Cybersecurity

Message From the Deputy Group CDO

The Group is accelerating the development of a diverse range of services utilizing digital technologies. At the same time, we recognize increasingly sophisticated cyber-attacks as a top risk and regard safeguarding our customers' important assets and social infrastructure as one of our most important management challenges. We view cybersecurity as an investment in "offensive governance" to promote safe and secure digitalization. In addition to maintaining a 24/7 monitoring structure through our security operations center (SOC) and conducting thorough external audits, we are preparing to stay ahead of emerging threats associated with frontier AI and other technologies through strong external collaboration with Chance-CSIRT, which is operated by banks sharing the core banking system, Financials ISAC Japan, and other organizations. The greatest key to enhancing the effectiveness of these measures is the resilience of our people and organization. We will continue to conduct practical training and develop highly specialized personnel, while further embedding a security-first culture across the Group.

Katsutoshi Hirano, Executive Officer, Deputy Group CDO

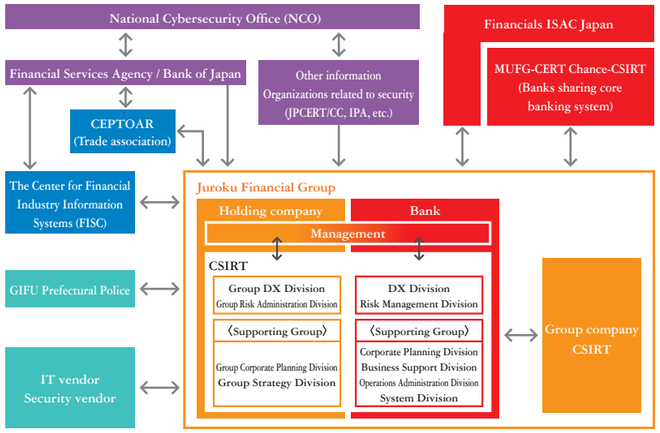
Governance system

In response to the increasing threat of sophisticated and advanced cyber-attacks, we have positioned cyber-attacks as one of the Group's top risks, and established the Information Security Management Rules and Information System Management Rules to prevent any cybersecurity incidents and prevent any damage from spreading. In doing so, we are working to strengthen cybersecurity management system.

Through timely and appropriate reports to the Board of Directors and Management Council, we are creating a governance structure that facilitates rational management decisions in response to environmental change. Moreover, through proactive contributions from management, we are promoting effective and efficient cybersecurity strategies and ensuring daily protection against cyber-attacks.

Cybersecurity management system

We have established a Computer Security Incident Response Team (CSIRT), with the Group DX Division and Group Risk Administration Division functioning as the secretariat as a cybersecurity incident response team, and are collaborating with Group companies. Mainly through the CSIRT, we respond to emergency incidents, offer education and awareness programs in times of normality, and collect and analyze information on potential threats.



Sharing of threat information and cooperative initiatives

Chance-CSIRT, the response team of regional banks jointly using the Chance core banking system, entered into an alliance in November 2017 with 'MUFG-CERT,' the security incident response team of Mitsubishi UFJ Financial Group, Inc., and has since been engaging in cooperative cybersecurity-related initiatives, such as the exchange of personnel, dispatch of trainees, and sharing of threat information. In addition, by sharing information through Financials ISAC Japan, which shares and analyzes cybersecurity-related information from Japan's financial institutions and promotes collaborative activities to improve cyber safety, we are working to improve security across the entire financial industry.

Incident response framework

The Group conducts cyber incident response training twice a year. Approximately 90 participants, including responsible officers, Group company employees, and external security vendors, take part in the exercises to verify the Group's response framework in preparation for emergencies. To make the exercises more practical, we use a blind format in which scenarios are not disclosed in advance. We are also diversifying exercise scenarios so that we can respond to a wide range of cyber-attack methods, including ransomware infections at Group companies.

When an incident occurs, we work with relevant departments to investigate the cause, implement corrective actions, and take measures to prevent recurrence, striving to respond appropriately.

Education and awareness programs for Group officers and employees

To improve digital literacy with cyber-attacks, we continue to offer education and awareness programs for all Group employees (including part-timers). This includes suspicious email training (more than twice a year), e-learning (more than twice a year), self-assessments of security action (around four times a year), and awareness-raising activities (as necessary).

We are also working to develop human resources with specialist expertise in the field by offering self-development qualification acquisition subsidy for those who passed Information Technology Engineers Examination and utilizing the internal expert system.

Initiatives for cybersecurity

Threat information analysis, security surveillance	To ensure that customers can use the Group's services in a safe and secure manner, we are reinforcing our cybersecurity measures through thorough vulnerability countermeasures, multilayer defense systems, analyses of threat trends, and detection and monitoring of abnormal activity. Moreover, we also have various surveillance systems in place, including a security operation center that is managed 24 hours a day, 365 days a year by a specialist external vendor.
Cybersecurity sophistication measures and external audits	Based on the concept of zero-trust security, the Group is implementing a range of measures to establish a multilayered defense framework. In addition, we conduct external audits (third-party assessments) as part of our governance system and penetration tests (simulated intrusion tests) by security vendors. By objectively identifying risks and promptly addressing issues revealed through these processes, we are further enhancing our defense framework. In October 2024, the Financial Services Agency announced the Guidelines for Cybersecurity in the Financial Sector, and we have since been engaged in efforts to comply with these guidelines.
Risk assessments and outsourcing management	When introducing new systems, we conduct advance reviews of whether said systems comply with the Group's standards using checklists according to levels of importance that are based on the safety standards from the Center for Financial Industry Information Systems (FISC). For cloud services used by the Group, we conduct assessments of compliance with Group's standards both at the time of introduction and annually thereafter. Moreover, to lessen the burden on contractors, on occasion we use services offering risk assessments from external experts.
Vulnerability assessment	To regularly check for unintended omissions or improper configurations in our public systems, we have introduced tools and services for automatic and highly frequent vulnerability assessments. Most frequently tested systems are assessed for vulnerability on a weekly basis. We also make sure to link any vulnerabilities or other findings to thorough improvements.

System risk management

As damage to information systems could have an impact on a broad range of operations, we have implemented various damage prevention measures to maintain their stable operation. These include double-layer system infrastructure and the installation of disaster countermeasure systems that use data centers in multiple locations. In addition, through the creation of contingency plans and training that simulates said damage, we are ensuring thorough preparations for unforeseen circumstances.

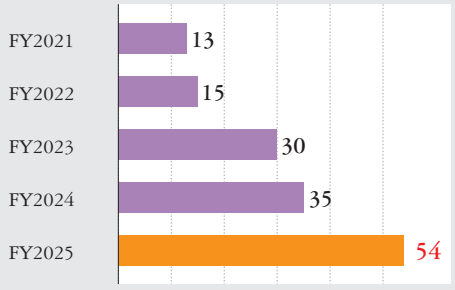
Dialogue With Investors

We strive to ensure information disclosure to further understanding of the Group's strategies, operations, and financial conditions among shareholders and investors so that they can make appropriate judgements on the soundness of Group management. In FY2025, we provided the following opportunities for dialogue with our shareholders and investors.

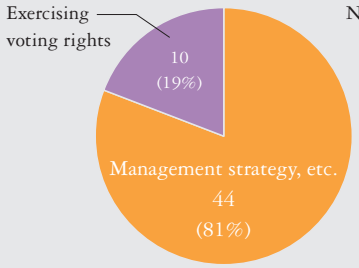
Nature of activity	Results	Explainer	Content
Financial results briefing for institutional investors (briefings on interim and full-year results for FY2025)	2 times	Group CEO Group CFO	Held both in-person and online 【November 2025: 43 participants in person, 28 online】 【May 2026: 42 participants in person, 63 online】
Small meeting	Once	Group CEO Group CFO	Held online 【11 Institutional investors】
One-on-one meeting	9 times		Held in-person 【Japanese investor: 9, overseas investor: 0】
	45 times	Group CFO and others	Held both in-person and online 【Japanese investor: 29, overseas investor: 16】

Breakdown of individual meetings in FY2025

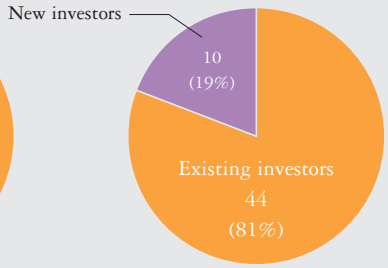
①Comparison with past no. of meetings



②Breakdown by theme



③Breakdown by investor type



Requirements and other opinions gained through these meetings are reported to the Board of Directors and management as necessary. In FY2025, we implemented the following measures in response to feedback.

Shareholder/investor requests	Our response
Enhance shareholder returns	● Increased dividend for the seventh consecutive term, and implemented share buybacks for the fifth consecutive term (total payout ratio: 42.1%, dividend payout ratio: 31.3%) ● Implemented a 5-for-1 share split on April 1, 2026 ● Expanded the shareholder benefits program
Reduce cross-shareholdings	● The ratio to consolidated net assets stood at 15.7% as of March 31, 2026, making steady progress
Strengthen governance	● Introduced the Chief Officer System to accelerate decision-making and enhance expertise
Improve productivity	● Introduced a numerical-data "dashboard" and rolled out the use of a generative AI "engagement tool"
Engage in climate change	● Selected for the Climate Change A List, the highest rating in the CDP Climate Change 2025 assessment
Investment in human capital	● Extension of the mandatory retirement age to 65 ● Introduced the regional banking industry's first Flexible Retirement Age System up to Age 65, allowing employees to choose their retirement age in one-year increments from 60 to 65 ● Launched the Knowledge Point Stage Certification Program to evaluate employees' day-to-day learning ● Promoted health management initiatives, including fully covering the cost of comprehensive health screenings
Enhance information disclosure	● In February 2026, our Integrated Report 2025 received the Excellence Award at the 5th NIKKEI Integrated Report Award organized by Nikkei Inc.