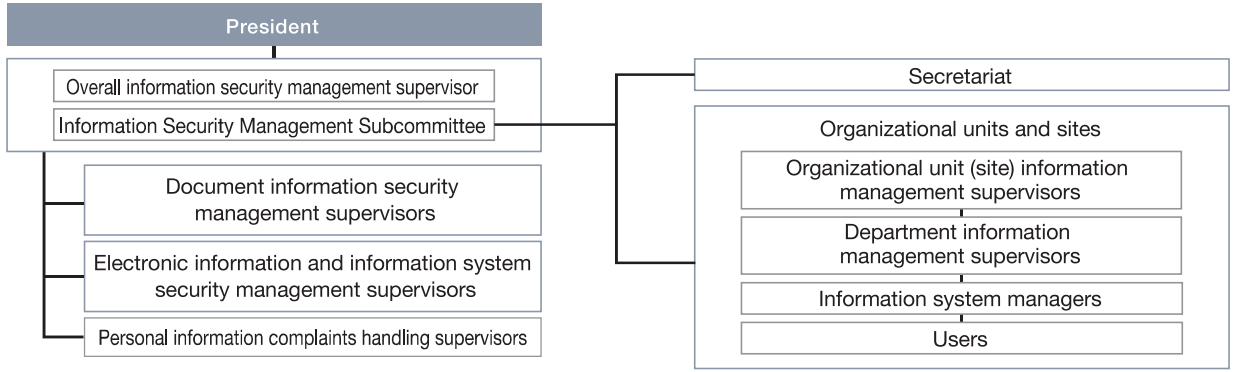
Corrective Process Against Negative Impacts | Risk Management

GRI 2-12,16,25/403-2,4

Diagram of NOF's information security management system



Risks and opportunities in information security and measures against risks

Risks and opportunities	Details	Measures
Risks	● Long-term stoppage of production, sales, and R&D activities and loss of corporate credibility due to cyberattacks (illicit access, malware infection) ● Loss of corporate trust and technological competitiveness due to leakage of confidential and personal information	● Conduct self-inspections, develop improvement plans, and implement improvement plans ● Information sharing through meetings of IT managers of domestic Group companies (once a year) ● Conduct training on handling suspicious emails (once a year) ● HDD encryption for computers taken outside the company, and restrictions on the use of private storage media ● Conduct information security-related training for employees (once a year)
Opportunities	● Improvement of company competitiveness through cybersecurity measures ● Earning of customer trust and enhancement of corporate brand value by strengthening information asset management ● Increased employee awareness through strengthened information security	-

Promotion of the Business Continuity Plan (BCP*)

NOF has formulated a BCP, to enable its core business to be continued or, if damaged, to be restored quickly while minimizing the loss of business assets in the event of a natural disaster such as an earthquake or tsunami, or an emergency situation such as the COVID-19 pandemic. The activities of the BCP Task Force to promote the BCP primarily focus on the formulation of the BCP manual which sets forth the responses to be implemented in normal times and in emergencies, in addition to the preparation and yearly renewal of information on the estimated damages to the plant and various government-, infrastructure- and supply chain-related information, which will be required when resuming operations. Additionally, the BCP Task Force performs annual internal audits and training in an effort to firmly establish the BCP and to enhance its effectiveness.

In fiscal 2023, as a response to information security risks, we conducted BCP training based on the assumption of a cyberattack, and confirmed the initial response procedures in the event of an incident and the roles of each department and site for business continuity. The training was designed to minimize damage in the event of a cyberattack and to improve response capabilities, including speediness.

* Abbreviation for Business Continuity Plan. The BCP illustrates policies, systems, and procedures designed to prevent important operations from being interrupted even in the face of unforeseen events, such as a major earthquake or other natural disaster, the spread of infectious disease, a terrorist incident, a major accident, a disrupted supply chain (supply network), or a sudden change in our business environment, and, if business is interrupted, that it is restored within the shortest possible timeframe.