KEIZAI DOYUKAI

Early Action in the Era of

“Cyber Security Everywhere”

～8 actions of management and 6 policy proposals to the government ～

Committee Chairpersons ：

Ito, Joichi（Director, Digital Garage / President, Chiba Institute of Technology）

Uenoyama, Katsuya（Director,PKSHA Technology Inc.）

Suzuki, Kunimasa（ Director & Chairman,Intel K. K.）

Oct. 23, 2024

Keizai Doyukai

Ⅰ. Perspectives for consideration of policy proposals and targets

Perspectives for consideration of policy proposals

・In the Russian invasion of Ukraine, which will be one of the tectonic shifts in geopolitics, cyber attacks on satellite communication systems and substations before an armed attack
・There have already been attacks from China and North Korea, especially North Korea's ballistic missile development with some inflow of funds exploited by cyber attacks in Japan

Cyber attacks are becoming more sophisticated, more sophisticated, complex, and organized

・The long-stalled engine of economic growth, including sustained wage increases and a return to a world with interest rates, is finally showing signs of getting moving again.
・Severe labor and human resource shortages, which are a stumbling block to grasping the fruits of growth again, are becoming the norm.

DX using digital technology is essential

Confronting the threat of cyber attacks at every turn

Enter the Era of 「Cyber Security Everywhere」

Targets

・We present our opinions from two perspectives: eight recommendations that corporate executives, particularly large corporations with a high degree of influence, should be aware of and act upon, and six recommendations that the government should promote.

2． Awareness of the existing situation

- Cyber attack risk continues to rise as an external factor, as 1) attack surfaces increase, 2) the cybercrime ecosystem matures, 3) attacks become more sophisticated with the development of IT and AI, and 4) geopolitical risks become more apparent.

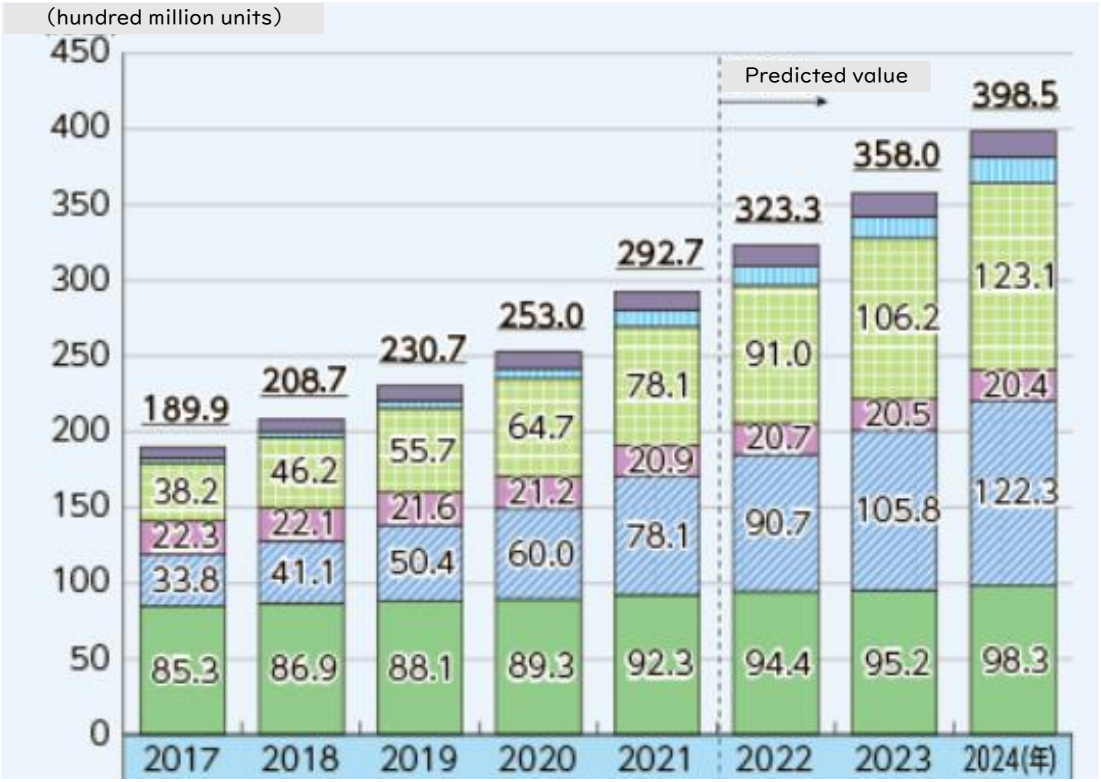
Awareness of the existing situation

- **Increase in Attack Surfaces**

  Expanding use of information systems and cloud computing
  by 2024 IoT devices are expected to increase
  1.7 times more than in 2019

- **Maturation and complexity of the cybercrime ecosystem**
- **Increasing sophistication of attacks due to IT and AI developments**
- **Increased geopolitical risks**

【Increased attack surface】



<Source> 2022 White Paper on Information and Communications:
Trends and Forecasts in the Number of IoT Devices Worldwide

2． Awareness of the existing situation

- As DX initiatives become more prevalent, interest in cybersecurity measures is growing.
- The number of cases is increasing, and the importance of management issues such as service suspension or discontinuation, decline in corporate value, executive responsibility, and lack of human resources continues to grow.

Awareness of the existing situation

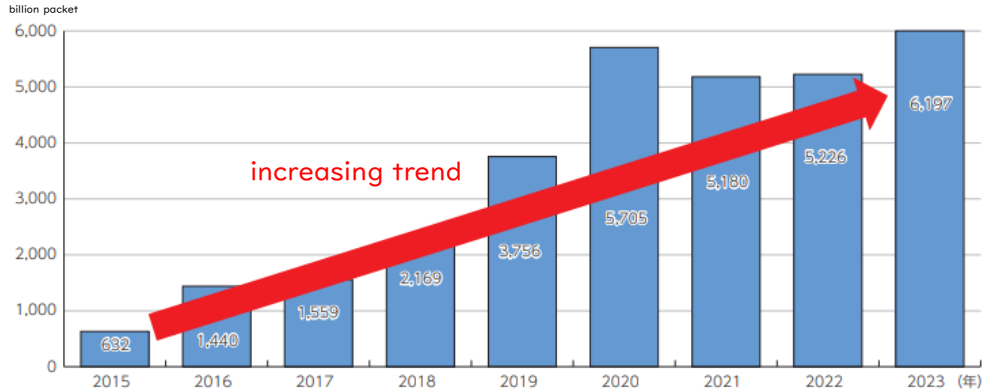
＋

- Steady penetration of DX into the corporate world
- Growing interest in cyber security measures

－

- **The number of cyber attacks is increasing every year**
  The total annual number of cyber attack-related communications (packets) in 2023 will reach a record high of approximately 619.7 billion packets
- **The reality of service suspension and discontinuation**
  If cyber security measures are not taken, the reality of not only the loss of confidential information and leakage due to unauthorized access, etc., but also the suspension or discontinuation of services in the core business has occurred.
- Cybersecurity Workforce Shortage

【Number of cyber attack-related communications】



<Source> DX Trend 2024

【Specific damage】

Company Type	summary	result
Retail	Fraudulent charges and usage occur	abolition
Human resources service industry	Consent form not implemented	suspension
Entertainment	Cyber attacks targeting servers of major services	Service suspension for more than 1 month

＜Source＞Prepared by the secretariat based on various media reports

3. Three issues from the current situation

- Organized into three issues based on the recognition of the current situation in the era of “Cyber Security Everywhere.

Awareness of the existing situation

Attack surfaces increase
The cybercrime ecosystem matures
Attacks become more sophisticated with the development
Geopolitical risks

【Awareness World】
「Cyber Security Everywhere」

＋
DX penetration
Growing interest in cyber security measures

－
Number of cyber attacks increases every year
Reality of service outages and discontinuance
Shortage of cyber security personnel

Three issues

Management issues, always contingency planning

- In the era of “Cyber Security Everywhere,” top management should shift from defense to offense in order to position cyber security as an important management issue.
- CISO and other systems should be established, and top management should always be aware of contingencies, have an organization that can respond promptly and effectively, understand risks, and promote flexible measures.

Strengthening Governance

- To strengthen cybersecurity governance, discussions and monitoring by specialized directors are needed.
- To support this, it is also important to visualize and quantify risks, formulate plans for incidents, and in terms of budgets, to keep IT and security budgets independent.
- Discuss and invest in the mid- to long-term and respond flexibly to changing threats

Human resource development and acquisition

- In order to strengthen the human resources supporting cybersecurity,
- it is important to define the human resources needed for cybersecurity based on the company's strategy.
- Build a strong security system by providing systematic training along with systems and information dissemination to secure human resources.

4. Eight action points for management

Three issues

Management issues, always contingency planning

- In the era of “Cyber Security Everywhere,” top management should shift from defense to offense in order to position cyber security as an important management issue.
- CISO and other systems should be established, and top management should always be aware of contingencies, have an organization that can respond promptly and effectively, understand risks, and promote flexible measures.

Strengthening Governance

- To strengthen cybersecurity governance, discussions and monitoring by specialized directors are needed.
- To support this, it is also important to visualize and quantify risks, formulate plans for incidents, and in terms of budgets, to keep IT and security budgets independent.
- Discuss and invest in the mid- to long-term and respond flexibly to changing threats

Human resource development and acquisition

- In order to strengthen the human resources supporting cybersecurity, it is important to define the human resources needed for cybersecurity based on the company's strategy.
- Build a strong security system by providing systematic training along with systems and information dissemination to secure human resources.

Eight actions that management should address

- ①Making Cybersecurity a Driver of Growth
- ②Systemic reinforcement
- ③Specialized director discussions/monitoring
- ④Visualization and quantification of risk
- ⑤Risk response planning
- ⑥Budget Independence
- ⑦Defining Human Resources
- ⑧Human resource development and acquisition

5． Six points of policy proposal to the government

- Based on the eight actions that management should take and global trends, we have organized our recommendations to the government into six categories.

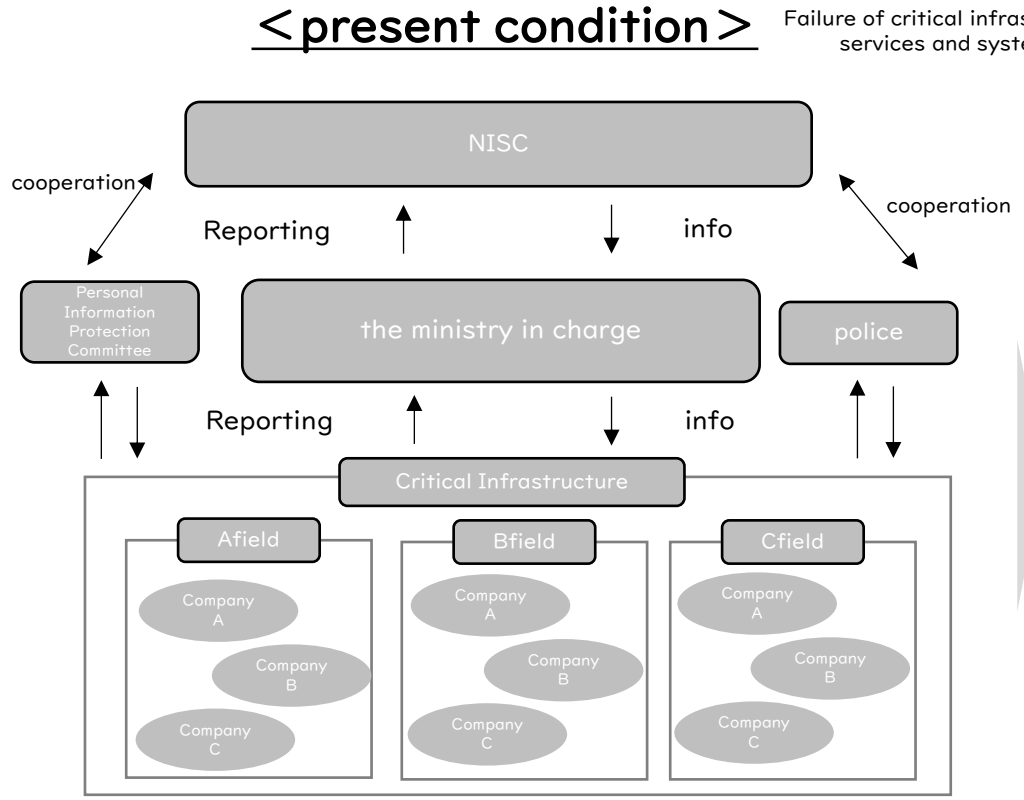
Theme	Message
①Active Cyber Defense・Strengthen NISC's command post functions	• With the reality that we live in an era of “Cyber Security Everywhere,” active cyber defense should be introduced as soon as possible to eliminate in advance or prevent the spread of infringement in the event of a security or serious cyber attack threat. • The Cabinet Cyber Security Center (NISC) must strengthen its command post function • Furthermore, in order for the security divisions of each ministry and agency to cooperate with each other, consideration should be given to **assigning cyber security personnel from each ministry and agency to NISC concurrently**, and to having the cyber security divisions of each ministry and agency physically **work together in the same office.**
②Mandatory reporting for critical infrastructure providers/Public-private partnership ※Reference Materials	• Information is the most important factor in cybersecurity. Therefore, **mandatory reporting to critical infrastructure providers should be introduced as soon as possible.** **＜New ways of public-private partnerships＞** • A public-private partnership organization in the field of cyber security should be created in NISC to strengthen its command post function. • With the concept of **“give and take” in mind**, the new public-private partnership organization should collect and provide information and support for incident response. **It should also seek to build a relationship of trust through regular meetings, workshops, and personnel exchanges between the public and private sectors.※** • Since this is a new public-private partnership initiative, NISC and other government ministries and agencies should cooperate with each other more than before. **＜Contents of information provided＞** • Information to be provided to the private sector should be useful in determining the awareness of management. For example, **information on the attacker's entity, purpose, and background; the urgency and importance of the attack; the expected damage and ripple effects of the attack; and the initial and medium- to long-term responses.** • The security clearance system should be utilized and fully utilized in the provision of information. ＜Methods for reporting and providing information＞ • Currently, indent reports are made to the supervising ministries and agencies of each service provider in accordance with each industry law, guidelines, etc., but real-time reporting is lacking. Therefore, **the incident reporting should be centralized**. • In addition, the content of reports differs depending on the supervising ministries and agencies, with many parts being left open-ended and formatted in Word or Excel. Therefore, in addition to **unifying the reporting format**, a mechanism should be established to **centralize reporting and consolidation to improve efficiency**.

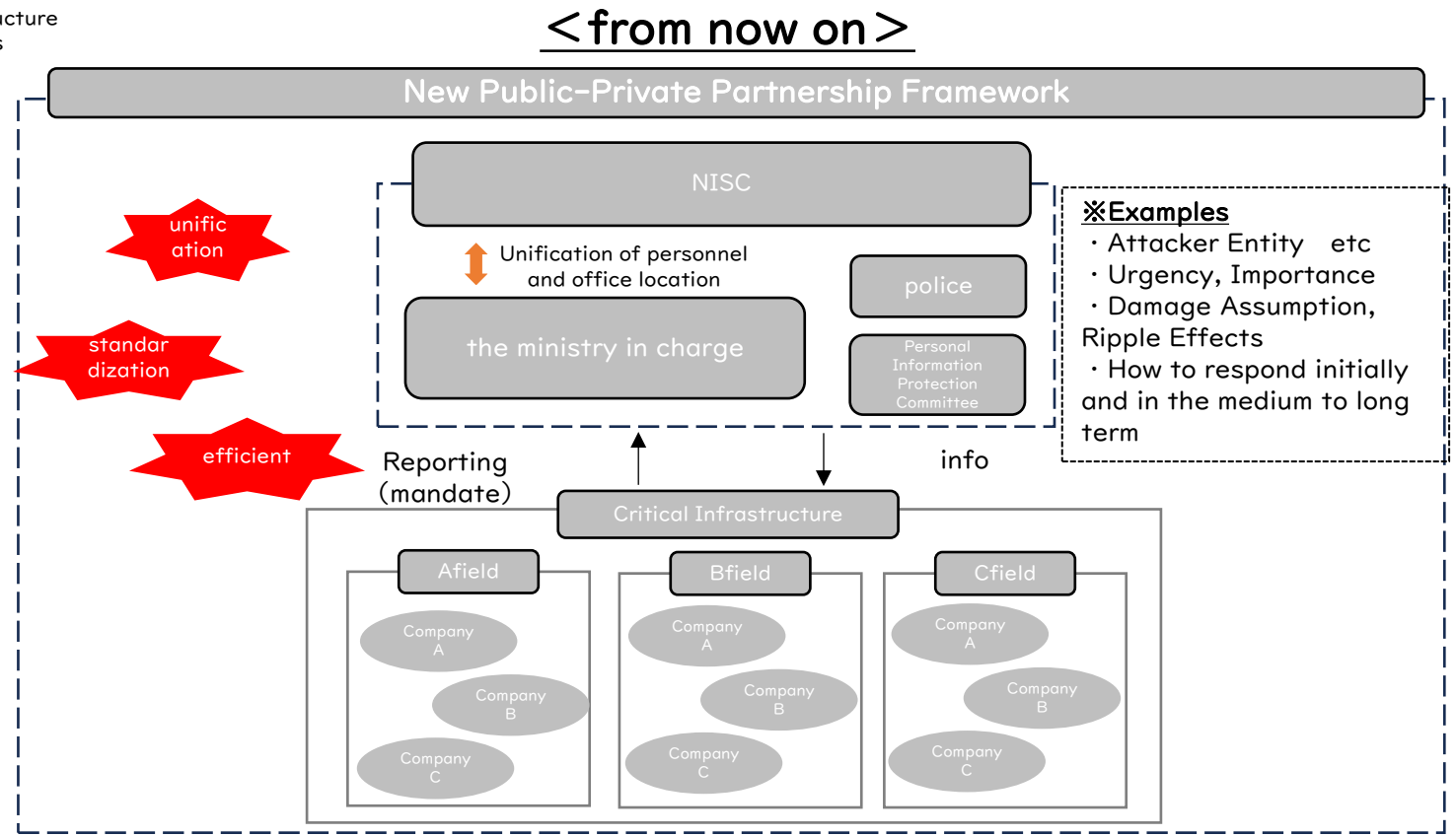
5． Six points of policy proposal to the government

Theme	Message
③Human Resource	＜Visualization of Human Resource Definition＞ • Visualization of human resource definition is important. The government should take the initiative in visualizing the definition of human resources, referring to the examples of other countries and domestic trends, in order to **establish a common understanding among industry, government, and academia in strengthening human resources for cyber security**. • In addition to the visualization of the definition of human resources, it is necessary to collaborate with educational institutions. The examples of other countries, such as the U.S. and Europe, should be referenced. ＜Expansion of the quality and quantity of educational institutions＞ • Security education should be provided from **the primary education level to secondary education**. • In order to expand top human resources**, it is necessary to expand the quality and quantity of human resources at technical colleges, universities, and graduate schools**. For example, a system that allows students to specialize in cyber security should be considered, based on the cyber academy introduced in Australia.
④Disclosure	• The Company should consider the obligation to include in **its annual securities report accurate and timely disclosure of material information on cybersecurity** (timely disclosure). In addition, the corporate governance code should include the formulation of policies on cybersecurity.
⑤Promotion of the cyber security industry	• **The supply of high-quality domestic security products and services should be strengthened。** • In addition, since it is necessary to deal with quantum computer resistant cryptography, a roadmap should be drawn by both the government-led and private sectors.
⑥Cyber insurance	• **The government should take the lead in creating options for data aggregation, analysis, etc., as a framework for risk assessment through cyber insurance.**

(Reference) The state of public-private partnerships

- NISC has established a new framework for public-private partnerships by becoming a command post for cyber security. The new framework will include meetings, incident response, human resource exchange, etc., as well as centralization of reporting parties, unification of content, etc., and streamlining of operations.





・Absence of a command post function in cyber security
・Lack of real-time incident reporting
・Variations in reporting content and format, and existence of manual work

・NISC functions as a cyber security command post
・Improvement of real-time performance by centralizing incident reporting
・Unification of reporting contents and format, and streamlining of work