新AI事業者ガイドライン スケルトン（案）に対する
BSA| The Software Allianceからの提言

2023年10月27日

総論

BSA｜The Software Alliance[1]（BSA | ザ・ソフトウェア・アライアンス、以下BSA）は、AI事業者が責任を持ってAIを開発、導入、利用することを支援するための「新AI事業者ガイドライン」（以下、新AIガイドライン）の策定が総務省および経済産業省のリーダーシップのもとで進んでいることを高く評価しています。我々は、ガイドラインのスケルトン案[2]が、イノベーションを妨げない、産業界の自主的な取り組みを支援するリスクベースアプローチの考えを採用していることを支持します。BSAとBSAの会員企業は、リスクを最小化する適切な安全対策を講じながら、AI活用を加速していくという目標を達成するために、日本政府と連携していけることを期待しています。

BSAは、世界のソフトウェア産業を代表する主唱者です。BSAの会員企業は、AI、クラウドコンピューティング、データアナリティクスなど、世界的な経済成長を牽引する、ソフトウェアによって実現されるイノベーションの最前線にいます。社会のあらゆる分野でAIのメリットが活用され、人々の生活が劇的に変化し、複雑な問題が解決されることをBSAの会員企業は支えており、世界中のイノベーションを促進しています。[3] BSAの会員企業は最先端技術の開発を主導しており、そのため、BSAは、先端技術の大きな可能性、また、それらの責任ある開発と利用を支援するための最良の政策、その両方に関して、独自の見解を持っています。

---

[1] BSAの活動にはAdobe, Adobe, Alteryx, Altium, Amazon Web Services, Asana, Atlassian, Autodesk, Bentley Systems, Box, Cisco, Cloudflare, CNC/Mastercam, Dassault, Databricks, DocuSign, Dropbox, Elastic, Graphisoft, IBM, Informatica, Juniper Networks, Kyndryl, MathWorks, Microsoft, Nikon, Okta, Oracle, Palo Alto Networks, Prokon, PTC, Rockwell, Rubrik, Salesforce, SAP, ServiceNow, Shopify Inc., Siemens Industry Software Inc., Splunk, Trend Micro, Trimble Solutions Corporation, TriNet, Twilio, Unity Technologies, Inc., Workday, Zendesk, and Zoom Video Communications, Inc.が加盟企業として参加しています。詳しくはウェブサイト（http://bsa.or.jp）をご覧ください。

[2] https://www8.cao.go.jp/cstp/ai/ai_senryaku/5kai/gaidorain.pdf

[3] 詳細については、2022年6月13日にリリースされた、“Artificial Intelligence in Every Sector”を参照ください。 https://www.bsa.org/policy-filings/artificial-intelligence-in-every-sector

22F Shibuya Mark City West
1-12-1 Dogenzaka Shibuyaku,
Tokyo 150-0043

P +81 3 4360 5473
F +81 3 4360 5301
W bsa.org

Japan Representative Office

BSAは、AIのライフサイクルの過程で出現する可能性のあるリスクを特定・軽減するために、AIシステムが徹底的に検証され、これが適切に実施されていることを一般市民に対して保証すべきであることを認識しており、これを踏まえ、以下の見解と提言を述べさせて頂きます。加えて、今後のガイドライン案の策定に役立つと思われる関連資料を添付します。添付資料に含まれるのは、AIバイアスリスクを特定して軽減する影響評価の初めてのフレームワークである「バイアスに挑む：AIの信頼性構築に向けたBSAのフレームワーク」[4]（以下、BSAのフレームワーク）、開発者と導入者の異なる役割を説明し、AI市場における組織の役割に応じた義務を考慮するための「AI開発者と AI 導入者：重要な違い」[5]、また、サイバーセキュリティを強化するための効果的なAIツール活用法を説明した「AI and Cybersecurity（AIとサイバーセキュリティ）」[6]です。

上記の資料は我々の提言を詳細に説明するものとなります。 AI政策の検討において、我々は政府に以下を推奨します。

- リスクの高いAIユースケースのみに適用する
- 影響評価の採用を支持する
- AIの開発者と導入者の異なる役割と責任を認識する
- 国際的に認知されつつある規格と整合させる
- AIの責任ある安全な開発・導入に対応するためのライフサイクル・アプローチを取り入れる
- イノベーションを促進するデータおよび知的財産の政策を維持する

公表になっているスケルトン案に基づき、総務省と経済産業省に対し、AI事業者の責任に関する具体的な提言内容を以下に記します。

定義

AIシステムは国際的な文脈で開発・導入されるため、AIに適用される定義、対策、規格は、AI技術のさらなる導入と利用を促進するために、異なる法域での運用を可能とすべきです。我々は以下を推奨します： (1) 国際的に支持されている定義に沿ってAIシステムを定義する (2) 新AIガイドラインの対象となる高リスクのAIユースケースを部

[4] https://www.bsa.org/files/reports/2021bsaaibiasjp.pdf
[5] https://www.bsa.org/files/policy-filings/jp04102023aidevdep.pdf
[6] https://www.bsa.org/files/policy-filings/20231004aiforcybersecurity.pdf

分的に示して定義する。

AIシステムの定義：BSAは日本がOECDのAIシステムの定義を採用することを提唱します。OECDは、人工知能に関する理事会勧告（Recommendation of the Council on Artificial Intelligence）[7] において、AIシステムを「人間が定義した一定の目的のために、実環境あるいは仮想環境に影響を及ぼす予測、推薦又は意思決定を行う機械ベースのシステム」と定義し、AIシステムが「様々なレベルの自律性を備えて稼働するよう設計されている」と明言しています。この定義は、欧州連合[8]を含む世界中の規制当局によって参照されています。 米国国立標準技術研究所（NIST）も、2023年1月に発表したAIリスク管理フレームワーク [9]で使用するために、OECDの定義を採用しています。 OECDの定義のように、国際的に認知されたAIシステムの定義を用いることで、新AIガイドラインの国際的な整合性が保たれ、本ガイドラインに関する議論や、その採用、遵守を促進することが可能となります。

高リスクなAIユースケースの定義：我々はAIの政策に関し、リスクベースアプローチが採択されていることを強く支持し、個人に対して高リスクとなるAIの利用に焦点をあてて事業者の責任を検討することを推奨します。このリスクベースのアプローチを採用するために、ガイドライン案においては、高リスクAIとして特定すべきユースケースを部分的に示し定義すべきと考えます。これには、住宅、雇用、信用、教育、医療、保険などに関し、個人の適格性を判断するAIシステムが含まれます。一方、個人に対して高いリスクを生じさせないAIの例としては、サイバーセキュリティのユースケースが含まれます。例えば、ログイン時にIPアドレスのリスクレベルを検知する際のAI利用です。また、他にもAI対応ビデオゲーム、AI在庫管理システム等があります。

規格

AIに関与する主体の責任を検討するにあたっては、国際的に認知された規格が、責任あるAIを支える上で果たしている役割を認識することが重要です。AIに関する日本独自の規格を策定することを避け、国際標準化組織や技術団体の取り組みを活用し、調和のとれたAI規格を策定することを推奨します。

---

[7] 2019年5月 人工知能に関する理事会勧告 https://www.soumu.go.jp/main_content/000642217.pdf
原文：https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449
勧告では、AIのステークホルダーのコミュニティには「直接的なものであるか間接的なものであるかを問わず、AIシステムに関与するか、又はAIシステムから影響を受ける組織及び個人の全てが含まれる」としている。

[8] 欧州連合のAI規制法の草案では現在、「AIシステム」を「... 人間が定義した一定の目的のために、コンテンツ、予測、推薦、または作用する環境に影響を与える決定などの出力を生成できるソフトウェア」と定義しています

[9] 2023年1月26日 NIST AI Risk Management Framework https://www.nist.gov/itl/ai-risk-management-framework

国際標準化機構（ISO）のAI標準化委員会[10]は、AIシステムにおけるバイアスやAIにおける信頼性を高めるアプローチなど、10種類の標準化作業を完了しました。[11] 現在、ISO委員会はさらに27の規格を開発中です。国際的に認知された規格と整合性がとれない、あるいは、国際的に認知された規格より先行しすぎた国内規格を制定するリスクは、要件が新しい慣行と乖離し、日本でのAI開発や導入を抑止し、テクノロジーが責任を持って開発・展開されることを保証する取り組みを阻害することになります。国内規格と国際的に認知された規格との不整合は、日本で開発されたAIシステムがグローバルに採用される可能性も低下させます。これとは対照的に、国際的に認知された規格との整合は、国際的な相互運用性を向上させ、AI開発者と導入者の双方を含む日本の組織が、利用可能な最先端のリソース、考え、選択肢から恩恵を受けることを可能とします。

責任

BSAは、AIの開発と導入に関わる主体の役割を認識した、スケルトン案で提案されている自主的かつリスクベースなアプローチを歓迎します。

リスクベースアプローチ：多くのテクノロジーと同様に、AIテクノロジーに関連するリスクが生じる可能性は、AIシステムの開発のみではなく、その導入、また、その利用方法にもあります。AIに関連するリスクはコンテクスト固有であるため、事業者の責任は、特定のAIシステムの利用で生じるリスクの大きさを考慮して検討すべきです。特定の利用方法が実害となるリスクを生じさせるかどうを考慮せずに、すべてのAIのユースケースに同等の責任を適用することは、結果的に、AIの導入を促進し、一般市民を保護するという目的を損なうことになりかねません。実際、このようなアプローチは、低リスクな場面において、AIシステムを開発または導入しようとしている企業、特に、中小企業や新興企業にとって、大きなコンプライアンス負担となります。我々は、新たな規律やガイドラインにおいては、AIテクノロジーの高リスクな利用に焦点を当てることを強く推奨します。

責任の明確な分担：スケルトン案における「サプライチェーンを念頭に置いたリスク管理・ガバナンスの維持」という記述が示す通り、AIシステムの開発・導入には様々な企業が関与し得るという認識がされていることを我々は支持します。AIのバリューチェーンが多様であることを考慮し、AIのバリューチェーンにおける責任が公平で、相応であり、義務が割り当てられる場合、遵守する上で最も適した主体を対象とすることを推奨します。

[10] ISO/IEC JTC 1/SC 42: https://www.iso.org/committee/6794475.html
[11] ISO/IEC TR 24027: 2021 (Bias in AI systems and AI aided decision making)
https://www.iso.org/standard/77607.html?browse=tc
ISO/IEC TR 24028:2020 (Overview of trustworthiness in artificial intelligence)
https://www.iso.org/standard/77608.html?browse=tc

本ガイドラインにおいては、AIシステムの開発者と導入者を区別することを我々は強く奨めます。これにより、本ガイドラインで特定された責任がAIエコシステムにおける企業の役割を反映したものになります。AI開発者は、AIシステムを設計、コーディング、製造する企業を指します。例えば、音声認識のためのAIシステムを開発するソフトウェア会社です。対照的に、AI導入者は、AIシステムを利用する企業であり、例えば、AIシステムを利用して融資の判断を行う銀行などを指します。開発者は一般的に、AIシステムの学習に使用するデータの出所を特定し、その特徴を説明することができますが、他の企業がAIシステムを購入して導入した後に、そのAIシステムがどのように使用されているかの実態を見抜くことはできません。その代わり、AIシステムを利用する導入者は、一般的に、システムの実際の利用方法、そのような利用を促進するためにどのようなデータが収集されているか、人間によるどのような監視が実施されているか、システムの実際の運用に苦情が出ているかどうかを理解するために最も適した立場にいます。

現在、スケルトン案では、(1) AIのアルゴリズム開発者　(2) AIの学習実施者　(3) AIシステム・サービス実装者　(4) AIを活用したサービス実施者　(5) 業務でAIを利用する者など、様々な事業者を示していますが、これらの分類を簡素化し、AIシステムを開発する企業とAIシステムを導入する企業に焦点を当て、分類の定義を明確化することを強く推奨します。このような明確で焦点を絞った分類は企業が自らの義務を容易に特定するのに役立ちます。現在の分類を維持するのであれば、これらを開発者（AIシステムを開発する企業）および導入者（AIシステムを利用する企業）の一部として示すことを強く提案します。

影響評価：BSAは、人権や重要な生活機会へのアクセスに悪影響を及ぼしかねない方法でAIが利用される場合、そのようなシステムが徹底的に吟味され、関連するリスクを考慮するために継続的に監視されることが一般市民に保証されるべきであると考えます。BSA は、この目的を達成するために影響度評価を採用することを奨励します。リスクの高いAIを開発または利用する企業は、影響評価を実施するための包括的なアプローチを確立すべきです。影響評価は、環境保護から個人データ保護に至るまで、他の様々な分野で広く用いられています。これは、システムが潜在的なリスクを考慮した上で設計されていることを示し、信頼を促進するための説明責任の仕組みです。企業は既に影響評価を実施しているため、AI関連のリスクを特定し、軽減するのに容易に適用することができます。

透明性：スケルトン案の検討事項には、AIシステムの開発者が、そのシステムを利用する企業に対してどのように透明性を確保すべきかが挙げられています。BSAは、本課題の重要性を認識しており、リスクの高いAIシステムに関する重要な情報を、開発者が当該システムの導入者に提供することを求めることを支持しています。これには、例えば、システムの能力と限界、また、把握済みもしくは予見可能な個人に及ぼすリスクに関する情報が含まれます。また、我々は、AIシステムの開発者が、AIシス

テムに関する透明性を顧客に対して確保するために、様々な新しいリソースを作成していることを認識しています。これには特定のAIサービスに関する、意図されたユースケースや制限、責任あるAI設計の選択、導入や性能最適化のベストプラクティスに関する情報を提供する文書などが含まれます。本ガイドラインでは、リスクの高いAIシステムの導入者にこのような情報提供をする取り組みを支援し、その一方で、企業秘密を脅かしたり、プライバシーの懸念を生じさせたり、ネットワークや情報システムのセキュリティを損なったりする可能性のある、基礎となる学習データやその他の情報を開示するよう開発者に求めることは避けるべきです。

透明性を確保するもうひとつの手段は、ユーザーがAIで作られたコンテンツを識別できるようにすることです。AIやその他のツールの誤用を減らすために、業界団体が自主的に行っている取り組みがあります。例えば、多様なステークホルダーのコミュニティであるContent Authenticity Initiative（CAI）[12]は、コンテンツの真正性と来歴に関するオープンな業界標準の採用を推進しています。これにより、閲覧者は、撮影者、画像が生成された場所、ソフトウェアを使用して編集されたかなど、画像や動画の出所を知ることができます。これらの情報は、閲覧者がコンテンツの真正性を判断するのに役立ちます。900人以上のメンバーがいる同グループは現在、誤情報を防ぎ、AI利用に関する透明性を高めるためのオープンソース・ツールを開発しています。日本政府がこのような取り組みを支援することを我々は推奨します。

外部監査：スケルトン案では、外部監査についての記述がいくつかあります。これは企業が説明責任と透明性を示すための選択肢として提示されていると理解していますが、AIに関する監査可能な基準の策定のプロセスは始まったばかりであることから、本ガイドラインにおける監査の記述を削除することを推奨します。現在、下記のいずれかを企業が実施する上で、既存の手順やベストプラクティスはほぼありません。

(1) AIシステムを監査できる信頼できる法人を選ぶ

(2) そのような監査法人がどのような基準を適用すべきかを決定する

実際、ISOはいくつかのAI関連規格を発行しており、その中にはリスク管理の実践に関するガイダンスも含まれますが、他の多くの規格はまだ開発中です。現在、AIシステムに対応する十分な自主的コンセンサスに基づく規格が不足しています。共通の基準がなければ、監査の質は大きく異なります。監査によって異なるベンチマークで測られる可能性があり、客観的なベンチマークに基づく評価を得るという目標が損なわれます。

[12] https://contentauthenticity.org/

さらに、特定の基準を満たし、AIシステムの監査を行う資格があることを示した信頼できる法人により監査が実施されることを保証する明確な方法がありません。既存の監査法人の間にはばらつきがあるため、組織は自分たちが好む基準、方法、範囲に基づいて監査人を選ぶことが可能となり、その結果、監査の信頼性が低くなり、説明責任を実証するという目的が意図せず後退する可能性もあります。監査人が倫理基準を遵守するためには、AI監査人を管理する専門機関が重要ですが、これが存在しないため、前述の懸念は悪化しています。また、革新的なソリューションの開発に多額の投資をしてきた組織の知的財産を損なう重大なリスクも懸念されています。このような監査が要求されたとすれば、知的財産を保護するために、限られた人員のみしか機密情報やデータにアクセスできない、厳格に管理された環境（「クリーンルーム」環境）下で実施する必要が生じるため、多額な費用を要する取り組みとなります。

また、BSAは透明性を促進する必要性を理解していますが、監査結果を公表することは、企業がAIシステムの厳格な評価を受ける意欲を失わせる可能性があるため、監査結果を公表しないことを推奨します。このような理由から、外部監査は透明性を達成するための適切な解決策ではありません。

AI導入の促進

クラウド導入の促進：クラウドコンピューティングの利用を可能にすることは、AIテクノロジーの可能性を最大限に活用するために不可欠です。クラウドコンピューティングはAI開発の最前線にあり、AIテクノロジーの多くはクラウド導入を前提に特別に開発され、調整されています。グローバルなクラウドサービスプロバイダーが提供する商用クラウドサービスを含む、様々な最先端のクラウドサービスを公共部門や民間部門において利用可能とし、推奨する政策を日本政府が確実に実行することを求めます。また、匿名化・仮名化されたデータの利用に係る政策においては、過度な規制や、当該データの利用にあたり、規制当局の事前承認を要することは避けるべきです。これにより、日本企業は、革新的なAIソリューションを開発・導入する上で、最新のAIテクノロジーと、最も広範で高品質なデータセットを利用することが可能となります。

結論

BSAと会員企業は、効果的なAI政策の策定をしていく、という目標を支援するために、総務省と経済産業省に協力していけることを期待しています。本提言を共有することに加え、この取り組みを今後どのように支援していけるかについて話し合う機会を継続的に頂ければ幸いです。