

Early Action to Address the “Sovereignty Gap” — Policy Recommendations for Securing Digital Sovereignty —

KDDI Research, Inc. Public Policy Group, Think Tank Division

September 2026 (First Edition)

Translator’s note. This is an English translation of the Japanese original published on September 30, 2026. Figures and tables have been redrawn in English. Statements, dates, figures, and references are translated as presented in the source; in case of discrepancy, the Japanese original prevails.

Current Situation — Why Action Is Needed Now

2

1. Competition over standards has begun

In 2026 the EU implemented SEAL, a system for quantitatively assessing cloud sovereignty, in government procurement, and the proposed Cloud and AI Development Act (CADA) is extending it into the legislative agenda. International competition over standards that make digital sovereignty visible has already begun

2. Dependence is becoming entrenched

About 97% of systems on the shared government cloud infrastructure (on a system basis) run on a single overseas service. Annual digital-related net payments abroad have settled in the JPY 6 trillion range (one pessimistic estimate puts the figure at about JPY 28 trillion in 2035)

3. No common yardstick

Japan has no common yardstick for measuring the sovereignty of cloud and other digital services — who owns them, which country's laws apply, and who controls their operation. Perspectives corresponding to about 65% of the EU assessment framework fall outside existing Japanese schemes

**Consequences: procurers lack a basis for decisions, users cannot verify whether a provider is “worthy of being entrusted with data,” and providers cannot convert trustworthiness into competitiveness
— The absence of a yardstick for assessment is the “sovereignty gap”**

The “Sovereignty Gap” in Numbers

3

97%

Share of systems on the shared government cloud infrastructure running on a single overseas service (end of March 2025)

Source: reporting based on Digital Agency figures

¥6.6tn

Annual digital-related net payments abroad (2025, three categories). Deficits in the JPY 6 trillion range have become entrenched

Source: Information and Communications White Paper 2026

65%

Share of the EU sovereignty assessment framework’s eight objectives not assessed by existing Japanese schemes (by assessment weight)

Source: KDDI Research analysis (Report, Chapter 4)

The core of the sovereignty gap is not the scale of dependence itself (97%, JPY 6.6 trillion) but the lack of a yardstick for measuring and verifying it (65%). Without a yardstick, procurement, use, and investment have no basis for decisions.

Basic Principles of the Recommendations — Four Principles

Principle 1 Fair assessment

Improve verifiability without seeking to exclude particular countries or providers. Non-discrimination between domestic and foreign providers; consistent with the U.S.–Japan Digital Trade Agreement and the WTO Agreement on Government Procurement. Distinct from localization requirements

Principle 2 Phased implementation

From disclosure to assessment. Implement progressively, starting with sensitive sectors (healthcare)

Principle 3 International alignment

Build compatibility with the EU assessment framework into the design from the outset, and secure the interoperability that implements DFFT

Principle 4 Public and private roles

Government establishes the framework and the procurement environment; the private sector puts trust into practice. Toward a market in which multiple providers compete on trustworthiness

Assessment prevents exclusion: if tensions rise without a yardstick, the “sovereignty gap” may be filled by blanket exclusion based on crude criteria such as the nationality of capital. Preparing an assessment framework in advance is the realistic route to filling the gap while keeping markets open

Overview — Five Recommendations

5

Rec. 1 Begin joint consideration of a Japanese sovereignty assessment framework across industry, academia, and government

Rec. 2 Standardize information disclosure on the sovereignty of cloud services

Rec. 3 Ensure the ability to switch cloud providers and expand available options

Rec. 4 Map sector-specific cloud dependencies, starting with medical information infrastructure managed by the state

Rec. 5 Ensure international interoperability of sovereignty assessment as a practical implementation of DFFT

Recommendation 1 (assessment framework) is central. Recommendations 2 (disclosure) and 3 (switching) support the procurement environment, Recommendation 4 (mapping dependencies) supplies the basic data, and Recommendation 5 (international interoperability) provides the outlet

Recommendation	Relevant provisions of the Basic Policy 2026
Rec. 1 Assessment framework	“Develop AI and data infrastructure while establishing open AI sovereignty” (Chapter 2, 1(2)) — provides institutional means to make verifiable the sovereignty of cloud, the infrastructure on which AI and data run
Rec. 2 Standardized disclosure	Promote adoption of cloud for highly confidential information and “reach certain conclusions on the optimal procurement method and related matters during 2026” (Chapter 2, 2(1)) — material that directly supports that examination
Rec. 3 Ability to switch	Gives concrete form to “strengthening the resilience and improving the autonomy of the government’s digital infrastructure” (Chapter 2, 1(2)) and “necessary measures to ensure the security and other relevant aspects of data centers and cloud services” (Chapter 2, 2(2))
Rec. 4 Mapping dependencies	The public–private investment roadmap positions “medical DX infrastructure optimized for cloud-native operation” among key products and technologies (Chapter 2, 1(1)) — makes its dependence structure identifiable
Rec. 5 International interoperability	Building a “trusted economic area,” international standardization, and stronger cooperation with like-minded countries (Chapter 2) — an implementation route through DFFT

Note: Each recommendation in the full policy proposal identifies the related government policy.

Recommendation 1 Begin joint consideration of a Japanese sovereignty assessment framework (industry, academia, government)

Establish, at an early date, an open forum involving industry, academia, and government to consider a Japanese framework for assessing the sovereignty of cloud services at graduated levels (a system of assessment criteria and levels), and develop a first, trial version of the assessment criteria for broad consultation.

Issues to examine: the design of the assessment criteria (ownership and capital relationships / governing law and risks from extraterritorial law / supply-chain composition / who controls operations, monitoring, and encryption-key management), the bodies and methods for third-party assessment, the relationship with existing schemes, and compatibility with the EU framework.

Whereas the EU requires consensus among 27 Member States, Japan has the structural advantage of being able to implement institutions rapidly as a single state.

Responsible parties	Stakeholders from industry, academia, and government
Timeline	Establish the forum at an early date and proceed to the development of, and consultation on, a first version of the assessment criteria
Expected benefits	A common basis for procurement decisions and user choice. Capacity to participate in shaping international standards

Recommendation 2 Standardize information disclosure on the sovereignty of cloud services

In government procurement, establish a mechanism for disclosing, in a common format and in addition to security information, basic information on sovereignty — ownership and capital relationships, the applicable governing law and risks from extraterritorial law, supply-chain composition, and the identity and location of those who carry out operations, monitoring, and encryption-key management.

The first stage is the standardization of disclosure, not assessment; once such information has accumulated as a basis for procurement decisions, consider its use for assessment as a second stage. Cloud services are “credence goods” whose quality is difficult to verify even after use, so standardized disclosure alone substantially reduces information asymmetry. There is more than one route to implementation: revisions to existing assessment schemes or improvements to procurement practice.

Responsible parties	Government (ministries and agencies responsible for IT procurement)
Timeline	Begin consideration of a disclosure format within FY2026, and promptly begin its use in procurement practice (submissions and references based on the format)
Expected benefits	Better information for procurement decisions. More predictable disclosure practice for providers. A smooth connection to the assessment system (Recommendation 1)

Recommendation 3 Ensure the ability to switch cloud providers and expand available options

For cloud use by government and in critical-infrastructure sectors, (1) regularly identify and publish the degree of concentration on particular services, and (2) ensure the portability and interoperability of data and systems so that users can effectively switch providers when necessary.

Excessive concentration on a particular service is a vulnerability to continuity in the face of major outages, price changes, and geopolitical interruptions of supply. Without the ability to switch, disclosure and assessment do not produce real choices. Conditions are improving — the EU Data Act’s rules on cloud switching, and the full approval of a domestic service in Japan (2026). Advance the government’s multi-cloud and approval-expansion efforts further, in measurable form.

Responsible parties	Government and the ministries and agencies responsible for critical infrastructure
Timeline	Consider a framework for measuring concentration within FY2026, followed by regular publication. Examine institutionalization of portability and interoperability, with reference to the EU Data Act’s switching rules
Expected benefits	Greater resilience to supply interruptions and outages. Choices in price and quality through the maintenance of competition

Recommendation 4 Map cloud dependencies, starting with state-managed medical information infrastructure

Advance efforts to identify which cloud infrastructure the core systems of Japan’s major sectors run on. No comprehensive official statistics describe private-sector dependencies; filling this gap is itself the first policy task, preceding any assessment system.

The leading target is medical information infrastructure managed by the state (standardized electronic health records, platforms for sharing medical information, etc.). Design and legislation are under way, so the window to build in the assessment perspective is open now (a window of institutional formation); for state-managed infrastructure, requests to identify dependencies are less likely to raise legal questions, and no burden falls on individual healthcare institutions. Rather than a new large-scale survey, it is realistic to add items on infrastructure usage to existing medical DX survey and reporting frameworks.

Responsible parties	Government (relevant ministries and agencies)
Timeline	Design the mapping method within FY2026, and begin initial mapping of state-managed medical information infrastructure in FY2027
Expected benefits	Basic data for policy decisions. Material for deciding priority sectors in phased implementation (Principle 2)

Recommendation 5 Ensure international interoperability of sovereignty assessment as a practical implementation of DFFT

A subsequent-stage initiative, premised on the domestic foundations established by Recommendations 1–4. Design the Japanese sovereignty assessment framework (Recommendation 1) to permit comparison with the EU framework (SEAL and the assurance levels in the proposed CADA), and begin dialogue toward future mutual recognition. The subject of recognition is not equivalence of security but the verifiability of sovereignty (transparency of governing law and of who controls operations, monitoring, and encryption-key management).

Seven years after DFFT was proposed, an implementation framework for measuring and assessing its “trust” has yet to take concrete shape. Interoperability of sovereignty assessment is a concrete route to implementing DFFT as an institution, and the Japan–EU ministerial dialogue planned for 2027 is a realistic opportunity. Over the medium to long term, extending the APEC CBPR model to mutual certification of cloud sovereignty (the APEC-CSCR concept) also comes into view.

Responsible parties	Government (relevant ministries and agencies)
Timeline	Begin international dialogue in parallel with consideration of the domestic assessment framework
Expected benefits	Demonstrable trustworthiness of Japanese providers in international markets. Concrete expression of Japan’s legitimacy as the originator of DFFT



For inquiries about this report, please contact us at:

<https://www.kddi-research.jp/inquiry.html>