Outline of the Cybersecurity Strategy

(tentative translation)

December 23, 2025

National Cybersecurity Office (NCO), Cabinet Secretariat

Overall Structure of the Cybersecurity Strategy

I. Background of Formulation

II. Fundamental Concepts of the Strategy

1. The desired state of cyberspace and its basic principles
2. The current situation and future outlook surrounding cyberspace
3. Key issues regarding cyberspace and policy directions

III. Measures for Achievement of the Objectives

1. Defense and deterrence against intensifying cyber threats
2. Enhancement of society-wide cybersecurity and resilience through broad stakeholder
3. Formation of an ecosystem for human resources and technologies supporting Japan’s cyber response capabilities

IV. Implementation Framework of the Strategy

Overview of the “Cybersecurity Strategy”

○ Based on the “**National Security Strategy**” and initiatives such as the **Cyber Response Capability Strengthening Act and Necessary Arrangement of Relevant Acts**, this strategy presents the objectives and policies necessary to promote coordinated efforts to respond to threats in cyberspace from a medium- to long-term perspective and **with the next five years in mind**.

Fundamental Concept

○ Cyberspace serves as a foundation supporting the sustainable development of the economy and society, as well as liberalism, democracy, and cultural advancement.
○ The international order based on universal values such as the rule of law and respect for fundamental human rights is facing a serious crisis, and cyber threats are heightening concerns over people’s daily lives, economic activities, and ultimately, national security.

By continuing to uphold the “five principles”* as its basic principles, the government will take a more proactive role and strengthen its measures to respond to the increasingly challenging situation in cyberspace, thereby clarifying its commitment to the realization of a “free, fair and secure cyberspace.”

*The five principles guiding the formulation and implementation of measures are: “Assurance of the free flow of information,” “The rule of law,” “Openness,” “Autonomy” and “Collaboration among multi-stakeholders.”

Situational awareness

- Increasingly challenging situation in cyberspace and growing state-sponsored cyber threats
- Advancement in digitalization across society and the escalation of cyber threats
- Emerging technological innovations, such as AI and quantum technology, and their impact on cybersecurity

Direction of measures

1. Defense and Deterrence Against Intensifying Cyber Threats

- To address the increasingly severe security environment in cyberspace, the government will combine a range of measures including active cyber defense, with existing measures such as incident responses, within a framework of public–private collaboration and international cooperation, thereby imposing costs on adversaries and strengthening defense and deterrence against intensified cyber threats.
- The government will proactively share information with the private sector

Defense and deterrence with the government playing pivotal roles

Formation of a public–private collaboration ecosystem

Promotion and strengthening of international cooperation

2. Enhancement of Cybersecurity and Resilience Across Society by Broad Participation

- Clarify and implement measures required of various stakeholders, along with approaches to ensure their effectiveness (government agencies and related organizations taking the lead as role models.)
- Promote digitalization and cybersecurity in parallel

Strengthening measures for government agencies and related entities

Strengthening measures for critical infrastructure operators and local governments

Ensuring resilience across the entire supply chain (SMEs and vendors, etc.)

Promoting cybersecurity improvement by full participation

Ensuring safety and security through countermeasures against cybercrime

3. Formation of an Ecosystem for Human Resources and Technologies Supporting Japan’s Cyber Response Capabilities

- Securing and developing cybersecurity talent through collaboration among industry, academia, and government
- Creating new technologies and services centered on domestically developed innovations

Efficient and effective development and retention of cyber workforce

Formation of an ecosystem for emerging technologies and services

Response and initiatives for advanced technologies such as AI and quantum technology

**Based on public–private and international collaboration, the government will take the pivotal role in cybersecurity measures, promoting Japan’s cybersecurity efforts through a whole-of-nation approach that earns the understanding and cooperation of citizens and stakeholders.
Through these efforts, Japan aims to become a nation with world-class resilience, capable of responding seamlessly and continuously to the increasingly severe conditions in cyberspace.**

Measures to Achieve the Objectives

1. Defense and Deterrence Against Intensifying Cyber Threats

(1) Defense and deterrence with the government playing pivotal roles

① Preventing the expansion and escalation of damage through advanced incident response

- ✓ Establishing platform for essential infrastructure service providers and others to report specified critical computing devices and incident occurrences to the government, in accordance with the new law. This includes the standardization of reporting formats and centralization of reporting channels.
- ✓ Collecting, organizing, and analyzing vulnerability information, with the government taking the initiative in providing effective information to private-sector entities to help prevent the expansion and escalation of damage.

② Aggregation, effective analysis, and utilization of cybersecurity-related information, including communications data

- ✓ Centralizing information in NCO and building a structure that fundamentally enhances analytical capabilities.
- ✓ By utilizing communications data, aiming to grasp attack patterns, etc. and conducting effective analysis that is also effective for remote access and neutralization measures.
- ✓ Based on laws and necessity, providing analyses to the government, to allied and like-minded countries, to agreement* parties, to members of the new council, to suppliers of computing devices.

*"Agreement" under the new law for obtaining communications data from essential infrastructure service providers and others.

③ Active defense and deterrence through a combination of multiple measures, including remote access and neutralization measures

- ✓ To make full use of Japan's national capabilities, Japan will build a structure for joint implementation of remote access and neutralization measures by the police and the Ministry of Defense/Self-Defense Forces. To ensure consistency with national security policies, NCO (National Cybersecurity Office), under the Minister of State for Cybersecurity, will work in coordination with the NSS (National Security Secretariat) to exercise a comprehensive coordination function. These measures will be conducted under a unified policy, within the scope permitted under international law, alongside a significant enhancement of capabilities and rapid development of systems, equipment, and related resources.
- ✓ NCO will exercise its comprehensive coordination function, appropriately combining existing measures (such as voluntary takedowns, public attribution, and disclosure of attack methods) and will implement active defense and deterrence in close collaboration with relevant ministries and agencies, as well as allied and like-minded countries.
- ✓ Conduct training and exercises necessary for active defense and deterrence and explore the utilization of advanced technologies.

④ Comprehensive development and operation of frameworks, infrastructure, and human resources, etc.

- ✓ To ensure sustained and effective engagement in national security in cyberspace, Japan will undertake the comprehensive development of necessary frameworks, infrastructure, and human resources, etc.
- ✓ Continually sharing information and insights regarding cybersecurity issues with the Japan Active Cyber Defense Oversight Commission (tentative translation).

(2) Formation of a public–private collaboration ecosystem and strengthening of cross-sectoral measures

① Establishing a cycle of two-way, proactive information sharing and enhanced countermeasures between the public and private sectors

- ✓ Conduct continuous, multi-layered dialogue between government and industry, not only seeking cooperation at the occurrence of emergencies but building trust on an ongoing basis. Utilize frameworks such as the new council established under the new law, through which the government proactively provides threat intelligence, and develops a shared public–private information platform.

② Expanding threat hunting activities across the public and private sectors

- ✓ A basic policy about spread promotion and implementation of threat hunting will be formulated. Clarifying position of threat hunting as a means of active cyber defense, building overall security capabilities.

③ Systematic implementation of cybersecurity exercises

- ✓ Enable efficient and effective cross-sectoral exercises that span multiple domains. Promote the mutual sharing of expertise and results gained from these exercises to strengthen readiness across sectors.

(3) Promotion and strengthening of international cooperation

① Cooperation with ally, like-minded countries and others in information and operational domains

- ✓ Strengthen cooperation with relevant agencies of other countries through continuous dialogues and multilateral meetings that contribute to enhancing Japan's response capabilities. Promote international joint investigations and reinforce efforts such as public attribution and diplomatic measures to deter malicious cyber activities.

② Support and promotion of enhancing response capabilities in the field of cybersecurity in the Indo-Pacific region

- ✓ Recognizing that the stability and prosperity of the Indo-Pacific region, including ASEAN, form the foundation of Japan's development, Japan will enhance capacity-building support through frameworks such as AJCCBC*.

*ASEAN-Japan Cybersecurity Capacity Building Centre

③ Promotion of international rule-making

- ✓ While communicating Japan's fundamental principles, play a proactive role in promoting the rule of law in cyberspace and in international rule-making.

Measures to Achieve the Objectives

2. Enhancement of Cybersecurity and Resilience Across Society by Broad Participation

(1) Strengthening cybersecurity measures for government agencies and related agencies

① Improving the level of cybersecurity and regularly reviewing of common cybersecurity standards

- ✓ Conduct regular reviews of unified government cybersecurity standards. Implement targeted and effective audits based on monitoring results. Ensure and enhance thorough implementation of measures across all government bodies, including external agencies and regional branches. Examine the handling of highly confidential information.

② Further strengthening and advancing government monitoring systems and incident response capabilities

- ✓ Strengthen and advance initiatives such as monitoring and analysis using CYXROSS sensors and cross-government monitoring of malicious activities by GSOC.

③ Building and operating robust government information systems

- ✓ The Digital Agency will strengthen security for critical systems through monitoring and vulnerability management, while each government agency will build and operate systems that maintain an appropriate level of security.

④ Development, retention, and strengthening of cybersecurity personnel and organizational structures in government agencies

- ✓ Clearly define the role and competencies of cybersecurity personnel, and enhance and strengthen training programs, exercises, and public–private personnel exchange in the government initiatives through the active utilization of such personnel.

(2) Strengthening cybersecurity measures for critical infrastructure operators and local governments, etc.

① Strengthening cybersecurity measures for critical infrastructure operators

- ✓ Formulate the common cybersecurity standards for critical infrastructure. Establish a PDCA (plan–do–check–act) cycle to continuously raise the overall cybersecurity level across all critical infrastructure fields.

② Strengthening cybersecurity measures for local governments

- ✓ Provide financial support to ensure the smooth renewal of local government information security cloud systems. Support the recruitment and development of digital talent within municipalities. Build a vulnerability assessment and diagnostic system.

③ Strengthening cybersecurity measures for universities and related institutions

- ✓ Offer advice and information sharing on cybersecurity measures and organizational frameworks. Conduct training and exercises. Provide advisory and technical support in the event of cybersecurity incidents.

(3) Ensuring cybersecurity and resilience across the entire supply chain, including vendors and SMEs

① Promoting responsible cybersecurity practices among vendors based on secure-by-design principles ,etc.

- ✓ Establish systems to ensure the responsibilities of information system suppliers are fully recognized. Further develop the JC-STAR certification framework and promote the use of it across society. Encourage the use of SBOM (software bill of materials) and promote secure software development.

② Ensuring cybersecurity and resilience throughout the supply chain

- ✓ Develop and promote a framework to visualize and certify the security levels companies should maintain based on supply-chain risks. Clarify the applicability of related laws regarding requests for security measures to business partners.

③ Strengthening measures for individual private companies, including SMEs

- ✓ Prepare and present guidelines and templates for cybersecurity measures. Review and improve the "Cybersecurity Supporters Service" to enhance its accessibility and effectiveness.

(4) Improving cybersecurity by full participation

- ✓ Promote active collaboration and cooperation among diverse stakeholders from industry, academia, government, and private sectors, along with public awareness and information dissemination.
- ✓ Update educational and outreach content appropriately in response to environmental changes and diverse needs.
- ✓ Enhance information education, including education on information security.

(5) Ensuring safety and security in cyberspace through measures against cybercrime

- ✓ Appropriately respond to cybercrimes by cracking down on criminal groups that exploit anonymity and malicious operators that provide criminal infrastructure, while also working to strengthen investigative capabilities and technological expertise.

Measures to Achieve the Objectives

3. Formation of an Ecosystem for Human Resources and Technologies Supporting Japan's Cyber Response Capabilities

(1) Efficient and effective development and retention of cyber workforce

① Cybersecurity workforce framework

✓ Establish a cybersecurity workforce framework to visualize career paths, enable appropriate matching of personnel in recruitment and placement, and promote linkages with education and training programs provided by various sectors.

② Further enhancement of education, exercises, and training for developing cybersecurity personnel

✓ Create environments where individuals can acquire skills progressively, from basic literacy to advanced expertise. Promote advanced technical education programs targeting younger generations. Provide practical exercises and training platforms, as well as curricula focused on cutting-edge security technologies and product development.

(2) Formation of an ecosystem for emerging technologies and services

✓ Through research and development, demonstration, as well as social implementation of new technologies and services, improve analytical and development capabilities, and build a virtuous ecosystem that nurtures both technologies and human resources, with domestic technologies and services at its core.

- Conduct and expand research and development, and verification activities that reflect government needs.
- Make effective use of technical data including primary information.
- Promote cybersecurity industry growth by encouraging government agencies to test and pilot promising products.
- Use data and training platforms owned by national research institutions to train young professionals and specialized experts in various industrial fields.

(3) Response and initiatives for advanced technologies

① Response and initiatives accompanying the advancement and spread of AI technology

✓ Promote research and development, rule-making through the establishment of guidelines, social implementation, and human resource development aimed at ensuring AI safety, strengthening cybersecurity using AI, and addressing cyberattacks that exploit AI.

✓ Work in close coordination with initiatives related to national security and industrial development in the AI field.

② Response and initiatives accompanying the advancement of quantum technology

✓ Aim for the transition to post-quantum cryptography (PQC) in government agencies and related agencies by 2035, in principle. Taking into account the current use of cryptographic and other technologies, a roadmap will be formulated in FY2026 under collaboration with relevant ministries and agencies to promote smooth nationwide transition.

✓ Regarding quantum key distribution (QKD), accelerate efforts toward social implementation around 2030, including the expansion and enhancement of testbeds, and the creation and validation of business models.

Implementation Framework of the Strategy

Cybersecurity Strategic Headquarters

- Strengthens coordination among relevant organizations so that initiatives based on this strategy contribute to ensuring national security and to digital reform led by the Digital Agency as the central command.

National Cybersecurity Office (NCO)

- Control tower of cybersecurity across both the public and private sectors, including national security in cyberspace.
- Lead role of comprehensive coordination among ministries and agencies.
- Working closely with the National Security Secretariat on national security in cyberspace and strongly carries out comprehensive coordination as a commanding organization. Having discussions and decisions at the National Security Council when it is necessary.

Ministries and Agencies

- Promotes measures based on this strategy and review the effectiveness and structure of related initiatives.

Promotion of the Strategy

- While maintaining consistency with other national strategies, prepares an annual plan, verifies progress of measures, compiles an annual report, and reflects findings in the plans for the following year.
- In addition to audits of government institutions, conducts evaluations based on the common cybersecurity standards for critical infrastructure and assesses the status of cybersecurity in government agencies and related organizations, using the results to improve cybersecurity measures in government agencies and critical infrastructure operators.
- Conducts continuous reviews of the legal and institutional frameworks related to cybersecurity.
- Taking into account changes in Japan’s overall environment, periodically reviews and updates this strategy as necessary.