Keidanren
Policy & Action

Proposal for Reinforcing Cybersecurity Measures (Summary)

February 17, 2015
KEIDANREN (Japan Business Federation)

Damage from cyberattacks is increasing its seriousness throughout the world. Japan has been enhancing measures. Keidanren made the proposal to enhance cybersecurity measures for critical infrastructures, etc. that would affect people's daily lives and economic activities.

1. Situations inside and outside Japan

(1) International situation

Cyberattacks occurred in the 2012 London Olympics in the U.K. and in the U.S. at the end of last year.

(2) Domestic situation

The number of cyberattacks has been increasing. Formulation of the Basic Act on Cybersecurity and establishment of the Cybersecurity Strategic Headquarters. Measures for the 2020 Tokyo Olympics/Paralympics are urgently required.

2. Threat of cyberattacks

If information and communication services, financial services, railway services, electric power supply services, and gas supply services, etc. shut down, it is difficult for Japan to maintain its function as a nation.

(1) Characteristics of cyberattacks: It is difficult to identify attackers. Attackers always maintain advantageous positions.

(2) Countermeasures against cyberattacks: It is difficult to prevent all of the attacks. Minimization of damage is important.

(3) Expansion in attack targets: Control systems and smartphones, etc. are attack targets in addition to information systems.

3. Cybersecurity measures against critical infrastructures, etc.

The government needs to make clear its intention to protect critical infrastructures, etc. from cyberattacks and to improve deterrent capabilities.

(1) Specific policies

① Enhancement of information sharing

Enhancement of the information sharing system among a number of committee bodies regarding cyberattacks.
Consideration of specific information sharing methods between public and private entities regarding damage, response, and prevention, etc.

② Implementation of training

Establishment of the decision-making standard and guidelines against major cyberattacks and joint implementation of training/demonstrations between public and private entities.

③ Technology development and system operation

Technology development to detect attacks beforehand, disable them, detect and trace them, and share information, etc.
Incorporation into the 5th Science and Technology Basic Plan. Continuous operation of reliable defense systems and enhancement of capabilities.

④ Enhancement of human resources

Enhancement of the quality and quantity of security human resources through the development of the top-level human resources and white-hat hackers as well as government-industry-academia collaboration.

⑤ Promotion of international cooperation

Sharing of information with overseas. Consideration of international systems to trace, identify, and respond to attackers.
Hosting of international conferences.

⑥ Review of critical infrastructure areas

Review of the current 13 areas. Consideration of adding new network-related services, such as smart cities and ITS.

⑦ Enhancement of internet safety

Enhancement of knowledge among internet users.

(2) Establishment of government system

Centralization of information aggregation functions in the Cabinet Secretariat. Cybersecurity Strategic Headquarters to execute leadership.

4. Business Community's Efforts

The business community will position cybersecurity as an important management task and promote the reform of the top management's awareness, organizational reforms, human resource development, cross-industrial information exchanges, and opinion exchanges. Companies will support security courses in universities/graduate schools. These efforts will lead to the enhancement of national cybersecurity.