Policy Approaches to Strengthen Cybersecurity for Cryptoasset Exchange Services

April 3, 2026

Financial Services Agency

I. Awareness of Issues

A cryptoasset constitutes property value that can be transferred on the internet, using blockchain technologies as its basis. Attackers can steal the assets with property value in a moment, unlike in conventional finance. The cross-border transfer of assets is also quite easy, and stolen assets can be laundered at once. Due to such characteristics, cryptoassets are prone to targeting for theft in cyberattacks. In fact, since the emergence of Bitcoin, a number of cyberattacks targeting cryptoasset exchange service providers that caused the outflow of cryptoassets have occurred worldwide.

Recent cases involving the outflow of cryptoassets are not necessarily caused by the theft of signing keys,[1] but the trend of employing various other ingenious tactics, including indirect attacks, such as a social engineering attack[2] and intrusion into outsourcees,[3] has become prominent. Furthermore, there have been cases of cyberattacks wherein attackers took time to prepare for the intrusion in advance without being noticed by relevant cryptoasset exchange service providers, etc. Under such circumstances, the safe management of cryptoassets cannot be ensured only by the use of cold wallets.[4] Rather, it is definitely necessary to strengthen the cybersecurity management systems of the entire supply chain, including outsourcees.[5] In addition, the occurrence of cyberattacks suspected of involving some national governments for the purpose of acquiring foreign currencies is also pointed out.[6] The protection of cryptoassets is required not only for protecting users' property, but also from the perspective of preventing national wealth from being robbed by attackers with the suspected involvement of foreign governments as a means for the acquisition of foreign currencies.

Japan was the first nation to introduce regulations on cryptoasset exchange services, and it has requested service providers to take measures against the risks of an outflow of cryptoassets and

1 A signing key is a secret key to be used for proving that a transaction was conducted by a person with the legitimate authority by assigning an electronic signature to transaction data in advance. A leak of information on a signing key causes a risk of illegal asset transfers. In the FSA's "Guidelines for Administrative Processes—Financial Companies," the term, "secret key," is used, but ISO/IEC 14888 specifies that the term, "signing key," should be used. Accordingly, the term, "signing key," is used here.

2 A social engineering attack is a type of attack to illegally obtain credentials or system access authorities by sending a forged email or making a phone call or through spoofing, while taking advantage of unguarded moments of the victims or staff members.

3 Meaning an attack wherein an attacker does not directly attack the service provider's system from outside, but infringes a network or an account of an outsourcee that operates or develops the service provider's system and illegally intrudes into the system by using the relevant right thus obtained.

4 Meaning a method of managing cryptoassets by recording signing keys or other information necessary for transferring cryptoassets on an electronic device, etc. that is not connected to the internet all the time, or other methods of managing cryptoassets by taking any equivalent technical safety management measures.

5 As shown in the case that occurred in September 2025, wherein a malicious code was mixed into widely-used JavaScript libraries, there have been cases wherein attackers infringe OSS developers by sending targeted email or by other means and contaminate dependent libraries, thereby affecting the information systems of a number of companies as a whole. Therefore, attention should be paid to such supply chain risks, not only risks concerning outsourcees.

6 "Status of Threats in Cyberspace in the Upper Half of 2025" (September 2025), Cyber Police Agency, National Police Agency (https://www.npa.go.jp/publications/statistics/cybersecurity/data/R7kami/R07_kami_cyber_jyosei.pdf)
"Review and Prospect of Internal and External Situations (2026)," Public Security Intelligence Agency (https://www.moj.go.jp/content/001452738.pdf)

properly manage system risks, as a case of an outflow of cryptoassets deposited by users had actually occurred. Under the current circumstances where domestic and foreign investors have come to position cryptoassets as investment targets, it is necessary for individual service providers to properly protect users' property from outflow risks, constantly review their system risk management depending on the advancement of technologies and sophistication of attack techniques, or otherwise build robust cybersecurity management systems in order to be trusted by the general public. However, individual service providers may not necessarily be able to make proper responses against recent cyber risks on their own, and joint government and private-sector efforts combining self-help, mutual assistance, and public assistance are required.

Since July 2025, the Working Group on the Cryptoasset System[7] of the Financial System Council had discussed how the cryptoasset system should be developed, and compiled a report[8] on December 10, 2025. The report also points out the need to enhance the cybersecurity of cryptoasset exchange service providers. Based on the content of the report as well, the FSA decided to formulate the Policy Approaches to Strengthen Cybersecurity for Cryptoasset Exchange Services, with the aim of ensuring steady self-help efforts by individual service providers, encouraging mutual assistance efforts by the industry as a whole, and implementing certain support measures as public assistance efforts. The FSA published the Policy Approaches to share its details broadly with cryptoasset exchange service providers, cryptoasset service users, and other related parties.

II. Self-help

As explained in "I. Awareness of Issues," techniques for attacks against cryptoasset exchange service providers are becoming more and more sophisticated. Considering such trend, individual service providers definitely need to improve their cybersecurity measures on an ongoing basis based on collected information. The management teams of individual service providers must not consider cybersecurity measures merely as cost and only aim to satisfy the minimum standard. Ensuring robust cybersecurity measures is a strategic investment for protecting business earnings and supporting sustainable growth. Management teams need to be aware of their position being required to protect national wealth from malicious attackers, as mentioned above.

Blockchain technologies promote innovation, but they are made up of combinations of existing technologies. Accordingly, it is naturally important for individual cryptoasset exchange service providers to secure cybersecurity management systems at a level equivalent to that required for existing financial institutions, not only from the perspective of responding to risks unique to cryptoassets. In that process, only taking technological countermeasures is not sufficient. They need

[7] https://www.fsa.go.jp/singi/singi_kinyu/angoshisanseido_wg/angoshisanseido_wg_index.html
[8] https://www.fsa.go.jp/singi/singi_kinyu/tosin/20251210.html

to also take appropriate comprehensive cybersecurity measures encompassing the aspects of human resources and processes.

Given these, the FSA will continue ascertaining the current situations of individual service providers' cybersecurity management systems, review "16 Guideline for Supervision of Crypto-Asset Exchange Service Providers" [9] (the "Guidelines for Supervision") of the "Guidelines for Administrative Processes—Financial Companies," which will contribute to enhancing the level of the relevant systems, and ensure individual service providers' steady self-support efforts through monitoring by the FSA and the self-regulatory organization.

1. Intensive Monitoring of the Industry

In light of the occurrence of the large-scale outflow of cryptoassets in the past, the FSA has intensively monitored countermeasures against outflow risks and system risk management of individual cryptoasset exchange service providers and has encouraged them to strengthen their cybersecurity capabilities so that they can respond to increasing cyberthreats. From Program Year 2026 onward, the FSA will request all cryptoasset exchange service providers to conduct cybersecurity self-assessment (CSSA),[10] which the FSA has so far requested other types of financial business operators to conduct, or will otherwise have dialogues with cryptoasset exchange service providers as required, in consideration of risks unique to cryptoassets and the latest trends in cyberattacks. Through ongoing dialogues, the FSA will ascertain the statuses of individual service providers' cybersecurity management systems and encourage them to make improvements necessary for responding to increasingly sophisticated threats.

2. Raising the Levels of the Guidelines for Supervision

Based on the current situations of individual cryptoasset exchange service providers obtained through intensive monitoring of the industry as a whole and the results of the Blockchain Multilateral Joint Research Project (mentioned later) carried out in PY2025, the FSA will endeavor to raise the levels of cybersecurity expected for cryptoasset exchange service providers by revising the Guidelines for Supervision. For example, the FSA will deliberate on the following points from the perspective of ensuring the effectiveness.

- Requirements for the personnel structure relating to cybersecurity

[9] https://www.fsa.go.jp/common/law/guide/kaisya/16.pdf (in Japanese)
https://www.fsa.go.jp/common/law/guide/kaisya/e016.pdf (in English)

[10] By requesting individual service providers to conduct self-assessment by using questions consistent with the Guidelines on Cybersecurity for the Financial Sector (https://www.fsa.go.jp/common/law/cybersecurity_guideline.pdf), CSSA aims to provide them with opportunities for self-help efforts and encourage them to make improvements autonomously by enabling them to understand the position of their own organization within the industry.

Ideal standards concerning required expertise, appropriate staffing, and the authority granted to personnel responsible for cybersecurity

- Requirements for external audits

  Ideal external validation regarding system risk management, signing key management, etc.

- Requirements for cybersecurity to be satisfied by outsourcees

  Ideal comprehensive requirements in consideration of issues in practical operations and the latest technological trends

III. Mutual Assistance

The extent to which individual cryptoasset exchange service providers can individually investigate and ascertain risks of cyberattacks, which change from day to day, is limited. Therefore, it is preferable for the self-regulatory organization and information sharing organizations to provide information helpful for financial institutions, etc., share examples of countermeasures, offer support to financial institutions, etc. for creating their systems, while cooperating with the FSA as required, thereby promoting activities for strengthening the cybersecurity management systems of cryptoasset exchange services as a whole (mutual assistance efforts).

In order to ensure the effectiveness of mutual assistance efforts, it is important to develop a mechanism under which industry associations, etc. function substantially instead of merely existing as formal structures. Accordingly, the FSA will encourage industry associations, etc. to develop effective operational systems based on the understanding of the meaning of mutual assistance efforts.

1. Strengthening the Self-Regulatory Organization's Systems

For strengthening the cybersecurity management systems of the industry as a whole, it is also important to provide for technological and practical particulars by self-regulatory rules, not only by laws and regulations and the FSA's guidelines. The self-regulatory organization is required to update the self-regulatory rules on an ongoing basis, while properly responding to increasingly sophisticated threats, and to effectively monitor individual service providers' compliance. The FSA will continue to follow up on the self-regulatory organization's efforts for developing its systems and encourage it to make improvements as necessary.

More specifically, the FSA will request the self-regulatory organization to strengthen the functions of the Security Committee[11] and other committees through securing and fostering personnel with expertise, and to develop systems for constantly improving and enhancing the content of the self-

[11] Organizational chart of the Japan Virtual and Crypto Assets Exchange Association (JVCEA) (https://jvcea.or.jp/cms2026/wp-content/uploads/2026/04/jvcea-sosiki20260401.pdf)

regulatory rules. The FSA will also follow up on whether the self-regulatory organization has developed an audit system by utilizing specialized personnel and is able to conduct regular onsite and offsite monitoring of individual service providers' cybersecurity management systems effectively.

2. Recommendation for Information Sharing Organizations to Make Efforts to Strengthen Their Systems and for Service Providers to Participate in Information Sharing Organizations

In order to secure robust cybersecurity management systems of cryptoasset exchange service providers, individual service providers' efforts for the detection of threats and vulnerabilities and information gathering are important, but an industry-wide cooperative framework for information sharing is also absolutely necessary. In particular, it is necessary to develop a system to promptly share information on attack techniques that are frequently employed most recently and on vulnerabilities in general systems, etc. and to jointly analyze such information and consider countermeasures.

When developing a relevant system, in the same manner as in the case of the existing ISAC,[12] which is already functioning well in the financial sector, etc., it is extremely important also for the cryptoasset industry not merely to develop formal structures but to create a relationship of trust among working-level personnel in charge of security at individual service providers and develop a culture to share information effectively.

From the perspective of strengthening the cybersecurity management systems of the entire supply chain, it is necessary to consider how to collaborate with a broad range of entities, including outsourcees and affiliated businesses. In addition, taking into account the global nature of transactions of cryptoassets, it is preferable to establish a system through collaboration with foreign organizations to make it possible to easily access the latest information on cyberthreats and vulnerabilities.

From these viewpoints, the FSA will encourage individual service providers to participate in information sharing organizations, such as JPCrypto-ISAC,[13] and will positively exchange views on the ideal form of effective information sharing organizations with JPCrypto-ISAC, which is a representative information sharing organization in the cryptoasset exchange service industry, or will otherwise make efforts for strengthening the cybersecurity of the industry as a whole.

IV. Public Assistance

The FSA has made public assistance efforts for the entire financial industry, including cryptoasset exchange service providers, in collaboration with relevant organizations and the industry, such as

[12] The Information Sharing and Analysis Center (ISAC) is a non-profitable organization where companies and associations belonging to the same industry gather and share information on cyberattacks, vulnerabilities, security incidents, best practices, etc.

[13] Official website of the JPCrypto-ISAC (https://crypto-isac.jp/)

providing the Guidelines on Cybersecurity for the Financial Sector and other forms of guidance, conducting monitoring, and organizing and implementing the industry-wide cybersecurity exercise called Delta Wall. In order to further facilitate these efforts, the FSA will implement the following with regard to cryptoasset exchange service providers, in particular.

1. Blockchain Multilateral Joint Research Project

Since PY2017, the FSA has promoted the Blockchain Multilateral Joint Research Project[14] and has provided knowledge on fundamental technology risks inherent to decentralized financial systems. In PY2025, the FSA conducted the Research Survey on Challenges and Measures Concerning Cybersecurity for Cryptoasset-Related Service Providers, picked up representative cyberattacks that had occurred in and outside Japan, and analyzed attack techniques, risks, and countermeasures.

The FSA will continue such research and surveys and provide the outcomes to cryptoasset exchange service providers and information sharing organizations, thereby contributing to the enhancement of self-help and mutual assistance efforts. Taking into account the global nature of cryptoassets, the FSA will endeavor to deepen international collaboration by providing our domestic efforts as agenda on occasions of international conferences.

2. Financial Industry-Wide Cybersecurity Exercise (Delta Wall)

The Guidelines on Cybersecurity for the Financial Sector requires financial institutions, etc. to formulate a cyber incident response plan[15] and a contingency plan.[16] Accordingly, the FSA has organized and implemented the Financial Industry-Wide Cybersecurity Exercise (Delta Wall)[17] with the aim of further enhancing the capability to respond to incidents of the financial industry as a whole, including cryptoasset exchange service providers. The FSA has provided feedback on problems that became clear through exercises to businesses to encourage them to make improvements as required and has thus endeavored to strengthen the cybersecurity management systems of the entire industry.

In PY2025, a scenario and assessment standards for cryptoasset exchange service providers were newly created. The FSA will continue to review the details of the exercise in consideration of the latest

[14] The FSA has consistently conducted research and surveys on technology risks, etc. relating to decentralized financial systems. The FSA has published the outcomes of [i] Research on Technology Risks in the Chain of Trust in Decentralized Financial Systems in PY2021; [ii] Research on Understanding Decentralized Financial Systems Using On-Chain and Off-Chain Data in PY2022; and [iii] Research on the Evolution of Tokenization in the Financial Sector and the Feasibility of the Use of Blockchain Technology for RegTech/SupTech in PY2023.

[15] A plan systematizing initial responses required in the event of a cyber incident and measures for preventing the spread of damage, eliminating the cause of damage, and achieving recovery, etc.

[16] A plan prescribing alternative means for financial institutions to continue and recover their material operations in the event of a serious failure or an emergency

[17] A cybersecurity exercise that the FSA organizes and implements every year with the aim of enhancing the capability to respond to incidents of the financial industry as a whole. Delta Wall stands for the triad (Delta) of “self-help, mutual assistance, and public assistance” and defense (Wall).

trends in cyberattacks in order to secure an even more practical environment for the exercise. The FSA will continue requesting cryptoasset exchange service providers to participate in the exercise regularly, aiming to achieve the participation of all service providers within three years.

3. Demonstration Project for Threat-Led Penetration Testing (TLPT)

Verification through Threat-Led Penetration Testing (TLPT)[18] is said to be effective in checking whether individual cryptoasset exchange service providers' current cybersecurity measures are sufficient against increasingly sophisticated cyberattacks. Individual service providers need to ascertain weak points in their entire organization, including human resources and processes, not only their technological weakness, through TLPT and make improvements appropriately.

As a policy for enhancing financial institutions' cyber resilience, the FSA has provided case examples concerning TLPT by financial institutions and has conducted a demonstration project for TLPT targeting regional financial institutions, etc.

With regard to cryptoasset exchange service providers as well, the FSA will demonstrate the effectiveness of TLPT with the aim of lowering barriers for them to implement TLPT and facilitate its dissemination. More specifically, within 2026, the FSA will conduct TLPT targeting several service providers regarding their actual operational environments, provide assessment results to the targeted service providers individually and extracted common issues to the industry as a whole,[19] thereby endeavoring to strengthen the cybersecurity of the entire cryptoasset industry.

V. Conclusion

The Policy Approaches present a direction for cryptoasset exchange service providers' efforts to strengthen cybersecurity amid the further sophistication and diversification of threats surrounding cryptoassets. The FSA will steadily implement various measures based on the Policy Approaches and will constantly review those measures as necessary in light of technological trends and attack techniques regarding cryptoassets and progress made in international discussions, aiming to improve and maintain the effectiveness of relevant measures.

It is important to maintain collaboration with cryptoasset exchange service providers, the self-regulatory organization, information sharing organizations, relevant businesses, foreign authorities, etc. and make joint government and private-sector efforts for the strengthening of cybersecurity.

[18] TLPT refers to more practical testing to verify the possibility of intrusion and falsification, the possibility of detection, and the promptness and appropriateness of responses by first analyzing the risks of one's own organization specifically and then launching a pseudo attack simulating tactics and techniques to be employed by real attackers. It is also called Red Team Testing. (Analysis Report on IT Resilience in the Financial Sector (June 2025)) (https://www.fsa.go.jp/news/r6/sonota/20250630-2/01.pdf)

[19] Recommendations upon conducting TLPT, Chapter 2, Section 2 of the Analysis Report on IT Resilience in the Financial Sector (June 2025) (https://www.fsa.go.jp/news/r6/sonota/20250630-2/01.pdf)

Individual cryptoasset exchange service providers are expected to carry out initiatives autonomously based on the Policy Approaches and continue playing positive roles in securing the safety and reliability of the cryptoasset market in Japan.