AI 開発者と AI 導入者：重要な違い

人工知能（AI）は、経済のあらゆる分野でデジタルトランスフォーメーション（DX）を加速させています。製造業者は、AI を利用して安全で持続可能な製品を設計しています。中小企業は、AI ベースの翻訳ツールを利用して世界中の顧客にリーチしています。医療研究者は、患者ケアの改善や新たな医学ブレークスルーの推進に AI を活用しています。また、あらゆる業種の企業が AI システムを利用して、障害者に対する製品のアクセシビリティを改善することができます。AI は、これらをはじめとする無数の分野で、複雑な課題を解決する新たな機会を生み出しています。

AI 製品や AI サービスの成功の鍵は、それらのテクノロジーに対する社会的信認と信頼にあると言えます。その信頼を獲得するために、AI を開発および利用する企業は、このテクノロジーがもたらす固有の機会やリスクに対して責任を負わなければなりません。また、政策立案者が責任あるイノベーションを後押しする法規制環境を整備することによって、AI に対する社会的信認と信頼を高めることもできます。その際、(1) ハイリスクな AI 利用に重点を置き、(2) AI システムの開発者と導入者の役割や責任の違いを認識する必要があります。

開発者
AI システムを設計、コーディング、または製造

例

AI 音声認識システムを開発するソフトウェア企業など、AI システムを設計、コーディング、または製造する企業は開発者です。

導入者
AI システムを利用

例

社内または社外で開発された AI システムを利用して融資審査を行う銀行など、AI システムを利用する企業は導入者です。

「開発者」と「導入者」の役割を兼ねうる企業

例

ネットワークトラフィックや顧客取引を監視する AI ソフトウェアを開発し、それを自社のプラットフォーム上で利用するサイバーセキュリティ企業は、開発者であると同時に導入者でもあります。

政策立案者は、開発者と導入者の役割の違いを認識することにより、AI 市場における企業の役割に合わせて義務を課すことができます。例えば、ある AI システムを利用する導入者が、その AI システムを開発した別の企業が下す設計上の決定をコントロールすることは通常できません。同様に、ある AI システムの開発者が、その AI システムを導入する別の企業によるその後の利用をコントロールすることも通常はできません。

例

ローン申請の選別を支援する AI システムを設計している開発者があるとします。その AI システムの開発者は、AI システムが共通の反応や特定の機能の操作方法を認識できるようにトレーニングする際に使用するデータに関する情報を持っています。しかし、その開発者がローンを申請する消費者とやりとりしたり、承認するローン申請を選定したりすることはありません。むしろ、消費者とやりとりし、申請を承認または拒否を決定するのは銀行です。導入者である銀行は、選別処理の結果を使用して、融資手続きの公平性を評価するのに最適な立場にあり、潜在的リスクを軽減するための防衛策を実施することができます。

開発者と導入者の区別が重要である理由

プライバシー法やセキュリティ法で消費者の個人データを扱うさまざまなタイプの企業が区別されているのと同様に、開発者と導入者を区別することで、AI エコシステムにおける役割に基づいて正確に企業に義務を課す法的枠組みが実現します。その結果、企業はそれぞれの義務を果たしやすくなり、消費者の保護を強化できます。例えば、開発者は AI システムのトレーニングに使用したデータの特徴を説明することはできますが、その AI システムが別の企業によって購入され、実装された後にどう利用されるかを見抜くことは通常できません。むしろ、AI システムの利用方法、その利用方法が使用目的に合っているかどうか、人間による監視を組み込むかどうか、組み込む場合はその方法、AI システムからの出力、寄せられる苦情、システムの性能に影響する実際の要因などを理解する最適な立場にあるのは、通常、システムを利用する導入者です。

AI システムを設計および利用する企業に対して義務を課す法律は、これらの役割の違いを反映して適切に義務を課すべきです。そうすることで、実際のさまざまな AI サプライチェーンを構成する各企業がリスクを認識し、軽減できるようになります。この種の区別は、世界中のプライバシーやセキュリティ関連の法律においても、同様の理由でベストプラクティスと考えられています。例えば、米国、ヨーロッパ、アジア、および中南米のプライバシー法では、データの処理方法と処理理由を決定する管理者と、管理者に代わって、その指示に従ってデータを処理する処理者との役割の違いが区別されています。同様に、さまざまな法域のサイバーセキュリティ法では、企業と企業にサービスを提供する事業者を区別するのが一般的です。

ハイリスク AI システムの開発者と導入者に課すべき義務とは？

AI のハイリスクな利用に関し、企業に影響評価の実施を求めることを BSA は支持しています。そうした評価は、企業が AI リスクを認識、文書化、軽減する上で役立つ重要な説明責任手段です。特に、不法な差別につながりかねない潜在的バイアスを発見し、軽減する手段としても有用です。

影響評価を義務付ける法律は、ハイリスクな利用に適用するべきであり、開発者と導入者に対する要件を明確に区別する必要があります。

開発者
AI システムを設計、コーディング、または製造

ハイリスク AI システムの設計評価を実施する開発者は、必要に応じて次のような情報を文書化するべきです。

- AI システムの意図された目的
- 初めから分かっている AI システムの能力限界
- 初めから分かっている発生しうる具体的なハイリスクとその軽減措置
- AI システムのトレーニングに使用したデータの概要
- AI システムが販売される前の評価方法の概要

導入者
AI システムを利用

ハイリスク AI システムの影響評価を実施する導入者は、必要に応じて次のような情報を文書化するべきです。

- 導入者が意図する AI システムの使用目的
- 透明性確保手段（影響を受ける人々に対する AI システムの利用に関する通知など）
- AI システムの評価方法の概要（該当する場合）
- 初めから分かっている発生しうる具体的なハイリスクとその軽減措置
- 導入後の監視とユーザー保護対策（該当する場合）