Information Security Management

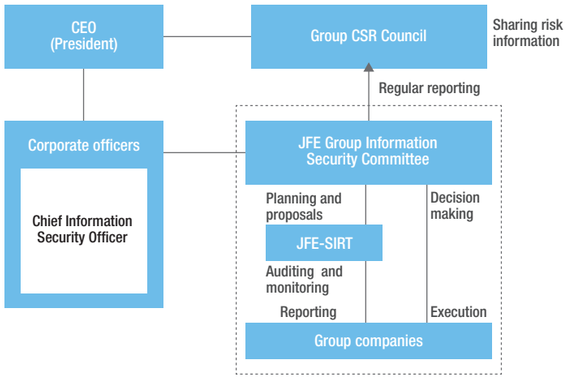
To prevent cyberattacks and unauthorized use of systems and thus confidently engage in business activities, the JFE Group is constantly working to improve its level of information security management through of the following measures.

1 Establish information security governance system

JFE Holdings established the JFE Group Information Security Committee as a substructure of the Group CSR Council. The committee is guided by JFE Group Chief Information Security Officer at the JFE Holdings and has the participation of officers responsible for IT divisions at each operating company. They discuss key issues related to IT, with an emphasis on information security, and determine the direction that the Group will take in that regard.

Based on the decisions made by this committee, the JFE-Security Integration and Response Team (JFE-SIRT), which has the participation of IT division managers from all operating companies, establishes rules and regulations, drafts and promotes the implementation of IT measures, performs information security audits and training, and offers guidance on responding to information security incidents. JFE-SIRT ensures the Group maintains a PDCA cycle for continuous improvements in information security.

JFE Group Information security governance system

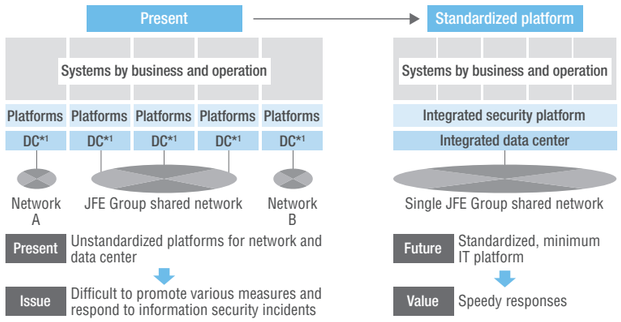


2 Key IT measures shared throughout the Group

JFE-SIRT and Group companies work together, as a cohesive unit, promoting a common information security platform comprising such components as networks, IT equipment and security-related software, to achieve the same level of information security initiatives throughout the Group and facilitate an immediate response just in case an information security incident arises. Also, efforts are directed toward consolidating procurement and reducing costs.

*1: DC = Data Center

JFE Group Key IT platform shared throughout the Group



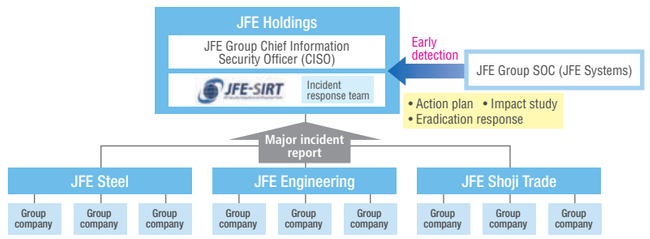
3 Establish information security incident response structure

JFE Holdings lays out the key points for responding when an information security incident occurs and, through JFE-SIRT, led by the JFE Group Chief Information Security Officer, the Company maintains a structure to ensure quick reporting, action and recovery should a situation occur and measures to prevent the situation from happening again.

To minimize damage caused by information security incidents, the Company has placed an integrated security monitoring net over the entire Group and is building a structure that enables the shared SOC*2 to detect emerging incidents at an early stage.

*2 SOC: Security Operation Center

JFE Group Integrated information security monitoring network

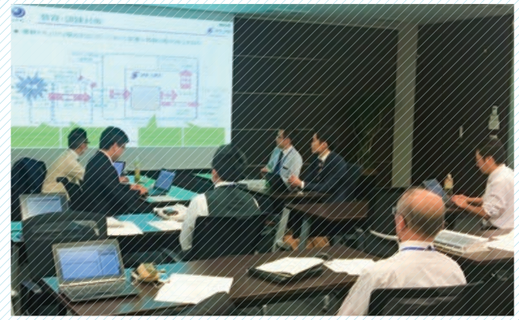


Cyberattack Response Drills (Tabletop)

To raise proficiency in responding to a cyberattack if one should occur, JFE-SIRT regularly runs cyberattack response drills in cooperation with three operating companies and an information systems subsidiary.

The participants are people who would take charge in the event of an incident. The scenario is modeled on past events and publicly disclosed cyberattacks, and built around key points for responding when an incident occurs.

Through these drills, participants confirm their roles and how they would cooperate with others and then discuss problem points to deepen their understanding of cyberattacks and responses. Measures for improvement that are identified during the drills are reflected in the daily activities of JFE-SIRT.



JFE-SIRT practice formats and direction of implementation

- Four practice formats matched to participants and purposes
- Gradually expand scenarios and scale of exercises to enhance response capability and reinforce responsiveness on an organizational level

Target	To enable CISO and JFE-SIRT-related divisions to acquire the ability to respond precisely to situations			
Method	Meeting-style discussions based on cyberattack scenarios to confirm and improve procedures			
Type	**Workshop**	**Tabletop drill**	**Function-specific drill**	**Integrated drill**
Purpose	Clarify incident-response procedures	Verify incident-response procedures based on anticipated practice scenarios	Confirm reporting procedures based on practice scenarios in actual operating environment	Cross-functional drill based on real and assumed scenarios with several structures involved
Invited participants	People who take initial action in an incident JFE-SIRT	People who take initial action in an incident JFE-SIRT	CISO JFE-SIRT	CISO JFE-SIRT Divisions involved in the incident
Goals	Stable, balanced response level			
Rules/procedures	Set out procedures	Improve procedures	Identify incident-response issues, improve rules	
Organization/ structure		Improve incident-response structure and monitoring functions	Improve incident-response structure and monitoring functions and confirm internal and external contacts	Confirm internal and external contacts
People		Raise participants' level of responsiveness		Cultivate awareness among management

JFE Holdings sent young engineers to the Core Human Resources Development Program at the Industrial Cyber Security Center of Excellence, established in 2017 by the Information-technology Promotion Agency, Japan. The knowledge gained will support enhanced security of the Group's control systems.