Measures to Ensure Security in Cyberspace

To prevent cyberattacks, it is essential to strengthen measures at both the individual and state level (image photo)

Photo: metamorworks / PIXTA

Japan is implementing a range of measures to ensure security in cyberspace.

SAWAJI OSAMU

In recent years, cyberattacks aimed at disrupting business operations, stealing confidential information, acquiring money and other nefarious goals have increased both in Japan and overseas. In Japan alone, this year (2022) the damages caused by cyberattacks have included forcing the affiliate of a major automaker to shut down plant operations, and rendering the electronic medical records of a hospital unusable. The methods employed by attackers have become increasingly sophisticated, including attacks that exploit vulnerabilities in computer systems, and attacks that exploit the psychology of the people using a system. Today the activities of malicious actors in cyberspace have come to represent a serious threat to economic development and the security of people's daily lives. On top of that, it is believed that some states are strengthening their cyber warfare capabilities involving activities such as stealing informa-

Functions of the Public Security Intelligence Agency (PSIA)

Figure: Courtesy of the Public Security Intelligence Agency

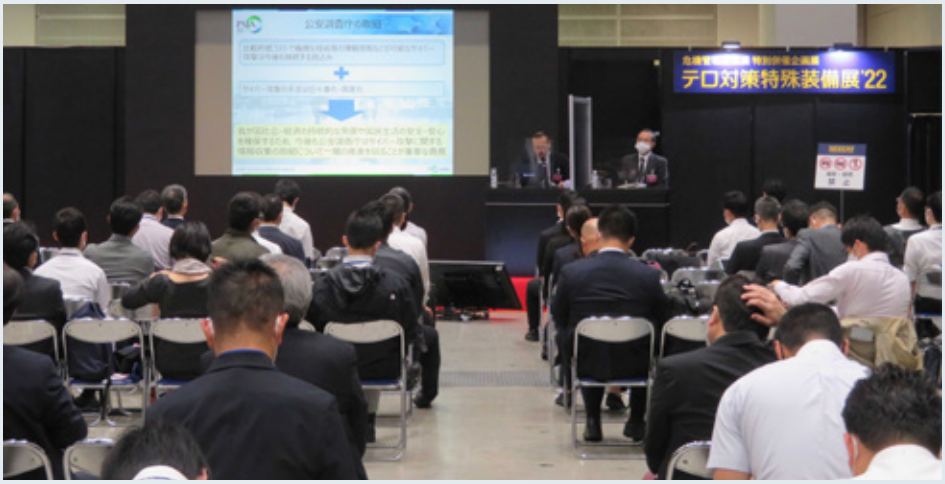
Cover of "Overview of Threats in Cyberspace 2022," a brochure published by the Public Security Intelligence Agency

Photo: Courtesy of the Public Security Intelligence Agency

tion or damaging infrastructure for political, economic or military ends, making the threat of cyberattacks of growing concern in terms of national security as well.

To prevent cyberattacks, each individual needs to keep the applications they use on devices such as PCs and smartphones up to date and take precautions such as not clicking on attachments or URLs in suspicious emails, SMS (short message service) and social media. It is also essential to strengthen measures at the state level.

Given these circumstances, in September 2021 the Japanese government established a Cybersecurity Strategy (hereinafter, "the Strategy") by Cabinet decision. The Strategy is formulated based on the Basic Act on Cybersecurity which was enacted in 2014 to comprehensively and efficiently promote measures on cybersecurity, and this latest version of the Strategy is the third one.



An official of the Public Security Intelligence Agency (PSIA) delivering a lecture at SEECAT (Special Equipment Exhibition & Conference for Anti-Terrorism) 2022 held in Tokyo in October

Photo: Courtesy of the Public Security Intelligence Agency

As for cybersecurity, the Strategy states, "to meet the expectations of the people, cybersecurity policies should safeguard their free economic and social activities, secure their rights and convenience, and protect them by deterring the activities of malicious actors through law enforcement and legal systems in a timely and appropriate manner." Under the Strategy, strengthening the framework for national CSIRTs/CERTs (Computer Security Incident Response Team/Computer Emergency Response Team) by the government is cited as one of the measures to be taken. National CSIRTs/CERTs are positioned as "a function responsible for general coordination in the event of a serious cyberattack to enable a series of actions ranging from information collection and analysis to investigation, evaluation, issuing alerts, responding to the attack, and subsequent planning of policy measures to prevent recurrence, etc., to be pursued in an integrated manner." The Strategy also incorporates measures to enhance the posture of cyber-related units and fundamentally strengthen cyber defense capabilities in the Ministry of Defense and Japan Self-Defense Forces, advance cooperation with like-minded countries including the United States, Australia, India and ASEAN members, and lead international cyber exercises.

The Public Security Intelligence Agency (PSIA) is one of the Japanese government agencies tasked with ensuring security in cyberspace. To ensure public security, the PSIA collects and analyzes information from Japan and abroad including the situation related to economic security, the trend of international terrorism, situation of neighboring countries and the activities of various domestic organizations, and provides the intelligence to relevant government agencies.

In terms of the role played by the PSIA in cybersecurity, Cybersecurity 2022, the latest annual plan based on the Strategy, states that the PSIA, "in order to promote investigation related to cyberspace, promotes efforts to contribute to cyber-intelligence countermeasures such as strengthening systems of collecting and analyzing HUMINT (human intelligence) information and providing it to relevant agencies and organizations in a timely and appropriate manner." More specifically, the PSIA clarifies the actual states of actors who have launched cyberattacks and provides the intelligence to government agencies, or identifies the signs of an impending cyberattack on government agencies or corporations at an early stage and provides the intelligence to the relevant bodies. To strengthen these initiatives, in April 2022 the PSIA launched the Cybersecurity Intelligence Office. The agency also exchanges views on cybersecurity with economic groups, companies, universities and research bodies, conducts lectures for the general public, and prepares cybersecurity brochures as part of efforts to raise awareness.

Cyberattacks are now events that affect all of us. The growing threat of cyberattacks has made it increasingly important for members of the public, companies and the government to work together.

Note: This article has been created with the consent of the PSIA and on the basis of materials published by the agency.