Information security governance to support DX promotion

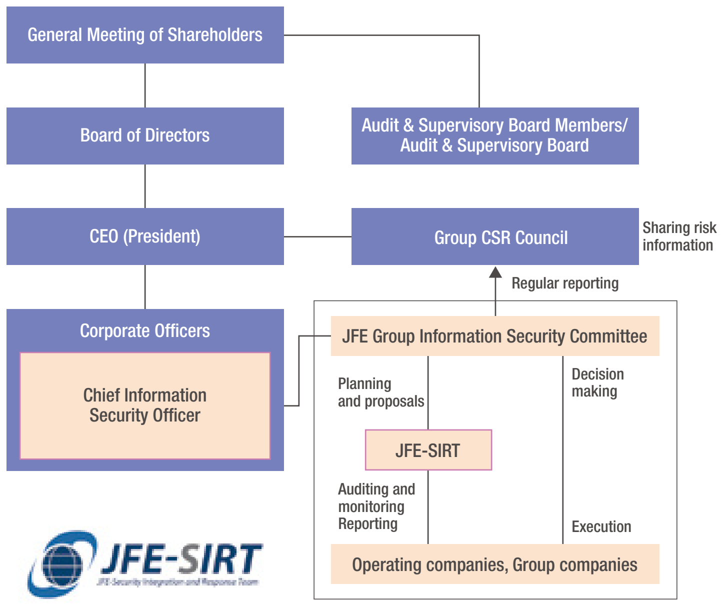
Information Security Management

To prevent cyberattacks and unauthorized use of systems and thus confidently engage in business activities, the JFE Group is constantly working to improve its level of information security management through the following measures.

JFE Group information security management structure

After the release of the Ministry of Economy, Trade and Industry's Cybersecurity Management Guidelines in 2015, JFE Holdings established the JFE Group Information Security Committee in April 2016 for the ongoing maintenance and strengthening of IT risk management functions Groupwide. Led by the JFE Group Chief Information Security Officer*1 at JFE Holdings, officers responsible for IT divisions at each operating company discuss important issues related to information technology and set Groupwide policies focusing on information security. In addition, JFE-SIRT, made up of IT division managers at all operating companies, was established and is working to strengthen security countermeasures and governance at operating companies and their group companies, on the basis of decisions made by the JFE Group Information Security Committee.

JFE Group information security management structure


General Meeting of Shareholders
Board of Directors
Audit & Supervisory Board Members/
Audit & Supervisory Board
CEO (President)
Group CSR Council
Sharing risk information
Regular reporting
Corporate Officers
Chief Information Security Officer
JFE Group Information Security Committee
Planning and proposals
Decision making
JFE-SIRT
Auditing and monitoring Reporting
Execution
Operating companies, Group companies
JFE-SIRT

The JFE Security Integration and Response Team (JFE-SIRT) is a CSIRT*2 responsible for planning, proposing, and promoting Groupwide measures, auditing Group companies, reviewing security policy, and responding to information security incidents.

*1. Chief Information Security Officer (CISO): The officer in charge of information security, who is responsible for information management and use within companies and organizations

*2. Computer Security Incident Response Team (CSIRT): A general term for a group that responds to internal computer security-related incidents when they occur

Message from JFE-SIRT

Digital transformation (DX) initiatives are becoming increasingly active. The JFE Group has designated working together to promote DX as an important Group strategy. Through DX, we are proactively incorporating new technologies and using information assets to increase productivity, transform businesses, and create new value, although use of DX also invites new cybersecurity risks. We need to appropriately protect these information assets from such risks to ensure that we provide our customers with high-quality and secure goods and services and meet our responsibilities as part of supply chains.

The JFE Group launched the Information Security Committee and JFE-SIRT framework in 2016, as we strive to raise the level of cybersecurity countermeasures across the entire Group, including in the areas of information technology and operational technology, in Japan and overseas. We will steadily continue to build on this framework and further develop it to contribute to promoting the DX strategy.

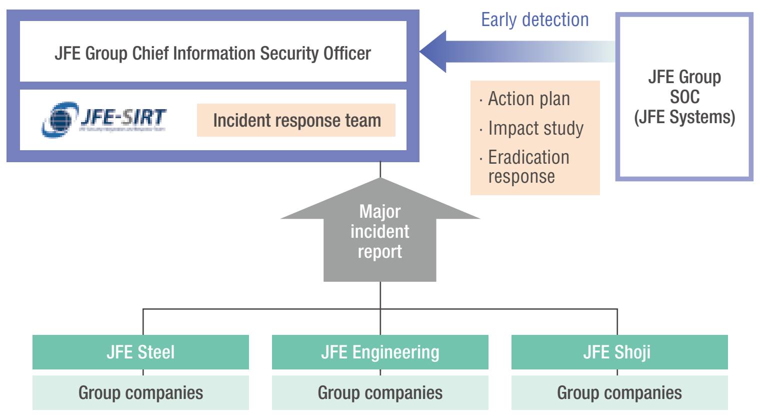
Ken Sakata
Team Leader, JFE-SIRT

Integrated security monitoring network

Targeted cyberattacks against companies are becoming more ingenious every day, including many cases in which significant time passes before a company learns it has been attacked, by which time information assets have already been stolen. To detect these threats at an early stage and prevent damage as much as possible, a framework for integrated security monitoring is required at multiple levels, from personal computers to networks. Our Groupwide SOC*3 structure was established to facilitate constant monitoring across the entire JFE Group. When a security incident does occur at a company, JFE-SIRT is the structure for swift reporting, responding, recovering, and proposing measures to prevent a reoccurrence, under the guidance of the JFE Group Chief Information Security Officer.

*3. Security Operation Center (SOC): The organization that monitors networks and devices by detecting, analyzing, and giving advice on responding to cyberattacks

Integrated security monitoring network

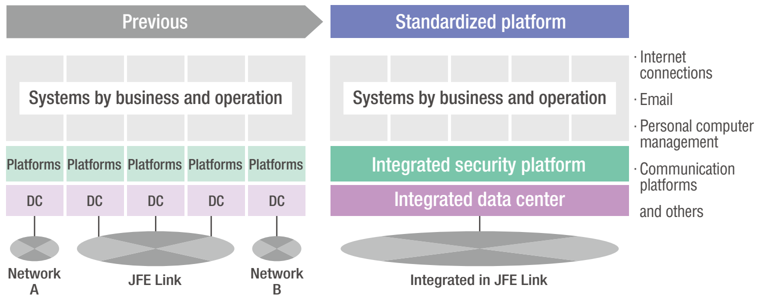


Integrating the Group's security platform

We are promoting a common information security platform covering networks, IT equipment, and security-related software, to raise the level of information security across the entire Group and protect the Group's information assets from increasingly sophisticated cyberattacks. Even if an information security incident were to occur, a common platform makes possible an accurate assessment of the threat and a rapid response.

We are also introducing a common information communication platform for cloud computing, which we recently began using, to promote the safe sharing of information within the Group and contribute to business creation across the Group in the area of DX.

Group security platform integration



Disclosure of cybersecurity information

JFE Holdings releases information about our information security initiatives to shareholders, customers, suppliers, and other stakeholders. In addition, the Company is working to increase security awareness and raise the security level within every Group company through various opportunities for communication within the Group to help promote every Group company's digital transformation (DX).

Target	Purposes of information disclosure
Customers	To provide a sense of security when they use our products and services
Suppliers	To build relationships of trust in supply chains and as business partners
Shareholders, institutional investors	To demonstrate that we are a corporate group with appropriate risk management functions in place To facilitate an understanding of our corporate value with non-financial information
Employees	To instill a sense of individual pride and responsibility as a member of the JFE Group
Media	To raise awareness of the JFE brand in society

Information disclosure media

- Annual securities report (in Japanese)
- CSR Report
- Integrated Report (JFE Group Report)
- DX Report (this report)
- JFE Holdings and Group company websites, etc.

Issued in February 2021

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.

JFE

JFE Group

JFE Holdings, Inc.

2-2-3 Uchisaiwaicho, Chiyoda-ku, Tokyo 100-0011, Japan
http://www.jfe-holdings.co.jp/en/

Inquiries: Corporate Planning Department
JFE Holdings, Inc.
Tel: +81-3-3597-4321