

岩田合同法律事務所 ニュースレター
2026 年 7 月

情報・テクノロジー

AI 事業者ガイドライン（第 1.2 版）における AI エージェント及びフィジカル AI の取扱い

弁護士 齋藤 弘樹

弁護士 田島 忠幸

第 1 はじめに

総務省及び経済産業省は、令和 8 年 3 月 31 日、AI 事業者ガイドライン検討会において取りまとめた「AI 事業者ガイドライン」の第 1.2 版を公表しました。併せて、「AI 事業者ガイドライン活用の手引き（案）」及び AI 事業者ガイドライン等について回答するチャットボットも公表されました。[1][2]

「AI 事業者ガイドライン」の第 1.0 版は、AI の安全かつ安心な活用を促進するための AI ガバナンスに関する統一的な指針として、2024 年 4 月 19 日に公開されました。その後、2025 年 3 月 28 日に第 1.1 版へ改訂され、主に AI 事業者が社内・部門の AI ポリシー・規則を策定・更新する際等に参照されています[3]。第 1.1 版から第 1.2 版への改訂（以下「本改訂」といいます。）では、AI エージェントやフィジカル AI 等の AI 技術の動向の反映、AI によるリスクに関する記載の見直し、各主体区分の役割に関する補足の追加、及び図表の更新等が行われています[4]。

本ニュースレターでは、第 1.2 版を「本ガイドライン」と呼びつつ、本改訂のうち、今回初めて定義が追加された AI エージェント及びフィジカル AI を中心に、AI 技術の動向の反映状況を解説します。

¹ 総務省＝経済産業省「AI 事業者ガイドライン（第 1.2 版）本編」（令和 8 年 3 月 31 日）
（https://www.soumu.go.jp/main_content/001064279.pdf、令和 8 年 7 月 17 日最終閲覧）。

² 総務省＝経済産業省「AI 事業者ガイドライン活用の手引き（案）」（令和 8 年 3 月 31 日）
（https://www.soumu.go.jp/main_content/001064304.pdf、令和 8 年 7 月 17 日最終閲覧）

³ 前掲注 2・3 頁

⁴ 総務省＝経済産業省「AI 事業者ガイドラインの令和 7 年度更新内容」3～4 頁（令和 8 年 3 月 31 日）
（https://www.soumu.go.jp/main_content/001064301.pdf、令和 8 年 7 月 17 日最終閲覧）

第2 本ガイドラインにおける AI エージェント及びフィジカル AI の定義

本ガイドライン本編の第1部「AI とは」では、AI の定義及び関連用語の説明がなされています。

本改訂では、AI エージェント及びフィジカル AI の技術発展や社会浸透を踏まえ、これらの用語について以下のとおり定義が追加されました^[5]。

AI エージェント	特定の目標を達成するために、環境を感知し自律的に行動する AI システムのこと。
フィジカル AI	センサ等によるセンシングを通じて物理環境の情報を取り込み、AI モデルによる処理を経て、設定された目的を達成するための最適な方策を自律的に推論・判断し、アクチュエータ（駆動系）等を介して物理的な行動へとつなげるシステムであり、サイバー空間での処理に留まらず、現実世界に対して直接的な働きかけ（移動、操作、加工など）を行うことを特徴とするもののこと。

なお、複数の AI エージェントが自律的に意思決定を行いアクションを起こす目標主導型の AI システムである「エージェントティック AI」についても、脚注で言及されています。もっとも、本文には定義やリスクに関する追記はなされておりません。エージェントティック AI については、今後の技術動向に加え、本ガイドラインの更なる改訂時に更に言及されるか否かにも注視する必要があります^[6]。

第3 AI エージェント及びフィジカル AI の便益とリスク

本改訂前から本ガイドラインに記載されていた内容の中には、AI エージェント及びフィジカル AI にも当てはまる部分があります。もっとも、本改訂では、以下のとおり、AI エージェント及びフィジカル AI 特有の便益やリスクに関する事項が別添に追記されました^[7]。

従前から記載のあった便益に加え、AI エージェントやフィジカル AI を取り入れることに固有の享受できる便益を正しく理解することや、これらのツールが生み出すリスクを認識することにより、後述する AI 事業者が留意すべき事項に対する理解を深めることができます。また、

⁵ 前掲注1・9頁以下、前掲注4・2～4頁

⁶ 前掲注4・6

⁷ 総務省＝経済産業省「AI 事業者ガイドライン（第1.2版）別添」（令和8年3月31日）17～18頁（https://www.soumu.go.jp/main_content/001064286.pdf、令和8年7月17日最終閲覧）。なお、AI エージェントやフィジカル AI の便益の事例については、同12～13頁に記載されています。

リスクの許容性及び便益とのバランスの検討結果を踏まえて、AI 事業者が積極的に開発・提供・利用を行うことで、競争力の強化、価値の創出、ひいてはイノベーションにつなげることが期待されます^[8]。

1 AI エージェントの便益とリスク^[9]

第2で述べたとおり、AI エージェントは、特定の目標を達成するために、環境を感知し、ユーザーの意図を理解し、自律的にタスクを遂行することができます。これにより、複雑な業務プロセスを効率化し、人的負荷を大幅に削減することが期待できます。また、複数のシステムやアプリケーションと連携し、状況に応じた判断や最適化を行うことで、従来は人手に依存していた調整・分析・意思決定の自動化が可能となります。具体的には、従来から存在する便益がAI エージェントにより更に向上するだけでなく、マーケティング分野において投稿から分析までを自律的に行う SNS 運用エージェントの活用など、AI エージェント特有の便益も期待されます。

他方、AI エージェントは多様な入力経路・外部連携先を持つことから、通常の生成 AI と比較して被攻撃対象が拡大し、データ汚染や悪意あるプロンプト攻撃のリスクが高まることが指摘されています。また、自律的な動作の中で、人間の意図しない商品の注文やファイル削除、内部データの不正な送付を行うリスクも指摘されています。加えて、AI エージェントの内部構造は複雑であるため、通常の AI システムと比較してメンテナンスやトラブルシューティングの難易度が上がります。更に、AI エージェントによりコードの生成が容易になることで、セキュリティホールを狙うマルウェアの作成等の技術の悪用が可能となり、個人情報の漏洩や重要インフラに関わるシステムの停止・情報の改ざん等につながるリスク（第三者による AI エージェントの利用によって自社が被害を受けるリスク）も指摘されています。

2 フィジカル AI の便益とリスク^[10]

第2で述べたとおり、フィジカル AI は、生成 AI などとは異なり、アクチュエータ（駆動系）等を介して物理的な行動へとつなげるシステムであり、現実世界に対して直接的な働きかけ（移動、操作、加工など）を行うことを特徴としています。これにより、少子高齢化による労働力不足を補い、人と協働して生産性を向上させることで、あらゆる産業や現場の自動化と効率化に寄与することが期待される旨指摘されています。具体的には、販売分野における店頭ロボットによる自動接客・販売や、物流・交通分野における自律搬送ロボット配送等での活用が期待されます。また、危険な環境で人の代わりに作業を行い、安全性を高めつつリスクを低減するとともに、介護や生活支援を通じて人々の自立と QOL 向上に寄与し、福祉や医療分野で新たな

⁸ 前掲注 7・17～18 頁

⁹ 前掲注 7・17～21 頁

¹⁰ 前掲注 7・16～19 頁

支援の創出にもつながり得る旨指摘されています。

他方、フィジカル AI も AI エージェントと同様にその内部構造の複雑さ故の制御の難易度の高さもリスクとして指摘されています。

第4 AI エージェント及びフィジカル AI の開発・提供・利用に際し留意すべき事項

本ガイドラインの別添では、AI 開発者、AI 提供者及び AI 利用者の各主体について、本編における記載内容のポイント及び具体的な手法、並びに本編「第2部 AI により目指すべき社会と各主体が取り組む事項」の「C.共通の指針」のうち特に留意すべき事項が記載されています。

本改訂の内容には、従来の AI 及び生成 AI、AI エージェント及びフィジカル AI に共通して当てはまるものと、AI エージェント及びフィジカル AI のみに当てはまるものがあります。

以下では、本改訂において追記された留意事項のうち、特に AI エージェント及びフィジカル AI について言及されているもの、AI エージェント及びフィジカル AI に当てはまりやすい（求められやすい）と筆者らが考えるものについて、以下紹介します。

1 AI 開発者が留意すべき事項^[1]

AI 開発者、すなわち AI システムの開発や AI 自体の研究開発をする事業者は、AI モデルやそのシステム基盤、入出力機能等を含む AI システムを構築する役割を担っています。AI の開発にあたっては、AI の入出力等の検証可能性の確保として、AI の予測性能及び出力の品質が活用開始後に大きく変動する可能性や、想定する精度に達しないこともある特性を踏まえ、事後検証のための作業記録を保存しつつ、その品質の維持・向上を行うことが求められています。

特に、自律的に判断を行う AI エージェントにおいては、適切な監査のために説明可能性が重要となります。もっとも、特に、LLM（大規模言語モデル）を用いた AI エージェントが呈示している推論過程の根拠提示は、内部の決定ロジックの説明ではなく、結果と根拠のもっともらしい組み合わせを出力している点に留意する必要があります。したがって、AI 開発者においてはこのような AI エージェントの特徴を踏まえ、従来型の AI の説明可能性とは異なる方法で検証可能性の確保のため、説明可能性・解釈可能性を高める手法を検討することが求められます。

2 AI 提供者が留意すべき事項^[2]

AI 提供者が留意すべき事項を、AI エージェントとフィジカル AI に分けて紹介します。

(1) AI エージェントにおけるホワイトリスト方式の導入検討等

AI 提供者は、AI システムをアプリケーション、製品、既存のシステム、ビジネスプロセス

¹¹ 前掲注 4・10 頁、前掲注 7・112～113 頁

¹² 前掲注 7・137～138 頁、前掲注 4・11 頁

等に組み込んだサービスとして提供する役割を担っているところ、AI システム実装時に、人間の生命・身体・財産、精神及び環境に配慮したリスク対策を講じることが求められています。具体的には、提供時点で予想される利用条件下でのパフォーマンスだけでなく、様々な状況下で AI システムがパフォーマンスレベルを維持できるようにし、不適切な出力等のリスクを最小限に抑える方法の検討が求められています。

また、自律的に動作するという AI エージェントの特徴を踏まえると、インシデントを未然に防止するため、人間の判断を介在させる仕組みの構築が求められやすいと考えます。

(2) フィジカル AI におけるプライバシー保護のための仕組み及び対策の導入等

本ガイドラインは、AI 提供者に対し、AI 利用者等関連するステークホルダー又は個人のプライバシーを侵害する情報を取得した場合、当該情報の消去、加工、AI のアルゴリズムの更新等、プライバシーを尊重するための対策を講じることが求めています。

第2で述べたとおり、フィジカル AI は、センサ等によるセンシングを通じて物理環境の情報を取り込むことから、個人情報を取得してしまう可能性があります。また、こうした情報がデバイス上に保存・残存し、解析や不適切な利用に結び付くことで、プライバシー侵害のおそれがあります。そこで、このようなフィジカル AI の特徴を踏まえ、不要な情報を取得・保持しない仕組みを設ける必要があるとともに、ハードウェアを廃棄する際は、機器やクラウドの記憶媒体に保存されたデータも適切に削除することが望ましいとされています。

以上を踏まえ、AI 提供者においても、不要な情報を取得・保持しない仕組みの構築や、当該仕組みを踏まえた社内規程の改訂を検討すべきです。

また、フィジカル AI も AI エージェントと同様に自律的に判断がなされるため、人間の判断を介在させる仕組みの構築を検討する必要もあると考えます。

3 AI 利用者が留意すべき事項^[13]

AI 利用者が留意すべき事項を、AI エージェント及びフィジカル AI の利用に分けて紹介します。

(1) AI エージェントの利用において求められる体制整備等

AI 利用者は、事業活動において、AI システム又は AI サービスを利用する事業者を指します。AI システム・サービスを利用するにあたり、AI 提供者からの情報提供（AI 開発者の情報を含みます。）及び説明を踏まえ、AI を活用する際の社会的文脈にも配慮して、安全に考慮した適正利用をすることが求められています。コード生成 AI の利用においては、生成 AI を利用した場合と比較して、AI エージェントを利用することによりコード生成が容易にな

¹³前掲注 4・12 頁、前掲注 7・166～173 頁

る反面、作成者の意図やコード構造の把握が難しくなり、保守・更新が困難になる可能性があります。そのため、ノーコード生成ツールも含め、社内ノウハウをいかに蓄積するかが重要となります。

また、AI 利用者はセキュリティ対策を実施する必要があります。特に、AI エージェントが自律性を持って行動することを踏まえ、定期的な操作履歴の確認や報告が重要となります。具体的には、システム利用状況や異常操作を把握するためのログの定期的なレビューや、異常な操作を検知した場合の即時報告体制の整備が求められています。

以上のような本改訂を踏まえ、AI 利用者においても、社内ノウハウのナレッジマネジメントの見直しや、ログの定期的な確認に係る社内規程・体制の整備が必要となります。

(2) フィジカル AI の利用において求められる体制整備等

AI 利用者についても、AI 提供者と同様に、フィジカル AI に係る不要な情報を取得・保持しない仕組みを設ける必要があるとされています。また、ハードウェアを廃棄する際は、機器やクラウドの記憶媒体に保存されたデータも適切に削除することが望ましいとされています。

また、フィジカル AI も AI エージェントと同様に自律性を持って行動するため、定期的な操作履歴の確認や報告が重要となります。必要に応じて、ログの定期的な確認に係る社内規程の見直しや体制の整備が求められると考えます。

第5 結語

以上のとおり、本改訂では、本ガイドラインの別添において、AI エージェントやフィジカル AI 等の新たな AI 技術の動向を踏まえた追記がなされています。本稿では、そのうち AI エージェント及びフィジカル AI に特有の追記がなされた事項や、特有の追記はないものの AI エージェントやフィジカル AI の特性に鑑みて関係性が深いと考えられる事項を取り上げました。

もっとも、AI 事業者は、それ以外にも、従前の AI や生成 AI に適用される本ガイドライン全体的内容についても検討したうえで、AI の社会実装及びガバナンスを実践する必要があります。

AI 技術の進展に伴い、求められるガバナンスの在り方も変化しています。AI 事業者においては、本改訂を踏まえ、各主体の区分に応じた役割や責任を改めて確認するとともに、第4に記載した留意事項も参照しながら、社内規程の見直しや必要な体制の整備等を検討することが望まれます。

【執筆者】



齋藤 弘樹（弁護士）
Email: hiroki.saito@iwatagodo.com

2010 年東京大学法学部卒業、2012 年東京大学法科大学院修了。危機管理業務（平時の内部統制システムの整備や有事対応）と IT 関連業務を中心に手掛けており、2 つの業務が交差する分野であるサイバー攻撃、情報漏えい、システム障害等に対する平時の体制整備・有事対応を得意とする。



田島 忠幸（弁護士）
Email: tadayuki.tajima@iwatagodo.com

2022 年早稲田大学法学部三年次早期卒業、2024 年早稲田大学法科大学院修了。紛争解決、知的財産法、情報・テクノロジー、非営利法人案件を中心に手掛ける。第一東京弁護士会総合法律研究所宇宙法研究部会部会員。

岩田合同法律事務所

1902 年(明治 35 年)、司法大臣や日本弁護士連合会会長を歴任した故・岩田宙造弁護士が「岩田宙造法律事務所」を開設したことに始まる、我が国において最も歴史のある法律事務所の一つです。開設当初より、我が国を代表する企業等の法律顧問として多数の企業法務案件に関与しております。日本法弁護士約 120 名が東京・札幌の両オフィスに所属し、日本語対応も可能な中国法弁護士、フランス法弁護士、米国各州弁護士資格を有する多数の弁護士のほか、特別招聘顧問として元最高裁判所長官大谷直人氏、特別顧問として前公正取引委員会委員長長古谷一之氏、前金融庁長官井藤英樹氏が在籍しております。

〒100-6315 千代田区丸の内二丁目 4 番 1 号 丸の内ビルディング 15 階
岩田合同法律事務所 広報: newsmail@iwatagodo.com

※本ニュースレターは一般的な情報提供を目的としたものであり、法的アドバイスではありません。また、その性質上、法令の条文や出展を意図的に省略している場合があり、また情報としての網羅性を保証するものではありません。個別具体的な案件については、必ず弁護士にご相談ください。