION"

- Further study vulnerability management related to SBOM utilization and measures to begin the operation of the IoT security conformity assessment scheme
  - ✓ Promote dissemination in cooperation with industry
  - ✓ Utilization through government procurement, etc.
  - ✓ Promote international system harmonization
- Organize issues with a view to successful operations after introducing SBOM in the communications field

## 2. Realizing a Digital Society where the People can Live with a Sense of Safety and Security

### Integrated Advancement along with Building a Safe and Secure Environment and Digital Transformation

**Examples of efforts last year**

- Released the "Security by Design Guidelines for Government Information Systems," the "Enterprise Architecture for Continuous Risk Scoring & Action (CRSA)"
- Promoted registration and improved the evaluation mechanism for SaaS with a low-security risk (ISMAP-LIU)
- Updated the Mynaportal app to improve convenience and ensure stable system operation
- Implemented legal reforms to extend and expand NOTICE initiatives

### Government Agency Efforts

**Examples of efforts last year**

- Revised the Common Measures Standards for Government Agencies
- Imparted advice on measures against supply chain risks, including a review of regulations and risk mitigation measures
- Performed management audits with a focus on areas where appropriate risk responses are considered necessary
- Alerted government agencies of cyber-attacks detected by GSOC and studied ways to form the next GSOC
- Installed sensors developed by NICT in some government devices and started to collect and analyze information from these terminals

### Critical Infrastructure Efforts

**Examples of efforts last year**

- Established the "Guideline for Establishing Safety Principles for Ensuring Cybersecurity of Critical Infrastructure"
- Revised the "Cybersecurity Policy for Critical Infrastructure Protection" and added harbors to the list of critical infrastructure
- Established the "Risk Management Handbook for Cybersecurity Departments in Critical Infrastructure"
- Conducted "cross-sectoral exercises" (Record number of 6,574 participants from 819 organizations)

### Evaluation

- Formulation and revision of guidelines and technical reports while investigating technological trends needs to be continued
- Initiatives are required to provide more convenient services for users while ensuring cybersecurity
- The present status of cybersecurity measures of government agencies, etc., was grasped properly, and advice was provided to strengthen these measures and implemented initiatives to promote them further, thereby the government agencies, etc., as a whole could further raise the level of cybersecurity measures
- It is necessary to continue and further promote the proactive initiatives of relevant ministries and agencies, promote studies to enhance information-sharing systems, promote initiatives to ensure that risk management activities as a whole continue to function effectively and continue strengthening the common infrastructure that supports the entire Action Plan, including human resources development

**Examples of efforts this year**

- Revise and publish new guidelines and technical reports and utilize them in the Digital Agency system
- Special measures to promote the spread and utilize ISMAP-LIU
- Expand Mynaportal services, continuously improve its UI/UX, and appropriate operation and management of the portal
- Establish a system for cooperation with ISPs, manufacturers, etc., to promote measures for "NOTICE"

**Examples of efforts this year**

- Promote the use of "IT Procurement Agreement" and "External Service Agreement" as measures against supply chain risks
- Continue to confirm risk responses, etc., in audits based on recent threat trends
- Collaboration between government agencies, etc., and GSOC, steady development of the next period GSOC, and introduction of technologies and services such as ASM and Protective DNS
- Share the results of collecting and analyzing information from government devices using sensors developed by NICT with NISC, etc.

**Examples of efforts this year**

- Organization of cross-sectoral and conformity basic requirements (Minimum Requirements) that even critical infrastructure operators of SMEs should comply with on priority
- Continuation of initiatives related to the five policy groups based on the action plan
- Implementation of "Cross-sectoral exercises" and exercises involving public and private sector collaboration

## 3. Contribution to the Peace and Stability of the International Community and Japan's National Security

### Examples of efforts last year

| Ensuring "a Free, Fair and Secure Cyberspace" | Strengthening Capabilities for Defense, Deterrence, and Situational Awareness | International Cooperation and Collaboration |
|---|---|---|
| ➢ Actively contributed to promoting the rule of law in cyberspace through cyber dialogues and other multilateral meetings<br>➢ Actively contributed to relevant discussions at the UN Open-Ended Working Group (OEWG) toward the proposed post-2025 UN Programme of Action (PoA)<br>➢ Strengthened international collaboration, including information exchange with national organizations within the G7, ASEAN, and Interpol (ICPO) frameworks, etc. | ➢ Implemented initiatives to deepen cooperation with entities related to mission assurance of SDF<br>➢ Strengthened defense capabilities through implementation of Risk Management Framework (RMF), etc.<br>➢ Discussed confidence-building measures to be undertaken within the framework of the ASEAN Regional Forum<br>➢ Close information exchange and analysis with foreign-related agencies and joint alerts with relevant ministries | ➢ Knowledge-sharing and policy coordination through cyber dialogues held in more than 15 countries and regions<br>➢ Organized various meetings and events on the occasion of the 50th Year of ASEAN-Japan Friendship and Cooperation and discussed future directions<br>➢ Strengthened international collaboration through participation in the 3rd International Counter Ransomware Initiative and the Quad Senior Cyber Group 3rd In-person Meeting of Principles |

### Evaluation

- ➢ Japan needs to further deepen discussions on international rules and norms by contributing to discussions at the UN OEWG sessions, etc.
- ➢ It is important to deepen cooperation by linking efforts to share knowledge and support capacity building through international cooperation and collaboration to increase the number of countries that are signatories to the Convention on Cybercrime
- ➢ Given the diversification and complexity of threats in cyberspace, it is necessary to continue strengthening capabilities for defense, deterrence, and situational awareness of Japan
- ➢ Japan must increase the number of countries with which it has a relationship of trust and deepen its relationship with countries with those it already has a relationship of trust
- ➢ Regarding support of capacity building, expanding the scope of support with a focus on the Indo-Pacific region and responding strategically through public-private partnerships is necessary

### Examples of efforts this year

| | | |
|---|---|---|
| ➢ Accelerate discussions on the application of international law in cyberspace through bilateral and multilateral meetings and the UN OEWG<br>➢ Build multilateral cooperative relationships through international conferences, strengthen collaboration with foreign law enforcement agencies, and promote accurate international investigations<br>➢ Discuss United Nations convention against cybercrime in collaboration with relevant countries | ➢ Given the increasingly severe security environment, continue to promote initiatives to ensure Japan's resilience against cyber-attacks and improve capabilities for defense, deterrence, and situational awareness | ➢ Implement measures aimed at setting off a ripple effect to achieve stability in cyberspace, such as support of capacity building in the ASEAN region, etc.<br>➢ Cooperate with the U.S. and Europe to conduct industrial control system cybersecurity exercises for critical infrastructure operators in the Indo-Pacific region<br>➢ Organize conferences and strengthen collaboration with key ally and like-minded countries regarding the protection of critical infrastructure, threat situation awareness, etc. |

## 4. Cross-Cutting Approaches to Cybersecurity

| | Promotion of R&D | Recruitment, Development, and Active Use of Human Resources | Awareness Raising, Establishment and Improvement of Literacy |
|---|---|---|---|
| Examples of efforts last year | ➢ Conducted research and development, including the development of innovative artificial intelligence infrastructure technologies such as reliable AI<br>➢ Upgraded "CYNEX," which serves as the hub of industry-academia-government collaboration, and full-fledged efforts to collect, analyze, and provide security information were started<br>➢ Started building a quantum cryptography communications network and R&D into elemental technologies of quantum internet | ➢ Implemented the "Core Human Resources Development Program" and dissemination of human resources development programs through the portal site "Manabi DX"<br>➢ Implemented CYDER after reorganizing and updating the course content based on the needs of the participants<br>➢ Reviewed government cybersecurity-related training and skills certification | ➢ Implemented public relations activities aimed at young people using the Internet and social media<br>➢ Updated content of the "Key Points to Ensure Safe Use of Smartphones" course<br>➢ Provided IPA educational materials for general users, instructors, etc. |
| Evaluation | ➢ There is a need to combine the perspectives of both R&D, which is the source of innovation, and the industry-academia-government ecosystem, including security perspectives<br>➢ Initiatives are necessary to ensure that research promotion measures are widely utilized in society<br>➢ With the rapid development of quantum technology, it is necessary to continue promoting R&D | ➢ The need for specialized human resources is increasing, making it necessary to constantly improve the environment for human resource development and broaden the base of human resources<br>➢ Given the growing threats in cyberspace, it is necessary to strengthen initiatives to secure and train digital human resources for the government | ➢ Considering the increase in the number of people participating in cyberspace, it is necessary to review the status of and improve initiatives, including measures for older people, children, and families |
| Examples of efforts this year | ➢ Continue support for research projects, including cybersecurity, in addition to the development of fundamental technologies<br>➢ Perform technical verification of unauthorized functions and unknown vulnerabilities that could lead to such functions<br>➢ Revise "CRYPTREC Cryptographic Technology Guideline" and R&D on Post-Quantum Cryptography (PQC), etc.<br>➢ Promote the social implementation of quantum cryptography communication and R&D on elemental technologies of quantum internet | ➢ Promote the dissemination and utilization of handbook, etc., concerning security-related workforces development, and raise awareness among managers<br>➢ Continue to implement "CYDER," "Public vocational training," "Security camps," etc., to promote independent security-related human resource development<br>➢ Promote the use of qualification exams, review training, and establish a system for updating skill certification | ➢ Implement public awareness initiatives in collaboration with related ministries and agencies and promote the utilization of various types of content<br>➢ Continue organizing seminars for the digital utilization support project<br>➢ Continue to provide educational materials and content to raise awareness regarding information security and organize seminars for instructors |

# Part 1 Executive Summary Glossary



| No. | Terms | Explanation |
|---|---|---|
| 1 | Security by Design | Ensures that IT products (especially software) are secure from the design stage. Identifying cyber threats and conducting risk assessments are essential prerequisites. |
| 2 | Secure by Default | Ensures that users (customers) can securely use IT products (especially software) immediately after purchase without incurring additional costs or effort. |
| 3 | Attack Surface Management | Initiatives to continuously evaluate the information systems of government agencies, etc., and other entities from the internet across various organizations, promoting the timely correction of vulnerabilities. |
| 4 | Protective DNS | Service that utilizes the Domain Name System (DNS) to protect users from threats such as malicious websites, malware, etc., and stores the domain names and IP addresses used by these threats. |
| 5 | CYXROSS | Abbreviation for CYNEX XROSS organ observatory project.<br>A demonstration project for collecting and analyzing cybersecurity information using government device information. |
| 6 | IPA | Information-technology Promotion Agency, Japan.<br>An incorporated administrative agency that implements measures for improving software security and reliability, integrated IT human resource development programs (Skill Standard, Japan Information Technology Engineers Examination, etc.), and receives reports on information related to computer viruses and unauthorized access, alerts and provides information to citizens and enterprises, as part of its information security measures. |
| 7 | NICT | National Institute of Information and Communications Technology.<br>An incorporated administrative agency that conducts research and development in the field of information and communication technology from a comprehensive perspective covering all aspects from basic research to applications and returns research results to society through collaboration between industry, academia, and government. |
| 8 | AISI | Abbreviation for AI Safety Institute. |
| 9 | SBOM | Abbreviation for Software Bill of Materials.<br>A machine-processable list that includes information on software components and their dependencies. |
| 10 | NOTICE | Abbreviation for National Operation Towards IoT Clean Environment.<br>Initiatives by NICT to investigate IoT devices that may be exploited for cyber-attacks and to alert users of such devices. |