The Policy Approaches to Strengthen Cyber Security in the Financial Sector (Summary)

July 2, 2015

Financial Services Agency

Challenge for Cyber Security in Financial Sector (1)

Necessity to Strengthen Cyber Security in Financial Sector

- The Financial Services Agency (FSA) has been conducting the supervision and inspection regarding cyber security management as a part of system risk control, etc.
- Now, the threat of cyber attacks is a significant risk for the stability of the financial system. It is necessary to enhance the resilience of the financial system by strengthening the cyber security of not only each financial institution but the financial industry as a whole.
- In the Cyber Security Basic Act enacted in November 2014, it is provided that the government takes measures in order to ensure the cyber security of critical infrastructure including the financial sector.

⇒ Clarify the policy approach to address the threat of cyber attacks in the financial sector

Situation Surrounding Cyber Security in Financial Sector

- Increased Internet use in the financial sector due to technical innovation
- Sophistication of cyber attacks (elaborate attack, and access facilitation to the attack technology)
- Threat of cyber-terrorism (need of preparation for the 2020 Tokyo Olympic and Paralympic Games)

Challenge for Cyber Security in Financial Sector (2)

Scope of Cyber Security in Financial Sector

Purpose of attacker	Target	Threat		Existent risk management system
Social Order Disruption	Financial Institution	**Functional failure of financial institution, financial market, or financial infrastructure**	Attacks directly from cyber space	Business Continuity Management, etc.
			Internal attacks to cause a malware infection of the system (Insider Threat)	
Financial Gain		**Leak of confidential information**	Attacks directly from cyber space	Information Security Management, etc.
			Internal attacks to cause a malware infection of the system (Insider Threat)	
		Illegal transactions such as fraudulent remittance	Malware infection of financial institutions' computers to cause illegal transactions such as fraudulent remittance	Customer Protection, etc.
	Customer		Malware infection of customers' computers to cause orders of money transfer to the financial institution against the customer's will, or phishing fraud, etc.	

Five Policies to Strengthen Cyber Security in Financial Sector

Basic Concept

- To enhance the cyber security initiatives in the financial sector, it is important to address this task by both public and private sectors together.
- Thus, the FSA will develop constructive dialogue on a regular basis based on the understanding that the FSA and financial institutions have a common purpose of ensuring cyber security, and the FSA will also address the five policies below in order to contribute to strengthening cyber security in the financial sector from the financial regulator's perspective.

Five Policies

1. Constructive dialogue with financial institutions and grasp of their current condition regarding cyber security

2. Improvement of the information sharing framework among financial institutions

3. Continuous implementation of industry-wide cyber security exercises

4. Cybersecurity human resource development in financial sector

5. Arrangement of cyber security initiatives in the FSA

1. Constructive Dialogue with Financial Institutions and Grasp of their Current Condition regarding Cyber Security

- ○ The FSA will continue constructive dialogues to enhance the effectiveness of cyber security management systems of financial institutions.
- ○ As a part of this process, the FSA will grasp the current condition regarding the cyber security of the whole financial sector this year through a questionnaire, and analyze issues associated with each type of financial institution.
- ○ The FSA will give the financial institutions feedback through dialogue with them and encourage the financial institutions to conduct self-checks, etc.

(Reference) Overview of the questionnaire items (draft)

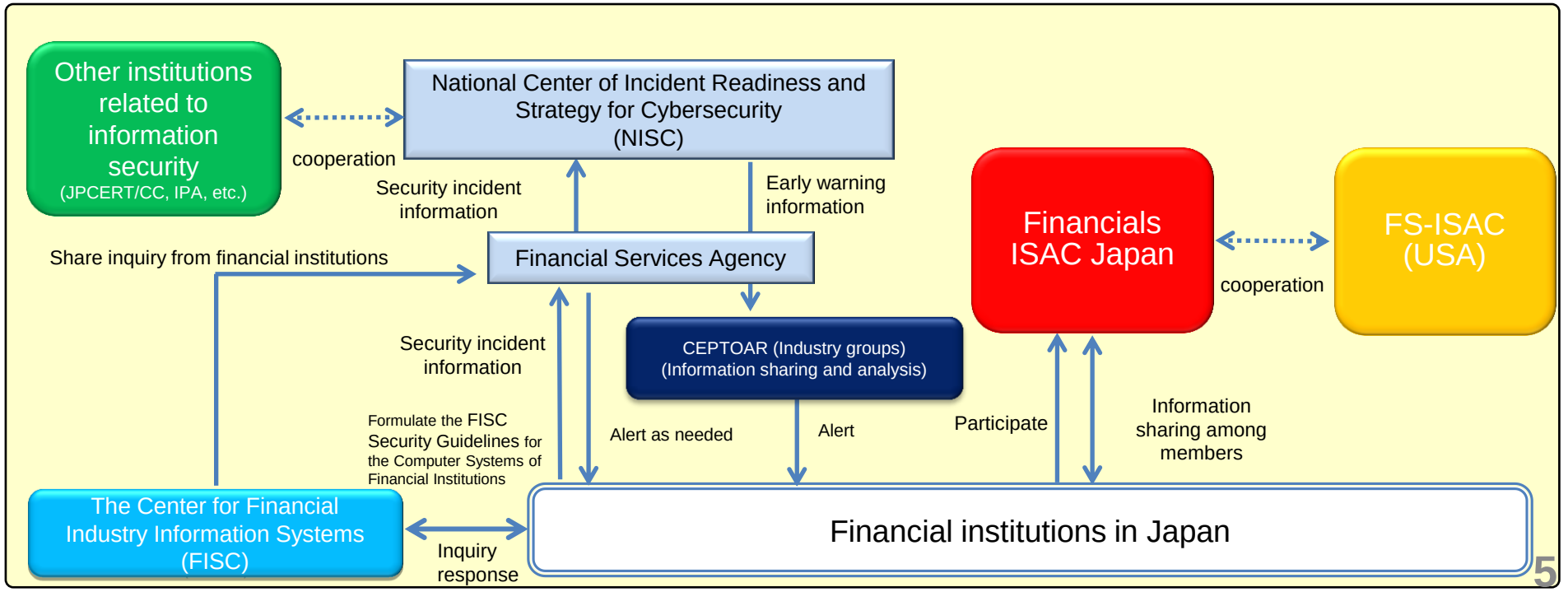
- Functional failure of financial institution or financial infrastructure
- Leak of confidential information
- Illegal transaction such as fraudulent remittance (attacks on financial institutions)

- Illegal transaction such as fraudulent remittance (attacks on customer)

	Specific response
Identify	- Grasp of the target (information asset, etc.) to protect against cyber attacks - Executive's recognition of the importance of cyber security - Periodical assessments of security levels - System development with the viewpoint of security management
Protect	- Preparation of emergency response and early warning system in the organization - Preparation for information collection and sharing through the information sharing institutions, etc. - Defense in depth (measures at entry point, internal, and exit phases) - Timely response to system vulnerabilities - Formulation of contingency plan, and participation in industry-wide cyber security exercises
Detect	- Monitoring for cyber attacks through the analysis of communication log data, etc.
Respond and Recover	- Appropriate response in accordance with contingency plans
Resilient service provision	- Combination of preventive measures including safer authentication methods
Alert to customer	- Enhancement of security levels of the customer's environment - Detection of anomaly transactions and notifications to the customer

2. Improvement of Information Sharing Framework among Financial Institutions

- The FSA will continuously raise awareness to financial institutions regarding the importance of collecting/providing information and strengthening measures (immediate grasp of vulnerabilities, introduction of security control technology, etc.) through utilizing the information sharing institution (Financials ISAC Japan, etc.).
- The FSA will voluntarily provide information through industry groups (CEPTOAR) as necessary in addition to the information provided by the National Center of Incident Readiness and Strategy for Cybersecurity (NISC) under Cabinet Secretariat.
- The Center for Financial Industry Information Systems (FISC) will drastically raise the level of FISC Security Guidelines, and will publish the answers to inquiries from financial institutions regarding the interpretation of FISC Security Guidelines as “Cyber Security reference information”.



3. Continuous Implementation of Industry-wide Cyber Security Exercises

- To enhance the ability to deal with cyber attacks, it is effective to, through cyber security exercises, cultivate practical abilities, check the system, and conduct the PDCA cycle.
- The FSA will promptly consider concrete methods (responsible organization (including cooperation with other authorities/related institutions), purpose of exercise and scenario, etc.) in order to implement the industry-wide cyber security exercise involving related authorities, while using the exercises in foreign countries as a reference.

4. Cybersecurity human resource development in financial sector

- To strengthen cyber security, financial institutions' staff such as not only IT engineers but also members of the board of directors and executives need to have a certain level of awareness and knowledge about cyber security. Also, it is necessary to improve the quality of human resources in the supervisory authority. After July 2015, the FSA will promote the following measures.
  - ✓ Organize seminars to improve the awareness of Financial institution's
  - ✓ Considering plans to develop human resources and to strengthen cyber security in the financial sector in cooperation with industry associations and information sharing institutions
  - ✓ Improving the expertise of the FSA's human resources (adoption of outside experts and education of internal personnel)

5. Arrangement of Cyber Security Initiatives in FSA

○ To strengthen the cyber security of the whole financial system, the FSA immediately establishes a division which collects and unifies relevant information in the FSA, accumulates knowledge through utilizing outside experts, and coordinates the policy across the FSA.