Information security governance underpinning competitive IT strategy

Information Security Management

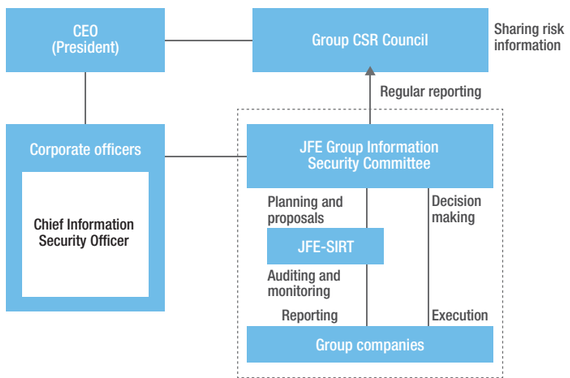
To prevent cyberattacks and unauthorized use of systems and thus confidently engage in business activities, the JFE Group is constantly working to improve its level of information security management through the following measures.

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 the JFE Group Chief Information Security Officer at 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

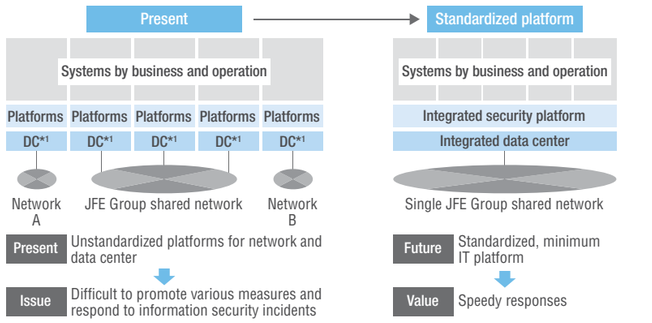


2 Key IT measures shared throughout the Group

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



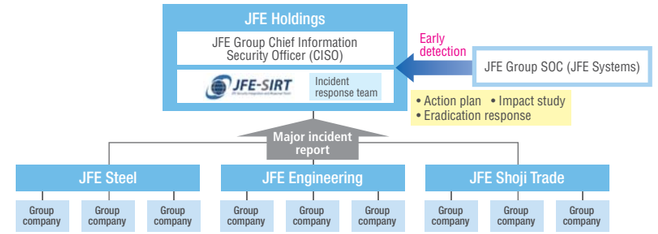
3 Establish information security incident response structure

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



Tabletop drills for JFE Group security staff

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

Based on key points for responding to an envisioned outbreak of an incident, participants confirm their respective roles and how they would cooperate with other persons involved, and discuss problems to deepen their understanding. Proposals for improvement arising from these drills are reflected in JFE-SIRT's daily activities.

From this fiscal year, tabletop drills are being carried out for information security staff at Group companies, to roll out SIRT's response expertise to Group companies.

Workshops are held to explain recent targeted cyberattacks and have group discussions in response to questions set in accordance with common cyberattack scenarios. These discussions review the situation at the company and consider response methods and preparations needed, from outbreak to resolution, providing an opportunity for these employees to recognize and take into account these issues in their daily work.

Group information security audit

During 2017–2018, JFE-SIRT carried out information security audits at approximately 260 JFE Group companies in Japan and overseas, to identify and respond to issues quickly, based on the common global information security policy. Notification of audit results and guidance for planning corrective measures lead to a higher level of information security across the entire Group, including an awareness of the importance and training in information security measures.

A second round of audits is also being carried out from the current fiscal year to raise the level of security even higher. These second audits confirm the progress being made in preparing logs and introducing common measures that are required in the event a security incident were to occur, to strengthen security measures at the Group overall.

Group Company Audit Policy

Self-examination Audited companies evaluate themselves and operating companies send an evaluation report via an operating company to JFE-SIRT, and JFE-SIRT audits the content and notifies the results.