Cybersecurity

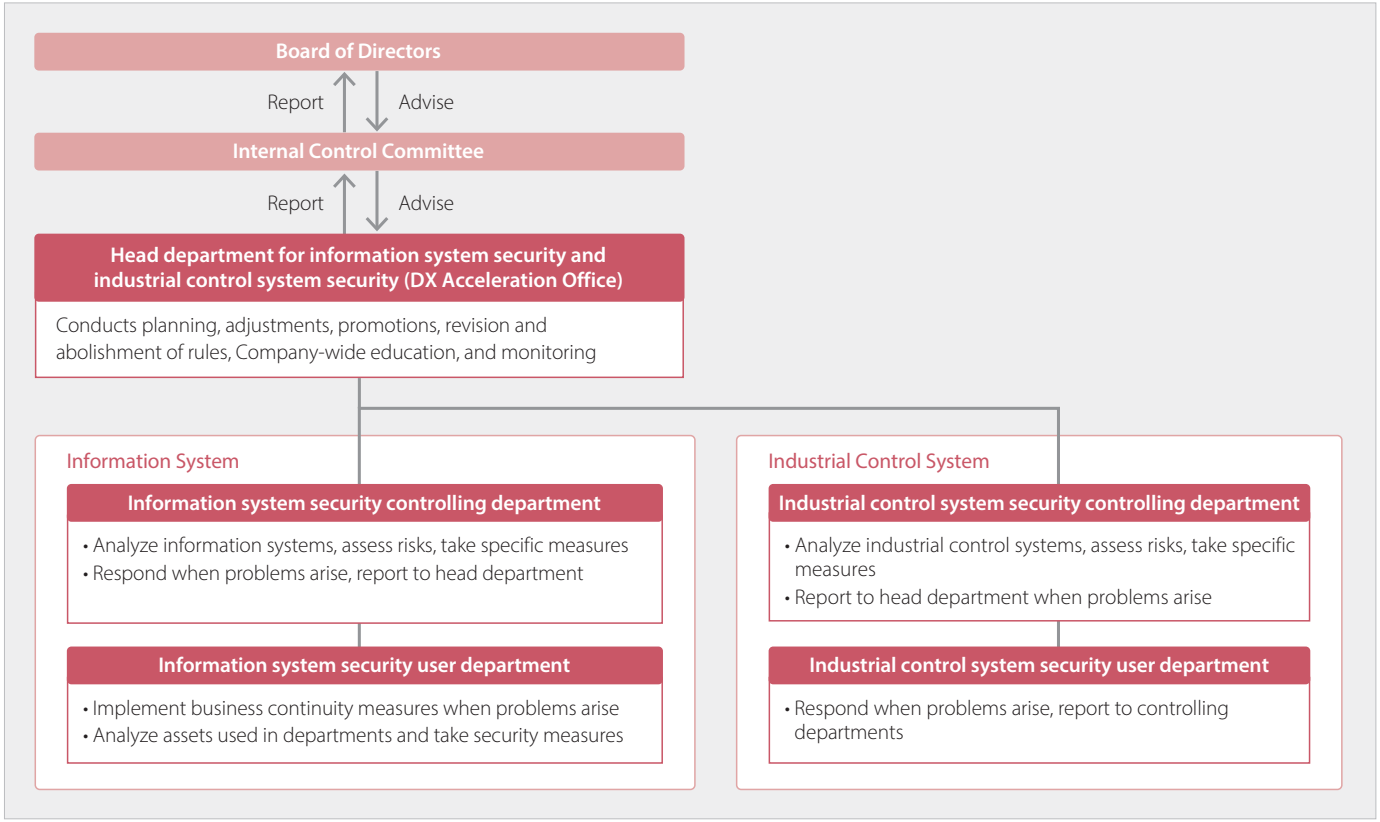
Basic Policy

Sumitomo Chemical has been accelerating Digital Transformation (DX) which seeks to strengthen business competitiveness and create new value through the utilization of IT. At the same time, however, the information system and industrial control system are facing ever greater risks due to skilled and sophisticated cyberattacks. The purpose of cyber security is mainly to prevent data leaks and loss by appropriately managing information systems, to prevent environmental impacts and ensuring health and safety by appropriately managing industrial control systems, and to minimize the impact of security incidents. We regard cyber security as a material issue for management as it works to fulfill its responsibility as a member of critical infrastructure operators, and takes multifaceted system security measures from organizational, institutional, human, technological, and physical aspects.

Management System

Sumitomo Chemical has constructed the following framework for information system security and industrial control system security, and is implementing the PDCA cycle.

■ Security Framework for Information System and Industrial Control System



Goals and Results

We have established a security policy in accordance with the concept of ISMS (Information Security Management System), an international standard for the organization's information security framework.

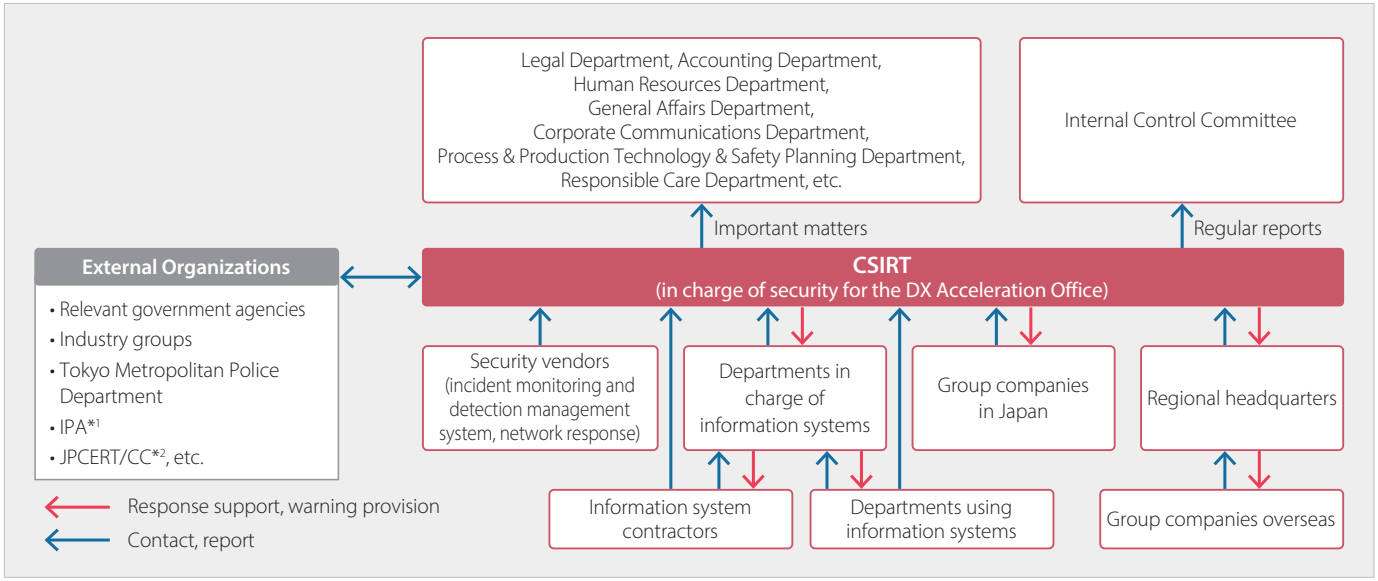
Our basic policy comprises multifaceted security measures (multilayered incident prevention and disaster mitigation), such as those outlined below.

Type of measure	Content of measure
Organizational measures	• Constructed an information system and industrial control system security framework • Constructed an information-sharing framework with inside and outside organizations to ensure preparedness against security incidents
Systematic measures	• Establish general standards and standards related to security, including for Group companies • Periodically conduct security self-inspections and conduct IT security internal audits that encompass Group companies
Personnel measures	• Conduct periodic security education using e-learning system, etc. • Conduct alerts and security incident response exercises
Technological measures	• Implement a range of measures, including access restriction, malware measures, and vulnerability measures, for individual servers and computers as well as networks
Physical measures	• Use cloud servers complete with entry/exit controls and other security features

Examples of Initiatives

We have established a CSIRT (Computer Security Incident Response Team) in the information system and industrial control system security head department (DX Acceleration Office). The team analyzes security information from external organizations, provides warnings to the Group, gathers information on security incidents that occur within the Group, and comprehensively manages the Group's response.

■ Security Incident Response Framework



*1 IPA: Information-Technology Promotion Agency, Japan

*2 JPCERT/CC: Japan Computer Emergency Response Team Coordination Center