Keidanren
Policy & Action

Second Proposal for Reinforcing Cybersecurity Measures (Summary)

January 19, 2016
KEIDANREN (Japan Business Federation)

1. Introduction

■The Japanese government's promotion system has been enhanced as seen in the examples of enforcement of the Basic Act on Cybersecurity and the establishment of the Cybersecurity Strategic Headquarters in January of last year.

■On the other hand, the number of cyberattacks against government organizations and companies has increased. Personal information leaked from Japan Pension Service in May of last year.

■Cyberspace is an important place to realize growth strategies through creation of innovations. We are facing a critical situation in preparation for the 2020 Tokyo Olympics/Paralympics. The government established the Cybersecurity Strategy in September of last year.

■Keidanren has published the second proposal regarding enhancement of government-industry-academia collaboration and specific efforts by the industry.

2. Significance of cybersecurity

■Enhancement of comprehensive measures in public organizations (central government ministries and agencies, independent administrative corporations, and quasi-governmental corporations, etc.). Enhancement of measures involving local public organizations through the introduction of the Individual Number system.

■Safe utilization of IoT (Internet of Things) connecting to the internet.

■Response to problems in companies' business operation and risks of loss of reliability due to information leaks, etc. caused by cyberattacks.

■Security of free international flow of information in cyberspace.

3. Cybersecurity measures

(1) Information sharing

Two-way information sharing between government organizations and companies. Establishment of ISAC (Information Sharing and Analysis Center) and CSIRT (Computer Security Incident Response Team), etc. in industries and companies. Information sharing while maintaining confidential information.

(2) Human resource development

Clarification of human resources requirements. Education according to human resource levels in universities, etc. Review of assessment and treatment in companies. Establishment of systems for human resource development and maintenance by the government, industry, and academia.

(3) Establishment of systems with high security levels

① Social systems

Focused protection of critical infrastructures and review of the scope. Establishment of a system in which sophisticated human resources can flexibly transfer between government, industry, and academia.

② Technology development and system operation

Technology development, such as communication detection and attack analysis. Stable operations of systems.

Expectations toward the Cabinet Office's SIP: Cross-ministerial Strategic Innovation Promotion Program and activities of the IoT Acceleration Consortium.

(4) Promotion of international cooperation

Proactive participation in international discussions. Collaboration with the U.S., Europe, ASEAN, etc.

(5) Response to the Tokyo Olympics/Paralympics

Implementation of comprehensive measures, including peripheral facilities, etc. in addition to competition venues. Early establishment of the core CSIRT. Promotion of demonstrations/training. Enhancement of capabilities of the existing human resources. Establishment of the system by NISC (National center of Incident readiness and Strategy for Cybersecurity in the Cabinet Secretariat) and formulation and implementation of a roadmap of measures.

4. Business Community's Efforts

The business community will position cybersecurity as an important management task and reform the awareness of the top management. It will also voluntarily and swiftly promote the establishment of organizations/systems, information sharing, and human resource development. Voluntary information disclosure to stakeholders.

Development of systems and provision of products that ensure security. Provision of cybersecurity insurance.