NISC National center of Incident readiness and Strategy for Cybersecurity

Overview of Cybersecurity 2023

July 4, 2023

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

“Cybersecurity 2023 (annual report / plan)” Overview （Part 1: Executive Summary）

1. Recent changes and circumstances surrounding cyberspace and policy issues

○ Recent changes and circumstances surrounding cyberspace

- The use of information systems is expanding in various sectors and organizations. Supply chains are becoming more diversified and complex. New technologies such as generative AI are also spreading.
- On the other hand, this has been accompanied by an increase in the number of entry points for cyber attacks and a rise in the risk of system failures and information leaks due to inadequate security measures, etc.
- In addition, state-sponsored cyber attacks are being conducted on a regular basis, as the national security environment becomes increasingly severe.

○ Policy issues based on recent changes in the situation

- The response capabilities in the field of cybersecurity should be strengthened equal to or surpassing the level of leading Western countries.
- Policy issues include (1) enhancement of countermeasures and response capabilities by each entity, (2) enhancement and reinforcement of government support, etc., and (3) strengthening of international partnerships and cooperation.

2. Measures to be taken with particular emphasis this year based on the policy issues(*1)

- Based on the National Security Strategy, promote necessary approaches in cyberspace to seamlessly protect Japan in all directions.
- Drive measures based on the "Three Directions(*2)" of the Cybersecurity Strategy. In promoting the measures, will pay attention to implementing future approaches while reviewing and considering advantage of the past achievements in Japan. Implement the following measures with particular emphasis this fiscal year.

(1) Enhancing Socio-economic Vitality and Sustainable Development - Enhancement of risk countermeasures for the promotion of DX -

- ✓ Enhancement of measures in local communities and SMEs that have not necessarily been proactive in utilizing ICT.
- ✓ Reinforcement of measures for upgrading software security in light of increasing supply chain risks.

(2) Realizing a Digital Society where People can Live with a Sense of Safety and Security - Improvement of resilience of government agencies and critical infrastructure -

- ✓ Improvement of resilience of government information systems through revision and familiarization of Common Standards for Government Agencies and understanding of threat trends in cyberspace.
- ✓ In promoting security enhancement for critical infrastructure sectors, enhance organization-wide measures by each business entity through the revision of the guidelines for establishing security standards, etc., and strengthen measures in each sector, including the healthcare sector.

(3) Contribution to the Peace and Stability of the International Community and Japan’s National Security - Promotion of international partnership and cooperation with allies and like-minded countries -

- ✓ Support of capacity building in the Indo-Pacific region through strengthening public-private partnerships by holding a conference to commemorate the 50th anniversary of ASEAN-Japan Friendship and Cooperation.
- ✓ Cooperation among Quad (Japan-US-Australia-India) and promotion of cooperation framework among like-minded countries to enhance anti-ransomware measures.

(*1) The "Draft FY2024 Budget Prioritization Policy" also places emphasis on these measures.
(*2) Simultaneous promotion of DX and cybersecurity / Ensuring safety and security from a bird's-eye view of the entire cyberspace, which is becoming a public space, etc. / Strengthening efforts from the perspective of national security

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

1. Background and Issues

- Need to strengthen measures against cyber attacks on SMEs, which are relatively weak in the supply chain, as such attacks are also affecting large companies that place orders with SMEs.
- On the other hand, there are many SMEs that do not recognize the risk as their own business, or do not know what to do, or are facing challenges in securing countermeasure costs and human resources.
- Need to raise the awareness of SME managements, promote familiarization and improve operation of security services that are easy for SMEs to use, and further dispel concerns about the applicability of related laws and regulations when large companies provide support and make requests for security measures to SMEs with whom they do business.

2. Summary of Approaches

(1) Method

- ✓ Expand and enhance “Cybersecurity Supporters Services" by revising the service standards to meet the various needs / demands of SMEs.
- ✓ Implement these efforts in cooperation with the Supply Chain Cybersecurity Consortium (SC3) to spread the measures to SMEs.

(2) Expected Results and Effects

- ✓ Through the spread of the “Supporters Services," the security of SMEs should improve, and the actual status of cyber-attack damage in SMEs can be identified through service providers. In addition, expected to promote the reporting and sharing of information to relevant organizations.
- ✓ In cooperation with the Supply Chain Cybersecurity Consortium (SC3), expected to strengthen cybersecurity for the entire industries.

■ Key takeaways from the expert members of the Cybersecurity Strategy Headquarters

- Even though being an important challenge for Japan’s security measures, cybersecurity measures for local communities and SMEs are still at the stage where they can finally be started. For the time being, it is necessary for the government to play a leading role and for the public and private sectors to work together to vigorously promote cybersecurity measures.
- There are issues unique to SMEs (size, cost, transfer of know-how, etc.), and detailed and specific measures are required to deal with these issues.
- According to the National Police Agency (NPA) 's press release dated March 16, 2023, "Threats in Cyberspace in 2022," 53% of the victims of ransomware attacks were SMEs, which calls for discussion on a cybersecurity measure involving support from both the national and local governments to help SMEs, who occupy an important position in supply chains.

[2] Efforts on Advancement of Software Security Based on Supply Chain Risks

1. Background and Issues

- In a world where cyberspace and the physical space are closely interrelated, with the risk of cyber attacks increasing, a framework that organizes the approach to cope with this situation is being developed, and the level of security measures need to be improved by promoting social implementation.
- In particular, as awareness of the importance of introducing SBOM, which manages information on software components and can be used for vulnerability management, is spreading mainly in the US, it is important to create a mechanism to take advantage of the merits of SBOM and spread it to various fields, while responding to such trends.
- SBOM needs to be introduced in the telecommunications sector urgently to cope with cyber attacks, which are occurring more frequently with the growing use of OSS in software for telecommunications systems.

2. Summary of Approaches

(1) Method

- ✓ To improve the efficiency of vulnerability management, etc., efforts up to FY2022 will be deepened, including demonstration of a method to automatically link vulnerability information with SBOM.
- ✓ Promote efforts to introduce SBOM in the telecommunications sector, such as by creating and evaluating SBOM for representative telecommunications systems.

(2) Expected Results and Effects

- ✓ Through the compilation of knowledge on SBOM and the development of tools such as contract models, etc., it is expected that an environment will be created in which software can be securely used, and that added value will be increased such as improved productivity and the creation of new services in all industries.
- ✓ Through the introduction of SBOM in the telecommunications sector, speedier response can be expected when vulnerabilities in software components such as OSS are identified.

■ Key takeaways from the expert members of the Cybersecurity Strategy Headquarters

- Since awareness of the importance of introducing SBOM, which can be used for vulnerability management, is rapidly spreading mainly in the US, it is important to achieve an early practical application of SBOM following the demonstration of the automatic linkage of vulnerability information with SBOM.
- US government has already taken a stance to emphasize SBOM in the US EO dated May 12, 2021, and cooperation including SBOM has been proposed in the “Quad Cybersecurity Partnership" in May 2022. Accordingly, there is a need to make collaborative approaches not only in Japan but also with allies and like-minded countries.
- While moves to strengthen the software supply chain, including the introduction of SBOM, are accelerating in Japan and abroad, few companies in Japan have yet put SBOM management into practical use, and at present SBOM is considered to be at the stage of becoming recognized as a concept and term. SBOM shall not merely be a list of vulnerability information (bill of materials), but a mandatory requirement (international qualification) to enter the value chain and supply chain.

[3] Centralized Approaches for Protection of Government Information Systems

1. Background and Issues

- Due to increasingly sophisticated and complex cyber attacks and unknown threats associated with the progress of ICT utilization, the risk of cyber attacks on government information systems is increasing. To respond to them rapidly, it is important to revise Common Standards for Government Agencies based on the latest threats and technological trends to ensure the information security of government information systems, as well as to collect and analyze information on cyber attacks, etc., for continuous production of effective technologies and knowledge. On the other hand, Japan is dependent on foreign security products and services for collecting and analyzing information on cyber attacks. The establishment of a system that enables Japan to collect and analyze cybersecurity information on its own, without excessive dependence on the security products of overseas operators, is an urgent issue.

2. Summary of Approaches

(1) Method

- ✓ Given the risk of frequent DDoS attacks on government websites and cyber attacks originating from vulnerabilities in the supply chain, revise Common Standards for Government Agencies, including enhancement of measures that take account of the characteristics of the latest DDoS attacks and measures for the protection of government information at outsourcing partners, and disseminate the latest information security measures in government agencies, etc., based on these standards.
- ✓ Introduce sensors capable of verifying safety and transparency into government devices to collect device data without relying on overseas products, and aggregate and analyze the obtained information in NICT's CYNEX (Cybersecurity Nexus). 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 generated data will be shared not only with the government ministries and agencies that have introduced the sensors, but also with NISC, GSOC, the Digital Agency, etc., which oversee the cybersecurity of the entire government.

(2) Expected Results and Effects

- ✓ Due to the reflection of the Common Standards for Government Agencies based on the latest threat trends, prevention of incidents at government agencies and improvement of resilience in the event of an incident can be expected.
- ✓ Japan's own cybersecurity related data can be generated without excessive dependence on overseas products.
- ✓ Further enhancement of cybersecurity measures can be expected by sharing analysis results with government ministries and agencies, NISC, GSOC, the Digital Agency, etc.

■ Key takeaways from the expert members of the Cybersecurity Strategy Headquarters

- Ensuring the autonomy of CTI (Cyber Threat Intelligence) in a broad sense is recognized as a top priority.
- The mechanism is expected to expand from national government organizations to critical infrastructure providers in a sequential manner.
- While cyber attacks are a universal phenomenon seen in various nations, on the other hand, some may have characteristics dependent on circumstances specific to the nation. There is an urgent need to establish a security related system specific to Japan in order to effectively deal with such situations.

[4] Enhancing Cybersecurity for Healthcare and Other Critical Infrastructure Operators

1. Background and Issues

- Need to further enhance critical infrastructure protection based on public-private partnerships by enabling the critical infrastructure sector as a whole to appropriately respond to future threat trends and changes in the environment surrounding systems and assets.
- Particularly, in the healthcare sector, each medical institution has so far voluntarily taken actions based on the "Guidelines for the Safe Management of Medical Information Systems". However, an emergency survey of hospitals conducted after a cyber attack caused a long-term suspension of medical services showed that voluntary measures alone were not sufficient. Therefore, there is a need to strongly promote measures at medical institutions.

2. Summary of Approaches

(1) Method

- ✓ (Critical infrastructure sector in general) Based on the action plan, through the revision of the guidelines for establishing security standards, etc., critical infrastructure operators, etc. should promote efforts to incorporate cybersecurity into their organizational governance, and further promote organization-wide measures including management, CISO, strategic management, and system personnel.
- ✓ (Healthcare sector) Promote consultation services in case of cybersecurity incidents through the "Security Education Support Portal Site for Medical Institutions," and conduct cybersecurity training and awareness-raising activities tailored to the characteristics of system security managers and management of medical institutions based on the "Guidelines for the Safe Management of Medical Information Systems" Version 6.0 (revised on May 31, 2023).

(2) Expected Results and Effects

- ✓ (Critical infrastructure sector in general) Ensure resilience of critical infrastructure services and realize secure and sustainable provision of critical infrastructure services without seriously affecting people's lives, socioeconomic activities, and national security environment.
- ✓ (Healthcare sector) 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 outage of medical services.

■ Key takeaways from the expert members of the Cybersecurity Strategy Headquarters

- (Critical infrastructure sector in general) While the importance of critical infrastructure defense has just been set forth in the Act on the Promotion of Security Assurance through Integrated Economic Measures (Economic Security Promotion Act) and the National Security Strategy, there is a need to enhance cybersecurity measures for critical infrastructure in line with this law and strategy.
- (Medical sector) Considering the recent situation where attacks on medical institutions are becoming common, it is expected that the level of cybersecurity measures for medical institutions as a whole will be raised, as such attacks will have a significant impact on people's lives.

1. Background and Issues

- Amid growing importance of contributing to the peace, stability and security of the international community by ensuring a "free, fair and secure cyberspace," supporting cybersecurity capacity building in countries around the world will not only ensure the stability of the lives of Japanese residents and the activities of Japanese companies that depend on critical infrastructure in the target countries, and promote the sound use of cyberspace in those countries, but also ensure the security of cyberspace as a whole, which in turn contributes to improving the security environment of the world as a whole, including Japan.

2. Summary of Approaches

(1) Method

- ✓ Convene ASEAN-Japan Cybersecurity Policy Meeting (AJCPM)
- ✓ Enhance public-private partnership by holding the 50th Anniversary of ASEAN-Japan Friendship and Cooperation Conference.
- ✓ Conduct various exercises and the Cyber SEA Game (ASEAN Youth Cybersecurity Technical Challenge) at the AJCCBC.
- ✓ Conduct industrial control system cybersecurity exercises for the Indo-Pacific region.
- ✓ Continue enhancement of material supply and technical cooperation through ODA.
- ✓ Support foreign investigative agencies in cooperation with JICA.
- ✓ Consider cybersecurity capacity building support project for Pacific island countries.
- ✓ Enhance support for capacity building in the cyber sector in developing countries, including those in the Indo-Pacific region, through contributions to the World Bank's Cybersecurity Multi-Donor Trust Fund, which is dedicated to supporting cybersecurity capacity building in developing countries.

(2) Expected Results and Effects

- ✓ Rise in the level of cybersecurity capacity of government officials and critical infrastructure operators in the Indo-Pacific region, including ASEAN, can be expected.

■ Key takeaways from the expert members of the Cybersecurity Strategy Headquarters

- Contributing to the enhancement of security capacities in the Indo-Pacific region is an essential activity for maintaining peace and industrial development not only in the region but also in the international community as a whole, and it is important to promote it with strategic intent.
- The National Security Strategy (approved by the Cabinet on December 16, 2022) calls for a fundamental strengthening of defense capabilities against the backdrop of the historical change in the balance of power, particularly in the Indo-Pacific region, and in this connection, points out the need "to promote efforts in four areas: research and development, public infrastructure development, cyber security, and international cooperation to enhance deterrence capabilities of Japan and other countries of the region under interagency framework, and to strengthen total defense posture." This initiative is expected to make a significant contribution to the government's security strategy.
- It is important to continue to enhance cybersecurity capacities in the Indo-Pacific region, including ASEAN, through strengthening public-private partnerships, various exercises and events such as cybersecurity exercises, and support for foreign investigative agencies.

[6] International Collaboration through the Framework of the Quad Senior Cyber Group and the Multilateral Anti-Ransomware Meeting

1. Background and Issues

- In an increasingly digital world with advanced cyber threats, there is an urgent need to take a collaborative approach to enhancing cybersecurity. Within the framework of Japan-US-Australia-India, efforts to strengthen the resilience of critical infrastructure are needed to realize the vision of a free and open Indo-Pacific region.
- In combating ransomware, international cooperation is needed on all elements of the ransomware threat, including collaboration with the private sector to build collective resilience and defense against ransomware, thwarting attacks and pursuing those responsible, and countering illicit financing that supports the attacker's ecosystem.

2. Summary of Approaches

(1) Method

- ✓ Through a Japan-US-Australia-India framework, formulate and implement common principles for critical infrastructure protection and software security for the four countries, and coordinate capacity-building programs and awareness-raising activities in the Indo-Pacific region.
- ✓ In the area of ransomware countermeasures, share our knowledge on public-private partnerships with like-minded countries and participate in discussions on international information sharing.

(2) Expected Results and Effects

- ✓ Through cooperation among Japan, the US, Australia, and India, enhance cybersecurity in the Indo-Pacific countries including the four Quad countries.
- ✓ In the area of ransomware countermeasures, contribute to the promotion of cross-sectoral and international cooperation both domestically and internationally.

■ Key takeaways from the expert members of the Cybersecurity Strategy Headquarters

- It is extremely important for the four Quad countries to cooperate closely in defending cyber infrastructure in the Indo-Pacific. In addition, against illicit financing activities such as ransomware and cryptocurrency crimes that have been rampant in recent years, it is necessary to closely share information and keep pace against common adversaries within the framework of multilateral meetings to achieve lasting freedom and peace. This is an important initiative that is highly anticipated by the international community and the public.
- Recognized the importance of measures that can be taken in cooperation with the Quad nations, especially India.
- It is hoped that, within the Quad framework, the formulation of common principles on critical infrastructure protection and software security will be promoted, as well as knowledge sharing on public-private partnerships and international information sharing among like-minded countries in the countermeasures against ransomware.
- With respect to challenges related to cybersecurity for the Quad nations, coordination of submarine cables and the various digital services that use them is important in meetings in the Pacific, particularly including Japan, Australia, Oceania, and Southeast Asia. The security challenges in this region are significant. Infrastructure development and future planning, not only measures against cybersecurity incidents, shall also be emphasized.

Part 1 (Annex) Achievements of Past Approaches (Legacy) (Summary)

- As a wide range of stakeholders in the cybersecurity field have worked together to establish institutional frameworks and public-private cooperative frameworks, a variety of achievements, including knowledge and know-how gained through these efforts, have been accumulated.
- In considering security measures, **it is appropriate to proceed with such efforts while making use of past achievements**.

【Examples of legacy initiatives】

○ Institutional framework (cybersecurity strategy)

- ✓ Described the conceptual shift from security "cost" to "investment," "functional assurance," and security by design, etc. (2015)
- ✓ Described efforts (Government CSIRT Office), etc., with a view to the success of the Tokyo Olympic Games and subsequent countermeasures (2018)
- ✓ Described "DX with Cybersecurity", strengthening the functions of the National SIRT, and enhancing security measures, etc. (2021)

○ Efforts to ensure the security of government agencies

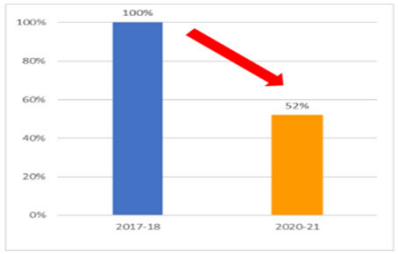
✓Established Common Standards for Government Agencies

- Added independent administrative agencies, etc., to the applicable scope (2016).
- Added robust measures like, CDN, EDR, etc. (2021)

✓Recognized the status of security measures in detail. Conducted advanced management audits and penetration testing.

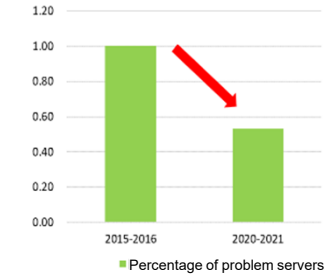
- Ensuring compliance with standards through management audits

Trends in findings on core LAN systems in government agency management audits



- Improvement of vulnerabilities through penetration testing

Trends in the percentage of problem servers in government agency penetration testing



○ Efforts to ensure security in critical infrastructure sector

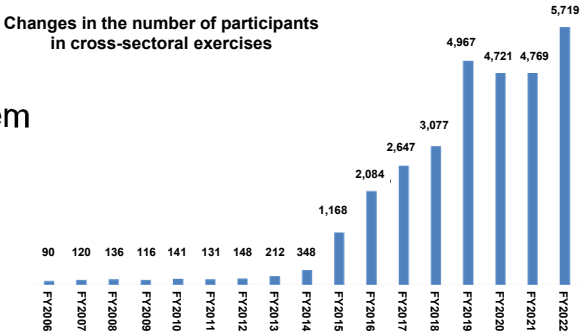
✓Established Critical Infrastructure Action Plan

- Added chemical, credit, and petroleum sectors (2015)
- Added airport sector (2017)
- Described promotion of efforts on secure and sustainable provision based on the concept of mission assurance, through public-private sector collaboration (2022)

✓ Realization of robust information sharing among related entities through "cross-sectoral exercises" CEPTOAR, ISAC, etc.

- Improvement of the problem response structure through "cross-sectoral exercises" (2006-)

Changes in the number of participants in cross-sectoral exercises



Part 1 and Part 2: The Status of Cybersecurity

Increasing dependence on cyberspace in socioeconomic activities and people's lives

Expanding use of cloud computing and other services in system construction and operation, diversification and complexity of supply chains, and development of new technologies and services through digitalization.

Increasing severity and sophistication of cyber attacks

Increase in the number of victims of ransomware (146 cases in FY2021, 230 cases in FY2022), resumption of Emotet activities and expansion of infection through new methods, increase in attacks suspected of state involvement and targeted attacks.

Enhancing Socio-economic Vitality and Sustainable Development

Management's perceptions of corporate governance

- No significant change in the perception of the management of domestic companies.
  Example: The majority of respondents answered that "Efforts are mainly entrusted to IT and other departments
- Compared to other countries, there exists a gap in awareness between management and IT departments.
  Example: "Top-down instructions from management triggered the implementation of countermeasures": 50% in the U.S. and 20% in Japan. ・
- Overseas, security risks have moved from an era in which they are assessed by the company itself to an era in which they are assessed by external parties as well.

Important to make management "aware" of the need for measures to raise awareness.

SMEs and supply chain measures

- No significant change in the implementation status of measures by SMEs.
  Example: Approximately 40% of respondents answered that they “do not feel the need for cybersecurity measures.
- About half of the victims of ransomware, which continues to increase, are SMEs.
- The presence of SMEs with insufficient countermeasures in their supply chains is a risk.

- Particularly need to provide support services and enhanced functions for SMEs.
- Need to strengthen security from a technological perspective to ensure a secure supply chain.

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

Situation at each entity supporting economic and social infrastructure

(1) Government agencies, etc.

- Number of incidents increasing year by year.
  (117 in FY2020, 207 in FY2021, 266 in FY2022)
- GSOC's provision of vulnerability information to government agencies increasing as well.
  (381 cases in FY2020, 598 cases in FY2021, 630 cases in FY2022)

- Need close cooperation between the first and second GSOCs.
- Need to work on collection and analysis of security information using government terminal information, etc.

(2) Critical infrastructure

Numerous cases of system failures and information leaks occurred in critical infrastructure sector in Japan and abroad.
Examples: Ransomware attacks on medical institutions, etc., and communication failures.

- Important to develop a BCP that assumes damage from cyber attacks.
- Need to assess the effectiveness of the BCP.

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

Need to take the initiative in maintaining and improving their security standards, taking into account their unique characteristics.

(4) Utilization of knowledge learned from the Tokyo Olympics and Paralympics

Important to utilize the knowledge learned for the G7 Hiroshima Summit and Osaka/Kansai Expo.

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

International trends (other foreign countries)

US
- Released the Biden administration's first "National Cyber Security Strategy" in March 2023.
- Promotion of measures based on the Critical Infrastructure Cyber Incident Reporting Act (enacted in March 2022)

UK
Established the National Cyber Advisory Board (NCAB) based on the "National Cyber Strategy 2022" and held its first meeting (November 2022)

EU
NIS2 Directive, which strengthens the power and oversight of the authorities, comes into effect (January 2023)

AUS
Cyber attacks on major telecommunications and other companies resulted in large-scale leaks of personal information and other data (October-November 2022)
Announced a review of Australia’s Cyber Security Strategy (December 2022)

CHN
Published White Paper on International Cooperation in Cyberspace (November 2022)

International cooperation is essential. Will work to strengthen it based on trends in each country.

Cross-Cutting Approaches to Cybersecurity

Research and development in the cybersecurity sector

In addition to the spread of generative AI, as the scope of national security has expanded to include the cyber sector due to the growing complexity of the international situation in recent years, the importance of research and development as a foundation for cyberspace safety and security is increasing further.
Example: the National Cyber Strategy of the U.S. calls for a national initiative in research, development, and demonstration for proactive risk prevention and mitigation.

- Considered a system for building an industry-academia-government ecosystem from the viewpoint of broadening the scope of research, and studied practical R&D concepts.
- Taking into account medium- to long-term technological trends, such as quantum technology, etc.

Human resources specializing in IT and cybersecurity

- In addition to the growing demand for human resources, as companies and organizations promote DX, demand is increasing for reskilling of human resources who do not have knowledge and work experience at this point in time.
- In the "Comprehensive Strategy for the Digital Rural City National Concept," proposed the development of 2.3 million digital human resources, including cybersecurity personnel, by the end of FY2026.

Need to enhance approaches for improving the environment for acquiring skills, raising awareness at the management level through "plus security," etc., and strengthening initiatives at universities, colleges of technology (KOSEN), etc.

Public awareness and behavior

While digitalization progresses steadily, a rising percentage of people feel insecure when using the Internet.
Example: Reached record number of consultations related to "support fraud" in January 2023 (IPA).

- Need for cybersecurity measures requires a more detailed approach according to the target of the message, as well as close cooperation and collaboration among various entities.
- Need to continue to promote awareness-raising 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	Cybersecurity Measures for Local Communities and SMEs	Ensure Reliability of Supply Chain, etc.
➢ Revised "Cybersecurity Management Guideline" to clarify roles and responsibilities for supply chain risks. ➢ Released a model curriculum to supplement "Plus Security" knowledge for management level. ➢ Compiled and published "Guidance for Sharing and Publicizing Information on Cyber Attack Damage".	➢ Conducted industry-government-academia collaboration training and incident exercises by local SECUNITY. ➢ While publicizing the "SECURITY ACTION" system, expanded its subsidies. ➢ Promoted dissemination of the "Information Security Measures Guideline for SMEs" and revised them based on the establishment of the "Cybersecurity Supporters Services", etc.	➢ Conducted demonstration experiments for the use of SBOM as a table of software components. ➢ Promoted R&D and social implementation of "Cyber-Physical Security Measure Foundation" for assuring the security of IoT systems and building a trust list for supply chains, etc. ➢ Analyzed attack information and conducted human resource development by utilizing NICT's "CYNEX".

Evaluation

- Need further efforts to raise awareness of the importance of cybersecurity from the perspective of corporate governance given concerns about further increase in the risk of attack damage in the future due to the expansion of supply chain risks.
- Need to encourage the spread of initiatives through regions and supply chains, as well as to address the risk of unintentional leakage of information assets due to inadequate settings, etc.
- Need to continue to develop various initiatives such as horizontal deployment of industry-specific practices, establishment of infrastructure that serves as a node for industry-academia-government, and creation of standards and specifications based on a framework that addresses both cyber and physical aspects.

Examples of efforts this year

➢ Support private sector initiatives based on the "Cybersecurity Measures Information Disclosure Guidance". ➢ Promote studies to strengthen the positioning of cyber security management as a part of corporate governance through cooperation among relevant ministries and agencies.	➢ Spread awareness to promote the use of "Cybersecurity Supporters Services". ➢ Promote guidelines for users and providers regarding appropriate settings for cloud services. ➢ Disseminate "Internet Safety and Security Handbook Ver 5.00 <excerpt for small and medium-sized organizations>". ➢ Support for further strengthening of local SECUNITY.	➢ Study on SBOM vulnerability management and introduction of SBOM to the information and telecommunications sector. ➢ Add "Device Verification Service" to the Information Security Service Examination and Registration System. ➢ Establish systems and formulate communities for this year's operational launch of NICT's CYNEX.

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

Examples of efforts last year

Integrated advancement along with building a safe and secure environment and digital transformation	Government agency efforts	Critical infrastructure efforts
➢ Enhanced national SIRT functions and strengthened measures for preventing damage, including compilation and publication of "Guidance for Sharing and Publicizing Information on Cyber Attack Damage". ➢ Established the Cyber Affairs Bureau and National Cyber Unit (NPA) ➢ Revised the "Guidelines for the Safe Management of Medical Information Systems" version 6.0 ➢ Started services related to moving procedures and online application for passports through Mynaportal	➢ Started operations of the evaluation mechanism for SaaS with low security risk (ISMAP-LIU) and revised the "SBD Manual" based on the revision of the Common Standards for Government Agencies. ➢ Established the "Guidelines for External Services" was established in light of the increased use of external services such as SNS by government agencies, etc. ➢ Conducted studies on the further expansion and upgrading of GSOC's monitoring infrastructure and on the construction of the next GSOC system.	➢ Established "Action Plan for Cybersecurity of Critical Infrastructure". ➢ Conducted studies to revise the guidelines for establishing security standards, etc. from the perspective of organizational governance and supply chain risk, etc. ➢ Further improved the information sharing posture using the "Information Sharing Guide". ➢ Conducted "cross-sectoral exercises" related to response to ransomware attacks, etc.

Evaluation

➢ Toward the safe and secure use of cyberspace, need to conduct multilayered cybersecurity measures from all perspectives, including information dissemination, technological infrastructure, and capacity building and awareness-raising, as well as continuing self-help, mutual aid, and public assistance by all entities involved in cyberspace.

➢ Need to promote initiatives to ensure the security of government information systems, such as enhancement of the ISMAP cloud service list and studies to rationalize the operation of the system.

➢ In light of the increased use of external services such as cloud services and social networking services, government agencies as a whole have further raised the level of cybersecurity measures by developing common standards and implementing necessary improvements through audits and other means.

➢ Need to continue active efforts by relevant ministries and agencies to further promote actions based on the Action Plan for Critical Infrastructures.

Examples of efforts this year

➢ Strengthen cooperation with various domestic and foreign entities by the Cyber Affairs Bureau and National Cyber Unit. ➢ Conduct proactive information dissemination and information sharing, such as alerting financial institutions and users. ➢ Conduct studies on submitting a bill to expand and extend "NOTICE" project ➢ Prepare the posture and environment to strengthen national SIRT.	➢ Conduct studies to revise Common Standards for Government Agencies and individual manuals based on new security measures required for government information systems. ➢ Continue studies for the establishment of the next GSOC system. ➢ Collect cybersecurity information on government devices using domestic security software, and consolidate and analyze the information at NICT's CYNEX.	➢ Revise guidelines for establishing security standards, etc. ➢ Continue efforts related to the 5 groups of measures (e.g., strengthening the information sharing posture) based on the Action Plan. ➢ Consider revision of relevant guidelines in the water supply and financial sectors, etc.

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
➢ Adopted "G7 DFFT Action Plan" to continue concrete efforts for the promotion of DFFT (Data Free Flow with Trust) at the G7 Digital Ministerial Meeting in 2022. ➢ Contributed actively to discussions at the UN Open-Ended Working Group (OEWG). ➢ Deepened cooperation with the G7 and other countries in law enforcement, and strengthened collaboration in bilateral criminal assistance treaties, etc.	➢ Ensured national resilience by expanding the capabilities of the SDF's protective systems and promoting the protection of advanced and defense-related technologies. ➢ Formulated and published the "National Security Strategy" and implemented initiatives to fundamentally strengthen cyber defense capabilities. ➢ Collected and analyzed information on suspected state involved cyber attacks, and alerted targeted business operators.	➢ Implemented measures to strengthen countermeasures under the "Quad Cybersecurity Partnership: Joint Principles" adopted at the Japan-U.S.-Australia-India Summit. ➢ Promoted multilateral cooperative efforts to combat ransomware, including participation in the 2nd multilateral conference on Counter Ransomware Initiative (CRI). ➢ Supported developing countries based on the "Basic Policy on Capacity Building Support for Developing Countries" in the area of cybersecurity.

Evaluation

➢ Need to further deepen discussions on international rules and norms through participation in discussions at UN OEWG meetings, etc.
➢ Need to deepen cooperation by linking efforts for knowledge sharing and capacity building support through international cooperation and collaboration to the expansion of the number of nations to the Convention on Cybercrime.
➢ Need to continue to strengthen Japan's defense, deterrence, and situational awareness in light of the diversification and complexity of threats in cyberspace.
➢ Need to expand the range of countries with which Japan has a relationship of trust, and to deepen the relationship with countries with which Japan already has a relationship of trust.
➢ Regarding capacity building support, need to expand the scope of support with a focus on the Indo-Pacific region, and to respond strategically through public-private partnership.

Examples of efforts this year

➢ Contribute to ensuring a free, fair and secure cyberspace through bilateral and multilateral consultations, UN OEWG, etc.

➢ As the chairing country of the G7, promote further strengthening of international cooperation through opportunities such as the High-Tech Crime Sub-Group Meeting. ➢ Actively participate in discussions on the UN Convention on Cybercrime in cooperation with relevant countries.	➢ In light of increasing security risks, continue to promote efforts to ensure national resilience against cyber attacks and to improve defense, deterrence, and situational awareness.	➢ Strengthen ASEAN-Japan relations in light of the 50th anniversary of ASEAN-Japan friendship and cooperation. ➢ Conduct studies on ways to support capacity building in Pacific island countries by leveraging ASEAN's expertise. ➢ Continue to strengthen relationship with major allies and like-minded countries such as the U.S., U.K., and Australia.

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	➢ In the vision (primary) for Key and Advanced Technology R&D through Cross Community Collaboration Program(K Program), indicated that the verification technologies of malicious functions, etc. would be supported on the "Transverse and Cyberspace Domain". ➢ Revised the CRYPTREC ciphers list.	➢ Developed "A Sample Curriculum for Plus Security Knowledge Supplement Course" ➢ Implemented "CYDER" after reorganizing the course according to the needs of the participants, etc. ➢ Defined the image of government digital human resources in government agencies, and organized the contents of training and certification examinations.	➢ Added a course on cybersecurity to the "Digital Utilization Support Promotion Project," which conducted seminars for the elderly, etc. ➢ Created teaching materials for instruction and conducted seminars for entities implementing dissemination and awareness-raising activities. ➢ Reviewed the "Cybersecurity Awareness and Action Enhancement Program".
Evaluation	➢ Need to combine the perspectives of both practical R&D and the industry-academia-government ecosystem, including from the perspective of security ➢ Need to capture medium- to long-term trends and work on them without being preoccupied with short-term results.	➢ Given the increasing need for expert human resource, need to continuously improve the environment for human resource development and to broaden the base of human resources. ➢ In light of the frequent attacks on government agencies, need to strengthen efforts to secure and train government digital human resources.	➢ Based on the demographic expansion of participants in cyberspace, need to review the "Awareness and Action Enhancement Program" based on the follow-up of the efforts, including measures for the elderly, children and families, as well as to focus on and strengthen efforts based on the program.
Examples of efforts this year	➢ Spread awareness of the "5G Security Guideline" and consider its revision. ➢ Identify issues related to understanding the actual situation of smartphone application behavior contrary to user intentions. ➢ Monitor cryptographic techniques on the CRYPTREC ciphers list, etc.	➢ Work on promotion of "Plus Security" in collaboration with SC3. ➢ Conduct efforts on dissemination and development of a model curriculum for universities and colleges of technology (KOSEN) ➢ Implement public vocational training based on the "Comprehensive Strategy for the Digital Rural City National Concept". ➢ Review training, etc. for government digital human resources based on the "Priority Plan for the Realization of a Digital Society".	➢ Conduct measures in cooperation with relevant ministries and agencies to steadily implement the "Awareness and Action Enhancement Program". ➢ Promote the use of various contents such as "9 Articles on Cybersecurity Measures" and "Internet Safety and Security Handbook".