CYBER SECURITY

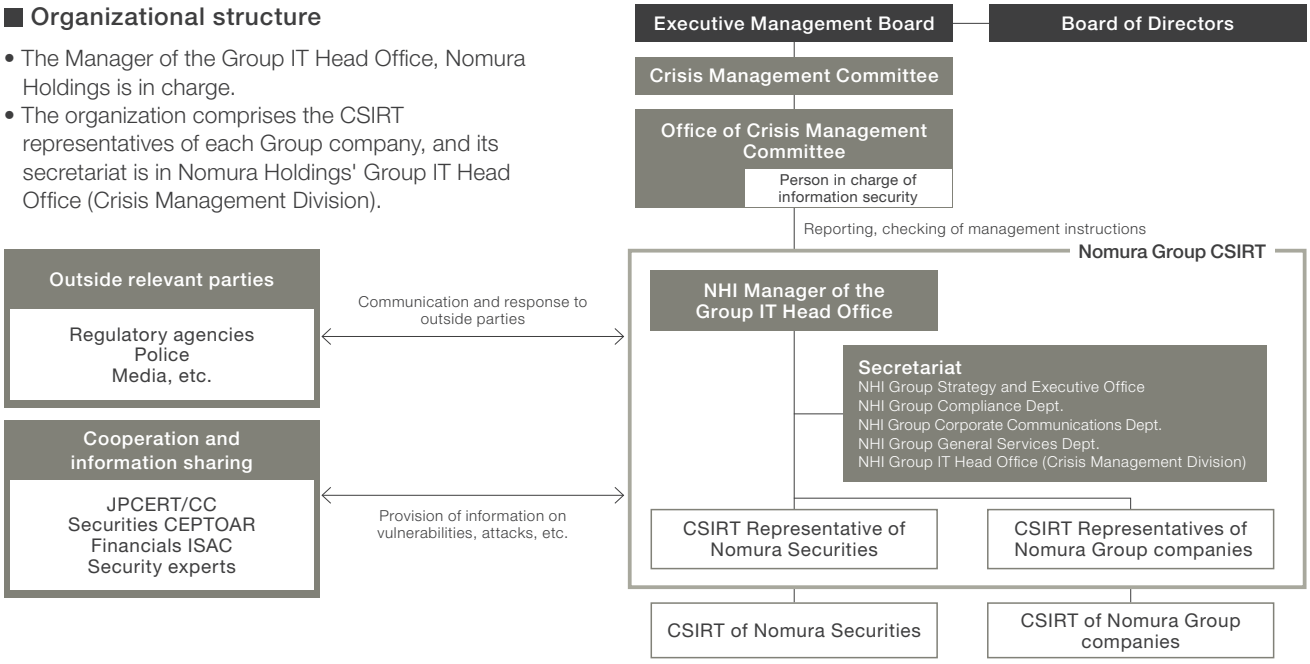
Nomura Group has for some time been undertaking security measures to protect systems against cyber-attacks. However, in light of the increasingly serious cyber security threats throughout the world, we recognize that our current countermeasures may not be sufficient in the future. In addition, in the financial sector, digitalization is proceeding at an accelerating pace. The connection of all financial systems to networks may increase the cyber security risk. In order to ensure that clients' information and assets are securely protected from these increasingly challenging cyber security threats, and to enable clients to conduct transactions with peace of mind, Nomura Group is working to strengthen its cyber security platform, using the Comprehensive Guidelines for Supervision of Financial Instruments Business Operators, etc. of the Financial Services Agency, and the Cybersecurity Management Guidelines of the Ministry of Economy, Trade and Industry based on ISO27001 and ISO27002, as references.

Cyber security system

Nomura Group, as a whole, has established a global organizational structure to deal with incidents stemming from cyber-attacks and to minimize potential damage. The Nomura Group Computer Security Incident Response Team (CSIRT), formed within Nomura Holdings, has spearheaded the formation of a CSIRT in Nomura Securities and other Group companies, and governs the CSIRT in each Group company. Each CSIRT works to protect its company's operational and information assets, as well as systems, promoting cyber security measures from four vantagepoints: organizational management, system security measures, human-level response, and coordination with outside organizations.

Organizational structure

- The Manager of the Group IT Head Office, Nomura Holdings is in charge.
- The organization comprises the CSIRT representatives of each Group company, and its secretariat is in Nomura Holdings' Group IT Head Office (Crisis Management Division).



Organization management	At normal times, we take part in cyber security drills, conduct Threat-Led Penetration Test, assess cyber risks and monitor actions taken by overseas subsidiaries and outside contractors in a constant effort to heighten our readiness. In the case of an incident such as obtaining dangerous vulnerability information or detecting a cyber-attack, the CSIRT leads the efforts to analyze the cause, minimize damage, and quickly restore systems.
System security measures	We adopt a multi-layered defense system, which includes multiple detection and defense mechanisms against unauthorized access and malicious programs such as computer viruses. We review these countermeasures as appropriate to deal with new threats.
Human-level response	In accordance with the Nomura Group Information Security Policy, relevant seminars and training programs are regularly provided to all executives and employees and they are kept alert in order to raise their awareness and knowledge about cyber security.
Cooperation with outside organizations	Nomura is cooperating with information sharing organizations such as Financial ISAC Japan and FS-ISAC and cyber security vendors to gather and share information on the cyber attackers and their approaches.