Japan's Expanding Economic Security Framework and Its Impact on Financial Institutions

Jun Tsutsumi

20 May 2026

Iakyara vol.415

Nomura Research Institute, Ltd.

Executive Summary

Japan is planning to establish a public-private council on economic security. Financial institutions required to participate will have to build rigorous information management regimes. With the data security provisions of the Economic Security Promotion Act's forthcoming amendment still under discussion, financial institutions should start preparing early instead of waiting until the amendment is finalized. Such preparations should reference European and US regulation and address matters such as PII handling and outsourcing controls.

Jun Tsutsumi
Senior Chief Expert
Financial Technology Solution Division

Amid mounting geopolitical tensions and the challenging security environment of recent years, national security's purview has expanded into the economic sphere. Japan enacted its Economic Security Promotion Act[1] (ESPA) four years ago in May 2022. In May 2024, Japan launched a critical infrastructure program, the aim of which is to ensure that critical infrastructure services are stably provided, including by financial institutions. The Cabinet Office reported that some 40% (386) of the infrastructure installation or third-party contracting plans the government reviewed in 2024 were from the financial sector. As this review process progressed, the Cabinet Office and Financial Services Agency (FSA) iteratively updated their interpretive guidance on the program.

The ESPA's Supplementary Provisions stated that the law was to be amended around three years after its enactment. A panel of experts has been working on the prospective amendment since July 2022. In January 2026, the panel released a set of recommendations for further promoting economic security. Draft legislation based on the recommendations was approved by the Cabinet on March 19. The legislation is expected to be deliberated on and enacted by the Diet during its 2026 special session. Below we discuss the expert panel's recommendations and the draft legislation's provisions on a public-private council and data security, both of which are important for financial institutions.

Another public-private council to be established

To expand the purview of national security to include the economy, the government must coordinate with the private sector given its predominant role in running the economy. The draft ESPA amendment therefore includes establishment of a

NOTE

1) The ESPA's official title is Act on the Promotion of Ensuring National Security Through Integrated Implementation of Economic Measures.

public-private council as recommended by the expert panel. The council's agenda will include addressing inherent risks, analyzing residual risks and assessing both routine and emergency measures. However, what will have the greatest impact is not the agenda itself, but rather how sensitive information is managed in the course of those discussions.

At council meetings, sensitive government information will presumably be shared with council members from the private sector. Council members will be required to sign an NDA, violation of which would subject them to the same penalties as national government employees. Another public-private council is slated to be established on October 1, 2026, under the recently enacted Active Cyber Defense Act[2] (ACDA). Members of the ACDA council will likewise have access to confidential government information, such as background information on cyberattacks. They will therefore be required to obtain security clearances[3] on an as-needed basis.

2) The ACDA's official title is Act on Prevention of Damage from Unauthorized Acts against Critical Computer Systems.
3) "Eligibility assessment" is the term used in the ACDA.

For the ESPA public-private council, security clearances have not yet been mentioned. However, the issue may arise during the Diet's upcoming deliberations on the ESPA amendment.

Sharing sensitive information is valuable, but disclosure will be restricted by NDAs. Companies receiving such information will therefore need to designate an internal unit responsible for handling it and establish information management frameworks and usage procedures.

Data security in economic security context

On the topic of data security, the ESPA expert panel recommended that the national government assume responsibility for determining how sensitive personal data and data related to critical infrastructure should be protected in light of the potential national security and public safety risks posed by leaks or other breaches of privately held data.

Sensitive personal information in particular is covered by the Personal Information Protection Act (PIPA), which aims to protect individuals' rights and interests, but Japan does not have any laws, regulations or institutions that address sensitive personal information from a national-security standpoint In terms of safeguards against leaks, tampering and data loss, the security measures implemented by

Japanese data owners, data centers and cloud providers compare unfavorably with the data security regimes now being developed in Europe and the United States. The data security provisions of the ESPA amendment may overlap with those of the PIPA, making it necessary to strike an appropriate balance between the two frameworks.

The ESPA expert panel also recognizes the need to ascertain the actual state of data security implemented by owners of data containing personally identifiable information (PII), data centers and other cloud providers. Although not specifically mentioned in the panel's recommendations or the draft ESPA amendment, direct government oversight of data centers and cloud providers is apparently under consideration as an option.

In any case, the expert panel has not reached any conclusions on data security. It has yet to complete its discussions on data security or release any details thereof, but it has mentioned US Executive Order 14117 in the context of managing sensitive personal data. In the context of data center and cloud service regulations, the panel has mentioned a US rule titled Securing the Information and Communications Technology and Services Supply Chain, aathe EU's NIS 2 Directive[4] and the UK's NIS Regulations. Japan's future data security regime may ultimately draw heavily from these European and US policy frameworks.

4) Network and Information Systems Directive 2022/2555

European and US data security regimes

US Executive Order 14117's final rule[5] took effect in October 2025. It prohibits or restricts specified transactions or agreements involving access to sensitive personal data in a quantity exceeding a specified threshold with countries of concern (China (including Hong Kong and Macau), Cuba, Iran, North Korea, Russia and Venezuela) or so-called covered persons (individuals or entities directly or indirectly affiliated with a country of concern). Sensitive personal data is defined to include financial data (when the dataset exceeds 10,000 persons). If the counterparty is a country of concern or covered person, outright sales of financial data are prohibited and vendor agreements or employment agreements that allow direct access to sensitive personal data are subject to restrictions.

5) https://www.federalregister.gov/documents/2025/01/08/2024-31486/preventing-access-to-us-sensitive-personal-data-and-government-related-data-by-countries-of-concern

The Executive Order's final rule provides examples of employment and vendor agreements. An employment agreement with an employee who is a citizen of and primarily resides in a country of concern would be a restricted transaction. Likewise,

a vendor agreement between a US data center and a vendor headquartered in a country of concern would also be a restricted transaction. Here, "restricted" means that the US Cybersecurity and Infrastructure Security Agency's security requirements[6] must be met, including organizational-level requirements, access controls and data masking. If these security requirements are not met, an employment agreement or a vendor agreement with a country of concern or covered person would be a prohibited transaction. The requirements pose a high hurdle.

6) https://www.cisa.gov/sites/default/files/2025-01/Security_Requirements_for_Restricted_Transaction-EO_14117_Implementation508.pdf

The NIS 2 Directive's regulatory purview includes the data center and cloud service sector[7], which is not within the scope of Japan's critical infrastructure program[8], in addition to the energy and financial sectors. The directive applies to (1) businesses designated by national authorities based on their scale and the nature of their services and (2) businesses that register of their own volition. National designation criteria differ among EU-member states. Businesses within the directive's purview are subject to direct oversight by national authorities.

7) Digital infrastructure and ICT service management (B2B)
8) The ESPA expert panel recommended adding healthcare to the 15 sectors already within the critical infrastructure program's purview.

The NIS 2 Directive applies to financial institutions but the Digital Operational Resilience Act (DORA), which is tailored specifically to financial services, takes precedence over it. In addition to regulating financial institutions themselves, DORA designates financial institutions' cloud service providers as critical third-party providers subject to direct oversight by financial authorities. Both NIS 2 and DORA are already in effect. The two-pronged framework left many operational details to be determined later. The European vendors we have spoken to appear to be placing priority on DORA compliance first.

Data security is not on the Diet's 2026 special session's agenda, so financial institutions will have a year or more to prepare. The government seems set to proceed with aligning the amendment with the PIPA and deciding whether to create a data security regime specifically for financial institutions like the EU's. Financial institutions may not be able to comply with the forthcoming data security requirements unless they soon begin preparing under the assumption that the requirements will be similar to US Executive Order 14117 and the EU's NIS 2 Directive and DORA.

about NRI

Founded in 1965, Nomura Research Institute (NRI) is a leading global provider of system solutions and consulting services with annual sales above $5.1 billion. NRI offers clients holistic support of all aspects of operations from back- to front-office, with NRI's research expertise and innovative solutions as well as understanding of operational challenges faced by financial services firms. The clients include broker-dealers, asset managers, banks and insurance providers. NRI has its offices globally including Tokyo, New York, London, Beijing and Sydney, with over 16,800 employees.

For more information, visit https://www.nri.com/en

Inquiries to : Business Planning Department, Financial Technology Solution Division
Nomura Research Institute, Ltd.
Otemachi Financial City Grand Cube,
1-9-2 Otemachi, Chiyoda-ku, Tokyo 100-0004, Japan
E-mail : kyara@nri.co.jp

https://www.nri.com/en/knowledge/publication/list.html#lakyara