DECLARATION OF CYBER SECURITY MANAGEMENT
経団連サイバーセキュリティ経営宣言

March 2018
Keidanren

Information technology is being integrated into an increasing number of spheres in the aim of realizing Society 5.0, where the latest technology and data will be used to enhance productivity and resolve issues throughout society. However, significant malicious conduct that threatens cyberspace safety and order is also widespread. From the dual perspectives of creating value and managing risk, cybersecurity measures are now a key management priority for all companies.

The business community takes responsibility for many vital elements of infrastructure and supplies a wide array of products and services, and is acutely aware of the need to take its own cybersecurity steps.

All businesses will implement cybersecurity measures and contribute to making cyberspace safe and secure. Placing priority on the run-up to the 2020 Tokyo Olympics and Paralympics, when cyberattacks are likely to intensify, business leaders pledge to address the following points:

1 Recognize Cybersecurity as a Management Issue

- Enhance their own understanding of the latest cybersecurity circumstances and actively engage in management by positioning cybersecurity spending as an investment.
- Take responsibility themselves for cybersecurity measures while recognizing that cybersecurity is a critical management issue, confronting realities, addressing risks, and exercising leadership.

2 Develop Management Policies and Declare Intentions

- Develop management policies and business continuity plans aimed at prompt recovery from security incidents while prioritizing detection, response, and recovery in addition to identifying and protecting against risks.
- Take the lead in declaring companies' intentions to internal and external stakeholders and make every effort to voluntarily disclose recognized risks, and measures to deal with them, in corporate reporting.

3 Build Internal and External Systems and Implement Security Measures

- Ensure sufficient resources including budgets and personnel, establish internal systems, and take necessary human, technical, and physical measures.
- Develop human resources and conduct training required for those at every level, including the management, corporate planning staff, technical specialists, and other employees.
- Manage cybersecurity throughout domestic and international supply chains, including business partners and outsourcing contractors.

4 Contribute to Widespread Use of Cybersafe Products, Systems, and Services

- Manage cybersecurity across the full spectrum of corporate activity, including development, design, production, and supply of products, systems, and services.

5 Contribute to Building Safe and Secure Ecosystems

- Collaborate with relevant government agencies, organizations, industry associations, and other bodies to actively share information, engage in dialogue, and build human networks, both in Japan and internationally.
- Contribute to reinforcement of cybersecurity throughout society by raising awareness of measures taken on the basis of such information.