

中国のAIがアメリカのAIを蒸留して学習していると報道されている。実際、アメリカのAIの能力を蒸留によって習得することが可能なのでしょうか？また、蒸留とは具体的にどのような作業であり通常の方法で実施することが可能なか教えてください。

🔍 Found 15 web pages 

結論から言えば、蒸留によって米国AIの能力の一部を習得することは技術的に可能です。これはAI分野で広く使われている標準的な手法であり、中国の商務省も「本質的に中立的な技術手段」と認めています^{1 8}。ただし、報道されているような「産業規模」での実施が、技術的に可能かどうかと、法的・倫理的に許容されるかどうかは別問題です。

蒸留とは具体的に何か

蒸留（Knowledge Distillation）は、簡単に言えば「優秀な先生モデルの出力を教材にして、小さな生徒モデルを訓練する」技術です^{5 12}。

具体的な作業の流れは以下の通りです。

1. **先生モデルに大量の質問をする**：ChatGPTやClaudeなどの高性能な「先生モデル」に対し、APIなどを通じて膨大な数の質問を送信します。
2. **回答（出力）を収集する**：先生モデルが生成した回答や、その推論プロセス（思考の連鎖）を大量に集めます^{5 15}。この際、単なる最終回答だけでなく、途中の思考プロセスも含めると、生徒モデルは「どう考えて答えを導いたか」を学べるため、能力の再現効率が高まります⁵。
3. **生徒モデルを訓練する**：収集した「質問と先生の回答」のペアを教師データとして使い、自社の小さなモデル（生徒モデル）をファインチューニングします¹⁰。これにより、生徒モデルは先生モデル特有の回答スタイルや推論パターン、特定タスク（コーディングや数学など）の能力を模倣できるようになります^{5 12}。

通常の方法で実施可能か

技術的には、通常の方法で実施可能です。特別なハッキング技術は必ずしも必要なく、以下の2つのアプローチが考えられます。

- **公開APIを利用する方法**：OpenAIやAnthropicのAPIは、開発者や企業が利用するために公開されています。理論上は、大量の質問をプログラムで自動送信し、返ってきた回答を保存して訓練データを構築することが可能です^{10 11}。ただし、この行為は多くの場合、**利用規約（ToS）で禁止**されています。OpenAIは「競合モデルの開発に出力を使用すること」を明確に禁じており、Anthropicも同様の規

制を設けています 4 6 。

- **オープンウェイトモデルを利用する方法**：LlamaやQwenなど、モデルの重みが公開されている（オープンウェイト）モデルであれば、APIを介さずにローカル環境で自由に行き、その出力を蒸留に利用できます。こちらは利用規約上の制約が比較的少なく、技術的にも容易です 3 。

報道されている「蒸留」の争点

米国政府機関（NSA, FBI, CISA）やAnthropicが問題視しているのは、単なる蒸留技術の使用そのものではなく、「**不正な蒸留（illicit distillation）**」、つまり許可なく大規模かつ組織的に能力を抽出する行為です 5 6 。

報道されている具体的な手口としては、以下のようなものが指摘されています。

- **規約違反と制限回避**：大量の偽アカウントを作成したり、サードパーティのAPIアグリゲーターを経由したりして、レート制限や地域制限を回避し、数百万回ものやり取りを行ったとされています 5 13 。
- **産業規模の抽出**：Anthropicの報告では、アリババが2026年5月から7月の間に**1億5,100万回以上**のやり取りを行い、Claudeの推論能力を抽出しようとしたと主張されています 5 。

一方で、中国商務省はこのような非難に対し、「**事実の根拠も法的根拠もない**」と強く反論しています。蒸留は世界中の企業が使う一般的な手法であり、米国企業も中国のモデルを大量に蒸留していると指摘し、米国側の措置は技術覇権を維持するための「**ダブルスタンダード**」であると批判しています 1 7 8 。

まとめ

蒸留は、高性能なAIの能力を効率的に別のモデルへ移転させるための、**技術的に確立された合法的な手法**です。したがって、米国AIの能力の一部を蒸留で習得することは可能です。

しかし、今回の報道で争点となっているのは、技術の可否ではなく、「**公開APIの利用規約に違反し、制限を回避しながら、競合モデル開発のために組織的・大規模に出力を収集したか否か**」という点にあります。この「不正な蒸留」に該当するかどうかは、データの入手経路やアクセス方法が規約に沿っているかによって判断されるべき問題です 5 。

 15 web pages