IISE 調査研究レポート（No.16）

「データ基盤・クラウド基盤をめぐるデジタル主権の国際動向」

（2026 年度「データ基盤・クラウド基盤を取り巻くデジタル主権に関する社会課題と政策動向に関する調査研究」報告書より抜粋）

2026 年 10 月
国際社会経済研究所　主任研究員　岡部 稔哉

近年、データの利活用は、行政サービスの高度化、重要インフラの安定運用、人工知能（AI）を含む産業競争力の向上を支える基盤として、重要性を高めている。これに伴い、国内外では「デジタル主権（Digital Sovereignty）」の確保が重要な政策課題として認識されるようになっている。

従来、クラウド政策は、行政システムの効率化、IT コストの削減、サービス開発の迅速化を主な目的として推進されてきた。しかし、行政、金融、医療、エネルギー、交通、通信、防衛などの機能がクラウドやデータ連携基盤に依存するようになる中で、これらの基盤は、社会機能の継続性や国家の自律性にも関わるものとして位置づけられつつある。

デジタル主権の必要性を認識させる象徴的な出来事も相次いでいる。2025 年 7 月には、ロシア国営石油大手ロスネフチが約 49%を出資するインドのエネルギー企業 Nayara Energy が EU の対ロシア制裁の対象となったことを受け、Microsoft のメールや Teams 等のサービスが停止した。この事案は、インド政府高官に「警鐘（wake up call）」と位置づけられ、同国におけるデジタル主権への関心を高めるきっかけとなった[1]。また、2024 年 11 月に国際刑事裁判所（ICC）がガザ紛争を巡りイスラエルのネタニヤフ首相らへ逮捕状を発付したことなどを受け、米国は 2025 年 2 月、カーン首席検察官を制裁対象とした。その後、同検察官の Microsoft のメールアカウントが利用できなくなったと報じられた[2]。Microsoft は ICC 全体へのサービス停止を否定しているものの、この事案は、米国の政策判断が米国企業のデジタルサービスを通じて域外の国際機関にも影響し得るとの懸念を喚起した。さらに、2026 年 3 月には、中東の軍事衝突に伴うドローン攻撃により、UAE に所在する AWS のデータセンター2 拠点が直接攻撃を受けて損傷し、地域のクラウドサービスに広範な障害が発生した。この事例は、米国企業のクラウド基盤が米国の戦略的資産と見なされ、軍事攻撃の対象となり得ることを示している。以上の出来事が示すように、域外適

[1] India eyes sovereign cloud push for key sectors amid geopolitical risks: Report https://www.moneycontrol.com/news/business/india-eyes-sovereign-cloud-push-for-key-sectors-amid-geopolitical-risks-report-13901721.html

[2] Trump's sanctions on ICC prosecutor have halted tribunal's work | AP News https://apnews.com/article/icc-trump-sanctions-karim-khan-court-a4b4c02751ab84c09718b1b95cbd5db3

用を伴う制裁、クラウド事業者の判断、物理的な軍事攻撃は、クラウドに依存する組織のサービス継続性やデータへのアクセスに直接影響し得る。

その背景には、クラウド市場のハイパースケーラーによる寡占がある。欧州のクラウド市場を例にとると、Amazon、Microsoft、Google の米国 3 社が約 7 割を占める一方、欧州事業者の域内シェアは 2017 年の 29%から 2022 年には 15%へ低下したとされる[3]。また、EU 企業によるソフトウェア・クラウド支出の約 8 割が米国企業向けであり[4]、EU の対米サービス貿易赤字は 2024 年に約 1,780 億ユーロに達したとの分析もある[5]。なお、こうした集中は欧州特有の現象ではない。世界のクラウド市場でも米国 3 社が約 3 分の 2 のシェアを占めており[6]、日本を含む各国のクラウド市場においても、米国企業への高い依存という状況は共通している。こうした特定国・少数事業者への依存は、平時には規模の経済、豊富な機能、利便性などの利益をもたらす一方、制裁、法執行、外交関係の変化、障害又は武力紛争が生じた際には、利用者側のみでは制御することが困難な戦略的リスクとなり得る。

上述した一連の事案やハイパースケーラーによる市場寡占の構造を踏まえ、データがどこに保存・処理され、誰によって運用され、どの法域の法令に基づいてアクセスされ得るのか、また、障害、サイバー攻撃、地政学的緊張、特定事業者への依存といったリスクが顕在化した場合に、公共部門や重要インフラがどの程度の統制可能性を維持できるのかが、各国・地域に共通する検討課題となっている。このため、デジタル主権は、単なるデータの国内保存や外国企業の排除ではなく、重要な機能について、供給元の多様化、代替可能性、法的・運用上の統制可能性及び技術的な移行可能性を確保するための課題として捉えられる。

１．各国のデジタル主権政策概要

各国・地域のデジタル主権政策は、データの国内保存だけでなく、クラウドの選定・運用、外

[3] European Cloud Providers' Local Market Share Now Holds Steady at 15% | Synergy Research Group
https://www.srgresearch.com/articles/european-cloud-providers-local-market-share-now-holds-steady-at-15

[4] European Software and Cyber Dependencies
https://www.europarl.europa.eu/RegData/etudes/ATAG/2025/780413/ECTI_ATA%282025%29780413_EN.pdf

[5] EU trade relations with United States
https://policy.trade.ec.europa.eu/eu-trade-relationships-country-and-region/countries-and-regions/united-states_en

[6] Q2 Cloud Market Passes $143 Billion; Highest Growth Rate in Eight Years | Synergy Research Group
https://www.srgresearch.com/articles/q2-cloud-market-passes-143-billion-highest-growth-rate-in-eight-years

国法の域外適用への対処、重要インフラの保護、特定事業者への依存低減など、幅広い政策で構成されている。本章では、今回調査対象とした、EU、フランス、ドイツ、インド、シンガポール、オーストラリア、米国、日本について、行政クラウドと重要インフラに関する代表的な施策を取り上げ、各国・地域が重視する統制の方法と政策上の特徴を整理する。

EU は、調査対象の国・地域の中で、デジタル主権を明示的な政策課題として正面から掲げ、包括的な政策パッケージとして体系的に立案している点で際立っている。その射程もデータ保護にとどまらず、クラウド、AI、半導体、オープンソース、重要インフラを含む技術基盤全体の自律性として捉える。象徴的な施策は European Tech Sovereignty Package（2026 年 6 月 3 日公表）[7]と、その中核をなす Cloud and AI Development Act（CADA）[8]であり、公共調達に 4 段階の主権保証水準を導入する方向を示す。さらに Cloud Sovereignty Framework[9]は CADA 法案に先行する 2025 年 10 月に欧州委員会の調達実務へ導入され、クラウド主権を調達上の評価基準として既に実装されている。これをデータ法、NIS2 指令[10]、金融デジタル運用レジリエンス規則（DORA）[11]を組み合わせ、データ所在、域外法リスク、運用体制、供給網、クラウド乗換え可能性等を用途の重要度に応じて評価する点が特徴である。

フランスは、行政のクラウド利用を進める Cloud au centre（クラウド中心ドクトリン）[12]と、機微データを扱うクラウドを厳格に選別する政策を併用している。中核は ANSSI（国家サイバーセキュリティ庁）の認証制度 SecNumCloud v3.2[13]で、技術・運用面の安全性に加え、EU 域内で

---

7 Commission proposes tech sovereignty package to strengthen Europe's digital autonomy and resilience | Shaping Europe's digital future
https://digital-strategy.ec.europa.eu/en/news/commission-proposes-tech-sovereignty-package-strengthen-europes-digital-autonomy-and-resilience

8 Cloud and AI Development Act | Shaping Europe's digital future
https://digital-strategy.ec.europa.eu/en/policies/cloud-and-ai-development-act

9 Cloud Sovereignty Framework Version 1.2.1 – Oct.2025
https://commission.europa.eu/document/download/09579818-64a6-4dd5-9577-446ab6219113_en

10 NIS2 Directive: securing network and information systems | Shaping Europe's digital future
https://digital-strategy.ec.europa.eu/en/policies/nis2-directive

11 Digital Operational Resilience Regulation - Finance - European Commission
https://finance.ec.europa.eu/regulation-and-supervision/financial-services-legislation/implementing-and-delegated-acts/digital-operational-resilience-regulation_en

12 La doctrine de l'État — numerique.gouv.fr
https://www.numerique.gouv.fr/offre-accompagnement/cloud-administrations/la-doctrine-cloud-etat/

13 Référentiel SecNumCloud v3.2

のデータ処理・管理、非欧州法の域外適用や非欧州主体の支配からの保護を重視する。SREN 法第 31 条[14]は、特に機微な行政データを民間クラウドで扱う際の要件を調達・契約実務に落とし込んだ。Bleu は、海外技術を活用しつつ法的・運用的統制を確保するソブリンクラウド事業者の代表例である。さらに、各省庁に域外デジタル依存の削減計画策定を求める[15]など、行政自身が率先して非欧州技術への依存低減を進めている点も特徴的である。

ドイツは、デジタル主権を、クラウド利用者が実際に統制できるかを測る基準として具体化している。BSI（連邦情報セキュリティ庁） C5:2026[16]がクラウドの情報セキュリティと監査可能性を確認し、C3A（Criteria enabling Cloud Computing Autonomy）[17]がデジタル主権（クラウド利用の自律性）を明示的な目的として、法的管轄、データ、運用、供給網、技術、非常時の切断・継続運用を評価する。行政分野ではドイツ行政クラウド戦略（DVS）[18]の下、海外技術を国内で独立運用するモデルを推進する。ソブリンクラウド事業者 Delos Cloud がその代表例のひとつである。NIS2 実施法と KRITIS-Dachgesetz（重要インフラ包括法）[19]も、重要インフラのサイバー・物理両面のレジリエンスを支えている。

インドは、クラウド活用と国内統制を組み合わせる実務型の政策を採る。行政分野の中核は政

---

https://s3.eu-west-par.io.cloud.ovh.net/sf-cyber/sf-cyber/documents/secnumcloud-requirements-baseline-v3.2.pdf

14 Article 31 - LOI n° 2024-449 du 21 mai 2024 visant à sécuriser et à réguler l'espace numérique (1) - Légifrance
https://www.legifrance.gouv.fr/loda/article_lc/LEGIARTI000049565888

15 デジタル主権：国家は欧州域外への依存度削減を加速
https://www.numerique.gouv.fr/sinformer/espace-presse/souverainete-numerique-reduction-dependances-extra-europeennes/

16 BSI - Bundesamt für Sicherheit in der Informationstechnik - Kriterienkatalog Cloud Computing C5:2026 (engl.)
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/CloudComputing/Anforderungskatalog/2026/C5_2026_en.pdf

17 BSI - Bundesamt für Sicherheit in der Informationstechnik - C3A - Criteria enabling Cloud Computing Autonomy
https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/CloudComputing/C3A_Cloud_Computing_Autonomy.pdf

18 DVS - Rahmenwerk Zielarchitektur_v1.0_final
https://www.it-planungsrat.de/fileadmin/beschluesse/2021/Beschluss2021-46_Deutsche_Verwaltungscloud-Strategie_AL1.pdf

19 Schutz kritischer Infrastruktur gestärkt | Bundesregierung
https://www.bundesregierung.de/breg-de/aktuelles/kritis-dachgesetz-2383682

府クラウド GI Cloud（MeghRaj）／MeghRaj 2.0 であり、政府専用環境と商用クラウドを組み合わせ、AI・データ分析機能の活用を進める。MeitY（電子・情報技術省） empanelment 制度は、政府向けクラウドの国内データ所在、セキュリティ、相互運用性、契約条件等を確認し、政府調達の候補として認定する仕組みである。さらに Cloud Selection Framework[20]は、情報の機微性に応じて利用可能なクラウド形態を選別する。RBI（インド準備銀行）は、決済データ国内保存規制[21] [22]により、当局による監査の実効性を確保している。また国産ソブリンクラウドスタックの研究開発[23]を通じて、外国技術への依存低減と、国内でクラウドを開発・運用する能力の強化も進めている。

シンガポールは、クラウドを国内に囲い込むより、国際的な商用クラウドを政府の統制下で活用する「統制された開放性」を特徴とする。Digital Government Blueprint v2[24]の Cloud-First 方針を受け、Government on Commercial Cloud（GCC 2.0）[25]が AWS、Azure、Google Cloud 等の商用クラウドを政府が安全に利用するための共通基盤であり、政府独自のセキュリティ基準、監視、利用ルールを適用する。Singapore Government Tech Stack（SGTS）[26]は政府共通の開発基盤や標準を提供し、CloudSCAPE[27]は、セキュリティ設定が政府基準に適合しているかを自動的に確認する。2025 年施行の Cybersecurity Act[28]改正は、クラウドやデータセンターを含む重要

---

[20] OFFICE MEMORANDUM – Guidelines for cloud selection framework https://www.meity.gov.in/static/uploads/2026/03/a49a9e2bfb5bbd9057cf3efafda5b8d7.pdf

[21] Notifications - Reserve Bank of India https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=11244

[22] Master Directions - Reserve Bank of India https://www.rbi.org.in/Scripts/BS_ViewMasDirections.aspx?id=12967

[23] TCS Signs Landmark MoU with C-DAC to Strengthen India's Sovereign Cloud Infrastructure https://www.tcs.com/who-we-are/newsroom/press-release/tcs-signs-landmark-mou-cdac-strengthen-indias-sovereign-cloud-infrastructure

[24] Digital Government Blueprint https://file.go.gov.sg/digitalgovernmentblueprint.pdf

[25] GCC | Singapore Government Developer Portal https://www.developer.tech.gov.sg/products/categories/infrastructure-and-hosting/gcc/overview

[26] https://www.developer.tech.gov.sg/singapore-government-tech-stack/

[27] CloudSCAPE | Singapore Government Developer Portal https://www.developer.tech.gov.sg/products/categories/cybersecurity/cloudscape/overview

[28] https://sso.agc.gov.sg/Acts-Supp/19-2024/Published/20240704?DocDate=20240704&ViewType=Pdf&_=20251208185116

デジタル基盤への監督を強化している。

オーストラリアは、デジタル主権を明示的な政策目標には掲げていないが、政府データの保護、サイバー強靭性、重要インフラ規制を通じて、政府によるデジタル基盤の統制を確保している。また、政府系ファンドによる国内主権クラウドへの投資[29]も行う。Whole-of-Government Cloud Computing Policy[30]の下でクラウド利用を進めつつ、Hosting Certification Framework（HCF）[31]により、政府データを扱うクラウド・データセンター事業者の所有、管理、運用、サプライチェーンを事業者単位で認定する（HCF は 2025 年から改定が進められており、完了まで新規認定を一時停止中）。SOCI 法[32]と ERP 法[33]は、データ保存・処理を重要インフラ分野として扱い、登録、リスク管理、インシデント報告、政府介入の枠組みを整備した。

米国は、デジタル主権という政策を掲げてはいないが、政府調達、国防、法執行、重要インフラの制度を組み合わせてクラウドとデータを統制する。連邦政府は FedRAMP[34]が商用クラウドの安全な利用を支え、最新の改定である FedRAMP 20x[35]では、文書中心の審査から機械可読な証拠と継続的な確認への転換が図られ、従来の Rev.5 からの移行が進められている。国防分野では DoD Cloud Computing SRG（Security Requirements Guide）[36]が Impact Level 別に追加要件

---

29 National Reconstruction Fund invests in Macquarie Technology Group | National Reconstruction Fund Corporation
https://www.nrf.gov.au/news-and-media-releases/national-reconstruction-fund-invests-macquarie-technology-group-strengthen-australias-sovereign-cloud-and-cybersecurity-capabilities

30 Hosting Certification Framework - March 2021.v2
https://www.hostingcertification.gov.au/sites/default/files/2021-11/Hosting%20Certification%20Framework%20-%20March%202021.v2.pdf

31 https://www.hostingcertification.gov.au/ https://www.hostingcertification.gov.au/

32 Security of Critical Infrastructure Act 2018 - Federal Register of Legislation
https://www.legislation.gov.au/C2018A00029/latest/versions

33 Security of Critical Infrastructure and Other Legislation Amendment (Enhanced Response and Prevention) Act 2024 - Federal Register of Legislation
https://www.legislation.gov.au/C2024A00100/latest/text

34 FedRAMP | FedRAMP.gov
https://www.fedramp.gov/

35 FedRAMP 20x
https://www.fedramp.gov/20x/

36 DoD Cloud Computing Security | Cyber Exchange
https://www.cyber.mil/dccs/

を設定する。CLOUD Act[37]は、米国当局が令状などの法的手続に基づき、米国企業の管理下にあるデータについて、保存場所が国外であっても提出を求め得ることを明確にした。一方で、他国から見れば米国系クラウド利用時の域外法適用リスクとして認識され、各国のクラウド主権政策に大きな影響を与えている。

日本では、デジタル主権を直接の目的とする単一制度ではなく、セキュリティ、行政デジタル化、経済安全保障、防衛、重要インフラの制度が主権的な要素を支えている。クラウド・バイ・デフォルト原則とガバメントクラウド（デジタル庁が整備する、国・地方公共団体が共通の基準で利用するクラウド環境）[38]が行政のクラウド利用を推進する。また、ISMAP[39]は、政府が利用するクラウドサービスのセキュリティ対策を監査・審査し、基準を満たすサービスを政府調達の候補として登録する制度である。防衛省の情報セキュリティ基準[40]と経済安全保障推進法の基幹インフラ制度[41]も、契約・調達・事前審査を通じて統制を補っている。

37 CLOUD Act Resources
https://www.justice.gov/criminal/cloud-act-resources

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

39 制度案内 - ISMAP 概要
https://www.ismap.go.jp/csm?id=kb_article_view&sysparm_article=KB0010005&sys_kb_id=8c0b2d3b831b3650aa68c6a8beaad346&spa=1

40 装備品等及び役務の調達における情報セキュリティ基準
https://www.mod.go.jp/atla/cybersecurity/01_kijun_0137_att_r05.pdf

41 基幹インフラ役務の安定的な提供の確保に関する制度 - 内閣府
https://www.cao.go.jp/keizai_anzen_hosho/suishinhou/infra/infra.html

表 1 各国・地域のデジタル主権政策（筆者まとめ）

国・地域	特徴
EU	・**EU Tech Sovereignty Package**（2026 年 6 月 3 日公表）により、クラウド、AI、半導体、OSS を含むフルスタック型の技術主権確保を公式政策化。 ・中核の **Cloud and AI Development Act（CADA）**は欧州域外クラウドへの過度な依存の低減を目指し、公共調達を主眼に**主権保証レベル（4 段階）**の共通枠組みを提案（重要インフラ等への拡張余地あり）。
フランス	・首相通達「**クラウド中心ドクトリン**」（2021）に基づき行政システムを原則クラウド化。 ・機微データは「信頼されたクラウド（cloud de confiance）」の利用を求める（ソブリンクラウド事業者 **Bleu** が代表例）。 ・国家の自律性を強調、**非欧州デジタル技術への依存低減を指向**。 ・主権クラウド認証制度 **SecNumCloud** を整備。SREN 法により主権性・信頼性要件を満たすクラウド利用を求める。
ドイツ	・ドイツ行政クラウド戦略（2021）に基づきクラウド化しつつデジタル主権確保を目指す。 ・**相互運用性（ベンダーロックイン回避）**と**評価可能な主権要件**を推進（ソブリンクラウド事業者 **Delos Cloud** が代表例）。 ・クラウドセキュリティ・透明性を評価する **BSI C5** を整備。クラウド自律性・主権性を評価する **C3A** を整備し C5 を補完。
インド	・Cloud-First 政策の下、**政府クラウド GI Cloud（MeghRaj）**を整備。 ・**MeitY empanelment 制度**は、政府向けクラウドサービスについて、国内データ所在、セキュリティ、相互運用性、契約条件等への適合を確認し、政府調達対象として認定する仕組み。 ・加えて、MeitY 系の政府研究機関（C-DAC）を中心に、民間大手（TCS）と連携した**「国産ソブリンクラウドスタック」の研究開発・実証**が 2025 年から始動しており、クラウド基盤そのものの技術的自律性を高める取り組みとして注目される。
シンガポール	・Cloud-First 政策を採用。 ・AWS、Azure、Google Cloud など外資クラウドの積極利用と統制を重視。 ・政府機関が商用クラウドを安全かつ効率的に利用するための共通基盤 **GCC（Government on Commercial Cloud）**を整備。
オーストラリア	・Whole-of-Government Cloud Computing Policy（2026 年 7 月 1 日施行）によりクラウド利用を推進。 ・外資を含む複数クラウドの利用と政府による統制を重視。 ・政府向けクラウド事業者認定制度 **HCF（Hosting Certification Framework）**を改定中。
アメリカ	・連邦政府は Cloud First（2010 年）、Cloud Smart（2019 年）等に基づきクラウド利用を推進し、各省庁が個別のクラウド戦略・要件を策定。国防総省は **DoD Cloud Computing SRG（Security Requirements Guide）**により Impact Level 別のセキュリティ要件を設定。 ・国産クラウドを優先する政策は設けず、安全保障要件による懸念国排除を指向。 ・政府クラウドのセキュリティ評価・認可制度として **FedRAMP** を整備（Rev.5 から 20x へ移行中）。（デジタル主権を明示した制度ではない）
日本	・政府情報システムは「クラウド・バイ・デフォルト原則」を採用。 ・国産クラウドを優先する政策は設けず、現状ハイパースケーラー中心。 ・政府情報システムのクラウドサービスは **ISMAP** によりセキュリティ・ガバナンス等を評価。（デジタル主権を目的とした制度ではない）

２．データ主権・運用主権・技術主権に関する施策

デジタル主権の定義は国・地域によって異なる。ここでは代表的な解釈として、デジタル主権を構成する主要な 3 つの要素「データ主権」「運用主権」「技術主権」に注目し、今回の調査対象国・地域による定義を総合して、下記のように定義する（筆者整理)。

データ主権：データの所在・アクセス権・利用目的・越境移転を、国内法令や組織方針に基づき自ら統制できる状態。施策例は、データ分類と保管場所の要件化（国内/域内保管)、越境移転プロセス、暗号化と鍵管理など。

運用主権：監視・障害対応・変更管理・パッチ適用など日々の運用判断を自組織が主導しつつ、運用を担う人材や事業者の統制（ガバナンス）も含めて自組織（自国）が実効的にコントロールできる状態。施策例は、運用体制の内製/共同運用、委託先監督・監査権、運用者の国籍/居住要件、国内での議決権比率・取締役会所在などの事業者ガバナンス要件、特権 ID の分離など。

技術主権：基盤技術や標準を自ら選択・検証し、必要時に代替や移行ができる能力。施策例は、政府ファンド等で自国企業・研究機関の R&D を推進する政策、OSS 活用と評価・標準 API/データ形式採用、マルチクラウド/ポータビリティ/ベンダーロックイン低減設計、サプライチェーンリスク対策など。

データ主権の代表施策について。EU の CADA 法案は、保証水準に応じて EU 域内でのデータ処理や機微データの域内限定を求める。さらに EU データ法は、第三国政府による法的根拠を欠くデータアクセスからの保護とクラウド事業者間の乗換え（ベンダーロックイン低減）を規定する。フランスの SecNumCloud v3.2 と SREN 法第 31 条は、機微な行政データの EU 域内保存・処理に加え、EU 域外の法律に基づく外国政府からのデータ開示要求等のリスクへの対処を調達・契約要件に反映する。インドの MeitY 認定と RBI 規制は、政府クラウドや決済データの国内所在を制度化し、日本の DS-310 は国内データセンターを基本に、海外設置時の法域・保存性や利用者による暗号鍵管理を点検・評価することを求める。オーストラリアの HCF は機微な政府データの国内保存を求める。これらは、所在・アクセス・移転・暗号鍵を一体的に統制する代表例である。

運用主権の代表的施策について。EU の CADA 法案は、主権保証水準に EU 域内の人員・運用、EU 市民による技術サポート、第三国支配リスクの統制を組み込む。フランスの SecNumCloud v3.2 は、EU 域内からの管理・監督、域外からの技術的アクセス制限に加え、事業者の本店所在と実効支配が EU 域内にあることを求める。ドイツの C3A は、運用要員の国籍・居住地、域内 SOC（Security Operations Center)、遠隔管理経路、非 EU 接続の切断試験、緊急時の運用引継ぎを評価する。オーストラリアの HCF も、クラウド・データセンター事業者の所有・支配、重要要員、リモート支援、供給網を認定対象とする。一方、シンガポールの GCC 2.0 と CloudSCAPE

は、外資クラウドを排除せず、政府共通基盤と準拠状況の自動確認により運用を統制する好例である。

技術主権の代表施策について。EU の European Tech Sovereignty Package は、CADA 法案、Chips Act 2.0 法案、EU Open Source Strategy を束ね、クラウド・AI・半導体・OSS を含む技術スタックと供給網を包括的に強化する。ドイツの C3A は、ソフトウェア部品表（SBOM）による部品把握、外部サービス依存の可視化、EU 域内でのソースコード保全を評価し、代替・移行できる能力を検証可能な基準に落とし込む。インドは国産ソブリンクラウドスタックの研究開発、オーストラリアは政府系ファンドによる主権クラウド投資を進める。これらは、技術を自ら選び、中身を検証し、必要時に乗り換えられる能力を自国・域内に育成する代表例である。

表 2 各国・地域の取組・施策の例（筆者まとめ）

国・地域	データ主権に関する取組・施策	運用主権に関する取組・施策	技術主権に関する取組・施策
EU	データ法：クラウド移行・相互運用性及び域外国政府アクセスへの対応。 CADA の保証水準：EU 域内のデータ処理・機微データの域内限定。	CADA の保証水準：EU 域内の人員・運用、EU 市民による運用・支援、第三国支配リスクの統制。 NIS2・CER・DORA：重要インフラを含む必須・重要事業体及び金融セクターに、リスク管理、監査、業務継続性を求める。	European Tech Sovereignty Package、CADA、Chips Act 2.0、EU Open Source Strategy：クラウド・AI・半導体・OSS 及び供給網能力の強化。
フランス	SecNumCloud v3.2 及び SREN 法第 31 条：機微な行政データの EU 域内保存・処理、域外法アクセスからの保護。	SecNumCloud v3.2：EU 域内からの管理・監督、EU 域外からの技術的・運用的アクセスの統制、EU 域内の本店・実効支配等を要求。ANSSI による監督。 Bleu 等フランス版ソブリンクラウド事業会社。	Cloud au centre、SecNumCloud を通じた信頼できる国内・欧州クラウドの育成。行政端末の Linux 移行等、域外ベンダー依存の低減。
ドイツ	BSI C3A：EU 又はドイツでのデータ保存・処理、外部鍵管理、クライアント側暗号化等を評価。	BSI C3A：運用要員の国籍・居住地、EU/ドイツ域内 SOC、遠隔管理経路、非 EU 接続の切断試験、緊急時の運用引継ぎを評価。 Delos Cloud 等ドイツ版ソブリンクラウド事業会社。	C3A：SBOM、供給者・外部サービス依存の把握、EU 内のソースコード保全・開発環境確保。 C5:2026 のサプライチェーン管理：クラウドサービスの供給網リスクを管理し、技術主権を下支えする。
インド	MeghRaj/NGC 及び Cloud Selection Framework：データ分類に応じた政府管理環境の選定。 MeitY 認定クラウドの国内データ所在。 RBI による決済データの国内保存。	クラウド事業者の NOC/SOC を国内に置くことを求め、政府が監査権・SLA・責任分界・契約終了時のデータ返還・移行を契約上確保する要件。 RBI の外部委託 Directions による取締役会統制、監査権、退出戦略。	MeghRaj 2.0/NGC：政府管理下のハイブリッドクラウド及び AI 対応基盤を整備。 MeitY 系の政府研究機関 C-DAC を中心に、TCS と連携した国産ソブリンクラウドスタックの研究開発・実証を 2025 年から推進。

国・地域	データ主権に関する取組・施策	運用主権に関する取組・施策	技術主権に関する取組・施策
シンガポール	政府データアーキテクチャ（SSOT・Trusted Centres）及びデータ分類に応じた GCC/GCC 2.0・専用環境の使い分け。	GCC/GCC 2.0 、 SGTS 、CloudSCAPE：商用クラウドの利用に、政府横断の標準・共通基盤、準拠状況の自動確認を組み込み、政府が運用を統制できるようにする仕組み。 Cybersecurity Act 改正及び DIA 構想によるクラウド・データセンターの強靭性監督。	SGTS：共通の開発・運用基盤、再利用可能な部品、標準化及び DevSecOps を整備。
オーストラリア	Hosting Certification Framework（HCF）：機微な政府データの国内保存及び、プライバシー・主権・安全性を備えたホスティング環境の認証。	Hosting Certification Framework（HCF）：事業者の所有・支配・運用、重要要員、リモート支援、サプライチェーン及び支配変更を評価。 SOCI 法・ERP 法：重要インフラを対象に、リスク管理及びインシデント報告を求める。	National Reconstruction Fund Corporation による Macquarie Technology Group への 2 億豪ドルの投資：主権クラウド、AI 対応サイバーセキュリティ、主権データ施設及び高度人材を強化。
米国	データの国内保管を求める規定の一例として、DoD Cloud Computing SRG の Impact Level 6（IL6）があり、対象となる国防情報を米国内の施設で処理・保管することを求める。 外国懸念国による米国人機微データ取得を制限するデータセキュリティ政策。	FedRAMP 及び DoD Cloud Computing SRG：影響度別に連邦・国防情報を扱うクラウドを認可。	NIST CSF 2.0 及び CISA Secure by Design：ソフトウェア・クラウドのサプライチェーンリスク管理と安全な設計を促進し、技術主権を下支えする。
日本	DS-310：政府クラウドのデータセンターは国内設置を基本とし、海外設置時は法域・保存性等を確認。暗号鍵をクラウド事業者任せにせず、利用者側で管理する方式（BYOK 等）の採用要否を判断。 統一基準群の情報格付によるデータ分類、DS-910 による機微情報のアクセス制御・暗号化等。	ISMAP：特権アクセス、再委託先、監査、責任分界を評価。 DS-910：利用者が構成・設置場所・運用体制を把握し、運用ガバナンスを確保する自律性を重視。 基幹インフラ制度：特定重要設備の導入・重要維持管理等の委託について、委託先・再委託先への外国からの影響リスクを審査。	経済安全保障重要技術育成プログラム（K Program）「ハイブリッドクラウド利用基盤技術の開発」：安全保障上重要なハイブリッドクラウド利用基盤の研究開発を支援。 さくらのクラウド等の国内クラウド／GPU クラウド基盤：国内におけるクラウド・AI 計算資源の供給能力確保。 防衛調達における情報セキュリティ基準：防衛産業のソフトウェア・部品・委託先を含むサプライチェーンリスクを管理。

日本でも、データ・運用・技術の各要素に関係する制度や取り組みが進められているが、本表に挙げた日本の施策の多くは、主権の確保を明示的な政策目的とするものというより、情報セキュリティ、経済安全保障、安定供給の確保を主目的とする施策として位置づけられる。

各国・地域では、データ主権、運用主権、技術主権のそれぞれについて、何らかの取り組みが進められていることがわかる。ただし、定量的な比較は困難であり、各要素の注力度、制度の拘束力、対象範囲及び実装の成熟度には差がある点は注意が必要である。

３．適用先基準と事業者選定施策

各国・地域の施策を比較すると、デジタル主権に関する取り組みは、大きく２つに分けることができる。「適用先基準や要件定義に関する施策」と「利用可能なクラウドサービスを選定・認可・監査する仕組み」である。

まず「適用先基準や要件定義に関する施策」では、扱うデータやシステムの機微性・重要性に応じて、クラウド利用条件、保証水準、認可水準を段階化するアプローチが代表的であり、EU、インド、アメリカにその例が見られる。EU の CADA 法案は 4 段階の主権保証水準を示し、インドの Cloud Selection Framework は政府データ分類に応じたクラウド利用可否を整理する。アメリカでは、FedRAMP と DoD Cloud Computing SRG が、連邦情報や国防総省データの影響度に応じた認可水準・利用条件を定める。

次に「利用可能なクラウドサービスを選定・認可・監査する仕組み」を見ると、フランスの SecNumCloud、ドイツの C5／C3A、インドの MeitY empanelment、オーストラリアの HCF、アメリカの FedRAMP／DoD SRG は、クラウドサービスの選定・評価・認可・監査、または選定時の確認に関する制度・基準として整理できる。シンガポールの GCC は、正確には事業者認定制度ではないが、商用クラウドを政府利用に適合させる実装・運用基盤である。

日本は、政府統一基準群や ISMAP など、安全なクラウド利用を支える制度を整えている。EU の主権保証水準やフランスの SecNumCloud のような主権クラウド認証の枠組みは設けていないが、セキュリティの確保から段階的に進めているといえる。

表 3 適用先基準と事業者選定施策（筆者まとめ）

国・地域	適用先基準・要件定義に関する施策	クラウド事業者選定・監査に関する施策
EU	**Cloud and AI Development Act（CADA）案の Union assurance levels（4 段階保証水準）**：主権性を 4 段階化し、リスクに応じ必要水準を選択。	**Cloud and AI Development Act（CADA）案の Union assurance levels（4 段階保証水準）**：監査・認定を通じ、主権要件に適合するサービスを選定。 **Cloud Sovereignty Framework**：EU 機関等のクラウド調達に主権性評価を導入した先行的な調達基準。 **EUCS（EU Cloud Services Scheme）**：正式採択前のクラウドサービス向け欧州サイバーセキュリティ認証制度案。
フラン	**ANSSI「機微情報システムのクラウドホスティン**	**SecNumCloud v3.2**：主権性・セキュリティを含む

国・地域	適用先基準・要件定義に関する施策	クラウド事業者選定・監査に関する施策
ス	**グに関する推奨」**：情報の機微性に応じ、利用すべきクラウド形態を整理。 **SREN 法第 31 条・施行令**：機微データの民間クラウド利用条件を法令上具体化。	クラウド事業者資格制度。
ドイツ	**BSI Criteria enabling Cloud Computing Autonomy（C3A）**：法定の適用先分類ではないが、利用者が用途・リスクに応じて自律性・主権性要件を整理する任意基準。	**BSI C5:2026（Cloud Computing Compliance Criteria Catalogue）**：情報セキュリティ管理策を第三者監査で確認する枠組み。 **BSI Criteria enabling Cloud Computing Autonomy（C3A）**：C5 を補完し、クラウド選定時に主権性・自律性を評価する非拘束的基準。
インド	**Guidelines for Cloud Selection Framework（2026）**：政府データの機微性に応じ、利用可能なクラウド形態を分類。	**MeitY empanelment**：政府向けクラウド事業者を認定・登録する制度。 **Guidelines for Procurement of Cloud Services v2.2**：政府機関のクラウド調達・契約・管理の実務基準。
シンガポール	**Government on Commercial Cloud（GCC／GCC 2.0）**：機微性の低い政府システム・データを中心に、商用クラウドを政府共通のセキュリティ・コンプライアンス統制下で利用するための基盤。	**Government on Commercial Cloud（GCC／GCC 2.0）**：事業者認定制度ではないが、選定した商用クラウドを政府利用に適合させる実装・運用基盤。
オーストラリア	**Hosting Certification Framework（HCF）の適用先規定**：政府データの機微性に応じ、認証済みサービス利用を求める。	**Hosting Certification Framework（HCF）の事業者認証・監査側面**：所有・支配・運用等のリスクを評価し認証区分を付与。
アメリカ	（デジタル主権を意図した制度ではない） **FedRAMP の適用先規定**：連邦情報の影響度に応じ認可水準を使い分ける制度。 **DoD Cloud Computing SRG の適用先規定**：国防総省データの機微性に応じ Impact Level を定義。	（デジタル主権を意図した制度ではない） **FedRAMP のクラウドサービス認可／監査側面**：連邦政府向けクラウドサービスを評価・認可・継続監視。 **DoD Cloud Computing SRG のサービス認可・利用条件側面**：FedRAMP に国防総省固有の追加要件を上乗せ。
日本	（デジタル主権を意図した制度ではない） **政府機関等のサイバーセキュリティ対策のための統一基準群**：情報の格付と情報システム重要度を定義。 **DS-910**：機微な政府情報システムの自律性・運用要件を提示。 **DS-310**：クラウド利用時のガバメントクラウド・ISMAP 選定原則。 ***ガバメントクラウド***：行政・自治体システム向け共通クラウド基盤。	（デジタル主権を意図した制度ではない） **ISMAP／ISMAP-LIU**：政府向けクラウドのセキュリティ適合性を監査・登録。

４．日本の課題

日本では、政府統一基準群、ガバメントクラウド、ISMAP など、デジタル主権のベースとなりうる制度要素は存在する。一方で、デジタル主権を横断的に定義し、どの案件にどの要件を適用するかを示す共通指針という形では明文化されていない。そのため現状は、クラウドやデータ基盤の調達・更改において、多くの場合、発注部門が個別案件ごとに必要な要件を判断する運用となっている。本章では、この現状を踏まえ、日本における今後の検討論点を整理する。

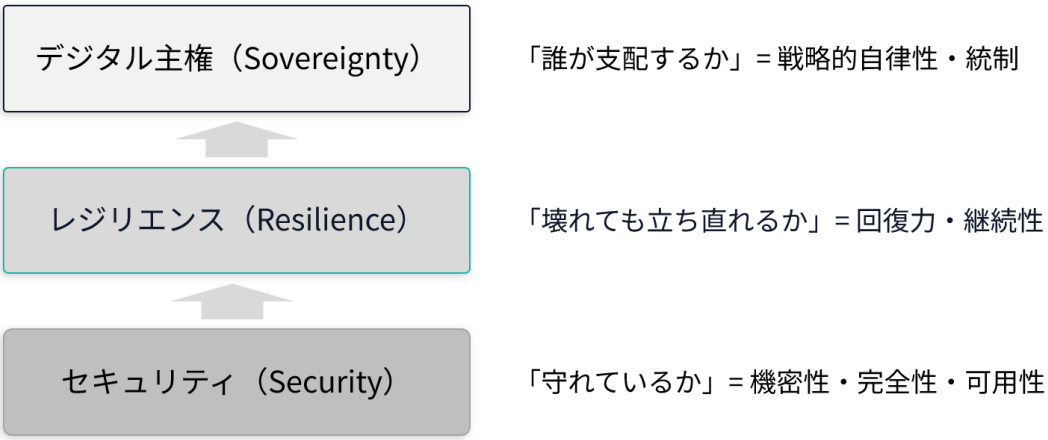


図 1 セキュリティ、レジリエンス、デジタル主権の段階的発展（筆者整理）

各国の施策を見ると、セキュリティ、レジリエンス、デジタル主権へと、段階的に検討領域を広げている。セキュリティは「守られているか」、レジリエンスは「障害等が生じても継続・回復できるか」、デジタル主権は「誰が、どの法域・運用体制の下で統制できるか」を問う考え方である。

日本では、セキュリティを軸とした制度整備が進められてきた。近年は、自然災害やシステム障害への対応に加え、サービス終了、規約変更、外国法令、サプライチェーン、運用継続性など、より広い意味でのレジリエンスも論点となり始めている。一方で、今回の調査対象国と比較すると、デジタル主権を目的・適用基準・事業者評価・実装モデルとして一体的に整理する余地がある。このような状況を踏まえ、今後の検討に向けた主な論点を四つに分けて整理する。

論点１：デジタル主権のねらい

第一の論点は、日本としてデジタル主権を何のために確保するのかである。

今回の多くの調査対象国では、ハイパースケーラーへの過度な依存をクラウド活用に伴う重要なリスクとして認識している。ただし、対応の方向性は国によって異なる。フランスは、機微領域を中心に非欧州技術や域外法リスクへの依存を抑える方針を行政主導で進めている。一方、ド

イツやシンガポールは、ハイパースケーラーの技術を活用しつつ、標準化、監査、運用統制、複数クラウド活用等により、ベンダーロックインや運用上の依存を抑える方向で施策を進めている。

日本においても、依存低減、最新技術活用、行政継続性、国内能力確保など、何を重視するのかを見定めていく必要がある。EU の Cloud Sovereignty Framework のように 8 つの主権目的を明示して調達評価の共通基盤とした例も参考に、日本として重視する目的を明文化し、共有していくことが重要である。

論点２：適用対象

第二の論点は、どのデータ、どのシステム、どの業務にデジタル主権の観点を適用するかである。

日本には、政府統一基準群における情報の格付や基幹インフラ制度における重要設備・重要維持管理等の考え方がある。これらは、適用対象を検討する際の基礎となり得る。一方で、デジタル主権の観点から、どの業務・データにどの程度の国内運用、法域統制、暗号鍵管理、代替可能性を求めるのかについては、案件横断で整理する余地がある。

論点３：事業者選定や監査の考え方

第三の論点は、クラウド事業者や関連事業者を、デジタル主権の観点からどのように評価するかである。

ISMAP は、政府向けクラウドサービスのセキュリティ適合性を評価・登録する制度として重要な役割を果たしている。一方で、デジタル主権の観点では、データ所在、運用者、暗号鍵、外国法令リスク、再委託、移行性、継続監査なども重要な論点となる。現状では、これらの主権関連論点をどの程度まで事業者選定や監査に反映するかについて、案件ごとの判断に委ねられている面がある。

論点４：実装モデルの蓄積

第四の論点は、日本国内において、デジタル主権を明示的に意識したクラウド・データ基盤の実装モデルがまだ十分に蓄積されていないことである。

ドイツの Delos Cloud やフランスの Bleu は、ハイパースケーラーの技術を活用しつつ、国内運用、法域統制、監査可能性などを組み合わせようとする先行事例である。これらは、デジタル主権を「外国クラウドを使うか使わないか」という二分法ではなく、どのように統制可能性を確保するかという設計課題として捉えている点で参考になる。日本でも、重要領域を対象としたフラッグシッププロジェクトを組成し、統制可能性や代替可能性を、実践を通して具体的に検証していくことが重要である。

日本は、デジタル主権のベースとなる制度要素を既に多く持っている。一方で、それらを横断的な政策として体系化し、案件ごとの判断を支える共通の考え方として整理する余地がある。今後は、デジタル主権をクラウド活用の制約としてではなく、行政・社会機能の継続性、重要データの保護、運用・法域の説明可能性を高めるための検討軸として位置づけ、日本として何を重視するのかを見定め、共有していくことが求められる。

以上