MORI HAMADA

Data Security Newsletter

2025年1月15日

AIに係る法整備に向けた動向
～AI戦略会議・AI制度研究会「中間とりまとめ（案）」の公表～

弁護士 岡田 淳
TEL. 03-5220-1821
atsushi.okada@morihamada.com

弁護士 飯野 悠介
TEL. 03-6266-8942
yusuke.iino@morihamada.com

Ⅰ. はじめに

政府のAI戦略会議の下で、法制度の要否を含むAI制度のあり方について2024年7月から検討を行ってきたAI制度研究会は、2024年12月26日、「中間とりまとめ（案）」（以下「中間とりまとめ案」といいます）を公表しました。中間とりまとめ案について、政府は同月27日から2025年1月23日までパブリックコメントを募集しています。

中間とりまとめ案は、イノベーション促進とリスク対応の両立を重視する方針の下、事業者の自主的な対応を尊重し、また既存の個別法令等の活用を前提としつつも、「政府による指針の整備・対応やAIに関する実態の調査・把握にあたっては、事業者による自主的な対応も重要であるが、実効性を確保することが必要であるため、事業者の活動にもたらす影響等を考慮しつつ、法制度により実施すべきである」と明記し、AIに係る速やかな法整備に向けた提言を行っています。今後、政府としては、寄せられたパブリックコメントを踏まえて、2025年の通常国会での法案提出を目指すことが予想されます。

本ニュースレターでは、中間とりまとめ案のうち、特に法整備という観点から民間事業者への関係が深い論点にフォーカスして解説します。

Ⅱ. 中間とりまとめ案の公表に至る背景

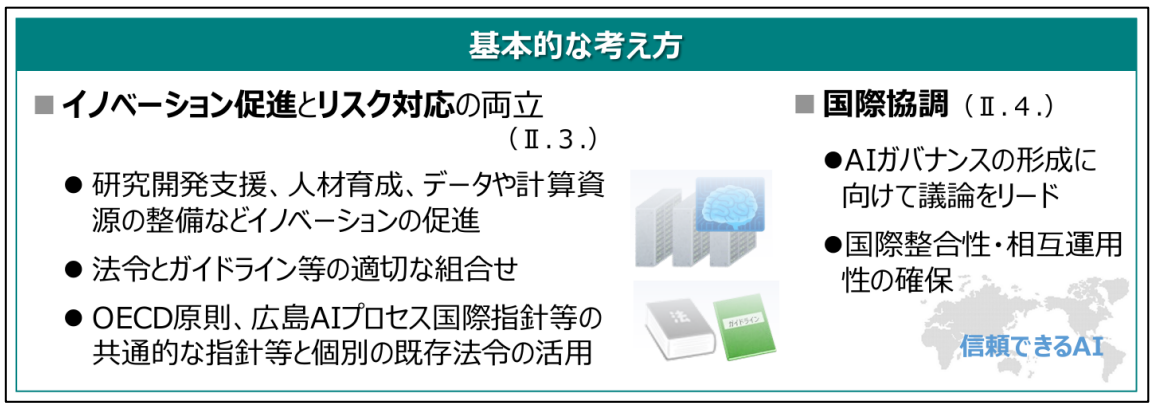
AI は国民生活の向上や国民経済の発展に大きく寄与する可能性がある一方、犯罪巧妙化のリスク、偽・誤情報の作成による情報操作、安全保障上のリスクなど多様なリスクが顕在化しつつあります。このようなリスクに対し、これまで日本では既存の法令やソフトロー（ガイドライン等）を中心として機動的に対応してきたものの、AI に関する国民の意識調査結果によれば、日本では「現在の規則や法律で AI を安全に利用できる」と思う回答者は 13%と低く、77%の人が「AI には規制が必要」と考えているなど、AI に対する不安の声も大きいのが実状です。また、欧米を中心とする各国においては AI に関する法制度の議論や検討も本格的に進んでいます。

そのような状況をふまえ、2024 年 7 月、政府は AI 戦略会議の下で AI 制度研究会を設置し、事業者、有識者、自治体を含む様々な関係者からヒアリングを行い、法制度の要否を含む AI 制度のあり方について検討を行ってきました。今回の中間とりまとめ案は、当該ヒアリングや議論を踏まえた検討結果を取りまとめたものです。

Ⅲ. 制度の基本的な考え方（中間とりまとめ案Ⅱ）

中間とりまとめ案は、「Ⅱ. 制度の基本的な考え方」において、今後の AI 制度設計に向けた基礎となる考え方を整理しています。とりわけ、AI はその開発・利用方法等によっては様々なリスクを生じさせ得る一方で、国民生活の向上、国民経済の発展に大きく寄与する可能性があるとし、AI の研究開発・実装がしやすい国を実現するため、「イノベーション促進とリスクへの対応の両立」の重要性を強調しています。また、広島 AI プロセスをはじめとする国際的な AI ガバナンスの議論や、国際整合性・相互運用性の確保のための AISI（AI セーフティ・インスティテュート）による取組など、国際協調の推進という観点も踏まえた検討が必要であるとしています。

〔基本的な考え方の概要（中間とりまとめ案の概要（1 頁）より抜粋）〕



上記のような基本方針を踏まえ、中間とりまとめ案Ⅱ.3.は、「イノベーション促進とリスクへの対応の両立を確保するため、法令とガイドライン等のソフトローを適切に組み合わせ、基本的には、事業者の自主性を尊重し、法令による規制は事業者の自主的な努力による対応が期待できないものに限定して対応していくべき」という方向性を明確にしています。

すなわち、技術の発展やサービスの変化が急速な AI の分野において、過度な規制により研究開発やサービスの開発・展開を抑制させてしまうことは、将来にわたって日本の国際競争力を損なう危険性があるとし、これまでの日本における既存法令を中心とした対応（例：個人情報保護委員会による注意喚起（2023 年 6 月）、文化審議会著作権分科会法制度小委員会による「AI と著作権に関する考え方について」（2024 年 3 月）、内閣府の AI 時代の知的財産権検討会による「中間とりまとめ」（2024 年 5 月））やソフトローによる迅速かつ柔軟な対応（例：総務省・経済産業省による「AI 事業者ガイドライン」（2024 年 4 月。同年 11 月改定））の意義を肯定的に評価しています。

他方で、中間とりまとめ案は、ソフトローでは事業者等の自主的な対応に頼らざるを得ないという限界も指摘しています。そして、AI の急速な発展に伴い今後新たに顕在化するリスクについても各分野の内容に応じて適切に対応する必要があるとし、特に「人の生命、身体、財産といった人間の基本的な権利利益や社会の安全、我が国の安全保障に対して実際に重大な問題を生じさせる、あるいは生じさせる可能性の高い AI に対しては、そのリスクの内容や当該リスクの社会的な影響の重大性に応じて規律の必要性の有無を検討すべき」と指摘しています。新たな法規制を導入する場合の留意点としては様々なものがありますが、特に以下のような視点が示されていることは注目されます。

1. リスク構成要素の分析に基づく必要最小限の規制

中間とりまとめ案Ⅱ.3.は、仮に法律上の規制による対応を行う場合には、事業者の活動にもたらす影響の大きさを考慮しつつ、AI のもたらすリスクを踏まえた上で、「真に守る必要のある権利利益を保護するために必要な適用内容とすべき」であり、その際に「政府と事業者との役割分担を意識した上で、何が規制の対象となり、事業者の活動はどこまで許容されているのかといった線引きを明確化することが重要である」としています。その前提として、「AI のモデルや用途が様々存在する中で、開発、提供、利用といった AI のライフサイクルの各場面において顕在化する可能性のあるリスクとは、いかなる種類の AI モデルのどのような性質に起因するリスクであって、誰にどのような影響を与えるものかといった要素を分析する必要がある」としています。

また、その際の検討の視点として、例えば以下のようなポイントを挙げています。

規制の技術中立性の原則	「規制はその目的を達成するために、特定の種類の技術の使用を強制したり、優遇したりすべきではない」という原則を踏まえた検討も重要である。
正当な研究等の保護	AI の安全性に関する正当な研究を行うために不適切な AI を試作するケース等における規制の適用については、その要否も含め検討を行う必要がある。
スタートアップ企業等の負担の考慮	広く事業者一般を対象とする制度を検討する際には、スタートアップ企業も含め、どのような規模の事業者であっても対応可能なものとなるよう、制度への対応に伴う事業者の負担を考慮する必要がある。

2. 罰則の要否

一口に新たな法規制を導入するといっても、義務の内容や違反時の執行等をめぐって様々なバリエーションがあり得ます。その意味では、もはやハードローとソフトローの境界は個別の制度設計に応じた相対的なものにすぎず、イノベーションに親和的な内容のハードローも十分存在し得るところです。この点につき、例えば罰則の要否という観点から、中間とりまとめ案Ⅱ.3.(2)は以下のように述べ、罰則を伴わない法規制の導入という選択肢に明示的に言及していることも注目されます。

> 「法令に基づく罰則がある場合には、公的機関が何かしらの強制力を発動することが可能であり、規律の実効性の確保が得られやすいという利点がある一方で、規制を行った分野の発展を阻害する可能性があるほか、国民の権利利益に影響を及ぼす規制が明確である必要があることに鑑み、その範囲を検討するには一定の時間を要するため、柔軟性に欠けるといった欠点がある。その他、規制を伴わない法令であっても、法令に事業者の義務や責務が明記されること自体によって国内外の事業者に対し規律を働かせ、一定の実効性を確保することが可能である。」

3. AI の規模等に応じた区別は合理的か

諸外国では、学習の計算量といった AI の規模や利用者数に応じて規制の有無・程度に差異を設けているケースがみられます。この点、様々なタスクを処理できる汎用型 AI は、一般的に学習データやモデルのパラメータ数が多くなれば性能が向上すると考えられていましたが、最近では学習データ等の規模によらず性能が高いものも登場しています。中間とりまとめ案Ⅱ.3.(3)は、このように「規模に依存しない高性能な AI が開発されていること等を踏まえ、どのような要素を考慮すべきか検討が必要である」としており、AI の規模等に応じて規制に差異を設けるべきかという点に対して留保を付しています。

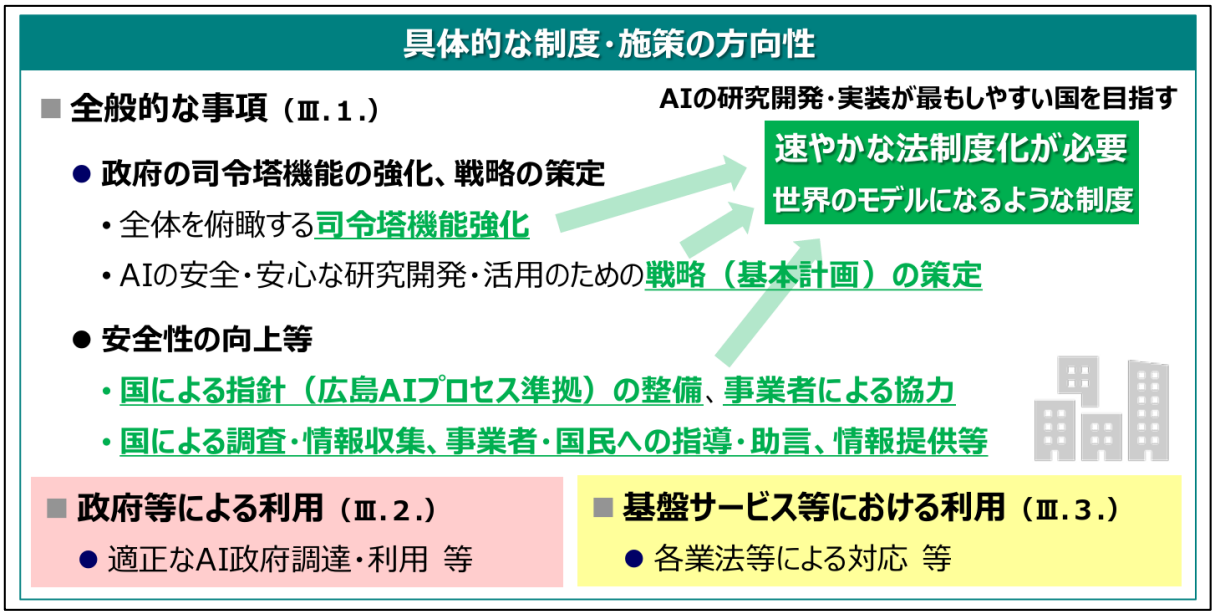
4. 国外事業者への対応

国内で利用される生成 AI の多くは国外事業者が提供しています。そのため、中間とりまとめ案Ⅱ.2.(2)は、国外事業者に対しても制度の実効性を確保するために国外事業者も明確に対象とするルール化を検討すべきであるとし、実務においては、国外事業者の日本支社や日本における代表者等を通じて対応を求めること等も考えられる、としています。

Ⅳ. 具体的な制度・施策の方向性(中間とりまとめ案Ⅲ)

中間とりまとめ案は、上記の基本方針を前提として、「Ⅲ. 具体的な制度・施策の方向性」において、今後の法制度化を含む具体的な制度・施策の方向性を提言しています。

〔具体的な制度・施策の方向性の概要(中間とりまとめ案の概要(1 頁)より抜粋)〕



中間とりまとめ案が提言する各施策の中には、必ずしも現時点での法制度化を求めているわけではないものもありますが、以下では、民間事業者への影響という観点から、法制度による対応が適当である旨が提言されている項目に絞って解説します。

(1)政府の司令塔機能の強化、戦略の策定(中間とりまとめ案Ⅲ.1.(1))

中間とりまとめ案は、AI の研究開発から活用に至るまでに介在する多様な主体や過程における取組が互

いに密接に関連し、一体的 ・横断的に行われる必要があるため、研究開発から経済社会における活用までの一体的な施策を推進する政府の司令塔機能を強化すべきことを提言するとともに、総合的な施策の推進にあたっては司令塔が戦略(基本計画)を策定する必要があるとしています。そして、AI の司令塔機能の強化や、司令塔による関係行政機関に対し協力を求めることができる等の権限を明確化するため、法定化すべきであるとしています。

(2)安全性の向上(中間とりまとめ案Ⅲ.1.(2))

中間とりまとめ案は、AI の安全性を向上させるためには、①研究開発から活用までのライフサイクルにおいて、少なくとも透明性や適正性を確保していく必要があること、②事業者が自主的に取り組む安全性評価や第三者による認証などを活用することも一つの有効な手段となること、③政府が、進化の著しい AI の技術や利用動向等の実態を調査して情報提供を行うとともに、必要に応じて、関係各主体に対応を求めていくべきこと、を示しています。そして、これらの事項のうち、政府による指針の整備・対応や AI に関する実態の調査・把握にあたっては、事業者による自主的な対応も重要であるものの、実効性を確保することが必要であるため、事業者の活動にもたらす影響等を考慮しつつ、法制度により実施すべきであると提言しています。個別の項目ごとに対応の方向性を簡単に整理すると、下表のようになります。

① **AI ライフサイクル全体を通じた透明性と適正性の確保**	AI の安全・安心な研究開発や活用には、開発者－提供者間、提供者－利用者間において必要な情報を共有する透明性を確保すべきである。他方で、事業者の事業運営に過度な負担や広汎すぎる情報開示とならないようにするため、情報の共有は真に必要な範囲に留めることが重要である。 ➡適正性の確保にあたっては、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**等し、**事業者に対し各種規範等に対する自主的な対応を促していく**ことが適当である。 ➡透明性の確保を含む適正性の確保については、調査等により政府が事業者の状況等を把握し、その結果を踏まえて既存の法令等に基づく対応を含む必要なサポートを講じるべきである。**政府による事業者の状況等の把握や必要なサポートについては、事業者の協力なしでは成り立たないため、国内外の事業者による情報提供等の協力を求められるように、法制度による対応が適当である。**
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**	安全性の評価や認証制度(①AI システムに関する評価・認証、②AI を利用する組織のガバナンス等に関する評価・認証)は有効な手段である。

な促進	**➡国内における制度整備は、国際的な規範を踏まえ、かつ、制度の実効性も考慮し対応すべきである。**AI の評価や認証を実施する場合には、利用者や利用目的に従ってレベルを設けることや、一定の安全性を確認するための利用者の負担が軽減する仕組みや評価・認証を実施する機関を認定する仕組みを構築できれば、より効果的で持続可能な制度となると考えられる。ただし、この仕組みを構築する際は、AISI や ISO 等の活動を前提にしつつ、どのような主体を巻き込み、どのような基準で評価を行っていくのか、詳細な検討が必要である。
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	技術及び事業活動の双方の側面から時々刻々と変化する AI の開発、提供、利用等に関する実態をまず政府において情報収集・把握し、事業者において AI が効果的かつ適正に利用されるとともに、広く国民が AI の研究開発や活用の促進に対する理解と関心を深められるよう、企業秘密等に配慮しつつも説明責任を果たせるように、必要な範囲で国民に情報提供することが適当である。 ・ 中でも、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。また、基盤サービス等における AI 導入の実態等に関しては、政府による情報収集が重要である。 ・ AI の利用に起因する重大な事故が実際に生じてしまった場合、政府としては、その発生又は拡大の防止を図るとともに、AI を開発・提供する事業者による再発防止策等について注意喚起を行っていく必要がある。 ➡この調査や情報発信は事業者の協力なしでは成り立たないため、**国内外の事業者による情報提供等の協力を求められるように、<u>法制度による対応</u>が適当である。**

上記整理からも分かるとおり、民間事業者の観点からみれば、法制化の主眼は透明性・適正性の確保や国による実態の調査・把握のための官民協調という点（特に、国に対する情報提供等の協力）にあるため、現時点で想定されている新法は、厳格な行為規制や体制整備といった義務を課すものではないと見込まれます。もっとも、比較的緩やかな義務付けとはいっても、情報提供等の協力義務の範囲や例外、政府が整備する予定の指針の粒度等を含め、具体的な法制化に向けた詳細化が必要な点はあるでしょう。

V. おわりに

上記のとおり、中間とりまとめ案については現在パブリックコメントを募集しており、それも踏まえて今年の通常国会での法案提出を目指し法制化作業が行われることになります。中間とりまとめ案で示された方向性が今後も維持されるのであれば、「AI の研究開発・実装が最もしやすい、他国のモデルとなるような AI に係る法制度を含む制度整備」と位置付けられているとおりイノベーション促進とリスク対応を両立させる観点から、民間事業者の自主的な対応を尊重しつつ、透明性・適正性の確保や国による実態の調査・把握のための官民協調に主眼を置いた制度の構築をまずは志向していくことになるでしょう。

生成 AI が爆発的に普及してきた現在、もはやハードローとソフトローの単純な二項対立の議論には実益が乏しいことが一層明らかになる中で、これまでの日本のソフトローを中心とした AI リスク対応の良いところは活かしつつ、現時点で想定し切れないリスクが将来顕在化する可能性を想定して、有事の際には実効性のある対応を取れるよう、また、海外事業者に対しても適切なモニタリングを行えるよう、法的な裏付けとしてのフレキシブルな土台となる法制度的な手当てをしておくという観点からも、今回の中間とりまとめ案は重要な第一歩であり、欧米とも異なる日本流のアプローチの表明といえます。他方で、今後も AI をめぐる技術発展や国内外の社会環境はめまぐるしく変化していくことが予想されるため、今回示された方向性はあくまで出発点であり、今後強化される政府の司令塔を中心として、新たに顕在化するリスクに対し適切に対応できるよう、法制度の設計や運用も不断に検証されていくことが引き続き期待されます。