IISE 調査研究レポート（No.8）

「米国 AI 行動計画と日米欧 AI 政策比較」

（2025 年度「AI 推進およびプライバシーを巡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）

2025 年 9 月

国際社会経済研究所　主幹研究員　小泉 雄介

1．米国 AI 行動計画

1．1　米国 AI 行動計画の概要

米国ホワイトハウスは 2025 年 7 月 23 日、AI 行動計画「AI 競争に勝利する：米国 AI 行動計画」[1]（米国 AI アクションプラン）を公表した。これは、トランプ大統領が就任早々に発布した大統領令「AI における米国リーダーシップの障壁の除去」[2]（大統領令 14179 号、2025 年 1 月 23 日）に基づくものである。「AI 競争に勝利することは、米国民にとって、人類の繁栄、経済競争力、国家安全保障の新たな黄金時代をもたらす」[3]としている。同行動計画は、「AI イノベーションの加速」、「米国製 AI インフラの構築」、「国際的な AI 外交と AI セキュリティの主導」という 3 つの大項目にわたって、トランプ政権が今後数週間から数か月間に取り組む 90 以上の連邦政策措置（施策）を特定している。

米国 AI 行動計画の作成者は、大統領令での指名のとおり、マイケル・J・クラティオス科学技術担当大統領補佐官（APST）、デイビッド・サックス AI・暗号担当特別顧問、マルコ・ルビオ国家安全保障問題担当大統領補佐官（APNSA）の 3 名となっている。

ホワイトハウスは、米国 AI 行動計画の主要なポリシーを以下としている[4]。

- 米国製 AI の輸出：商務省と国務省は産業界と連携し、ハードウェア、AI モデル、ソフトウェア、アプリケーション、標準規格を含む、安全なフルスタック AI 輸出パッケージを世界中の米国の友好国や同盟国（allies、友好国）に提供する（それにより中国の影響力拡大を阻止する）。
- データセンターの迅速な構築の促進：データセンターと半導体工場の許可を迅速化および近代化するとともに、電気技術者や空調設備技術者などの需要の高い職業を増やすための新しい国家的な取組みを創出する。
- AI イノベーションと導入の促進：AI の開発と展開を妨げる煩雑な連邦規制を撤廃し、撤廃すべきルールについて民間部門からの意見を求める。
- フロンティアモデルにおける言論の自由の擁護：連邦政府の調達ガイドラインを更新し、システムに客観性がありトップダウンのイデオロギー的偏向（民主党政権が進めた Woke 的価

[1] https://www.whitehouse.gov/wp-content/uploads/2025/07/Americas-AI-Action-Plan.pdf。
[2] https://www.whitehouse.gov/presidential-actions/2025/01/removing-barriers-to-american-leadership-in-artificial-intelligence/。
[3] https://www.whitehouse.gov/articles/2025/07/white-house-unveils-americas-ai-action-plan/。
[4] 同上。

値観へのバイアス）がないことを保証するフロンティア LLM 開発者とのみ連邦政府が契約することを保証する。

また、AI 行動計画の全体構成は下図のとおりである。

図表 1　米国 AI 行動計画の全体構成（出典：米国大統領府資料に基づき筆者作成）

- はしがき
- 序文
- Pillar I：AIイノベーションの加速
- ○お役所仕事（rad tape）と煩雑な規制の廃止
- ○フロンティアAIが言論の自由と米国の価値観を守ることを保証する
- ○オープンソースとオープンウェイトのAIを奨励する
- ○AI導入を可能にする
- ○AI時代における米国労働者のエンパワーメント
- ○次世代製造業をサポートする
- ○AIを活用した科学への投資
- ○世界クラスの科学データセットの構築
- ○AI科学を進歩させる
- ○AIの解釈可能性、制御、堅牢性のブレークスルーへの投資
- ○AI評価エコシステムの構築
- ○連邦政府におけるAI導入の加速
- ○国防総省におけるAI導入の推進
- ○民間および政府のAIイノベーションを保護する
- ○法制度における合成メディアへの対策
- Pillar II：米国製AIインフラの構築
- ○データセンター・半導体製造施設・エネルギーインフラへの効率的な許可制度を構築すると共に、セキュリティを保証する
- ○AIイノベーションのペースに合った電力網の構築
- ○米国の半導体製造業の復興
- ○軍事および諜報コミュニティ向け高セキュリティ・データセンターの構築
- ○AIインフラのための熟練労働者の訓練
- ○重要インフラのサイバーセキュリティ強化
- ○セキュア・バイ・デザインのAI技術とアプリケーションの推進
- ○AIインシデント対応における連邦政府の成熟した能力の促進
- Pillar III：国際的なAI外交とAIセキュリティの主導
- ○同盟国およびパートナー国への米国製AIの輸出
- ○国際ガバナンス機関における中国の影響への対抗
- ○AIコンピューティングの輸出管理執行の強化
- ○既存の半導体製造輸出規制の抜け穴を塞ぐ
- ○保護措置の世界的な整合
- ○米国政府がフロンティアモデルにおける国家安全保障リスクの評価において最前線に立つことを保証する
- ○バイオセキュリティへの投資

1．2　米国 AI 行動計画の主な内容

トランプ政権の取る政策は、基本的に以下の 3 つに対する「剥き出しの対抗心・敵愾心」が元になっている（すなわち行動原理となっている）と考えると理解しやすい。それは、①米国の覇権を脅かす中国政府・中国企業、②前バイデン政権・民主党政権、③（トランプの考える）国際金融資本や大手メディアなどの「影の政府」である。

今回の米国 AI 行動計画について、上記 3 つの観点に安全面の観点を加えた 4 つの観点から内容を整理したい。

（1）ライバル国・中国への対抗

- データセンター・半導体製造施設・エネルギーインフラに対する効率的な許可制度の構築、環境規制の見直し
- ハードウェア（半導体を含む）・AI モデル・ソフトウェア・アプリケーション・標準規格を米国製 AI としてパッケージ化して友好国に輸出
- 半導体チップの位置検証機能の活用などを通じた中国への半導体輸出規制の実効性強化

（2）バイデン政権の政策の否定

- AI イノベーションと導入を阻害する煩雑な手続きの連邦規制の廃止
- 煩雑な手続きの AI 規制を導入する州には AI 関連資金提供を制限するが、「イノベーションを過度に制限しない賢明な州法」は許容

- イデオロギー的偏向（Woke 的 DEI 価値観）のないフロンティア LLM 開発者とのみ連邦機関は契約
- NIST の AI リスク管理フレームワークを改訂し、誤情報・多様性・公平性・包摂性・気候変動への言及を削除
- バイデン政権下で FTC 前委員長が推し進めた GAFAM に対するプラットフォーマー規制や決定の見直し

（3）米国労働者ファースト
- 実体経済から乖離して巨大化した金融経済への「当てつけ」として、成長から取り残された労働者の支援を強調
- AI 関連インフラを担う旧来型の技術職（電気技術者、空調設備技術者等）の雇用拡大、労働者の再訓練の機会拡大

（4）AI リスクへの対処
- AI に起因する新たなリスクや予期せぬリスクの監視
- AI 開発企業と協力し、フロンティア AI による CBRN（化学・生物・放射線・核）兵器の開発やサイバー攻撃等の国家安全保障リスクを評価
- AI の解釈可能性、AI の制御、敵対行動に対する堅牢性への投資

（1）ライバル国・中国への対抗

米国 AI 行動計画は、世界的 AI 競争における米国のリーダーシップ維持を呼びかけたトランプ AI 大統領令において策定を指示されたものであり、行動計画の序文でも「AI 競争に勝利することは、米国民にとって、人類の繁栄、経済競争力、国家安全保障という新たな黄金時代をもたらす」とされ、AI により新たな産業革命・情報革命・ルネサンスが引き起こされるとする。その AI 競争の最大のライバルが中国である。そのため、（バイデン政権時代の煩雑な規制で AI 開発を縛ることを見直し）、データセンター・半導体製造工場・電力網といった AI 開発を支えるインフラの構築を容易化し、ハードウェア（半導体を含む）・AI モデル・ソフトウェア・アプリケーション・標準規格などを米国製 AI としてパッケージ化して友好国に広範に輸出しようとしている。また、半導体チップの位置検証機能の活用などを通じて、中国への半導体輸出規制の実効性を高めようとしている。グローバルサウスの国々としては、実質的に米国製 AI か中国製 AI かの二者択一を迫られる状況に置かれている。

・データセンター・半導体製造施設・エネルギーインフラに対する効率的な許可制度の構築、環境規制の見直し

具体的には、「〇データセンター・半導体製造施設・エネルギーインフラへの効率的な許可制度を構築すると共に、セキュリティを保証する」の項目で、「AI には新たなインフラが必要となる。半導体チップ製造工場、それらのチップを稼働させるデータセンター、それらすべてを動か

す新たなエネルギー源である。米国の環境許可制度やその他の規制により、必要なスピードで米国内においてこれらのインフラを構築することはほぼ不可能となっている。さらに、これらのインフラは、米国の AI 優位性を損ないうる敵対的な技術を用いて構築されてはならない」との認識の上で、これらの AI 関連インフラの迅速な構築のために様々な環境規制を緩和させ、環境許可を簡易化させ、「連邦政府の土地をデータセンター建設およびデータセンター用の発電インフラの建設に利用できる」ようにする施策を掲げている。また、「敵対者がこれらのインフラにセンシティブなインプットを挿入することを阻止するためのセキュリティガードレールを維持する。国内の AI コンピューティング・スタックが米国製品に基づいて構築され、エネルギーや通信などの AI 開発を支えるインフラが、ソフトウェアや関連ハードウェアを含む外国の敵対的な情報通信技術・サービスを含んでいないことを保証する」と、AI開発・展開用の計算資源を米国製品で構築し、その他の AI 関連インフラ（エネルギーや通信など）から中国製品を排除することが謳われている。

「〇AIイノベーションのペースに合った電力網の構築」の項目では「将来のデータセンターやその他のエネルギー集約型産業を支えるためには、電力網のアップグレードも必要」とし、「〇米国の半導体製造業の復興」の項目では「米国は半導体製造業を米国本土に戻さなければならない」としている。

・ハードウェア（半導体を含む）・AI モデル・ソフトウェア・アプリケーション・標準規格を米国製 AI としてパッケージ化して友好国に輸出

「〇同盟国およびパートナー国への米国製AIの輸出」の項目では、「米国は、AIに対する世界的な需要を満たすため、ハードウェア、AI モデル、ソフトウェア、アプリケーション、標準規格を含むAI技術スタック全体を、米国のAI同盟への参加を希望するすべての国に輸出しなければならない。この需要に応えられなければ、自滅的なミスとなり、これらの国々はライバル国に目を向けることになる。米国製技術の普及・拡散は、戦略的ライバル国が友好国を外国の敵対的技術に依存させることを阻止するだろう」と中国への敵愾心を剥き出しにし、「商務省内に、産業界コンソーシアムからフルスタックAI輸出パッケージの提案を集めるためのプログラムを設立」するという施策を掲げている。

「〇国際ガバナンス機関における中国の影響への対抗」の項目でも、「国連、OECD、G7、G20、国際電気通信連合（ITU）、ICANN など、多くの国際機関が AI ガバナンスの枠組みや AI 開発戦略を提案している。米国は、共通の価値観に沿って AI 開発を促進するために、志を同じくする国々が協力することを支持する。しかし、これらの取組みの多くは、煩雑な規制や、米国の価値観に合致しない文化的アジェンダを推進する曖昧な「行動規範」を提唱したり、顔認識や監視の標準規格策定を試みる中国企業の影響を受けたりしている」として、国際機関での中国企業の影響を危惧するとともに、バイデン政権下で進められたDEI的な価値観の混入や、煩雑な規制手続きの擁護を「是正」しようしている。

・半導体チップの位置検証機能の活用などを通じた中国への半導体輸出規制の実効性強化

「〇AI コンピューティングの輸出管理執行の強化」の項目では、「高度な AI コンピューティング[5]は経済のダイナミズムと新たな軍事能力の両方を実現する。したがって、外国の敵対勢力によるこの計算資源へのアクセスを阻止することは、地政学的競争と国家安全保障の両方に関わる問題である。したがって、輸出管理執行において創造的なアプローチを追求するべきである」とした上で、「高度な AI コンピューティング上の新規および既存の位置検証機能を活用し、チップが懸念国に存在しないことを保証する方法を検討する」、「チップが転用されている可能性のある国や地域を完全に網羅するために、AI コンピューティングにおける新興技術の開発をモニタリングする」といった施策を打ち出している。また「〇既存の半導体製造輸出規制の抜け穴を塞ぐ」の項目では、「敵対国が米国のイノベーションを自国の目的のために利用し、我々の国家安全保障を損なうことを阻止しなければならない。そのためには、半導体製造輸出規制のギャップに対処するための新たな措置と、強化された執行が必要」としている。

・その他

「〇AI 導入を可能にする」の項目で、米国では「特に大規模で確立された組織における AI の導入が限定的で遅いことがボトルネックとなっている。医療など米国の最も重要なセクターの多くは、技術への不信感や理解不足、複雑な規制環境、明確なガバナンスとリスク軽減基準の欠如など、様々な要因により AI 導入が特に遅れている」という課題認識を示した上で、「米国、その競争国、および敵対国の国家安全保障機関による AI ツールの導入状況の比較に関する共同評価を定期的に更新する」施策を掲げている。

「〇世界クラスの科学データセットの構築」の項目では、「敵対国を含む他国は、膨大な科学データの蓄積において米国に先行している。米国は、個人の権利を尊重し、市民の自由、プライバシー、機密保護を確保しながら、世界最大かつ最高品質の AI 向け科学データセットの構築を主導しなければならない」と、中国における国家主権の下での人権を度外視した学習データの集積に危機感を表明している。

「〇オープンソースとオープンウェイトの AI を奨励する」の項目では「米国が米国の価値観に基づいた先進的なオープンモデルを持つことを保証する必要がある。オープンソースおよびオープンウェイトのモデルは、一部のビジネス分野や世界中の学術研究において、世界標準となる可能性がある。そのため、地政学的価値も持っている」としている。

「〇軍事および諜報コミュニティ向け高セキュリティ・データセンターの構築」の項目では、「AI は米国政府の最も機密性の高いデータと共に使用される可能性が高い。これらのモデルが導入されるデータセンターは、最も断固とした能力を持つ国家主体による攻撃に耐えられるものでなければならない」と、中国等からのサイバー攻撃を念頭においている。

さらに、「〇国防総省における AI 導入の推進」の項目では、「AI は、国防総省の戦闘業務とバックオフィス業務の両方を変革するポテンシャルを持つ。米国は、世界的な軍事的優位性を維持

[5] 原文は AI compute であり、AI の学習と展開のための計算資源を意味する。

し、本行動計画全体を通して概説されているように、AIの活用が安全かつ信頼できるものであることを保証するために、自国の軍隊において AI を積極的に導入しなければならない」と、軍における AI の積極導入も謳っている。

（2）バイデン政権の政策の否定

・AI イノベーションと導入を阻害する煩雑な手続きの連邦規制の廃止

トランプ大統領が就任当日にバイデンの AI 大統領令「安全でセキュアで信頼できる AI に関する大統領令」[6]を撤回し、ヴァンス副大統領は 2025 年 2 月のパリ AI アクションサミットで、「煩雑な規制で AI 開発を制限することは既存企業（既得権益層）に不当な利益をもたらすだけでなく、ここ何世代にもわたって見てきた最も有望な技術の一つを麻痺させることを意味する」と述べたように、バイデン政権時代に導入された AI 規制を見直すことが行動計画の 1 つの目的となっている。

「〇お役所仕事（rad tape）と煩雑な規制の廃止」の項目において、「大統領令 14192 号「規制緩和による繁栄の解放」（2025 年 1 月 31 日）に基づき、すべての連邦機関と協力し、AI の開発または展開を不必要に妨げる規制・ルール・覚書・行政命令・ガイダンス文書・政策声明・機関間協定を特定、改正、または廃止する」としている。

ただしバイデン政権時代の AI 規制に対する見直しは、規制の「煩雑な手続き」（民間の開発速度を落とす障壁）に向けられており、後述（4）で見るように規制における「安全性への配慮」に向けられたものではない。

・煩雑な手続きの AI 規制を導入する州には AI 関連資金提供を制限するが、「イノベーションを過度に制限しない賢明な州法」は許容

「〇お役所仕事と煩雑な規制の廃止」の項目では「連邦政府は、AI関連の連邦資金が、これらの資金を無駄にする煩雑な AI 規制を有する州に向けられることを許すべきではないが、同時に、イノベーションを過度に制限しない賢明な法律を制定する州の権利を侵害すべきでもない」と、煩雑な手続きの AI 規制を導入する州には AI 関連資金提供を制限するが、「イノベーションを過度に制限しない賢明な州法」に対しては理解を示している。

・イデオロギー的偏向のないフロンティア LLM 開発者とのみ連邦機関は契約

・NIST の AI リスク管理フレームワークを改訂し、誤情報・多様性・公平性・包摂性・気候変動への言及を削除

また、民主党政権で推進された DEI 政策を反映した（とトランプ政権がみなしている）各社 AI モデルでの「イデオロギー的偏向」を問題視し、行動計画の序文において「米国の AI システムは、イデオロギー的偏向がないものでなければならず、利用者が事実に基づく情報や分析を求

[6] https://bidenwhitehouse.archives.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/。

める際に、ソーシャルエンジニアリング[7]の目的ではなく、客観的な真実を追求するように設計されていなければならない」[8]としている。

「○フロンティア AI が言論の自由と米国の価値観を守ることを保証する」の項目において、「AI システムは、言論の自由と表現の自由を念頭に置いて根本から構築され、米国政府の政策がその目的を妨げないことが不可欠である。AI 時代において言論の自由が尊重され、連邦政府が調達する AI がソーシャルエンジニアリング的な意図ではなく、客観的に真実を反映することを保証しなければならない」とされ、具体的には「NIST の AI リスク管理フレームワークを改訂し、誤情報・多様性・公平性・包摂性・気候変動への言及を削除」、「連邦政府の調達ガイドラインを更新し、トップダウンのイデオロギー的偏向から自由であることを保証するフロンティア LLM 開発者とのみ契約することを保証」といった施策が計画されている。中国への対抗とも関連して、「NIST の AI 標準イノベーションセンター（CAISI）[9]を通じて、中国のフロンティアモデルについて、中国共産党の主張や検閲との整合性に関する調査を実施」することも挙げられている。

・バイデン政権下で FTC 前委員長が推し進めた GAFAM に対するプラットフォーマー規制や決定の見直し

さらに、「○お役所仕事と煩雑な規制の廃止」の項目では「前政権下で開始された連邦取引委員会（FTC）の調査をすべて見直し、AI イノベーションに過度の負担をかけるような責任理論を推し進めていないことを保証する。さらに、FTC の最終命令、同意判決、差止命令をすべて見直し、必要に応じて、AI イノベーションに過度の負担をかけるものを修正または無効にするよう努める」としており、バイデン政権時代にリナ・カーン FTC 前委員長（2025 年 1 月 31 日に退任）が推し進めた GAFAM に対するプラットフォーマー規制や決定を見直すとしている。

バイデン政権時代に標的とされたプラットフォーマーは、逆にトランプ政権下では AI 推進政策と相まって「優遇」されることとなった[10]。

・その他

なお、前述（１）とも関連するが、行動計画の序文で「我々は、広大な AI インフラとそれを支えるエネルギーを構築・維持する必要がある。そのためには、政権が就任式以来行ってきたように、過激な気候変動に関するドグマや官僚主義的なお役所仕事を今後も拒否していく。端的に言えば、『立てて、立てて、立てまくれ！』である」と記載されているように、バイデン政権下で維持されてきた環境規制を見直し、AI関連インフラ（データセンター、半導体製造工場、電力網）の構築を迅速化する方針も示されている。

---

[7] 気が付かないうちに人々を特定の価値観に染めてしまう、といった意味。
[8] これは、行動計画に共通する 2 つ目の原則として挙げられている。
[9] https://www.nist.gov/caisi。バイデン政権下で設立された AISI（AI Safety Institute）を 2025 年 6 月 3 日に改名・改組したもの。
[10] 前述のイデオロギー的偏向（Wake 的 DEI 価値観）の排除以外。

（3）米国労働者ファースト

・実体経済から乖離して巨大化した金融経済への「当てつけ」として、成長から取り残された労働者の支援を強調

AI 行動計画では、実体経済から乖離して巨大化した金融経済（やデジタル経済）への一種の「当てつけ」として、成長から取り残された（ラストベルトなどの）労働者の支援を強調している。旧来の労働者が AI 時代に職を奪われるのではなく新たな職に就けるように、国内での AI 関連インフラの設備投資とインフラを担う技術職の雇用拡大、労働者の再訓練の機会拡大を謳っている。

まず序文で、行動計画に共通する第一の原則として「米国の労働者はトランプ政権の AI 政策の中心である。トランプ政権は、この技術革命によって創出された機会から、米国の労働者とその家族が恩恵を受けられることを保証する。AI インフラの構築は、米国の労働者に高給の仕事を生み出すだろう。そして、AI が可能にする医療、製造業、その他多くの分野における飛躍的な進歩は、すべての米国民の生活水準を向上させるだろう。AI は米国人の仕事を奪うのではなく、仕事を補完することで、生活を向上させる」ことを掲げている[11]。

・AI 関連インフラを担う旧来型の技術職（電気技術者、空調設備技術者等）の雇用拡大、労働者の再訓練の機会拡大

具体的には、「○AI 時代における米国労働者のエンパワーメント」の項目で、「AI リテラシーとスキル開発の拡大、AI が労働市場に与える影響の継続的な評価、そして AI 主導型経済において労働者が迅速に再訓練を受けて活躍できるよう支援するための新たなイノベーションの試行といった、一連の優先的な行動を推進していく」としている。

さらに「○AI インフラのための熟練労働者の訓練」の項目では、「AI に必要なインフラを構築するには、電気技術者、高度な空調設備技術者、その他多くの高収入職種など、インフラの構築、運用、維持を担う労働力に投資しなければならない。これらの重要な職種の多くにおける人材不足に対処するため、トランプ政権は AI インフラを支える優先的な役割を特定し、最新のスキルフレームワークを開発し、業界主導の研修を支援し、一般教育、CTE（専門教育）、登録実習制度を通じて早期の人材パイプラインを拡大」するとし、AI 推進・導入のためには新世代の AI 技術者のみならず、旧来からの「電気技術者」や「空調設備技術者」等も必要だとして労働者層を鼓舞し、スキルアップを促し、また若者を AI インフラ関連の優先職種につかせるための研修制度を拡大する施策を掲げている。

（4）AI リスクへの対処

バイデン AI 大統領令「安全でセキュアで信頼できる AI に関する大統領令」は大規模な基盤モデルを提供する大手 AI 事業者に対する規制（安全性テストの結果等の報告義務）を含むものであった。この大統領令等における規制を見直すことで、AI 行動計画では AI の安全性は度外視さ

[11] トランプ政権は、2025 年 4 月の大統領令 14277 号「米国の若者のための AI 教育の推進」や 14278 号「将来の高給の熟練職業への米国民の準備」でも既に雇用対策を打ち出していた。

れ、なりふりかまわぬ AI 推進に舵が切られたという論調の報道も見られる。しかし、行動計画では実際には AI が米国社会にもたらすリスクに対する安全性への配慮についても、AI が CBRN（化学・生物・放射線・核）兵器の製造に使われるリスクを含め、多くの箇所で規定されている。ただし、バイデン政権との「差異」を演出するためか、「安全性（safety）」という言葉は極力使わず、「セキュリティ」「国家安全保障」という言葉が頻繁に使われている。

・AI に起因する新たなリスクや予期せぬリスクの監視

まず序文では、行動計画に共通する原則の 1 つとして、「第三に、我々は、悪意のある者による高度な技術の悪用や盗難を防ぐとともに、AI に起因する新たなリスクや予期せぬリスクを監視しなければならない。そのためには、絶え間ない警戒が必要である」とする。

・AI 開発企業と協力し、フロンティア AI による CBRN（化学・生物・放射線・核）兵器の開発やサイバー攻撃等の国家安全保障リスクを評価

「〇米国政府がフロンティアモデルにおける国家安全保障リスクの評価において最前線に立つことを保証する」の項目では、「最も強力な AI システムは、サイバー攻撃や化学・生物・放射線・核・爆発物（CBRNE）兵器の開発、そして新たなセキュリティ上の脆弱性といった分野において、近い将来、新たな国家安全保障リスクをもたらす可能性がある。米国は現在 AI 能力において世界をリードしているため、米国のフロンティアモデルに存在するリスクは、近い将来、外国の敵対勢力が保有するであろうフロンティアモデルのリスクの先駆けとなる可能性が高い。これらのリスクが出現するにつれて、その性質を理解することは、国防と国土安全保障にとって不可欠である」とした上で、「商務省の CAISI が主導し、CBRNE およびサイバーリスクに関する専門知識を持つ他の機関と連携して、フロンティア AI 開発者と協力し、フロンティア AI システムの国家安全保障リスクを評価する」と、AI が社会にもたらす CBRN リスク等に対処するための安全面での取組みを指示している。また、同項目には「商務省の CAISI が主導し、国家安全保障機関と連携して、重要インフラや米国経済のその他の分野における敵対国製 AI システムの使用から生じる潜在的なセキュリティ上の脆弱性と悪意のある外国の影響（バックドアやその他の悪意のある行為の可能性を含む）を評価する」という、中国製 AI のセキュリティリスクを念頭に置いた施策も掲げている。

CBRN リスクの内、生物兵器のリスクについては「〇バイオセキュリティへの投資」の項目で改めて焦点が当てられ、「AI は悪意のある者が有害な病原体やその他の生体分子を合成するための新たな経路を生み出す可能性もある。この問題の解決策は、悪意のある者をスクリーニングするための多層的なアプローチと、より効果的なスクリーニングのための新たなツールとインフラである」とされている。

・AI の解釈可能性、AI の制御、敵対行動に対する堅牢性への投資

また、「〇AI の解釈可能性、制御、堅牢性のブレークスルーへの投資」の項目では、「技術者は LLM の働きを高次レベルでは理解しているが、モデルが特定の出力を生成した理由をしばしば

説明できない。そのため、特定の AI システムの挙動を予測することが困難になりうる。この予測可能性の欠如は、国防、国家安全保障、あるいは人命に関わるその他の用途において、高度な AI を活用することをチャレンジングにしうる」という現状認識の上で、「国防高等研究計画局（DARPA）が、商務省の CAISI および NSF と協力し、AI の解釈可能性、AI 制御システム、そして敵対行動に対する堅牢性を向上させる技術開発プログラムを開始する」という施策を掲げている。

・その他

さらに、「〇民間および政府の AI イノベーションを保護する」の項目では、「米国政府が産業界と緊密に連携し、最先端の AI 技術の普及と国家安全保障上の懸念を適切にバランスさせることが不可欠」とした上で、「米国の主要 AI 開発者と協力し、民間部門が悪意のあるサイバー攻撃者、内部脅威などのセキュリティリスクから AI イノベーションを積極的に保護」するという施策が挙げられている。

「〇重要インフラのサイバーセキュリティ強化」の項目では、「サイバーインフラや重要インフラにおける AI の使用は、これらの AI システムを敵対的な脅威にも晒す。安全性が極めて重要なアプリケーションや国土安全保障アプリケーションにおける AI の使用は、パフォーマンスの変化を検知し、データポイズニングや敵対的サンプル攻撃などの潜在的な悪意のある活動を警告する機能を備えた、セキュア・バイ・デザイン（secure-by-design）で、堅牢で回復力のある AI システムの採用を必須とするべき」としている。また、「〇セキュア・バイ・デザインの AI 技術とアプリケーションの推進」の項目でも、「AI システムは、一部の敵対的入力（データポイズニングやプライバシー攻撃など）の影響を受けやすく、パフォーマンスがリスクに晒されてしまう。米国政府は、（特に国家安全保障アプリケーションにおいて）自らが依存する AI システムが偽装入力または悪意のある入力から保護されることを保証する責任を負っている。AI アシュアランスの分野の発展に向けて多くの取組みが行われてきたが、回復力とセキュリティに優れた AI の開発と展開の促進は、米国政府の中核的な活動であるべき」との認識が示されている。

２．日米欧の AI 政策の比較

２．１　日米欧の AI 政策の概要

米国においては、前述のとおり、バイデン政権下で発令された事業者規制を含む AI 大統領令の廃止とトランプ大統領令「AI における米国リーダーシップの障壁の除去」の発令（2025 年 1 月）、フランス開催 AI アクションサミットでの「持続可能な AI に関する声明」への非署名とヴァンス副大統領による EU の「過度な規制」の批判（2025 年 2 月）が行われた。2025 年 7 月には、大統領令の規定を受けて、米国製 AI の開発・展開を強化する米国 AI 行動計画が策定された。州レベルでは、カリフォルニア州のフロンティア AI モデル規制法案に対して州知事が拒否権を発動し不成立となった（2024 年 9 月）。総体的には、AI の安全性を重視する立場よりも AI 覇権の維持強化する立場が前面に出ることとなった。

EU では包括な AI 規則（AI 法）[12]を世界に先駆けて制定するが（2024 年 5 月）、「ドラギ報告書」[13]（2024 年 9 月）の提言（行き過ぎた規制は EU の競争力を阻害する）を行動計画化した「競争力コンパス」[14]（2025 年 1 月）において主要分野での AI 開発と産業導入を促進するために AI 計算インフラ構築や AI 導入イニシアティブの提案がなされた。また AI アクションサミット（2025 年 2 月）において AI に対して 2,000 億ユーロの投資をモビライズする「InvestAI イニシアティブ」[15]を公表した。「AI Continent Action Plan」[16]（2025 年 4 月）では計算資源・データ・AI 導入・人材・規制の 5 つの観点から AI イノベーション能力の強化が図られると共に、中小企業向けに AI 法の適用簡素化を予告している。

日本の「AI 関連技術の研究開発・活用推進法」（AI 推進法）[17]（2025 年 6 月公布）はイノベーション推進とリスク対応が 2 本柱である。AI 事業者に対して、国が実施する施策への協力義務（具体的には AI に起因する人権侵害の事案発生時などに国が行う調査への情報提供等の協力義務と考えられる）を規定しているが、2024 年時点の当初案よりも AI 開発／提供事業者に配慮した内容となった。自動車・医療・雇用・教育・行政手続きなど個別分野での AI リスクやネット空間での偽情報等については、既存業法／法令の下で対応する。AI 推進法の課題として、外国 AI 事業者の大規模基盤モデルに起因する AI リスクへの抑止力としては機能しにくいことや、AI 事業者ガイドラインとの関係の不明確性が挙げられる。AI 推進法の規定を受けて 2025 年内を目途として人工知能基本計画（AI 基本計画）を策定予定[18]である。

2．2　米欧政府における AI 安全面へのコミットメント

米欧日の 3 極ともに、2024 年までは AI 規制政策が主流であったが、2025 年からは（米国トランプ大統領による前バイデン政権の政策の否定という強い動機の影響も受けて）AI 推進政策が主流となっている。ただし、EU や米国の個別の政策を見ると、AI の安全面が決してなおざりにされている訳ではなく、ジェフリー・ヒントンやヨシュア・ベンジオといった「AI 界のゴッドファーザー」やスチュアート・ラッセルらの著名 AI 研究者が過去から繰り返し主張している AI の社会的リスクをベースに、むしろ共通的な危機意識の下に政策が準備されていることが見て取れる。

例えば、EU の AI 法の汎用目的 AI モデル実践規範[19]では、「安全性とセキュリティ」の章でシステミックリスクの 4 類型として「化学・生物・放射線・核（CBRN）」「制御の喪失」「サイバー攻撃」「有害な操作」が挙げられている。中でも、最も深刻なシステミックリスクである「制御の喪失」については、「モデルを確実に指揮したり、変更したり、シャットダウンしたりする能力を人間が喪失することによるリスク。そのようなリスクは、人間の意図または価値観とのミ

[12] https://eur-lex.europa.eu/eli/reg/2024/1689/oj。
[13] https://commission.europa.eu/topics/eu-competitiveness/draghi-report_en。
[14] https://commission.europa.eu/topics/eu-competitiveness/competitiveness-compass_en。
[15] https://ec.europa.eu/commission/presscorner/detail/en/ip_25_467。
[16] https://digital-strategy.ec.europa.eu/en/library/ai-continent-action-plan。
[17] https://laws.e-gov.go.jp/law/507AC0000000053。
[18] 2025 年 9 月 12 日には人工知能基本計画の骨子（たたき台）が公表された。
https://www8.cao.go.jp/cstp/ai/ai_hq/1kai/shiryo2_2.pdf。
[19] https://digital-strategy.ec.europa.eu/en/policies/contents-code-gpai。

スアライメント、自己推論、自己複製、自己改善、欺瞞、目標変更への抵抗、力を得ようとする行動（power-seeking behaviour）、AI モデルや AI システムの自律的な作成や改善から生じうる」と説明されている。

米国の連邦政府 AI 利用ポリシー文書である「OMB 覚書 M-25-21：イノベーション、ガバナンス、パブリックトラストを通じた連邦政府による AI 利用の加速」[20]においても、表向きは「バイデン前政権のようなリスク回避型のアプローチを追求するのではなく、前向きでイノベーションと競争を重視する考え方に移行した」[21]としているが、ハイインパクト AI ユースケース（EU のハイリスク AI システムに相当）の分類義務やハイインパクト AI ユースケースに対する一連のリスク管理プラクティスの実施義務など、実際にはリスク回避型のアプローチが維持されている。AI 覇権の維持強化を前面に打ち出した米国 AI 行動計画においても、実際には AI が米国社会にもたらすリスクに対する安全性への配慮に関して、フロンティアモデルが CBRN（化学・生物・放射線・核）兵器の製造に使われるリスクを官民で評価することを含め、多くの箇所で規定が設けられている。また、ニューヨーク州の「責任ある AI 安全・教育法案（RAISE 法案）」[22]も、大規模 AI モデル開発者を規制対象とし、AI が CBRN 兵器の製造に用いられたり、自律的に「犯罪行為」を行うことに起因して一定以上の損害や死傷者を引き起こすような深刻なリスクから一般市民を保護することを目的としている。

このような AI の社会的リスクに対する米欧の共通的な危機意識は、日本の政策立案の場では希薄であるように見受けられる。日本では産業界・経済界からの政策提言といえば「規制緩和要求」が常道であるため事業者としては声を上げにくい面もあるが、日本の AI 推進法の下でも事業者（特にフロンティアモデルを開発する海外事業者）に対する安全面での義務規定を設けることは喫緊の課題と考えられる。また、AI の安全面やリスク対策に関する多くの規定を設けている、既存の AI 事業者ガイドライン[23]の有効活用も求められることとなるだろう。

2．3　米欧におけるソブリン AI・ソブリンクラウド政策

米国は AI 行動計画において、世界的 AI 競争における米国のリーダーシップを維持し、AI 競争の最大のライバルである中国に勝利するために、「AI 開発・展開用の計算資源を米国製品で構築する（AI 関連インフラから中国製品を排除する）」、「米国製 AI パッケージ（AI モデル・半導体含むハードウェア・ソフトウェア・アプリケーション・標準規格等）を友好国に輸出する」ことを掲げている。連邦政府 AI 利用ポリシー文書や連邦政府 AI 調達ポリシー文書[24]でも AI イノベーションにおける米国のグローバルな優位性を強化するために「米国製 AI の利用の最大化」が再三謳われている。

---

[20] https://www.whitehouse.gov/wp-content/uploads/2025/02/M-25-21-Accelerating-Federal-Use-of-AI-through-Innovation-Governance-and-Public-Trust.pdf。
[21] https://www.whitehouse.gov/wp-content/uploads/2025/02/AI-Memo-Fact-Sheet.pdf。
[22] 2025 年 6 月 12 日に州議会で可決されており、州知事が署名すれば成立となる。
[23] https://www.soumu.go.jp/main_sosiki/kenkyu/ai_network/02ryutsu20_04000019.html。
[24] https://www.whitehouse.gov/wp-content/uploads/2025/02/M-25-22-Driving-Efficient-Acquisition-of-Artificial-Intelligence-in-Government.pdf。

また、EU の AI Continent Action Plan では「EU はデータセンター能力の点で米国や中国に遅れをとっている」、「EU ユーザーは（米国企業等の）クラウド経由で EU 域外に設置されているインフラに大きく依存している」、「革新的で手頃な価格のクラウドサービスへのアクセスは EU の競争力にとって不可欠であり、EU 域外インフラへの過度の依存は経済安全保障上のリスクをもたらしうる」との認識の上で、「EU 全域の企業や行政機関の AI・計算資源ニーズに適切に対応し、競争力と主権を保証するために、EU ベースのクラウドとデータセンター能力を増強する」、「クラウドとデータセンターへの民間投資を促進するために、クラウド・AI 開発法案（Cloud and AI Development Act）を提案する（2025 年 4Q~2026 年 1Q）」、「今後 5～7 年で EU のデータセンター能力を少なくとも 3 倍に増強する」という意欲的な目標が掲げられている。

米欧の政策において、このようにソブリン AI・ソブリンクラウド構築に対する明確な意思表示がなされているのに対し、日本の生成 AI 調達・利活用ガイドライン[25]を始めとする既存の政策では、国産 AI（ソブリン AI）の調達・利用やソブリンクラウド強化に関する言及は特に見られない[26]。

本稿の最後に、米欧日の AI 政策の比較表を記載する。

図表 2　米欧日の AI 政策の比較（筆者作成）

	米国 （米国 AI 行動計画）	EU（AI Continent Action Plan、AI 法）	日本[27]
AI 開発・展開用の計算資源	・AI インフラ（データセンター・半導体工場・発電施設）の許可迅速化・環境規制緩和	・大規模 AI 計算インフラ（AI ファクトリー／ギガファクトリー）の選定と投資	・AI 橋渡しクラウド（産総研）や GENIAC（経済産業省）で計算資源の利用支援 ・AI データセンター、効率的な電力・通信インフラの整備、オール光ネットワーク、次世代情報通信基盤の研究開発【たたき台】
ソブリン AI	・AI 用の計算資源を米国製品で構築 ・米国製 AI パッケージ（AI モデル・半導体・標準規格等）を友好国に輸出 ・連邦機関で米国製 AI の利用を最大化	・EU のクラウドおよびデータセンター（ソブリンクラウド）の能力増強（クラウド・AI 開発法案を作成中）	・（GENIAC-PRIZE（経済産業省）で国産基盤モデルを用いた AI エージェント開発を支援） ・AI エコシステムを日本国内に構築、積極的に海外展開することで、国際競争力も強化し、日本の自律性・不可欠性を確保【たたき台】

[25] https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/e2a06143-ed29-4f1d-9c31-0f06fca67afc/80419aea/20250527_resources_standard_guidelines_guideline_01.pdf。
[26] ただし、前述の「人工知能基本計画骨子（たたき台）」（2025 年 9 月 12 日）では「AI エコシステムを日本国内に構築」等が予告されている。
[27] 「人工知能基本計画骨子（たたき台）」（2025 年 9 月 12 日）で予告された内容については【たたき台】として記載。

AI 開発用の学習データ	・ビッグテックが大量のデータを集積しているが、科学データ蓄積で中国（人権度外視で収集）の後塵を拝することに危機感	・データスペース（14 分野）の整備、データ集積のため法律で提供義務化（EHDS 規則、データ法、バッテリー規則等）	・データ利活用制度基本方針で、法令でのデータ提供義務化やデジタル公共財としての整備を今後検討 ・個人情報保護法改正で AI 開発時の本人同意なき第三者提供等を可能に ・AI 開発に必要なマルチモーダルなデータの創出・提供等のデータ連携基盤の構築【たたき台】
各分野での AI 導入	・医療分野などの既存セクターでの導入遅れ。連邦機関や軍で率先して AI 導入	・戦略分野や行政分野における AI 開発と AI 導入の促進	・各省庁での生成 AI 利活用を推進 ・まずは政府自らが積極的に利活用。各分野での AI エージェントやフィジカル AI 等の開発・実証・導入促進【たたき台】
AI 人材の強化	・AI インフラを担う旧来型の技術職（電気技術者、空調設備技術者等）の雇用拡大	・EU に AI 研究者を招聘・呼び戻す	・生成 AI に合わせたデジタルスキル標準の改訂など ・国内外から AI 開発者を確保するための待遇面や生活環境を含めた包括的な取組【たたき台】
安全性の確保	・バイデン政権の AI 規制（大統領令）を廃止 ・CBRN（化学・生物・放射線・核）兵器の開発やサイバー攻撃等の AI リスクを官民で評価 ・連邦機関でのハイインパクト AI 導入においてはリスク管理義務	・AI 法でハイリスク AI や GPAI モデルを包括的に規制 ・GPAI モデルのシステミックリスクとして CBRN（化学・生物・放射線・核）、制御の喪失、サイバー攻撃、有害な操作の 4 類型を規定	・AI 推進法で事業者は人権侵害事案発生時等の国の調査への協力義務 ・AI 法に基づく指針その他ガイドライン等の整備・周知徹底、AI モデル適正性に係る評価機能の構築を含む AISI の抜本的強化【たたき台】

参考文献

- The White House「Winning the Race: America's AI Action Plan」（2025 年 7 月 23 日）（https://www.whitehouse.gov/wp-content/uploads/2025/07/Americas-AI-Action-Plan.pdf）
- Office of Management and Budget「OMB Memorandum M-25-21, Accelerating Federal Use of AI through Innovation, Governance, and Public Trust」（2025 年 4 月 3 日）（https://www.whitehouse.gov/wp-content/uploads/2025/02/M-25-21-Accelerating-Federal-Use-of-AI-through-Innovation-Governance-and-Public-Trust.pdf）
- The White House「Removing Barriers to American Leadership in Artificial Intelligence: Executive Order」（2025 年 1 月 25 日）（https://www.whitehouse.gov/presidential-actions/2025/01/removing-barriers-to-american-leadership-in-artificial-intelligence/）
- The White House「Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence」（2023 年 10 月 30 日）

（https://bidenwhitehouse.archives.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/）
- The New York State Senate「Senate Bill S6953B: Responsible AI safety and education act (RAISE act)」（https://www.nysenate.gov/legislation/bills/2025/S6953/amendment/B）
- European Commission「The AI Continent Action Plan」（2025 年 4 月 9 日）（https://digital-strategy.ec.europa.eu/en/library/ai-continent-action-plan）
- European Commission「The General-Purpose AI Code of Practice」（https://digital-strategy.ec.europa.eu/en/policies/contents-code-gpai）
- 小泉雄介「EU の AI 法（AI 規則）の概要」（2024 年 7 月 12 日）（https://www.i-ise.com/jp/information/media/2024/240718.pdf）
- 小泉雄介「AI が意識を持つと社会はどうなるのか：リスクと対策」（IISE 調査研究レポート No.6）（2025 年 5 月）（https://www.i-ise.com/jp/information/report/pdf/rep_it_202503a.pdf）

以　上