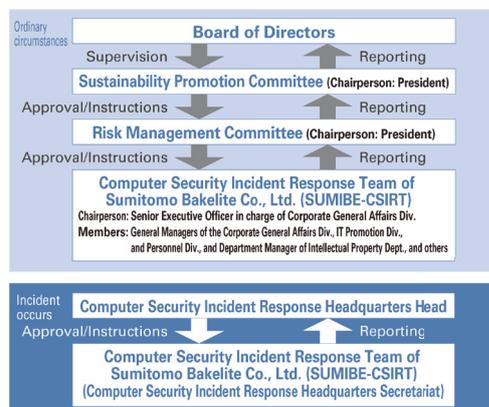# Information Security

Systems (Governance)

Our Group has established SUMIBE-CSIRT, a cross-organizational body to prepare for the occurrence of information security incidents, to share topics through regular meetings, formulate preventive measures to prevent information security-related incidents, and develop response procedures in the event of an incident. When an incident occurs, it is designed to respond to the situation, including management, and to cooperate with external security-related organizations.

● **Information Security Management Structure**

Risk Management

The identification, assessment, and management of risks and opportunities related to information security pertaining to our Group are carried out in accordance with the risk management system and risk management process described on the following link.

● Risk Management

Metrics and Targets

We have selected cybersecurity as one of our Group's material issues, and set the number of major cybersecurity incidents, cybersecurity training participation rate, and the number of cybersecurity incident response training sessions as KPIs.

● Material Issues
● Detailed Data Related to Sustainability (Governance) > Risk Management

Key Initiatives

Specific measures to prevent information security incidents include thorough responses to vulnerabilities that may become targets of unauthorized attacks, detection of risks through the introduction of security products, constant monitoring of cyber-attacks with the assistance of external security companies, and the performance of security assessments by external organizations. In addition, we participate in external organizations that share information and strengthen our response to cyber-attacks, including the Nippon Computer Security Incident Response Team (CSIRT) Association and Initiative for Cyber Security Information Sharing Partnership of Japan (J-CSIP) and proactively obtain related information. We will continue to establish a globally coordinated incident response system with the support of external security companies.

Furthermore, we are working to strengthen prevention of information security incidents and raise awareness of information security, such as by issuing alerts within the Group as appropriate to imminent cyber risks and conducting regular information security training for all Officers and employees in Japan and overseas based on cyber risk trends.

In order to minimize damage in the event of a security incident and recover quickly, in addition to in-house internal incident response drill, we are also working to strengthen our system by participating in joint drills with external organizations.

We will promote acquisition of the national certification "Registered Information Security Specialist" as measure to improve the skill sets of our in-house information security staff. We will also promote the assignment and development of security personnel at bases outside Japan.

Internal incident response drill