Section 4 Cybersecurity

While the use of digital technologies is expanding in all aspects of society, cyberattacks are becoming more complex and sophisticated against the backdrop of a destabilizing and tense global situation, and the expansion of digital use is leading to increased system complexity and an broadening of the attack surface facing the Internet. As a result, security risks such as the leakage of confidential information due to ransomware and zero-day attacks and the suspension of services of critical infrastructure are on the rise.

As society becomes more dependent on digital infrastructure, the scale and scope of damage caused by a cyber incident is expected to expand further, posing serious security concerns.

Ensuring cybersecurity in the digital space requires that stakeholders raise their standards and work together. It is important to take comprehensive measures by all stakeholders, including government responses, public-private collaboration, international cooperation, technological measures, and the improvement of citizens' literacy.

1. Overview of key challenges

The risk of cyberattacks is increasing year by year. For example, according to the National Institute of Information and Communications Technology (NICT), the total number of packets observed per IP address in NICTER's darknet observation network increased in 2024 compared to the previous year, suggesting that reconnaissance activities on the Internet are becoming even more active[1].

Furthermore, if critical infrastructure for socio-economic activities were to be damaged or its services suspended due to a cyberattack, it could cause major social unrest. During FY2024, various cyberattacks targeting critical infrastructure and other areas occurred.

Figure (related data) Examples of cyberattack damage related to critical infrastructure in Japan in FY2024
Source: Prepared from published materials, etc.
URL: https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r07/html/datashu.html#f00075
(Data collection)

2. Direction of response

Ensuring cybersecurity in the digital space requires that all stakeholders raise their standards and work together. Here, a recent trend in the government's response, which is the establishment of legislation regarding active cyber defense, will be discussed.

In recent years, the theft of information from internal systems of governments and companies through cyberattacks has become a major problem, and concerns are rapidly growing about cyberattacks with advanced intrusion and hiding capabilities aimed at shutting down the functions of critical infrastructure, etc. In particular, serious cyberattacks aimed at disrupting or destroying critical infrastructure are becoming a major security concern, as they are being carried out on a daily basis, including state-sponsored cyberattacks.

In order to address this situation, based on the "National Security Strategy" (Cabinet decision of December 16, 2022), and to improve Japan's response capabilities in the field of cybersecurity to the same level as major European and American countries, two bills were submitted to the 217th session of the Diet (ordinary session) in 2025: "the Act on the Prevention of Damage from Unauthorized Acts Against Critical Computers" and "the Act Concerning Development of Laws Related to Enforcement of the Act on the Prevention of Damage from Unauthorized Acts Against Critical Computers" After amendments to the original drafts, the bills were passed and enacted in May 2025.

[1] Refer to "Current status of cybersecurity" in Section 10, 2, Chapter 1, Part II