VISION by protiviti®

In Focus

2025
2月18日

DeepSeekは企業にAI戦略の変革を迫るか?

著 クリスティン・リビングストン
プロティビティ マネージングディレクタ

先月末、中国を拠点とするAIスタートアップのDeepSeekが最新モデル「DeepSeek R1」をリリースし、世界中に衝撃を与えました。同社は、このモデルがOpenAIのChatGPTと同等の能力を有すると主張しています。OpenAIのo1モデルは2024年9月12日にリリースされ、DeepSeekのR1モデルは、その約4か月後の2025年1月にリリースされました。

OpenAIの推論モデルと同様に、DeepSeekは、人間が問題を推論するプロセスをシミュレートするように、段階的に応答する大規模言語モデルを使用しています。しかし、OpenAIとは異なり、DeepSeekはモデル(コードと重み)をオープンソース化しており、誰でもコピー、ダウンロード、およびそれを基にした開発を行うことができます。その結果、より民主化されたAIが実現し、小規模なプレイヤーでも迅速に追いつくことができるかもしれません。

しかし、米国のAI企業にとってさらに懸念されるのは、OpenAIの推定開発コストが1億ドルであることに対し、DeepSeekが発表したコストが600万ドルだったとされている点です。もしそれが本当なら、DeepSeekはAI競争に大きな影響を与え、企業はそのAI戦略を根本的に変えるべきであるかもしれません。

なぜ重要なのか

DeepSeekのAI業界に対する破壊力は相当なもので、DeepSeekはすでにChatGPTを抜いて、米国のApple App Storeで最もダウンロードされた無料アプリとなっています。また、DeepSeekは米国のテック業界にも心理的な影響を与え、米国企業が急成長するAI市場を支配できるかどうかということに疑問を投げかけています。DeepSeekの登場前は、多くの技術の専門家がそのように予想していました。しかし、中国は多くの人が思っていたよりもはるかに進んでいる可能性があり、ドナルド・トランプ米大統領はDeepSeekをアメリカのテック企業への「警鐘」と呼びました。

DeepSeekのR1オープンソースモデルには、セキュリティリスクが内在しています。例えば、オープンソースモデルを使用する場合、責任を負うべき第三者が存在しないため、企業自身が強固な安全性とセキュリティテストを実施し、脆弱性が埋め込まれていないことを確認する必要があります。その他の課題としては以下があります:

セキュリティ:DeepSeekや他のオープンソースAIモデルには、アクセス可能なソースコードが含まれているため、アーキテクチャ上の脆弱性が悪用される可能性があります。

信頼性:DeepSeekのいくつかの主張の正確性には疑念があり、AIの盗用やバイアスに関する指摘もされています。

スキルセット：通常、オープンソースのモデルには即座に利用できるサポートが欠けており、モデルを修正するにはAIや機械学習のスキルが必要になる場合があります。

コンプライアンスと規制：DeepSeekがコンプライアンスおよび規制要件に与える影響は依然として不明です。米国では、ニューヨーク州、テキサス州、バージニア州が州全体でアプリの使用を禁止しており、オレゴン州とノースカロライナ州では州のデバイスでのDeepSeekの使用が禁止されています。グローバルでは、韓国がDeepSeekアプリを禁止し、オーストラリアが政府デバイスでのDeepSeekアプリの使用を禁止しています。

一方で、オープンソースAIモデルには以下のような利点もあります：

透明性：モデルをオープンソース化し、コードベースへの完全なアクセスを提供することにより、DeepSeekや他のオープンソースモデルは、クローズドモデルでは実現できないアルゴリズムやデータソースの透明性を提供します。これは、特定のユースケースにおいて規制遵守のために必要となる場合があります。

カスタマイズ性：DeepSeekのようなオープンソースモデルは、ユーザーがモデルを特定のニーズに合わせて適応させ、そのカスタマイズを保持しながら将来のモデルバージョンにシームレスに統合することを可能にします。これは、クローズドソースモデルを微調整するよりも容易です。

参入障壁：オープンソースモデルは、オープンソースライセンスを利用しており、これらはクローズドライセンスまたは商業ライセンスよりもはるかに安価または無料です。

彼らの見解

ダリオ・アモデイ、安全なAIシステムの構築に取り組む公益法人AnthropicのCEO

「DeepSeekは、米国の7～10か月古いモデルのパフォーマンスに近いモデルを、はるかに低コストで作り上げました。これらはすべて、DeepSeekが独自のブレークスルーでも、大規模言語モデルの経済を根本的に変えるものでもなく、継続的なコスト削減曲線上の予想されるポイントであると言うことです。これらすべてが示唆しているのは、DeepSeekが特異なブレークスルーでもなく、大規模言語モデルの経済性を根本的に変えるものでもないということです。それはむしろ、継続的なコスト削減曲線上の予想された一点に過ぎません。今回何が異なるのかといえば、期待されるコスト削減を最初に実証した会社が中国企業であったということです。これはこれまでにないことであり、地政学的に重要なことです。」

私たちの見解

企業のリーダーは、DeepSeekを重要な反省のポイントとして捉えるべきです。堅実な企業AI戦略は、オープンソースとクローズドソースのAIモデルを組み合わせ、単一のプロバイダーへの依存を避け、モデルをシームレスに交換できる柔軟性を持つべきです。AIに関する規制が急速に緩和しているなかで、多くのAIアプリケーションは高い透明性を求められるでしょう。この透明性のレベルを達成することは、多くのクローズドソースモデルでは難しく、場合によっては不可能です。

結論

アメリカと中国の両国が強力なAIモデルを保有していますが、DeepSeekは中国がAI競争においてアメリカとの能力差を縮めていることを示しています。アメリカはこれを注視すべきです。MetaのLlama、GoogleのGemma、DeepSeekのR1といったオープンソースモデルは、企業が自社のデータに適用したAIの独自の活用方法で差別化を図る中で、企業において重要な役割を果たすでしょう。オープンソースモデルはカスタマイズや拡張の柔軟性を提供する可能性がありますが、それらを設定・展開し、包括的にテストし、脆弱性を特定し、セキュリティリスクを軽減するためには、新たな能力と才能が必要となります。企業がオープンソースとクローズドソースAIを自社のアーキテクチャやビジネスプロセスに統合し続けるなかで、AIのレッドチーミング（セキュリティ評価）が今後ますます普及することが予想されます。

VISION by Protivitiについて

VISION by Protivitiは、今後10年およびそれ以降にビジネスを変革する、大きな変革をもたらすトピックを探求するグローバルコンテンツリソースです。経営幹部および取締役会のエグゼクティブ向けに書かれており、VISION by Protivitiは、今日および未来を形作る破壊的な力の影響を検討します。多様な声と多様な視点を通じて、VISION by Protivitiは、10年後、そしてその先のビジネスの姿についての見解を提供します。

protiviti®