

2025 年 11 月 19 日 全 8 頁

世界が再注目、実現に動き出すソブリン AI

日本の AI 基本計画が描く データ主権と技術的自立への道筋

経済調査部 主任研究員 田邊 美穂

[要約]

- AI 技術の急速な進化を背景に「ソブリン AI」が再び注目されている。ソブリン AI とは、国や企業が自国・自社のデータや技術基盤を活用し、外部への依存を最小限に抑えつつ AI システムを自立的に開発・運用する能力を指す。その根幹には、「データ主権」や「技術的自立性」の確保を目指し、自らのデータを自国・自社で管理・運用するという戦略的な姿勢がある。
- 国や企業は AI を戦略的に活用する段階へと移行しつつある。その結果、①データ主権および安全保障の確保、②技術的自立性の確保、③国内産業の強化、④文化・社会的適合性の確保など、AI 技術を外部へ依存することによる多面的な課題が浮上してきた。米中による技術覇権争いが続く中、EU や韓国など第三国では、AI 基盤モデルの開発力強化やインフラ整備、人材育成などを柱とした政策的取り組みが加速している。
- 日本においても、信頼できる AI の開発支援を盛り込んだ「人工知能基本計画（AI 基本計画）」の策定が進められている。骨子では、技術的自立性の確保を目指し、日本語や産業データの整備、民間連携による研究開発体制、高性能 AI 半導体などのインフラ強化などが挙げられている。これらの取り組みを通じて、国内の AI エコシステムの構築および国際競争力の強化を図る方針だ。
- 実現に向けては、技術・人材・資金面で多くの課題がある。AI 関連技術の優位性の獲得・維持には継続的な研究開発が不可欠であり、必要な環境の整備や運用コスト、人材確保などの負担も大きい。民間企業が単独で持続的な体制を構築するには限界がある。今後は、国際的なルール形成や、他国との連携・協力を通じた競争力強化と技術的自立性の確保の両立を目指しつつ、官民が連携して AI エコシステムを構築し、実効性のある制度運営を通じて競争力を高めていくことが重要となる。

1. はじめに

「ソブリン AI」という言葉をニュースや専門メディアで目にする機会が、ここ最近増えてきた。ソブリン AI 自体は、生成 AI が話題になった 2023 年頃には既に存在していた概念であり、当時も話題となっていた。しかし、AI 技術の飛躍的な進化と社会的インパクトの拡大を背景に、各国政府や企業が自国主導の AI を戦略的に位置づける動きが今再び加速している。

こうした動きの背景には、AI の性能向上により、機密性の高い領域での実用化が現実味を帯びてきたことがある。AI が社会の中核的なインフラとして組み込まれる可能性が高まる中で、機密データの保護や技術の自立性を確保する必要性が強く意識されるようになってきた。さらに、データ主権や安全保障、そして自国の言語・文化に根ざした AI 開発による文化的自立といった複数の要因が、現実のリスクとして認識されるようになり、国家戦略としての対応が急務となりつつある。

本レポートでは、ソブリン AI の概念と世界的な動向を整理した上で、日本の現状および今後の情報社会における AI 戦略のあり方について考察する。

2. 各国でソブリン AI に向けた政策的取り組みが進む

ソブリン AI とは：「データ主権」と「技術的自立性」の確保を目指す

ソブリン AI に関する国際的に統一された公式な定義は現時点では存在しないが、一般的には、「**国や企業が自国・自社のデータ、技術基盤、インフラを活用し、外部への依存を最小限に抑えつつ、AI システムを自立的に開発・運用する能力**」として理解されている。

ここでいう AI システムとは、AI モデル単体にとどまらず、データの取得・処理、計算インフラ、運用体制、セキュリティ管理などを含む、AI 技術を活用したサービス全体を指す。一部には、「国産 AI モデル＝ソブリン AI」といった狭義の定義も見られるが、実際にはより広範な技術・運用基盤を含む概念である。

ソブリン AI の根幹には、「データ主権」や「技術的自立性¹⁾」の確保を目指し、自らのデータを自国・自社で管理・運用するという戦略的な姿勢がある²⁾。

ソブリン AI が再注目される背景：AI 技術の急速な進化による環境の変化

ソブリン AI が再び注目される背景には、AI 技術の急速な進化により、国や企業が AI を戦略

¹⁾ 技術的自立性とは、外部に依存せず、自国で必要な技術を確保できる状態を指す。

²⁾ ソブリン AI は、自国または自社での完全自給を目指すものではなく、むしろ戦略的に国内製品・サービスを選択・活用し、外部（特に海外の製品・サービス）に依存することで生じるリスクを最小化することを目的としている。前提として国内製品・サービスの選択肢を確保するための技術力強化は不可欠だが、外部の活用を排除するものではない点に留意されたい。

的に活用する段階へと移行しつつあることが挙げられる。こうした状況の中で、以前から指摘されていた AI システムを外部に依存することで生じる社会的・経済的な課題（図表 1）が、より差し迫ったものとして認識されるようになってきた。

1 つ目の課題として、**データ主権および安全保障の確保**がある。国や企業が AI 活用を本格的に進めるにあたり、これまで対象としていなかった機密性の高い情報やデータを含めた活用を検討せざるを得ない段階に入ってきている。以前から問題視されてきたように、海外のクラウドサービスや外部 AI 基盤にデータの管理・運用を依存する場合、機密情報や個人データが国外に流出するリスクや、他国の法規制・政策変更による影響を受けるリスクがある。

特に国が活用する場合、緊急時や国際的な摩擦が生じた際に、サービスの停止やデータアクセスの制限などが起これば、安全保障上の脅威となり得る。日本でもガバメントクラウドの整備が進められているが、採択された事業者のうち日本企業はさくらインターネット株式会社のみであり、その他はすべて海外企業である³。こうしたリスクを確実に回避するためにも、自国・自社でデータを管理し、必要なときに自由にアクセス・活用できる体制の確立は、データ主権の維持と安全保障の観点から不可欠となる。

2 つ目の課題として、**技術的自立性の確保**がある。現状、AI モデルの開発やその関連技術は、主に米中が牽引しており、両国による技術覇権争いは他国と比較しても抜きんできている。そのため日本を含む第三国が、AI の活用において施策的に優れた技術を選択しようとする、外部技術に依存せざるを得ない状況が続いている。実際に、国際的な技術流通に関するリスク（半導体の輸出規制など）は、以前から問題視されてきた。

こうした状況の中、直近では高性能なオープンソース LLM（大規模言語モデル）の登場により、技術情報が広く公開され、国際的な開発エコシステムが形成されつつある⁴。これにより、技術の民主化⁵が進み、得られた知見を活用することで、高性能な LLM の開発が以前より容易になってきている。こうした環境の変化は、自国で AI 関連技術を自立的に開発・運用するための敷居を下げ、技術的自立性の確保を目指す動きを後押しするだろう。

3 つ目の課題として、**国内産業の強化**がある。AI 技術や関連インフラは、製造業、金融、医療などの重要産業の安定的な運営ならびに国際競争力の維持・向上に不可欠な要素として注目されている。今後 AI の適用領域が拡大することが予想される中、国内産業の競争力強化や新たなイノベーション創出も一層重要となる。

こうした状況では、AI 技術の研究開発及び運用に精通した人材のみならず、実務レベルで AI をビジネス活用できる多様な人材育成が不可欠である。自国で AI および関連インフラの開発・

³ ガバメントクラウドのサービス事業者（CSP）には、政府情報システムのためのセキュリティ評価制度（ISMAP）に基づき、データ保存場所が国内であることや国外移転の制限、外国政府への開示禁止などの要件が課されている。

⁴ 2025 年 1 月に DeepSeek が高性能なオープンソース LLM を発表し、DeepSeek ショックを引き起こしたことは記憶に新しい。以降、LLM に関する主要な性能評価ランキングにおいて、オープンソース LLM が多く登場するようになってきており、技術のオープン化と民主化の流れが一層加速している。

⁵ 技術の民主化とは、特定の国や企業だけでなく誰もがその技術を使えるようになる状態を指す。

運用体制を構築することは、現場における実践経験やノウハウの蓄積が期待されるほか、産業自体の活性化やイノベーションの促進につながる。また、こうした環境が整うことで、優秀な人材の海外流出を防ぎ、国内に人材を定着させる効果も期待される。

4 つ目の課題として、**文化・社会的適合性の確保**がある。AI 技術の普及が進む中で、日本語や国内の文化、社会的価値観に適合した AI モデルの開発・運用が求められている。例えば、日本でも利用者の多い米国発の AI モデルは多言語対応しているものの、学習データの多くは英語が中心のため、生成された結果に欧米の価値観や文化的前提が反映されやすい傾向がある。

また、AI モデルは開発国の法規制や思想が反映されることもある。DeepSeek ショックの際に、天安門事件についての回答を避ける事例などが話題となったように、開発国の政治的意向や検閲方針が意図的に組み込まれるケースも指摘されている⁶。このような背景から、自国の文化や社会的背景に根ざした AI モデルの開発・運用は、国内ユーザーのニーズに合ったサービス提供や、社会的受容性・信頼性の向上につながると考えられる。

このように AI 技術の進化とその活用が社会・経済・産業・文化に浸透しつつある結果、各側面で新たな課題やリスクが顕在化している。そこで、自国の主権や価値観を守りつつ、持続的な競争力と社会的信頼性を確保するための戦略として、ソブリン AI が今、改めて注目されている。

図表 1 ソブリン AI が再び注目される 4 つの理由

データ主権および安全保障の確保

海外のサービスや製品にデータの管理・運用を依存する場合

- ➡ 機密情報や個人データが国外に流出するリスク
他国の法規制・政策変更による影響を受けるリスク

自国・自社でデータを管理し、
必要ときに自由にアクセス・活用できる体制の確立



技術的自立性の確保

AI の活用において施策的に優れた技術を選択しようとすると、
外部技術に依存せざるを得ない状況

- ➡ 半導体の輸出規制など、国際的な技術流通に関するリスク

国際的な開発エコシステムの形成などオープン化の流れが、
AI 関連技術を自国で自立的に開発・運用する動きを後押し



国内産業の強化

製造業、金融、医療などの重要産業の安定的な運営ならびに
国際競争力の維持・向上に不可欠な要素

- ➡ 国内産業の競争力強化や新たなイノベーション創出も
一層重要となる

AI 技術の研究開発及び運用に精通した人材のみならず、
実務レベルで AI をビジネス活用できる多様な人材育成が不可欠



文化・社会的適合性の確保

利用者の多い米国発の AI モデルは多言語対応しているものの、
学習データの多くは英語が中心

- ➡ 欧米の価値観や文化的前提が反映されやすい傾向
政治的意向や検閲方針が意図的に組み込まれるケースも

AI 技術の普及が進む中で、日本語や国内の文化、
社会的価値観に適合した AI モデルの開発・運用が求められる



(出所) 大和総研作成 (イラストはソコスト (<https://soco-st.com/>))

⁶ 日本経済新聞「DeepSeek の AI 試してみた 中国政治や『天安門』に回答」(2025 年 2 月 1 日)

諸外国でも進む、AI 技術の自立性を重視した政策的取り組み

各国の直近の動向を見ても、ソブリン AI の概念と方向性に親和性のある政策的取り組みが多く打ち出されていることがわかる。

欧州連合（EU）では、2025 年 4 月に「AI 大陸行動計画（AI Continent Action Plan）」を発表⁷し、欧州域内での AI 基盤モデル（LLM など）開発・運用能力の強化や、スーパーコンピュータ、AI チップ、データセンターなどの AI インフラ拡充を柱とした政策を打ち出している。これは、欧州が米中の AI に依存しない技術的自立性の確立を目指すものであり、同年 10 月には、この計画を進めるための 2 つの戦略も公表している⁸。

加えて、EU 加盟国の中でも独自に国家戦略や国内法を制定し、自国発の AI 基盤モデル開発や産業支援策を進める動きが見られる。実際に、フランスの AI スタートアップ企業 Mistral AI 社が開発した LLM は、高い性能と応答性を示し、国際的な評価を受けている。

またアジアに目を向けると、韓国では世界トップ 3 の AI 強国を目指す方針のもと、2025 年 9 月に「国家 AI 戦略委員会」が発足した⁹。同委員会は、AI 政策の司令塔として、AI アクションプランの策定、AI 関連予算の調整、国際連携の推進などを担う。アクションプランでは、AI インフラの整備や次世代技術の確保、人材育成、国産 AI モデルの開発支援などを含む 3 つの政策軸と 12 の戦略分野が示されており、同年 11 月を目途に具体的な実行計画の策定が進められている。また既に、Upstage 社の Solar や LG AI Research の EXAONE など、国際的な評価の高い AI モデルが複数登場している。

3. 日本でも技術的自立性を意識した取り組みが始まる

日本における AI 戦略、政府が策定を進める AI 基本計画とは

日本政府も、AI 技術の急速な進展と国際競争の激化を受け、国家戦略の構築を本格化させている。2025 年 9 月には AI 戦略本部において、信頼できる国産 AI の開発支援などを盛り込んだ「人工知能基本計画（以下、AI 基本計画）」の骨子が提示された¹⁰。これは、同月 1 日に全面施行された「人工知能関連技術の研究開発及び活用の推進に関する法律（AI 法）」¹¹に基づき、政府が策定を進める国家戦略であり、年内の正式決定を目指している。

この AI 基本計画（骨子）では、「世界で最も AI を開発・活用しやすい国」を目指すと掲げられており、①AI 利活用の加速的推進（「AI を使う」）、②AI 開発力の戦略的強化（「AI を創る」）、

⁷ European Commission “[Commission sets course for Europe’s AI leadership with an ambitious AI Continent Action Plan](#)”, April 9, 2025.

⁸ European Commission “[Commission launches two strategies to speed up AI uptake in European industry and science*](#)”, October 8, 2025.

⁹ Ministry of Science and ICT “[National AI Strategy Committee Launched as Korea’s Top-Level AI Policy Body](#)”, September 16, 2025.

¹⁰ 内閣府「[人工知能基本計画骨子（案）](#)」（令和 7 年 11 月 4 日）

¹¹ 内閣府「[AI 法 全面施行 一次なるフェーズへ](#)」（2025 年 10 月 3 日）

③AI ガバナンスの主導（「AI の信頼性を高める」）、④AI 社会に向けた継続的変革（「AI と協働する」）の4つを基本方針としている（図表2）。

図表 2 AI 基本計画（骨子）の4つの基本方針

AI利活用の加速的推進（AIを使う）

日本社会全体で、世界最先端のAI技術を、適切なリスク対応を行いながら積極的に活用することで、新たなイノベーションを創出する

【具体的な取り組み例】

- ・ 政府・自治体でのAIの徹底した利活用
- ・ 社会課題解決に向けたAI利活用の推進
- ・ AI利活用推進で新しい事業や産業を創出
- ・ 更なるAI利活用に向けた仕組みづくり

AI開発力の戦略的強化（AIを創る）

インフラからアプリまでのAIエコシステムに関する各層での開発を進めつつ、それらを有機的に組み合わせることで、日本の強みとして「信頼できるAI」を開発

【具体的な取り組み例】

- ・ 日本国内のAI開発力の強化
- ・ 日本の勝ち筋となるAIモデル等の開発推進
- ・ 信頼できるAI基盤モデルの開発
- ・ AI開発・利用基盤の増強、確保

AIガバナンスの主導（AIの信頼性を高める）

人とAIが協働し、イノベーションの好循環を実現するために、AIの適正性を確保するガバナンスを構築

【具体的な取り組み例】

- ・ 信頼できるAIエコシステムの構築
- ・ グローバルサウスを含めた国際協調

AI社会に向けた継続的変革（AIと協働する）

人とAIが協働する社会の実現のため、産業や雇用のあり方、制度や社会の仕組みを先導的かつ継続的に変革

【具体的な取り組み例】

- ・ AIを基軸とした産業構造の構築
- ・ AI社会における枠組みの検討・実証
- ・ AI人材の育成・確保
- ・ AI時代における人間力の向上支援

（出所）内閣府「人工知能基本計画骨子（案）」（脚注10）pp. 5-12 より、大和総研作成

データ主権や技術的自立性の確保に向けた日本の戦略的アプローチ

特に、②AI 開発力の戦略的強化において、日本の文化や習慣などを踏まえた「信頼できる AI」の開発が掲げられている。その実現には、日本が独自に AI エコシステムを研究および開発する能力の強化が不可欠となる。具体的な取り組み例としては、日本語データや産業データをはじめとする高品質なデータの整備および連携基盤の構築、民間の連携・協働を促進する研究開発体制、高性能 AI 半導体などの AI インフラに関連する技術の研究及び開発、さらにデータセンターなどの AI 開発・利活用基盤の増強・確保などが挙げられている。

こうした取り組みを通して、AI 関連分野における国内の自立性を高めるとともに、構築した AI エコシステムを海外に展開することで、国際競争力の強化を図ることも期待されている。こうした方向性は、自国の技術基盤と文化的背景に根ざした AI の整備につながるものであり、「データ主権」や「技術的自立性」を重視したソブリン AI の概念と重なる部分がある。

また、この AI 基本計画（骨子）では、AI の新たな技術動向として注目される「フィジカル AI」を日本の勝ち筋の1つとして位置づけている¹²。AI ロボットの公的需要創出を含めたフィ

¹² フィジカル AI の動向については、田邊美穂[2025]「[フィジカル AI の進展で注目の人型ロボット：日本はロボット技術の優位性を武器に AI 分野で存在感を示せるか](#)」大和総研レポート（2025 年 9 月 1 日）を参考にされたい。

ジカル AI の開発・実証の促進が掲げられており、この点からも計画の実行に求められるスピード感がうかがえる。

AI 利活用の拡大により重要性を増す国内の基盤整備

さらに、①AI 利活用の加速的推進では、まずは政府自らが積極的かつ先導的に AI を利活用することを挙げている。行政業務においては、令和 7 年度の「デジタル社会の実現に向けた重点計画」¹³にも記載されている「ガバメント AI」の推進による効率化が期待されているほか、医療、介護、農林水産業など、社会課題の解決に資する幅広い分野への導入促進が検討されている。

これらの分野には、国民の安全・安心の確保や安全保障の高度化に関わる領域も多く含まれており、今後、こうした分野での AI 利活用が進むにつれ、より機密性の高い情報を扱うことが想定される。そのため、政府が安心して AI を活用できる環境として、セキュリティや法制度面での対応が可能な水準を備えた国産クラウドや国産 AI の整備が、データ主権を確保するうえでも、より重要な課題として浮上してくるだろう。

4. AI 戦略の実現に向け、官民連携が鍵となる

先述の通り、「ソブリン AI」という表現を直接使用してはいないものの、各国においては自国主導による AI システムの開発および運用能力の確立を目指した施策が展開されている。日本においても、AI 基本計画の年内正式決定に向けた議論が進められているが、技術面・人材面・資金面において、依然として多くの解決すべき課題が残されている。

技術面では、AI モデルの開発に必要となる計算資源（高性能 AI 半導体など）やクラウド基盤などについては大半を海外に依存しており、その確保が喫緊の課題となっている。特に、民間企業が単独で十分な計算資源を整備することは容易ではなく、電力コストや設備投資などの運用面の負担も大きいことから、官民連携によるインフラ整備が求められる。

一方で、進んでいる点もある。経済産業省と NEDO¹⁴が推進する「GENIAC (Generative AI Accelerator Challenge)」では、2024 年から国産生成 AI の基盤モデル開発力の強化を目的に、計算資源の提供支援やデータ利活用の実証支援などを継続して行っており、国内の AI 基盤モデルの技術力向上に貢献している。また、日本の文化や習慣などを踏まえた信頼性の高い AI 基盤モデルの開発に必要な良質な日本語データとしては、国立研究開発法人情報通信研究機構（以下、NICT）が保有する日本語に特化した学習データが既に存在している点も大きい。2025 年 9 月には、この NICT と、AI 基盤モデル開発などを手掛ける株式会社 Preferred Networks、クラウド基盤などを提供するさくらインターネット株式会社の 3 者が集まり、国産生成 AI のエ

¹³ デジタル庁「[デジタル社会の実現に向けた重点計画](#)」（2025 年 6 月 13 日）

¹⁴ 国立研究開発法人新エネルギー・産業技術総合開発機構

コシステム構築を目指す基本合意の締結を発表しており¹⁵、信頼性の高い国産 AI モデルの実現が期待される。

資金面の課題においては、AI 関連分野の技術は日々進歩しており、技術的優位性を獲得・維持するためには継続的な研究開発が求められる。だが、仮に技術優位性を持つ製品やサービスが開発できたとしても収益の見通しは立てにくい。また、技術面での課題でも挙げた計算資源などの確保にかかるコストや、これらの研究開発を支える人材確保に係るコストなど、多くの費用負担が想定される。そのため、民間企業が単独で AI 関連分野への大規模投資を継続的に行うための財源を確保することは、現実的に難しいといえる。官民連携による資金支援や、民間投資を呼び込むための制度設計が重要な課題となる。

そして人材面においては、この研究開発を支える AI 研究者やエンジニアといった人材をどのような確保するかが課題となる。先述の AI 基本計画（骨子）では、国内外からトップ人材を集約するための待遇面や生活環境を含めた包括的な取り組みを具体例として挙げているが、こうした人材の確保に向けては、国による支援が不可欠となるだろう。

このように、ソブリン AI の実現、すなわち自国で開発および運用する能力の確保は、現時点では容易ではない。海外の技術や知見も柔軟に取り入れつつ、重要な技術を優先して技術的自立性の確保を目指し、国際的なルール形成や他国との連携・協力によって競争力を強化する、戦略的自立と国際協調の両立を図ることが現実的な方向性といえるだろう。日本の強みである高品質な日本語データは、日本語特化型の AI モデル開発において不可欠な要素であり、信頼性の高い応答を可能にする基盤となる。また、医療や製造などの分野で蓄積された高品質な産業データや高い現場実装力は、フィジカル AI をはじめとする業務特化型 AI の開発に活かすことが期待される。こうした強みを戦略的に活用することで、日本が国際競争力を獲得していくことが求められる。

そのためには、官民連携による AI エコシステムの形成が不可欠である。政府による制度整備や支援策の強化とともに、民間企業・研究機関・自治体などが連携し、開発・利活用・人材育成の各面で持続可能な体制を構築していくことが求められる。日本では、高市政権においても成長戦略会議にて、総合経済対策に盛り込むべき重点施策の 1 つに AI・半導体分野を挙げ、成長戦略の検討を進めている。また、AI 基本計画が今まさに策定されようとしている段階にある。策定した計画を着実に進めていくための実効性のある制度設計と政策運営が、今後の競争力確保に向けた鍵となる。

以上

¹⁵ NICT プレスリリース「[Preferred Networks、さくらインターネット、情報通信研究機構、安心安全で日本社会と調和する国産生成 AI のエコシステム構築に向け、基本合意を締結](#)」（2025 年 9 月 18 日）