

Research Report on Digital Sovereignty

Concepts, Institutions, International Comparisons, Public Trust, and Policy Implications

September 2026 (First Edition)

KDDI Research, Inc.

Public Policy Group, Think Tank Division

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.

Contents

Executive Summary

Chapter 1. Why Digital Sovereignty Now? The Issues at Stake

- 1.1 Purpose and Background of This Report
- 1.2 Structural Change: The Convergence of Three Trends
 - 1.2.1 Geopolitical Risks Become Tangible
 - 1.2.2 Rapid Growth of the Sovereign Cloud Market
 - 1.2.3 Japan's Structural Challenges
- 1.3 The Questions Addressed in This Report

Chapter 2. The Origins and Transformation of Sovereignty: Its Extension into the Digital Space

- 2.1 The Traditional Concept of Sovereignty
- 2.2 The "Threefold Mismatch" of Sovereignty in the Digital Space
- 2.3 Multiple Layers of Sovereign Actors: States, Businesses, and Individuals
- 2.4 Academic Debates on the Definition of Digital Sovereignty

Chapter 3. National and Regional Digital Sovereignty Strategies: A Comparative Analysis of Four Models

- 3.1 The EU Model: From "Strategic Autonomy" through Regulation to "Sovereignty through Implementation"
- 3.2 The U.S. Model: "De Facto Sovereignty" through Technological Dominance and Extraterritorial Law
- 3.3 The Chinese Model: State-Controlled "Cyber Sovereignty"
- 3.4 Japan's DFFT Model: "Coexistence Based on Trust"
- 3.5 Comparison and Classification

Chapter 4. Japan Today: Institutional Gaps and the "Sovereignty Gap"

- 4.1 A Systematic Overview of Japan's Relevant Legal and Institutional Frameworks
 - 4.1.1 Economic Security Promotion Act
 - 4.1.2 ISMAP
 - 4.1.3 Government Cloud
 - 4.1.4 Three Laws Regulating Platforms
- 4.2 Structural Analysis of the "Sovereignty Gap"
- 4.3 Policy Implications

Chapter 5. Digital Sovereignty and Public Trust: The Two Axes of Capability and Legitimacy

- 5.1 The Academic Origins of the Social License to Operate (SLO)
- 5.2 A Two-Axis Framework of Capability and Legitimacy
- 5.3 The Potential for a Japanese Approach

Chapter 6. Key Findings and Policy Implications

- 6.1 Findings from the Discussion So Far
- 6.2 Japan's Options: Four Future Scenarios and the Collaborative Model
- 6.3 Policy Recommendations
 - 6.3.1 Adding a "Sovereignty Assessment Layer" to ISMAP
 - 6.3.2 Phased Consideration of a Japanese Sovereignty Assessment Framework (J-SEAL)
 - 6.3.3 International Development: Mutual Recognition with EU SEAL and the APEC-CSCR Concept
 - 6.3.4 Broadening Implementation of the Economic Security Promotion Act
- 6.4 A Phased Approach: Why Start with Healthcare?
- 6.5 The Role of Providers: Multiple Actors Responsible for Public Trust
- 6.6 Activities to Begin Implementing the Recommendations

Acknowledgments

Endnotes

References

Foreign-Language Literature

Japanese-Language Literature

Policy and Institutional Documents

Executive Summary

This report aims to answer the questions "What is digital sovereignty?" and "What position should Japan adopt?" through international comparisons of concepts and institutions. These questions arise from structural challenges in Japan's digital infrastructure. Existing frameworks, including government procurement, assess cloud security but lack a yardstick for assessing sovereignty: which country's laws apply, and who controls operations and encryption keys.

This report deliberately defines digital sovereignty as "the ability of individuals, businesses, and states to autonomously control their own data and systems in the digital space." International comparisons show that the EU is shifting its emphasis toward "sovereignty through implementation," using assessment and procurement. The EU Cloud Sovereignty Framework (SEAL) quantitatively assesses sovereignty across five levels and eight sovereignty objectives. It was first applied to government procurement in April 2026 and is being extended into the legislative agenda through the proposed Cloud and AI Development Act (CADA). The United States exercises de facto sovereignty through the extraterritorial application of its laws, while China is building a closed model based on state control. Japan advocates Data Free Flow with Trust (DFFT), but without an implementation framework for measuring and verifying "trust," the principle itself risks becoming hollow.

An examination of Japan's institutions shows that ISMAP specializes in security assessment, while the cloud program under the Economic Security Promotion Act focuses on ensuring production and supply capacity. No institutional framework assesses areas corresponding to 65% of the sovereignty objectives in the EU framework, including strategic sovereignty, legal and jurisdictional sovereignty, supply-chain sovereignty, and technological sovereignty. This report calls this the "sovereignty gap." To address it, the report presents two axes: Capability and social Legitimacy. The first stage is to secure multiple domestic options through sovereignty assessment. The subsequent question is whether the providers of those options can earn and maintain public trust. The report proposes a Japanese approach using the Social License to Operate (SLO) as an axis for assessing trust.

The report compares four future scenarios: maintaining the status quo, a domestic-technology-led model, a hyperscaler-led model, and a collaborative model. It presents the collaborative model as a realistic starting point. Policy directions discussed include consideration of a sovereignty assessment framework, standardization of information disclosure, and international interoperability. Specific actions have been compiled separately in a companion policy proposal containing five recommendations.

This first edition is based on research using publicly available information and interviews with domestic stakeholders. An updated edition is scheduled for publication in March 2027, incorporating the findings of overseas research planned from the second half of fiscal year 2026 onward.

Chapter 1. Why Digital Sovereignty Now? The Issues at Stake

1.1 Purpose and Background of This Report

In a world where digital technologies underpin society, the economy, and security, digital sovereignty is no longer merely a technological trend. It is a structural issue at the heart of national governance, industrial competitiveness, and the protection of individuals' rights and interests. This report therefore aims to systematically organize academic and policy debates on digital sovereignty and clarify the position Japan should adopt and the roles expected of private-sector providers.

The report organizes social debates on digital sovereignty from an interdisciplinary perspective. It presents the origins of the concept (Chapter 2), compares national and regional strategies (Chapter 3), examines Japan's institutional challenges (Chapter 4), and introduces the new perspective of "public trust" (Social License) (Chapter 5), before discussing Japan's options and policy implications in Chapter 6. The main text is intended to be accessible; academic and institutional supporting material is compiled in the endnotes.

This report was prepared as part of research conducted by KDDI Research, Inc. Its analysis and recommendations are based on publicly available information and academic literature and do not recommend the use of any particular provider or service. This first edition is based on desk research using publicly available information and interviews with domestic stakeholders. We plan to conduct overseas research from the second half of fiscal year 2026 onward and will update the report in light of its findings. Please consult our website for the latest edition.

1.2 Structural Change: The Convergence of Three Trends

Before considering the report's questions - "What is digital sovereignty?" and "What position should Japan adopt?" - we first examine how the environment surrounding Japan is changing and the effects of those changes.

1.2.1 Geopolitical Risks Become Tangible

In recent years, countries around the world have made the enclosure of data and technologies a national strategy. In April 2026, the EU conducted its first procurement under the Cloud Sovereignty Framework, worth up to approximately EUR 180 million over six years, applying quantitative sovereignty scores as procurement criteria for the first time [Note 1]. In the United States, under the TikTok divestiture law enacted in 2024 (the Protecting Americans from Foreign Adversary Controlled Applications Act), a joint venture to operate the company's U.S. business was established in January 2026. Its framework provides for retraining a copy of the recommendation algorithm using only U.S. user data [Note 2]. In October 2025, China comprehensively revised its Cybersecurity Law for the first time, effective January 2026, introducing an AI provision covering oversight of AI safety management and ethical standards, as well as support for AI development [Note 3]. These developments all reflect efforts by states to exercise their sovereignty in the digital space, indicating that its reinforcement is moving into the implementation phase through concrete policies.

1.2.2 Rapid Growth of the Sovereign Cloud Market

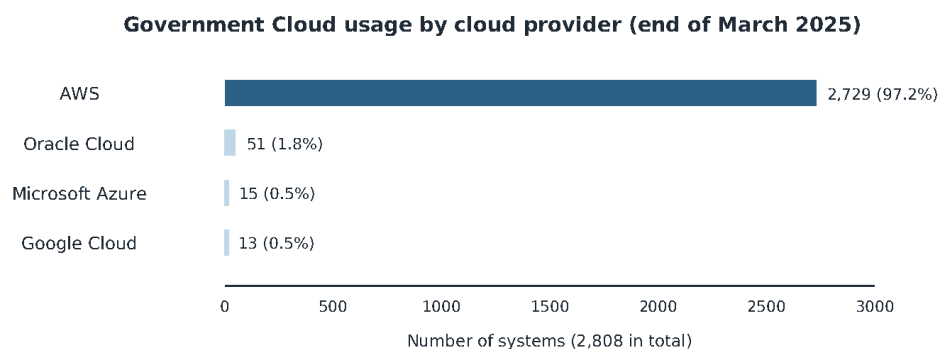
Meanwhile, markets related to digital sovereignty, such as sovereign cloud, are expanding rapidly. Gartner estimates that worldwide sovereign cloud IaaS spending will reach approximately USD 80.4 billion in 2026, up 35.6% year on year. European spending is expected to almost double from approximately USD 12.6 billion in 2026 to approximately USD 23.1 billion in 2027, exceeding North America for the first time. Japan's market, although small, is also expected to more than triple, from approximately USD 520 million in 2025 to

approximately USD 1.82 billion in 2027 [Note 4]. Estimates by private research firms vary considerably depending on how "sovereign cloud" is defined. Nevertheless, they share a common finding: investment is shifting from "where data is stored" toward "operational autonomy." In other words, the expansion of the sovereign cloud market shows that countries worldwide are building the foundations for extending their sovereignty over cloud infrastructure used to store and process data.

Three factors appear to underlie this market expansion. First, government procurement incorporating sovereignty assessment creates policy-driven demand, as exemplified by the EU Cloud Sovereignty Framework (the SEAL system; see Chapter 3). Second, tighter national and regional regulation, including the NIS2 Directive, which sets cybersecurity obligations for critical sectors, and DORA, the EU Digital Operational Resilience Act governing ICT risk management in the financial sector, is driving demand in finance, healthcare, and energy. Third, growing awareness of risks associated with the extraterritorial application of laws such as the U.S. CLOUD Act (Clarifying Lawful Overseas Use of Data Act) has created a need for measures that go beyond domestic data storage.

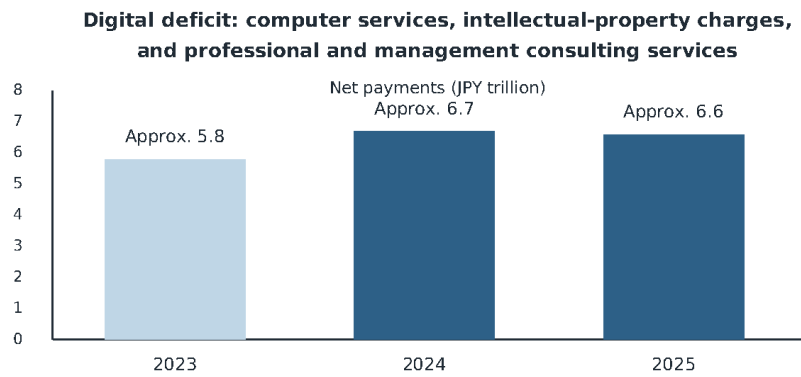
1.2.3 Japan's Structural Challenges

Japan faces several structural challenges concerning digital sovereignty. First, clarification of the concept of digital sovereignty has lagged behind other countries. Second, in the shared government cloud infrastructure (Government Cloud), 2,729 of the 2,808 systems used by national and local governments - approximately 97% - were using AWS as of the end of March 2025. At the municipal level, 823 of the 862 municipalities using Government Cloud (95.5%) had adopted AWS (Figure 1-1), demonstrating continued heavy dependence on a particular overseas provider. Even at the end of March 2026, approximately 85% of national government information systems were running on AWS [Note 5]. Third, Japan's so-called "digital deficit" - the combined balance for computer services, charges for the use of intellectual property, and professional and management consulting services - reached approximately JPY 6.7 trillion in 2024 (approximately JPY 6.8 trillion across five categories when telecommunications and information services are included). It remained high at approximately JPY 6.6 trillion in 2025 (Figure 1-2) [Note 6]. A study team at the Ministry of Economy, Trade and Industry estimates that, in a pessimistic scenario, it could expand to approximately JPY 28 trillion annually by 2035 [Note 7]. Capital outflows in the digital economy thus exhibit structural lock-in rather than a temporary phenomenon.



Source: Digital Agency figures reported by ITmedia NEWS (May 8, 2025).

Figure 1-1. Government Cloud usage by cloud provider



Source: MIC White Papers 2025 and 2026, based on Ministry of Finance balance-of-payments statistics.
2023 derived from the 2025 White Paper: JPY 6.7 trillion in 2024, up JPY 0.9 trillion year on year.

Figure 1-2. Trends in the digital deficit

1.3 The Questions Addressed in This Report

Against this background, this report examines the following questions. What is digital sovereignty? How does it relate to the traditional concept of sovereignty? How do different countries and regions interpret the concept, and what policies have they adopted? What gaps exist in Japan's institutions, and how should they be addressed? Finally, what does it mean to earn public trust beyond technical capability, and how can this be implemented institutionally? The report proceeds by examining these five questions.

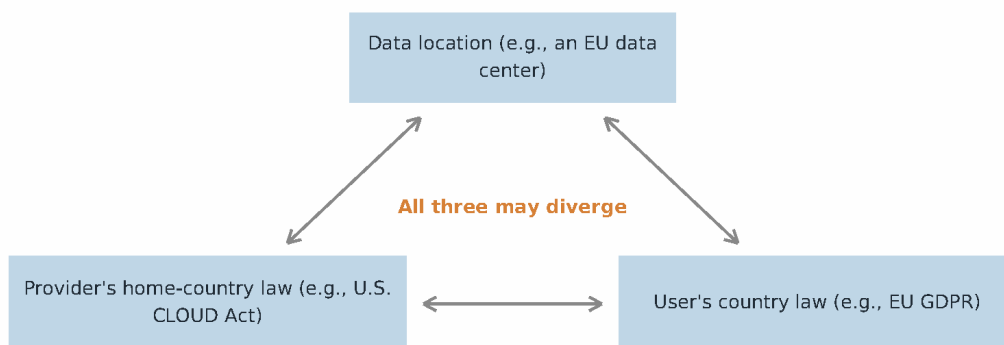
Chapter 2. The Origins and Transformation of Sovereignty: Its Extension into the Digital Space

2.1 The Traditional Concept of Sovereignty

Sovereignty is one of the most fundamental and contested concepts in law and political science. Since the Westphalian system of 1648, it has been understood as power that is "supreme" within a territory and "independent" in relations with actors outside it. Modern sovereignty is also said to encompass both power itself and authority underpinning the legitimacy of its exercise [Note 8]. This traditional understanding, however, still assumes that territory and jurisdiction coincide. It rests on the principle that a state exercises exclusive legal authority within its territory and that other states respect that authority. This report does not enter into constitutional debates on sovereignty; the following discussion provides only an operational account for policy analysis.

2.2 The "Threefold Mismatch" of Sovereignty in the Digital Space

The equation "territory = jurisdiction," assumed by traditional sovereignty, often does not hold in the digital space. The location of data, the law of the service provider's home country, and the law of the user's country may all diverge, creating a "threefold jurisdictional mismatch" (Figure 2-1).



The equation "territory = jurisdiction" often does not hold in the digital space.

Figure 2-1. The threefold jurisdictional mismatch

A typical example of competing jurisdictions is the conflict between the U.S. CLOUD Act and the EU General Data Protection Regulation (GDPR). Enacted in 2018, the CLOUD Act uses the "nationality of the entity controlling the data," rather than the "storage location," as its criterion. Data controlled by U.S. companies may therefore be subject to disclosure requests even when stored abroad. By contrast, Article 48 GDPR generally does not permit transfers of personal data based on decisions of courts or administrative authorities in third countries unless they are based on an international agreement [Note 9]. This conflict between laws symbolically illustrates competing sovereignties in the digital space.

In June 2025, a Microsoft executive testified under oath at a French Senate hearing that even if data were stored in a data center within the EU, the company might be unable to refuse disclosure in response to a legal request from U.S. authorities [Note 10]. This clearly demonstrates that data localization alone cannot secure control over data. From the perspective of Japanese law, the cross-border transfer rules under the Act on the Protection of Personal Information and rules under the Telecommunications Business Act provide domestic response frameworks, but do not resolve the jurisdictional mismatch itself. A detailed analysis from the perspective of Japanese law is reserved for the updated edition.

2.3 Multiple Layers of Sovereign Actors: States, Businesses, and Individuals

Chapter 1 outlined moves by states to assert sovereignty in the digital space. Yet sovereign actors in that space are not limited to states. Platform companies, for example, exercise sovereign power as de facto "rulers," creating a distinctively modern tension in which state and corporate sovereignty directly collide. COVID-19 contact-tracing apps provide a typical example. Government public-health apps effectively had to follow the technical specifications of the exposure notification APIs provided by Apple and Google, including Japan's contact-tracing app. This revealed a structure in which national policy design was constrained by technical conditions set by private companies. The issue also concerns relationships with individuals: social media providers' decisions to suspend accounts or remove content, and app store operators' decisions on whether apps can be distributed, may function as exercises of power that effectively determine the possibilities for speech and business, even though the decision-makers are private actors. Specifically, technological means supplied by companies, including control of cloud infrastructure, API access, and encryption keys, function as substantive enforcement tools in place of military or police power. This means that technology companies may effectively substitute for the exercise of coercive power traditionally undertaken by the state [Note 11].

This issue is related to constitutional debates on the horizontal effect of fundamental rights and public-administration debates on regulatory governance. Existing legal frameworks do not adequately capture the reality that platform companies, as de facto administrators of spaces for expression, wield influence comparable to that of public regulatory authorities. Discussion must therefore encompass private actors in the digital space and the relationships among multiple actors: states, businesses, and individuals.

2.4 Academic Debates on the Definition of Digital Sovereignty

It is useful here to briefly consider recent academic debates on digital sovereignty.

Pohle and Thiel (2020) observe that digital sovereignty functions less as a legal or organizational concept than as a "discursive practice" in politics and policy. It can thus be described as a concept with "strategic ambiguity," allowing countries and other actors to interpret it in ways suited to their own policy objectives [Note 12].

Floridi (2020) argues that digital sovereignty concerns everyone, rather than only experts and politicians, and calls for a "hybrid system of control" combining full democratic legitimacy with innovative flexibility. Pohle (2025) also critically examines the origins, objectives, and practices of digital sovereignty [Note 13].

In light of these discussions, this report deliberately defines digital sovereignty as "the ability of individuals, businesses, and states to autonomously control their own data and systems in the digital space." Recognizing the multiple meanings identified in the literature, this definition is distinctive in two respects: (1) it treats actors as multilayered rather than limiting them to states; and (2) it focuses on ability rather than legal status. This "ability to control" primarily concerns the power dimension of sovereignty discussed in Section 2.1. In this report, "digital space" is used broadly to encompass digital resources as a whole, including data, systems, and programs [Note 14]. The report then develops a two-layer framework by adding the dimension of social Legitimacy [Note 15] in Chapter 5 to this dimension of Capability. The two layers, however, are not parallel definitions. The definition in Section 2.4 - capability - is the starting point. The perspective in Chapter 5 - legitimacy - is a complementary dimension asking whether those possessing that capability can earn and maintain public trust (see Section 5.1). The scope of the study should also be made explicit. Among the various aspects of digital sovereignty, this report focuses primarily on the sovereignty of cloud infrastructure, where the institutionalization of assessment is most advanced internationally. Extensions to AI, semiconductors, and data flows will be addressed in the updated edition following

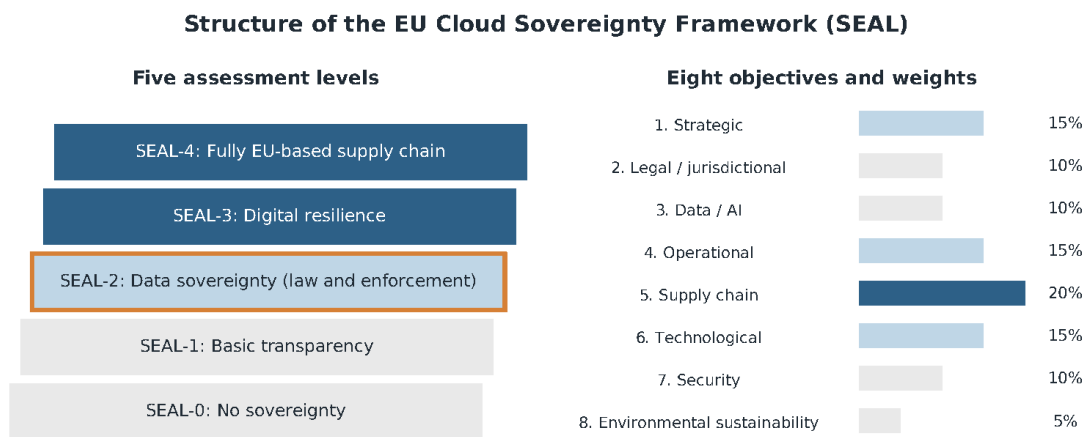
overseas research.

Chapter 3. National and Regional Digital Sovereignty Strategies: A Comparative Analysis of Four Models

3.1 The EU Model: From "Strategic Autonomy" through Regulation to "Sovereignty through Implementation"

The EU is at the forefront of institutionalizing digital sovereignty. Beginning with the GDPR, it has built a comprehensive legal system comprising the AI Act, Data Act, NIS2 Directive, and DORA [Note 16]. Digital sovereignty is the overarching concept connecting these individual laws. The EU has developed the Cloud Sovereignty Framework as one methodology for assessing it quantitatively.

SEAL (Sovereignty Effectiveness Assurance Level) is a five-level assessment scale that objectively evaluates the sovereignty of cloud services, from SEAL-0 (no sovereignty) to SEAL-4 (a fully EU-based supply chain from chips to software). Assessment is based on eight sovereignty objectives, with supply-chain sovereignty receiving the greatest weight, at 20% [Note 17]. These weights allocate points in the overall assessment and indicate what the EU prioritizes in judging sovereignty, particularly supply-chain autonomy (Figure 3-1).



Orange outline: minimum eligibility level in the April 2026 EU procurement.

Source: European Commission, Cloud Sovereignty Framework, Version 1.2.1 (October 2025).

Figure 3-1. Structure of the EU Cloud Sovereignty Framework (SEAL)

On April 17, 2026, the European Commission concluded its first procurement contracts using this framework with four European consortia. Three providers developing their own technologies - Post Telecom (Luxembourg, working with France's CleverCloud and OVHcloud), STACKIT (Germany), and Scaleway (France) - obtained SEAL-3 (digital resilience). By contrast, the Proximus (Belgium) consortium, which includes S3NS, a joint venture between France's Thales and the U.S. Google Cloud, remained at SEAL-2 (data sovereignty), the minimum level for procurement eligibility [Note 1]. This demonstrated that arrangements relying on non-EU technology can meet minimum sovereignty requirements. CISPE, the association of European cloud infrastructure providers, nevertheless criticized the outcome as "sovereignty washing": allowing services to appear sovereign through certification without substantive sovereignty. The debate continues.

On June 3, 2026, the European Commission published the proposed Cloud and AI Development Act (CADA) as the core of its Tech Sovereignty Package. Addressing two vulnerabilities - insufficient EU data-center capacity and dependence on non-EU cloud providers - the proposal uses four "Union assurance levels" to progressively link compliance with security, resilience, and sovereignty requirements to eligibility for use in the public sector, including EU institutions and national and local public authorities in Member States. Rather than excluding non-EU providers, the proposed CADA allows participation through public-

procurement requirements subject to risk-based assessment. It also introduces a mechanism for considering "EU added value," meaning technological and economic contributions within the EU, as a non-price procurement criterion. This shows that SEAL is moving beyond a one-off procurement experiment and becoming connected to the EU legislative agenda. The proposal remains at the proposal stage and will undergo deliberation in the European Parliament and Council [Note 18].

The EU's recent approach is not confined to strengthening regulation. While shifting toward regulatory simplification, exemplified by the Digital Omnibus published in November 2025, it is strengthening industrial and procurement policies such as CADA. This can be understood as a shift from "sovereignty through regulation" to "sovereignty through implementation," an important context for considering Japan's institutional design below. In other words, the direction is toward securing sovereignty through everyday procurement, certification, and operations, rather than merely declaring it in regulatory provisions.

3.2 The U.S. Model: "De Facto Sovereignty" through Technological Dominance and Extraterritorial Law

The United States does not use the term "digital sovereignty" in policy, but exercises it de facto through the CLOUD Act, Section 702 FISA, and technology controls imposed through executive orders. These legal frameworks support the U.S. government's extraterritorial exercise of authority; they do not guarantee the autonomous control of individuals and businesses described in Section 2.4. The United States has also established mechanisms for data disclosure that respect partner countries' judicial procedures through executive agreements with "trusted allies," termed "qualifying foreign governments" in the legislation. Japan has not yet concluded such an agreement, making this a policy issue.

3.3 The Chinese Model: State-Controlled "Cyber Sovereignty"

Under the banner of "cyber sovereignty," China has established a three-law system comprising the Cybersecurity Law, Data Security Law, and Personal Information Protection Law, restricting overseas data transfers and requiring domestic storage. In October 2025, the first comprehensive revision of the Cybersecurity Law since its entry into force in 2017 was adopted, effective January 1, 2026. Alongside substantially increased legal liability and expanded extraterritorial application, it introduced an AI provision covering support for AI development and oversight of safety management and ethical standards [Note 3]. China's approach can be characterized as building a distinct, vertically integrated ecosystem and prioritizing domestic control over international interoperability.

3.4 Japan's DFFT Model: "Coexistence Based on Trust"

As its name indicates, Data Free Flow with Trust (DFFT) embodies the concept of "free flows of data based on trust." It was proposed by then Prime Minister Abe at the Davos meeting in January 2019 and gained support at the G20 Osaka Summit. At the 2023 G7 meeting in Takasaki, Gunma, the Institutional Arrangement for Partnership (IAP) was launched by agreement among the G7 countries, and its secretariat was established at the OECD.

DFFT is a countervailing concept that seeks to ensure free data flows on the condition of trust, relativizing sovereignty in response to countries' moves to strengthen it. DFFT aims at coexistence mediated by trust; it does not itself seek to secure each country's autonomy. In this sense, it stands in tension with digital sovereignty, which centers on ensuring autonomy. Yet if national sovereignty continues to strengthen without an implementation framework for measuring and verifying trust, the DFFT principle itself may become hollow. In this sense, tools for measuring trust - sovereignty assessment - are a condition for DFFT's viability rather than its opposite. Since the establishment of the IAP, this implementation framework has

not been concretely developed, and DFFT remains driven by principles. Now that the EU has established a methodology for quantitatively assessing trust through SEAL and is extending it into the legislative agenda through the proposed CADA, Japan risks a paradox: despite originating DFFT, it may be unable to participate in shaping standards unless it develops mechanisms for concretely defining and assessing its "trust." This is the starting point for the discussion of Japan's institutional challenges and assessment frameworks in the following chapters.

3.5 Comparison and Classification

Table 3-1 organizes the four approaches discussed in this chapter in terms of their basic principles, sovereign actors, means of implementation, and challenges. The comparison highlights differences in the degree of institutionalization. The EU has entered the stage of "sovereignty through implementation" using assessment and procurement. The United States exercises de facto sovereignty through the extraterritorial application of its laws, and China has established a closed system based on state control. Japan, by contrast, advocates the international principle of DFFT but lacks an implementation framework for measuring and verifying its "trust." It therefore has the largest distance between principle and implementation. The next chapter examines the current institutional conditions in Japan that have produced this distance.

Table 3-1. Comparison of four models (compiled by KDDI Research) [Note 19]

	EU	United States	China	Japan (DFFT)
Basic principle	Strategic autonomy	Technological dominance and security	State-controlled cyber sovereignty	Coexistence based on trust
Regulatory intensity	High: comprehensive laws; recent shift to simplification and industrial policy	Medium: primarily extraterritorial law	Highest: state control	Medium: general laws in place; no sovereignty assessment framework
Sovereignty assessment	SEAL: five quantitative levels; proposed CADA extends to public procurement	None (self-reporting)	None (state review)	None (ISMAP limited to security)
Challenges	Balance reduced regulatory burdens with innovation	Conflict with other countries' digital sovereignty	Lack of international interoperability	Develop a concrete implementation framework

Chapter 4. Japan Today: Institutional Gaps and the "Sovereignty Gap"

4.1 A Systematic Overview of Japan's Relevant Legal and Institutional Frameworks

4.1.1 Economic Security Promotion Act

The Economic Security Promotion Act, which entered into force in 2022, comprises four pillars: stable supply of critical products, security of core infrastructure, support for advanced technology development, and non-disclosure of patent applications. In December 2022, "cloud programs" were designated as specified critical products. In April 2024, pursuant to Article 9(4) of the Act, the Ministry of Economy, Trade and Industry approved subsidies totaling up to JPY 72.5 billion for five supply assurance plans to develop computing resources needed for AI development. Additional approvals have followed [Note 20]. This means that a legal foothold already exists for considering a SEAL-style sovereignty assessment system.

4.1.2 ISMAP

ISMAP assesses and registers the security of cloud services procured by the government, based on approximately 1,200 control criteria. Following public consultation, a proposal for a comprehensive revision of the ISMAP control standards was published in December 2025. As of September 2026, the revised standards, including a substantial reduction in detailed controls, are scheduled for publication and implementation around March 2027 together with the related rules. Sovereignty factors, however, including ownership structure, extraterritorial law, and supply-chain independence, fall outside the framework's scope.

4.1.3 Government Cloud

The shared government cloud infrastructure primarily aims to reduce costs and improve efficiency; sovereignty is not incorporated into its institutional design. AWS usage has reached approximately 97% on a system basis (see Section 1.2.3). The domestic service "Sakura Cloud," conditionally selected in 2023, was confirmed to satisfy all technical requirements in March 2026, becoming the first domestic service to receive full approval. As of June 2026, five services had been approved after the Digital Agency confirmed compliance with Government Cloud technical requirements: AWS, Microsoft Azure, Oracle Cloud Infrastructure, Google Cloud, and Sakura Cloud. Yet full approval of a domestic service and resolution of imbalanced actual usage are separate matters; the dependency structure itself remains unchanged [Note 21].

4.1.4 Three Laws Regulating Platforms

The Act on Improving Transparency and Fairness of Digital Platforms (Transparency Act), the Act on Promotion of Competition for Specified Smartphone Software (Smartphone Act), and the Act on Measures against Infringements of Rights, etc. Arising from the Distribution of Information by Specified Telecommunications (Information Distribution Platform Act) aim to strengthen rules governing major platform companies. Unlike the EU, however, they do not cover guarantees of users' rights to manage their own data or algorithmic accountability. In the EU, platform regulation includes arrangements that protect users' rights and thereby contribute to digital sovereignty. Japan's three laws do not incorporate such mechanisms.

4.2 Structural Analysis of the "Sovereignty Gap"

Of the eight sovereignty objectives in the EU's SEAL framework described above, strategic sovereignty (15%), legal and jurisdictional sovereignty (10%), supply-chain sovereignty (20%), technological sovereignty (15%),

and environmental sustainability (5%) - totaling 65% - are outside the assessment scope of both ISMAP and Government Cloud. These percentages are the weights in the EU SEAL assessment (see Figure 3-1) [Note 17]. This constitutes the "sovereignty gap."

Table 4-1. EU sovereignty objectives and Japanese frameworks

Explicit = explicitly assessed; Partial / indirect = indirectly or partially covered; Outside scope = not assessed. Provisional classification by KDDI Research.

Sovereignty objective (weight)	EU SEAL	ISMAP	Government Cloud
1. Strategic sovereignty (15%)	Explicit	Outside scope	Outside scope
2. Legal / jurisdictional sovereignty (10%)	Explicit	Outside scope	Outside scope
3. Data / AI sovereignty (10%)	Explicit	Partial / indirect	Partial / indirect
4. Operational sovereignty (15%)	Explicit	Partial / indirect	Partial / indirect
5. Supply-chain sovereignty (20%)	Explicit	Outside scope	Outside scope
6. Technological sovereignty (15%)	Explicit	Outside scope	Outside scope
7. Security sovereignty (10%)	Explicit	Explicit	Explicit
8. Environmental sustainability (5%)	Explicit	Outside scope	Outside scope

The correspondences in Table 4-1 are this report's provisional classification. Detailed, provision-by-provision comparison with ISMAP control standards and Government Cloud technical requirements remains a task for future consideration in an open forum involving industry, academia, and government (see Section 6.6).

This gap produces a "paradoxical reversal." An arrangement that remained at SEAL-2, the lowest level among the four successful bids in the EU's first SEAL procurement - the consortium including S3NS, which relies on Google technology - could instead demonstrate the highest degree of compliance with Japan's Government Cloud criteria because of its extensive managed services. The EU procurement results show that even when an entity and its data centers are located within the EU, it cannot obtain a higher sovereignty rating so long as its technology stack depends on a non-EU hyperscaler. This contrast makes clear the consequences of Japan's emphasis on security and efficiency without a framework for systematically assessing supply-chain autonomy or risks from extraterritorial law.

4.3 Policy Implications

The policy implications of this analysis - adding a sovereignty assessment layer to ISMAP, considering a Japanese sovereignty assessment framework (J-SEAL) with compatibility with EU SEAL in mind, and international mutual recognition of sovereignty assessments in the context of promoting DFFT - are discussed in detail in Chapter 6.

Chapter 5. Digital Sovereignty and Public Trust: The Two Axes of Capability and Legitimacy

5.1 The Academic Origins of the Social License to Operate (SLO)

For digital sovereignty to have substance, providers to whom data and systems can be entrusted must exist, and users must have choices. This chapter draws on the Social License to Operate (SLO) as a concept for capturing the trust involved in that entrustment. SLO does not replace the definition of digital sovereignty in Section 2.4. Starting from the consideration of digital sovereignty in Japan, the first stage is to establish a sovereignty assessment framework (Chapter 6) and secure multiple domestic options: the issue of digital sovereignty. The subsequent, second-stage question is whether the providers of those options can earn and maintain public trust. The SLO perspective discussed here is conceptual preparation for that second stage.

SLO developed in the extractive industries in the 1990s and refers to "acceptance of an organization's practices by multiple stakeholders." It is not a legal license or authorization and has neither an issuing authority nor a certificate. The concept arose from mining experience: even with government permission, a business cannot continue operating reliably if it loses acceptance among affected communities and others. It is understood as something that must be maintained continuously, rather than acquired once and for all. Academic models also describe deepening acceptance through the stages of legitimacy, credibility, and trust [Note 22]. In recent years, the concept has been extended to digital technologies, with scholarly discussion of social licenses for AI and big data. Leonard (2018) discusses social license in data-driven applications and AI, while Shaw and colleagues (2020) examine it in the use of big data during the pandemic [Note 23].

SLO originally denotes acceptance that providers earn from society. Its range of actors and scope of power differ from those of traditional sovereignty. This report therefore relates SLO particularly to the authority dimension of sovereignty (see Section 2.1), using it to identify the conditions of trust that infrastructure providers supporting digital sovereignty must satisfy.

5.2 A Two-Axis Framework of Capability and Legitimacy

The central proposition of this report is to reconceptualize digital sovereignty as a comprehensive framework integrating social Legitimacy with technical Capability, rather than limiting it to the latter: the two-layer framework discussed in Section 2.4. The "ability" in that section's definition is not confined to technical matters. In the context of infrastructure providers, the following discussion uses Capability mainly to refer to the technical and organizational ability to control operations, monitoring, encryption-key management, and related functions (the terminology used in this report). These two layers broadly correspond to the two dimensions of sovereignty discussed in Chapter 2. Capability corresponds to power, but denotes the de facto ability to control data and systems rather than legal authority. Legitimacy corresponds to authority and means that society accepts the exercise of that capability. In relation to the SLO debate above, gaining social acceptance and trustworthiness is likely to be central to establishing Legitimacy or designing its framework.

Capability (technical capability): the ability to bring data under one's management and control it technically and legally. The perspective is inside-out: "What can we do?" Metaphorically, it is a high-performance safe.

Legitimacy (social legitimacy): earning the public's trust that one is "worthy of being entrusted with data." The perspective is outside-in: "What does society want?" Metaphorically, it is the trust required to hold the key to the safe.

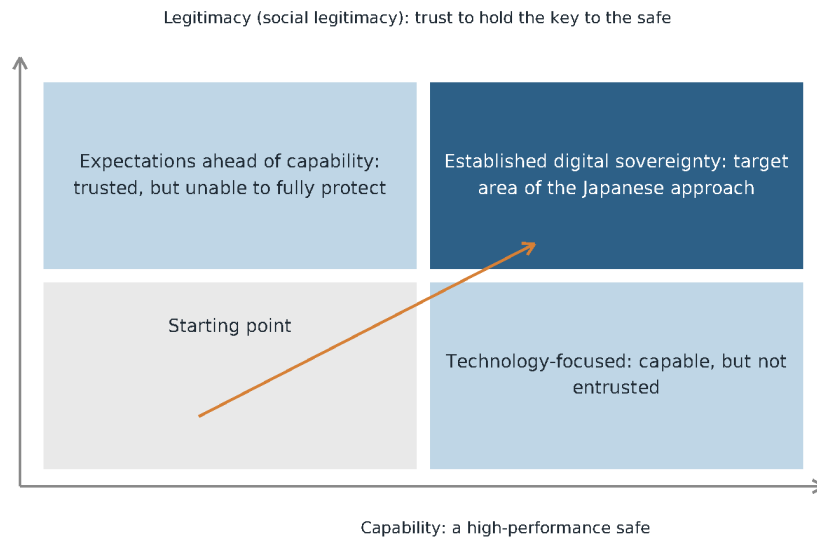


Figure 5-1. The two-axis framework of Capability and Legitimacy

This two-axis framework (Figure 5-1) provides a perspective that positions trust as an important element of competitiveness beyond regulatory compliance. Economically, cloud services have the characteristics of "credence goods": users find it difficult to verify their quality, including sovereignty, even after use. Institutional design to overcome information asymmetry - third-party assessment and certification - is therefore essential.

5.3 The Potential for a Japanese Approach

Distinctiveness in itself is not the point. While the EU framework measures sovereignty on the Capability side in detail, it has not institutionalized a mechanism for assessing whether providers have earned public trust (Legitimacy). The United States lacks a systematic assessment framework altogether. If Japan can address these shortcomings and present an institutional design assessing both capability and legitimacy, it could establish an interoperable standard that other countries can draw upon, rather than a unique model confined to Japan. Japan's record as the originator of DFFT provides an international foundation. Its ability to implement institutions rapidly as a single state is also an advantage in implementation speed. Chapter 6 discusses concrete directions.

Chapter 6. Key Findings and Policy Implications

6.1 Findings from the Discussion So Far

First, digital sovereignty is not a simple extension of traditional sovereignty. It requires a new conceptual framework consisting of two layers: Capability and Legitimacy.

Second, the EU has achieved quantitative assessment of sovereignty through SEAL and is extending it into the legislative agenda through the proposed CADA. International competition over sovereignty assessment standards has already begun. Without its own assessment framework, Japan risks remaining a recipient of standards set by others and being unable to participate in shaping them. Without such participation, Japanese providers would bear the costs of complying with other countries' standards unilaterally and lose opportunities to reflect Japan's institutional environment and users' needs in assessment criteria.

Third, Japan's institutions contain a sovereignty gap. ISMAP and Government Cloud assess security and efficiency but lack assessment criteria corresponding to 65% of the EU's sovereignty objectives.

Fourth, treating digital sovereignty as a two-layer framework encompassing the acquisition of public trust makes it possible to envision a Japanese approach that goes beyond regulatory compliance.

6.2 Japan's Options: Four Future Scenarios and the Collaborative Model

Japan's future sovereign cloud landscape will differ substantially depending on policy choices. This report presents four qualitative scenarios. The first is the "status quo": if Japan remains limited to security assessment (ISMAP) without introducing quantitative sovereignty assessment, the gap described in Chapter 4 will persist. The second is "domestic-technology-led": placing a domestic technology stack at the core would maximize technological sovereignty, but constraints may remain for the time being on the timeline for practical deployment and the breadth of available managed services. The third is "hyperscaler-led," referring to large overseas cloud providers: market expansion would be fastest, but sovereignty would depend on providers' self-reporting, and risks from extraterritorial law would remain. The fourth is the "collaborative model": domestic and overseas providers work together, for example through joint ventures, to use overseas technologies "within a sovereignty framework," while domestic actors retain control over operations, monitoring, and encryption-key management. An assessment system objectively verifies the level of sovereignty (Figure 6-1). Arrangements in which domestic actors control these functions while using overseas technologies have already been implemented, including by S3NS in France.

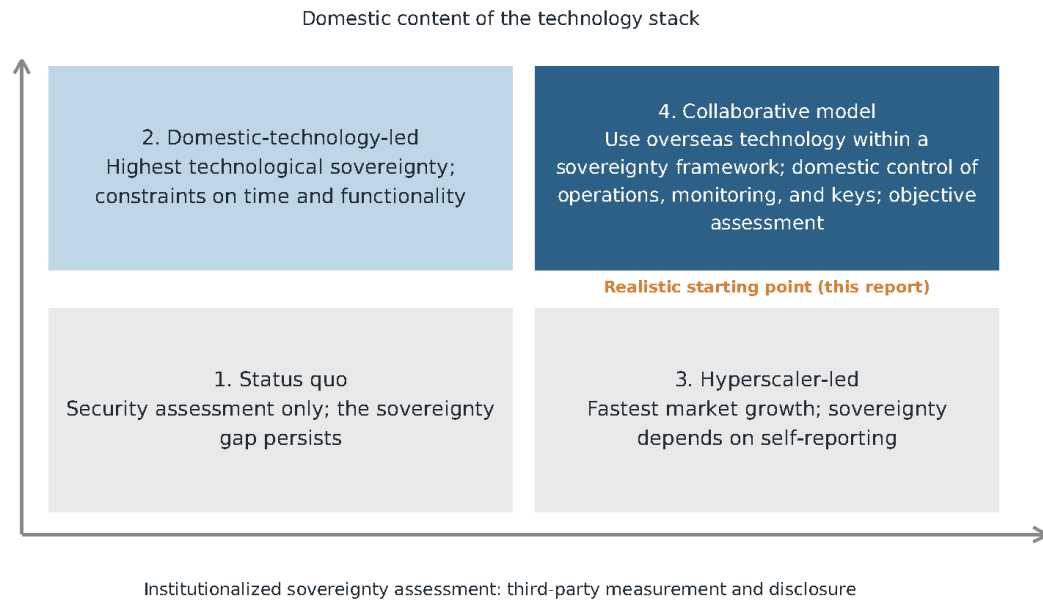


Figure 6-1. Japan's options: four future scenarios (compiled by KDDI Research)

The outcome of the EU's first SEAL procurement - a two-tier structure in which providers operating entirely with their own technologies obtained SEAL-3, while collaborative arrangements relying on hyperscaler technologies, such as France's S3NS, remained at SEAL-2 - has important implications for Japan. It made the trade-off between technological self-sufficiency and functionality visible within the institutional framework [Note 1]. Because securing sovereignty through entirely domestic technology is difficult in the short term, a realistic starting point is to permit collaborative models while requiring their sovereignty levels to be measured and disclosed through an assessment system.

The crucial point is for society to possess a yardstick for assessment, rather than leaving the choice of model entirely to the market. This means preparing objective indicators, established through transparent discussion, before a crisis occurs. Developing such a yardstick is not only the opposite of exclusion; it also helps prevent exclusion. If geopolitical tensions rise in the absence of tools for measuring sovereignty, the gap may be filled by blanket exclusion based on crude criteria such as the nationality of capital or place of origin. Preparing a graduated assessment framework in advance is the realistic route to filling the gap while maintaining an open market. The EU's first procurement, which gave arrangements relying on non-EU technologies a defined position through assessment rather than exclusion, provides an example.

6.3 Policy Recommendations

The recommendations in this section are discussed through examples of specific institutions, but implementation is not limited to a single route. Possible pathways include reviewing existing frameworks, improving procurement practices, and establishing new frameworks. The four items in this section correspond to the five recommendations in the separately published policy proposal as follows. Sections 6.3.1 and 6.3.2 correspond to Recommendation 1 (consideration of an assessment framework) and Recommendation 2 (standardization of information disclosure). Section 6.3.3 corresponds to Recommendation 5 (international interoperability). Section 6.3.4 provides supplementary consideration of the legal foundations for these measures. Recommendation 3 (ensuring switching possibilities) is based on the analysis in Chapters 1 and 4; Recommendation 4 (understanding dependency structures) is based on Section 6.4.

6.3.1 Adding a "Sovereignty Assessment Layer" to ISMAP

To fill the sovereignty gap analyzed in Chapter 4, this report recommends adding a fourth "sovereignty assessment layer" to ISMAP's three layers of control standards: governance criteria, management criteria, and control criteria. This layer should maintain compatibility with the eight sovereignty objectives of EU SEAL while incorporating assessment items suited to Japan's institutional environment. Candidates include assessments of ownership and capital relationships, risks from extraterritorial law, supply-chain sovereignty, and technological independence.

6.3.2 Phased Consideration of a Japanese Sovereignty Assessment Framework (J-SEAL)

This report recommends developing a Japanese system of sovereignty assessment levels corresponding to EU SEAL's five levels and considering its phased application to government procurement and critical infrastructure. Possible phases are institutional design, pilot application, and full operation. Numerous design issues require examination, including assessment criteria, the bodies and methods for third-party assessment, and relationships with existing frameworks such as ISMAP and Government Cloud technical requirements. This report proposes placing these issues on the agenda for open discussion among stakeholders in industry, academia, and government. Whereas EU SEAL requires consensus among 27 Member States, Japan has the structural advantage of being able to implement institutions rapidly as a single state.

6.3.3 International Development: Mutual Recognition with EU SEAL and the APEC-CSCR Concept

A Japanese sovereignty assessment framework should incorporate international interoperability from the outset, rather than remain a closed domestic system. First, it should pursue mutual recognition with EU SEAL and the Union assurance levels in the proposed CADA. Establishing a framework under which Japanese cloud providers' sovereignty is recognized in the EU market would concretely implement DFFT's "data flows based on trust" at the institutional level and should be advanced alongside international standardization proposals. Second, this report proposes the concept of APEC-CSCR (Cloud Sovereignty Cross-border Rules). This would extend the model of "interoperability of trust" achieved by APEC-CBPR, established in 2011 to mutually recognize trust through certification for cross-border transfers of personal information within APEC, to mutual certification of cloud sovereignty. What would be mutually recognized here, however, is not equivalence of security levels but the verifiability of sovereignty: the ability to confirm which country's laws apply and who controls operations, monitoring, and encryption-key management. Using equivalence of security as the criterion could merely endorse concentration among large regional providers, failing to address the concern underlying sovereignty. Within this framework, arrangements that retain each country's data domestically while allowing only trained models or the results of federated learning to cross borders could provide one technical implementation of DFFT. As the originator of DFFT, Japan has a record of leading the expansion of CBPR and therefore possesses legitimacy to exercise leadership in this field. APEC-CSCR is a proposal made by this report; no official policy proposal currently exists.

6.3.4 Broadening Implementation of the Economic Security Promotion Act

Taking advantage of the existing designation of cloud programs as specified critical products, broader implementation of the Economic Security Promotion Act should be considered as the legal foundation for a sovereignty assessment system. One possible direction is to incorporate sovereign cloud considerations into the security of core infrastructure and refer to sovereignty assessments when critical infrastructure operators procure cloud services.

6.4 A Phased Approach: Why Start with Healthcare?

It is realistic to introduce sovereignty assessment progressively, starting with highly sensitive areas of strong public concern rather than applying it uniformly across all sectors. This report proposes the sequence of healthcare, finance, and general government procurement. There are three reasons to start with healthcare. First, the design and legislation of infrastructure managed by the state, such as standardized electronic health records and platforms for sharing medical information, are currently underway. There is a "window of institutional formation": the opportunity to incorporate assessment perspectives into these frameworks is open now. Second, where the state manages the infrastructure, legal questions concerning assessment requirements are less likely to arise; this can be separated from questions of justification and practical burden when targeting individual private healthcare institutions' systems. Third, healthcare data are highly sensitive, making it the area where the public demand for trust - for providers "worthy of being entrusted with data" - is most acute. High sensitivity also creates implementation costs by increasing stakeholders' caution. Initial implementation should therefore be limited to state-managed medical information infrastructure, on the premise that individual healthcare institutions will not face new burdens. Finance is well suited to be the second area, given growing international convergence in regulation, including the application of EU DORA from January 2025.



Prerequisite: identify sector-specific cloud dependencies.

This fact-finding exercise is itself the first policy task.

Figure 6-2. Overview of the phased approach

As a prerequisite, it is essential to establish which cloud infrastructure Japan's major sectors actually depend on, particularly healthcare cloud services such as electronic health record SaaS and personal health record (PHR) platforms. Although Government Cloud usage is disclosed, no comprehensive official statistics show sector-specific dependency structures. This fact-finding survey is itself the first policy task, preceding the sovereignty assessment system.

6.5 The Role of Providers: Multiple Actors Responsible for Public Trust

Securing digital sovereignty cannot be accomplished through government institutional design alone. Domestic providers responsible for the physical infrastructure of data flows must possess both (1) technical Capability, meaning domestic control of operations, monitoring, and encryption-key management; and (2) social Legitimacy, meaning trust that they are worthy of being entrusted with data. This role should not fall to one particular company. Multiple domestic providers should share responsibilities and compete, avoiding concentration in a single provider while forming a market in which trustworthiness is an important component of competitiveness. As Chapter 5 explains, because cloud services have the characteristics of credence goods, providers' practices can receive fair market recognition only once institutions that make trust verifiable - sovereignty assessment - are in place. Institutions and practice are mutually dependent.

6.6 Activities to Begin Implementing the Recommendations

The activities needed to implement the recommendations in Section 6.3 are set out below, together with the recommendations to which they correspond. For consideration of an assessment framework (Sections 6.3.1 and 6.3.2), detailed comparison of ISMAP control standards and Government Cloud technical requirements with the EU framework should come first, followed by concrete design of assessment criteria. For the phased approach (Section 6.4), an empirical survey of sector-specific cloud dependency structures is a prerequisite. For international development (Section 6.3.3), the institutional and diplomatic feasibility of mutual recognition with EU SEAL and the APEC-CSCR concept must be examined. Quantitative estimates of Japan's sovereign cloud market size provide the background supporting this work as a whole. Overseas institutional practices and market conditions should also be verified through field research. We plan overseas research from the second half of fiscal year 2026 onward. These issues should be entrusted to continuing discussion in an open forum involving industry, academia, and government.

— End of Main Text —

Acknowledgments

In preparing this report, we received individual comments from the following experts, to whom we express our gratitude. Responsibility for the report's contents and any errors rests entirely with KDDI Research, Inc. The statements in this report do not represent the views of the individuals who provided comments.

Listed in Japanese syllabary order; honorifics omitted. Affiliations and positions are as of September 2026.

Yukiko Ito - Professor, Faculty of Business and Commerce, Keio University

Masahiro Sogabe - Professor, Graduate School of Law, Kyoto University

Ryoji Mori - Attorney, Eichi Law Offices

Akira Morita - Professor Emeritus, University of Tokyo

Kento Yamamoto - Associate Professor, Media Studies Major, Faculty of Sociology, Kansai University

Endnotes

[Note 1] European Commission, "Commission advances cloud sovereignty through strategic procurement" (April 17, 2026). Total contract value is up to EUR 180 million over six years. Procurement began in October 2025 under the Cloud III DPS, with SEAL-2 set as the minimum eligibility level. Of the four successful bids, Post Telecom (working with CleverCloud and OVHcloud), STACKIT, and Scaleway obtained SEAL-3. The Proximus consortium, including S3NS, Clarence, and Mistral, obtained SEAL-2.

[Note 2] Protecting Americans from Foreign Adversary Controlled Applications Act (enacted April 2024). The Act requires divestiture, reducing ByteDance's shareholding below 20%. Retraining the algorithm is not a statutory requirement. Rather, under the framework of the U.S. joint venture established on January 22, 2026 following a binding agreement in December 2025, a licensed copy of the recommendation algorithm is to be retrained using only U.S. user data and managed in Oracle's U.S. cloud environment. Oracle, Silver Lake, and MGX each invested 15%, among other investors. This account is based on reporting by AP and others.

[Note 3] Revision of the Cybersecurity Law of the People's Republic of China (adopted by the Standing Committee of the National People's Congress on October 28, 2025; effective January 1, 2026). This was the first comprehensive revision since the law entered into force in 2017. In addition to increased legal liability and expanded extraterritorial application, it introduced an AI provision supporting basic research and core technology development and strengthening oversight of ethical standards, safety, and risk management. See, among other sources, JETRO Beijing Office, "Key Points and Response Measures for the Cybersecurity Law (2025 Revision) and the Measures for the Administration of Reporting National Cybersecurity Incidents" (February 2026). For details of strengthened penalties and related matters, see also CISTEC, "On the Revision of China's Cybersecurity Law" (November 27, 2025), https://www.cistec.or.jp/service/keizai_anzenhosho/china/data/20251127.pdf.

[Note 4] Gartner, "Gartner Says Worldwide Sovereign Cloud IaaS Spending Will Total \$80 Billion in 2026" (press release, February 9, 2026). Worldwide spending is approximately USD 80.4 billion in 2026, up 35.6% year on year. Regional figures, in USD millions, for 2025 / 2026 / 2027 are: Europe, 6,868 / 12,587 / 23,118; North America, 12,667 / 16,394 / 21,127; Japan, 519 / 932 / 1,816. Private research firms' estimates differ substantially depending on their definition of sovereign cloud. Fortune Business Insights, for example, estimates the worldwide market at approximately USD 154.7 billion in 2025. This report uses Gartner's spending-based estimate as its reference because its definition is relatively clear.

[Note 5] Reporting based on Digital Agency figures as of the end of March 2025 (ITmedia NEWS, May 8, 2025). AWS was used by 2,729 of the 2,808 national and local government systems, approximately 97%. Oracle Cloud Infrastructure was next with 51 systems (1.8%). Among municipalities, 823 of the 862 using Government Cloud (95.5%) used AWS. As of March 31, 2026, approximately 85% of national government information systems were reported to be running on AWS, based on Digital Agency materials (ITmedia Business Online, June 17, 2026).

[Note 6] The 2024 figures are from the Ministry of Internal Affairs and Communications, Information and Communications in Japan: White Paper 2025: approximately JPY 6.7 trillion across three categories, up approximately JPY 0.9 trillion year on year, or approximately JPY 6.8 trillion across five categories. The 2025 figures are from the Ministry's White Paper 2026: a deficit of approximately JPY 6.6 trillion across three categories, down approximately JPY 0.1 trillion year on year. These figures are based on Ministry of Finance balance-of-payments statistics. Although growth of the deficit appears to have paused, a deficit in the mid-JPY 6 trillion range has become entrenched.

[Note 7] Ministry of Economy, Trade and Industry, Minister's Secretariat, Young Officials' New Policy Project (PIVOT), Digital Economy Report: A World Engulfed by Data - Survival Strategies in a Digital Market without Sanctuaries (published April 30, 2025). Under a pessimistic scenario taking the AI revolution into account, the report estimates that total net payments originating from software and data could reach a maximum of JPY 45.3 trillion in 2035. This includes the "hidden digital deficit" from embedded software and related areas, as well as net payments on the trade-balance side associated with SDX (Software Defined Everything).

[Note 8] Sovereignty is generally said to have three meanings: (1) governing power; (2) the supreme and independent character of state power; and (3) the highest decision-making authority over affairs of state. As the source of power shifted from monarchs to the people following the French Revolution, sovereignty came to be understood as consisting of the dimensions of power and authority. In democratic societies in particular, obedience to state law is justified because the source of power, including legislative power, derives from the people as sovereign. For detailed doctrinal discussion, see Nobuyoshi Ashibe, supplemented and revised by Kazuyuki Takahashi, *Constitutional Law*, 8th ed. (Iwanami Shoten, 2023), pp. 39 ff.; Koji Sato, *A Treatise on the Constitution of Japan* (Seibundo, 2020), pp. 425 ff.; and Shigenori Matsui, *The Constitution of Japan*, 4th ed. (Yuhikaku, 2022), pp. 118 ff.

[Note 9] CLOUD Act, H.R.4943 (2018); Article 48 GDPR. For details, see Nishimura Institute of Advanced Legal Studies, CLOUD Act Study Group Report.

[Note 10] Hearing of the French Senate inquiry committee on "Public Procurement and Digital Sovereignty" (June 10, 2025).

Asked whether he could guarantee that French citizens' data would not be transferred to U.S. authorities without the express approval of French authorities, Microsoft France's Director of Public and Legal Affairs, Anton Carniaux, testified under oath: "No, I cannot guarantee it" ("Non, je ne peux pas le garantir"). See the committee's minutes for June 9-10, 2025 on the French Senate website (senat.fr).

[Note 11] In constitutional debates on relations between states and platform companies, Professor Tatsuhiko Yamamoto observes that a "new monster" - platform companies - has emerged alongside the "traditional monster" of the powerful state. At present, only the state can counter this power, leaving societies compelled to pit the old and new monsters against one another to protect freedom and democracy. See Tatsuhiko Yamamoto, "Can We Create a Mechanism to Counter the 'Monster' of the Attention Economy?", Stella net (NHK Foundation), September 13, 2024, <https://www.steranet.jp/articles/-/3519>.

[Note 12] Pohle, J. & Thiel, T. (2020). Digital sovereignty. *Internet Policy Review*, 9(4). <https://doi.org/10.14763/2020.4.1532> (CC BY 3.0 DE).

[Note 13] Floridi, L. (2020). The Fight for Digital Sovereignty. *Philosophy & Technology*, 33(3), 369-378. / Pohle, J. (2025). Unthinking Digital Sovereignty: A Critical Reflection on Origins, Objectives, and Practices. *Policy & Internet*, 16(4), 666-671 (published May 16, 2025). <https://doi.org/10.1002/poi3.437>. / For recent comprehensive studies of digital sovereignty, see also Chander, A. & Sun, H. (eds.), *Data Sovereignty: From the Digital Silk Road to the Return of the State* (Oxford University Press, 2023), and Bradford, A., *Digital Empires: The Global Battle to Regulate Technology* (Oxford University Press, 2023). The review of academic perspectives will be expanded in the updated edition.

[Note 14] Examples of related concepts in government documents. The Basic Policy on Economic and Fiscal Management and Reform 2026, approved by the Cabinet on July 21, 2026, explicitly calls for "developing AI and data infrastructure while establishing open AI sovereignty" (Chapter 2, 1(2)) and "strengthening the resilience and improving the autonomy of the government's digital infrastructure" (same section). In the economic security context, it states that "necessary measures will be taken to ensure the security and other relevant aspects of data centers and cloud services" (Chapter 2, 2(2)). This report's definition and analysis connect with these policy contexts.

[Note 15] In organizational theory and related fields, "legitimacy" is sometimes rendered in Japanese as 正当性 (seitosei, connoting justification or rightfulness). This report uses 正統性 (seitosei, connoting legitimacy acquired through procedure) to convey acceptance acquired through procedures.

[Note 16] The EU legislation cited in Section 3.1 can be summarized as follows. GDPR (General Data Protection Regulation): general legislation protecting personal data. AI Act (AI Regulation): a regulation governing AI systems on a risk basis. Data Act (Data Regulation): a regulation governing access to and sharing of IoT and other data, and switching between cloud services. NIS2 Directive: a directive imposing cybersecurity obligations across a broad range of critical sectors, including energy and healthcare. DORA: a regulation governing ICT risk management in the financial sector.

[Note 17] European Commission, Cloud Sovereignty Framework, Version 1.2.1 (October 20, 2025). The framework comprises eight sovereignty objectives (SOV-1 to SOV-8) and 48 assessment criteria, with five levels from SEAL-0 to SEAL-4. Weights are: SOV-1 strategic sovereignty, 15%; SOV-2 legal and jurisdictional sovereignty, 10%; SOV-3 data and AI sovereignty, 10%; SOV-4 operational sovereignty, 15%; SOV-5 supply-chain sovereignty, 20% (the largest); SOV-6 technological sovereignty, 15%; SOV-7 security and compliance sovereignty, 10%; and SOV-8 environmental sustainability, 5%. The 65% in Section 4.2 is the sum of the weights for SOV-1, 2, 5, 6, and 8, classified as outside the scope of ISMAP and related frameworks.

[Note 18] European Commission, Proposal for the Cloud and AI Development Act (CADA), COM(2026) 502 (June 3, 2026). In addition to CADA, the Tech Sovereignty Package comprises the Chips Act 2.0, the EU open-source strategy, and other measures. The proposed CADA requires consideration of "EU added value" as a supplementary non-price criterion in public procurement, interpreted as a weight of up to 15 points out of 120.

[Note 19] The term "model" used for countries and regions in this report is a convenient label denoting types of approach.

[Note 20] Ministry of Economy, Trade and Industry news release, "Approval of Supply Assurance Plans for Ensuring the Stable Supply of Cloud Programs under the Economic Security Promotion Act" (April 19, 2024). Subsequent approvals include Sakura Internet's second investment plan, worth approximately JPY 100 billion.

[Note 21] Digital Agency, "Government Cloud" website. Regarding Sakura Cloud, the Agency announced: "As we have confirmed that all technical requirements have been met, production environments can be provided from March 27, 2026 onward." For the current status of the five approved services, see ITmedia Business Online (June 17, 2026).

[Note 22] On the origins and theoretical development of SLO. The term is said to have begun to be used in the mining industry in 1997. For a retrospective by its originator, see Cooney, J. (2017). Reflections on the 20th anniversary of the term 'social licence'. *Journal of Energy & Natural Resources Law*, 35(2), 197-200. For an examination of the concept's origins in the mining sector, see Prno, J. & Slocombe, D. S. (2012). Exploring the origins of 'social license to operate' in the mining sector: Perspectives from governance and sustainability theories. *Resources Policy*, 37(3), 346-357. For an empirical analysis of social license as a constraint on corporate conduct separate from legal authorization, see Gunningham, N., Kagan, R. A., & Thornton,

D. (2004). Social license and environmental protection: Why businesses go beyond compliance. *Law & Social Inquiry*, 29(2), 307-341. The staged model of legitimacy, credibility, and trust is from Boutilier, R. G., & Thomson, I. (2011). The Social License to Operate. *Society for Mining, Metallurgy and Exploration*.

[Note 23] Leonard, P.G. (2018). Social Licence and Digital Trust in Data-Driven Applications and AI. SSRN. / Shaw, J. et al. (2020). Social license for the use of big data in the COVID-19 era. *npj Digital Medicine*, 3, 128. / Verhulst, S.G. (2023). Social License for Data. *Stanford Social Innovation Review*.

References

Foreign-Language Literature

- Boutillier, R. G., & Thomson, I. (2011). The Social License to Operate. Society for Mining, Metallurgy and Exploration.
- Bradford, A. (2023). Digital Empires: The Global Battle to Regulate Technology. Oxford University Press.
- Chander, A. & Sun, H. (eds.) (2023). Data Sovereignty: From the Digital Silk Road to the Return of the State. Oxford University Press.
- Cooney, J. (2017). Reflections on the 20th anniversary of the term 'social licence'. Journal of Energy & Natural Resources Law, 35(2), 197-200.
- Couture, S. & Toupin, S. (2019). What Does the Notion of 'Sovereignty' Mean When Referring to the Digital? New Media & Society, 21(10), 2305-2322.
- Floridi, L. (2020). The Fight for Digital Sovereignty. Philosophy & Technology, 33(3), 369-378.
- Gunningham, N., Kagan, R. A., & Thornton, D. (2004). Social license and environmental protection: Why businesses go beyond compliance. Law & Social Inquiry, 29(2), 307-341.
- Leonard, P.G. (2018). Social Licence and Digital Trust in Data-Driven Applications and AI. SSRN.
- Pohle, J. & Thiel, T. (2020). Digital sovereignty. Internet Policy Review, 9(4).
- Pohle, J. (2025). Unthinking Digital Sovereignty: A Critical Reflection on Origins, Objectives, and Practices. Policy & Internet, 16(4), 666-671.
- Prno, J. & Slocombe, D. S. (2012). Exploring the origins of 'social license to operate' in the mining sector: Perspectives from governance and sustainability theories. Resources Policy, 37(3), 346-357.
- Roberts, H. et al. (2021). Safeguarding European Values With Digital Sovereignty. Internet Policy Review, 10(3).
- Shaw, J. et al. (2020). Social license for the use of big data in the COVID-19 era. npj Digital Medicine, 3, 128.

Japanese-Language Literature

- Ashibe, Nobuyoshi (supplemented and revised by Kazuyuki Takahashi). Constitutional Law, 8th ed. Iwanami Shoten, 2023.
- Sato, Koji. A Treatise on the Constitution of Japan, 2nd ed. Seibundo, 2020.
- Matsui, Shigenori. The Constitution of Japan, 4th ed. Yuhikaku, 2022.
- Yamamoto, Tatsuhiko. "Can We Create a Mechanism to Counter the 'Monster' of the Attention Economy? An Interview with Professor Tatsuhiko Yamamoto of Keio University (Constitutional Law)." Stella net (NHK Foundation), September 13, 2024. <https://www.steranet.jp/articles/-/3519>.

Policy and Institutional Documents

- European Commission (2025). Cloud Sovereignty Framework.
- European Commission (2026). Commission advances cloud sovereignty through strategic procurement. April 17, 2026.
- European Commission (2026). Proposal for the Cloud and AI Development Act (CADA), COM(2026) 502. June 3, 2026.
- U.S. Congress (2018). Clarifying Lawful Overseas Use of Data Act (CLOUD Act). H.R.4943.
- U.S. Congress (2024). Protecting Americans from Foreign Adversary Controlled Applications Act.
- Standing Committee of the National People's Congress (2025). Cybersecurity Law of the People's Republic of China (2025 revision; effective January 1, 2026).
- JETRO Beijing Office (2026). Key Points and Response Measures for the Cybersecurity Law (2025 Revision) and the

Measures for the Administration of Reporting National Cybersecurity Incidents. February 2026.

Ministry of Economy, Trade and Industry (2024). Approval of Supply Assurance Plans for Ensuring the Stable Supply of Cloud Programs under the Economic Security Promotion Act. April 19, 2024.

Digital Agency. DFFT. <https://www.digital.go.jp/policies/dfft>

Digital Agency. Government Cloud. https://www.digital.go.jp/policies/gov_cloud

Cabinet Office. Economic Security. https://www.cao.go.jp/keizai_anzen_hosho/

Ministry of Internal Affairs and Communications (2025). Information and Communications in Japan: White Paper 2025. <https://www.soumu.go.jp/johotsusintokei/whitepaper/r07.html>

Nishimura Institute of Advanced Legal Studies. CLOUD Act Study Group Report.
https://www.nishimura.com/sites/default/files/images/13700_1.pdf