In Nomura Group, natural disasters such as earthquakes and typhoons, man-made disasters such as fires and terrorism, infectious diseases such as the COVID-19, system failures, and information asset leaks are considered as crisis events that must be prepared for. In order to respond to such an event, we have a comprehensive global business continuity framework and are working on a broad range of measures, including awareness raising activities for our employees.

Nomura Group has organized the Group Crisis Management Committee to continually strengthen the capability of the business continuity in Japan as well as outside of Japan. The Group Crisis Management Committee is chaired by a senior officer appointed by the Group CEO, and comprised of senior management from Group companies. Resolution passed by the committee are reported to the Executive Management Board. In the event of a major disaster, the committee establishes a command center and takes appropriate measures to ensure the safety of employees and their families, control the spread of damage, and maintain business continuity arrangements.

**Business Continuity Management/ Cybersecurity**

In order to ensure that clients’ information and assets are securely protected from increasingly challenging cyber security threats, and to enable clients to conduct transactions with peace of mind, Nomura Group continues to strengthen its cybersecurity platform under the leadership of the Crisis Management Committee and Group IT Officer.

The leadership team will be leveraging the Comprehensive Guidelines for Supervision of Financial Instruments Business Operators, etc., of the Financial Services Agency, the Cybersecurity Framework of the National Institute of Standards and Technology (NIST) and other overseas frameworks, as references to manage the cybersecurity operations throughout the entire Nomura Group.

Nomura Group has established the Nomura Group Computer Security Incident Response Team (CSIRT) under the Crisis Management Committee’s secretariat.

In addition, Nomura Securities and Nomura Group companies have established CSIRTS to protect their operations, information assets, and systems.

**Cybercountermeasures**

The following cyber countermeasures are being promoted for each of the five functional categories defined by the NIST Cybersecurity Framework.

- **Identify**
  - Based on our management vision and risk appetite, we have established information assets to be protected, and have established a governance system.
  - We are continuously strengthening our system through threat-based penetration testing and third-party risk assessments.
  - We are conducting cyber risk assessments and countermeasures, including programs utilizing collaboration with financial institutions.

- **Protect**
  - We have deployed a system that monitors 24 hours a day, 365 days a year, for intrusions.
  - We have established a system to collect and share information on attackers and attack methods.

- **Detect**
  - We have established a monitoring system that operates 24 hours a day, 365 days a year, to detect abnormalities in a timely manner.
  - We have established a system to collect and analyze system logs and to detect abnormalities, including internal misconduct.

- **Respond**
  - In preparation for cyber incidents, we have established a system for quickly contacting clients, related institutions, and senior management.
  - We conduct post-event analysis by incident response team and other countermeasures such as risk assessments and countermeasures.

- **Recover**
  - We have established a business continuity plan and a backup data center.
  - We have prepared for rapid recovery of system operation through system switching and training exercises.