JFE-SIRT

Like approaches preventing pollution during the years of high economic growth and more recent efforts curbing global warming, enhancing information security to safeguard corporate activities, in cooperation with stakeholders, including customers, business partners and government agencies, is one of top management's priorities that companies must proactively address to realize continuous growth.

It is thus important to establish a structure applicable on a groupwide basis and to maintain investment at a level commensurate to risk.

Every employee must also understand the vital significance of information security, taking a sense of ownership and treating systems and information carefully. This awareness and attitude have the potential to dramatically reduce the risk of major incidents, and I believe that cultivating a corporate culture that emphasizes information security through messages from management, education and drills is of great importance.

With this in mind, we created JFE-SIRT by gathering an elite team from all areas. As a team, we work with the three operating companies and other Group companies to promote measures covering systems, technologies and training on information security.

Michinari Tanaka
Team Leader, JFE-SIRT

Formulating the Declaration of Cybersecurity Management

The JFE Group*1 formulated its Declaration of Cyber Security Management, based on the Declaration by Keidanren, the Japanese Business Federation, in March 2018.

The JFE Group acknowledges the importance of cybersecurity measures. In formulating our management strategy, we recognize the risk of cyberattack as a key management priority. We have drafted appropriate management strategies to counteract this threat. Also, we assign high-level professionals to cybersecurity management, hinging on JFE-SIRT. We take a variety of measures drawing on intelligence and advanced technologies gathered through links to external specialists, and also direct concerted efforts into human resources development from a medium- to long-term perspective.

Under this declaration, for fighting further serious and sophisticated cyberthreats, we are more greatly reinforcing management-led cybersecurity measures.

*1 Group companies subject to this declaration:
JFE Holdings, Inc., JFE Steel Corporation, JFE Engineering Corporation, JFE Shoji Trade Corporation and all group companies of the three operating companies.

JFE Group Declaration of Cybersecurity Management

1 Recognize cybersecurity as a management issue

The JFE Group recognizes cyber-related risk as a key management priority. We shall enhance our own understanding of the latest cybersecurity developments and actively engage in management by positioning cybersecurity spending as an investment.

Management shall enhance their cybersecurity measures with responsibility while confronting realities, addressing risks, and exercising leadership. Members of management shall chair cybersecurity-related committees at JFE Holdings and its three operating companies, promote constructive discussions, validate various measures and allocate appropriate resources to whatever measures deemed necessary.

2 Determine management policies and declare intentions

The JFE Group shall determine management policies and draft a business continuity plan (BCP) aimed at quick recovery in the event of a cybersecurity incident, emphasizing not only identification and defense, but also detection, response and recovery.

Every year, the JFE Group shall lay out a cybersecurity action plan for the Group, reflecting a review of risk identification, defense mechanisms and guidelines for responding to an information security incident. Also, the JFE Group shall strengthen incident response capabilities through regular drills and prepare the BCP. Furthermore the JFE Group shall periodically conduct cybersecurity audits on JFE Group companies. Through these efforts, the JFE Group aims to steadily raise the level of the overall Group.

Management shall 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

The JFE Group shall establish internal systems mainly through JFE-SIRT, ensure sufficient resources including budgets and personnel, and take necessary human, technical, and physical measures.

Using various internal and external human resources development programs, the JFE Group shall cultivate the skills of high-level, professional staff with detailed knowledge of cybersecurity and shall work with external specialists to leverage the benefits of sharing know-how. The JFE Group shall strive to educate and motivate employees at every level in all divisions at each company under the JFE Group umbrella through in-house training and drills, as well as participation in cross-industry exercises.

The JFE Group shall manage cybersecurity throughout domestic and international supply chains by monitoring security measures at outsourcing contractors and others on the supply chain.

4 Encourage widespread use of cybersafe products, systems and services

The JFE Group shall manage cybersecurity across the full spectrum of corporate activity, including development, design, production, and supply of products, systems, and services.

5 Help build safe and secure ecosystems

The JFE Group shall 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. The JFE Group shall contribute to reinforcement of cybersecurity throughout global society by raising awareness of measures taken on the basis of such information.