Security Management

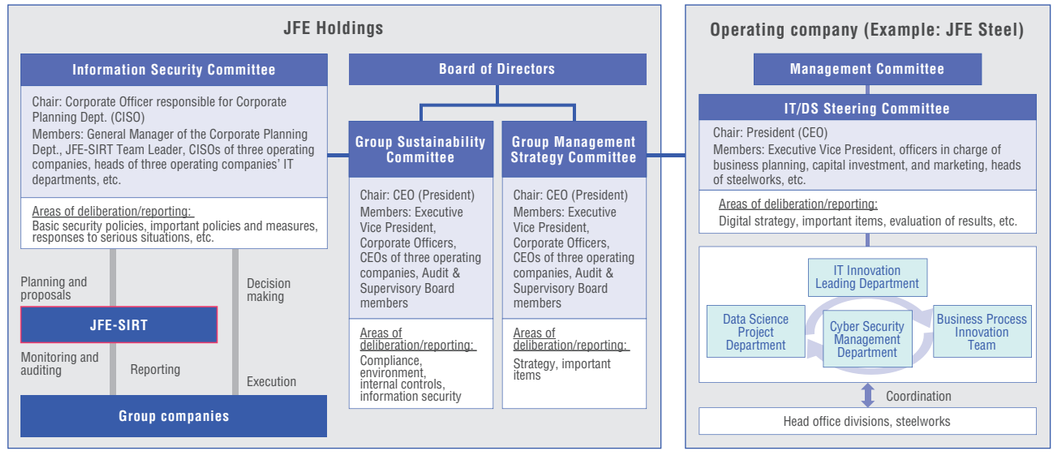
The JFE Group, which views security as an important activity that goes hand in hand with DX promotion, is working to strengthen security Groupwide in the face of increasingly serious and sophisticated threats.

With regulations for security management shared across the Group, we are strengthening our security under a uniform policy. Employees engage in drills and training at the Group level to respond to cyberattacks, and we are working to instill a thorough understanding of rules and raise the level of security-related knowledge. In addition to all Group companies implementing shared IT measures, we are working to raise the level of security management Groupwide through regular information security audits and other measures.

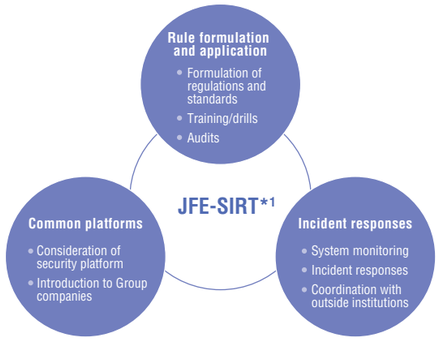
Security management

JFE Group's digital governance and cybersecurity framework

A Group digital governance structure and security structure are part of our corporate governance framework.

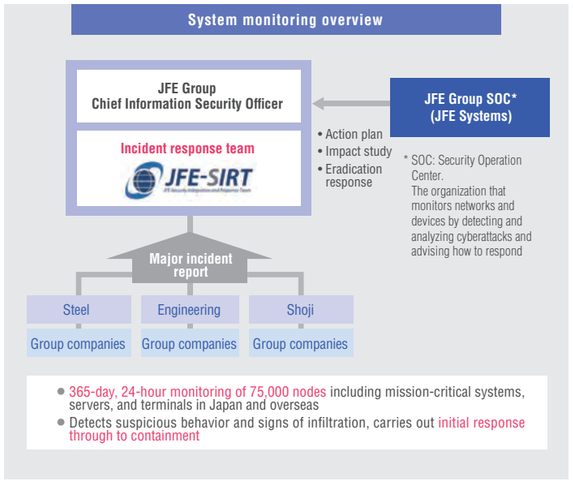


Cybersecurity monitoring initiatives



*1 JFE-SIRT: A CSIRT*2 responsible for responding to incidents of information security, as well as planning, proposing, and promoting Groupwide measures, auditing Group companies, and reviewing security policy

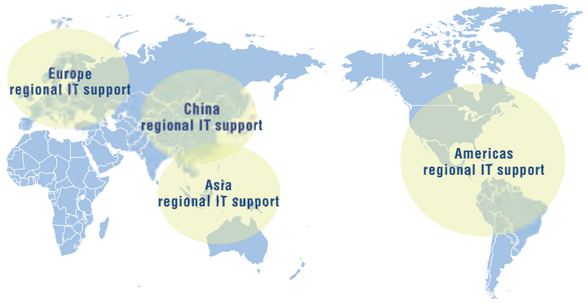
*2 CSIRT: Computer Security Incident Response Team. A general term for a group that responds to internal computer security-related incidents

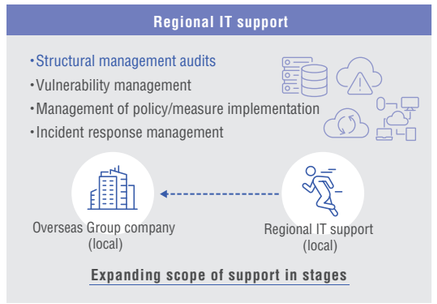


- 365-day, 24-hour monitoring of 75,000 nodes including mission-critical systems, servers, and terminals in Japan and overseas
- Detects suspicious behavior and signs of infiltration, carries out initial response through to containment

Strengthening the global structure

To strengthen security at overseas Group companies, Asia regional IT support began operating in fiscal 2023.





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 that is critical to DX promotion.

In facing the risks associated with digitalization, management recognizes the importance of strengthening cybersecurity across the entire supply chain, and will exercise leadership as it implements measures under its responsibility. 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 strive to address the entire supply chain, including overseas, using cybersecurity guidelines and frameworks, cooperating with government activities to support cybersecurity measures, and monitoring cybersecurity measures at subcontractors and other parties.

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.

Revised January 2023