

デジタル主権に関する調査報告書

— 概念・制度・国際比較・社会からの信頼、そして政策への示唆 —

2026 年 9 月（初版）

株式会社 KDDI 総合研究所

シンクタンク部門 公共政策グループ

エグゼクティブサマリー

本報告書は、「デジタル主権とは何か」「日本として求められる立ち位置とは何か」という問いに対し、概念・制度の国際比較を通じて答えることを目的とする。その背景には、日本におけるデジタル基盤の構造的な課題がある。政府調達をはじめとする現行制度は、クラウドのセキュリティを評価しても、その主権性——どの国の法が及び、誰が運用と暗号鍵を掌握しているか——を評価する物差しを持っていない。

本報告書は、デジタル主権を「デジタル空間において、個人・企業・国家が自らのデータやシステムを自律的にコントロールできる能力」と操作的に定義する。デジタル主権の国際比較からは、EU が、評価・調達を通じた「実装による主権」へ重心を移していることが確認された。EU クラウド主権フレームワーク（SEAL）は主権性を 5 段階・8 つの主権目的で定量評価し、2026 年 4 月には初の政府調達に適用され、さらにクラウド・AI 開発法（CADA）案によって立法アジェンダへと展開されつつある。米国は法制度の域外適用を通じて事実上の主権を行使し、中国は国家統制型の閉鎖モデルを構築している。日本は DFFT（信頼性のある自由なデータ流通）を掲げるが、「信頼」を測定・検証する実装枠組みを欠けばその理念自体が空洞化する。

日本の制度を検証すると、ISMAP はセキュリティ評価に、経済安全保障推進法のクラウドプログラムは製造供給能力の確保にそれぞれ特化しており、EU の評価枠組みが対象とする主権目的の 65%に相当する領域——戦略的主権、法的・管轄権的主権、サプライチェーン主権、技術的主権等——を評価する制度が存在しない。本報告書はこれを「主権の空白」と呼ぶ。この空白を埋める枠組みとして、能力（Capability）と社会的正統性（Legitimacy）の二軸を提示した。主権評価によって国内に複数の選択肢を確保することが第一段階であり、その担い手が社会からの信頼を獲得・維持できるかが、これに続く第二段階の問いである。信頼の測定軸として Social License to Operate（SLO）を用いた日本型アプローチを提案した。

将来像として、現状維持、国内技術主導、ハイパースケーラー主導、協調モデルの 4 つのシナリオを比較し、協調モデルを、現実的な出発点として提示した。政策の方向性として、主権評価枠組みの検討、情報開示の共通化、国際相互運用性の確保等を論じており、その具体的な行動は、別冊の政策提言（5 提言）として取りまとめた。

本報告書は、公開情報の調査と国内関係者へのヒアリングに基づく初版である。2026 年度下期以降に予定する海外調査の結果を踏まえ、2027 年 3 月に更新版を公表する予定である。

目次

エグゼクティブサマリー	2
第1章 なぜ今「デジタル主権」か——問題の所在	5
1.1 本報告書の目的と背景	5
1.2 構造的変化：3つの潮流の収斂	5
1.2.1 地政学リスクの顕在化	5
1.2.2 ソブリンクラウド市場の急成長	6
1.2.3 日本の構造的課題	6
1.3 本報告書の問い	8
第2章 「主権」概念の系譜と変容——デジタル空間への拡張	9
2.1 伝統的主権概念の整理	9
2.2 デジタル空間における主権の「三重のずれ」	9
2.3 主権「主体」の多層化——国家・企業・個人	10
2.4 「デジタル主権」の定義をめぐる学術的議論	11
第3章 各国・地域のデジタル主権戦略——4つのモデルの比較分析	12
3.1 EUモデル：規制を通じた「戦略的自律性」から「実装による主権」へ	12
3.2 米国モデル：技術覇権と域外法による「事実上の主権」	13
3.3 中国モデル：国家統制型「サイバー主権」	14
3.4 日本の DFPT モデル：「信頼に基づく共存」	14
3.5 比較と類型化	15
第4章 日本の現状——制度的ギャップと「主権の空白」	16
4.1 日本の関連法制度の体系的整理	16
4.1.1 経済安全保障推進法	16
4.1.2 ISMAP	16
4.1.3 ガバメントクラウド	16
4.1.4 プラットフォーム規制三法	16
4.2 「主権の空白」の構造分析	17
4.3 政策的含意	18
第5章 デジタル主権と社会からの信頼——能力と正統性の二軸	19
5.1 Social License to Operate (SLO) 概念の学術的系譜	19
5.2 Capability と Legitimacy の二軸フレームワーク	19
5.3 「日本型アプローチ」の可能性	21
第6章 論点の整理と政策への示唆	22
6.1 ここまでの考察から得られた知見	22
6.2 日本の選択肢——4つの将来像と協調モデル	22
6.3 政策提言	23
6.3.1 ISMAP への「主権評価レイヤー」の追加	24
6.3.2 日本版主権評価枠組み (J-SEAL) の段階的検討	24

6.3.3 国際展開——EU SEAL との相互承認と APEC-CSCR 構想	24
6.3.4 経済安全保障推進法の運用拡大	25
6.4 段階的アプローチ——医療分野から始める意義	25
6.5 事業者の役割——社会からの信頼を担う複数の主体	26
6.6 提言の実行に向けて着手すべき活動.....	26
謝辞	28
巻末注.....	29
参考文献一覧.....	33
外国語文献.....	33
日本語文献.....	33
政策文書・制度文書	34

第1章 なぜ今「デジタル主権」か——問題の所在

1.1 本報告書の目的と背景

デジタル技術が社会・経済・安全保障の基盤を構成する現代において、「デジタル主権」(Digital Sovereignty) は、もはや技術トレンドの一つではなく、国家経営・産業競争力・個人の権利利益の保護の根幹に関わる構造的テーマである。そこで本報告書では、この「デジタル主権」概念の学術的・政策的議論を体系的に整理し、日本が立つべき位置と、民間事業者に求められる役割を明らかにすることを目的とする。

本報告書は、デジタル主権をめぐる社会的議論を学際的に整理し、概念の系譜(第2章)、各国・地域の戦略比較(第3章)、日本の制度的課題(第4章)、および「社会からの信頼」(Social License) という新たな視座(第5章)を提示したうえで、第6章において日本の選択肢と政策への示唆を論じる。本文は平易な記述を旨とし、学術的・制度的な裏付けは巻末注に整理した。

なお、本報告書は株式会社 KDDI 総合研究所の調査研究として作成されたものである。本文中の分析および提言は公開情報および学術文献に基づくものであり、特定の事業者またはサービスの利用を推奨するものではない。また、本報告書は、公開情報の調査(デスクトップリサーチ)および国内関係者へのヒアリングに基づく初版である。当社は 2026 年度下期以降に海外調査を予定しており、その結果を踏まえて本報告書を更新していく。最新版は当社ウェブサイトを参照されたい。

1.2 構造的変化：3つの潮流の収斂

本報告書の問い——「デジタル主権とは何か」「日本として求められる立ち位置とは何か」——を検討する前提として、まず、日本を取り巻く環境がどのように変化し、どのような影響を及ぼしているのかを整理する。

1.2.1 地政学リスクの顕在化

近年、世界各国においてデータと技術の囲い込みが国家戦略化している。EU は 2026 年 4 月、クラウド主権フレームワークに基づく初の調達(総額最大約 1 億 8,000 万ユーロ・6 年間)を実施し、主権を定量評価するスコアリングを調達基準として初めて適用した[注 1]。米国では、2024 年に成立した TikTok 売却強制法(外国敵対勢力支配アプリケーション規制法)に基づき、

2026 年 1 月に同社の米国事業を運営する合併会社が発足し、推奨アルゴリズムの複製を米国ユーザーデータのみで再訓練する枠組みが採られた [注 2]。中国は 2025 年 10 月にサイバーセキュリティ法を初めて全面改正し（2026 年 1 月施行）、AI の安全管理・倫理規範に対する監督と AI 開発支援を定める AI 条項を新設した [注 3]。これらはいずれも、国家が自らの「主権」をデジタル空間においても行使しようとする動きであり、その強化が具体的な政策として実行段階へ移行していることがうかがえる。

1.2.2 ソブリンクラウド市場の急成長

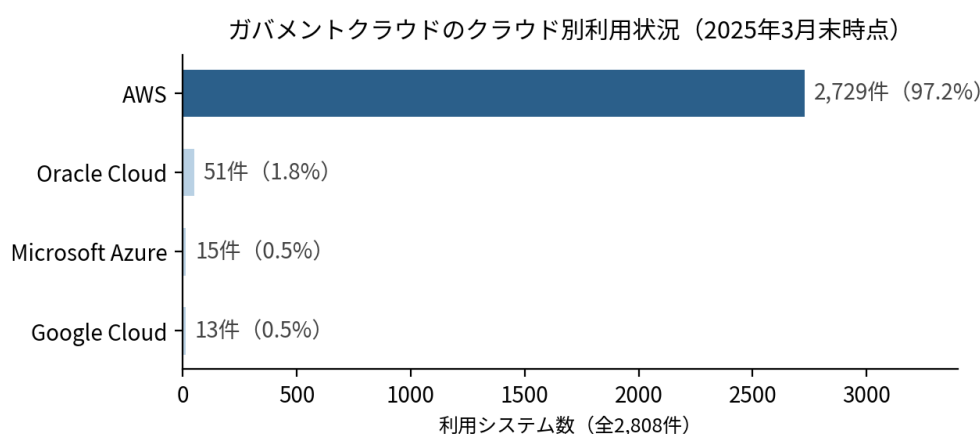
一方で、ソブリンクラウドのようなデジタル主権と関連性を持つ市場も急速に拡大している。Gartner の推計によれば、世界のソブリンクラウド IaaS 支出は 2026 年に約 804 億ドル（前年比 35.6%増）に達し、欧州は 2026 年の約 126 億ドルから 2027 年には約 231 億ドルへとほぼ倍増して、初めて北米を上回る見通しである。日本も 2025 年の約 5.2 億ドルから 2027 年には約 18.2 億ドルへと、規模は小さいながら 3 倍超の拡大が見込まれている [注 4]。民間調査会社による市場推計は「ソブリンクラウド」の定義次第で数値が大きく異なる点に留意が必要だが、いずれの推計においても、投資の焦点が「データの保存場所」から「運用の自律性」へとシフトしている点は共通している。つまり、ソブリンクラウド市場の拡大が示しているのは、データの保管・処理の基盤であるクラウドに対して、各国が自らの「主権」を及ぼすための基盤づくりが世界的に進みつつあるということである。

市場拡大の背景には 3 つの要因が関係していると考えられる。第一に、EU のクラウド主権フレームワーク（SEAL 制度、第 3 章参照）に代表される、主権評価を組み込んだ政府調達による政策的需要の創出である。第二に、NIS2 指令（重要セクターのサイバーセキュリティ義務を定める EU 指令）や DORA（金融セクターの ICT リスク管理を定める EU のデジタル・オペレーショナル・レジリエンス規則）といった各国・地域による規制強化が、金融・医療・エネルギー分野の需要を押し上げていることである。第三に、米国 CLOUD 法（Clarifying Lawful Overseas Use of Data Act）等の法律の域外適用に係るリスクへの認知が広がり、データの国内保存にとどまらない対応が求められるようになったことである。

1.2.3 日本の構造的課題

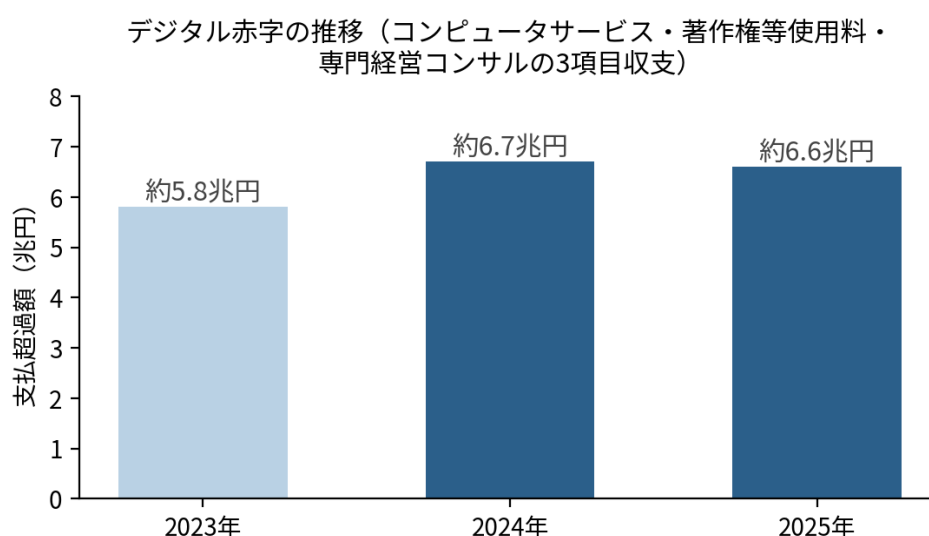
一方で、日本は、デジタル主権に関する複数の構造的課題に直面している。第一に、「デジタル主権」概念の整理が諸外国に比べて遅れている。第二に、政府共通クラウド基盤（ガバメン

トクラウド）では、2025 年 3 月末時点で国・自治体の全システム 2,808 件のうち約 97%にあたる 2,729 件が AWS を利用しており、自治体単位でも利用 862 自治体のうち 823 自治体（95.5%）が AWS を採用するなど（図 1-1）、特定の海外事業者への著しい依存が続いている（2026 年 3 月末時点でも、国の情報システムの約 85%が AWS 上で稼働している）〔注 5〕。第三に、いわゆる「デジタル赤字」（コンピュータサービス、著作権等使用料、専門・経営コンサルティングサービスの 3 項目の収支）は 2024 年に約 6.7 兆円（通信サービス・情報サービスを加えた 5 項目合計では約 6.8 兆円）に達し、2025 年も約 6.6 兆円と高止まりしている（図 1-2）〔注 6〕。経済産業省の検討チームは、悲観シナリオでは 2035 年に年間約 28 兆円へ拡大しうると推計しており〔注 7〕、デジタル経済における資金の海外流出は、一過性の現象ではなく構造的なロックインの様相を呈している。



出典：デジタル庁公表値に基づく報道（ITmedia NEWS 2025年5月8日）を基に作成

図 1-1 ガバメントクラウドのクラウド別利用状況



出典：総務省『令和7年版・令和8年版情報通信白書』（財務省「国際収支統計」に基づく）を基に作成。
2023年値は令和7年版白書記載の2024年値（約6.7兆円・前年比約0.9兆円増）から算出

図 1-2 デジタル赤字の推移

1.3 本報告書の問い

以上の背景を踏まえ、本報告書では以下の問いを検討する。「デジタル主権」とは何か。伝統的な主権概念とどのような関係にあるのか。各国・地域はこの概念をどのように解釈し、どのような政策を採用しているのか。日本の制度にはどのようなギャップがあり、それをどう埋めるべきか。そして、技術的能力を超えた「社会からの信頼」の獲得とは何を意味し、それを制度としてどう実装しうるのか。これらの5つについて、検討を進める。

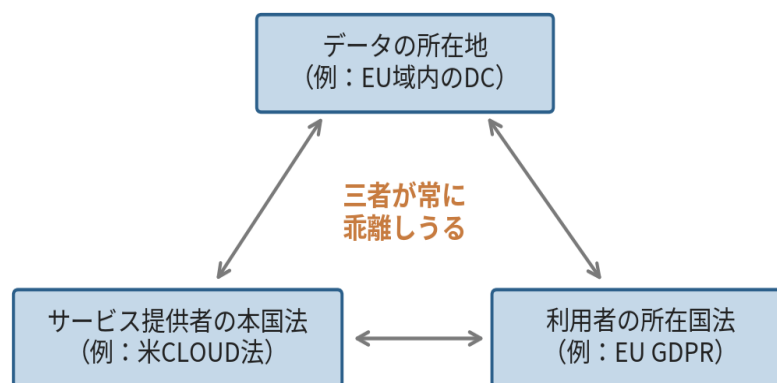
第2章 「主権」概念の系譜と変容——デジタル空間への拡張

2.1 伝統的主権概念の整理

「主権」(sovereignty)は、法学・政治学における最も基本的かつ論争的な概念の一つである。1648年のウェストファリア体制以降、主権は、領域内においては「最高」、領域外との関係では「独立」した権力であることを表すものとして捉えられてきた。また、近代以降の主権概念には、権力そのもの(power)としての側面と、その権力行使の正統性を支える権威(authority)としての側面が含まれると説明される[注8]。もっとも、この伝統的理解は、領土と管轄権の一致をなお前提としており、国家はその領土内において排他的な法的権限を行使し、他国はそれを尊重するという原則の上に立つ。なお、本報告書は、憲法学における主権論争に立ち入るものではなく、以下では政策論を進めるための操作的な整理にとどめる。

2.2 デジタル空間における主権の「三重のずれ」

伝統的主権が前提とする「領土＝管轄権」の等式は、デジタル空間では多くの場合成立しない。データの所在地、サービス提供者の本国法、利用者の所在国法の三者が常に乖離するという構造が、「管轄権の三重のずれ」を生んでいる(図2-1)。



「領土＝管轄権」の等式がデジタル空間では多くの場合成立しない(管轄権の三重のずれ)

図2-1 管轄権の「三重のずれ」

この管轄権の競合の典型例が、米国 CLOUD 法と EU の GDPR (一般データ保護規則) の衝突である。2018年に成立した CLOUD 法は、データの「保存場所」ではなく「管理者の国籍」を基準とし、米国企業が管理するデータであれば国外に保存されていても開示要求の対象となる。一方、GDPR 第 48 条は、第三国の裁判所または行政当局の決定に基づく個人データの移

転を、国際協定に基づかない限り原則として認めない [注 9]。この「法律間の衝突」は、デジタル空間における主権の競合を象徴的に示している。

2025 年 6 月には、フランス上院の公聴会において Microsoft の幹部が、EU 域内のデータセンターにデータを置いて米国当局からの法的要求があればデータ開示を拒否できない可能性があるとして宣誓下で証言した [注 10]。この事実は、データローカライゼーションだけではデータに対するコントロールを確保できないことを明確に示している。日本法の観点では、個人情報保護法の越境移転規制や電気通信事業法上の規律が国内側の対応枠組みを提供するものの、これらは管轄権のずれそのものを解消するものではない（日本法からの詳細な分析は更新版の課題とする）。

2.3 主権「主体」の多層化——国家・企業・個人

第 1 章では、国家がデジタル空間において主権を主張する動きを概観した。もっとも、デジタル空間では、主権の主体は国家に限定されない。例えば、プラットフォーム企業が事実上の「統治者」として主権的権力を行使しており、国家と企業の主権が正面衝突する現代固有の緊張が存在する。その典型例が、新型コロナ禍の接触確認アプリである。各国政府の公衆衛生アプリは、Apple と Google が提供する曝露通知 API の技術仕様に事実上従わざるを得ず（日本の接触確認アプリも同様である）、国家の政策設計が私企業の定める技術条件に制約されるという構図が顕在化した。また、国家との関係のみならず個人との関係でも、SNS 事業者によるアカウント停止やコンテンツ削除の判断、アプリストア運営者によるアプリ配信可否の決定は、私人でありながら、言論や事業の可否を事実上左右する権力の行使として機能しうる。具体的には、クラウドインフラのコントロール、API アクセスの制御、暗号鍵の管理といった企業の提供する技術を用いた手段が、軍事力・警察力に代わる実質的な執行手段として機能している。これは、強制力の行使という伝統的に国家が担ってきた任務を、テクノロジー企業が事実上代替しうることを意味する [注 11]。

この問題は、憲法学における「私人間効力」や行政学における「規制のガバナンス」の議論と関連性を有する。プラットフォーム企業が事実上の言論空間の管理者として規制主体である公権力に匹敵する影響力を持つという現実には、既存の法的フレームワークでは十分に捕捉できない。それゆえ、デジタル空間における私的な主体、それも国家・企業・個人の複数の主体の関係性を射程に入れた議論が求められるといえる。

2.4 「デジタル主権」の定義をめぐる学術的議論

ここで、「デジタル主権」を巡る近年の学術的議論についても若干触れておく。

Pohle & Thiel (2020) は、「デジタル主権」が法的・組織的概念というよりも、政治・政策における「言説的实践」(discursive practice) として機能していることを指摘している。すなわち、各国・各主体が自らの政策目的に都合よく解釈できる「戦略的曖昧さ」を持つ概念であると言えるであろう [注 12]。

Floridi (2020) は、デジタル主権が専門家や政治家だけの問題ではなく、すべての人々に影響する問題であると論じ、完全な民主的正当性と革新的柔軟性を兼備する「ハイブリッド型のコントロールシステム」の必要性を提起した。また、Pohle (2025) はデジタル主権概念の起源・目的・実践に対する批判的検討を行っている [注 13]。

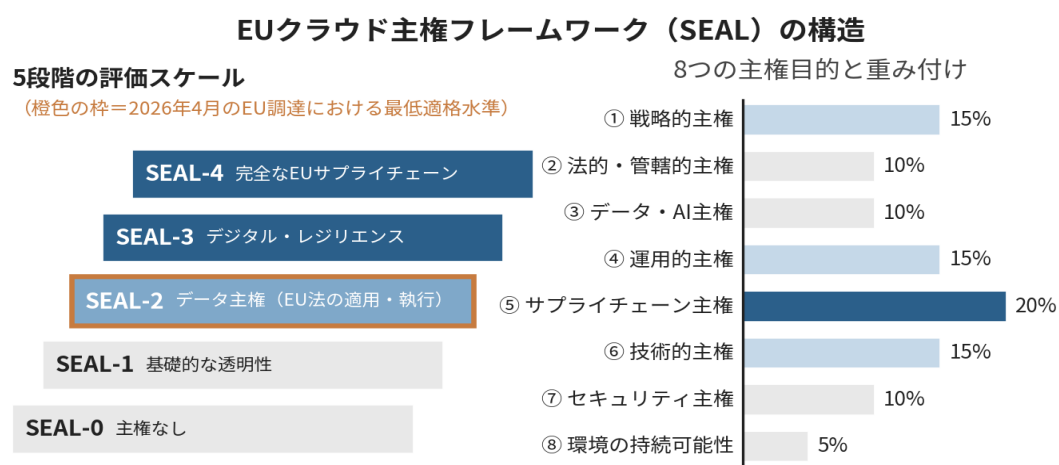
このようなこれまでの議論に鑑み、本報告書では、「デジタル主権」を「デジタル空間において、個人・企業・国家が自らのデータやシステムを自律的にコントロールできる能力」と操作的に定義する。この定義は、上記の学術的議論が示す概念の多義性を踏まえ、(1) 主体を国家に限定せず多層的に捉える点、(2) 法的地位ではなく「能力」に着目する点に特徴がある。この「コントロールできる能力」は、2.1 節で述べた主権概念の二側面のうち、主として権力(power)の側面に着目した整理である。なお、本報告書にいう「デジタル空間」は、データ、システム、プログラム等のデジタル資源の総体を含む広義で用いる [注 14]。そのうえで本報告書は、この「能力」(Capability)の次元に、第 5 章で「社会的正統性」(Legitimacy) [注 15]の次元を加えた二層の枠組みとして議論を展開する。ただし、この二層は並列の定義ではない。2.4 節の定義(能力)が本報告書の出発点であり、第 5 章の観点(正統性)は、その能力の担い手が社会からの信頼を獲得・維持できるかという補完的な次元である(5.1 節参照)。あわせて、検討対象の範囲を明示しておく。本報告書は、デジタル主権の諸相のうち、評価の制度化が国際的に最も先行しているクラウド基盤の主権性を中心的な検討対象とし、AI や半導体、データ流通等への拡張は、海外調査を踏まえた更新版において扱う。

第3章 各国・地域のデジタル主権戦略——4つのモデルの比較分析

3.1 EUモデル：規制を通じた「戦略的自律性」から「実装による主権」へ

EU はデジタル主権の制度化において最も先進的な位置にある。GDPR を起点とし、AI 法、データ法、NIS2 指令、DORA と、包括的な法体系を構築してきた [注 16]。これらの個別法制を貫く上位概念が「デジタル主権」であり、EU はこれを定量的に評価する方法論の一つとしてクラウド主権フレームワークを開発した。

SEAL (Sovereignty Effectiveness Assurance Level) は 5 段階の評価スケールであり、SEAL-0 (主権なし) から SEAL-4 (チップからソフトウェアまで完全な EU サプライチェーン) まで、クラウドサービスの主権性を客観的に評価する。評価は 8 つの主権目的に基づき、サプライチェーン主権が最大の重み (20%) を持つ [注 17]。この重み付けは総合評価における配点であり、EU が主権性の判定に際して何を重視しているか——とりわけサプライチェーンの自律性——を示している (図 3-1)。



出典：European Commission, Cloud Sovereignty Framework, Version 1.2.1 (2025年10月) を基に作成

図 3-1 EU クラウド主権フレームワーク (SEAL) の構造

2026 年 4 月 17 日、欧州委員会はこのフレームワークを用いた初の調達契約を 4 つの欧州コンソーシアムと締結した。自社技術を開発する Post Telecom (ルクセンブルク。仏 CleverCloud・仏 OVHcloud と協働)、STACKIT (独)、Scaleway (仏) の 3 件が SEAL-3 (デジタル・レジリエンス) を取得した一方、S3NS (仏 Thales と米 Google Cloud の合併) を含む Proximus (ベル

ギー) コンソーシアムは、調達 lowest 適格水準である SEAL-2 (データ主権) にとどまった [注 1]。非 EU 技術に依拠する構成でも最低限の主権要件を満たしうることが実証された一方、CISPE (欧州のクラウドインフラ事業者団体) はこれを「主権ウォッシング (sovereignty washing)」 (実質的な主権性を伴わないまま、認証の取得によって主権的であるかのように見せかけることを可能にする、という趣旨の批判) と批判しており、議論は現在でも続いている。

さらに 2026 年 6 月 3 日、欧州委員会は「技術主権パッケージ (Tech Sovereignty Package)」の中核として、クラウド・AI 開発法 (CADA: Cloud and AI Development Act) 案を公表した。同案は、EU 域内のデータセンター容量不足と非 EU クラウド事業者への依存という 2 つの脆弱性への対応を掲げ、4 段階の「Union 保証レベル」によって、セキュリティ・レジリエンス・主権に関する要件の充足を公共部門 (EU 機関や加盟国の政府・自治体等の公的機関) での利用資格に段階的に紐づける。CADA 案は非 EU 事業者を排除するのではなく、リスクベースの審査を前提に、公共調達の要件を通じて参加を認める設計であり、公共調達において「EU 付加価値」 (EU 域内への技術・経済面の貢献) を価格以外の評価要素として考慮する仕組みも導入する。SEAL が単発の調達実験にとどまらず、EU の立法アジェンダへと接続されつつあることを示すものである (同案は提案段階にあり、今後欧州議会・理事会の審議を経る) [注 18]。

なお、近年の EU は規制強化一辺倒ではない。2025 年 11 月に公表されたデジタル・オムニバスに象徴される規制簡素化へと軸足を移しつつ、CADA のような産業政策・調達政策を強化している。「規制による主権」から「実装による主権」への重心移動と捉えることができ、後述する日本の制度設計を考えるうえでも重要な文脈である。すなわち、規制の条文で主権を宣言するだけではなく、調達・認証・運用という日々の実務の中で主権を確保していく方向への転換である。

3.2 米国モデル：技術覇権と域外法による「事実上の主権」

米国は「デジタル主権」の用語を政策的に使用しないが、CLOUD 法、FISA 第 702 条、大統領令による技術管理を通じて事実上のデジタル主権を行使している。なお、これらの法制度は米国政府による域外的な権限行使を支えるものであり、2.4 節で述べた個人や企業の自律的なコントロールを保障するものではない。また、「信頼できる同盟国」 (法文上は「適格外国政府」 (qualifying foreign government)) との執行協定 (executive agreement) を通じて、相手国の司法手続きを尊重しながらデータ開示を行う仕組みも整備している。日本はまだ締結しておら

ず、政策課題である。

3.3 中国モデル：国家統制型「サイバー主権」

中国は「サイバー主権」の名の下に、サイバーセキュリティ法、データ安全法、個人情報保護法の三法体制を整備し、国外へのデータ移転を制限し国内保存を義務化している。2025 年 10 月には、2017 年の施行以来初となるサイバーセキュリティ法の全面改正が可決され（2026 年 1 月 1 日施行）、法的責任の大幅な強化、域外適用の拡大とともに、AI の開発支援と安全管理・倫理規範に対する監督を定める AI 条項が新設された [注 3]。こうした中国の動向は、独自の垂直統合エコシステムを構築し、国際的な相互運用性よりも自国の統制力を優先する特徴があると言えるであろう。

3.4 日本の DFFT モデル：「信頼に基づく共存」

DFFT（Data Free Flow with Trust）は、その名のとおり「信頼性のある自由なデータ流通」というコンセプトをもち、2019 年 1 月のダボス会議において安倍総理（当時）が提唱し、G20 大阪サミットで各国からの支持を得た。2023 年の G7 群馬高崎会合では、IAP（Institutional Arrangement for Partnership）が G7 各国の合意により立ち上がり、OECD に事務局が設置された経緯がある。

DFFT は、各国が主権の強化に向かう潮流に対し、「信頼」を条件として自由なデータ流通を確保しようとする、主権を相対化する対抗的な構想である。DFFT が志向するのは「信頼」を媒介とした共存であり、それ自体が各国の「自律」の確保を目的とするものではない。この意味で、自律の確保を核とするデジタル主権とは緊張関係に立つ。ただし、信頼を測定・検証する実装枠組みを欠いたまま各国の主権強化が進めば、DFFT の理念そのものが空洞化しかねない。この意味で、信頼の測定手段（主権評価）は DFFT の対立物ではなく、その存立条件である。IAP の設置以降、この実装フレームワークの具体化には至っておらず、DFFT は理念先行の状態にとどまっている。EU が SEAL 制度によって「信頼」を定量的に評価する方法論を確立し、さらに CADA 案によってこれを立法アジェンダへと展開しつつある今、日本も DFFT の「信頼」を具体的に定義・評価する仕組みを持たなければ、提唱国でありながら基準形成に参画できないという逆説的な状況に陥りかねない。この点は、次章以降で検討する日本の制度的課題と評価枠組みの議論の出発点となる。

3.5 比較と類型化

表 3-1 は、本章で見た 4 つのアプローチを、基本理念、主権の主体、実装の手段、課題の観点から整理したものである。比較から浮かび上がるのは、制度化の程度の差である。EU は評価と調達を通じた「実装による主権」の段階に入り、米国は法制度の域外適用を通じて事実上の主権を行使し、中国は国家統制による閉鎖的な体系を確立している。これに対して日本は、DFFT という国際的な理念を提唱しながら、その「信頼」を測定・検証する実装枠組みを持たない点で、理念と実装の間の距離が最も大きい。この距離を生んでいる日本の制度的な現状を検証することが、次章の論点である。

表 3-1 4 つのモデルの比較（当社整理） [注 19]

	EU	米国	中国	日本（DFFT）
基本理念	戦略的自律性	技術覇権・安全保障	国家統制型サイバー主権	信頼に基づく共存
規制強度	高（包括的法体系。近年は簡素化と産業政策へ重心移動）	中（域外法中心）	最高（国家統制）	中（一般法は整備。主権観点の評価枠組みは未整備）
主権評価	SEAL（5 段階定量）。CADA 案で公共部門調達へ拡張中	なし（自己申告）	なし（国家審査）	なし（ISMAP はセキュリティ評価に限定）
課題	規制負担の軽減とイノベーションとの両立	他国のデジタル主権との衝突	国際的相互運用性の欠如	実装フレームワークの具体化

第4章 日本の現状——制度的ギャップと「主権の空白」

4.1 日本の関連法制度の体系的整理

4.1.1 経済安全保障推進法

2022 年施行の経済安全保障推進法は、重要物資の安定供給、基幹インフラの安全確保、先端技術の開発支援、特許出願の非公開化の 4 つの柱からなる。2022 年 12 月には「クラウドプログラム」が特定重要物資に指定され、2024 年 4 月には経済産業省が同法第 9 条第 4 項に基づき、AI 開発に必要な計算資源の整備に係る 5 件の供給確保計画に対し合計最大 725 億円の助成を決定した。その後も追加認定が続いている [注 20]。SEAL 型の主権評価制度を検討するうえで、法的な足掛かりが既に存在することを意味する。

4.1.2 ISMAP

ISMAP は政府が調達するクラウドサービスのセキュリティを評価・登録する制度であり、約 1,200 項目の管理策基準に基づく。なお、ISMAP 管理基準については、意見公募を経て 2025 年 12 月に全般的な改定案が公表されており、詳細管理策の大幅な削減を含む改定後の基準は、関係規程類とともに 2027 年 3 月頃に公表・施行される予定である（2026 年 9 月時点）。ただし、主権（所有構造、域外法、サプライチェーン独立性といった要素）は制度の射程外である。

4.1.3 ガバメントクラウド

政府共通クラウド基盤はコスト削減・効率化が主目的であり、主権は制度設計に組み込まれていない。システムベースでの AWS 利用率は約 97%に達している（1.2.3 節参照）。なお、2023 年に条件付きで採択されていた国内サービス「さくらのクラウド」は、2026 年 3 月にすべての技術要件の充足が確認され、国内サービスとして初めて正式認定に至った。デジタル庁がガバメントクラウドの技術要件への適合を確認して認定したサービスは、2026 年 6 月時点で 5 つ（AWS、Microsoft Azure、Oracle Cloud Infrastructure、Google Cloud、さくらのクラウド）となったが、国内サービスの正式認定と利用実態の偏りの解消は別の問題であり、依存構造そのものは変わっていない [注 21]。

4.1.4 プラットフォーム規制三法

特定デジタルプラットフォームの透明性及び公正性の向上に関する法律（透明化法）・スマートフォンにおいて利用される特定ソフトウェアに係る競争の促進に関する法律（スマホ法）・特

定電気通信による情報の流通によって発生する権利侵害等への対処に関する法律(情報流通プラットフォーム対処法)の3つの法律は巨大プラットフォーム企業への規律強化が目的だが、EUと異なり利用者が自らのデータを管理できる権利の保障やアルゴリズムの説明責任は射程外である。EU ではプラットフォーム規制を通じて利用者の権利保障に資する制度が設けられ、それがデジタル主権の保護の一翼を担っているのに対し、日本の三法にはそのような仕組みが組み込まれていない。

4.2 「主権の空白」の構造分析

上記に整理した EU における制度「SEAL」の8つの主権目的のうち、戦略的主権（15%）、法的・管轄権的主権（10%）、サプライチェーン主権（20%）、技術的主権（15%）、環境の持続可能性（5%）の合計65%相当（各割合は、EU の SEAL における評価の重み。図3-1 参照）が、ISMAP・ガバメントクラウドのいずれにおいても評価対象外となっている〔注17〕。これが「主権の空白」である。

表 4-1 EU の8つの主権目的と日本の制度の対応関係
(○明示的に評価／△間接的・部分的／×評価対象外。当社による暫定的な整理)

主権目的（重み）	EU SEAL	ISMAP	ガバメントクラウド
① 戦略的主権（15%）	○	×	×
② 法的・管轄権的主権（10%）	○	×	×
③ データ・AI 主権（10%）	○	△	△
④ 運用的主権（15%）	○	△	△
⑤ サプライチェーン主権（20%）	○	×	×
⑥ 技術的主権（15%）	○	×	×
⑦ セキュリティ主権（10%）	○	○	○
⑧ 環境の持続可能性（5%）	○	×	×

なお、表 4-1 の対応関係は本報告書による暫定的な整理である。ISMAP 管理基準・ガバメントクラウド技術要件との条項レベルでの詳細な対照検証は、産学官の開かれた場での検討に委ねるべき今後の課題である（6.6 節参照）。

この「空白」は「逆転のパラドクス」を生んでいる。EU の初回 SEAL 調達において採択4件中最低位の SEAL-2 にとどまった構成（Google 技術に依拠する S3NS を含むコンソーシアム）が、

日本のガバメントクラウド基準ではマネージドサービスの豊富さからむしろ最も高い適合性を示しうる。EU の調達結果は、法人格やデータセンターの所在が EU 域内にあっても、技術スタックが非 EU ハイパースケーラーに依拠する限り上位の主権評価を得られないことを示しており、この対比は、日本の制度がセキュリティと効率性を重視する一方で、サプライチェーンの自律性や域外法リスクを体系的に評価する枠組みを持たないことの帰結を鮮明にしている。

4.3 政策的含意

以上の分析から導かれる政策的含意——ISMAP への「主権評価レイヤー」の追加、EU SEAL との互換性を視野に入れた日本版主権評価枠組み（J-SEAL）の検討、DFFT 推進の文脈での主権評価の国際相互承認——については、第 6 章で詳述する。

第5章 デジタル主権と社会からの信頼——能力と正統性の二軸

5.1 Social License to Operate (SLO) 概念の学術的系譜

デジタル主権が実質を持つためには、データとシステムを託しうる事業者が存在し、利用者に選択肢があることが前提となる。その「託しうる」という信頼を捉える概念として、本章では Social License to Operate (SLO) を参照する。SLO は、2.4 節で示したデジタル主権の定義を置き換えるものではない。日本におけるデジタル主権の検討を出発点とすれば、まず主権評価の枠組み（第6章）を構築し、国内に複数の選択肢を確保することが第一段階（デジタル主権の問題）である。そのうえで、確保された選択肢の担い手が社会からの信頼を獲得・維持できるかが、これに続く第二段階の問いであり、本章で扱う SLO の考え方は、この第二段階に備えるための概念的な準備として参照するものである。

SLO は 1990 年代に採掘産業で発展した概念で、「複数のステークホルダーが組織の実践を受容すること」を意味する。SLO は法律上の免許・許認可ではなく、発行主体も証書も存在しない。政府の許可を得ていても、影響を受ける地域社会等の受容を失えば事業を安定的に継続できない——という鉱業の経験から生まれた概念であり、一度の取得で完結せず継続的に維持されるべきものとされる。学説上は、受容の深まりを正統性 (legitimacy) ・信認 (credibility) ・信頼 (trust) の段階として捉えるモデルも提示されている [注 22]。近年、デジタル技術領域へと拡張され、AI やビッグデータに対する Social License が学術的に論じられている。Leonard (2018) はデータ駆動型アプリケーションと AI における Social License を、Shaw ら (2020) はパンデミック下のビッグデータ活用における Social License をそれぞれ論じている [注 23]。

なお、SLO は本来、事業者が社会から獲得する「受容」を指す概念であり、伝統的な主権概念とは主体の範囲や権力の射程が異なる。そこで本報告書は、主権概念に含まれる二つの側面 (2.1 節参照) のうち、SLO をとりわけ権威 (authority) の側面に関連するものとして捉え、デジタル主権を支えるインフラ事業者が満たすべき信頼の条件という次元に位置づけて用いる。

5.2 Capability と Legitimacy の二軸フレームワーク

本報告書の中心的な提起は、デジタル主権を「技術的能力」(Capability) の次元にとどめず、「社会的正統性」(Legitimacy) の次元を統合した包括的フレームワークとして捉え直すことである (2.4 節で述べた二層の枠組み)。なお、2.4 節の定義における「能力」は技術的なものに限定されない。以下では、インフラ事業者の文脈における Capability を、運用・監視・暗号鍵管

理等を掌握する技術的・組織的な能力を中心に用いる（本報告書の用語法）。この二層は、第2章で述べた主権概念の二側面におおむね対応する。すなわち、Capability は権力（power）の側面に対応するが、法的な権限ではなく、データとシステムを現に掌握する事実上の能力を指す。Legitimacy は権威（authority）の側面に対応し、その能力の行使が社会から受容されていることを意味する。上記で検討した SLO に係る議論との関連性でいえば、Legitimacy の確立ないしフレームワークを設計するためには、社会からの受容および信頼性の獲得が鍵となるであろう。

Capability（技術的能力）——データを管理下に置き、技術的・法的にコントロールできる能力。思考はインサイド・アウト（我々は何ができるか）。比喩的に言えば高性能な「金庫」。

Legitimacy（社会的正統性）——社会から「データを託すに値する」という信頼を獲得すること。思考はアウトサイド・イン（社会は何を望んでいるか）。比喩的に言えば「金庫の鍵を預かる信頼」。

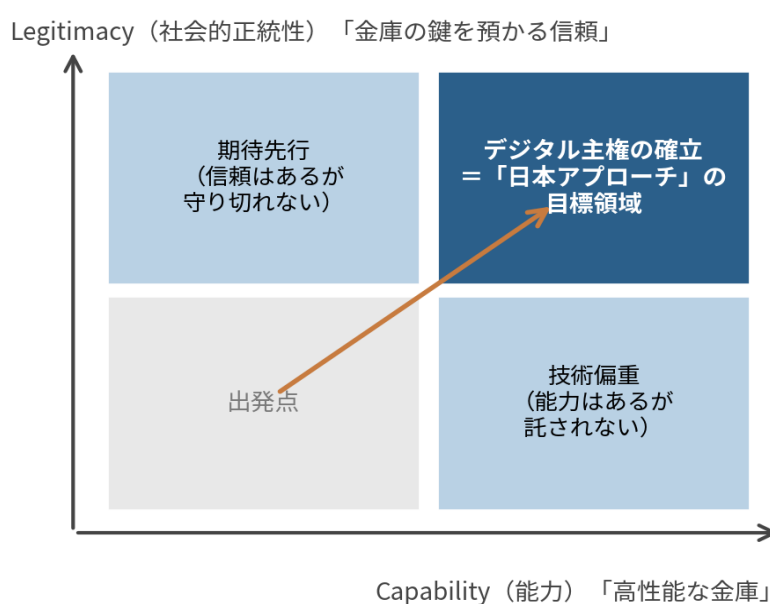


図 5-1 Capability と Legitimacy の二軸フレームワーク

この二軸フレームワーク（図 5-1）は、規制対応にとどまらず、信頼を競争力の重要な要素として位置づける視点を提供する。経済学的には、クラウドサービスは「信頼財」（credence goods）の性格を持ち、利用者がその品質（主権性を含む）を事後的にも検証しにくいいため、情報の非対称性を克服するための制度設計——第三者による評価・認証——が不可欠である。

5.3 「日本型アプローチ」の可能性

重要なのは、独自性それ自体ではない。EU の評価枠組みは能力（Capability）面の主権性を精緻に測る一方、事業者が社会からの信頼を獲得しているか（Legitimacy）を評価する仕組みは制度化されていない。米国は体系的な評価枠組み自体を持たない。この不十分な部分を補い、能力と正統性の両面を評価する制度設計を示せるなら、それは日本に閉じた「独自モデル」ではなく、他国からも参照されうる相互運用可能な水準となりうる。DFFT 提唱国としての実績はその国際的な足場となり、単一国家として制度実装を迅速に進めうることは、実装スピード面の利点である。その具体的な方向性については、第 6 章で論じる。

第 6 章 論点の整理と政策への示唆

6.1 ここまでの考察から得られた知見

第一に、「デジタル主権」は伝統的主権の単純な拡張ではなく、能力（Capability）と正統性（Legitimacy）の二層からなる新たな概念フレームワークを必要とする。

第二に、EU は SEAL 制度により主権の定量評価を実現し、CADA 案によってこれを立法アジェンダへと展開しつつある。主権評価をめぐる国際的な基準競争は既に始まっており、日本が独自の評価枠組みを持たなければ、他国の定めた基準の受け手にとどまり、基準形成に参画できないリスクがある。参画できなければ、日本の事業者は他国基準への適合コストを一方的に負い、日本の制度環境や利用者の要請を評価軸に反映させる機会を失うことになる。

第三に、日本の制度には「主権の空白」が存在する。ISMAP・ガバメントクラウドはセキュリティと効率性を評価する一方、EU の主権目的の 65%相当に対応する評価軸を持たない。

第四に、デジタル主権を「社会からの信頼」の獲得まで含めた二層の枠組みとして捉えることで、規制対応にとどまらない「日本型アプローチ」の方向性を構想できる。

6.2 日本の選択肢——4 つの将来像と協調モデル

日本のソブリンクラウドをめぐる将来像は、政策選択によって大きく異なる。本報告書では、定性的に 4 つのシナリオを提示する。第一は「現状維持」であり、セキュリティ評価（ISMAP）にとどまり主権性の定量評価を導入しない場合、第 4 章で述べた「主権の空白」が継続する。第二は「国内技術主導」であり、国産技術スタックを中核に据える場合、技術的主権は最も高まるが、当面は実用化までの時間軸と提供可能なマネージドサービスの幅に制約が残る可能性がある。第三は「ハイパースケーラー（大規模海外クラウド事業者）主導」であり、市場拡大は最も速いが、主権性は事業者の自己申告に依存し、域外法リスクが残存する。第四は「協調モデル」であり、国内事業者と海外事業者の協働（合弁等）により海外技術を「主権の枠内」で活用しつつ、運用・監視・暗号鍵管理を国内で掌握し、その主権性の水準を評価制度によって客観的に検証する（図 6-1）。なお、海外技術を用いつつ運用・監視・暗号鍵管理を国内主体が担う形態は、仏 S3NS 等で現に実装されている。

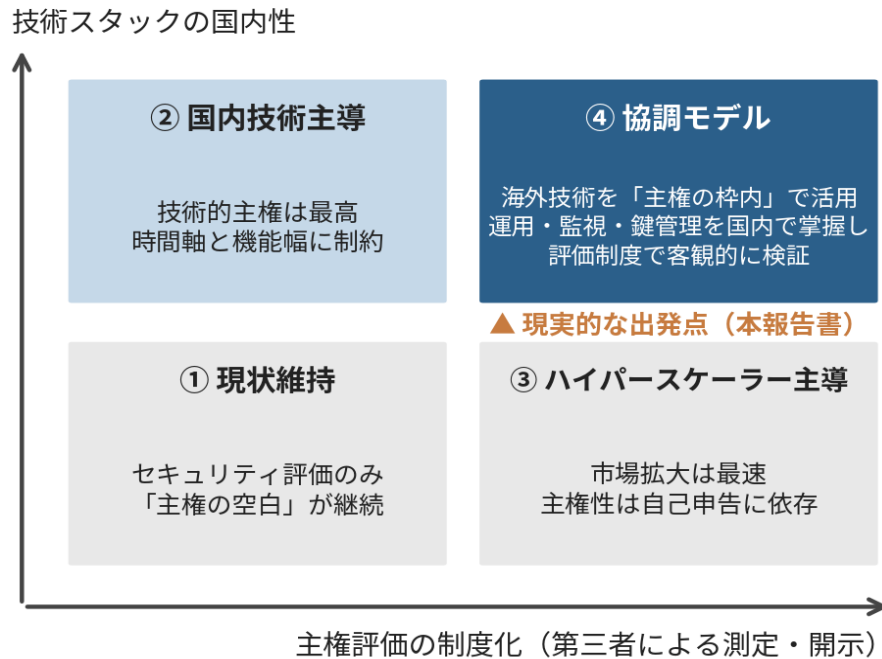


図 6-1 日本の選択肢——4つの将来像（当社整理）

EU の初回 SEAL 調達の結果——自社技術で完結する事業者が SEAL-3 を取得し、ハイパースケーラー技術に依拠する協調型（仏 S3NS 等）が SEAL-2 にとどまるという二層構造——は、技術自給と機能性のトレードオフを制度の中で可視化した点で、日本にとって重要な示唆を持つ〔注1〕。完全な国産技術による主権確保が短期的には困難である以上、協調モデルを許容しつつ、その主権性の水準を評価制度によって測定・開示させるアプローチが、現実的な出発点となる。重要なのは、いずれのモデルを選ぶかを市場任せにするのではなく、評価の物差しを社会の側が持つことである。その要点は、透明性のある議論を通じて確立された客観的な指標を、危機が生じる前にあらかじめ用意しておくことにある。評価の物差しを整えることは、排除の対極にあるだけでなく、排除を予防する装置でもある。主権性を測る手段が存在しないまま地政学的な緊張が高まれば、「主権の空白」は資本国籍や原産地といった粗い基準による一律の排除措置で埋められかねない。段階的な評価の枠組みを事前に整備しておくことこそが、開かれた市場を維持しながら空白を埋める現実的な経路であり、EU の初回調達において非 EU 技術に依拠する構成が排除ではなく評価によって位置づけを与えられた事実は、その実例である。

6.3 政策提言

本節の提言は、具体的な制度を例に挙げて論じるが、実装の経路は一つに限られない。既存制

度の見直し、調達実務の改善、新たな枠組みの創設など、複数の道筋がありうることを予め付言する。なお、本節の 4 項目は、別途公表する政策提言の 5 提言と次のように対応する。6.3.1 節と 6.3.2 節は提言 1（評価枠組みの検討）および提言 2（情報開示の共通化）に、6.3.3 節は提言 5（国際相互運用性）に対応し、6.3.4 節はこれらの法的基盤に関する補足的な検討である。提言 3（切替可能性の確保）は第 1 章・第 4 章の分析を、提言 4（依存構造の把握）は 6.4 節を基礎とする。

6.3.1 ISMAP への「主権評価レイヤー」の追加

第 4 章で分析した「主権の空白」を埋めるため、ISMAP の 3 層管理基準（ガバナンス基準・マネジメント基準・管理策基準）に、第 4 の層として「主権評価レイヤー」を追加することを提言する。このレイヤーは、EU SEAL の 8 つの主権目的との互換性を確保しつつ、日本の制度環境に適合した評価項目を含むべきである。具体的には、所有構造・資本関係の評価、域外法リスクの評価、サプライチェーン主権の評価、技術的独立性の評価が候補となる。

6.3.2 日本版主権評価枠組み（J-SEAL）の段階的検討

EU SEAL の 5 段階に対応する日本版の主権評価レベル体系を構築し、政府調達・重要インフラ分野への段階的な適用可能性を検討することを提言する。制度設計、パイロット適用、本格運用という段階的な工程が考えられるが、評価軸の設計、第三者評価の主体・方法、既存制度（ISMAP・ガバメントクラウド技術要件）との関係整理など、制度設計において検討すべき論点が多い。本報告書は、これらの論点を産学官の関係者による開かれた検討の俎上に載せることを提案するものである。なお、EU の SEAL が 27 加盟国の合意形成を要するのに対し、日本は単一国家として制度実装を迅速に進めうるという構造的な優位性を持つ。

6.3.3 国際展開——EU SEAL との相互承認と APEC-CSCR 構想

日本版の主権評価枠組みは、国内制度として閉じるのではなく、国際的な相互運用性を当初から設計に組み込むべきである。第一に、EU SEAL（および CADA 案の Union 保証レベル）との相互承認である。日本のクラウド事業者が EU 市場において主権性を認められる枠組みを構築することは、DFFT の「信頼に基づくデータ流通」を制度レベルで具体化するものであり、国際標準化提案と並行して推進すべきである。第二に、APEC-CSCR（Cloud Sovereignty Cross-border Rules）構想を提案したい。これは、APEC-CBPR（APEC 域内の個人情報の越境移転について、認証を通じて信頼を相互に承認する仕組み。2011 年策定）が実現した「信頼の相互運用性」の

モデルを、クラウド主権の相互認証へと拡張するものである。ただし、ここで相互承認の対象となるのは、セキュリティ水準の同等性ではなく、主権性の検証可能性——どの国の法が及び、誰が運用・監視・暗号鍵管理を掌握しているかを相互に確認できること——である。安全性の同等性を基準とすれば、域内の大規模事業者への集中がそのまま追認されかねず、主権の問題意識と接続しないからである。この枠組みは、各国のデータを各国内に保管しつつ、学習済みモデルや連合学習（フェデレーテッドラーニング）の成果のみが越境する形態は、DFFT の理念を技術的に実装する一つの形となりうる。日本は DFFT 提唱国として CBPR の拡張を主導してきた実績があり、この領域でリーダーシップを発揮する正統性を持つ。なお、APEC-CSCR は本報告書による提案であり、現時点で公式の政策提案が存在するものではない。

6.3.4 経済安全保障推進法の運用拡大

「クラウドプログラム」が特定重要物資に既に指定されていることを活用し、主権評価制度の法的基盤として経済安全保障推進法の運用拡大を検討すべきである。具体的には、基幹インフラの安全確保の文脈にソブリンクラウドの観点を組み込み、重要インフラ事業者のクラウド調達において主権評価を参照する方向性が考えられる。

6.4 段階的アプローチ——医療分野から始める意義

主権評価制度の導入は、全セクター一律ではなく、機微性が高く国民的関心の強い分野から段階的に進めることが現実的である。本報告書は、医療（ヘルスケア）、金融、政府調達一般という順序を提案する。医療分野を先行領域とする理由は3つある。第一に、標準型電子カルテや医療情報の連携基盤など、国が管理者となる基盤の設計・法制化が現に進行しており、評価の観点を制度に組み込む余地が開いているのは今しかないという「制度形成の窓」が存在すること。第二に、国が管理者となる基盤であれば、評価の要請に法的な疑義が生じにくいこと（民間医療機関の個別システムを対象とする場合の正当性・実務負担の問題とは切り分けられる）。第三に、データの機微性が高く、「データを託すに値する」という社会からの信頼の要請が最も先鋭に表れる領域であること。もっとも、機微性の高さは関係者の警戒を招く実装上のコストでもあるため、先行対象は国が管理者となる医療情報基盤に絞り、個別の医療機関に新たな負担を課さないことを前提とすべきである。金融分野は、EU の DORA が 2025 年 1 月から適用されるなど規制動向の国際的収斂が進んでおり、第二の適用領域として親和性が高い。

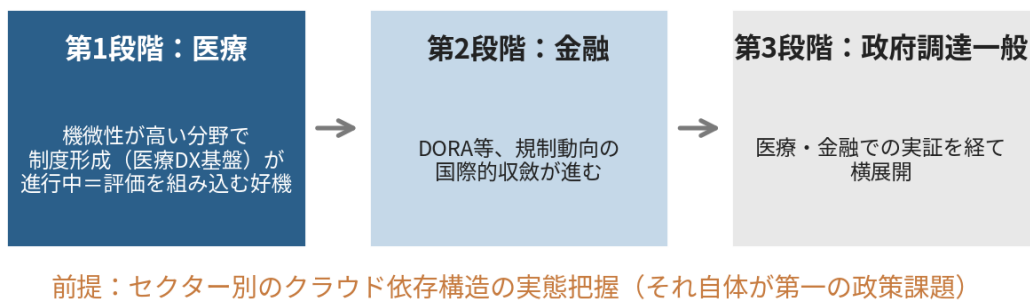


図 6-2 段階的アプローチの全体像

なお、その前提として、国内の主要セクター——とりわけ医療クラウド（電子カルテ SaaS、PHR 基盤等）——が現にどのクラウド基盤に依拠しているかの実態把握が不可欠である。ガバメントクラウドについては利用状況が公表されている一方、セクター別の依存構造を示す包括的な公的統計は存在しない。この実態調査自体が、主権評価制度に先立つ第一の政策課題である。

6.5 事業者の役割——社会からの信頼を担う複数の主体

デジタル主権の確保は、政府の制度設計だけで完結するものではない。データ流通の物理的基盤を担う国内事業者には、（1）技術的能力（Capability）——運用・監視・暗号鍵管理の国内掌握、そして（2）社会的正統性（Legitimacy）——データを託すに値するという信頼の獲得、の両面が求められる。この役割は特定の一社が担うべきものではなく、複数の国内事業者が分担し競い合うことで、単一事業者への集中を避けつつ、信頼性を競争力の重要な要素とする市場環境を形成することが望ましい。第5章で述べたとおり、クラウドサービスが「信頼財」の性格を持つ以上、信頼を検証可能にする制度（主権評価）が整ってはじめて、事業者の実践は市場で正当に評価される。制度と実践は相互に依存する関係にある。

6.6 提言の実行に向けて着手すべき活動

6.3 節の提言を実行に移すために着手すべき活動を、対応関係とともに整理する。評価枠組みの検討（6.3.1 節・6.3.2 節）に向けては、まず ISMAP 管理基準・ガバメントクラウド技術要件と EU フレームワークとの詳細な対照分析を行い、その結果を踏まえて評価軸の具体設計に進む。段階的アプローチ（6.4 節）に向けては、セクター別のクラウド依存構造の実態調査が前提となる。国際展開（6.3.3 節）に向けては、EU SEAL との相互承認および APEC-CSCR 構想の制度

的・外交的な実現可能性の検証が必要である。これらの背景として、日本のソブリンクラウド市場規模の定量的な推計が全体を支える。あわせて、海外における制度運用と市場実態の現地調査による検証を行う（2026 年度下期以降に当社として海外調査を予定している）。これらは、産学官の開かれた場での継続的な検討に委ねたい。

—— 以上 ——

謝辞

本報告書の作成にあたっては、以下の先生方から個別にご意見をいただいた。記して感謝申し上げます。なお、本報告書の内容および誤りに関する責任はすべて株式会社 KDDI 総合研究所に帰属するものであり、本報告書の記載は、ご意見をいただいた各氏のご見解を示すものではない。

（五十音順・敬称略。所属・職名は2026年9月時点）

伊藤 由希子 （慶應義塾大学 商学部 教授）

曾我部 真裕 （京都大学大学院 法学研究科 教授）

森 亮二 （英知法律事務所 弁護士）

森田 朗 （東京大学 名誉教授）

山本 健人 （関西大学 社会学部メディア専攻 准教授）

巻末注

[注 1] European Commission, “Commission advances cloud sovereignty through strategic procurement” (2026 年 4 月 17 日)。契約総額は 6 年間で最大 1 億 8,000 万ユーロ。調達は Cloud III DPS の下で 2025 年 10 月に開始され、SEAL-2 が最低適格水準とされた。採択 4 件のうち、Post Telecom (CleverCloud・OVHcloud と協働)、STACKIT、Scaleway が SEAL-3、Proximus コンソーシアム (S3NS、Clarence、Mistral を含む) が SEAL-2 を取得。

[注 2] Protecting Americans from Foreign Adversary Controlled Applications Act (2024 年 4 月成立)。同法は売却 (ByteDance の持分 20%未満化) を義務付けるものであり、アルゴリズムの再訓練は法律上の義務ではなく、2025 年 12 月の拘束的合意を経て 2026 年 1 月 22 日に発足した米国合弁会社 (Oracle・Silver Lake・MGX が各 15%等を出資) の枠組みにおいて、推奨アルゴリズムのライセンス複製を米国ユーザーデータのみで再訓練し、Oracle の米国クラウド環境で管理することとされたもの (AP 通信等の報道による)。

[注 3] 中華人民共和国サイバーセキュリティ法の改正 (2025 年 10 月 28 日全国人民代表大会常務委員会可決、2026 年 1 月 1 日施行)。2017 年の施行以来初の全面改正であり、法的責任の強化、域外適用の拡大に加え、AI の基礎研究・コア技術開発の支援と、AI の倫理規範・安全・リスク管理に対する監督管理の強化を定める AI 条項を新設した。ジェトロ北京事務所「『サイバーセキュリティ法 (2025 年改正)』および『国家サイバーセキュリティインシデント報告管理弁法』の要点整理と対応策」(2026 年 2 月)等を参照。罰則強化等の詳細は、CISTEC「中国サイバーセキュリティ法の改正について」(2025 年 11 月 27 日)も参照 (https://www.cistec.or.jp/service/keizai_anzenhosho/china/data/20251127.pdf)。

[注 4] Gartner, “Gartner Says Worldwide Sovereign Cloud IaaS Spending Will Total \$80 Billion in 2026” (2026 年 2 月 9 日プレスリリース)。世界のソブリンクラウド IaaS 支出は 2026 年に約 804 億ドル (前年比 35.6%増)。地域別 (100 万ドル) では、欧州が 2025 年 6,868→2026 年 12,587→2027 年 23,118、北米が同 12,667→16,394→21,127、日本が同 519→932→1,816。なお民間調査会社の市場推計は「ソブリンクラウド」の定義により大きく異なり、例えば Fortune Business Insights は世界市場を 2025 年時点で約 1,547 億ドルと推計している。本報告書は、支出ベースで定義が比較的明確な Gartner 推計を基準として参照する。

[注 5] デジタル庁公表値 (2025 年 3 月末時点) に基づく報道 (ITmedia NEWS 2025 年 5 月 8 日)。国・地方自治体の全システム 2,808 件のうち 2,729 件 (約 97%) が AWS を利用。次点は Oracle Cloud Infrastructure の 51 件 (1.8%)。自治体に限るとガバメントクラウド利用 862 自治体のうち 823 自治体 (95.5%) が AWS を利用。2026 年 3 月 31 日時点では、デジタル庁資料に基づき国の情報システムの約 85%が AWS 上で稼働と報じられている (ITmedia ビジネスオンライン 2026 年 6 月 17 日)。

[注 6] 2024 年値は総務省『令和 7 年版情報通信白書』(3 項目で約 6.7 兆円・前年比約 0.9 兆円増、5 項目合計で約 6.8 兆円)。2025 年値は総務省『令和 8 年版情報通信白書』(3 項目で約 6.6 兆円の支払

超・前年比約 0.1 兆円減)。財務省「国際収支統計」に基づく。赤字幅の拡大には一服感があるものの、6 兆円台半ばの支払超過が定着している。

[注 7] 経済産業省 大臣官房 若手新政策プロジェクト (PIVOT) 『デジタル経済レポート：データに飲み込まれる世界、聖域なきデジタル市場の生存戦略』(2025 年 4 月 30 日公表)。同レポートは、AI 革命を踏まえた悲観シナリオにおいて、組込みソフトウェア等の「隠れデジタル赤字」および SDX (Software Defined Everything) 化に伴う貿易収支側の支払超過まで含めた、ソフトウェア・データを由来とする支払超過の総額が、2035 年の最大推計で 45.3 兆円に到達するとの試算を示している。

[注 8] 一般に、「主権」には、①統治権、②国家権力の最高独立性、③国政についての最高決定権の 3 つの意味があるとされる。そして、フランス革命を契機に権力の源泉が君主から国民へ移行する過程で、主権概念は権力 (power) の側面と権威 (authority) の側面から成るものとして捉えられるようになったと説明される。とりわけ、民主主義社会において国家の法への服従が正当化されるのは、立法権を含む権力の源泉が主権者である国民に由来することによる。学説の詳細は、芦部信喜 (高橋和之補訂) 『憲法〔第 8 版〕』(岩波書店、2023 年) 39 頁以下、佐藤幸治『日本国憲法論』(成文堂、2020 年) 425 頁以下、松井茂記『日本国憲法〔第 4 版〕』(有斐閣、2022 年) 118 頁以下を参照。

[注 9] CLOUD Act, H.R.4943 (2018 年)。GDPR 第 48 条。詳細は西村高等法務研究所『CLOUD Act 研究会報告書』参照。

[注 10] フランス上院「公共調達とデジタル主権」調査委員会公聴会 (2025 年 6 月 10 日)。Microsoft France 公共・法務担当ディレクター Anton Carniaux 氏は、フランス市民のデータが仏当局の明示的な承認なく米当局に移転されないと保証できるかとの質問に対し、宣誓下で「保証できない (Non, je ne peux pas le garantir)」と証言した。議事録は仏上院ウェブサイト (senat.fr) の当該委員会議事録 (2025 年 6 月 9-10 日) 参照。

[注 11] 国家とプラットフォーム企業の間をめぐると憲法学の議論として、山本龍彦教授は、強大な権力を持つ国家という「伝統的なモンスター」に対し、プラットフォーム企業という「新しいモンスター」が現れ、現状ではこの力に対抗できるのは国家しかなく、新旧のモンスターを対抗させて自由と民主主義を守らざるを得ない状況にあると指摘する (山本龍彦「「アテンションエコノミー」という“モンスター”に対抗する仕組みはできるのか？」ステラ net (NHK 財団)、2024 年 9 月 13 日、<https://www.steranet.jp/articles/-/3519>)。

[注 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)

[注 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 (2025 年 5 月 16 日公開) . <https://doi.org/10.1002/poi3.437> / デジタル主権をめぐる近年の包括的研究として、Chander, A. & Sun, H. (eds.), Data Sovereignty: From the Digital Silk Road to the Return of the State (Oxford University Press, 2023)、Bradford, A., Digita

l Empires: The Global Battle to Regulate Technology (Oxford University Press, 2023) も参照（学説整理の拡充は更新版で行う）。

[注 14] 政府文書における関連概念の用例。骨太方針 2026（経済財政運営と改革の基本方針 2026、令和 8 年 7 月 21 日閣議決定）は、「開かれた A I 主権を確立しながら A I ・データ基盤を整備する」（第 2 章 1.（2））、「政府のデジタル基盤の強靱化・自律性向上」（同）を明記し、経済安全保障の文脈では「データセンター・クラウドの安全性等を確保するために必要な措置を講ずる」（第 2 章 2.（2））としている。本報告書の定義と分析は、これらの政策文脈と接続するものである。

[注 15] legitimacy の訳語には組織論等で「正当性」も用いられるが、本報告書では、手続を通じて獲得される受容という含意を踏まえ「正統性」を用いる。

[注 16] 本文 3.1 で挙げた EU 法制の概要は次のとおり。GDPR（一般データ保護規則）：個人データ保護の一般法。AI 法（AI 規則）：リスクベースで AI システムを規律する規則。データ法（データ規則）：IoT データ等へのアクセス・共有やクラウド間の切替（スイッチング）を規律する規則。NIS2 指令：エネルギー・医療等の重要セクターに広くサイバーセキュリティ義務を課す指令。DORA：金融セクターの ICT リスク管理を定める規則。

[注 17] European Commission, Cloud Sovereignty Framework, Version 1.2.1（2025 年 10 月 20 日）。8 つの主権目的（SOV-1～SOV-8）と 48 の評価基準からなり、SEAL-0～SEAL-4 の 5 段階で評価する。重み付けは、SOV-1 戦略的主権 15%、SOV-2 法的・管轄的主権 10%、SOV-3 データ・AI 主権 10%、SOV-4 運用的主権 15%、SOV-5 サプライチェーン主権 20%（最大）、SOV-6 技術的主権 15%、SOV-7 セキュリティ・コンプライアンス主権 10%、SOV-8 環境の持続可能性 5%。本文 4.2 の 65%は、IS MAP 等の射程外と整理した SOV-1・2・5・6・8 の重みの合計。

[注 18] European Commission, Proposal for the Cloud and AI Development Act（CADA）, COM(2026) 502（2026 年 6 月 3 日）。技術主権パッケージは CADA のほか、Chips Act 2.0、EU オープンソース戦略等から構成される。CADA 案は、公共調達において「EU 付加価値」を補助的な非価格基準（解釈上、120 点中最大 15 点の重み付け）として考慮することを求める。

[注 19] 本報告書で各国・地域について用いる「モデル」の語は、アプローチの類型を指す便宜的な呼称である。

[注 20] 経済産業省ニュースリリース「経済安全保障推進法に基づくクラウドプログラムの安定供給確保に係る供給確保計画の認定等について」（2024 年 4 月 19 日）。その後、さくらインターネットの第 2 次投資計画（約 1,000 億円）の認定等が続いている。

[注 21] デジタル庁「ガバメントクラウド」ウェブサイト。さくらのクラウドについて「すべての技術要件を満たしたことを確認できたので、2026 年 3 月 27 日以降本番環境の提供が可能」と公表。認定 5 サービスの現況は ITmedia ビジネスオンライン（2026 年 6 月 17 日）参照。

[注 22] SLO の起源と理論的展開について。用語は 1997 年に鉱業界で用いられ始めたとされ、提唱者自身による回顧として、Cooney, J. (2017). Reflections on the 20th anniversary of the term 'social licence'.

Journal of Energy & Natural Resources Law, 35(2), 197–200。鉱業部門における概念の起源の検証として、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。法的許認可とは別に企業行動を規律する社会的ライセンスの実証分析として、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。正統性 (legitimacy) ・信認 (credibility) ・信頼 (trust) の段階モデルは、Boutilier, R. G., & Thomson, I. (2011). The Social License to Operate. Society for Mining, Metallurgy and Exploration による。

[注 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.

参考文献一覧

外国語文献

- Boutilier, 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.

日本語文献

- 芦部信喜（高橋和之補訂）『憲法（第8版）』岩波書店、2023年。
- 佐藤幸治『日本国憲法論（第2版）』成文堂、2020年。

松井茂記『日本国憲法（第4版）』有斐閣、2022年。

山本龍彦「「アテンションエコノミー」という“モンスター”に対抗する仕組みはできるのか？ 慶応義塾大学・山本龍彦教授（憲法学）インタビュー」ステラ net（NHK 財団）、2024年9月13日（<https://www.steranet.jp/articles/-/3519>）。

政策文書・制度文書

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.

全国人民代表大会常務委員会 (2025). 中華人民共和國サイバーセキュリティ法（2025年改正、2026年1月1日施行）。

ジェトロ北京事務所 (2026). 「サイバーセキュリティ法（2025年改正）」および「国家サイバーセキュリティインシデント報告管理弁法」の要点整理と対応策. 2026年2月.

経済産業省 (2024). 経済安全保障推進法に基づくクラウドプログラムの安定供給確保に係る供給確保計画の認定等について. 2024年4月19日.

デジタル庁. DFFT. <https://www.digital.go.jp/policies/dfft>

デジタル庁. ガバメントクラウド. https://www.digital.go.jp/policies/gov_cloud

内閣府. 経済安全保障. https://www.cao.go.jp/keizai_anzen_hosho/

総務省 (2025). 令和7年版情報通信白書.

<https://www.soumu.go.jp/johotsusintokei/whitepaper/r07.html>

西村高等法務研究所. CLOUD Act 研究会報告書.

https://www.nishimura.com/sites/default/files/images/13700_1.pdf