西村あさひ法律事務所

AI・IoT をめぐる米国の政策動向～米国 FTC の動向を踏まえて～

独禁 / 通商・経済安全保障ニューズレター　2023 年 7 月 25 日号

執筆者:
E-mail 角田 龍哉

米国 FTC（連邦取引委員会）は、AI を活用したサービスの消費者被害に対する注意喚起を精力的に行い、セキュリティや情報保護の観点から生成 AI やボイスアシスタントに対する調査も開始したとされています。さらにバイデン政権は、IoT のセキュリティラベリングの取組みを進め、大手 AI 企業から AI の開発・実装に関するコミットを得るなど、米国における AI 関連サービスの開発・上市環境に対する変化の兆しになるかもしれない動向が見られつつあります。そこで、以下では、これらの関連動向を概観します。

1. 米国 FTC による AI の不公正な利用に対する規制

(1) 米国 FTC のガイダンス

米国 FTC は、2020 年 4 月、AI・アルゴリズムの利用において、消費者に対する透明性や、説明責任、公正性、データ・モデルの頑健性・実証的な正確性、コンプライアンス・倫理・公正性・無差別に対する責任を担保することを求めるガイダンスを公表した。その後も、2021 年 4 月に事業者による AI の利用において真実性・公平性・衡平性を確保することを求めるガイダンス、2023 年 2 月に"AI Powered"製品の広告表示に関して確認すべきポイントをまとめたガイダンス[1]、2023 年 3 月に生成 AI を利用したチャットボット、ディープフェイク、音声クローン等による詐欺や欺瞞的行為を（故意がなくとも）行わないように制御・検証するためのポイントをまとめたガイダンス、2023 年 5 月に消費者に生成 AI を用いたサービスを信頼させることによる弊害を防止するためのポイントをまとめたガイダンスを相次いで公表しました。

2023 年 5 月に公表されたガイダンスでは、広告を特定のグループ向けにカスタマイズ等するために生成 AI を利用し、人々を欺罔して有害な選択をさせる仕様・デザインすることは、米国 FTC 法 5 条による執行の対象となった金融商品、ゲーム内購入、サービスの購入取消し等のケースで共通して確認された仕様・デザインであることが指摘されています。また、同ガイダンスでは、検索結果に広告を配置するのと同じように、生成 AI の機能内に広告を配置することを例に、以下の措置を講じるべきである旨を指摘しています。

① 広告は広告であることを常に明確にすること。
② 検索結果や AI により生成されたアウトプット上では、（クエリとの関連性等に基づいて表示された）オーガニックなものと有料のものとを明確に区別すること。
③ （米国 FTC の新しいステルス・インフルエンサーマーケティングガイドラインを踏まえて）人々が AI 製品の応答が特定のウェブサイト、サービスプロバイダ、製品等に誘導されていないかを把握すること。
④ 人々が生身の人間か機械のいずれと対話しているのかを把握すること。

(2) 米国 FTC による AI 関連の調査

米国 FTC は、2023 年 7 月、Amazon の Alexa について、Children's Online Privacy Protection Act Rule に基づき、子どもに関するデータの削除措置やプライバシー保護措置の強化を求めて調査を開始しました。

さらに、米国 FTC は、2023 年 7 月、OpenAI に対して、不公正又は欺瞞的なプライバシー又はデータセキュリティに関する行為を行い、又は信用・名誉毀損を含む消費者被害のリスクに関する不公正又は欺瞞的な行為を行い、米国 FTC 法 5 条に違反し

[1] 解説については、「米国 FTC による"AI Powered"製品の広告表示に関するガイダンス」（2023 年 3 月 17 日号）を参照。

ていないか等を確認するための調査を開始した旨が報じられました。調査範囲は、モデル開発・トレーニング、リスク評価・対策プロセス、プライバシーやプロンプトインジェクションによるリスクと対策内容、API インテレグレーションやプラグイン、個人情報の収集等の広範にわたっているようで、今後の展開が注目されます。

2. バイデン政権による AI・IoT 関連の取組み

(1) IoT のセキュリティに関する取組み

バイデン政権では、AI・IoT 関連の取組みが進んでいます。2021 年 5 月に発令された大統領令（Executive Order on Improving the Nation's Cybersecurity）は、米国標準技術研究所（NIST）が、IoT のサイバーセキュリティ基準を策定し、製造業者が製品のセキュリティについて消費者に知らせるために使用している既存のラベリング又はそれと互換性があるものを利用すること等を検討するよう指示しました。

その後、NIST は、「Recommended Criteria for Cybersecurity Labeling for Consumer IoT Products」と題する白書を公表し、IoT 製品について、バイナリーラベル（当該製品が基準を満たしていることを示す単一のラベル）に URL 等を記載して、IoT のセキュリティ情報等に関する追加的な情報を提供するアプローチ（階層的なアプローチ）を推奨していました。また、NIST は、2022 年 5 月に、「Report for the Assistant to the President for National Security Affairs (APNSA) on Cybersecurity Labeling for Consumers: Internet of Things (IoT) Devices and Software」と題するレポートを公表し、前記大統領令を踏まえたラベリング制度のパイロットプログラムの実施状況についてとりまとめました。

その後も、NIST は、2022 年 9 月に、「Profile of the IoT Core Baseline for Consumer IoT Products」を発表したり、ホワイトハウスも、2022 年 10 月、有識者を招集したうえで談話の場を設け、IoT 機器のラベリング制度につき議論を行ったりしました。そして、2023 年 5 月、NIST は、消費者向け IoT デバイス等に関するパイロットを実施し、（特定のラベルの仕様等を提案するものではなく、あくまでプロバイダと消費者の選択に委ねられるものであるものの、）一貫したラベル仕様であること、普及のためには多大な投資と時間を要すること等の留意事項をまとめた報告書を公表しました。ただし、この留意事項を踏まえた今後のタイムライン等は今のところ明らかにされていません。

(2) AI に関する取組み

ホワイトハウスは、2022 年 10 月、「AI 権利章典のためのブループリント」を公表し[2]、AI の設計者、利用者、実装者において遵守されるべき、①安全で効果的なシステムであること、②アルゴリズムによる差別からの保護、③データ・プライバシーの保護、④AI システムの使用に関する通知と説明、⑤人間による代替や、人間による検証・修復といった 5 つの原則を提示しました。

その後、ホワイトハウスは、2023 年 7 月、米欧貿易技術評議会や G7 における広島 AI プロセス、OECD での検討等の進展とタイミングを同じくして、主導的な AI 企業 7 社との間で、安全性（safety）、セキュリティ（security）、及び信頼（trust）の三つを原則とした、以下の 8 つの内容のコミットメント（本 AI コミット）を確保した旨のファクトシートを公表しました[3]。本 AI コミットは、実質的に同様の課題をカバーする規制が発効するまでの間、実施され続けるものとされています。また、各社が追加でのコミットを行うことも可能であるとしています。

安全性（公開前の AI システムの安全性確保）	① バイオ、サイバー、その他の安全分野等、悪用や、社会的リスク、国家安全保障上の懸念を含む分野で、モデルやシステムに対する社内外のレッドチーム[4]を実施する。 ファクトシートでは、これは、リリース前に AI システムの内部および外部のセキュリティテストを実施することを指しており（このテストの一部は独立した専門家によって実施される）、これにより、一定の AI のリスクの最も重大な原因（バイオセキュリティ、サイバーセキュリティ等）、及びその広範な社会的影響を制御すると説明されています。 ② 信頼・安全性に対するリスク、危険で、又は出現しつつある能力、及びセーフガード措置の回避

2 いわゆる米国憲法（権利章典）そのものと異なり、このブループリントには法的拘束力はないとされている。

3 本 AI コミットに Apple や Meta は含まれていないので、いわゆる GAFAM が参加したものというわけではない。

4 本 AI コミットで定義されているわけではないが、典型的には、実際のサイバー攻撃を想定した演習を指す。

	の試みに関する企業と政府間での情報共有に向けて取組む。 ファクトシートでは、AI のリスクの管理について、業界全体、並びに政府、市民社会、及びアカデミアと情報（安全性のためのベストプラクティス、保護措置を回避する施策に関する情報、及び技術協力を含む）を共有するものであると説明されています。
セキュリティ（セキュリティ・ファーストのシステム構築）	③ 自社のモデルウェイトや未効果のモデルウェイトを保護するために、サイバーセキュリティ、及びインサイダー脅威に対するセーフガード措置に投資する。 ファクトシートでは、自社のモデルウェイト、及び未公開のモデルウェイトを保護するため、サイバーセキュリティ、及びインサイダー脅威への対策に投資するものであり、これらのモデルウェイトは AI システムの最も重要な部分であり、モデルウェイトは、意図され、かつ、セキュリティリスクが検証された場合に限り、公開されることが重要であると説明されています。 ④ サードパーティによる問題、及び脆弱性の発見、及び報告を奨励する。 ファクトシートでは、AI システムの脆弱性について、第三者による発見及び報告を促進する。AI システムがリリースされた後でも、いくつかの問題は残っている可能性があり、頑健な報告メカニズムは、それらを速やかに発見し、修正することを可能にすると説明されています。
トラスト（公の信頼を得る）	⑤ AI で生成された音声、又は映像コンテンツに関する出所・来歴証明、ウォーターマーキング、又はその両方を含め、利用者が、その音声又は映像コンテンツが AI で生成されたものであるか否かを理解できるようにする頑健なメカニズムを開発及び実装する[5]。 ファクトシートでは、コンテンツが AI によって生成されたものであることをユーザーが確実に認識できる頑健な技術的メカニズム（電子的なウォーターマークシステム等）を開発する。これにより、AI を使った創造性が発揮され、詐欺や欺瞞の危険性を減少させることを可能にすると説明されています。 ⑥ 公平性やバイアスへの影響等の社会的リスクの議論を含め、モデル又はシステムの機能、制限、及び適切・不適切な使用の領域を公に報告する（透明性レポート）。 ⑦ 有害な偏見や差別の回避、プライバシーの保護等の AI システムによってもたらされる社会的リスクに関する研究に優先的に取組む。 ⑧ 社会の大きな課題への対処を支援する最先端の AI システムを開発及び実装を行う。

本 AI コミットの公表後、Amazon、Google、Microsoft、OpenAI（アルファベット順）も関連する投稿を行いました。他方で、来年 11 月に大統領選挙が控えた状況での動向であることや[6]前記 IoT の取組みのステータスも踏まえると、米国内ではどの程度のスピード感を以て取り組まれるか、今のところ未知数の面も大きいように思われます。

3. 日本への若干の示唆

生成系 AI の開発・利用をめぐり、米国では、上記のような開発企業による動向のほか、ニュース、メディア、エンターテイメント等の様々な関係企業・団体が自らが重視する原理原則やその対応スタンスを決定・提示したうえで、（政府機関の一定の関与の下で）社会的なルール整備を進める動向が見られます。これに対して、EU では、基本的な権利や価値をベースに、包括的な法規制を制定することを通じて、社会的なルール整備を進める動向が見られます。いずれにせよ、これらはルールメイキングの途上にあるため、こうした動向を方々に追いかけても、何をすると日本やグローバルでお墨付きを得られるのかという「答え」が手に入るわけではない状況にあるように思われます。日本の場合は、主に行政がガイドラインの形でルール整備を進めてきていることもあり、今後、日本でも、（行政によるルール形成の完了を待った動き出しというよりは）AI の開発・実装に携わる個々の事業者、機関等の原理原則をめぐる発意やスタンスが表明、尊重され、ルール整備もそれらを一層参酌した形で行われることが期待されます。

---

5 ウォーターマーキング（追跡）システムが開発された後に導入された生成系 AI を対象にしている。また、現実世界と容易に区別できる視聴覚コンテンツ、又は企業の AI システムによって生成されたものとして容易に認識できるように設計された視聴覚コンテンツ（AI アシスタントのデフォルトの音声等）は対象外となっている。他方で、特定のコンテンツが自社のシステムで生成されたか否かを判断するためのツールや API を開発するものとされている。

6 2022 年に提案された「American Data Privacy and Protection Act」（ADPPA）も、国内外で成立への期待が示された一方で、米国内では中間選挙に向けた動向の一つという受け止めも少なくなかったことも、一つの参考になるかもしれない。

当事務所では、クライアントの皆様のビジネスニーズに即応すべく、弁護士等が各分野で時宜にかなったトピックを解説したニューズレターを執筆し、随時発行しております。N&A ニューズレター購読をご希望の方は N&A ニューズレター　配信申込・変更フォームよりお手続きをお願いいたします。また、バックナンバーはこちらに掲載しておりますので、あわせてご覧ください。

本ニューズレターはリーガルアドバイスを目的とするものではなく、個別の案件については当該案件の個別の状況に応じ、日本法又は現地法弁護士の適切なアドバイスを求めていただく必要があります。また、本稿に記載の見解は執筆担当者の個人的見解であり、当事務所又は当事務所のクライアントの見解ではありません。

西村あさひ法律事務所　広報室　E-mail