

2025 年 1 月 23 日

AI 戦略会議・AI 制度研究会 中間とりまとめ（案）に関する意見

該当箇所	ページ数	行番号	意見のカテゴリ (賛成又は反対)	意見のカテゴリ (事実誤認又は事実誤認以外)	意見
II. 制度の基本的な考え方 4. 国際協調の推進 (2) 国際整合性・相互運用性の確保)	12p	21-37	賛成	事実誤認以外	Business Software Alliance (ビジネス・ソフトウェア・アライアンス、以下 BSA) *は AI 戦略会議・AI 制度研究会の「中間とりまとめ（案）」(以下、とりまとめ案)に関する意見を提出する機会が得られたことに感謝します。 [*ビジネス ソフトウェア アライアンス (www.bsa.org) は、エンタープライズソフトウェア業界のグローバルな業界団体であり、人工知能、サイバーセキュリティ、クラウ

				<p>ドコンピューティング、その他の最先端技術におけるリーダー企業を代表しています。米国、欧州、アジアの 20 を超える市場で活動し、あらゆる産業分野および一般市民がイノベーションの恩恵を受けられるよう、技術に対する信頼を構築する政策を提唱しています。BSA の会員には以下の企業が含まれます: Adobe, Alteryx, Amazon Web Services, Asana, Atlassian, Autodesk, Bentley Systems, Box, Cisco, Cloudflare, Cohere, Databricks, DocuSign, Dropbox, Elastic, EY, Graphisoft, HubSpot, IBM, Informatica, Kyndryl, MathWorks, Microsoft, Notion, Okta, OpenAI, Oracle, PagerDuty, Palo Alto Networks, Rubrik, Salesforce, SAP, ServiceNow, Shopify Inc., Siemens Industry Software Inc., Trend Micro, TriNet, Twilio, Workday, Zendesk, and Zoom Video Communications, Inc.]</p> <p>BSA は、AI システムが責任を持って開発・利用されることを確実にする政策を支持します。今日のテクノロジーをとりまくエコシステムは、そのグローバルな性質により、イノベーションを促進するための協調的な政策対応を必要としています。この点において、イノベーション促進とリスク対応の両立の重要性や、AI ガバナンスに不可欠な国際整合性と相互運用性を推奨しているとりまとめ案を我々は支持します。高リスクな AI の利用のみに法規制を適用するリスクベースのアプローチを採用し、広島 AI プロセス</p>
--	--	--	--	--

				<p>における行動規範のための OECD の報告枠組みなど、国際的なベストプラクティスの枠組みを活用して国際規範との調和に向けた取り組みを政府が続けていくことを推奨します。このような整合性により、企業による報告作業の重複が回避され、一貫性が保たれます。</p> <p>また、日本がマルチステークホルダー間の対話を通じて相互運用性を引き続き追求し、共通の AI 課題に対処するためのリスクベースの政策アプローチに関する共通ビジョンを策定することを推奨します。リスクベースの規制アプローチに基づき、AI バリューチェーンにおける役割に応じて公平な責任分担をし、AI の高リスクな利用に焦点を当てた、責任ある AI ガバナンスの規範を推進していくことを我々は奨めます。</p> <p>とりまとめ案において認識されているように、OECD や GPAI を通じて AI に関するグローバルな規範設定を主導する日本のリーダーシップを我々は高く評価しています。AI に関連する多くの機会と課題に関しては、世界規模で検討されていることから、日本が同盟国と協力して相互運用可能な政策対応を引き続き調整することが重要と考えます。この点において、相互運用性を高め、国際整合性を推進するために、日本の AI セーフティ・インスティテュートが「AI 事業者ガイドライン」と米国 NIST の「AI リスク管理フレームワーク」を比較したクロスウォークを公表した</p>
--	--	--	--	--

					ことを歓迎します。我々は、各国における国内の規制制度のギャップを埋めるために、日本が貿易相手国と共に国際的な技術基準を策定することを奨励します。
II. 制度の基本的な考え方 2. 関係主体 (1) 主な主体	5p	17-27	反対	事実誤認以外	<p>AI バリューチェーンにおける多様な主体がとりまとめ案において認識されていることを高く評価します。AI システムの開発と利用において異なる役割を持つ様々なタイプの企業を区別するために定義を決めることを強く支持します。こうした役割を明確に定義することは極めて重要であり、これにより、どのような法制度においても各役割に対して明確で適切な義務を課すことが可能となります。</p> <p>とりまとめ案では、(1) 開発者 (2) 提供者 (3) 利用者という3つの異なる役割が認識されていますが、これらの役割間の明確な区別がされていないことを我々は懸念しています。</p> <p>主要な国際的アプローチに沿い、システムを設計する「開発者」とAI システムを利用する「導入者」を、より明確に定義することを奨めます。具体的には、以下の定義を推奨します。</p> <p>開発者(developer)：日本国内におけるAI システムの一般利用を可能にする主体であり、(1) 特に高インパクトのAI システムとなることを意図してAI システムを設計し、(2) 高インパクトAI システムを大幅に変更する、または(3) 高</p>

					<p>インパクト AI システムではない AI システムを大幅に変更して高インパクト AI システムとする主体。</p> <p>導入者(deployer)：高インパクトの AI システムを利用する主体。</p> <p>もう一つの役割を日本政府が認識するのであれば、AI システムを「提供する」企業という曖昧な用語ではなく、AI モデルやシステムを製品やサービスに「インテグレート（統合、integrate）」する企業に焦点を当てた定義を強く推奨します。以下が、インテグレーターを定義する一つの考え方です。</p> <p>インテグレーター (integrator)とは、(1) ソフトウェアまたはプラットフォームを利用して顧客をサード・パーティーの高インパクト AI システムにつなぐ、または(2)サード・パーティーが利用する製品またはサービスに、高インパクト AI システムの実質的な変更を加えることなくインテグレートする主体。</p>
II. 制度の基本的な考え方 2. 関係主体	6p	14-24	賛成	事実誤認以外	<p>とりまとめ案では、国外事業者についても国内事業者と同じく法制度の対象とすることが提言されています。主要な国際的アプローチに沿って、「国外事業者」をより明確に定義することを提案します。</p>

(2) 国外事業者					<p>また、「国外事業者」に関連する制度やルールは、日本語と同時に英語で公表すべきと考えます。</p>
<p>III. 具体的制度・施策の策定</p> <p>1. 全体的な事項</p> <p>(2) 安全性の向上等</p> <p>①AI ライフサイクル全体を通じた透明性と適正性の確保</p>	<p>13p 14p</p>	<p>35-36 1-30</p>	<p>賛成</p>	<p>事実誤認以外</p>	<p>とりまとめ案が、リスクベースのアプローチを採用し、AI エコシステムにおける主体の異なる役割と義務を反映することの重要性を認識していること高く評価します。</p> <p>とりまとめ案では、リスクに対応するために、AI 開発者—提供者、提供者—利用者間の情報共有を奨めています。とりまとめ案において正しく認識されているように、バリューチェーン内の異なる主体は、AI システムの特性、能力、限界、開発方法、運用方法について、それぞれ異なる情報を持ちます。このため、これらの企業は情報共有能力が他の主体と異なることとなります。この点を明確にし、異なる主体間の透明性を支援することを目的に、BSA は「汎用 AI (GPAI) のバリューチェーンにおける情報共有のベストプラクティス」を作成しました。これが政府にとって有益な参考資料となることを期待し、下記に共有します。</p> <p>https://www.bsa.org/files/policy-filings/jp09032024aiinfosharing.pdf</p> <p>また、とりまとめ案において、機密情報の開示を避けるために情報共有を制限することの重要性が認識されているこ</p>

				<p>とを支持します。政府の広範な情報収集に協力することを企業に義務付けることは、多大な負荷を企業に強いることとなります。これは、リスクを実質的に軽減することなくAIの実装を遅らせることとなります。したがって、企業から情報収集する際の指針を策定する際には、基礎的な学習データやその他の情報に関し、知的財産や企業秘密を含む可能性がある場合、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危険にさらす可能性がある場合は、開示要件を課すことを避けるようにすべきです。事業者が提供する情報の機密性を政府が保持することは重要であり、とりまとめ案で提唱されているAI法案の策定においては、情報公開を義務づけないことを推奨します。</p> <p>また、説明責任要件の目的を我々は理解していますが、この目標を達成するにあたっては、企業が柔軟に対応できるようにすることを政府に推奨します。テクノロジーが日々発展していく性質をもつ以上、そのような義務を果たすには、実務的な限界があることを踏まえるべきです。また、AIの高リスクな利用に関しては、適切な人的監視やテスト等も代替的な保護策として政府は検討すべきです。</p> <p>また、とりまとめ案においては、AIライフサイクル全体を通じた透明性と適正性の確保にあたり、広島AIプロセス等の国際的な規範の趣旨を踏まえた指針を政府が整備する</p>
--	--	--	--	--

					<p>ことを推奨しています。2024年に「AI事業者ガイドライン」が策定され、AIの開発者、提供者、利用者向けに詳細な指針が提供されていることを踏まえ、新たな法律の下で策定される可能性がある新たな指針と、これらの既存のガイドラインとの重複を避けるように求めます。政府からの重複する詳細な指針は、義務ではないとしても、AIのイノベーションのペースを遅らせる可能性があります。</p>
<p>III. 具体的制度・施策の策定</p> <p>1. 全体的な事項</p> <p>(2) 安全性の向上等</p> <p>③ 重大インシデント等に関する政府による調査と情報発信</p>	<p>15p</p> <p>16p</p>	<p>31-37</p> <p>1-15</p>	<p>反対</p>	<p>事実誤認以外</p>	<p>とりまとめ案では、「多くの国民が日々利用するようなAIモデルについては、政府がサプライチェーン・リスク対策を含むAIの安全性や透明性等に関する情報収集を行う」ことが奨められています。個人に高いリスクをもたらすユースケースに焦点を当てた政策を我々は強く支持しており、この点において、利用の広さではなく、AIモデルのリスクの度合いに焦点を当てることを推奨します。国境を越えるリスクに対処し、技術の開発と利用における国際協力を可能にするためには、世界的に一貫したAIガバナンスの枠組みを策定することが重要です。高リスクのAIに焦点を当てた、リスクベースのアプローチを採用し、低リスクで、高い価値のあるAIに対し不要な規制を課すことは避けることを政府に強く推奨します。例えば、電子メールのスパムフィルターなど、最小限のリスクで大きな価値をもたらすAIの利用事例は数多くあります。広島AIプロセスが高度なAIに焦点を当てていること、またEUのAI法やその他の地域におけるAI関連の立法案がリスクベースのアプローチを採用し、高リスクな分野を優先している</p>

				<p>ことを踏まえると、国際的な整合性を維持することが重要であると考えます。</p> <p>また、AIの高リスク利用と低リスク利用を明確に区別し、高リスクな利用の定義・区別、また、そのような区別により、政府の情報収集がどのように適用されるのかを示すことを推奨します。例えば、AIシステムが、個人の適格性を判断して住宅、雇用、信用、教育、公共施設への物理的なアクセス、医療や保険の提供または拒否につながる重大な決定を下す場合、高リスクであると考えられます。</p> <p>さらに、とりまとめ案では、重大インシデントに関し、政府が調査や情報発信を行うことを推奨しており、インシデントが生じているといえるか否かの判断は、上述した「情報収集・把握を通じて政府に蓄積された事例や知見をもとに判断していくことが重要」と述べています。</p> <p>AIインシデントの報告枠組みを策定することに関し、政府は慎重になるべきであると我々は考えます。原因の特定、報告を行うべき主体、報告を受けつける適切な場など、枠組みを策定する上では様々な課題があります。また、報告枠組みが課すコンプライアンスの負荷に関連したところでは、複数のインシデントに関する情報の収集・保管により得られる恩恵は限定的です。また広範な開示はサイバーセキュリティの脅威を生じさせる可能性があります。</p>
--	--	--	--	--

				<p>それでも、政府がこのような枠組みの策定を進めるのであれば、「重大インシデント」の定義を明確にし、インシデントの範囲を死亡や重傷などの最も深刻な被害に絞り、既存の報告枠組みの対象範囲との重複を避け、事業者が複数の省庁に重複した情報提供をすることを義務づけないようにすることを推奨します。また、とりまとめ案は、一定の状況下で、外部のステークホルダーに対してインシデントを知らせるべきであると提案しています。重大インシデントに対応することの重要性を我々は認識していますが、影響を受けるステークホルダーの特定を含め、政府は、上述のような実装上の様々な課題を考慮すべきであると考えます。</p> <p>また、AIのバリューチェーンは多様かつ複雑であるため、特に重大インシデントの場合、AI利用者の役割と責任を明確にすべきと考えます。企業間（B2B）の文脈においては、導入後にAIに送信されるデータを最終的に管理し、AIの構築方法を指示し、AIシステムを利用するタイミングと状況を決定し、そして最も重要なこととして、AIシステムによって生成された結果の利用方法を決定するのは、多くの場合、利用者です。AI利用者は一般的に、システムがどのように利用されているかに関し、詳細な情報を提供できる最適な立場にあり、データ入力およびAIシステムによって生成された出力に関する、より深い洞察力を有し</p>
--	--	--	--	--

					<p>ています。AI システムの利用が自社のユースケースに適切であるかどうかを評価し、適切なテストを実施する責任を負う等、AI の安全性と責任ある利用を確保するために利用者が重要な役割を果たすことを明確にすることを推奨します。利用者は重大インシデントを回避するために重要な役割を果たしているのです。</p>
<p>III. 具体的制度・施策の策定 1. 全体的な事項 （2）安全性の向上等 ②国内外の組織が実践する安全性評価と認証に関する戦略的な促進</p>	15p	1-30 行	賛成	事実誤認以外	<p>とりまとめ案においては、第三者認証に関して数カ所で触れられています。この点において、慎重なアプローチがとられていることを我々は評価します。サイバーセキュリティやプライバシーと異なり、現時点では AI に関する監査可能な基準が成熟していません。現在、以下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択する。（2）上記の監査法人がどのような基準を適用すべきかを決定する。</p> <p>ISO はいくつかの AI 関連規格を発行していますが、多くの規格は他の機関において開発中です。また、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基準で測られる可能性があり、客観的な基準に基づく評価を得るという目標が損なわれます。</p>

					<p>また、透明性を促進する必要性を我々は理解していますが、機密情報や専有情報を含む監査結果を公表することを事業者に求めないことを推奨します。公表することは、AIシステムの厳格な評価を受ける意欲を企業に失わせることとなります。</p> <p>高リスクのユースケースに関し、社内での徹底した影響評価の実践を奨励することで、ビジネスのイノベーションを妨げることなく、有意義な保護策を講じることができます。</p>
III. 具体的制度・施策の策定 3. 生命・身体の安全、システミック・リスク、国の安全保障に関わるもの	18p	3-20	賛成	事実誤認以外	「基盤サービス」に関するリスクは、十分に対応可能な範囲において既存の法律で対処することが妥当とする考えに同意します。「基盤サービス」を新たなAI規制に含める必要がある場合、個人の生命・身体の安全等、差し迫ったリスクをもたらす基盤サービスにおけるAIの利用を対象とするよう明確にすべきです。
III. 具体的制度・施策の策定 2. 政府等による利用	16p	17-21	賛成	事実誤認以外	政府によるAIの利用を促進するという、とりまとめ案の提言を歓迎します。とりまとめ案において「政府」をより明確に定義すること、特に、政府出資の企業にも適用されるかどうかについて明示することを推奨します。
II. 制度の基本的な考え方	7p	16-28	賛成	事実誤認以外	高い安全性があるAIシステムが市場において拡大することを促進するため、とりまとめ案では、認証取得者へのインセンティブを付与し、認証取得事業者を増やすことを提

<p>3.イノベーション促進とリスクへの対応の両立 (1) イノベーションの促進 ② 事業者による利用</p>					<p>言っています。AIの監査基準がまだ成熟していないことを踏まえ、現段階では、第三者認証ではなく、リスクの高いユースケースに対して、徹底した社内での影響評価実施に重点を置くことを推奨します。環境が成熟し、将来的にこのようなインセンティブ措置が講じられる場合には、「国内事業者」と「国外事業者」の両者が、日本の「認証取得事業者」になれることを確実にすることを求めます。</p>
<p>II.制度の基本的な考え方 3.イノベーション促進とリスクへの対応の両立</p>	6p	26-29	賛成	事実誤認以外	<p>とりまとめ案において強調されているように、AIは、国民経済の発展に大きく寄与する可能性があります。特に、生成AIは、日本社会を劇的に変革させ、日本の強みであるコンテンツ産業の強化や、多くの産業分野の改善に貢献することができます。生成AIは、スキルや能力に関係なく、あらゆる表現手段において人間が作品を容易に創ることを可能とします。政府が著作権および知的財産に関する現行の政策を維持し、生成AIモデルの開発を支援し、さらに促進することを推奨します。著作権法第30条の4の柔軟な規定は、社会利益のために企業が新しい有用なサービスを開発し、提供することを可能とします。モデル開発者が生成AIモデルを開発するために十分な品質の学習データに引き続きアクセスできるようにすることを我々は強く求めます。</p> <p>また、AI開発者や導入者に利用者の行動すべてに責任を負わせるような厳格な責任規定を適用することは避けるべき</p>

				<p>です。そのような規定はこの分野への参入に際して、財務上および技術上の大きな追加的障壁を課すことになり、その結果、小規模なスタートアップ企業の参入を阻むこととなります。著作権のある素材を含む学習データの入手が日本において限定されるという障壁は、AI 学習の業務を海外に移すインセンティブをモデル開発者に与えることになり、日本国内での AI 開発を促進する機会を逸することとなります。</p>
--	--	--	--	---