Financial Sector Cybersecurity Report

June 2020

Financial Services Agency

金融庁
Financial Services Agency

[Contents]

Introduction

Recognizing that cybersecurity in the financial sector is of utmost importance for the stability of the financial system, the Financial Services Agency (hereinafter, "FSA") formulated and published "The Policy Approaches to Strengthen Cybersecurity in the Financial Sector" (hereinafter, "Policy Approaches") in July 2015.

In consideration of digitalization in the financial sector and in international discussions about Cybersecurity, preparations for the 2020 Tokyo Olympic and Paralympic Games (hereinafter, "2020 Tokyo Olympics and Paralympics") and other situational changes, the FSA updated the Policy Approaches in October 2018 and has endeavored to strengthen cybersecurity in the financial sector through public-private partnership .

In PY2019, the FSA endeavored to improve the effectiveness of FIs' cybersecurity countermeasures through the enhancement of cybersecurity management systems as usual and responses to incidents in anticipation of the 2020 Tokyo Olympics and Paralympics. As the financial sector environment changed, with telework expanding in response to progress in digitalization and the novel coronavirus disease 2019 (hereinafter, COVID-19), the FSA also endeavored to identify and analyze emerging cyber risks through the collection of information on threats and proactively encouraged FIs to respond to those risks.

As FIs innovate business operations in line with IT advancement, it is important to ensure the security of services (protection of service users) through adequate cybersecurity countermeasures to improve user convenience.

Given that cyberattacks continue to grow more complicated and sophisticated, the FSA, FIs and relevant organizations in public and private sectors must be cooperated to improve cyberattack countermeasure in the financial sector.

This Report publishes facts and common challenges identified in the course of conducting initiatives during PY2019.

The updated Policy Approaches state that the FSA will promote stronger cybersecurity countermeasures by actively disseminating information on common challenges in the financial sector. The publication of this Report is designed to establish a shared awareness among the FSA, FIs and relevant organizations, which will lead to more robust cybersecurity in the financial sector.

1. Current situation with cybersecurity in the financial sector

(1) Threats in recent years

In recent years, business corporations, private sector organizations and public offices in Japan have frequently been subjected to cyber incidents, including targeted attacks for information theft, as well as ransomware[1] and DDoS[2] attacks.

Although FIs in Japan have not experienced any large-scale cyber incident, Victims are invited to fake websites of FI and others to heist cash or credit card information.

Among overseas FIs, a major U.S. financial holding company underwent a cyberattack in March 2019, where personal data for some 100 million people were leaked. In December 2019, a major U.K. foreign exchange company faced a cyberattack that prevented FIs cyberattack that impeded FIs from processing customer orders via its foreign exchange services. In October 2019, Cyber incidents that adversary demands cash foretelling the DDoS attack occurred in Japan and other countries.

Given that cyber incidents have occurred everywhere in Japan and other countries, further efforts are required to ensure security.

(2) Cyber incidents at FIs in Japan

Reported cyberattacks on FIs in Japan primarily include list-based attacks,[3] unauthorized logins attributable to setting mistakes and DDoS attacks.

Cyber incidents have occurred during test operations of computer systems as well as their commercial operations and include attacks in Japan via overseas branches.

Given that unauthorized logins through list-based attacks and DDoS attacks accompanied by threats at some FIs are particularly feared to occur at other FIs, the FSA issued warnings to FIs in October 2019, asking them to reaffirm appropriate authentication methods and arrangements against actual DDoS attacks.

Among FIs, depositary financial institutions, financial instruments business operators and money-lending institutions have seen personal information theft through unauthorized logins and service disruption through DDoS attacks. At crypto-asset exchange service providers, private keys for hot wallets were stolen, leading massive crypto-assets heisted.

Given the situation, the FSA must timely identify and analyze emerging threats and vulnerabilities and encourage FIs to enhance cybersecurity management systems in the financial sector.

(3) Impacts of COVID-19 on cybersecurity

While COVID-19 exerts serious impacts on Japan and other countries around the world, cyber attacks, taking advantage of the pandemic and targeting telework environments introduced in response to the pandemic, are increased.

---

[1] Ransomware is a kind of computer virus that limits access to a virus-infected computer or encodes system files through the computer, demanding a ransom for lifting the limit or encoding.

[2] DDoS stands for Distributed Denial of Service.

[3] In a list-based attack, a malicious attacker gets an account information list in some way and uses the list for logging in to an attack target's account.

【Figure 1: Cyber attacks, taking advantage of COVID-19】

No.	Cyberattack category	Case
1	Targeted attacks using email, social networking services (hereinafter, SNS), etc.	Cyber attackers offer cash handouts assumed public organizations like the World Health Organization (hereinafter, WHO) and the National Institute of Infectious Diseases and use mail or SNS to infect computers with Emotet and other malware or direct computer users to phishing sites.
2	Phishing sites	Attackers use fake sites for mask sales and government agencies to steal credit card and other personal information.
3	Malware	Applications posed as useful for COVID-19 countermeasures are used for stealing credit card and other personal information.
4	Ransomware, DDoS	Attacks seek to lead healthcare facilities, government agencies, research institutes, etc. to Disruption.
5	Attacks on telework environments	Attackers take advantage of teleworking and remote access environments for stealing information.

Source: FSA

As shown by the above figure, Although cyberattacks taking advantage of COVID-19 mostly use conventional methods, attackers change targets and their email contents in response to hour-to-hour changes. FIs are thus required to timely identify and appropriately respond to cyber threats.

So far, FIs in Japan have implemented telework, shift-work systems, staggered office hours and split operations[4] to continue business operations while securing safety to prevent COVID-19 infection, seeing no grave problems.[5]

As new lifestyles spread in response to the COVID-19 pandemic, new workstyles using telework and the digitalization of financial services are expected to make further progress in the financial sector, requiring the sector to pay attention to security measures based on such environmental changes.

2. Current initiatives to strengthen cybersecurity in the financial sector

(1) Strengthening of cybersecurity management systems of FIs

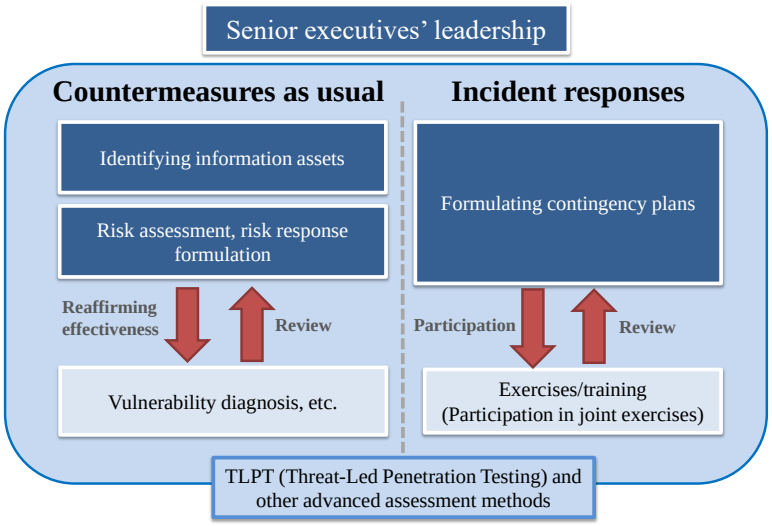
The FSA has so far strengthened FIs' cybersecurity countermeasures from two aspects of cybersecurity: countermeasures as usual and incident responses. In PY2019, the FSA encouraged FIs to improve the effectiveness of cybersecurity countermeasures regarding each aspect through dialogues and exercises with them.

The FSA also endeavored to understand and upgrade FIs' cybersecurity systems in anticipation of the 2020 Tokyo Olympics and Paralympics.

[4] A split operation means that a business operation is divided between two or more teams to avoid simultaneous infections.

[5] In an incident that differed from any cyber incident, computer system troubles occurred at some FIs in March 2020 due to more-than-expected stock trading volume caused by wild stock price fluctuations triggered by the COVID-19 pandemic. See "Analysis Report on Financial Institutions' Computer System Failures" (published in June 2020).

【Figure 2 Concept of countermeasures as usual and incident responses】



Source: FSA

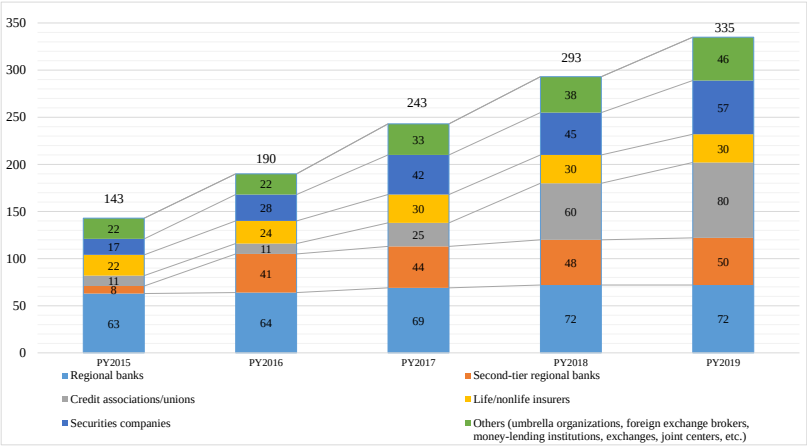
① Cybersecurity countermeasures as usual

(a) Small and medium financial institutions

As for small and medium FIs, the FSA has so far verified the status of basic cybersecurity management system development through cybersecurity assessments [6] (monitoring through dialogues). Since PY2018, the FSA has added the monitoring and analysis of security incidents and the status of vulnerability scan as new viewpoints for cybersecurity assessments.

In PY2019, the FSA sought to upgrade cybersecurity in the financial sector by conducting cybersecurity assessments mainly for FIs that are feared to delay the development of basic cybersecurity management systems.

【Figure 3: Trend of cybersecurity assessments by FI type (total numbers of FIs subjected to cybersecurity assessments (including second-round assessments) 】



Source: FSA

[6] ① Management initiatives, ② risk management frameworks, ③ arrangements for technical and other countermeasures, ④ development of contingency plans and implementation of exercises to secure their effectiveness, ⑤ cybersecurity audit

○ Regional banks, credit associations/unions

The FSA conducted cybersecurity assessments for regional banks and credit associations/unions selected based on risks, such as those feared to delay the development of basic cybersecurity management systems, reaffirming their efforts to develop the basic systems and verifying the effectiveness of their cybersecurity countermeasures.

Cybersecurity assessments found that while senior executives at some of them were proactively engaging in management and monitoring based on plans to enhance cybersecurity, others had challenges[7] in developing basic cybersecurity management systems.

The FSA directly asked those plagued with challenges at dialogues to accelerate developing basic cybersecurity management systems. It has also cooperated with local finance bureaus to follow up and promote their development of systems for resolving challenges under the leadership of their senior executives.

○ Securities companies, etc.

The FSA performed cybersecurity assessments at regional securities companies, FX brokers and PTS[8] operators that had not undergone such assessments and had been found through risk profiling as likely to delay for developing basic cybersecurity management systems. As a result, the FSA found that while a rising number of such companies were making progress in such efforts, some companies failed to make progress.

At some of those subjected to the cybersecurity assessments, senior executives were highly cognizant of risks and proactively involved in the formulation of action plans for developing basic cybersecurity management systems and are moving independently to beef up cybersecurity. As is the case with credit associations/unions, however, the others were still in the process of developing basic cybersecurity management systems. Some of them were complacent with the isolation of the core inhouse system network from the Internet network, failing to develop policy for data exchanges between those networks. Some others outsourced the management of their websites while failing to check responses to vulnerability. The FSA directly asked these companies to accelerate to develop basic cybersecurity management systems. It has also cooperated with local finance bureaus to follow up on such and promote their development of systems for resolving challenges under the leadership of their senior executives.

○ Payment service providers (prepaid payment instrument issuers and fund transfer service providers), etc.

In response to illegal uses of payment services seen in PY2019, the FSA assessed cybersecurity countermeasures at major smartphone payment service providers. As a result, it

[7] The following are the challenges found through the assessments:
・Senior executives fail to engage in monitoring progress in plans to develop basic cybersecurity management systems.
・Senior executives fail to be aware of risks as risk assessments are too nominal to identify residue risks.
・Contingency plans fail to meet organizational conditions as no process is developed to verify the effectiveness of such plans.

[8] PTS stands for Proprietary Trading System.

found that some of them had problems regarding user identification methods and monitoring of illegal transactions.

The FSA encouraged those payment service providers through dialogues to improve cybersecurity countermeasures. It also recommended payment service providers[9] in general to develop cybersecurity management systems.

(b) Large financial institutions

Regarding large FIs, the FSA has so far engaged in regular dialogues mainly[10] with the three mega-banks that form the core of Japan's financial system, while keeping in mind large U.S. banks' sophisticated operations and global trends.

At dialogues with the three mega-banks and other large FIs in PY2019, the FSA examined mainly the advancement of group-wide and global cybersecurity management systems and the use of TLPT,[11] while keeping in mind the complication and sophistication of cyberattacks and global trends.[12] Among trust and Internet banks, the FSA used questionnaire surveys for off-site monitoring of those that apparently have relatively high risks.

○ Three mega-banks, etc.

The three mega-banks and other large FIs are trying to sophisticate unified group-wide and global cybersecurity management systems by conducting risk assessments for core systems at group companies (including overseas ones) and detailed cybersecurity maturity assessments at major group companies.

They are expected to beef up access control and cyber resilience in consideration of cyberattack risks for group companies and outsourcee to enhance unified group-wide and global cybersecurity management systems.

They use the TLPT to improve the effectiveness of cybersecurity. In particular, the three mega-banks are expanding the TLPT to cover major non-bank group companies.

In a bid to make the TLPT more effective, they are expected to abide by various guidelines[13] and use international frameworks[14] to advance the assessment of attack scenarios developed by attackers (red teams) and of incident response capabilities by defenders (blue teams). They are also expected to continue the development of higher-level specialists required for such initiatives.

○ Trust and Internet banks, etc.

[9] "Recommendations to cashless payment service providers" (published on August 6, 2019) (https://www.fsa.go.jp/policy/shikinkessai/01.pdf)
[10] The FSA holds regular talks with three mega-banks, large securities companies, large life and nonlife insurers and Japan Post Bank.
[11] TLPT stands for Threat-Led Penetration Testing.
[12] In particular, the FSA promoted the enhancement of cybersecurity at agents for insurance companies in cooperation with their associations.
[13] "G7 fundamental elements for threat-led penetration testing," "The Guide for Financial Institutions to Implementing TLPT" by the Center for Financial Industry Information Systems (FISC)
[14] These frameworks are assumed to include ATT&CK by MITRE.

The FSA has monitored cybersecurity management systems[15] at trust and Internet banks, etc. through questionnaire and other surveys, confirming that they have generally developed basic cybersecurity management systems. In anticipation of the 2020 Tokyo Olympics and Paralympics, the FSA in PY2019 used questionnaire surveys for off-site monitoring of those that apparently have relatively greater risks.[16]

As a result, the FSA confirmed that basic cybersecurity management systems were generally maintained and found that some of them were promoting initiatives to advance cybersecurity. As some banks had room to improve the promotion of initiatives and the recognition of risks under the leadership of senior executives, however, the FSA shared problems with them and encouraged them to conduct improvement campaigns through dialogues.

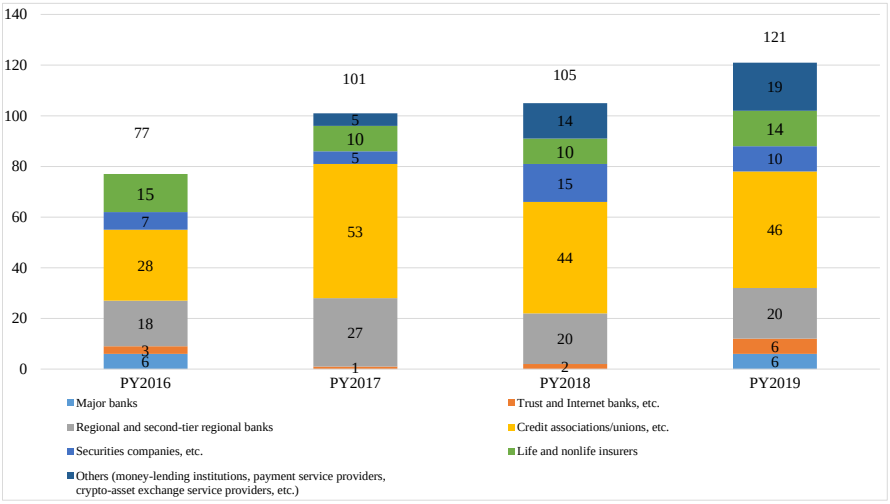
② Incident responses

As cyberattacks become more complex and sophisticated, FIs have limited ability to swiftly contain and defend against cyberattacks, indicating the importance of responses to attacks.

To respond accurately to cyberattacks, we must improve incident response capabilities through the plan-do-check-act cycle with exercise to checks on whether current response arrangements and procedures are sufficient.

Given the above, the FSA implements an annual Financial Industry-wide Cybersecurity Exercise called "Delta Wall" to improve FIs' incident response capabilities.

【Figure 4: Number of cybersecurity exercise participants by business type (by year)】



Source: FSA

In PY2019, a total of 121 companies (about 2,000 individuals) participated in the exercise to improve cybersecurity in preparation for potential large-scale incidents in the run-up to the 2020 Tokyo Olympics and Paralympics. The Exercise aims to improve cybersecurity as the entire financial industry, in which large, small, and medium-sized entities participated. The participating entities include funds transfer service

[15] The monitoring was implemented in PY2016-2017.
[16] They included FIs that were founded or changed business operations in or after FY2017 or just suffered cyberattack damage.

providers, issuers of prepaid payment instruments and audit firms, and so on, which were newly included business types. Through the exercise giving priority to ex-post assessment, many of those participants are implementing or planning revisions to their relevant inhouse policy and measures for enhancing internal and external information sharing, indicating that incident response arrangements are being improved through the exercise.

Among FIs, large banks, regional banks and insurance companies in general were found capable to respond to incidents. However, problems were seen at some FIs in regard to the restoration of computer systems and communications with customers. Other FIs generally had room to improve analyses of incidents, triage decisions on priority responses, communications with customers before an increase in their inquiries, and procedures for considering how to prevent similar incidents.

Based on findings through the exercise, the FSA needs to encourage improving incident response capabilities at FIs found having room to make improvements. Those found fully prepared to respond to incidents will be urged to deepen inhouse discussions on incident scenarios to further advance their incident response capabilities.

As well as the FSA, the National Center of Incident Readiness and Strategy for Cybersecurity (NISC), Financial ISAC (Information Sharing and Analysis Center) Japan, and industry group organize various cybersecurity exercises. It is important for FIs to improve incident response capabilities through participation in such exercises.

【Delta Wall (Financial Industry-wide Cybersecurity Exercise)】

The FSA has performed the Delta Wall (Financial Industry-wide Cybersecurity Exercise) every October since 2016 to upgrade the industry's incident response capabilities. Participants numbered 77 in PY2016, 101 in PY2017, 105 in PY2018 and 121 in PY2020.

➢ Delta Wall

"Delta" refers to the three keys to cybersecurity: self-help, public help and mutual help. "Wall" represents defense.

○ The exercise features the following:

- The exercise is designed to assess arrangements and procedures regarding FIs' internal and external information sharing in the event of an incident.
- Senior executives and other numerous stakeholders (including those belonging to computer system, public relations, planning and other divisions) participate in the exercise under the workplace participation approach.
- The exercise identify cyber risks based on private sector experts' knowledge and real attacks to indicate weaknesses into which FIs tend to plunge, leading participants to get such findings.
- The exercise gives priority to ex-post assessment to indicate specific solutions that would allow participating FIs to improve their incident response capabilities through the plan-do-check-act cycle.
- Common problems and good practices found through the exercise are fed back not only to participating FIs but also to the entire financial industry.
- Based on learnings from the past exercise, the FSA will continuously improve exercise methods to make it more effective.

③ Strengthening management systems in anticipation of 2020 Tokyo Olympics and Paralympics

As the 2020 Tokyo Olympics and Paralympics attracts global attention, not only stakeholders in the event but also Critical infrastructure operators such as FIs are feared to become cyberattack targets. Therefore, FIs should address their known vulnerabilities tending to trigger cyberattacks under measures as usual and secure their readiness to appropriately respond to cyberattacks to improve the effectiveness of basic cybersecurity management systems[17] developed so far. FIs should also be aware of the status of monitoring/analysis on their respective information assets to quickly detect and respond to incidents.

(a) Improving effectiveness of basic cybersecurity management systems

Based on the abovementioned recognition, the FSA asked regional banks and credit associations/unions to 1) conduct vulnerability scan, 2) to improve the effectiveness of contingency

[17] In particular, many credit associations/unions cooperated with their respective umbrella organizations in conducting risk assessments and formulating contingency plans in PY2018.

plans through exercises and training and 3) to straighten out and enhance the status of monitoring/analysis by the end of March 2020 and cooperated with their industry group in encouraging them to do so.

As a result, many of them conducted vulnerability scan, participated in exercises and training, and straightened out the status of monitoring/analysis by the deadline (the end of March 2020). In particular, those implementing vulnerability scan were limited to some 10% of credit associations/unions in PY2018, with those participating in external exercises accounting for only 60%. Both the percentages rose beyond 90% in PY2019. Nevertheless, some of them lagged behind others in meeting the FSA requests. The FSA will follow them up in cooperation with their industry group.

The FSA also conducted questionnaire and other surveys to examine whether the other FIs[18] met the three FSA requests, including the implementation of vulnerability scan. Although no particular problems were found regarding the three requests, the FSA will check and follow up their relevant initiatives as necessary.

(b) Effectiveness improvement practices and problems identified through request responses and questionnaire surveys

Regarding the vulnerability scan, the FSA found good practices to perform it as planned such scan for a specified scope, such as external websites (including websites of FIs and their group companies) and high-risk internal networks. However, some FIs, while recognizing that measures were required to address vulnerabilities found in the scan, were taking much time to decide on such measures due to their insufficient risk awareness.

Regarding exercises and training, the FSA found good practices to Participate involve external exercises and conduct internal training to revise contingency plans. However, some FIs failed to review their participation in exercises or link the exercise results to the identification and resolution of problems.

Regarding the cyber-incident monitoring/analysis, the FSA found good practices to develop arrangements to quickly detect and analyze incidents. However, some FIs, though having acquired relevant logs, failed to check or analyze them as usual.

Regarding the management of outsourcing, because some FIs failed to specify in their contracts that they have right to perform vulnerability scan and log monitoring, making it impossible to accomplish them. Some others' outsourcee refused to disclose cybersecurity countermeasures. Given these cases, it is important for FIs to improve the management of outsourcee, such as to clarifying how to share roles and responsibilities with outsourcee in their contracts.

Although a decision to postpone the 2020 Tokyo Olympics and Paralympics due to the COVID-19 pandemic was announced in March 2020, cyber risks have become even greater, indicating that it is important for FIs to refer to the abovementioned cases and continuously tackle the maintain and improve of basic cybersecurity management systems under senior executives' strong leadership. In particular, FIs that implemented vulnerability scan and cyber exercises for the first time in response

[18] City banks, trust banks, other banks, fund transfer service providers, securities companies, life/nonlife insurers, money-lending institutions, etc.

to the FSA requests should regularly implement such measures.

④ Responses to accelerating digitalization

In PY2018, the FSA classified digitalization into five broad realms[19] and interviewed large and other FIs to find out about and analyze their responses to challenges and risks.

In PY2019, the FSA interviewed domestic and foreign FIs and IT vendors to find out about and analyze progress in digitalization, including cloud computing.

(a) Overall cloud services

FIs in Japan have increasingly used cloud services, with more than 50% of them having introduced the services.[20] In particular, most banks have introduced the services. While the cloud services have been used primarily for emailing, internal information sharing and sales support systems, some FIs are building core business systems on public clouds.

Although FIs in Japan have reported no major cyber incidents originating from cloud services, a cyber incident attributable to incorrect cloud service settings occurred at a major U.S. financial holding company in March 2019.

Even though responsibility boundaries usually differ by type of cloud services (SaaS,[21] IaaS,[22] etc.), Cloud service users hold responsible to set, manage, and operate services properly. To this end, they must acquire skillful human resources[23] and continuously upgrade their skills according to changes in the services.

Large FIs were found trying to adopt new services early and continuously upgrade skills through training provided by Cloud service providers (CSP), target setting for the number of qualifies employees qualified to use cloud services, orientation meetings on new services and events sponsored by cloud service operators. They have also introduced systems or tools provided by cloud service operators or third parties to automatically detect and correct cloud service settings.

(b) Transition to new security models

Conventional security models feature security countermeasures for setting up boundary defense between reliable internal networks and unreliable external ones and have no concern.

As confidential information is put outside the boundaries through cloud services, however, conventional boundaries have become vague. As the workstyle reform and the COVID-19 pandemic have increased the needs for connecting external networks (including those of affiliates and third parties) to internal ones for telework, the risk of penetration has risen.[24]

Under such situation, large FIs are adopting security countermeasures (including the sophistication

[19] The five realms are (1) cloud services, (2) AI (RPA), (3) external cooperation (outsourcing), (4) external connection (external environment), and (5) IoT.

[20] According to a poll of FIs in PY2019 by the Center for Financial Industry Information Systems (FISC) (*Financial information Systems, November 2019*), 52.9% of FIs in Japan were using cloud services in PY2018.

[21] SaaS stands for Software as a Service.

[22] IaaS stands for Infrastructure as a Service.

[23] Those failing to secure relevant human resources may use managed cloud services.

[24] Even if a virtual private network is built, a connected terminal infected with malware could allow the malware to penetrate into an internal network through the VPN.

of user and device authentication and authorization[25]) under the Zero Trust Security Model, which considers even internal networks to be unreliable.

[25] The software defined perimeter (SDP) is cited for the sophistication of authentication under the Zero Trust Security Model. While two-factor authentication is used as a measure to sophisticate authentication, a scam to use the expanding smishing message service for mobile terminals for stealing one-time passwords could be exploited for breaking through the two-factor authentication for cloud services or VPN access, according to the "2019 Japan Security Roundup" by Trend Micro. It is risky to believe that two-factor authentication guarantees safety.

【A technological initiative】

●Container and microservices

Internet and other business sectors that feature rapid business changes and high uncertainties implement initiatives to introduce container, microservice architecture and other new technologies to quickly and continuously improve cloud services in line with user requests.

- Container technology:
  The container technology for virtualization creates independent spaces on a single operating system and realizes an operating system for each independent space to implement applications. It features lower system asset costs and greater portability.

- Microservice architecture:
  The microservice architecture designs a software application as a combination of small, independent and loosely coupled services. It enables a smaller application to be developed more quickly. Each application is created as an independent service that can be changed without affecting any other service.

In the financial sector, fund transfer service providers were found using these new technologies for their production environment. Internet and regional banks were also using such technologies for building core banking system on cloud services.

When introducing new technologies, FIs should ensure IT governance on selecting system projects for introducing it and appropriate approaches (agile development, etc.) for developing it, designing operating model (including DevSecOps)

for such technologies, and training and securing human resources versed in it.

- Need for training and securing human resources versed in new technologies
  New technologies feature frequent version upgrade to add new functions. To promptly respond to it, human resources must be continuously trained and secured not only for the development stage but also for the later operation stage.

Cyberattacks taking advantage of the container technology's vulnerabilities have already been detected, indicating that cybersecurity countermeasures are still required for such a new technologies. Such countermeasures include risk assessments considering new technologies' characteristics and differences from conventional ones and the adoption of security measures(Security by Design) even in the initial phase of development process.

(2) Initiatives through cooperation with relevant organizations and foreign authorities

① Improving effectiveness of information-sharing frameworks

To enhance cybersecurity in the financial sector, FIs should promote mutual help, including information sharing and joint analysis, based on their self-help.

As the FSA has taken every opportunity to promote FIs' understanding about the significance of their mutual help using information-sharing organizations, the number of FIs participating in Financial ISAC Japan has steadily increased.

Mutual help initiatives include not only the sharing of information about cyber threats and vulnerabilities but also that of information on effective security measures and the mutual provision of cybersecurity countermeasures. Although Financial ISAC Japan has played a leading role in FIs' sharing of information on cyber threats and vulnerabilities and about effective security countermeasures, FIs are expected to deepen mutual help, including the mutual provision of cybersecurity countermeasures by expanding cooperation with industry group further to enhance cybersecurity more and more. The FSA will continue to proactively support their mutual help.

② Cooperation in responding to large-scale incidents

The FSA launched the Liaison Council for Cybersecurity Stakeholders (hereinafter, the Liaison Council) in June 2019 to facilitate financial sector stakeholders' sharing of information in the event of cyber incidents, including large-scale ones.

The FSA has utilized the Liaison Council to enhance the financial sector's cooperation arrangements through the development of procedures and cyber exercises regarding large-scale incidents in anticipation of the 2020 Tokyo Olympics and Paralympics. Developing cooperation procedures, checking them through a cyber exercise (Delta Wall IV) and deciding to adopt the JISP (Japan cybersecurity Information Sharing Platform).

In the future, the FSA will promote information sharing based on its action plan,[26] participate in NISC-sponsored exercises to check the effectiveness of JISP-based information cooperation between Liaison Council members, and reaffirm information cooperation between Liaison Council members through cyber exercises(Delta Wall) to upgrade the entire financial system's incident response capabilities.

③ International cooperation

Because the financial system is globally interconnected, international fora, such as the G7 and G20 have promoted initiatives to ensure cybersecurity based on their partnership. In particular, the G7 Finance Ministers and Central Bank Governors Meeting in 2015 set up the Cyber Expert Group, which has accumulated discussions concerning cybersecurity. The annual meeting has published fundamental elements compiling best practices concerning cybersecurity since 2016 and formulated and published The Fundamental Elements for Threat-led Penetration Testing [27] in 2018. Given the publication of the elements, the FSA has encouraged large FIs to use the TLPT and cooperated with the Center for Financial Industry Information Systems (hereinafter, FISC), which published "The Guide for Financial Institutions

[26] "Fourth Action Plan for Critical Infrastructure Protection" (approved by the Cybersecurity Strategy Headquarters on April 18, 2017)
[27] Four sets of "fundamental element" have so far been published.

to Implementing TLPT" in September 2019 to make contributions to Japanese FIs' implementation of the TLPT.

In June 2019, a joint exercise to tackle an assumed large-scale cyber incident took place to check cross-border cooperation, mainly between G7 authorities.[28] In a follow-up to the exercise, discussions have been promoted on the enhancement of international cooperation, including the improvement of procedures for cooperation between G7 authorities, based on knowledge and lessons gained through the exercise.

Recent international discussions[29] have covered third parties including cloud services and operational resilience" concept such as restoration or recovery from cyber incidents. It is important to accurately assess and respond to international trends including such discussions.

3. Future FSA initiatives

Cyber risks surrounding FIs have increased further due to external environment changes accompanying the expanding COVID-19 pandemic and the postponement of the 2020 Tokyo Olympics and Paralympics until 2021. Given the situation, FIs should recognize the significance of cybersecurity and tackle cybersecurity countermeasures under their senior executives' leadership.

The FSA will promote primarily the following initiatives to further strengthen cybersecurity countermeasures in the financial sector:

○ Responses to financial sector environment changes

While digitalization use makes progress in the financial sector, a shift to online and remote services is accelerating in response to the COVID-19 pandemic, leading the financial sector environment to turn around. Cybersecurity has become an even more important challenge as the premise for such new financial services and infrastructure.

The FSA will proactively collect information on new security threats based on such environmental changes and encourage necessary responses, while tackling cybersecurity based on progress in digitalization.[30]

○ FIs' actions to strengthen cybersecurity

The FSA will encourage small and medium FIs to maintain and improve the effectiveness of their basic cybersecurity management systems through cooperation with their industry group and upgrade their incident response capabilities through cyber exercises. It will also collect practices through dialogues with each type of FIs making progress in cybersecurity countermeasures and proactively recommend good practices to small and medium FIs.

With international discussions in mind, the FSA will encourage large FIs through regular dialogues to upgrade risk management regarding group-wide and global cybersecurity and further advance cybersecurity countermeasures through the improvement of the TLPT effectiveness. As caution against destructive

[28] Japanese participants in the joint exercise included the FSA, the Bank of Japan, Financial ISAC Japan and large FIs.
[29] Discussions have taken place at the G20 FSB (Financial Stability Board), etc.
[30] This report is accompanied by the "Research Report Regarding IT Governance of Financial Institutions" and the "Analysis Report on Financial Institutions' Computer System Failure." Cybersecurity and system failure analysis are part of the IT governance to create corporate value. For example, it is important to perform IT governance and take note of security under adequate IT management to respond to progress in digitalization and new lifestyles

malware activities[31] is growing overseas, the FSA and FIs will also discuss cyber resilience initiatives in consideration of the risk of such malware failing to quickly be detected and continuing to work within networks over a long term.

[31] For example, the Office of the Comptroller of the Currency (OCC) issued the "Joint Statement on Heightened Cybersecurity Risk" (on January 16, 2020).