NAGASHIMA OHNO & TSUNEMATSU
長島・大野・常松法律事務所
NO&T Technology Law Update
テクノロジー法ニュースレター

2023年11月
テクノロジー法ニュースレター　No. 43
米国最新法律情報　No. 105

AIに関する米国大統領令の公表と日本企業への影響

弁護士・ニューヨーク州弁護士　塚本　宏達
弁護士　殿村　桂司
弁護士　今野　由紀子
弁護士　丸田　颯人

はじめに

2023年10月30日、米国のバイデン大統領は、「AIの安全、安心、信頼できる開発と利用に関する大統領令」（Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence[1]、以下「AI大統領令」といいます。）を公布しました。バイデン政権は、これまでも2022年10月にAI権利章典の青写真（Blueprint for an AI Bill of Rights）を公表し、更に2023年7月には大手AI企業7社（同年9月に8社追加され、合計15社）からのVoluntary Commitmentsを得るなど、AIの規制に関連した政策を打ち出してきましたが、多くは拘束力のないガイドラインや企業による自主規制の支援が中心でした。今回のAI大統領令は、今後、既存の法令に基づき又は新たな立法等を通じて、米国で拘束力のあるAI規制が導入されることを意味しており、大きな注目を集めています。

AI大統領令は、安全かつ責任あるAIの開発と利用を促進する目的で、優先的に取り組む8つの指導原則（guiding principles）を明らかにしていますが、本稿では、日本の事業者に特に影響があると思われる内容に焦点を当ててご紹介いたします。

8つの指導原則と主な内容

AI大統領令は、以下の8つの指導原則を掲げています。

1. AI技術の安全性とセキュリティの確保	2. イノベーションと競争の促進
3. 労働者の支援	4. 公平性と公民権の推進
5. 消費者、患者、乗客、学生の保護	6. プライバシーの保護
7. 連邦政府によるAI利用の促進	8. 海外における米国のリーダーシップの強化

AI大統領令は、連邦政府機関に対して法的拘束力を有するにとどまり、民間事業者の権利義務や罰則を直接定めているわけではありません。しかし、AI大統領令では、既存の法令に基づき又は新たな立法等を通じて、特定のAI開発者に対する報告義務やAIの利用者に対する規律の検討を含む一定の措置を、一定の期間内（項目によって

[1] https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/

30 日から 540 日以内）に講ずるよう関係当局の長官に指示しているため、今後、関係官庁において AI 大統領令に従った措置が講じられることによって、AI の開発者及び利用者に重大な影響を及ぼすことが想定されます。AI 大統領令は 100 頁近い非常に詳細なものですが、以下では、特に日本企業にも影響があると思われる内容について概観します。

1. AI 技術の安全性とセキュリティの確保

(1) デュアルユース基盤モデルの開発者等に対する報告義務

AI 大統領令は、国防生産法（Defense Production Act）に基づき、「デュアルユース基盤モデル」（dual use foundation models）の開発者に対し、AI システム一般公開前の安全性テスト（AI レッドチーム（AI red-teaming）[2]テスト）の結果やデュアルユース基盤モデルのトレーニング、開発又は製造に関する情報等について、連邦政府への報告義務を課すことを求めています（4.2 項(a)(i)）。「デュアルユース基盤モデル」とは、悪用されると安全保障、国家経済安全保障、国家公衆衛生もしくは安全に対する深刻なリスクをもたらしうる AI モデルを意味しており、具体例として①CBRN（化学、生物、放射線、核）兵器の設計等を容易にするもの、②サイバー上の脆弱性を発見しやすくすることで強力なサイバー攻撃につながるもの及び③欺瞞等によって人間の制御や監視を回避することを可能とするものが掲げられています[3]（3 項(k)）。

また、その他、大規模計算クラスタ（large-scale computing cluster）の所有者等に対する報告義務（4.2 項(a)(ii)）、インフラストラクチャー・アズ・ア・サービス（Infrastructure as a Service（IaaS））提供者に対する外国の者との取引に関する報告義務（4.2 項(c)）を課すことも求めています。

(2) 生成 AI のラベリング等に関するガイダンスの策定

AI 大統領令は、生成 AI のリスクを踏まえ、AI が生成したコンテンツを識別する能力を高めるために、デジタルコンテンツ認証（digital content authentication）及び生成コンテンツのラベリング（watermarking[4]等）等に関するガイダンスを策定することを求めています（4.5 項(b)）。

(3) AI の安全、安心、信頼性を確保するための標準等の策定

AI 大統領令は、NIST（国立標準技術研究所）が AI レッドチームテストの手順を含むガイドラインや生成 AI のリスクマネジメントフレームワーク等に関するガイドライン等を策定することを求めています（4.1 項(a)）。

2. イノベーションと競争の促進

この指導原則では AI 人材の米国への誘致、イノベーションの促進及び競争の促進を定めています。日本企業に直接関係のある項目は少ないですが、イノベーションの促進の観点では、特許審査官及び出願人に対する発明者責任と、発明プロセスにおける AI の利用に関するガイダンスの公表、AI 関連の知的財産リスクを軽減するための研修、分析、評価プログラムの開発や社会的・世界的な課題に関する研究における AI の潜在的役割に関する報告書の公表等、米国における AI 規制の考え方を示す重要文書を公開することを定めているため（5.2 項(c)、(d)、(h)）、日本企業もこれらの文書を参照し、研究することが有益であると思われます。

また、競争の促進の観点では、例えば 5.3 項(a)は、連邦取引委員会は、AI 市場における公正な競争を確保し、AI による損害から消費者と労働者を守るために権限行使の検討が奨励される旨を定め、今後の権限行使の大方針に言及しています。米国の競争法は積極的に域外適用されているという状況を踏まえると、日本企業としても、AI の分野でも、公正競争確保、消費者及び労働者保護の観点から今後競争法が適用されうるということを認識しておくことは有益でしょう。

---

[2] 「AI レッドチーム」（AI red-teaming）とは、AI システムの欠陥や脆弱性を発見するための構造化されたテストを意味します（3 項(d)）。

[3] なお、ユーザーによる安全でない機能の利用を回避するための技術的安全措置を講じた上で、当該モデルがエンドユーザーに提供される場合であっても、この定義に該当することとされています（3 項(k)）。

[4] 「watermarking」は、アウトプットの真正性等を証明する目的で、AI が生成したアウトプットに、通常除去することが困難な情報を埋め込むこととされています（3 項(gg)）。

3. 労働者の支援

この指導原則では、今後 AI の労働市場への影響に関する報告書が作成されること（6 項(a)）、職場に導入された AI が従業員の福利増進に資するようなベストプラクティスを公表することが定められています（6 項(b)）。特に後者については最低限、①AI に関連する離職リスクとキャリア、②AI の公平性等を含む労働基準及び職務の質、③透明性等の使用者が労働者の情報を AI で収集・利用することによる労働者への影響を含めなければならないとされており（6 項(b)(i)）、具体的なベストプラクティスが公表されると想定されます。職場での AI 利用を考える日本企業にとっても参考になると思われるので引き続き動向を注視する必要があります。

4. 公平性と公民権の推進

この指導原則は主に刑事司法及び公的給付における AI の公平な活用について言及されていますが、採用における AI 利用についても言及されています（7.3 項）。同項では採用における AI の利用によって差別が生じないようにするための連邦契約業者向けのガイダンスを公表するとされています。米国政府との契約に関するものではあるものの、日本企業にとっても参考になる部分はある可能性があり、こちらも確認しておくことが望ましいでしょう。また、住宅の取引に関して AI の利用によってもたらされる差別軽減のための追加ガイダンスを発行することが関係当局の長官に奨励されており、具体的な反差別のためのガイダンスが発行される可能性があります。

5. 消費者、患者、乗客、学生の保護

この指導原則では、消費者、医療、運輸及び教育における AI の利用に関する規制の策定を関係当局に検討するよう求めており、今後具体的な規制がなされる可能性が高く、重要な内容を含んでいますのでそれぞれの規制対象ごとに概要を紹介します。

(1) 消費者保護

8 項(a)は、詐欺、差別、プライバシーへの脅威からの消費者保護及び金融安定性へのリスクを含む AI の利用から生じうるその他のリスクへの対処を目的に、規制を策定することを奨励しています。また、既存の規制やガイダンスが AI に適用される箇所を強調・明確化することも指示されています。この明確化には、規制対象主体が利用する第三者の AI サービスについてデューデリジェンスを実施し、監視する責任を明確化することや、AI の透明性や規制対象主体の AI 利用に関する説明能力についての要件の明確化が含まれるとされており、責任ある AI 利用のために具体的な規制が導入されることが想定されます。

(2) 医療、公衆衛生及び福祉分野における AI の利用

8 項(b)は医療・福祉サービスの分野における責任ある AI の利用のためのフレームワーク等を策定することを関係当局の長官に求めています。当該フレームワーク等には AI が生成したアウトプットについて人間による監督を考慮に入れることや AI による差別や偏見を特定し緩和すること、プライバシー及びセキュリティの基準を開発ライフサイクルに組み込むこと、並びに AI を適切かつ安全に利用するための文書の作成等を内容として盛り込むこととされています（8 項(b)(i)）。また、AI の性能に関する市場投入前評価及び市場投入後の監視のための措置を検討すべきことを関係当局の長官に求めており、AI の品質維持のための評価・監視のための措置が採られると考えられます。

(3) 運輸及び教育分野における AI の利用

8 項(c)(d)は運輸・教育分野における AI の利用について言及しており、主には政府による自動運転技術に関する現状の調査等や教育において差別のない責任ある AI の利用を取り上げるべきである旨定められていますが、上記(1)の消費者保護や(2)の医療、公衆衛生及び福祉分野における AI の利用とは異なり具体的な規制等には言及されていません。

6. プライバシーの保護

バイデン政権は、議会に対し、すべての米国民（特に子供）のプライバシー保護を強化するため、超党派の連邦

プライバシー法案を可決するよう呼びかけていますが[5]、AI 大統領令では、連邦政府がプライバシー拡張技術（Privacy Enhancing Technology、以下「PETs」といいます。）の開発等を支援することが強調されています（8 項(c)）。その他、この指導原則では、主に政府における AI の利用に伴うプライバシーリスクの軽減措置をとることが求められていますが、以下の点は日本企業にとっても参考になります。まず、AI によって悪化する可能性のあるプライバシーリスクとして AI が個人に関する情報の収集や利用を促進すること及び個人に関する推論を行うことが指摘されており（8 項(a)）、少なくともこれら二つは AI 利用によってもたらされる典型的なプライバシーリスクとして指摘されています。

また、PETs の利用促進のために差分プライバシー保護[6]の有効性評価の省庁向けガイドラインを策定することとされている（8 項(b)）ことは、日本企業にとってもプライバシー保護のための取組みをする上で参考になると思われます。

7. 連邦政府による AI 利用の促進

この指導原則は専ら連邦政府による AI 利用に関する指示ですが、以下の各省庁への勧告（10.1 項(b)(viii)）は、AI 利用のリスク管理の観点から日本企業にとっても参考になると思われるのでご紹介します。

- 生成 AI のための AI レッドチームを含む、AI の外部テスト
- 生成 AI について、差別的、誤解を招く、扇動的、安全でない又は欺瞞的な出力に対するテストと保護措置、児童性的虐待資料の作成に対するテストと保護措置及び実在する個人の同意なしの性的な画像（識別可能な個人の身体又は身体の一部の性的なデジタル描写を含む）の作成に対するテストと保護措置
- 生成 AI からの出力に透かし（watermark）やその他のラベルを付けるための合理的な措置
- 必要とされる最低限のリスク管理慣行。これには、必要に応じて、AI 権利章典の青写真（Blueprint for an AI Bill of Rights）や NIST の AI リスク管理フレームワークから派生したプラクティスが含まれる
- 提供する AI の有効性とリスク軽減の両方に関するベンダーの主張に関する独立した評価
- 調達した AI の文書化と監督
- 調達された AI の継続的改善のためのインセンティブの提供
- AI に関連する AI 大統領令及び他の文献に示された原則に従った AI に関する研修
- 本ガイダンスの遵守に関する公的報告

また、この指導原則では、生成 AI の利用促進についても述べられており、少なくとも個人の権利に影響を与えるリスクの低い場合や日常的な作業のために生成 AI を活用することは、禁止されるべきでないとされています（10.1 項(f)(i)）。

8. 海外における米国のリーダーシップの強化

この指導原則は日本企業との関連が薄いため、本稿では詳しくは取り上げませんが、米国が AI のグローバルスタンダードを作り上げていくための各種取組みが列挙されているほか、責任ある AI のための枠組み構築に向けた有志国連携の重要性が強調されており、日本における AI 規制の議論の観点からも留意が必要です。

おわりに

今後米国内では、AI 大統領令で指示された内容に基づき、各政府機関が具体的な措置を講じることとなるため、日本企業への影響の有無も含め、引き続き注視する必要があります。

---

[5] https://www.whitehouse.gov/briefing-room/statements-releases/2023/10/30/fact-sheet-president-biden-issues-executive-order-on-safe-secure-and-trustworthy-artificial-intelligence/?utm_source=newsletter&utm_medium=email&utm_campaign=newsletter_axiosam&stream=top

[6] 差分プライバシー保護とは、簡単に言うと特定の個人のデータが分析対象のデータセットに含まれていてもいなくても同じようなアウトプットが得られるように適切なノイズを付加する技術をいいます。

その他海外に目を向けると、AI の開発や利用に関する法規制を導入・検討する動きが各国で加速する可能性も考えられます。これまでは EU の AI 規則案[7]や中国における生成 AI 関連規制[8]等一部の国で規制が導入される動きが見られた一方で、包括的な法規制を導入するのではなく、規格、標準等の非拘束的な枠組みや既存の法令の執行を通じて AI のリスクに対処しようとする立場をとる国もあり、各国の政策アプローチは多様であったと言えます。今回の AI 大統領令によって、米国でも法的拘束力を有する規制を導入する姿勢が明確に打ち出されたことにより、今後、日本をはじめとする他の国での検討状況にも影響が及ぶ可能性があります。

当事務所では引き続き最新の AI 規制の動向をお伝えして参ります。

2023 年 11 月 22 日

---

[7] 欧州委員会が公表した AI 規則案の内容については、テクノロジー法ニュースレターNo.6「EU が AI に関する包括的な規則案を公表」（2021 年 4 月）をご参照ください。

[8] 中国における近時の生成 AI 規制については、テクノロジー法ニュースレターNo.35「生成系 AI に関する規制（生成系人工知能サービス管理弁法（パブコメ版）の公表）」（2023 年 5 月）をご参照ください。

[執筆者]

塚本 宏達
（Nagashima Ohno & Tsunematsu NY LLP 弁護士・ニューヨーク州弁護士 パートナー）
hironobu_tsukamoto@noandt.com
京都大学法学部及び The University of Chicago Law School 卒業。05 年～07 年 Weil, Gotshal & Manges LLP（シリコンバレー）勤務。雇用関連法と知的財産法の分野を中心として国内外の依頼者に対しリーガルサービスを提供するほか、会社法関連紛争、不動産取引関連紛争等、企業活動に関連する多様な紛争案件の代理経験も豊富に有する。また、海外訴訟のマネジメントや国際仲裁案件の代理といった国際紛争対応も行っている。

殿村 桂司（長島・大野・常松法律事務所 弁護士 パートナー）
keiji_tonomura@noandt.com
企業買収（M&A）取引・知財関連取引を中心に、企業法務全般に関するアドバイスを提供している。TMT（technology, media and telecoms）業界の案件にも幅広い経験を有しており、TMT 業界における買収、合弁その他の戦略的提携のほか、シェアリング・エコノミー、Fintech、IoT、AI などテクノロジーの発展が生み出す新しい事業分野の案件も数多く取り扱っている。2004 年京都大学法学部卒業。2006 年京都大学法科大学院修了。2013 年 Columbia Law School 卒業（LL.M., Harlan Fiske Stone Scholar）。2013 年～2014 年 Kirkland & Ellis（シカゴ）勤務。2018 年～経済産業省「AI・データの利用に関する契約ガイドライン」検討会作業部会構成員。

今野 由紀子（長島・大野・常松法律事務所 弁護士）
yukiko_konno@noandt.com
主な取扱分野は、クロスボーダーを中心とする企業法務一般のほか、国内外の個人情報・データプロテクション、ガバナンス、サイバーセキュリティ、データセキュリティその他データにまつわる様々な法律問題に関する助言。2005 年慶應義塾大学経済学部卒業、2008 年中央大学法科大学院修了。2015 年 Columbia Law School 卒業（LL.M, Harlan Fiske Stone Scholar）。2015 年～2017 年三菱商事株式会社勤務、2019 年～2022 年経済産業省勤務。

丸田 颯人（長島・大野・常松法律事務所 弁護士・情報処理安全確保支援士）
hayato_maruta@noandt.com
2019 年長島・大野・常松法律事務所入所。情報漏えい、製品不正やパワハラに関する調査等、広く危機管理・企業不祥事対応、コンプライアンス等に関する案件を主に取り扱っている。その他、テクノロジー関連法務やコーポレートを中心に広く企業法務一般に携わっている。

[編集者]

藤原 総一郎（弁護士・パートナー）
s_fujiwara@noandt.com
企業買収（M&A）取引を中心に、企業法務全般に関するアドバイスを提供している。また、インターネット/IT 関連取引を得意としており、いわゆる Fintech やシェアリング・エコノミー等のテクノロジー関連のアドバイスの経験も豊富である。

殿村 桂司（弁護士・パートナー）
keiji_tonomura@noandt.com
企業買収（M&A）取引・知財関連取引を中心に企業法務全般に関するアドバイスを提供している。TMT 業界の案件にも幅広い経験を有しているほか、シェアリング・エコノミー、Fintech、IoT、AI などテクノロジーの発展が生み出す新しい事業分野の案件も数多く取り扱っている。

長島･大野･常松 法律事務所　www.noandt.com

〒100-7036　東京都千代田区丸の内二丁目７番２号　ＪＰタワー
Tel: 03-6889-7000（代表）　Fax: 03-6889-8000（代表）　Email: info@noandt.com

長島・大野・常松法律事務所は、500 名を超える弁護士が所属する日本有数の総合法律事務所であり、東京、ニューヨーク、シンガポール、バンコク、ホーチミン、ハノイ、ジャカルタ及び上海に拠点を構えています。企業法務におけるあらゆる分野のリーガルサービスをワンストップで提供し、国内案件及び国際案件の双方に豊富な経験と実績を有しています。

テクノロジー法ニュースレター及び米国最新法律情報の配信登録を希望される場合には、<https://www.noandt.com/newsletters/>よりお申込みください。テクノロジー法ニュースレターに関するお問い合わせ等につきましては、<newsletter-technology@noandt.com>まで、米国最新法律情報に関するお問い合わせ等につきましては、<newsletter-us@noandt.com>までご連絡ください。なお、配信先としてご登録いただきましたメールアドレスには、長島・大野・常松法律事務所からその他のご案内もお送りする場合がございますので予めご了承いただけますようお願いいたします。