Financial Industry-wide Cybersecurity Exercise (Delta Wall IV)

Situation Surrounding Cybersecurity in the Financial Industry

- There have been incidents of large-scale cyberattacks in many countries, and their modus operandi are becoming increasingly more sophisticated and complicated.
- In Japan, cyberattacks no longer affect only large financial institutions. Cyberattacks have also amplified to small and medium financial institutions and crypto-asset exchange service providers. Implementing effective cybersecurity measures is therefore an urgent task.
- Cyberattacks have become a major threat to the stability of the financial system, making it imperative to improve the overall ability of financial institutions to respond to incidents.

Overview of previous exercises

- Three exercises (Delta Wall I ,II and III) were conducted in 2016 -2018.
- In Delta Wall I, about 900 individuals at 77 financial institutions participated from banking, securities and life/nonlife insurance sectors and so on.
- In Delta Wall II, about 1,400 individuals at 101 financial institutions participated.
- In Delta Wall III, about 1,400 individuals at 105 financial institutions participated. (crypto-asset exchange service providers etc. were newly included.)

Financial Industry-wide Cybersecurity Exercise (Delta Wall IV)

◆With a view to the 2020 Tokyo Olympic and Paralympic Games, we have prepared for major incidents. In October 2019, the **Financial Services Agency organized the fourth financial industry-wide cybersecurity exercise called "Delta Wall IV*"** for the entire financial industry , in which large, small and medium-*sized entities* participated.

* Delta Wall means a key element in cyber security: the triad (Delta) of "self-help," "mutual assistance," and "public assistance."

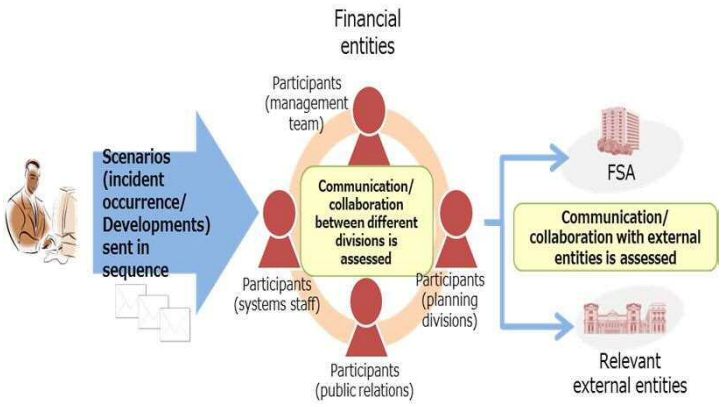
◆ **Approximately 120 entities participated, including funds transfer service providers, issuers of prepaid payment instruments and audit firms**, and so on, which were **newly included business types**.

◆ **The exercise scenario that reflects risks that could materialize at the 2020 Tokyo Olympic and Paralympics Game**. We set out two scenarios are for depository corporations as well as securities companies, and other sectors.

Features of This Exercise

- ☐ This is a **tabletop exercise** that aims for verifying the procedure and response system of the entities in terms of internal and external information sharing in case of incidents.
- ☐ The exercise **was conducted at each participant's workplace** to facilitate the participation of managers and members from as many relevant divisions as possible, including IT, public relations and general planning.
- ☐ The scenarios were designed with **expert knowledge and examples of actual cyber attacks** to **allow participants to raise their awareness for weaknesses that they tend to fall into.**
- ☐ The exercise **focused on assessing the participants' actions and decision making during the exercise including** concrete improvement measures. It enables participants to improve their ability to respond to incidents following their management cycle.
- ☐ **The feedback (or lessons-learned) will be shared with the entire industry,** not just the participants.

Exercise Scheme



【Scenario Example】

For banks, securities companies, and so on.

- ✓ Network failure and DDoS attacks on website occurred during the Tokyo 2020 games.
- ✓ Due to a failure of network that cooperated with other financial institutions, settlement system outage.
- ✓ The cause of the network failure and the types of the DDoS attacks are identified.

For other sectors (insurance companies, crypto-asset exchange service providers, audit firms, and so on.)

- ✓ Giving a cyberattacks alert related to Tokyo 2020 Games.
- ✓ DDoS attack on website and targeted attack are occurred.
- ✓ The DDoS attack type and the cause of incident are identified.