Financial Industry-wide Cybersecurity Exercise (Delta Wall III)

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, too, there have been incidents of massive leakage of personal information due to cyberattacks and those targeting multiple small-to-medium financial institutions.
- 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

- Two exercises (Delta Wall I and II) were conducted last year and the year before last.
- In Delta Wall I, about 900 individuals at 77 financial institutions participated from the banking, shinkin banking, credit union, securities and life/nonlife insurance sectors.
- In Delta Wall II, about 1,400 individuals at 101 financial institutions participated from labor banks and money lending businesses, in addition to the sectors that participated in Delta Wall I.

Financial Industry-wide Cybersecurity Exercise (Delta Wall III)

◆ In late October, the **Financial Services Agency organized the third financial industry-wide cybersecurity exercise (Delta Wall III*)** with the purpose to improve the overall ability of the financial industry, particularly small-to-medium financial institutions, to respond to security incidents.

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

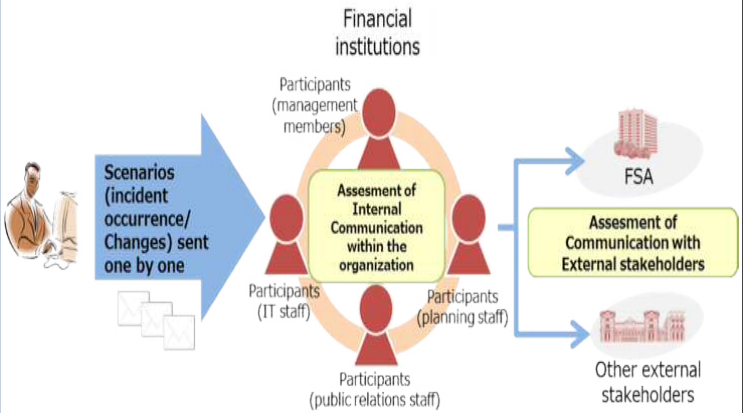
◆ **About 100 entities participated, including FX trading companies and virtual currency exchanges**, which were **newly included business types**.

◆ In addition to the common scenario, **sector-specific scenarios were newly introduced. A blind-scenario style** (the main points of the scenario are not disclosed to participants), which is more practical than an open-scenario style, **was applied to the banking sector** given its maturity.

Features of This Exercise

- 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 feed-back (or lessons-learned) will be shared with the entire industry**, not just the participants.

Exercise Scheme



【Scenario Example】

Website falsification (shinkin bank, credit union)

- ✓ Customers inquire as to why they receive a notification using the online service even though they should NOT.
- ✓ Due to website falsification, users get transferred to a phishing site when they browse, and are forced to input their ID / PW.
- ✓ The cause seems to be the vulnerability of the website.

DDoS attack on online services (securities, FX)

- ✓ A DDoS attack occurs, and customer inquire as to why they cannot access the service
- ✓ In parallel with the DDoS attack, a targeted mail attack freezes an employee’s PC and a blackmail message demanding a ransom is displayed.
- ✓ The DDoS attack blows over and the attack type is identified.