# Comments on the New Cybersecurity Strategy

November 18, 2025

Keizai Doyukai
Corporate DX Promotion Committee  ITO Joichi
Geoeconomics Committee  KOSHIBA Mitsunobu

The Act on Prevention of Damage Caused by Unauthorized Acts Against Important Computers and the Act on Revision of Related Laws in Connection with the Enforcement of the Act on Prevention of Damage Caused by Unauthorized Acts Against Important Computers (hereinafter referred to as the Act on Enhancement of Cyber Response Capabilities, etc.) was enacted and promulgated by the Diet on May 16 this year. Subsequently, the Cybersecurity Strategy Headquarters compiled urgent matters requiring immediate attention to address threats in cyberspace (May 29). Now, the Cybersecurity Promotion Expert Council has published the draft Cybersecurity Strategy (October 30).

Cyberspace brings immense benefits such as democratizing information access, expanding networks, and creating economic opportunities, while also carrying risks like cyberattacks and the spread of disinformation. While leveraging DX is essential for accelerating corporate growth investments and transforming business models, cyberattack methods are becoming increasingly sophisticated, advanced, complex, and organized. The advancement of digitalization presents benefits and risks as two sides of the same coin, making the improvement of cybersecurity response capabilities an urgent priority.

Japan now stands at a critical juncture where it must build an offensive cyber strategy that contributes to both economic security and industrial policy/competitiveness enhancement, alongside strengthening defensive cybersecurity. The Economic Security Promotion Act enacted in May 2022 recognizes that, amid increasingly complex international circumstances and changes in socioeconomic structures, preventing acts that harm national and citizen security in economic activities has become crucial for ensuring security. Accordingly, it positions massive public-private investment to secure autonomy in critical technologies and supply chains. As safeguards to protect these outcomes, guardrail measures such as “research security” and “security clearance” are being advanced. While these represent a defensive step, establishing a system for the secure, two-way exchange of sensitive national-level information with allies and like-minded nations remains a task for the future.

The following points address four areas where the matters and discussions outlined in the draft cybersecurity strategy by the Cybersecurity Promotion Expert Panel are insufficient, while anticipating a proactive national cybersecurity strategy that balances cybersecurity and economic security.

## 1．Formation of a Public-Private Partnership Ecosystem and Specific Measures

- Information is the most critical factor in cybersecurity. While the Act on Strengthening Cyber Response Capabilities and other legislation mandates incident reporting obligations for designated critical infrastructure operators—the foundation of national life and economic activity—additional measures should be implemented regarding the following points.

### (1) The Future of Public-Private Partnership Organizations

- The new public-private partnership organization will be structured with the concept of "give and take" in mind, possessing functions such as information gathering and provision, incident response support, and risk communication. It will also hold regular meetings and workshops to promote the exchange of information and opinions among participating companies, while facilitating personnel exchanges between the public and private sectors to build trust.
- When establishing the organization, we should draw heavily on examples from other countries, such as the U.S. Joint Cyber Defense Collaboration (JCDC), the UK's Industry 100 (i100), and Australia's Cyber Threat Intelligence Sharing (CTIS).

### (2) Content of the information provided

- Information provided to the private sector (see examples below) shall provide useful information for management decision-making.
  - ✓ Attacker's identity, purpose, and background
  - ✓ Attack urgency and importance
  - ✓ Estimated damage from attacks, ripple effects
  - ✓ Initial response and medium-to-long-term response measures
- The security clearance system should be appropriately designed and operated, and it should also be fully utilized in the provision of information.[1]。

### (3) Methods of Providing Information

- This October saw the standardization of DDoS attack and ransomware

[1] Opinion of the Japan Association of Corporate Executives on Security Clearance Legislation(February22,2024) https://www.doyukai.or.jp/policyproposals/2023/240222.html

reporting formats. While discussions are underway to centralize reporting channels, including system development, this should be advanced promptly, taking into account operational feasibility, realism, and efficiency.

## 2．Human Resource Development and Retention

### (1) Visualization of Talent Definition

- To establish a shared understanding among industry, government, and academia regarding cybersecurity talent development, it is necessary for the government to take the lead in visualizing talent definitions and collaborating with educational institutions, drawing on examples from other countries and domestic initiatives.
- In undertaking these initiatives, reference should be made to the following examples from Western countries.
  - ✓ In the United States, the NICE Cybersecurity Workforce Framework (NIST SP 800-181) defines roles, knowledge, and skills. Furthermore, the National Centers of Academic Excellence in Cybersecurity (NCAE-C) program certifies cybersecurity degrees offered by U.S. educational institutions.
  - ✓ Europe is promoting a common understanding of cybersecurity roles, competencies, skills, and knowledge through the European Cybersecurity Skills Framework (ECSF), as well as advancing skill recognition. Furthermore, through Cyber HEAD, it maintains a database of cybersecurity higher education programs across EU and EFTA countries, enhancing the visibility of universities online.

### (2) Expanding the Quality and Quantity of Educational Institutions

- From the perspective of improving cybersecurity literacy and developing and securing talent, implement security education from elementary through secondary education. Additionally, utilize private-sector personnel to enhance students' educational levels and improve the knowledge of teachers who deliver instruction.
- To expand the pool of immediately deployable cybersecurity personnel and top talent, it is necessary to enhance both the quality and quantity of personnel at technical colleges, universities, and graduate schools. For example, consider establishing a specialized cybersecurity learning framework modeled after Australia's Cyber Academy.

## 3．Response and Initiatives Regarding Cutting-Edge Technologies

### (1) National Roadmap Development for Post-Quantum Cryptography (PQC)

- Public-key cryptography, including RSA encryption, is used for security measures such as communication encryption, authentication, and digital signatures. With the development of quantum computers capable of cryptanalysis through technological innovations like quantum algorithm improvements, increased quantum bit counts, larger quantum circuit scales, and error correction, there is a risk that widely used cryptosystems like RSA encryption could be broken.

- Multiple quantum computer development companies indicate that the likelihood of fault-tolerant quantum computers entering the market by 2029 is extremely high, further increasing the risk of the aforementioned public-key cryptography being compromised. This means that during the 2020s, society must implement measures to protect against cyberattacks that will intensify the current threats to cyberspace. Introducing post-quantum cryptography (PQC) is the most realistic solution for this purpose.
- The National Cyber Coordination Office should finalize the PQC implementation guidelines currently under development by the end of December this year. Implementation should then commence, starting with the critical infrastructure designated by the government, to facilitate the transition to PQC through public-private cooperation.
- In the cyber society connected by IoT, vulnerabilities in cyberspace are most likely to originate from legacy wired systems connecting edge devices to citizens and businesses. These systems—such as routers converting fiber optic cables into electronic data and set-top boxes connecting televisions—are predominantly inexpensive products manufactured and imported from China. Therefore, measures for edge devices—not only for critical infrastructure but also for individual residences—should be urgently initiated for consideration by the National Cyber Coordination Office.

### (2) Add “Quantum-Resilient Information Infrastructure” to Government Support Programs under the Economic Security Promotion Act

- Discussions on revising the Economic Security Promotion Act are currently underway at the Cabinet Office and the Ministry of Economy, Trade and Industry. As stated above, the introduction of PQC should be added to the measures for strengthening critical infrastructure. Furthermore, the development of countermeasures against quantum computing cryptography should be explicitly included as a target for Japan’s information infrastructure enhancement technology development under the public-private technology development cooperation for advanced technologies.
- To verify the effectiveness of quantum-resistant cryptography developed or implemented, “attack techniques” for validating “defense

technologies” are required, and attack techniques should also be included in public-private technical cooperation. However, this matter likely involves sensitive national information, and we believe its handling requires the utmost care.

### (3) Promoting PQC international standardization discussions with the United States, the EU, and others

- To position Japan as a “trustworthy infrastructure provider” in international collaboration on critical technologies and cybersecurity, the country should actively participate in the entire process from PQC standard development to implementation.
- Our nation must recognize that it cannot join the international intelligence community without implementing a security clearance system and protecting the cyber information space.

## 4 Other

### (1) Mandatory disclosure in annual securities reports

- With a view to facilitating communication between management and investors and ensuring accurate and timely disclosure of important cybersecurity information, consider mandating disclosure in securities reports. Furthermore, cybersecurity measures should be clearly stated in the Corporate Governance Code.
- In the United States, in 2023, publicly traded companies were mandated to: ① Disclose certain information regarding cybersecurity risk management, strategy, and governance in their Form 10-K (annual report); and ② Disclose cybersecurity incidents, such as unauthorized access to customer information, within four business days of determining the incident to be material, using Form 8-K (current report). Japan should promptly address this matter, drawing on these examples.

### (2) Establishing a Framework for Cyber Insurance

- The global cybersecurity insurance market is expanding annually and is projected to exceed $20 billion by fiscal year 2024. However, Japan's cybersecurity insurance market is estimated to be only about ¥30 billion, indicating a small market size. Furthermore, the cyber insurance adoption rate among Japanese companies is 7.8%[2], significantly lower than in Europe and the United States. As cyber insurance is a new field, individual

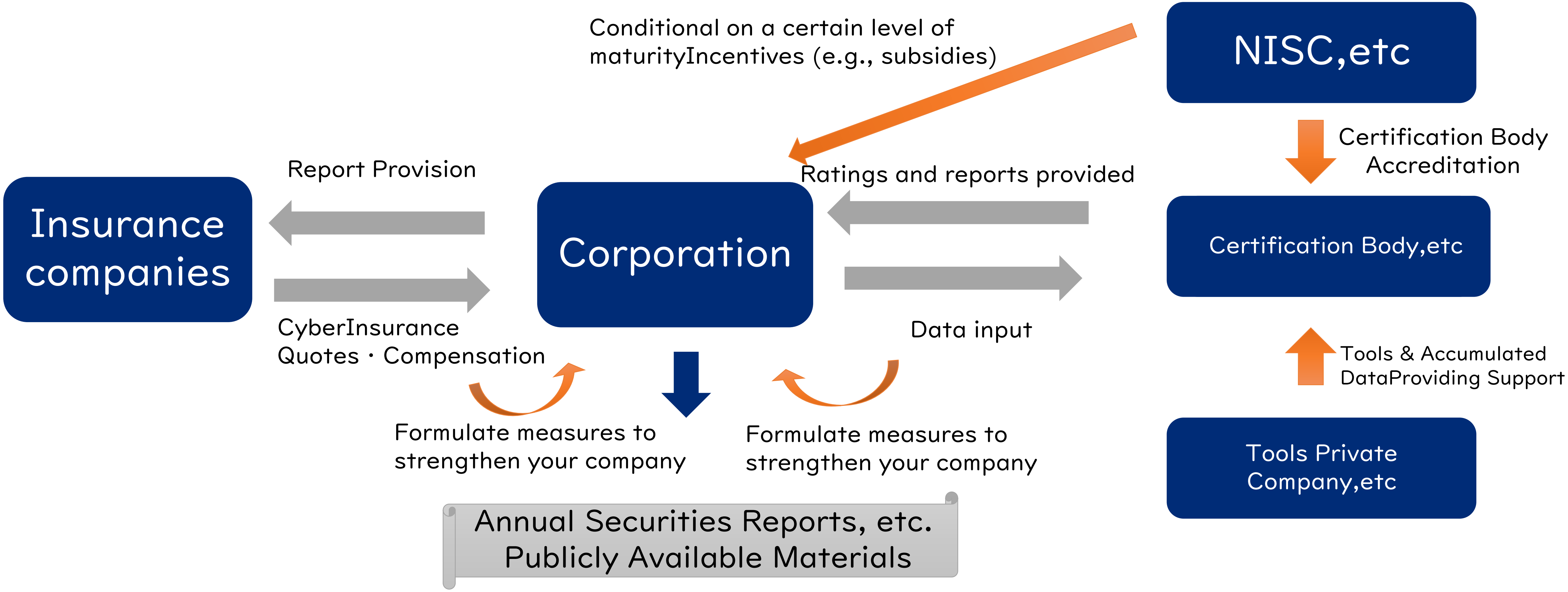
[2] Japan General Insurance Association “Survey on Cyber Risk Awareness and Countermeasures Among Domestic Companies 2020” (December 2020)

insurance companies lack sufficient data. The government should take the lead in aggregating data, conducting analysis, and establishing rules to create options for a risk assessment framework through cyber insurance.

- Cybersecurity assessments, cyber insurance, and securities reports should be managed as an integrated whole. (Appendix)

# (Appendix) Image of Cyber Insurance and Disclosure Reporting

- Also utilize cybersecurity maturity certification systems with solutions from private companies and other organizations
- Providing a transparent risk assessment framework to enable cyber insurance and disclosure reporting



Conditional on a certain level of maturityIncentives (e.g., subsidies)

NISC,etc

Certification Body Accreditation

Report Provision

Ratings and reports provided

Insurance companies

Corporation

Certification Body,etc

CyberInsurance Quotes・Compensation

Data input

Tools & Accumulated DataProviding Support

Formulate measures to strengthen your company

Formulate measures to strengthen your company

Tools Private Company,etc

Annual Securities Reports, etc. Publicly Available Materials