

2025 年 10 月 28 日

AI 法に基づく指針および AI 基本計画骨子（たたき台）に対する BSA の提言

Business Software Alliance（ビジネス・ソフトウェア・アライアンス、以下 BSA）¹は、日本政府が、「世界で最も AI を開発・活用しやすい国」を目指して、AI 利活用で日本の長年の課題である人口減少、国内への投資不足、賃金停滞を解決すべく継続的取組みをしていることを高く評価しています。また、本目標の達成に向けた施策をまとめた「AI 基本計画」および AI 法に基づく「指針」の策定において、関係者を関与させていることを歓迎します。

BSA はグローバルなソフトウェア産業を代表する業界団体であり、会員は AI、クラウドストレージサービス、サイバーセキュリティソリューション、量子コンピューティングなどの革新的技術で業界をリードするエンタープライズソフトウェア企業で構成されています。これらの企業は経済のあらゆる分野のビジネスを支援し、他社の革新と成長を支える信頼性の高いツールを提供しています。

エンタープライズ AI システム開発のリーダーとして、BSA 会員企業はデジタル変革を促進する技術の大きな可能性と、AI の責任ある利用を最も効果的に支援する政策について独自の知見を有しています。

BSA のグローバルな知見は「AI ポリシー・リソースセンター」²で公開されており、BSA がまとめた「日本におけるエンタープライズ AI 導入アジェンダ」³においては、人材/労働力、インフラと

¹ BSA のメンバーは以下の通り：Adobe, Alteryx, Amazon Web Services, Asana, Atlassian, Autodesk, Avalara, Bentley Systems, Box, Cisco, Cloudflare, Cohere, Cohesity, Dassault Systemes, Databricks, Docusign, Dropbox, Elastic, EY, Graphisoft, HubSpot, IBM, Informatica, Kyndryl, MathWorks, Microsoft, Notion, Okta, OpenAI, Oracle, PagerDuty, Palo Alto Networks, PTC, Rubrik, Salesforce, SAP, ServiceNow, Shopify Inc., Siemens Industry Software Inc., Trend Micro, TriNet, Veeam, Workday, Zendesk, and Zoom Communications Inc.

² BSA のポリシー・リソース・センター(Policy Resource Center): <https://ai.bsa.org/>

³ BSA の「日本におけるエンタープライズ AI 導入アジェンダ」：
<https://www.bsa.org/files/policy-filings/jp09282025bsajapanaiadoption.pdf>

データ、ガバナンスフレームワークの三つの柱を通して AI 導入を国家優先課題とするための具体的な施策を提案しています。

AI 基本計画骨子（以下、「計画案」）及び指針案に関する以下の提言が、日本での AI イノベーションを促進する政策に寄与することを我々は期待しています。

本提言は、以下に焦点を当てています。

- 公共部門における AI 導入を促進するために政府が講じられる措置
- 民間部門における AI 導入を支援するためのアプローチ
- AI ガバナンスにおける国際的な整合性の実現
- グローバルなソフトウェア企業との連携による「信頼できる AI」の開発

公共部門における積極的 AI 利活用を通じた模範の提示

政府が計画案において、行政業務における AI の積極的利活用にコミットしたことを BSA は歓迎します。公共部門における AI の導入を強固なガバナンスと併せて促進することで、国民のニーズへより効率的に対応することが可能になります。

これを実現するために、我々は政府機関におけるクラウド導入の更なる推進を強く推奨します。具体的には、政府情報システムのためのセキュリティ評価制度（ISMAP）を継続的に改善していくことを求めます。内閣府より公表された「規制改革実施計画」⁴では、他の認証制度を活用し、監査負担を軽減することが記されています。ISO 27000 シリーズや SOC 2 等、クラウドサービスプロバイダー（CSP）が取得した証跡の再利用の仕方に関して、関係者と十分な協議を行うことを奨めます。

国際的な相互運用性を確保するため、BSA は、同志国が適用可能な部分を相互に認め合う、相互認証制度の採用を推奨します（例：日本の ISMAP と米国の FedRAMP）。このようなアプローチにより、サイバーセキュリティとレジリエンスを広く向上させ、AI に関する国際的な連携を促進することが可能となります。

公共部門における AI 導入を促進するために、デジタル庁は「行政の進化と革新のための生成 AI の調達・利活用に係るガイドライン」⁵を策定しました。本ガイドラインにおいては、各府省庁に AI 統括責任者（CAIO）を設置し、生成 AI の利活用の状況を先進的 AI 利活用アドバイザリーボード（以下、「アドバイザリーボード」）へ報告し、アドバイザリーボードが高リスクの可能性のある活用を評価するという政府の方針が示されています。我々はこうした枠組みを支持しますが、モデルやユースケースだけでなく、事業者のガバナンスや利用者のリテラシー等、アドバイザリーボードがリスクを総合的に捉えることが重要です。一般的に高リスクの可能性が高いと考えられるユー

⁴ https://www8.cao.go.jp/kisei-kaikaku/kisei/publication/program/250613/01_program.pdf

⁵ <https://www.digital.go.jp/news/3579c42d-b11c-4756-b66e-3d3e35175623>

スペースであっても適切なガードレールや事前設定により総合的にはリスクを抑えて活用できる可能性があります。

また、計画案では、行政機関が利用する「ガバメント AI」のプラットフォーム整備やアプリケーション開発をデジタル庁が推進することが強調されています。コスト効率とセキュリティ基準の遵守が重要であることは理解しておりますが、先進技術と実績を有する信頼性を備えた民間の商用生成 AI サービスも活用し、行政サービスの向上を図ることを推奨します。これにより、政府がその使命を推進する上で、業界最先端の製品・サービスを活用することが可能となります。また、そのためには、商用化できない特注変更を強いられることなく、業界が政府にサービスを継続的に提供できるようにすることが重要です。特注変更は投資収益率を低下させ、タイムリーに更新されないツールの使用を招きます。そして、「ガバメントクラウド」においても、中央政府および地方自治体は、認定された IaaS プロバイダーが提供するサービスだけでなく、SaaS プロバイダーが提供する様々な AI サービスを利用できるようにすべきです。

行政効率と公共サービスの向上に向け、政府が AI 導入を加速化していく上では、パブリック AI ツールと「シャドーAI」ツールの拡散がもたらす重大なリスクに対処するため、生成 AI アプリケーションを安全かつ責任を持って業務に統合する能力を組織に備えさせる必要があります。こうしたリスクには、機密データ、知的財産、専有情報が外部 AI モデルへ意図せず漏洩することが含まれます。体制を整えることで、組織全体でどの AI アプリケーションが、誰によって、どのように使用されているかを可視化でき、追跡が困難な状況を改善し、日本の強固なセキュリティ態勢維持に寄与することが可能となります。こうした使用状況を把握する能力がなければ、組織は新たなサイバー攻撃ベクトルやコンプライアンス違反へのリスクを高めることになります。

同様に、他の AI 技術導入と同様に、エージェント型 AI もセキュリティを中核に据えた全組織的な取り組みとして扱うべきです。日本政府が AI エージェントの迅速な導入を検討するにあたり、それらのエージェントと広範な AI エコシステムのセキュリティ、レジリエンス、継続的な監視を優先すべきです。テクノロジー・スタックの他の層と同様に、これには継続的な監視、制御、説明責任に焦点を当てた強固なガバナンスとデータ保護が必要となります。

日本政府が生成 AI および AI エージェントに関するガイドライン策定を進めていく上では、現在これらのサービスを提供中または提供予定の事業者との十分な協議をするをことを奨めます。これにより、当ガイドラインがサービスを開発・導入する事業主体にとって実用的かつ実現可能な内容となり、さまざまな状況を認識しながらも、特定の技術への不必要な特別措置を設けてイノベーションを阻害することなく、関連する国際的に認知された基準やアプローチとの整合性によりグローバルな相互運用性を推進することが可能となります。

民間部門における AI 導入の支援

計画案においては中小企業を含めたあらゆる産業における AI 導入促進を目標としています。この実現に向け、以下を推奨します：

- 業界別のベストプラクティスを収集し、企業と従業員が AI を事業・リスク管理戦略に統合することを支援し、競争力、安全性、生産性の向上を図ること
- AI 研修コースを教育補助金の対象とし、既存の政府のスキル習得プラットフォーム⁶を促進すると共に、民間のスキル習得プログラム⁷を活用し、これらの教育コースの修了資格を認定することで、人材育成を支援すること
- AI 研究と産業応用を促進するため、非機密政府データを利用可能な形式で提供拡大すること
- 重要インフラ事業主に対し、重要ネットワーク内の老朽化した資産を特定し対処するための拘束力のある措置を制定すること

AI ガバナンスにおける国際的な整合性の実現

広島 AI プロセス⁸など国際的な AI ガバナンス枠組みにおける日本のリーダーシップを我々は高く評価しています。今後、日本が国内の「AI 事業者ガイドライン」⁹を更新するにあたっては、以下を推奨します：

- 国際的なベストプラクティスフレームワーク（例：NIST AI リスクマネジメントフレームワーク、高度な AI システム開発者向けの G7 国際行動規）との整合性がとれていれば、ガイドラインの関連部分を網羅しているとみなすこと
- 特にデータの公平性に関連し、入力への規範的要件ではなくシステム出力に焦点を当てた成果志向型アプローチを採用すること

国際的な整合性は極めて重要であり、日本は国内のガイドラインを G7 国際行動規範に整合させ、継続的に改善することでリーダーシップをさらに強化することができます。

日本が国内のガイドラインを更新する際には、以下についても、追加検討することを推奨します。

第一に、開発者、インテグレーター、導入者など AI エコシステム内の異なる主体を明確化することです。これは計画案で取り上げられている、AI エージェントを含む AI 導入を加速する上で重要となります。組織によって関連情報へのアクセス状況や発生しうる課題への対応能力が異なるため、責任は実行可能かつ役割に適したものであるべきです。

第二に、サイバーセキュリティの推進における AI の役割を検討することを奨めます。特に、サイバーセキュリティ対策は既存のネットワークセキュリティ運用を維持するためだけでなく、AI エー

⁶<https://manabi-dx.ipa.go.jp/>

⁷<https://bsa.or.jp/policy/digitalskill/>

⁸<https://www.soumu.go.jp/hiroshimaaiprocess/documents.html>

⁹https://www.meti.go.jp/shingikai/mono_info_service/ai_shakai_jisso/20240419_report.html

ジェントのセキュリティを確保し、悪意のある入力や機密データの漏洩などから保護するためにも必要です。関係者が AI エージェント・エコシステム内の責任を評価するにあたり、AI 事業主体の異なる役割を認識することは、AI の開発と利用を導く上で役立ちます。

第三に、計画案に記されている、個人情報保護法の改正¹⁰を進め、AI 開発等における本人同意の要件を見直し、規律遵守の実効性を確保することを奨めます。様々な状況におけるデータ処理において、同意以外の仕組みを認めることを我々は支持しています。例えば、日本の個人情報保護制度に正当な利益（legitimate interests）の枠組みを取り入れることで、より柔軟で適応性のあるアプローチがとられ、企業は、個人、企業、社会の利益のために様々な製品やサービスをサポート、提供、改善する上で必要な個人データを収集できるようになります。また、同時に、そのような処理が個人の権利を損なわないようにすることが可能となります。

最後に、データ活用促進のため「官民データ活用推進基本法」¹¹の改正が検討されていると我々は認識しております。内閣府における「デジタル行財政改革会議」の下で進められている議論に、産業界を参画させることを我々は推奨します。

グローバルなソフトウェア企業との連携による「信頼できる AI」の開発

インフラ、モデル、アプリケーションに至る全レイヤーにおいて強固な AI エコシステムを構築するという日本の目標を我々は支持します。特にインフラ・レイヤーにおいては、資本を集約した投資が必要となることから、モデルやアプリケーションなど日本が競争優位性を発揮できる分野にまず注力することを提案します。また、国内事業者以外からの提供であっても、既存インフラを活用することが重要です。日本が世界最高の技術を集結できるよう、コンピューティングリソースやクラウドインフラを含む、同志国のソフトウェアプロバイダーが提供する既存のテクノロジーやデジタルインフラを最大限活用することを推奨します。これにより、日本は重複した取り組みを避け、AI エコシステムにおける付加価値の高い活動に注力できるようになります。例えば自国のニーズに合わせたドメイン特化型モデルやアプリケーション開発です。「信頼できる AI」の開発という日本の目標は、国内の事業主体のみの努力ではなく、グローバル企業とのこうした技術提携によってより効果的に達成することができます。

これを実現するには、高品質な日本語データへのアクセスが不可欠となります。国立研究開発法人情報通信研究機構（NICT）が保有する日本語学習データへのアクセス提供などを含め、日本政府がこうしたデータ資源の改善・拡充に取り組んでいると我々は認識しています。例えばオープンデータライセンスの下で、厳選された代表的な日本語データを公開提供することは、AI 開発者が自社のシステムが日本市場で安全かつ効果的に機能することを検証するのに役立ちます。これは、それらのコンポーネントを自社の AI システムに統合しようとする日本企業にも利益をもたらします。さらに、AI セーフティ・インスティテュート（AISI）は、AI レッドチームングのための敵対的データ

¹⁰<https://www.japaneselawtranslation.go.jp/ja/laws/view/4241>

¹¹<https://www.japaneselawtranslation.go.jp/ja/laws/view/2975>

セットやコンテンツフィルタ開発用データセットなど、最も必要とされるデータセットを特定し、優先順位付けする上で重要な役割を果たし得ます。

政府が AI の安全性評価や具体的なガイドラインの策定を進める際には、日本の価値観と一致する国々に拠点を置く AI サービスプロバイダーとの継続的な連携を確保することを奨めます。これらの企業に政府の審議会等への参加を認めることは理想的であり、これにより、これらの事業者は、AI を活用したイノベーションと生産性向上を推進する価値ある技術や提案を提供する積極的なパートナーとなることができます。

結論

我々の提言をご検討頂けることに感謝します。計画案に関して、さらに議論できることを期待しています。今回の提言に関し、ご質問や詳細な協議のご希望があれば、ぜひお知らせください。