NISC National center of Incident readiness and Strategy for Cybersecurity

Japan's Next Cybersecurity Strategy

(Note)
Japan is now revising the current Cybersecurity Strategy 2018 and decides on its New Strategy by the end of this year. This document shows its direction and the main elements of its outline discussed at the Cybersecurity Strategy Headquarters held on May 13, 2021. This outline is now available only in Japanese and its English provisional translation will get ready soon.

Cybersecurity Strategy 2018
https://www.nisc.go.jp/eng/pdf/cs-strategy2018-en-booklet.pdf

Outline of Next Cybersecurity Strategy (Japanese)
https://www.nisc.go.jp/conference/cs/dai28/pdf/28shiryou01.pdf

As of 1 of June 2021

Issues and Direction of the Japan's Next Cybersecurity Strategy

Japan in the 2020s: Era of the "new normal" and the digital society

- ✓ Digital economy
- ✓ **Digital transformation (DX)**

- ✓ **COVID-19**
- ✓ Remote working, online education, etc.

- ✓ Increasingly harsh national **security** landscape

- ✓ Expectations for the contribution of digital technology to **SDGs**

- ✓ **Tokyo Games**

Issues in cyberspace: Inclusion of all the people in cyberspace

- ✓ Cyberspace is becoming **a public space where all stakeholders participate**
- ✓ **Interconnections and interrelationships across cyber and physical boundaries are becoming deeper**
- ✓ These changes increase vulnerabilities that attackers can exploit

- ✓ Geopolitical tensions brought into cyberspace
- ✓ **International competition**
- ✓ National security issues

- ✓ Concerns about rifts between nations and the suppression of human rights

- ✓ Public and private partnership

Need for all stakeholders to ensure their own cybersecurity
Japan's Commitment to the 5 basic principles*

"Cybersecurity for All"

Cybersecurity which leaves no-one behind

Advancing DX and cybersecurity simultaneously

Enhancing initiatives from the perspective of Japan's national security

Ensuring the overall safety and security of cyberspace as it becomes increasingly public and interconnected

Ensuring "a free, fair and secure cyberspace"

* Assuring the free flow of information, the rule of law, openness, autonomy, and collaboration among multi-stakeholders

Enhancing Socio-Economic Vitality and Sustainable Development

Issues and direction—DX with Cybersecurity

- The Digital Agency will be established in September of this year. Such initiatives will greatly advance DX. To this end, it is important to build trust in cyberspace, which leads to participation and commitment.
- As operations, products, and services become increasingly digitalized, ensuring cybersecurity will be directly linked to corporate value. "Security by design" will become ever more important, and digital investments and security measures will likely become increasingly integrated.

⇨ Advance cybersecurity in parallel with digitalization

Specific measures

(1) Raising executive awareness

→Visualize and incentivize initiatives based on the guidelines of cybersecurity management, and further promote such initiatives, by implementing guidelines for digital management.

(2) Advancing DX with Cybersecurity among local communities and SMEs

→Address the shortage of knowledge and human resources required for digitalization, through the development of local communities and the establishment of a registration scheme for services targeting SMEs.

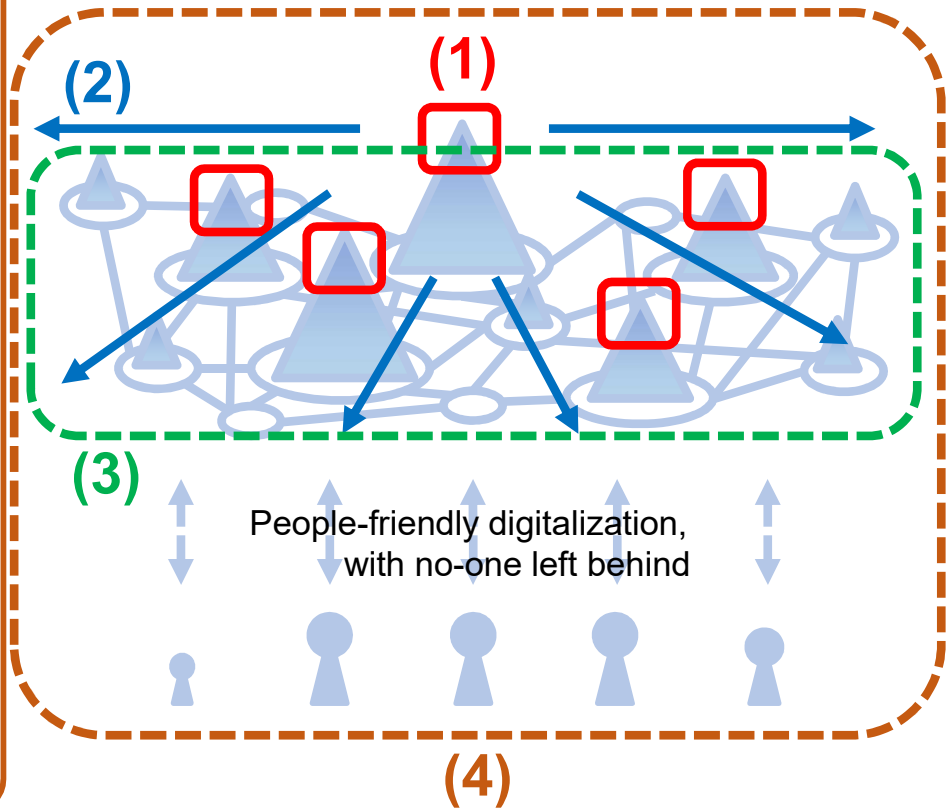
(3) Building a foundation for ensuring trustworthiness of supply chains

→Advance initiatives based on the frameworks which respond to Society5.0.

- Supply chains: Industry-led consortium
- Data Flow: Definition of data management, promotion of "trusted services"
- Security products/services: Promotion of third-party verification services
- Advanced technology: Building a common foundation for collecting, accumulating, analyzing, and providing information

(4) Advancing digital/security literacy inclusively

→Advance initiatives which provide assistance in the use of digital technology, along with efforts to drive information education.



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

Issues and direction— Ensuring the overall safety and security of cyberspace as it becomes increasingly public and interconnected

- Evolution of cyberspace into a public space where all stakeholders are involved.
- Deepening interconnection and interrelationship of socio-economic activities across cyber and physical boundaries.
- Cyberattacks which are becoming more organized and sophisticated.

The national government, in cooperation with various stakeholders, will take a comprehensive and multilayered approach to cybersecurity, which is based on self-help, mutual help and public help, and which reduces risks and increases resilience for the entire country.

Specific measures

○ **Ensure cybersecurity combined with digital transformation (led by the Digital Agency)**

○ **Promote efforts by stakeholders which underpin the socio-economic infrastructure**
1) Government agencies, etc.
2) Critical infrastructure
3) Universities, education and research institutions, etc.

○ **Promote seamless information sharing among multiple stakeholders and make good use of knowledge gained through the Tokyo Games, etc.**

○ **Enhance readiness to respond to massive cyberattacks, etc.**

○ Cybersecurity environment to protect people and society

◆Ensure safety and security in cyberspace through
(1) Supply chain management
(2) Responses to new technologies and services (e.g., IoT, 5G)

◆Cooperate with new providers of cybersecurity
(Efforts to enable users to use cyberspace technologies and services, including cloud services, safely and securely)

◆Address cyber crimes

◆Deploy comprehensive cyber defense
(Improvement of response capabilities by enhancing national CSIRT functions and enhancing interagency collaboration in the event of incidents.

◆Ensure trustworthiness of cyberspace
(1) Protection of personal information and intellectual property information
(2) Ensuring “trustworthiness” of IT systems and services from the perspective of economic security

Issues and direction—Enhancing initiatives from the perspective of national security

- The national security environment surrounding Japan has become increasingly harsh, and cyberspace has become an area of competition that reflects geopolitical tensions. China, Russia and North Korea are apparently building and strengthening cyber capabilities, and sponsoring cyberattacks.
- Like-minded countries are working together to defend against such cyberattacks and tackle conflicts over international rules concerning cyberspace.

⇨ To ensure the safety and security of cyberspace, we will raise the priority of cyber in diplomacy and national security. We also commit to (1) promoting the rule of law, (2) strengthening capabilities for defense, deterrence, and situational awareness against cyberattacks, and (3) further enhancing international cooperation and collaboration.

Specific measures

(1) Commitment to a free, fair and secure cyberspace

- Advance the rule of law in cyberspace through activities at the UN and elsewhere
- Formulate international rules in line with Japan's basic vision

(2) Strengthening Japan's capabilities for defense, deterrence, and situational awareness

- Build stronger cyber units in MOD, maintain security of critical technologies and industries, and strengthen alliance with the US
- Further fact-finding with regards to cyberattacks by leveraging nationwide network technology units

(3) International cooperation and collaboration

- Strengthen multi-layered frameworks for international collaboration within and across ministries and agencies
- Promote joint efforts by the government, industry, and academia to build capabilities in the Indo-Pacific region, including ASEAN

Cross-Cutting Approaches to Cybersecurity

Advance DX and cybersecurity simultaneously

Ensure the overall safety and security of cyberspace as it becomes increasingly public and interconnected

Enhance initiatives from the perspective of national security

● Taking a cross-cutting, medium- to long-term view, promote R&D, development of human resources, and awareness-raising activities in order to advance the above.

1. Advancement of R&D

Build a government-industry-academia ecosystem, and pursue practical R&D using that as a foundation.
Take medium- to long-term technological trends into consideration.

(2) Advance practical R&D

(1) Address supply chain risks

(2) Cultivate/develop domestic industries

(3) Monitor/analyze attacks and their common foundations

(4) Advance research of cryptography, etc.

(3) Take medium- to long-term technological trends into consideration

(1) Advancement of AI technology
AI for Security / Security for AI

(2) Advancement of quantum technology, post-quantum cryptography, quantum communications/cryptography

(1) Strengthen international competitiveness Build a government-industry-academia ecosystem

- Leverage measures to promote research and government-industry-academia collaboration
- Enhance research environment, etc.

2. Recruitment, development, and active use of human resources

Develop the quality and quantity of public and private sector, with a focus on efforts to address environmental changes. Create an environment that enables career development spanning both public and private sectors.

(1) Advance DX with Cybersecurity

- Create an environment where people can gain additional security knowledge
- Promote practices which encourage function building and staff mobility, etc. (xSIRT, side/concurrent business, etc.)

(2) Address increasingly sophisticated and complex threats

- Strengthen human resources development programs
  SecHack365/CYDER/enPiT
  ICSCoE Core Human Resource Development Program, etc.
- Build a common foundation for human resources development and make it available to industry and academia
- Promote the use of qualification systems, etc.

Create an environment that enables talented human resources to develop careers which span the private sectors, municipalities, and government agencies

(3) Pursue government agency initiatives

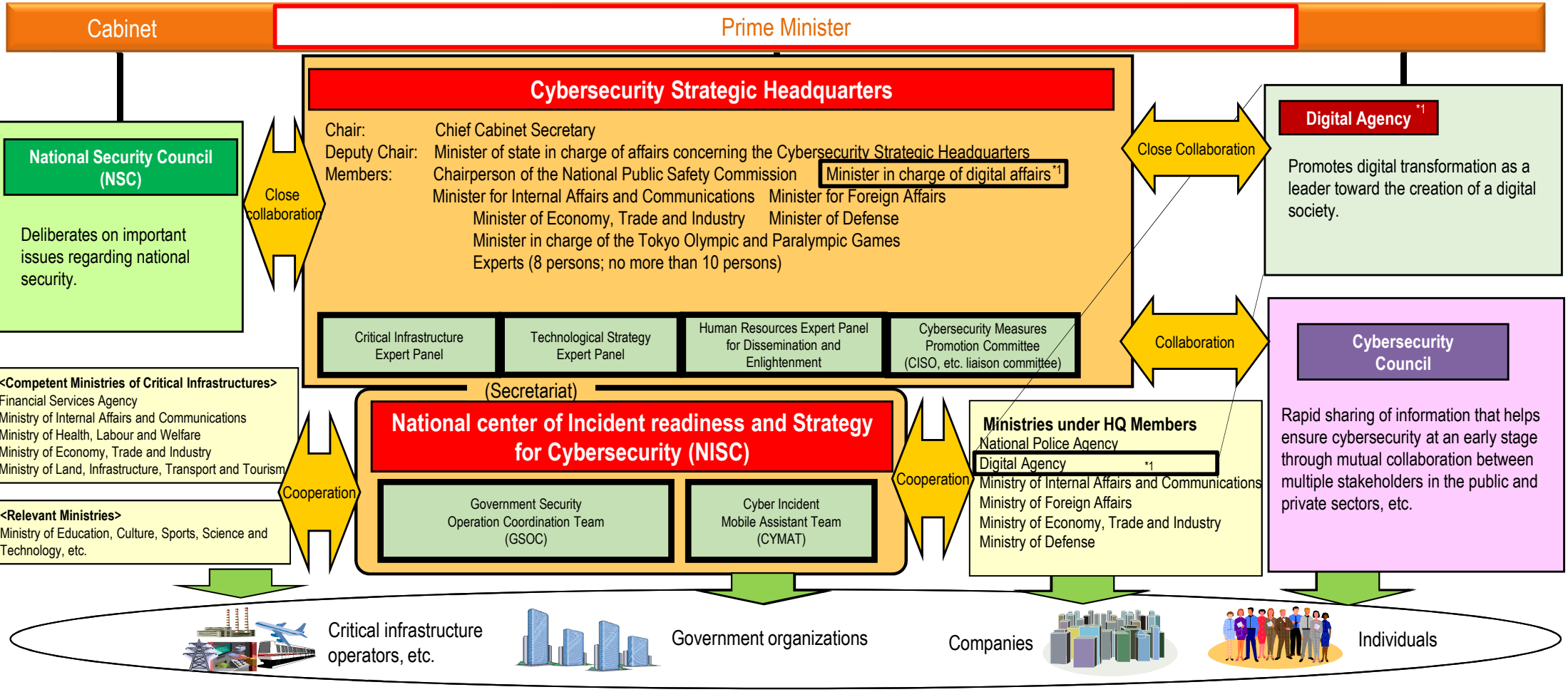
* Update the “Enhancement Policy” in the first half of FY2021

3. Collaboration based on full participation and awareness raising

Improve and review action plans to advance digitalization.

Implementation Framework

- A concerted effort by the whole of government is needed to promote and implement cybersecurity policy in order to ensure a free, fair and secure cyberspace in line with Japan's cybersecurity policies. Further efforts will be made to strengthen the capabilities and collaboration of relevant bodies so that they can contribute to the digital transformation led by the Digital Agency, and leverage the limited resources of public institutions to fulfill their roles.
- NISC and relevant ministries and agencies must work together to actively communicate this strategy to stakeholders both in Japan and abroad, in order to encourage Japanese stakeholders to take practical action based on the recognition of the importance of international cooperation, and with the goals of increasing international understanding of Japan's stance and enhancing deterrence against attacks.
- Building on the information collection and analysis function, discuss the system needed to enhance the ability to quickly detect, analyze, assess, and address cyberattacks in an integrated cycle.
- Annual reports and plans should be discussed in an integrated manner, and activities for the next year aligned with the results and evaluation of the previous year's activities, in order to develop a cohesive flow of activity which is in line with the strategy.



(*1) Stated based on the bill to establish a basic act on the creation of a digital society (approved at a Cabinet meeting on February 9, 2021), etc.

Outline of the Next Cybersecurity Strategy

1 Japan in the 2020s

1-1 Establishment of the digital economy and promotion of digital transformation, expectations for contribution to SDGs, changing national security environment, impact and experience of COVID-19, and application of efforts toward the Tokyo Games.

2 Basic concept

2-1 Ensuring a cyberspace which is “free, fair and secure”

2-2 The basic principles adhere to the 5 principles set forth in the previous strategies (assurance of the free flow of information, the rule of law, openness, autonomy, and collaboration among multi-stakeholders)

3 Issues surrounding cyberspace

3-1 Increasing risks in cyberspace

- Spread of and increased reliance on new technologies, wider use of cloud services and technologies which transcend the borders of national security, increased complexity of supply chains of systems forming cyberspace, manifestation of potential vulnerabilities for attackers to target such as gaps in literacy and shortage or uneven distribution of human resources, and international situation surrounding cyberspace

3-2 Challenges and direction—Cybersecurity for All

- Promotion of DX and cybersecurity simultaneously, ensuring the overall safety and security of cyberspace as it becomes increasingly public and interconnected, and enhancing initiatives from the perspective of national security

4 Policy approaches

Enhancing Socio-Economic Vitality and Sustainable Development

1. Raising executive awareness
2. Promotion of DX with Cybersecurity among local communities and SMEs
3. Building a foundation for ensuring trustworthiness of supply chains
4. Establishing digital/security literacy inclusively

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

1. Providing a cybersecurity environment which protects people and society
2. Ensuring cybersecurity while pursuing digital transformation (led by the Digital Agency)
3, 4, 5. Promoting efforts by stakeholders which underpin the foundations of the economy and society
   - (1) (Government agencies, etc.)
   - (2) (Critical infrastructure)
   - (3) Universities, education and research institutions, etc.
6. Use of seamless information sharing systems run by multiple stakeholders and application of knowledge gained through efforts toward the Tokyo Games, etc.
7. Enhancement of readiness to respond to massive cyberattacks, etc.

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

1. Commitment to “a free, fair and secure cyberspace”
2. Strengthening Japan’s capabilities for defense, deterrence, and situational awareness
3. International cooperation and collaboration

Cross-Cutting Approaches to Cybersecurity

- Promotion of R&D
- Recruitment, development, and active use of human resources
- Collaboration based on full participation and awareness raising

5 Implementation Framework

A concerted effort by the whole of government is needed to promote and implement cybersecurity policy in order to ensure a free, fair and secure cyberspace in line with cybersecurity policies.

Further efforts will be made to strengthen the capabilities and collaboration of relevant agencies so that they can contribute to the digital transformation led by the Digital Agency, and leverage their limited resources to fulfill their roles.