NISC

National center of Incident readiness and Strategy for Cybersecurity

Overview of Cybersecurity 2022

June 17, 2022

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

Part 1: Executive Summary

- This annual report summarizes the efforts made each fiscal year to be reflected in the annual plan for the next fiscal year, as set forth in the Cybersecurity Strategy.
- For this year's report, we added an executive summary at the beginning to clarify the challenges surrounding cyberspace and how they will be addressed. To reinforce the information provided, we also stated challenges in light of recent international affairs and the measures that the Strategic Headquarters will particularly focus on.

1. Major changes in circumstances surrounding cyberspace and the current situation

- Spread of the "new normal" triggered by the pandemic
- Advancement of digital transformation (DX)
- Growing cyber risks due to changes in international affairs

⇒

- Various incidents occurring in Japan
  - ✓ Increasing damage caused by ransomware
  - ✓ Increasing damage caused by Emotet

2. Policy issues emerging in the wake of changing circumstances

(1) **Prevention of incidents** to address growing threats in cyberspace

(2) **Security enhancement and support for local companies, SMEs, etc.** to counter the spread of risks as a result of positioning cyberspace as a public space, and ensuring the overall safety and security by **strengthening measures against cybercrimes**

(3) **Strengthening international cooperation and collaboration** amid the growing severity of the security environment

3. Measures of particular focus for ensuring "a free, fair and secure cyberspace"

1) An all-Japan implementation framework for public-private collaboration (enhancement of national CERT/CSIRT functions)
Increase information collection and analysis capabilities and strengthen information sharing systems between the public and private sectors to help prevent incidents

2) Enhancement of cybersecurity in the private sector, including critical infrastructure operators
Advance initiatives based on the "The Cybersecurity Policy for Critical Infrastructure Protection," ensure resilience of cyber infrastructure, etc.

3) Cybersecurity measures tailored to the integration of cyberspace and physical space
Advance initiatives designed to facilitate the adoption of software bill of materials (SBOM*) for managing vulnerabilities in software, etc.

4) Cybersecurity measures for local companies and SMEs
Raise awareness of business managers, promote activities of regional security communities (regional SECUNITY) advancing local mutual-help initiatives, and promote “cybersecurity supporters services” for SMEs

*SBOM: Software Bill Of Materials

5) Advancement of public-private and international collaboration through the establishment of the Cyber Affairs Bureau and the National Cyber Unit within the National Police Agency
Properly address the increasingly serious threats in cyberspace to ensure safety and security

6) Advancement of capacity building support in the Indo-Pacific region
Further advance capacity building support in the Indo-Pacific region through exercises, etc. for the government agencies including ASEAN member states

Realize "a free, fair and secure cyberspace" set forth in the Cybersecurity Strategy **(approved by the Cabinet on September 28, 2021)**

[1] Enhancement of National CSIRT/CERT Functions

1. Background and Issues

- Growing need for the national government to actively implement comprehensive cyber defense against serious cyberattacks, in collaboration with relevant agencies.
- Need to enhance the national CSIRT/CERT framework as a function for managing comprehensive coordination to advance efforts in an integrated manner, ranging from information collection and analysis to investigation, evaluation, issuing alerts, and handling incidents.

2. Overview of Efforts

① Approach

✓ Establish an adequate system:

[NISC] Enhancement of the system from the perspectives of information collection and sharing, aggregation and analysis, incident handling and coordination, etc.
Collaboration and coordination with policy goals, including diplomacy and national security.

[Ministries] Establishment and enhancement of the functions of CSIRTs for own organization and relevant agencies.
Enhancement of support functions for cyber defense in the industries and fields the ministry oversees.

[Entire government] Establishment of a close collaborative system between NISC and relevant ministries.

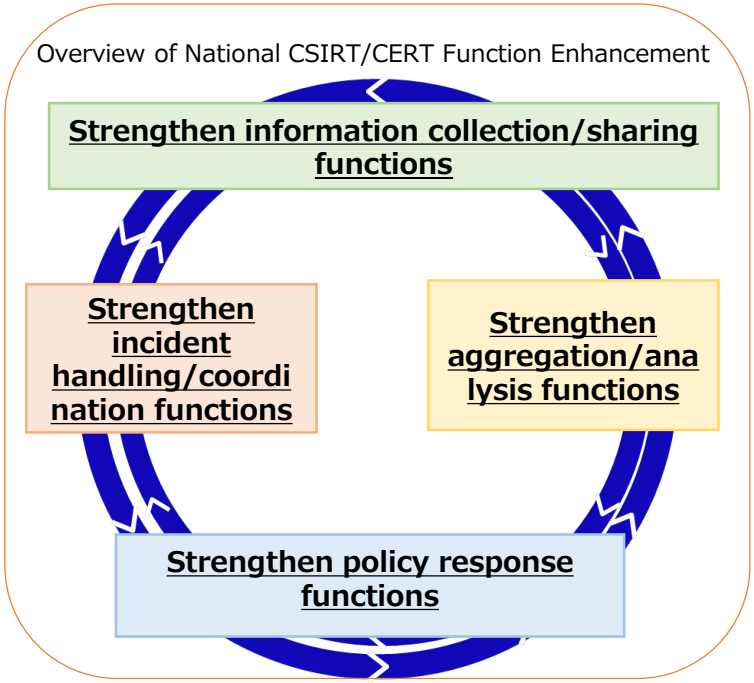
✓ Create an environment:

○ Advancement of information sharing between the public and private sectors, including critical infrastructure operators as well as other private sector players (e.g., enhancement of the Cybersecurity Council through the integration of JISP, which is a legacy of the Tokyo Games).

○ Meeting of the "Investigative Commission on the Guidance for Sharing and Announcing Information concerning Damage from Cyberattacks".

② Expected results and effects of the efforts

✓ Ability to rapidly collect information and ascertain damage as needed, greater validity and coverage of information provided, precise response tailored to the nature and severity of attacks, etc.



■ Key feedback from experts of the Cybersecurity Strategic Headquarters

- Development of a comprehensive cyber defense is essential for Japan from the perspectives of national security and increasing cybersecurity capabilities.
- Stronger international collaboration is expected, including the establishment of a system for communicating Japan's stance to audiences both at home and abroad, while engaging in real-time exchange of information and building close relationships with related organizations overseas.
- National CSIRT/CERT is expected to serve as trusted sources of information and contact points for reporting information.
- It should be possible to establish a flexible system that can immediately respond to changes in circumstances, with the entire government, companies, and the people playing their respective roles.

[2] Practical Application of Cyber/Physical Security Framework (CPSF)

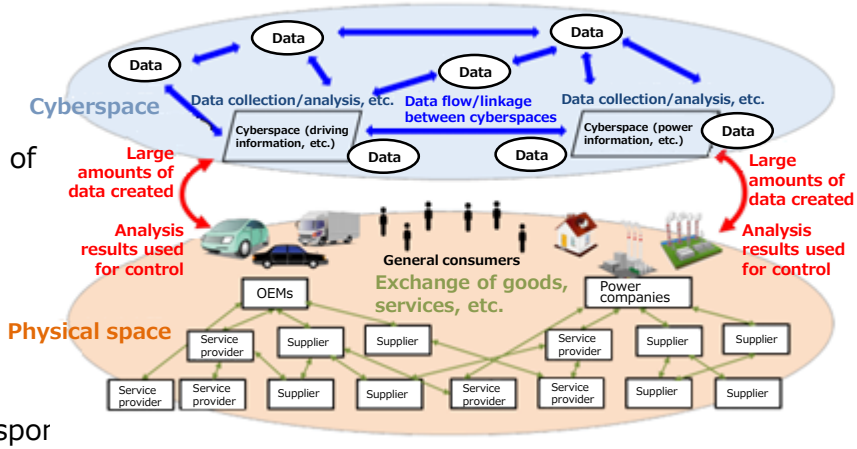
1. Background and Issues

- A framework needs to be created for practical application to address the threats of cyberattacks that are increasing due to the integration of cyberspace and physical space.

2. Overview of Efforts

① Approach

- ✓ Advancement of activities to raise awareness about CPSF and related frameworks, international standardization, cooperation with related organizations and companies, etc.
- ✓ [OSS] Widespread adoption of OSS case studies.
  [SBOM] Advancement of deliberations toward the establishment of effective utilization models for sharing SBOM, know-how, etc. aimed at the promotion of SBOM, which is useful for quickly addressing vulnerabilities and organizing information needed for software management, including vulnerabilities and licenses.



② Expected results and effects of the efforts

[Ongoing measures]

- ✓ Greater understanding of cyber/physical systems, and increased ability to respor to risks that arise as a result.
- ✓ The newly acquired ability to identify stakeholders, visualize risks, share countermeasures, and organize the separation of responsibilities concerning data, as well as the clarified roles of stakeholders, contributes to the free flow of data and an increase in new added value.

■ Key feedback from experts of the Cybersecurity Strategic Headquarters

- It is clear that once a vulnerability is found in software, nearly all societies are significantly impacted. To minimize economic losses that result from addressing such incidents, it is necessary to raise the level of security through the practical application of CPSF.
- Considering the introduction and promotion of SBOM is an issue that needs to be advanced as a member of the international community without lagging behind other states (especially the United States). It is necessary to position SBOM as part of Japan's international standardization strategy, anticipating that it will become an international standard in the future, and steadily work to organize knowledge related to SBOM and create tools including transaction models.

[3] Promotion of Cybersecurity Measures by Local Companies and SMEs

1. Background and Issues

- Cyberattacks targeting vulnerable parts of supply chains and affecting the entire supply chains are emerging as a new type of threat. Local companies and SMEs must urgently introduce security measures from the perspective of economic security as well.
- Widespread adoption of security measures by local companies and SMEs is also an essential aspect in realizing the Vision for a Digital Garden City Nation.

2. Overview of Efforts

① Approach

- ✓ Promotion of cybersecurity supporters services that provide SMEs with all the necessary measures in a single package, utilizing IT introduction subsidies and other support measures, and also collaborating with the Supply-Chain Cybersecurity Consortium (SC3).
- ✓ Promotion of activities of regional security communities (regional SECUNITY) advancing local mutual-help initiatives.

② Expected results and effects of the efforts

- ✓ Prevention of the occurrence and spread of damage from cyberattacks among many SMEs.
- ✓ Dissemination of information that local companies need, and facilitating the resolution of issues faced by local regions, including the lack of security talent.
- ✓ Promotion of cybersecurity enhancement for the whole industry through collaboration with the industry-led SC3.

■ Key feedback from experts of the Cybersecurity Strategic Headquarters

- Improving the security of local companies and SMEs, which underpin Japan's industry, is an urgent issue. Local companies and SMEs that lack human and financial resources are often unable to take adequate security measures on their own. From the perspective of economic security as well, efforts need to be advanced in this regard with clear objectives and strong support from the government.
- Local regions are moving forward with new initiatives using digital technology to realize the Vision for a Digital Garden City Nation, and security measures tailored to these initiatives (e.g., security by design) are essential.
- Efforts should be made to raise the level of cybersecurity literacy among local companies and SMEs by providing easy-to-understand information and implementing policies to support the accelerated introduction of measures.

[4] Promotion of Public-Private and International Collaboration through the Establishment of the Cyber Affairs Bureau and the National Cyber Unit

1. Background and Issues

- To secure the safety and security of cyberspace, the police need to team up with a wide range of stakeholders in and outside Japan, in addition to enhancing readiness to properly address threats in cyberspace that are becoming increasingly serious, and powerfully advance initiatives to improve cybersecurity with the whole society working together.

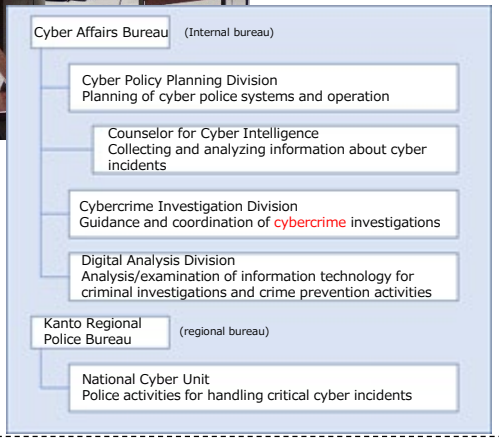
2. Overview of Efforts

① Approach

- ✓ Establish the Cyber Affairs Bureau within the National Police Agency, collaborate with other NPA bureaus and various stakeholders in and outside Japan, and have the Cyber Affairs Bureau play a central role in advancing cyber policies.
- ✓ Establish the National Cyber Unit within the Kanto Regional Police Bureau to handle critical cyber incidents, including active participation in international joint investigations with foreign investigation agencies, etc.

② Expected results and effects of the efforts [new measures]

- ✓ Through this initiative, team up with a wide range of stakeholders in and outside Japan, in addition to enhancing readiness to properly address threats in cyberspace that are becoming increasingly serious, and powerfully advance initiatives to improve cybersecurity with the whole society working together.



■ Key feedback from experts of the Cybersecurity Strategic Headquarters

- Cyberattacks target all types of stakeholders, whether public or private sector organizations or individuals, and they are borderless. Cybercrimes are sophisticated crimes that are extremely difficult to handle compared to conventional crimes, in that anyone can become a victim and attacks can be launched from anywhere. As such, public-private and international collaborations must be powerfully advanced.
- This initiative is important in raising the level of Japan's cybersecurity and particularly its attribution, and smooth progress can be expected in international joint investigations with foreign investigation agencies.
- In terms of international collaboration, it is essential to actively promote diverse talent and possess information sources unique to Japan.

[5] Advancement of Capacity Building Support in the Indo-Pacific Region

1. Background and Issues

- It is necessary to assist capacity building in other states to help ensure the stability of the lives of Japanese residents and the activities of Japanese companies in other countries that depend on critical infrastructure in recipient countries and to promote the development of the sound use of cyberspace and the security of the entire cyberspace.

2. Overview of Efforts

① Approach

- ✓ **ASEAN-Japan Cybersecurity Policy Meeting**
  Discussion of measures for capacity building support with ASEAN member states and secretariats, and coordination with related organizations.
- ✓ **Various Exercises at AJCCBC**
  At the ASEAN-Japan Cybersecurity Capacity Building Centre (AJCCBC) in Thailand, conducting exercises such as Practical Cyber Defense Exercise for government officials and operators of critical infrastructure in ASEAN member states ~~Using the ASEAN-Japan~~
- ✓ **Industrial Control System Cybersecurity Exercises for the Indo-Pacific Region**
  The Japanese Ministry of Economy, Trade and Industry, IPA, the United States, EU, and others have collaborated to conduct exercises.
- ✓ **Support for Foreign Investigation Agencies, etc. in Collaboration with JICA**
  Support provided to ODA-eligible countries in collaboration with the Japan International Cooperation Agency (JICA).

② Expected results and effects of the efforts

- ✓ Increased capabilities of government officials and critical infrastructure operators in the Indo-Pacific region.

Basic Policy on Cybersecurity Capacity Building Support for Developing Countries (Outline)
(Approved by the Cybersecurity Strategic Headquarters in December 2021)

(i) Reducing cybersecurity risks to countries around the world
(ii) Ensuring stable activities of Japanese residents and companies
(iii) Obtaining general understanding of Japan's position based on the basic principles of the free flow of information and the rule of law
(iv) Developing a foundation for Japan's industry and others to operate locally in those states
(v) Contributing to Free and Open Indo-Pacific and other policies

Engage in close collaboration between relevant ministries and the public and private sectors to provide effective support according to the diverse needs of developing countries

■ Key feedback from experts of the Cybersecurity Strategic Headquarters

- Raising the security level of the relevant states included in the supply chain is essential. To build a foundation for the future development of Japan's industry, Japan should exercise leadership in the security field while fostering positive relationships with the CSIRTs and security engineers of the states in the Indo-Pacific region in particular, with which Japan is expected to develop closer economic ties, and provide active support to help increase security capabilities in the region.
- Building stronger relationships with like-minded countries can be an important form of international contribution that helps increase national security in the relevant regions, and it is also a vital initiative for Japan's cyber defense.
- Japan should strive to build relationships with other states to enable close collaboration, using its own unique approach including original training programs.

Part 2 Circumstances Surrounding Cybersecurity

- **The circumstances surrounding cybersecurity are summarized in line with items of the Cybersecurity Strategy ("the Strategy")**
- **The Strategy provides further details on such topics as raising executive awareness about cybersecurity, changing national security environment, application of knowledge gained through efforts toward the Tokyo 2020 Olympic and Paralympic Games, research and development, human resources development, and literacy, as well as a summary of cybersecurity incidents that occurred in FY2021**

Enhancing Socio-Economic Vitality and Sustainable Development

Executive Awareness from the Perspective of Corporate Governance

- No major change in the awareness of cybersecurity among executives at Japanese companies.
  Ex. Companies that deliberate cybersecurity in management meetings, etc. have remained in the 30% range since 2014
- There is a wide gap in executive awareness compared to other countries.
  Ex. Executives give directions to take measures at 55% of the companies in the US, and 22% in Japan
- Damage caused by ransomware, which forces the victims to make a decision regarding monetary payments, is growing.
  Ex. 146 cases of damage were reported to the police in 2021, with the number in the second half increasing fourfold year on year

⇒Information on damage and measures is not shared inside and outside companies (including communication with investors), and critical risks may be overlooked.

Measures for SMEs and Supply Chains

- No major change in the status of measures taken by SMEs.
  Ex. About 20% of the companies say they have never felt the need for cybersecurity measures
  (no major change from the survey five years ago)
- In addition to the problem of awareness and literacy to begin with, lack of progress in mandating or requesting outsourcing companies and suppliers to implement cybersecurity measures has been pointed out as the reason for this.
  Ex. Issues at the time of request included the burden of costs required to implement measures (57%), and infringement of subcontractor laws, etc. (19%)
- In Japan, there have been incidents affecting business operation, such as the case where a subcontractor of a major corporation was subjected to attack and led to suspension of the entire supply chain.

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

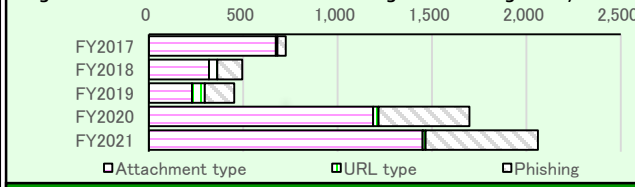
Increasingly Advanced and Sophisticated Attacks against Government Agencies, etc.

Greater numbers of software are used with the spread of telecommuting at government agencies, etc., leading to an increase in the number of information provided about vulnerabilities, etc. that need to be addressed urgently (Figure 1). As for malicious email in FY2021, attachment types and phishing were seen in great numbers as in FY2020, owing to the activities of Emotet malware (Figure 2).

Figure 1 Number of software vulnerability information provided by GSOC*5

Fiscal Year	FY2018	FY2019	FY2020	FY2021
Number of information provided	290	284	381	598

Figure 2 Trends in malicious email sent to government agencies, etc.



Cybersecurity Incidents

- Colonial Pipeline's system suspension due to ransomware attack (May 2021)
- Suspension of local government services due to cloud service failure (September 2021)
- Intermittent system failures at a financial institution (until February 2022)
- Spread of Emotet malware infections (February 2022 onward)
- Submarine cable damaged due to undersea volcanic eruption in the Tongan Archipelago (January 2022), etc.

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

International Developments

US

The Biden Administration positions cybersecurity as a top priority affecting national security

- Executive Order on improving the nation's cybersecurity issued (May 2021)
- The Joint Cyber Defense Collaborative (JCDC), a framework for information sharing between the public and private sectors, established (August 2021)
- Bill to require the private sector to report cyber incidents to the government passed (March 2022)

UK

- National Cyber Strategy 2022 announced (December 2021)
  Vision: Presented five pillars, including building a resilient and prosperous digital UK, and taking the lead in the technologies vital to cyber power

EU

- Amendments to the NIS2 Directive adopted (December 2021)
  * Established a baseline for mandating the reporting of cybersecurity risk control measures for all sectors covered by the Directive

AUS

- Security Legislation Amendment Act 2021 (December 2021, March 2022)
  * Expanded the definition of critical infrastructure, registered critical infrastructure assets covered by the expansion, and defined incident reporting obligations and government support measures for said assets

CHN

- It is assessed that China presents the broadest, most active, and persistent cyber espionage threat to US government and private sector networks
  * As per the 2022 Annual Threat Assessment of the U.S. Intelligence Community

Cross-Cutting Approaches to Cybersecurity

Research and Development in the Cybersecurity Field

- The United States, China, and Germany continue to lead in the number of paper presentations at top conferences. Ex. There were six papers that included Japanese research institutions
- However, Japan showed some presence at cryptographic research conferences. Japanese research institutions are also involved in NIST's selection work toward standardization of post-quantum cryptography (currently in round 3).
- In Japan, as well as in other countries, progress is seen in moves toward research and development funding that is expected to be used in the cybersecurity field.

Human Resources Specializing in IT and Cybersecurity

- In the digital field, particularly the cybersecurity field, there is growing demand for the reskilling of human resources that currently do not have relevant expertise or work experience, in addition to demand for securing human resources.
  Ex. Digital skills sought by employers: cybersecurity ranks 2nd (39%)
- On the other hand, human resources investment in areas other than OJT tends to lag in Japan, not just in these fields. Awareness is an issue for both employers and workers.
  Ex. Percentage of individuals who do not engage in learning activities outside the company or personal development: 46%
  Workers: Too busy working (55%), too expensive (29%), too busy with housework and childcare (25%)
  Employers: Interferes with core business (57%), training content is not practical (24%)

Awareness and Behavior of the People

- Demographics of participants in cyberspace have expanded to include the elderly and children in particular. On the other hand, there may be some people who use the internet without knowing it.
- Based on these trends, recent threat trends have also changed. In particular, phishing attacks targeting the elderly have increased sharply. Anxiety is growing as well.
  Ex. Number of reports to the consumer hotline regarding fake SMS delivery attempt notification: 2019⇒2020 (Percentage aged 70+)
  3,800⇒8,500 (18%⇒28%)
- The methodology needs to be deliberated with regard to the elderly and children, as they differ in terms of family involvement, experience taking ethics education, and the media they use.

Part 3 Results and Evaluation of Efforts in FY2021 Based on the Strategy, and Efforts in FY2022 (1/5)

1. Enhancing socio-economic vitality and sustainable development—Advancing DX with Cybersecurity

* Establishment and improvement of literacy is discussed in 4.

Examples of efforts in FY2021

Raising executive awareness

- Released the online version of the Management Visualization Tool
- Incorporated the need for cybersecurity measures in an appendix to the Tokyo Stock Exchange's Corporate Governance Code
- Incorporated the topic in the Digital Governance Code, and used it as criteria for the DX Certification, DX Stocks, and Noteworthy DX Companies (incentive)

Measures by local regions and SMEs

- Working in collaboration with the Supply-Chain Cybersecurity Consortium (SC3), strengthened measures by SMEs, communicated information to executives, promoted industry-academia-government collaboration, and promoted the formation of regional SECUNITY.
- Launched the Supporter Service Review Registration System (registered 12 services). Recommended its use in SC3.
- Positioned "Security Action" as an application requirement for subsidies for SMEs (incentive)

Ensuring trustworthiness of supply chains, etc.

- Developed a data management framework
- Issued an international standard for IoT based on an approach developed in Japan

Evaluation

As the risk of damage from cyberattacks continues to grow, radical efforts to raise the awareness of the importance of cybersecurity in corporate governance are required as a precondition for further advancing the above efforts.

In addition, from the perspective of further advancing the spread of measures through supply chains and local regions, it is necessary to develop and promote the use of resources (e.g., broad application of leading practices, guidelines) that will serve as references in advancing efforts on the ground.

New Efforts in FY2022

- Revise the " Cybersecurity Management Guidelines " in light of the progress of various efforts related to the commitment of executives, including the establishment of the "Guidance for Sharing and Announcing Information concerning Damage from Cyberattacks" and revision of the "Guideline for Establishing Safety Principles for Ensuring Information Security of Critical Infrastructure"
- Relevant ministries and agencies will collaborate and discuss how to reinforce the positioning of cybersecurity management
- Support the cybersecurity measures of SMEs, etc. to ensure the stable supply of goods and services is not disrupted [economic measure]
- Clarify the relevant laws and regulations that apply to the support (support for the use of Supporter Services, funded by IT introduction subsidies) and request for measures by suppliers [economic measure]
- Support the enhancement of regional SECUNITY and release a map that visualizes its existence
- Establish user and provider guidelines for the proper configuration of the cloud
- Create a system for visualizing reliable verification providers
- CYNEX: Deepen domestic analyst community relationships and build trust (go live in FY2023)

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

Examples of efforts in FY2021

Integrated advancement along with building a safe and secure environment and digital transformation	Government agency efforts	Critical infrastructure efforts
➢ Established the "Basic Policies for Cybersecurity concerning the Administration of Government Information Systems" ➢ Connected all local governments to the Mynaportal to improve convenience for the people ➢ Implemented the "NOTICE" initiative to alert users through telecommunications carriers	➢ Revised the common Cybersecurity standards in light of the recent trends in cybersecurity measures ➢ Operated the first GSOC team (fourth GSOC), conducted efficient and effective cross-government monitoring, and advanced collaboration between government agencies, etc. and GSOC ➢ Conducted additional registration and renewal review for cloud services based on unified security requirement standards, with respect to the Information System Security Management and Assessment Program (ISMAP)	➢ Steadily conducted efforts based on the 4th Edition of the Cybersecurity Policy for Critical Infrastructure Protection, including the maintenance and promotion of the safety principles, enhancement of information sharing system, enhancement of incident response capability, risk management and preparation of incident readiness, and enhancement of the basis for CIP.

Evaluation

Toward the safe and secure use of cyberspace, conduct efforts from various perspectives, including information provision, technological foundation, increasing capabilities, and raising awareness, and continue to advance multi-layered cybersecurity measures based on the self-help, mutual help, and public help of all stakeholders involved in cyberspace.

In revising the common Cybersecurity standards, security measures were enhanced in light of the growing use of cloud services and diversified workstyles. The establishment of the fourth GSOC system has enabled cross-governmental cybersecurity enhancement to address the growing use of the cloud by government agencies.

As for efforts based on the 4th Edition of the Cybersecurity Policy for Critical Infrastructure Protection, relevant ministries and agencies must continue to make active efforts and further advancement. In addition, they must conduct efforts toward the revision of the Policy, including radical enhancement of incident response capabilities, given the increasingly interdependent relationships of economic and social activities.

New Efforts in FY2022

➢ Enhancement of national CSIRT/CERT functions ➢ Establishment of the "Guidance for Sharing and Announcing Information concerning Damage from Cyberattacks" ➢ Advancement of public-private and international collaboration through the establishment of the Cyber Affairs Bureau and the National Cyber Unit ➢ Technical verification to ensure the safety and reliability of telecommunications networks	➢ Establishment of the outline of the next common Cybersecurity standards based on new security measures required for government information systems ➢ Deliberations toward establishment of the fifth GSOC system ➢ Introduction of a new system toward greater use of cloud services with respect to ISMAP	➢ Revision of the 4th Edition of the Cybersecurity Policy for Critical Infrastructure Protection ➢ Steady implementation of the five measures (e.g., enhancement of incident response capability) based on the revised policy ➢ Verification project toward the establishment of an adequate system for cyber incident investigations

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

Examples of efforts in FY2021

Ensuring "a free, fair and secure cyberspace"	Strengthening capabilities for defense, deterrence, and situational awareness	International cooperation and collaboration
➢ Conveyed the importance of leading the effort to establish international rules based on the concept of Data Free Flow with Trust (DFFT) at the G20 Rome Summit in 2021 ➢ Contributed actively to the effort to develop international rules and norms to advance the rule of law in cyberspace	➢ Continued to protect defense-related technologies to ensure national resilience ➢ Conducted efforts to fundamentally enhance cyber defense capabilities with the aim of increasing deterrence capabilities ➢ Collected and analyzed information about how leading states were handling cyberattacks, cyberattacks suspected of state involvement, etc. to enhance situational awareness capabilities	➢ Advanced international cooperation and collaboration by actively participating in multilateral meetings to address ransomware attacks that were rapidly doing damage, and contributing to building momentum toward effective, multilateral effort to contain them ➢ Conducted efforts based on the new Basic Policy on Cybersecurity Capacity Building for Developing Countries

Evaluation

While Japan is working to ensure a free, fair and secure cyberspace in close collaboration with relevant foreign agencies, the threat of cyberattacks is becoming increasingly diverse and complex. As such, it is necessary to continue to strengthen Japan's capabilities for defense, deterrence, and situational awareness while advancing the steady practice of international rules and norms in close collaboration with its ally and like-minded countries.

As for capacity building support, it is necessary to continue to make active efforts, including the expansion of support to the Indo-Pacific region, building on the results and experience in the ASEAN region, based on the Basic Policy.

New Efforts in FY2022

➢ Contribute to international cooperation with relevant states through bilateral talks and multilateral talks at the United Nations and elsewhere

➢ Active involvement in discussions on the application of international law and development of international rules and norms in cyberspace ➢ Active contribution to the development of new international rules and norms in line with Japan's basic principles	➢ Advancement of effort to secure Japan's resilience against cyberattacks, in order to protect national security interests ➢ Continued effort to strengthen Japan's capabilities for defense, deterrence, and situational awareness	➢ Sharing expertise, coordinating policy, sharing information about cyber threats including even during peacetime, and advancing capacity building support ➢ Advancing active effort on capacity building support for developing countries, in accordance with the Basic Policy

Part 3 Results and Evaluation of Efforts in FY2021 Based on the Strategy, and Efforts in FY2022 (4/5)

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 in FY2021	➢ Deliberations toward establishment of a technical verification mechanism ➢ CYNEX: Trial aimed at providing testing environments using system platforms for domestic security products ➢ Research and development of fundamental technologies for quantum key distribution (e.g., longer distance, relay)	➢ Development of a sample curriculum for gaining Plus Security knowledge (for managers and general managers) ➢ CYNEX: Trial aimed at making exercise platforms using system platforms open ➢ "Digital human resources development platform": Establishment of DX literacy standards, launch of portal site “Manabi DX” (*”Manabi” means Learning)	➢ Enhancement of content for teachers and students toward establishment of a new "Information I" high school course ➢ Full revision of the "Telecommuting Security Guidelines" (checklist for SMEs) ➢ Cybersecurity Awareness Month: Collaboration with OS and wireless LAN router vendors
Evaluation	It is necessary to have the viewpoints of both practical research and development and government-industry-academia ecosystems, including the perspective of national security. It is necessary to ensure research promotion measures are widely used in industry, academia and the government.	It is necessary to further enhance efforts toward the development of human resources equipped with practical response capabilities, including promoting the use of qualification systems. It is necessary to create a market for programs by private businesses and to track and strengthen efforts by educational institutions.	It is necessary to enhance measures targeting children and the elderly, instead of simply continuing the existing awareness-raising practices. ↓ Review the current action plan and prioritize efforts.
New Efforts in FY2022	➢ Promote the use of research and development funding that is expected to be used in the cybersecurity field, in industry, academia, and the government ➢ CYNEX: Deepen community relationships, build trust, and strengthen the system of analysis, accumulation, evaluation and human resource development. (go live in FY2023) ➢ Establish CRYPTREC guidelines on post-quantum cryptography etc., fully revise the CRYPTREC Ciphers List ➢ Develop quantum key distribution networks and optical ground station testbeds	➢ "Digital human resources development platform": Establish skill standards for specialists, post courses provided by companies and universities ➢ Track, communicate, and promote efforts at universities, technical colleges, and other educational institutions ➢ Government agency personnel: Sort out existing training, consider a system where qualification tests are used to certify skills ➢ Improve "Cyber Defense Exercises with Recurrence" and provide them to the employees of local governments who cannot take them easily.	➢ Review the "Awareness and Behavior Reinforcement Program" ➢ Visualize local contact points in a centralized manner, and promote collaboration by stakeholders ➢ Deliberate the addition of cybersecurity courses for the project to advance assistance in the use of digital technology, which offers classes for the elderly ➢ Advance the e-Net Caravan delivery lecture for students, parents, and teachers

5. Implementation Framework

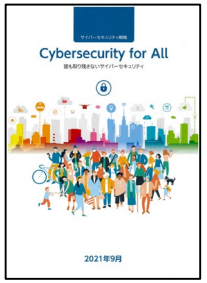
Results in FY2021

- Shared information about incidents and cyberattacks in Japan and abroad based on partnerships with relevant agencies, led by NISC. Also advanced enhancement of comprehensive analysis functions through meetings with international counterparts and provision of information about IWWN analysis reports.
- To effectively communicate the aim of the Strategy to stakeholders in Japan and abroad, and obtain sufficient understanding, produced a color pamphlet of the Strategy and a booklet of Cybersecurity 2021. The National Security Secretariat and relevant ministries used the pamphlet and booklet to give explanations at seminars, communicating information about Japan's cybersecurity policies.
- From the perspective of the importance of international cooperation, explained the Strategy and Japan's basic policy on capacity building support for developing countries to the cybersecurity authorities of other states and the embassies of other states in Japan. In addition, actively provided information about the status of efforts regarding Japan's cybersecurity policies to audiences in Japan and abroad, such as by posting information on NISC's website or the United Nation's portal site.

Evaluation

It is important to continue these efforts to further familiarize stakeholders in Japan and abroad with Japan's cybersecurity policies. Responding flexibly to the new lifestyles referred to as the "new normal," which became established through the COVID-19 pandemic, we will continue to engage in public relations activities targeting a wide range of businesses and individuals, such as by holding online events and distributing electronic materials. In addition, it is essential that we seek broad understanding and acceptance of Japan's cybersecurity policies, including the message of "Cybersecurity for All—Cybersecurity which leaves no-one behind" upheld in the Strategy. It is also necessary to pursue further enhancement of collaboration with relevant agencies, and communicate the Strategy and Cybersecurity 2022.

Cybersecurity Strategy



Cybersecurity 2021

Efforts in FY2022

- For the further enhancement of the capabilities of relevant agencies, we will seek to improve the functions of systems that are already established, and review collaborative systems as needed.
- To promote autonomous efforts by all stakeholders, we will continue to actively communicate the Strategy and the annual plan that is based on this to external audiences, and strive to ensure that Japan's cybersecurity policies are widely understood and accepted.