Legal Wire

Japan Practice

Vol. 156 / December 2023

バイデン氏、安心、安全で信頼できる AI に関する待望の大統領令を発令

ジェリー・マクナニー元下院議員、エリザベス・ヴェラ・モーラー、アーロン・M・オーサー、ブライアン・E・フィンチ、ブルック・L・ダニエルズ、トニー・フィリップス、ベンジャミン・J・コート、リー・G・ペトロ、サマンサ・フランクス、アマリス・トロッツォ

- バイデン政権は、大統領令により、AI の安全性とセキュリティ、プライバシー保護、公平性と市民権、消費者と労働者の権利およびイノベーションと競争に向けた新しいガイドラインを策定します。

- 大統領令の規定は、国家安全保障、経済安全保障または公衆衛生と公共の安全に影響を与える可能性のある AI 製品を開発する一定の企業に対し、国防生産法の権限を利用して、モデルのトレーニングとセキュリティ対策に関する定期的な報告を政府に提出させ、また、すべてのレッドチームの安全性テストの結果を共有させることを要求します。

- 先日、議会は 2023 年人工知能推進法案を提出しました。この法案は、人工知能のバグバウンティプログラムを創設し、様々な AI 利用の事例に関する報告と分析を要求するものです。

2023 年 10 月 30 日、バイデン大統領は待望の人工知能（AI）の安心、安全で信頼できる開発と利用に関する大統領令を発表しました。これは、さまざまな分野における AI の影響を調整し、政府機関や消費者が AI の利点を最大限に活用しつつ、リスクを軽減するための初の大統領令です。

AI に関する行政措置

バイデン大統領が初めて AI に言及したのは 2022 年 10 月の「AI 権利章典のための青写真（Blueprint for an AI Bill of Rights）」でした。それ以来、行政機関は AI 権利章典の原則を行政活動に取り入れ、各機関の管轄内での潜在的な AI による被害から消費者を保護することを優先しました。また、米政府は 2023 年 8 月にいくつかの主要な生成 AI の企業と、生成 AI の安全性、セキュリティおよび公衆の信頼を促進するための自主的な合意を取り付けました。

連邦通信委員会（FCC）は、2023 年 7 月 13 日に米国国立科学財団とともに分野横断的な AI の問題を議論するための公聴会を開催し、後日大統領令で示された AI に対する関心を既に表明していました。また、FCC は、2023 年 11 月の会議で、AI 技術を使用して生成された違法な迷惑電話やテキストメッセージから消費者を保護するための規則を導入すべきかについて調査するために、情報請求告示（Notice of Inquiry）を行うことを検討しています。

これらの動きは、待望の大統領令に発展しました。さらに、ハリス副大統領とライモンド商務長官は、イギリスのブレッチリーパークで開催された AI セーフティサミット 2023 に参加し、副大統領はバイデン政権による大統領令と AI の将来像について概説するスピーチを行いました。

【人工知能に関する大統領令】

大統領令の概要

この大統領令は、複数の連邦政府機関の規制権限を活用して、(a) AI の使用とプログラムから生じるリスクを監視し、(b) 技術の新しい革新的な使用法を開発し、(c) これらの新しい技術を安全に導入することを目的としています。大統領令は、連邦政府機関による AI の安全で責任ある倫理的な使用を促進し、既存の規制当局を通じて消費者を保護することを規定しています。

AI を使用または開発している企業は、連邦政府と契約を結んでいるか、または連邦政府による規制を受けている場合、大統領令の下で制定される様々な基準を注視する必要があります。例えば、商務省は、電子透かし（watermarking）の基準を作成することになっており、これは連邦調達規則に組み込まれる可能性があります。また、企業は、化学的リスク、生物学的リスク、原子力に係るリスクその他の潜在的な AI リスクをテストしてこれに対処するエネルギー省の取組みにも注意を払うべきでしょう。さらに、米国国立標準技術研究所（NIST）は、2 つのガイドラインを策定します。1 つ目は、業界標準を推進するという目標を支援するもので、AI リスク管理フレームワークの補足リソース、セキュアソフトウェア開発フレームワークの補足リソースおよび AI の能力の監査のためのベンチマークが含まれます。2 つ目のガイドラインは、AI システムのレッドチームテストのプロセスと手順を概説するものです。

大統領令はまた、議会に対し、データプライバシー法を策定し、成立させるよう求めています。今年はまだ提出されていませんが、2022 年に連邦政府のフレームワークの有望な手段として期待される米国データプライバシー法（ADPPA）の法案が注目を集めました。ADPPA は、パローン下院議員（民主党・ニュージャージー州）およびマクモリス・ロジャーズ下院議員（共和党・ワシントン州）によって提案され、消費者のデータプライバシーおよびセキュリティを保護し、個人の権利としてのプライバシー権を強化するための国家的なフレームワークを確立するものです。米国連邦下院エネルギー・商業委員会の委員長として、ロジャーズ下院議員は、今後のプライバシー規制の策定において重要な役割を果たすでしょう。

国防生産法

この大統領令はまた、国防生産法（DPA）を活用して、「軍民両用のデュアルユース基盤モデル」を開発しているまたは開発しようとしている企業に対して、レッドチームの安全性テストの結果を政府に報告すること、およびモデルのトレーニング時に政府に通知することを要求しています。これらの企業は、どのようにしてトレーニングプロセスとモデルの重み（ウエイト：モデルのトレーニング中に調整されるパラメータと、モデルがトレーニングセットから学習するメカニズム）の正確さと一貫性を確保し、外部の脅威から物理的セキュリティおよびサイバーセキュリティを守るかを示した計画について、商務省に報告することが義務付けられています。

デュアルユース基盤モデルは、大統領令において「広範なデータに基づいてトレーニングされ、一般的に「自己教師あり学習」（self-supervision）を使用し、少なくとも数百億のパラメータを含み、様々な場面に適用され、安全保障、国家経済安全保障、国家公衆衛生もしくは安全性などに深刻なリスクをもたらすタスクにおいて、高い性能を発揮するか、または高い性能を発揮するように容易に修正可能なモデル」であると定義されています。

大統領令はまた、国際緊急経済権限法に基づき、IaaS（Infrastructure as a Service）製品またはクラウドサービスに対し、非米国人が大規模な AI モデルのトレーニングのためにサーバースペースを借りる場合に、商務長官にこれを報告することを義務付ける権限を行使します。この規定に従い、米国外の再販業者が非米国人による米国の IaaS 製品の取引のすべての事例を報告しない限り、米国の IaaS プロバイダーは米国外の再販業者による米国 IaaS 製品の提供を禁止しなければなりません。商務長官は、90 日以内に報告要件に関する規制を提案します。

商務省は、180 日以内に、米国の IaaS プロバイダーに対し、米国外の再販業者が IaaS アカウントを取得する非米国人の身元を確認するための規制を提案します。

大統領令の詳細

大統領令は、AI に関するすべての行政府の活動を調整するためにホワイトハウス人工知能評議会を設置します。政策担当副首席補佐官が評議会の議長を務め、各政府機関の取組みを指揮して大統領令の使命を遂行します。詳細は以下のとおりです。

1. 安全性

大統領令は、人工知能の安全性とセキュリティを促進するためのガイドライン、基準およびベストプラクティスの策定を命じています。

- デュアルユース基盤モデルのプロバイダーは、AI モデルのトレーニング時に政府に通知し、国防生産法に基づいて安全性テストの結果を報告することが求められます。
- 米国国立標準技術研究所は、AI システムが開発される前に安心、安全で、信頼できることを保証するための基準、ツールおよびテストを策定するように指示されています。
- 国土安全保障省は、AI 安全セキュリティ委員会を設立します。この委員会は、民間、学界および政府の専門家で構成され、重要なインフラにおける AI 使用の安全性、レジリエンス、事故対応計画を向上させるための助言と勧告を行います。
- 国家安全保障会議は、軍事機関および情報機関が AI を安全、倫理的かつ効果的に使用するための国家安全保障覚書を作成するように指示されています。
- エネルギー省は、AI システムの能力の短期予測を評価し、核、核不拡散、生物学的、化学的、重要なインフラおよびエネルギー安全保障上の脅威および危険を特定するためのテストベッドを作成し、これらのリスクに対するガードレールを準備します。

2. サイバーセキュリティ

大統領令は、サイバー脅威に対する防御として AI 技術の利用を促進します。

- 大統領令は、米国防高等研究計画局（DARPA）が中心となって主催した AI サイバー・チャレンジ・コンテストを活用して、AI を使用して脆弱性を見つけ、修復するツールを開発します。
- 財務省は、金融セクターがサイバーセキュリティリスクを管理するためのベストプラクティスをまとめた公開レポートを提出することが求められています。
- 国土安全保障省と国防総省は、AI 技術の能力をテストして政府ネットワークの脆弱性を発見し、改善するためのパイロットプログラムをそれぞれ立ち上げるよう指示されています。
- デュアルユース基盤モデルを開発している企業は、国防生産法に基づいて、潜在的なサイバー脅威からトレーニングプロセスとモデルの重み（ウエイト）の正確さと一貫性をどのように保護しているかについてまとめた報告書を商務長官に提出する必要があります。

3. 透明性

大統領令は、合成コンテンツによるリスクを理解し、合成コンテンツを特定する能力を高めることでリスクを削減することを目指しています。

- 商務省は、AI が生成したコンテンツを区別するためのコンテンツ認証および電子透かしのための指針を策定します。連邦政府機関は電子透かしツールを使用するよう指示されています。
    - 連邦調達規制評議会は、商務省が作成し合成コンテンツを区別する方法に関する指針を調達要件に組み込むことを奨励されており、最終的には政府と契約している生成 AI を使用する企業に、電子透かしまたはその他のラベリングの仕組みを自ら採用するように求める可能性があります。
- 商務省の下で、米国電気通信情報局は、オープンソースまたはオンラインで公開されているモデルの重み（ウエイト）のリスクと利点に関する報告をするよう指示されています。

4. プライバシー

大統領令は、AI が進歩を続ける中で、米国人のプライバシーと市民権を保護する活動を指示しています。

- 大統領令は、議会に対して、超党派のデータプライバシー保護法案を可決するよう求めています。
- 大統領令は、連邦政府機関に対して、最先端の AI 技術を使用するツールを含む、プライバシー保護技術の開発または促進させるプロジェクトを優先的に支援するよう指示しています。
- 行政管理予算局（OMB）の局長は、各政府機関によって入手された個人を特定できる情報（PII）の調査を実施します。これには間接的にベンダーを通じて得られたまたは処理された情報も含まれます。この調査の結果は、今後プライバシーリスクを軽減する戦略を立てるにあたっての基礎となります。大統領令は OMB に対して、大統領令から 180 日以内に情報提供依頼（RFI）を行い、プライバシー影響評価をより効果的にする方法についてのフィードバックを募集するよう指示し、政府機関には RFI プロセスを通じて確定された戦略を実施するために必要な措置を講じるよう指示します。
- 大統領令により、プライバシー技術の急速な進展と開発を推進する研究協力ネットワークが設立されます。このネットワークは、連邦政府がプライバシー保護技術を活用するために、米国国立科学財団と連携します。
- 大統領令は、連邦政府機関がプライバシー保護技術の効果を評価するためのガイドラインを策定します。

5. 移民

大統領令は、米国外の AI 人材を呼び込み、米国における就労資格取得の障壁を下げることを目指しています。

- 国務省と国土安全保障省は、AI の専門知識を持つ移民のビザ申請手続を簡素化するよう指示されています。また、国務省は、米国に滞在する非米国人が「不必要な中断」

をすることなく AI やエマージングテクノロジーに取り組むことができるようにするための規則を作成します。

- 国務省、商務省、およびホワイトハウス科学技術政策局は、米国の能力を宣伝する新しいリソースや報告書を開発することで、AI の専門家を呼び込んで雇い、科学技術に係る仕事を推進するために協力します。

6. 競争

大統領令の一つの目的は、米国のイノベーションを優先し、市場参入する小規模な企業を支援する、開かれたかつ健全な競争のある AI 市場を作り出すことです。

- 公正で開かれた競争力のある AI システムをサポートするため、大統領令は政府機関に対して、小規模な開発者と起業家に商業的ブレークスルーを支援するための技術支援を提供するよう指示しています。
    - 商務省はまた、小規模な半導体企業が国立半導体技術センターに参加できる「柔軟なメンバーシップ体制」を保持するよう指示されています。
    - 商務省は半導体産業への関心を高めるメンターシッププログラムを作成するよう指示されています。
- 大統領令は、国家人工知能研究リソース（NAIRR）を実施するためのパイロットプログラムを承認し、ヘルスケアおよび気候変動に関する AI 研究の助成金を拡大します。NAIRR は 2020 年国家 AI イニシアティブ法に基づいて設立され、米国国立科学財団と科学技術政策局に対して、AI 開発に従事する者に対して重要なデータへのアクセスを拡大する全米の研究リソースの実現可能性について調査するためのタスクフォースの設立を指示しました。NAIRR タスクフォースは最終報告書を議会に提出しましたが、NAIRR はまだ連邦政府の助成を受けていません。
- 連邦取引委員会は、AI 業界における反競争的な行動に対抗し、消費者被害に対処するように指示されています。
- デュアルユース基盤モデルを開発している企業は、その技術保護計画を商務省に定期的に報告する必要があります。これらの計画には、米国の競争力に影響を与える可能性のあるスパイ行為などのリスクをどのように軽減するかに関する詳細が含まれる可能性があります。
- 米国外の敵対勢力が米国の AI 技術にアクセスする懸念に対処するため、大統領令はクラウドサービスに対して、米国外の個人やエンティティが大規模な AI モデルをトレーニングするためにサーバースペースを借りる際に政府に通知するよう指示しています。

7. 著作権

大統領令は、投資家とクリエイターを保護するために、新しい知的財産の問題と行動を取り上げています。

- 特許商標庁は、特許審査官と出願者に対して、出願における AI の取扱いについての指針を提供します。同庁は、120 日以内に、AI の発明プロセスでの使用や、様々なシナリオで発明者が誰であるかという問題がどのように分析されるかについての指針を示します。同庁は、その後 150 日以内に、特許適格性などの AI と知的財産が交差するその他の問題に取り組みます。

- 特許商標庁は、AI によって生成または作成された作品や AI モデルのトレーニングに使用される作品を保護するために、行政が講じるべき措置について勧告します。

8. 労働

大統領令は、AI への移行期において、米国の労働者のサポートへのコミットメントについて言及しています。

- 経済諮問会議は、180 日以内に、AI が労働市場に与える影響についての報告書を作成します。
- 労働省は、連邦政府が労働争議に巻き込まれる労働者を支援し、労働者の保護を強化する機会を見極めるために大統領への報告書を作成し、提出することになっています。
- 労働長官は、雇用主が従業員に AI から生じる潜在的な被害を軽減するための原則とベストプラクティスを策定します。これには、AI に仕事を代替されるリスク、労働基準、労働の質（公平性に関連する問題を含む。）について対処することや、雇用主が従業員から収集または使用する情報に関する従業員の権利を確認することも含まれます。また、労働長官は、AI を使用して従業員の仕事を監視または補完する雇用主が公正労働基準法に基づく保護規定を遵守しなければならないことを確認する指針を発行するよう指示されています。
- 人事管理局は、連邦政府の職場での生成 AI の使用について、政府の方針またはガードレールを策定します。科学技術政策局局長と行政予算管理局局長は、他の行政機関と協議して、できる限り既存の人材プログラムを利用しながら、連邦政府内で AI 人材を増やし、連邦政府の AI 人材の能力を向上させるための計画を策定します。

9. 公平性と市民権

大統領令は、政府のすべての取組みを通じて、公平性を守り、優先することに取り組んでいます。

- 大統領令は、AI アルゴリズムが差別を行わないようにする方法について、不動産の所有者、連邦福祉プログラムおよび連邦政府の調達請負業者のための明確な指針を示すよう行政機関に求めています。
- 司法省および連邦公民権局は、AI による市民権の侵害の捜査および訴追に関するベストプラクティスを策定します。これには、公民権局間での追加のトレーニングと技術支援も含まれます。
- 司法長官は、判決、仮釈放および保護観察、公判前の釈放と勾留、リスク評価、監視、犯罪予測および予測型警察活動ならびに法医学的分析において AI を公正かつ安全に使用する方法を特定する報告書を作成します。この報告書は、これらの意思決定において AI が使用される場合に、法執行機関が公平性と市民権に与える影響に関する懸念に対処するためのベストプラクティスを推奨するものでもあります。

10. 住宅

大統領令は、住宅やその他の不動産取引へのアクセスに関する決定における違法な差別を防ぐことを目指しています。

- 住宅または住宅ローンの広告における AI による差別に対して、公正信用報告法および信用機会均等法がどのように適用されるかについての指針を、消費者金融保護局（CFPB）が公表する可能性があり、また、住宅都市開発省（HUD）はこれを公表する予定です。提供される指針は、入居審査システムや AI システムによる特定のデータの使用が差別的な結果を招く可能性にも対処します。

11. 健康

大統領令は、市民の健康とヘルスケア分野における AI の潜在的な活用を考慮した、責任ある AI の展開を促進しています。

- 保健福祉省（HHS）は、AI が関与し、安全性に疑問があるヘルスケアに関する報告を受け付ける AI セーフティプログラムを作成し、ヘルスケア分野での AI または AI 対応のツールの使用を規制する戦略を策定します。

- 同省は、HHS AI タスクフォースを設立するよう義務付けられています。このタスクフォースは、創設から 1 年後に、ヘルスケア分野における責任ある AI および AI 対応技術の展開に関する戦略計画を公表します。

- HHS は、2024 年の Leading Edge Acceleration Project によるものを含め、AI 健康技術に関する助成金の機会を見極めて、優先させ、ヘルスケアデータの改善方法を探ります。

12. 運輸

大統領令は、AI の運輸部門への安全な統合をサポートしています。

- 運輸省は、AI を使用した輸送に関するパイロットプログラムを支援し、これらのパイロットプログラムの効果を検討して、AI の統合に対応するための更なる提案や規制措置を行います。

- 運輸省は、インフラ高等研究計画局（ARPA-I）に対して、AI 輸送プロジェクトへの資金提供の機会を模索し、優先順位をつけるように指示します。

13. 教育

大統領令は、教育省に対して、適切な文書やリソースを通じて、教育における AI の安全で責任ある差別のない利用について対応するように求めています。

- 教育省は、報告書「AI および教育と学習の未来」における同省の提言の実施を支援するための AI ツールキットを作成します。

14. 通信

大統領令の下で、連邦通信委員会（FCC）は、AI が通信ネットワークと消費者にどのように影響を与えるかについて検討するよう奨励されています。

- FCC は、AI がネットワークのレジリエンシーとスペクトラムの効率を向上させ、また自動音声による迷惑電話に対処する方法を検討する可能性があります。これらの対策は、5G および 6G 技術の展開に影響を与える可能性があります。

15. 国際協力

大統領令は、米国外におけるリーダーシップを強化する戦略を推進しています。

- 国務省と商務省は、AI の利点を活かしながら AI のリスクを管理するための「グローバル AI 研究アジェンダ」と呼ばれる強力な国際的な枠組みを確立するよう指示されています。
- 連邦政府は、国際的なパートナーおよび標準化機構と協力して、重要なインフラのセキュリティガイドラインに関する多国間の合意を含む AI の標準を策定し、これを実施するための取組みを行います。

現在の議会の動き

AI に取り組んでいるのは連邦行政府だけでなく、下院と上院の議員も AI 立法に注力しています。大統領令は既存の支出額および支出権限に制約されていますが、議会は新しい権限を創設し、追加資金を割り当てることを内容とする、AI 開発に影響を与える法律を制定することができます。下院と上院の両方の議員は、積極的に法案を提出し、AI 立法の基礎を築くための公聴会を開催しています。

特に、上院多数党院内総務であるシューマー上院議員（民主党・ニューヨーク州）は、6 月に SAFE イノベーションフレームワークを発表しました。それに伴う AI フォーラムでは、上院議員と業界および学界の専門家との一連の会議が行われ、上院議員が AI 技術の概要について学ぶことが目的とされています。最初の AI フォーラムには 60 人の上院議員が参加し、著名な AI 企業のリーダーも出席しました。10 月 24 日の第 2 回の AI フォーラムでは、AI のイノベーションに焦点が当てられ、次世代の AI システムに取り組むベンチャーキャピタリストや企業リーダー、市民社会団体をフィーチャーしました。次のフォーラムは 11 月 1 日に開催され、AI と労働に焦点が当てられました。

上院における AI 立法で重要なのは、「Gang of Four」であるラウンズ上院議員（共和党・サウスダコタ州）、ハインリッヒ上院議員（民主党・ニューメキシコ州）、シューマー上院議員（民主党・ニューヨーク州）、ヤング上院議員（共和党・インディアナ州）の活動です。第 2 回 AI フォーラムの後、Gang of Four は 2023 年人工知能推進法案（S. 3050）を提出しました。この法案が成立すれば、人工知能のバグバウンティプログラムが創設され、金融サービスでの AI プラットフォームの使用、AI 対応の軍事アプリケーションの脆弱性、およびデータ共有と連携に関する各報告書の作成が求められます。また、AI フォーラムに続いて、シャッツ上院議員（民主党・ハワイ州）とケネディ上院議員（共和党・ルイジアナ州）は、AI 生成コンテンツに関する透明性を提供するシャッツ - ケネディラベリング法（S. 2691）の法案を提出しました。

もう 1 つの重要なマイルストーンは、上院司法委員会のプライバシー・技術・法律小委員会議長のブルーメンソール上院議員（民主党・コネチカット州）と同委員会幹部のホーリー上院議員（共和党・ミズーリ州）による AI 立法のための両党の枠組みの提案でした。この両党の枠組みは、「高度な汎用 AI モデル」を対象とし、独立した監督機関が管理するライセンス制度を提案しています。この枠組みはまた、通信品位法 230 条のプロバイダー免責が AI に適用されないことを規定し、透明性を促進し、子供を保護するための対策を提示しています。最後に、当該枠組みは、米国外の敵対勢力に使用され、又は人権侵害に使用される可能性のある高度な AI モデルの移転を制限するために、輸出規制、制裁およびその他の制約をするよう議会に促しています。当該上院議員および小委員会の働きにより、この分野における重要な機運が高まっており、年内に草案を作成する予定です。

立法活動は AI の利点とリスクについての議論を活発化させました。ただし、シューマー上院議員は、議会が AI に関する包括的な法律を来年までに可決する可能性は低いと警告しています。

当事務所の AI プラクティスチームについて詳細はこちらをご覧ください。

本稿の原文（英文）につきましては、President Biden Issues Long-Awaited Executive Order on Safe, Secure and Trustworthy Artificial Intelligence をご参照ください。

本稿の内容に関する連絡先

Jerry McNerney
jerry.mcnerney@pillsburylaw.com

Elizabeth Vella Moeller
elizabeth.moeller@pillsburylaw.com

Aaron M. Oser
aaron.oser@pillsburylaw.com

Brian E. Finch
brian.finch@pillsburylaw.com

Brooke L. Daniels
brooke.daniels@pillsburylaw.com

Tony Phillips
tony.phillips@pillsburylaw.com

Benjamin J. Cote
benjamin.cote@pillsburylaw.com

Lee G. Petro
lee.petro@pillsburylaw.com

Samantha Franks
samantha.franks@pillsburylaw.com

Amaris Trozzo
amaris.trozzo@pillsburylaw.com

奈良 房永（日本語版監修）
fusae.nara@pillsburylaw.com

湯淺 幹也（日本語版作成協力）

東京オフィス連絡先

ジェフ・シュレップファー（日本語対応可）
jeff.schrepfer@pillsburylaw.com

サイモン・バレット
simon.barrett@pillsburylaw.com

松下 オリビア（日本語対応可）
olivia.matsushita@pillsburylaw.com

ニューヨークオフィス連絡先

秋山 真也
shinya.akiyama@pillsburylaw.com

Legal Wire 配信に関するお問い合わせ

田中里美
satomi.tanaka@pillsburylaw.com

This publication is issued periodically to keep Pillsbury Winthrop Shaw Pittman LLP clients and other interested parties informed of current legal developments that may affect or otherwise be of interest to them. The comments contained herein do not constitute legal opinion and should not be regarded as a substitute for legal advice.
© 2023 Pillsbury Winthrop Shaw Pittman LLP. All Rights Reserved.