



AIバリューチェーンに沿った効果的な説明責任： 役割に応じたAIの責任範囲の適正化

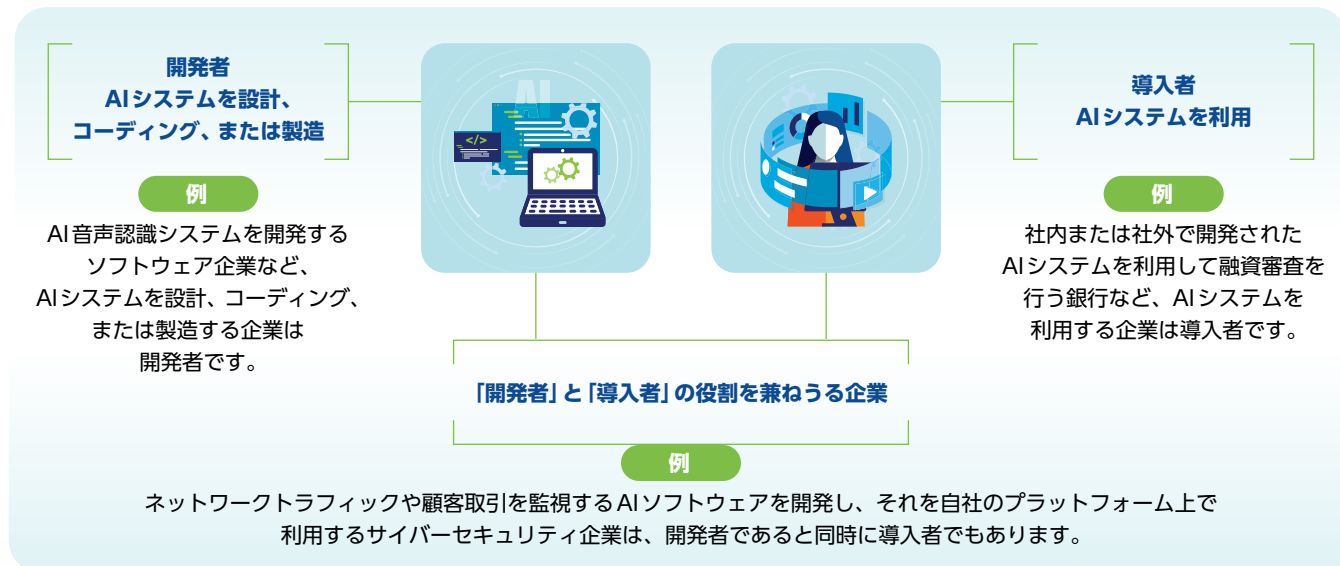
人工知能 (AI) は、経済のあらゆる分野でデジタルトランスフォーメーション (DX) を加速させています。製造業者は、AIを利用して安全で持続可能な製品を設計しています。中小企業は、AIベースの翻訳ツールを利用して世界中の顧客にリーチしています。医療研究者は、患者ケアの改善や新たな医学ブレイクスルーの推進にAIを活用しています。また、あらゆる業種の企業がAIシステムを利用して、障害者に対する製品のアクセシビリティを改善することができます。AIは、これらをはじめとする無数の分野で、複雑な課題を解決する新たな機会を生み出しています。

AIの導入を成功させるには、この革新的技術に対する信頼と確信が必要です。政策立案者は、信頼性と説明責任を高めるための枠組み作りに当たって、責任は企業の役割に見合ったものでなければならないという重要な原則を認識すべきです。

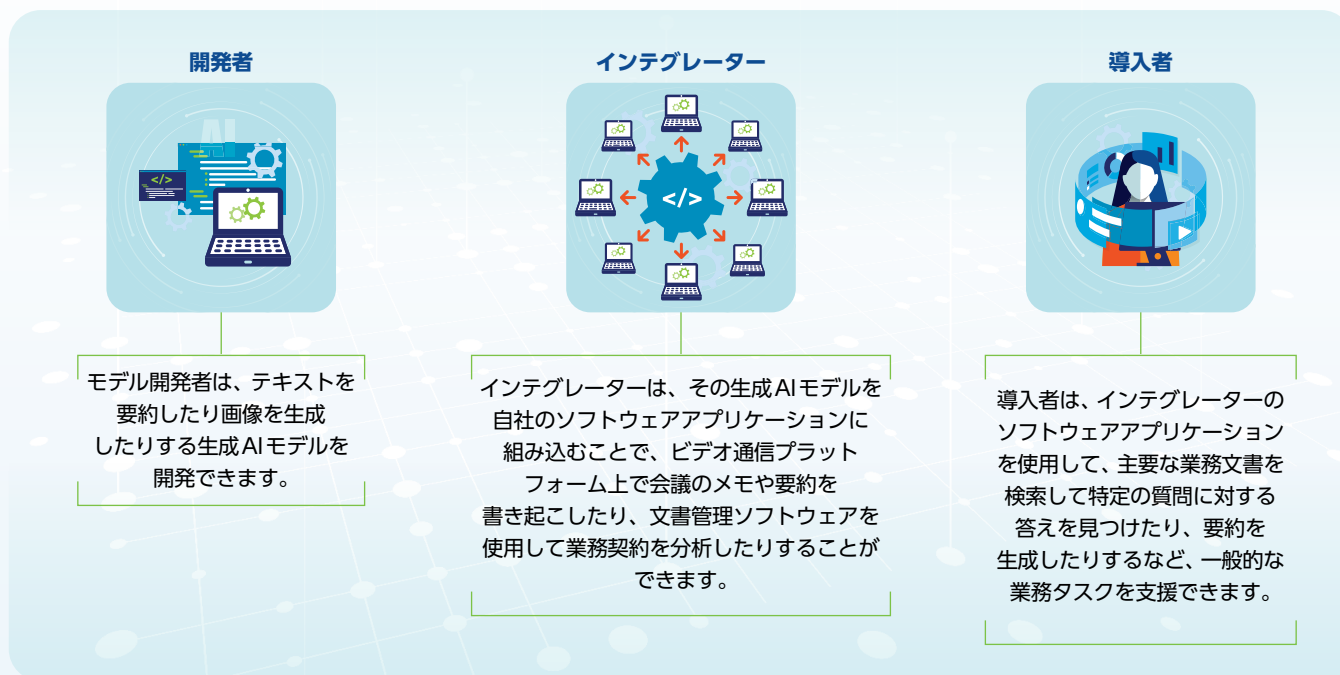
さまざまなAI主体に役割に応じた責任を負わせることは、いくつかの相互に関連する理由から重要です。第一に、関連情報へのアクセス権限とAIサプライチェーンにおける立場に基づいて、遂行可能な責任を企業に割り当て、それによって企業が自社の管理が及ばない事柄について、履行不可能な義務を負うことを防ぎます。第二に、消費者と企業顧客の保護が強化されます。なぜなら、リスクを特定して対処するのに最適な立場にある企業が、適切な保護措置を講じる主体として指定されることになるからです。第三に、実際に機能する政策枠組みの構築につながります。

AIエコシステムにおける主要な主体

AIサプライチェーンは、AI開発者、インテグレーター、導入者などのさまざまな企業で構成されており、複雑で常に進化しています。多くの場面では、開発者がAIシステムを開発し、導入者がそのシステムを実際に利用します。



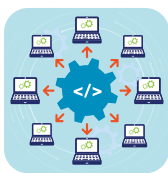
そのほかにも、ある企業がAIモデルを開発し、別の企業がそのAIモデルをアプリケーションまたはプラットフォーム(AIシステム)に統合し、さらに別の企業がそのAIシステムを使用して業務機能を実行する(企業の財務取引データから洞察を生成するコンテンツ管理プラットフォーム上で文書を要約するなど)といったケースが考えられます。





開発者

開発者には、基礎となるモデルを含め、AIシステムを開発する企業や、AIシステム全体を顧客に販売またはライセンスする企業が含まれます。そうしたAIシステムの例として、企業向けの人材管理ソフトウェアやワークフローコラボレーションソフトウェアなどが挙げられます。汎用型AIの場合、モデル開発者はさまざまなアプリケーションで使用できるAIモデルを開発します。例えば、ある企業がさまざまなユースケースに適応できる基盤モデルを構築すると、その同じ基盤モデルを使用して、検索エンジン、チャットボット、スパム検出ソフトウェア、長文テキストの要約ツールなどのさまざまなアプリケーションを強化することができます。開発者は、自社のAIモデルやAIシステムがどのように開発されたかについての情報を持っていますが、他の企業が自社のAIツールをどのように展開しているかについての情報は通常持ち合わせていません。



インテグレーター

インテグレーターは、特定のアプリケーションにAIモデルを統合して、他の企業が使用できるようにします。インテグレーターによっては、AIモデルを特定のAIシステムやアプリケーションに接続する場合もあれば、AIモデルをファインチューニングまたは変更した上でAIシステムやアプリケーションに搭載する場合があります。例えば、1つ以上のサードパーティーAIモデルを組み込んだAIアプリケーションを開発する企業は、インテグレーターとしての役割を果たすことがあります。インテグレーターは通常、AIモデルに加えた変更についての情報は持っていますが、モデルの初期開発や、その後の導入者によるAIシステムの使用に関する直接の知見は持ち合わせていません。



導入者

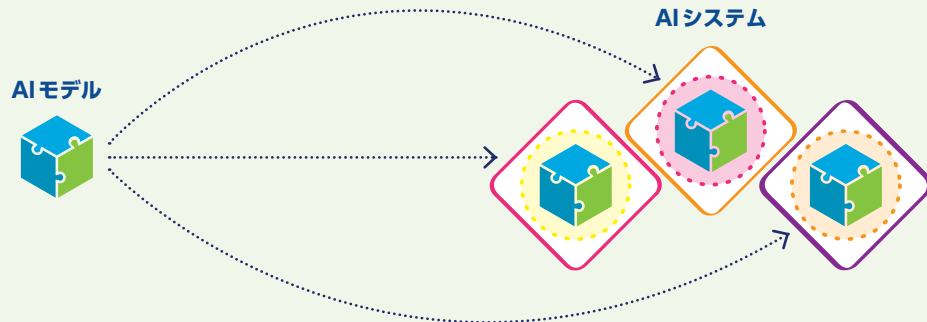
特定の目的にAIツールを使用する企業は、多くの場合、導入者と呼ばれます。導入者は、特定のAI技術をいつ、どのように使用するかを決定するため、特定のユースケースの事実について知見を得ることになります。しかし、他の企業からAIツールを入手することが多いため、通常はAIツールの初期トレーニングに関する直接の知見を持ち合わせていません。多くの場合、導入者は消費者と直接的関係を持つ企業です。

政策と説明責任の枠組みを効果的なものにするには、これらの大きく異なるタイプの企業を認識しなければなりません。そうすることで、画一的な要件を回避し、役割に応じた責任を負わせることが可能になります。このことは重要です。なぜなら、AIサプライチェーンを構成する企業のタイプによって、アクセスできる情報も異なれば、消費者や企業顧客を保護するために、関連するリスクを特定して対処する上で必要な措置を講じることができる立場も異なるからです。

例えば、基盤モデルの開発者は、自社のモデルの設計と学習に関する問題を説明することはできますが、インテグレーターがそのモデルを特定のアプリケーションに合わせてどうカスタマイズするかや、導入者がそのAIシステムをどう利用するかを見抜くことは通常できません。むしろ、AIシステムがどう利用されているか、その利用方法が使用目的に合っているかどうか、人間による監視をどう組み込むか、AIシステムが生成した出力をどう審査するか、エンドユーザーからの苦情をどう受けるか、システムの性能に影響する実際の要因をどう評価するか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。

他の背景と同様に、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または政策枠組みでは、これらの役割の違いを反映して適切に責任を割り当てるべきです。

AIモデルとAIシステムの違いとは？



AIモデルとは？

AIモデルとは、パターン認識、予測、コンテンツ生成などのために、大量のデータでトレーニングされたソフトウェアのことです。

例えるなら：

- » 多くの事例から学んできた、あるいは経験から学び続けている**熟練した専門家**、または
- » 言語、画像、または数字を処理できる**頭脳**

AIモデルの機能例：

- » 文中の次の単語の予測
- » 画像内の物体の認識
- » テキスト、画像、またはコードの生成

一般に、AIモデル自体は**簡単に使えるものではなく**、ユーザーインターフェース、ボタン、画面、ワークフローなどは備えていません。

AIシステムとは？

AIシステムとは、1つ以上のAIモデルを使用してタスクを実行したり、問題を解決したりする完全なツールまたは製品のことです。

例えるなら：

- » エンジン (AIモデル) に加えて、ハンドルや運転席、操作類などを搭載した**自動車**

AIアプリケーションには、チャットインターフェース、ボタン、メニュー、音声入力のほか、ルール、セーフガード、統合 (電子メール、カレンダー、データベースなどとの) なども含まれます。

例：

- » 顧客の質問に答えるチャットボット
- » 画像を加工するフォトアプリ
- » 電子メールの下書きを支援するライティングアシスタント

役割に応じた政策アプローチの先例

役割に応じて義務を定めることは、世界中のプライバシー法やセキュリティ法でベストプラクティスと見なされています。例えば、米国をはじめとする世界中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。

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、AIサプライチェーンを構成するさまざまなタイプの企業を区別することで、AIエコシステムにおける役割に基づいて適切に企業に義務を課す法的枠組みが実現します。その結果、企業が課された義務を意味のある形で果たし、消費者をより一層保護することが可能になります。