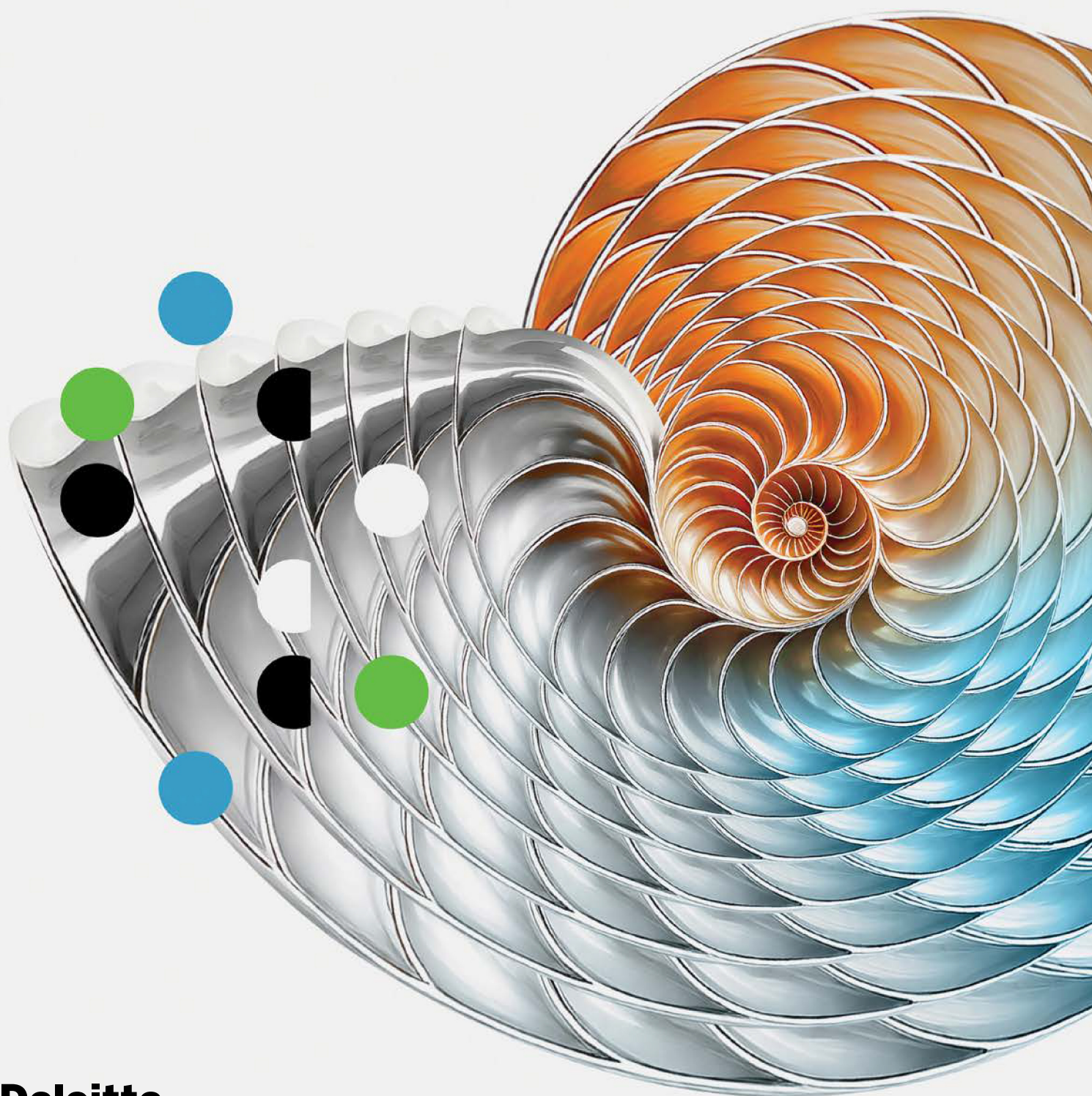


# Tech Trends 2026

日本語版

テクノロジーのイノベーションと導入が加速する中、5つのトレンドは、成功している組織がいかんしてトライアルから効果創出へと移行しているかを明らかにしている



**Deloitte.**  
Insights



**02... Tech Trends 2026: エグゼクティブサマリー**

**04... イノベーションの複利効果**

**09... AIは物理世界へ: AIとロボティクスの融合がもたらす新たな可能性**

**21... エージェント化のリアリティチェック: シリコンベースの労働力に備える**

**33... AIインフラの転換点: 推論エコノミクス時代におけるコンピューティング戦略の最適化**

**43... テクノロジー組織の再構築: AIネイティブなテクノロジー組織の設計**

**53... AIのジレンマ: サイバー防御のためのAIの確保と活用**

**62... ノイズを切り裂く: AIの進展に伴い追跡すべき技術シグナル**



# Tech Trends 2026

## エグゼクティブサマリー

**T**ech Trends 2025では、AI (Artificial Intelligence、人工知能) が電気のような存在、すなわち、非常に広範な製品やサービスにシームレスに組み込まれる基盤要素になると予測した。17年目となる今年のレポートは、その仮説を証明している。インテリジェントなオペレーションへの需要が、コンピューティングハードウェアから物理的なロボティクスに至るまで、あらゆる意思決定に影響を与える中、AIの影響を受けていない企業テクノロジーの領域は存在しない。そして、昨年の焦点がPoC (Proof of Concept、概念実証) プロジェクトの構築と「アート・オブ・ザ・ポッシブル (可能性の探求)」であったのに対し、今年はスケーリングが主題である。さまざまな業界の企業が、AI主導のプロセスを実用化している。理由は単純である。リーダーたちは競争上の差別化の鍵が、AIを活用して自動化・イノベーション・アクセラレーションを促進することにあると気づいたからだ。

### イノベーションの複利効果

テクノロジーリーダーは、AIのパイロットから測定可能な効果を求める段階への重要な転換に直面している。イノベーションは今や指数関数的に増大している。たとえば、生成AIがわずか2ヶ月で約1億人のユーザーに達したのに対し、電話のユーザー数は5,000万人に達するのに50年を要した。これにより、テクノロジー・データ・投資・インフラといった各領域での改善が同時に加速する相乗効果が生まれている。従来のインフラや段階的な改善プロセスでは、このペースについていくことはできない。成功には、高度なテクノロジー以上のものが必要である。組織は、単にプロセスを自動化するのではなく、再設計し、投資をビジネスの成果に結びつけ、迅速に実行しなければならない。

### AIは物理世界へ：AIとロボティクスの融合がもたらす新たな可能性

フィジカルAIは、ロボットを事前にプログラムされた機械から、複雑な環境で自律的に知覚・学習・操作する適応型システムへと進化させている。これらの能力は、産業用ロボット・自動運転車・ドローン・その他のシステムに現れている。現在の課題には、トレーニングのギャップ、安全性の課題、サイバーセキュリティリスクが含まれるが、コストの低下により、スマート倉庫やサプライチェーン業務を越えて、一般市場への導入が拡大している。ヒューマノイドロボットは次のフロンティアであり、2035年までに職場に200万体のヒューマノイドが導入されるとの予測がある。将来の発展には、バイオハイブリッドロボットや量子ロボティクスが含まれる可能性がある。

### エージェント化のリアリティチェック：シリコンベースの労働力に備える

Agentic AIはその登場当初の熱狂にもかかわらず、多くの企業ではその導入後も大きな変革を経験するに至っていない。その理由は、ほとんどの企業がプロセスを根本的に再設計するのではなく、単に既存のプロセスを自動化していることによる。調査対象企業のうち、わずか11%しかエージェントシステムを本番環境に導入していない。低迷の理由はレガシーシステムの統合、データアーキテクチャーの制約、不十分なガバナンスフレームワークといった解決すべき課題に取り組む必要があるためである。Agentic AIに対して先進的な企業では、エージェントファーストのプロセス再設計を実施し、新たなプロトコルを用いたマルチエージェントオーケストレーションを導入している。そしてエージェントを専用の管理フレームワーク内でのシリコンベースの労働力として位置づけている。この管理には、エージェントのオンボーディング、パフォーマンス追跡、FinOpsによるコスト管理が含まれる。将来的には、段階的な自律レベルの引き上げ、人間とデジタルのハイブリッド構成による労働力の実現、そしてエージェントが生成したデータの継続的な学習へと向かっており、これらが企業の運営方法の変革を推進し競争力を押し上げていくだろう。

## AIインフラの転換点：推論エコノミクス時代におけるコンピューティング戦略の最適化

AI活用が実験段階から本番運用へと移行する中で、企業はインフラに関する重要なジレンマに直面している。トークン単価自体は大幅に低下している一方で、利用量の急激な増加により、AI関連支出の総額は爆発的に拡大している。結果として、多くの企業では、大規模なワークロードに対してクラウドサービスのコストが見合わなくなる転換点を迎えており、月額コストが数千ドルに達するケースも珍しくない。先進的な企業は、こうした状況を受け、戦略的なハイブリッドアーキテクチャーの採用を進めている。変動性の高いワークロードにはクラウドを活用し、安定した本番推論処理はオンプレミスで担い、遅延が許されない用途についてはエッジで処理する構成である。このアプローチを支えるためには、GPU処理に最適化されたハードウェア、高速かつ高帯域なネットワーク、専用の冷却技術を備えた、AI向けに設計されたデータセンターの整備が求められる場合もある。今後の課題としては、インフラ運用を担う人材の再スキリング、AIエージェントによるインフラ管理の高度化、さらには再生可能エネルギーの活用や将来的には軌道上データセンターも視野に入れた、持続可能なコンピューティング技術の進展が挙げられる。

## テクノロジー組織の再構築：AIネイティブなテクノロジー組織の設計

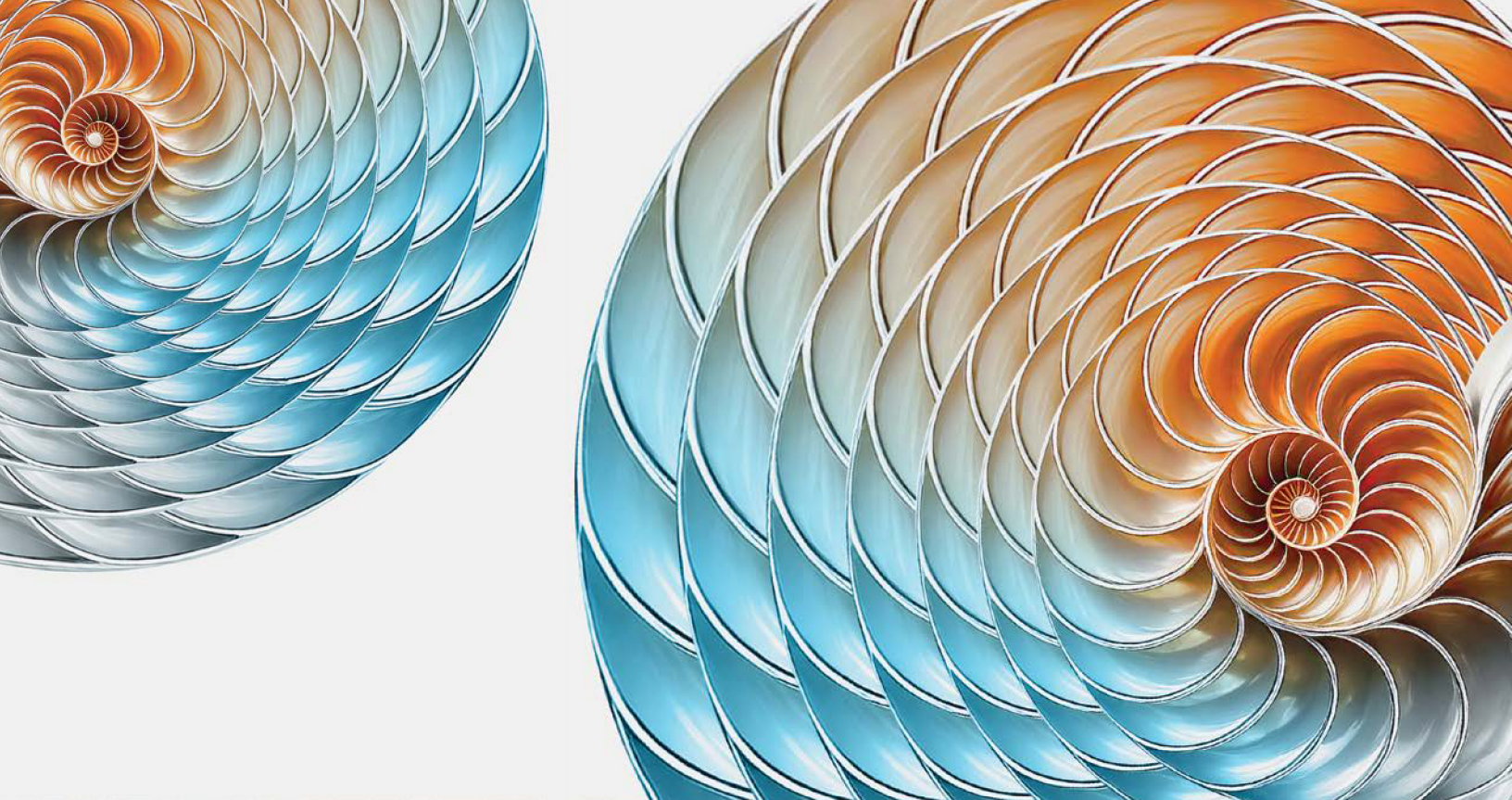
AIは、単なる自動化を超えて、テクノロジー部門の在り方を根本から再構築している。64%の企業がAIへの投資を拡大し、技術予算がAIに重点配分される中、テクノロジー部門に期待する役割の優先順位は、インフラの維持管理から戦略的リーダーシップへと移行している。先進的な企業は、AIイニシアティブを測定可能なビジネス成果に結びつけ、柔軟性を高めるモジュラーアーキテクチャーを設計し、人間と機械の協働に向けた人材戦略を再定義している。AIコラボレーションデザイナー、エッジAIエンジニア、プロンプトエンジニアなどの新しい役割が台頭する一方で、CIO（Chief Information Officer、最高情報責任者）はテクノロジーストラテジストからAIのエバンジェリストやオーケストレーターへと進化している。未来のテクノロジー部門は、エージェントアーキテクチャー、リニアプロダクト主導型チーム、人間とAIエージェントの融合、適応型ガバナンス、エコシステム指向のイノベーションを特徴とするだろう。成功には、継続的な進化を受け入れ、漸進的な改善ではなく、大胆にオペレーションを再創造することが求められる。

## AIのジレンマ：サイバー防御のためのAIの確保と活用

AIはサイバーセキュリティのパラドックスを生み出す。ビジネスのイノベーションを推進する能力は、同時に新たなリスクももたらしているのだ。組織は、データ、モデル、アプリケーション、インフラという4つの領域にわたり、シャドーAI、敵対的攻撃、AIシステム固有の脆弱性といった脅威に直面している。既存のセキュリティプラクティスは、堅牢なアクセス制御、モデルの分離、安全なデプロイメントのアーキテクチャーを通じて、AI特有のリスクに対処するために適応させることができる。同時にAIは、それ自体が生み出す脆弱性に対抗し得る、強力な新機能を提供する。先進的な企業は、AIエージェントによるレッドチーム演習、敵対的トレーニング、マシンスピードでの自動的な脅威検出を通じて、AIを防御に活用している。将来の課題には、AIと物理的なインフラの融合、自律的なサイバー戦争、量子および宇宙空間におけるセキュリティの脅威が含まれる。成功の鍵は、AI施策の初期段階からセキュリティを組み込み、イノベーションの制約ではなくイネーブラーとして扱うことである。

## ノイズを切り裂く：AIの進展に伴い追跡すべき技術シグナル

本レポートでは、ビジネスのあり方を再構築する5つのテクノロジー動向を深く掘り下げているが、いかなる瞬間においても企業に影響を与えているトレンドは5つだけではない。隣接する8つの「シグナル」もまた、注視する必要がある。その中には、AIモデルがプラトーに達している可能性、合成データがモデルに与える影響、ニューロモーフィックコンピューティングの発展、新たなエッジAIのユースケース、AIウェアラブルの成長、生体認証の機会、AIエージェントがプライバシーに与える影響、そして生成エンジン最適化の出現などが含まれる。これらのシグナルのいくつかは支配的な力へと成熟するかもしれない。その他は消え去るかもしれない。しかし、それらすべてが根底にある同じ現実を反映している。すなわち、技術変化のペースは根本的に変化しており、これらのパターンを早期に認識した企業には適応する時間があるということだ。



## イノベーションの複利効果

テクノロジーのイノベーションと導入が加速する中、5つのトレンドは、成功している組織がいかにしてトライアルから効果創出へと移行しているかを明らかにしている。

Kelly Raskovich

# 私

は1年の大半をテクノロジーリーダーとの対話に費やし、何が機能し、何が機能していないのか、そして何が彼らを夜も眠れなくさせているのかを尋ねている。最近、そうした対話の質は異なるものになってきた。

かつての問いは「AIで何ができるか」であった。今やそれは「いかにしてトライアルから効果創出へと移行するか」である。焦点は、終わりのないパイロットから真のビジネス価値へと移っており、そのすべてに切迫感がある。それはテクノロジーが向上しているからだけではなく、変化そのもののスピードが加速しているからである。

数字が物語っている（図1）。電話は5,000万人のユーザーに到達するのに50年かかった。インターネットは7年だ。ある主要な生成AIツールは、2ヶ月でその約2倍に達した<sup>1</sup>。本稿執筆時点で、そのツールの週間ユーザー数は8億人を超えており、これは地球人口の約10%に相当する<sup>2</sup>。

しかし、急速な普及は表面的なものにすぎない。イノベーションは複利的に積み重なっている。各要因は単に加算的ではなく、乗算的である。フライホイールのように考えてみるとよい。より優れたテクノロジーは、より多くのアプリケーションを可能にする。アプリケーションが増えると、より多くのデータが生まれる。データが増えれば、より多くの投資を呼び込む。投資が増えれば、より良いインフラが構築される。より良いインフラは、コストを削減する。コストが下がれば、より多くの実験を可能にする。こうしたそれぞれの改善が、他のすべての改善を同時に加速させるのである。

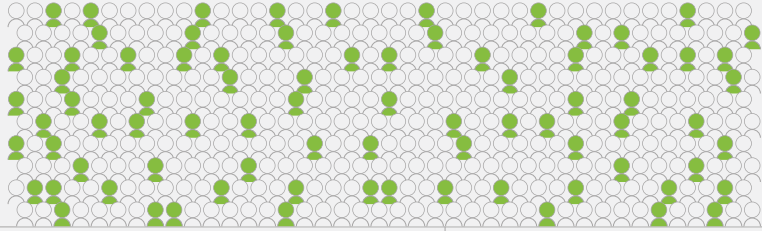
AIスタートアップが売上を100万米ドルから3,000万米ドルにスケールアップする速さが、かつてのSaaS企業の5倍であるのはこのためである<sup>3</sup>。AIにおける知識の半減期が年単位から月単位に短縮されたのもこのためである<sup>4</sup>。そして、あるCIOが私に「新しいテクノロジーを検討するのにかかる時間が、いまやそのテクノロジーの有効期間を上回っている」と語ったのもこのためである。

図1

## 数字で見るAIトランスフォーメーション

**800M**

主要AIツールの週間ユーザー数  
(地球人口の10%)



**35%**

エージェント戦略が  
不在な組織

**5x faster**

SaaS、AIスタートアップ  
の収益スケール差



**Only 11%**

エージェントの  
本番利用



**280-fold**

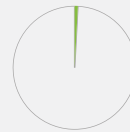
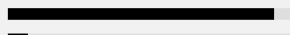
直近2年間で推論コスト  
は280分の1に削減  
(但し、請求額は依然数  
千万ドルにのぼる)



投資の不均衡:

**93% on tech**

**7% on people**



**Only 1%**

オペレーティングモデル  
変更不要の声

出所： Rebecca Bellan, "Sam Altman says ChatGPT has hit 800M weekly active users," TechCrunch, Oct. 6, 2025; Deloitte Emerging Technology Trends in the Enterprise Survey; Wing Venture Capital, "AI growing faster than SaaS"; Stanford Human-Centered AI Institute, "AI Index Report 2025"; Deloitte research on AI investment allocation patterns, 2025; Deloitte 2025 Tech Spending Outlook.

我々が調査したすべての組織が、同じ真実に気づいている。すなわち、ここまで導いてくれたものは、これから先へは進めない、ということである

クラウドファースト戦略を前提に構築されたインフラでは、AIの経済性に対応できない。人間の作業者のために設計されたプロセスは、エージェントには機能しない。境界防御を想定したセキュリティモデルは、マシンスピードで動作する脅威を防げない。サービス提供のために構築されたIT運用モデルは、ビジネス変革を推進しない。

これは単なる機能強化ではない。再構築なのである

Tech Trendsは過去17年間、今後1年半から2年の間にビジネスを再構築する可能性を秘めたエマージングテクノロジーを探求してきた。我々の調査は、デロイト

の社内専門家や外部のテクノロジーリーダーとの対話によるトレンドセンシング、ならびにエマージングテクノロジーに関するデロイト独自の調査に基づいている。今年、データから相互に関連する5つの力が明らかになった。

### AIは物理世界へ：AIとロボティクスの融合がもたらす新たな可能性

Amazonは100万台目のロボットを導入し、DeepFleetというAIがロボット群全体を統括して、倉庫内の移動効率を10%向上させている<sup>5</sup>。BMWの工場では、車両がキロメートル単位の生産ルートを自律走行している<sup>6</sup>。知能はもはやスクリーンの中に限定されない。それは具現化され、自律的であり、物理世界の現実の問題を解決している。

## エージェント化のリアリティチェック：シリコンベースの労働力に備える

38%の組織がエージェントを試験導入しているにもかかわらず、本番環境で運用しているのはわずか11%である。パイロットから本番環境への移行ギャップがすべてを物語っている。42%は依然として戦略を策定中であり、35%はそもそも戦略がない<sup>7</sup>。Gartnerは、2027年までにエージェント関連プロジェクトの40%が失敗すると予測している<sup>8</sup>。これはテクノロジーが機能しないからではなく、組織が壊れたプロセスを自動化するだけで、オペレーションを再設計していないからである。HPEの最高財務責任者は、成功するアプローチを次のように捉えている。「我々は、単一のペインポイントを解決するだけでなく、真に変革できるエンドツーエンドのプロセスを選択したかったのだ」<sup>9</sup>。自動化ではなく、再設計する。これが成功と失敗を分けるパターンである。

## AIインフラの転換点：推論エコノミクスの時代におけるコンピューティング戦略の最適化

トークンコストはこの2年間で280分の1までに低下したが<sup>10</sup>、それでも月額請求額が数千万ドルに達している企業もある。利用量の急増が、コスト低下のペースを上回ったのだ。組織は、既存のインフラ戦略がAIを本番規模の展開にスケールさせる設計になっていないことに気づき始めている。彼らはクラウドファーストから戦略的ハイブリッドへと移行している。すなわち、拡張性にはクラウド、一貫性のためのオンプレミス、そして即時性にはエッジを活用する。

## テクノロジー組織の再構築：AIネイティブなテクノロジー組織の設計

AIはテクノロジー組織を再構築し、よりリーンに、より速く、より戦略的にしている。デロイトが調査したITリーダーのうち、大規模な運用モデルの変更が進行中ではないと回答したのはわずか1%であった<sup>11</sup>。リーダーたちは、漸進的なIT管理から人間とエージェントのチームを編成することへと移行しており、CIOはAIのエバンジェリストになりつつある。成功には大胆な再構想が不可欠だ。モジュラーアーキテクチャー、組み込みガバナンス、そして永続的な進化をコア能力として備えることが求められる。

## AIのジレンマ：サイバー防御のためのAIの確保と活用

企業に優位性を与えるはずのテクノロジーが、企業を攻撃するための標的になりつつある。AT&Tの最高情報セキュリティ責任者は、**その課題を次のように捉えている**。「今日我々が経験していることは、過去に経験してきたことと何ら変わりはない。AIで異なるのは、そのスピードとインパクトの大きさだけだ」<sup>12</sup> 組織は、データ・モデル・アプリケーション・インフラという4つの領域にわたってAIを保護しなければならないが、同時に、マシンスピードで作動する脅威と戦うためにAI駆動の防御を活用する機会も手にしている。本レポートを通じて、この大きな変化をうまく乗り切っているテクノロジーリーダーたちに出会える。彼らがすべての答えを持っているわけではないが、彼らが未来への道を照らす中で、注目すべきパターンが見えてくる。

- **テクノロジーではなく課題から始める** BroadcomのCIOは次のように述べている。「特定のビジネス課題と、そこから得たい価値に焦点を当てなければ、AIに投資してもリターンが得られないということになりかねない」<sup>13</sup>
- **とりわけ、最大の課題に挑む** UiPathのCEOは次のように述べている。「永続的なPoCのサイクルに陥るのではなく、最大の問題に立ち向かい、大きな成果を目指すことを検討すべきだ」<sup>14</sup>
- **完璧さよりもスピードを優先する** Western DigitalのCIOは次のように述べている。「波に完全に乗り遅れるよりは、小さなパイロットで素早く失敗する方がましだ」<sup>15</sup>
- **人のために設計するだけでなく、人と共に設計する** Walmartは、店舗従業員をスケジューリングアプリの構築に参加させた。このアプリには、シフト交換、スケジュールの可視化、従業員による管理機能が含まれている。その結果、スケジューリングに要する時間は90分から30分に短縮され、従業員は実際にそのアプリを使用するようになった<sup>16</sup>。
- **変化を連続的なものとして扱う** Coca-ColaのCIOは、自社の歩みを「何ができるか」から「何をすべきか」<sup>17</sup>へのシフトだと表現した。そのシフト、すなわち「できること優先」から「必要なこと優先」への転換こそが、生産的な実験と終わりなきパイロットの堂々巡りを分けるものである。

私はテクノロジーの進化を長年追ってきたので、そのパターンを認識することができた。インターネットはすべてを変えた。モバイルは消費者の行動を変えた。クラウドコンピューティングは変革をもたらした。

しかし、今はそれとは違う。

AIが強力だというだけの話ではない。**S字カーブ**が圧縮されているのだ。新興からメインストリームまでの間の距離が急速に縮まっている。

段階的な改善を前提に構築された組織は、継続的な学習ループで活動する組織には太刀打ちできない。従来のプレイブックは、正しく行うための時間があることを前提としていた。その前提はもはや成り立たない。

成功するのは、最も洗練されたテクノロジーを持つ組織とは限らない。自動化ではなく再設計に踏み切る勇氣、すべての投資をビジネスの成果に結びつける規律、

機会の窓が閉じる前にやり切るスピードを備えた組織であろう。

イノベーションは複利的に積み重なる。後れを取る者と先導する者とのギャップは指数関数的に拡大する。あなたがどのように対応するかが、そのギャップのどちら側に立つかを決定する。

ただ、この航海を一人で行う必要はない。本レポートが、誰もがこの急速な変化のペースに直面していることを思い起こさせ、共に次に来るものを形作ることができるということ、あなたに気づかせることを願っている。



Kelly Raskovich  
Executive editor, Tech Trends

## Endnotes

1. Jeff Desjardins, "In the race to 50 million users there's one clear winner - and it might surprise you," World Economic Forum, June 26, 2018; Alexandra Garfinkle, "ChatGPT on track to surpass 100 million users faster than TikTok or Instagram: UBS," Yahoo Finance, Feb. 2, 2023.
2. Rebecca Bellan, "Sam Altman says ChatGPT has hit 800M weekly active users," TechCrunch, Oct. 6, 2025.
3. Zach DeWitt, "AI growing faster than SaaS," Wing Venture Capital, November 7, 2024.
4. Based on Deloitte analysis of technology adoption cycles and AI capability evolution timelines.
5. Scott Dresser, "Amazon deploys over 1 million robots and launches new AI foundation model," Amazon, July 1, 2025.
6. Brad Anderson, "Who needs factory drivers when cars drive themselves at BMW plants," CarScoop, Nov. 26, 2024.
7. Deloitte 2025 Emerging Technology Trends in the Enterprise Survey. From June to July 2025, Deloitte conducted an online survey of 500 US technology leaders to quantify the prevalence, engagement, and perceptions surrounding the adoption of emerging technologies across industries.
8. Gartner, "Gartner predicts over 40 % of agentic AI projects will be canceled by end of 2027," press release, June 25, 2025.
9. Marie Myers (executive vice president and chief financial officer, HPE), interview with Deloitte, March 1, 2025.
10. Stanford Institute for Human-Centered Artificial Intelligence, "The AI Index report 2025," accessed Nov. 12, 2025.
11. Deloitte 2025 Tech Spending Outlook. From June to July 2025, Deloitte conducted an online survey of 302 IT procurement leaders, heads of IT, and non-IT executives with technology spending oversight to understand how US enterprises in key industries are managing technology budgets.
12. "A no-nonsense approach to secure AI enablement at AT&T," *Deloitte Insights*, Nov. 21, 2025.
13. Katherine Noyes, "Broadcom CIO: 'Modernization should be driven by the business'," CIO Journal, *The Wall Street Journal*, and Deloitte, Sept. 10, 2025.
14. Katherine Noyes, "UiPath CEO: Agentic automation will 'usher in a new era of work'," CIO Journal, *The Wall Street Journal*, and Deloitte, Feb. 21, 2025.
15. Katherine Noyes, "Western Digital CIO: In the AI era, 'Play offense or get left behind'," CIO Journal, *The Wall Street Journal*, and Deloitte, Sept. 6, 2025.
16. Walmart, "Walmart unveils new AI-powered tools to empower 1.5 million associates," June 24, 2025.
17. Katherine Noyes, "Coca-Cola CIO on scaling AI: From 'What can we do?' to 'What should we do'," CIO Journal, *The Wall Street Journal*, and Deloitte, Jan. 18, 2025.





# AIは物理世界へ: AIとロボティクスの融合がもたらす新たな可能性

従来型ロボットはAIの搭載により、複雑環境でも学習・適応する機械へ進化し安全性と精度の向上を実現している。

Jim Rowan, Tim Gaus, Franz Gilbert, and Caroline Brown

**フ**ィジカルAIを搭載したロボットは、もはや研究室や工場のフロアに限定されるものではない。送電網の点検・手術の支援・市街地の走行・倉庫での人との協働など、その活動は多岐にわたる。プロトタイプからプロダクションへの移行は、今まさに起きている。

フィジカルAIとは、機械が物理世界をリアルタイムで自律的に知覚・理解・推論し、リアルタイムで相互作用することを可能にする人工知能システムを指す。これらの能力は、ロボット・車両・シミュレーション・センサーシステムに現れる。事前にプログラムされた指示に従う従来型ロボットとは異なり、フィジカルAIシステムは環境を知覚し、経験から学び、リアルタイムのデータに基づいて行動を適応させる。革命的なのは単なる自動化ではなく、デジタルインテリジェンスと物理のギャップを埋める能力にある。むしろ、デジタルインテリジェンスと物理世界とのギャップを埋める能力こそが、その核心なのである。

黎明期にありながら急速に進化するロボットの分野において、フィジカルAIはロボットを、複雑で予測不可能な環境で活動できる、適応力のある学習マシンへと変える。AI・移動技術・物理行動能力の組み合わせにより、ロボットは移動し、タスクを実行し、高性能な家電製品とは根本的に異なる方法で世界と相互作用することが可能になる。ロボットシステムに組み込まれたフィジカルAIは、動き出している。

今日、AI搭載のドローン・自動運転車・その他のロボットは、特にスマート倉庫やサプライチェーン業務において、ますます一般的になりつつある。業界・規制当局・そして導入を検討している企業は、ソリューションの大規模な展開を妨げる障壁を取り除くために取り組んでいる。組織がこれらの課題を克服するにつれて、AI搭載ロボットはニッチな領域における導入から主流の導入へと移行する可能性が高い。最終的には、フィジカルAI

の次なる進化の飛躍として、これまでにない能力で人間の空間を移動できるヒューマノイドロボットの登場を目の当たりにすることになるだろう。

## プロトタイプからプロダクションへ

デジタル環境のみで動作する従来型AIシステムとは異なり、フィジカルAIシステムは、感覚入力・空間理解・意思決定能力を統合し、機械が3次元環境や物理的状態に適応・応答することを可能にする。これらは、ニューラルグラフィックス・合成データ生成・物理法則に基づくシミュレーション・高度なAI推論の組み合わせに依存している。強化学習や模倣学習といったトレーニングアプローチにより、これらのシステムは、実世界に展開される前に、仮想環境で重力や摩擦といった原理を習得することができる。

ロボットはフィジカルAIの一つの具体例にすぎない。フィジカルAIはまた、固定カメラとコンピュータービジョンを使用して工場や倉庫の業務を最適化するスマートスペース、物理システムの仮想テストと最適化を可能にするデジタルツインシミュレーション、そしてロボットによる操作を必要とせずに人間のチームが複雑な物理環境を管理するのを支援するセンサーベースのAIシステムも包含する。

従来型ロボットがプログラムされた指示に従うのに対し、フィジカルAIシステムは環境を知覚し、経験から学び、リアルタイムのデータと変化する状況に基づいて行動を適応させる。物体を操作し、予測不可能な空間を移動し、実世界に影響を与える一瞬の判断を下す。ロボット犬は音響波形データを処理して、壊滅的な事態になる前に機器の故障を検出する。工場のロボットは、稼働中に生産スケジュールが変更されるとルートを再計算する。自動運転車はセンサーデータを使用して、人間のドライバーよりも早く自車を検知する。配送ドローンは、風の状況が変化すると飛行経路を調整する。これらのシス

テムを革命的にしているのは、単なるタスクの自動化ではなく、知覚・推論・適応する能力であり、それによってデジタルインテリジェンスと物理世界とのギャップを埋めることができる<sup>1</sup>。

### 技術の進歩がフィジカルAIとロボティクスの統合を推進

フィジカルAIの主流展開の準備が整ったのは、ロボットが環境をどのように知覚し、情報を処理し、リアルタイムで行動を実行するかに影響を与えるいくつかの技術が成熟したためである。

**視覚・言語・行動モデル** フィジカルAIは、大規模言語モデル（LLM）のトレーニング手法を採用しつつ、物理世界に関するデータを取り入れている。マルチモーダルな視覚言語行動（VLA）モデルは、コンピュータービジョン、自然言語処理、運動制御を統合する<sup>2</sup>。人間の脳のように、VLAモデルはロボットが周囲の状況を解釈し、行動を選択することを支援する（図1）。

**オンボードでの計算と処理** ニューラルプロセッシングユニット（エッジコンピューティングに最適化された特殊なプロセッサ）は、低遅延でエネルギー効率の高いリアルタイムAI処理をロボット上で可能にする。オンボード機能により、フィジカルAIシステムはLLMやVLAモデルを実行し、高速センサーデータを処理し、クラウドに依存せずに安全上重要な判断を瞬時に下すことができる。これは自動運転車、産業用ロボティクス、遠隔手術に不可欠である<sup>3</sup>。また、ロボットを孤立した機械から、インテリジェントネットワーク全体で知識を共有し、行動を調整できる自律システムへと変革することも可能だ。

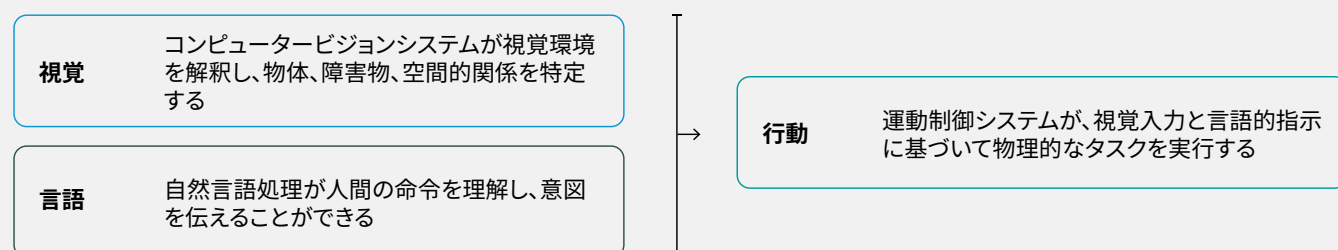
**ロボティクスの進歩**により、ロボットはよりアクセスしやすく、有能になった<sup>4</sup>：

- 周囲を「見て」理解するための**コンピュータービジョン**
- 音、光、温度、接触などの情報を捉えるための**センサー**
- 人間の筋肉に着想を得た、動きのための**アクチュエーター**
- 3D環境をナビゲートするための**空間コンピューティング**
- 頻繁な再充電なしで長時間の稼働を可能にする**改良されたバッテリー**

**トレーニングと学習** 強化学習では、ロボットは報酬や罰則を受け取ることで試行錯誤を通じて洗練された行動を発達させる。模倣学習では、ロボットは専門家のデモンストレーションを模倣する。どちらのアプローチも、シミュレーション環境または実世界のハードウェアで適用できる<sup>5</sup>。シミュレーションベースの強化学習から始め、次に的を絞った物理的なデモンストレーションでファインチューニングするという、これらの技術の組み合わせによって、継続的な学習ループを生み出すことができる。これにより、ロボットは実世界のデータを学習方策やシミュレーション空間にフィードバックすることで、改善を続けることができる<sup>6</sup>。

図1

## 視覚-言語-行動モデルの仕組み



出所： Deloitte analysis.

## 魅力的な経済性が産業利用を後押し

技術が進歩するにつれてコストは低下し、実世界での適用例も多く登場している。

高度化した製造インフラは現在、複雑なロボティクスやフィジカルAIシステムの企業規模での生産を可能としている。これは、フィジカルAIロボットがスマートフォンや自動車と同等の信頼性と品質管理で生産できることを意味し、日常的な産業利用において実用的になっている。

コンポーネントのコモディティ化とオープンソース開発により、フィジカルAIシステムの参入コストは低下している。しかし、これらのロボットは高度なAIチップとプロセッサを必要とするため、従来の産業用ロボットよりも高価なままである。全体の価格は徐々に低下しているものの、当面はこのコスト差が残る見込み。

これらの経済性が、特定のユースケースにおけるフィジカルAIとロボティクスの採用を推進している。自動運転車とドローンは、最も身近な例である(図2)。Waymoのロボタクシーサービスは1,000万回以上の有料のタクシーサービスを提供し、Aurora Innovationはダラスとヒューストン間で定期的な貨物輸送を行う初の商用自動運転トラックサービスを開始した<sup>7</sup>。

AI搭載ドローンは、スピードと利便性に関する消費者の期待を根本的に変える一方で、強力な商用ツールとしても機能している。高度なカメラとセンサーを装備したドローンは、棚の間を自律的に移動し、バーコードやQRコードリーダーで製品をスキャンすることで、倉庫の在庫を管理している<sup>8</sup>。







産業分野では、労働市場の圧力から、倉庫業務とサプライチェーン業務がフィジカルAIロボットシステムの最も初期の導入領域となっている<sup>9</sup>。

多くの組織が現在、これらのシステムを大規模に使用している。例えば、Amazonは最近、人間と協働する多様な搬送システムの一部として、100万台目のロボットを導入した<sup>10</sup>。同社のDeepFleet AIモデルは、この巨大なロボット軍団の動きを物流フルフィルメントネットワーク全体で調整し、Amazonの報告によると、これによりロボット搬送システムの移動効率が10%向上するという<sup>11</sup>。

同様に、BMWは世界中の工場にAIオートメーションを統合している。ある斬新な導入例では、BMWはセンサー、デジタルマッピング、モーションプランナーの支援を受けた自動運転技術を利用して、組み立てラインからテストを経て工場の仕上げエリアまで、新しく製造された車が人間の支援なしで自ら運転できるようにしている<sup>12</sup>。

図2

## ロボティクスとフィジカルAIの6つの主要なフォームファクター

 <p><b>タスク特化型</b> 特定の目的のために設計され、人間よりも効果的または効率的に所定のタスクを達成するロボット</p>	 <p><b>自動運転車</b> 道路で人や物を輸送する自動運転車両</p>	 <p><b>ヒューマノイド</b> 人間のタスクを補完または代替できるように、人間のよう見え、機能するように設計されたロボット</p>
 <p><b>四足歩行ロボット</b> ヒューマノイド形態を必要としない、または対応できないタスクを完了するために設計された4本足のロボット</p>	 <p><b>ドローン</b> 配送・監視・セキュリティのために自律的に観察・決定・行動できる空中ロボット</p>	 <p><b>自律移動ロボット</b> 汎用のナビゲーション・監視・ハンドリング・配送のために設計されたロボット</p>

出所：Mark Osis, Raquel Buscaino, and Caroline Brown, "Robotics & physical AI," Deloitte, 2025.

## フィジカルAIの変曲点

技術が進歩・収束し、コストが低下し、実行可能なユースケースが出現するにつれて、フィジカルAI駆動のロボットは、技術的・運用的・社会的な課題を克服できれば、ニッチな採用から主流へと移行する態勢が整っている。

### 実装の障壁を打ち破る

組織がフィジカルAIを展開しようとする中で、複雑で相互に関連する一連の実装課題に直面している。テクノロジーは機能するが、それを大規模に機能させるには、技術・運用・規制の領域にまたがる問題を解決する必要がある。これらの課題に正面から取り組む組織が、次の展開の波を定義するだろう。

**トレーニングと学習** シミュレーション環境は、速度・安全性・スケーラビリティにおいて重要な利点を提供するが、近似的な物理モデルに基づくシミュレーションと実世界の性能との間には根強いギャップがある<sup>13</sup>。「シミュレーション環境の視覚的な画像はかなり精緻だが、実世界には異なって見えるニュアンスがある」と、オハイオ州立大学工学部長のAyanna Howardは言う。「ロボットはシミュレーションで何かをつかむことを学ぶかもしれないが、物理的な空間に入ると、必ずしも同じようにはいきません」<sup>14</sup>

物理エンジン・合成データ生成・仮想トレーニングと実世界での応用を組み合わせたアプローチの進歩は、組織がシミュレーションの規模と安全性で物理トレーニングの品質を達成するのに役立つはずだ。

---

## ヒューマンファクター：AYANNA HOWARDが語るフィジカルAIとロボティクスの未来

---

Ayanna Howardは、オハイオ州立大学工学部長であり、著名なロボット研究者であり、AIの安全性とアラインメントの提唱者でもある。以前は、NASAのジェット推進研究所で上級ロボット研究者として勤務し、その後、ジョージア工科大学のインタラクティブ・コンピューティング学部の学部長を務め、ヒューマン・オートメーション・システム・ラボを設立した。

### Q:フィジカルAIとロボティクスの進歩を妨げている技術的な課題は何か

**A:** 根本的な課題の一つは、物理世界が本質的に動的である点である。私は毎日自分のオフィスに入るが、そこには常に何かしらの違いがある。誰かが掃除機をかけたかもしれない、物が動かされているかもしれない、私のコンピューターが起動しないこともありうる。問題は、ロボットが人間のように適応し、歩行し、持ち上げ、不確実性と相互作用することを学べるよう、これらすべてのパリエーションをいかにシミュレートするかである。実世界で無制限に練習することはできない。物を壊してしまうからである。

さらに、私が「操作能力対自重比」と呼んでいるハードウェア上の制約も存在する。人間の中には自分の体重以上を持ち上げられる者

もいるが、従来のロボットはアクチュエーターの制限により、重いロボットであっても自重の半分すら持ち上げられないことが少なくない。ロボットにはアクチュエーターの硬い動作を相殺する人間のような筋肉がなく、それが相互作用できる対象や動かせる物体を制限している。

最後に、リアルタイム処理の課題がある。大規模模言語モデルや視覚言語モデルは、通常、私が「人間時間」と呼ぶペースで機能する。私たちは応答に1~2秒待つことを問題とはしない。しかし、ロボットが歩行中で意思決定を要する場合、1~2秒の遅延は、物を落としたり、衝突したり、潜在的に誰かを傷つけたりすることにつながりうる。リアルタイム処理の能力は向上してきているが、まだ完全ではない。

### Q:あなたはAIシステムにおける信頼と過信について広範な研究を行ってきた。両極端はそれぞれどのような課題をもたらすのでしょうか

**A:** 表明された信頼と行動に表れる信頼の間には大きな違いがあることが分かっている。言い換えれば、人はよく「AIを信頼していない」というが、スマートフォンやコンピューターを使っているか、あるいは家の外に出ているかがどうかを尋ねると、実は日常生

活を送るだけでも彼らはAIを使っていることが分かるのだ。私の過信に関する研究は、人々が言うことではなく、その行動に焦点を当てている。我々は、間違いを犯すようにプログラムされたロボットシステムと人々が対話する研究を行った。調査では、参加者はシステムがエラーを犯すのを見たので信頼していないと述べた。しかし、彼らの実際の行動を分析すると、違う結果が見えた。彼らの行動は、ロボットを信頼していることを示していた。AIが物理的実態を伴う場合、この行動的な過信は危険になる。なぜなら、これらのロボットは環境に物理的な力を加えるからである。彼らが何かをするとき、その結果は不可逆になる可能性がある。今日のAIでは、ほとんどのタスクにまだ人間による操作が必要だが、エージェント型AIはその状況を変え始めている。

### Q:投資が必要な最も重要な研究分野は何か

**A:** 害を及ぼさずに物理空間で学習させることだ。シミュレーションでの学習を安全に物理世界に移行する方法はまだ確立されていない。シミュレーション環境の視覚的な画像はかなり精緻だが、実世界には異なって見えるニュアンスがある。ロボットはシミュレーションで何かをつかむことを学ぶかもし

## ヒューマンファクター: AYANNA HOWARDが語るフィジカルAIとロボティクスの未来

れないが、物理的な空間に入ると、必ずしも同じようにはいかない。

研究では、ロボットはシミュレーションから物理環境に移行した後に適応するが、彼らはタスクに付随する範囲で学習するのであって、全体的な環境との相互作用ではない。彼らは、摩擦係数が異なるさまざまな表面でボールをつかむことを学ぶかもしれない。しかし、シミュレートされた社会的相互作用に基づいて、ショッピングモールや大学のキャン

パスで、それらのつかんだボールをジャグリングしながら人々にどれだけ近づくべきかを学んでいるわけではない。そのような包括的な環境適応はまだ存在しない。

### Q: 通説に反するような見解はあるか

A: 私は根本的に、どこかに必ず人間が介入すべきであると考えている。必ずだ。そして、これを言っている私はロボット研究者である。100%の安全を保証するものではない

が、過信を軽減するのに役立つ。もしかしたら、CEOがロボットの年次レビューを行うことでもよいかもしれない。そのフィードバックの仕組みがなければ、我々の手に負えなくなる可能性がある。

**信頼できるAIと安全性** 物理システムでは、ごくわずかなエラー率が連鎖的な影響を及ぼし、生産ロス、製品欠陥、機器の損傷、または安全上のインシデントにつながる可能性がある。AIシステムがハルシネーション(幻覚)を起こした場合、エラーが生産工程全体に広がり、コストや業務に悪影響が連鎖的に拡大する可能性がある。

AI搭載の機械は、広範な安全性テストの後でも予測不能な振る舞いをする可能性がある。公共の場では、自律システムが予測不可能な人間の行動に対応しなければならぬため、そのリスクは著しく高まる。さまざまな業界でフィジカルAIシステムをスケールさせるためには、規制遵守、リスク評価、継続的な監視を統合した包括的な安全戦略が必要である<sup>15</sup>。

**規制環境** 企業は、管轄区域をまたいで重複し、時には矛盾する要件をナビゲートしなければならない<sup>16</sup>。ロボットが管理された工場環境から公共の場へ移動するにつれて、規制機関は安全性認証、責任、および運用監督のための新しいフレームワークを開発する可能性が高い。

**データ管理** 組織は、大量のセンサーデータ、3D環境モデル、およびリアルタイム情報を収集し、管理しなければならない。物理資産の高精度なデジタルツインは、効果的なトレーニングと展開に不可欠であり、物理的特性、オブジェクトのプロパティ、および相互作用に関する広範なデータを必要とする。組織はまた、異なるソースからのマルチモーダルデータを統合し、データセキュリティを確保し、データインフラコストを管理する必要がある。

**人間の受容** ほとんどの労働者は、予測可能でルールベースのロボットには一般的に抵抗がないが、学習し適応するフィジカルAIシステムは、特に雇用の喪失に関する心配など、新たな不安が生まれる。しかし、専門家は、ほとんどの仕事が置き換えではなく、人間とロボットの協働へと変化すると予測している<sup>17</sup>。目標は、ロボットが反復的または危険なタスクを処理し、人間が創造的な問題解決と複雑な意思決定に集中できる環境を作ることである。

**サイバーセキュリティの脆弱性 「AIのジレンマ」**で議論されているように、フィジカルAIシステムは、デジタル領域と物理領域を橋渡しする新たな攻撃対象領域を生み出す。ネットワーク接続されたフリートはサイバーリスクを増大させ、脆弱性は不正アクセス、データ侵害、さらには悪意のあるロボット制御につながる可能性がある。セキュリティ侵害が物理的な安全性と運用の継続性に影響を与える可能性がある場合、そのリスクはさらに高まる。

**ロボットフリートのオーケストレーション** フィジカルAIシステムが成熟するにつれて、組織はますます、複数のベンダーから提供される、それぞれが独自のプロトコルを持つ異種のロボット・自動運転車・AIエージェントのフリートを展開するようになるだろう。これにより、相互運用性の課題が生じ、事故、ダウンタイム、システムの混雑、および運用効率の低下につながる可能性がある<sup>18</sup>。自律的なフリート管理およびオーケストレーションシステムは、これらの問題を解決するのに役立つ。

今後18~24ヶ月で、これらの基礎的な問題を解決することで、フィジカルAIとロボティクスは従来の産業を超えて拡大することが可能になるだろう。倉庫業務とロ

ジスティクスはフィジカルAIの実験場として機能したかもしれないが、このテクノロジーは業界の境界に縛られない。

## 崩れゆく業界の境界

官民の主要な組織がフィジカルAIの大規模展開の基礎を築くにつれて、採用は指数関数的に加速している。フィジカルAIが実際の問題を解決する領域ならどこでも、新たな用途が出現している。

世界的な人材不足に直面しているヘルスケア分野では、医療技術企業がAI駆動のロボット手術やデジタル画像装置を開発している。GE HealthCareは、ロボットアームとマシンビジョン技術を備えた自律型X線および超音波システムを構築している。他の医療技術企業は、患者ケアを支援し、外科的タスクを自動化できるインテリジェントなロボットアシスタントを設計している<sup>19</sup>。

レストランもまた、労働力不足に対処するためにロボットを導入している。歩道を這うように進む配送ロボットは歩行者の速度で移動し、レストラン内ではロボットがハンバーガーを焼いたりサラダを準備したりするタスクをこなし、サービスロボットが顧客を席に案内し、食事を提供する。

スペインの多国籍天然ガス・電力会社であるNaturgy Energy Groupは、現在、点検目的でドローンを使用している。NaturgyのチーフデータオフィサーであるRafael Blesaは、技術が固まるにつれて、特に高電圧や開放されたガス管が関わる危険な現場作業において、フィジカルAIの役割が拡大すると見込んでいる。「グリッドメンテナンスに関連する多くの作業は、長期的にはロボットによって実行される可能性がある」と彼は説明する。「私の期待では、3～4年後にはロボットが物理的な作業を行い、それが人命を救うことになるだろう」<sup>20</sup>

同様に、シンシナティ市はAI搭載ドローンを使用して、橋の構造や路面を自律的に点検することで、コストを削減し、人間の検査員を危険な状況から遠ざけ、数ヶ月の分析を数分に短縮している。「この種の技術は、市長が仕事をより良く行い、より良い情報、決定、そしてコスト効率を市民に提供することを可能にするための根幹となるだろう」とシンシナティ市長のAftab Purevalは述べた<sup>21</sup>。

2024年、デトロイト市は、従来の交通システムでは移動が著しく制限されていた高齢者や障害を持つ人々のために設計された無料の自律型シャトルサービスを開

始した。Accessibili-Dとして知られるこの自動運転車は、車椅子でのアクセス対応と訓練を受けた安全オペレーターが同乗する。3台の自動運転車がデトロイトの11平方マイルの区画内で運行し、110の異なる停留所を提供した<sup>22</sup>。

業界に関係なく、これらの導入には共通する特徴がある。それは、安全性、精度、またはアクセシビリティがとりわけ重要な状況で、人間の能力を補強することである。

## ヒューマノイドロボットとその先

私たちは皆、流れるような、人間そっくりではないがかなり近い動きをするヒューマノイドロボットの話題性の高い動画を見たことがあるだろう。それらは最も魅力的なロボットの形態であるが、それは最も効率的な設計だからではなく、私たちの世界が人間の身体のために作られているからだ。これは、専門的なロボットシステムに対応するための高価な改造なしに、既存のインフラ（出入り口、階段、工場のフロア、家庭のキッチン）をナビゲートできることを意味する<sup>23</sup>。

「人々は世界と対話する方法において非常に柔軟で、常に環境と接触している。これは商用ロボットにとっては非常に難しいことである」と、オレゴン州立大学のロボット研究者であり、Agility Roboticsの共同創設者であるJonathan Hurstは言う。「通常、ロボットは非常に位置制御されたデバイスだ。CNC加工（正確で反復可能な位置決めを必要とする精密製造）やスポット溶接のようなものには適しているが、構造化されていない空間での組み立て、操作、または移動には適していない」<sup>24</sup>

いくつかの企業が、より精密な指の制御を持つ二足歩行ロボットを開発し、改良を続けている。最近、人間の認知能力に匹敵する思考連鎖推論能力が導入されたことで、技術基盤は進化し続けている<sup>25</sup>。

次の10年間で、**エージェント型AIシステム**とフィジカルAIロボットシステムの融合が進み、その「脳」がエージェント型AIであるロボットが生まれるだろう。ロボットは形態を問わず、新しい環境に適応し、複数ステップのタスクを計画し、失敗から回復し、不確実性の下で動作する能力をますます高めるはずだ。この技術の収束の影響は、ヒューマノイドロボットにとって特に顕著なものになるだろう。

各領域毎にカスタムされたロボットを用意する代わりに、より汎用的なエージェントモジュールが倉庫・家庭・

ヘルスケア・農業・その他の分野で再利用される可能性がある。エージェント型ヒューマノイドは、いつの日か、より直感的な対話・推論・交渉能力を持つアシスタント、同僚、またはヘルスケア補助者として機能するかもしれない。

ヒューマノイドの大量採用は、おそらく数年先のことだろう。それでも、UBSは2035年までに職場に200万体のヒューマノイドが存在すると推定しており、その数は2050年までに3億体増加すると予想している。同社は、これらのロボットの獲得可能な最大市場規模が2035年までに300億ドルから500億ドルに達し、2050年までに1.4兆ドルから1.7兆ドルに上昇すると推定している<sup>26</sup>。

倉庫業務やロジスティクスのような企業用途は、労働力不足に牽引され、ヒューマノイド展開の実験場であり続けている。BMWは、サウスカロライナ州の工場で、従

来の産業用ロボットにはない器用さを必要とするタスク（精密な操作、複雑な把持、両手での協調作業）のためにヒューマノイドロボットが使用可能かを検証している<sup>27</sup>。同様の理由で、ヒューマノイドはヘルスケアで役割を果たす可能性がある。あるヘルスケア企業は、リハビリテーションセンターでヒューマノイドをテスト運用しており、セラピストを支援して患者に運動を指導し、体重を支えている<sup>28</sup>。

より大きな長期的な機会は、高齢者や障害者のケア、清掃やメンテナンス、食事の準備、洗濯などの包括的な家事を視野に入れた消費者市場にある。バンク・オブ・アメリカ・インスティテュートは、ヒューマノイドロボットの材料費が2025年の約35,000ドルから次の10年で1台あたり13,000ドルから17,000ドルに低下すると予測しており、ゴールドマン・サックスは、ヒューマノイドの製造コストが2023年から2024年の間に40%低下したと報告している<sup>29</sup>。

## 研究室から実世界へ: JONATHAN HURSTが語るヒューマノイドロボット

Jonathan Hurstは、オレゴン州立大学のロボット工学教授であり、同校のロボティクス研究所の共同創設者でもある。彼の研究は脚式移動に焦点を当てている。彼はまた、商業用途で人間の労働者と並行して動作するヒューマノイドロボットを開発・展開するAgility Roboticsの共同創設者兼チーフ・ロボット・オフィサーでもある。

### Q: ヒューマノイド形態のロボットを構築することで、特定の問題を解決しようとしていたのか

**A:** 我々は、動物や人々のように動き、人間の空間にも存在できる機械を作りたいかったのだ。人々は世界と対話する方法において非常に柔軟で、常に環境と接触している。これは商用ロボットにとっては非常に難しいことである。通常、ロボットは非常に位置制御されたデバイスである。CNC加工（正確で反復可能な位置決めを必要とする精密製造）やスポット溶接のようなものには適しているが、構造化されていない空間での組み立て・操作・移動には適していない。我々のロボットは、通常の人間のような脚の構成（二足歩行・直立した胴体・両腕）にかなり近づいた。最も重要なことは、これらの各特徴には目的がある

ということだ。我々はその形態の根底にある機能を捉えている。

### Q: ヒューマノイドができることを見つけ出すにはどうしたのか

**A:** 最初から、我々は人間中心の汎用ロボットを構築することを目指していた。我々は数百のユースケースを検討した。結局、ピンやトートを持ち上げて移動するという単純なタスクが、この技術に非常に適していることが分かった。このタスクでは、廊下を移動し、ドアを通過し、人間のいる空間でも使えるように、コンパクトなサイズが求められる。2メートルの棚の最上部に25キログラムのような重いものを持ち上げる能力が必要である。

このためには、動的に安定しているもの、つまり動きながらバランスを保つロボットが必要である。静的に安定したベースは、これらのものを持ち上げようとするとう転倒する。したがって、二足歩行の脚のペアは、動的に安定し、転倒しないための最も効果的な方法である。それがスタート地点である。そこから、大きなものを持つためには両側に掴む必要があるため、両腕とした。地面から何か

を拾い上げて高く持ち上げるための到達可能な作業空間が必要であり、そのためには直立した胴体が必要で、こうした点でこの用途はこの技術に特に適している。

これは既存の自動化では非常に難しいことである。すべてのワークフローが独特であるため、かなりの柔軟性が必要である。例えば、異なる種類のトートが異なる場所に行く。トートを積み重ねたり、パレットに載せたり、コンベアベルトに置いたり、AMR（自律移動ロボット）から降ろしたりする。この種の多様性は、従来の自動化には難しいが、それでもかなり構造化されている。半構造化されていると言えるかもしれない。それは、十分に管理され、プロセスが自動化された産業環境にあり、ヒューマノイドにとって非常に良い出発点となっている。

### Q: ヒューマノイドの利用はどのようにスケールできるのか

**A:** ヒューマノイドの市場は、25年後には自動車産業の2倍の規模になるだろう。その時点で到達するまでには、多くのスケールアップが必要である。なぜなら、数百万台ものロボ

---

## 研究室から実世界へ: JONATHAN HURSTが語るヒューマノイドロボット

---

ットが必要となるからである。今日、ロボットは数百台しかない。

市場として大きいのは機能的に安全なヒューマノイド、つまり専用の作業セルに閉じ込められる必要のないロボットである。そこまで来れば数千台規模でロボットを展開し始めること

ができるだろう。現場でそれらをどのようにサポートするのか。独自の帯域幅制限やすべてのユニークな制約の中で、ロボットフリート管理ソフトウェアをどのように機能させるのか。それはロボティクスでは難しいことだが、可能である。Waymoは基本的に道路上にロボットを展開しているので、間違いなく実現可能で

ある。何かを発明する必要があるわけではないが、組織はそれを実行するために非常に有能でなければならない。ロボットがその規模での運用ができるくらいに安全になれば、それが我々が進むべき道である。

### ヒューマノイドの先へ

ヒューマノイドロボットは、その馴染み深い二足歩行の形態で人々の想像力をかき立てる。そこからどこへ向かうのだろうか。

物理的な形態の観点から、境界を押し広げるエンジニアたちは、生物学的な境界線を曖昧にする機械による実験を増やしている。生きたキノコの組織を動力源とするロボット、ネズミの筋肉組織を使って動きを模倣するロボット、または磁場を使って固体と液体の状態を遷移できる機械を想像してみたい。今日の革新的な研究室では、科学者たちは生きた有機体を機械システムに統合し、複数の移動モードを通じて複雑な環境を移動できるロボットを開発し、タスクに合わせて物理的な形態を適応させる機械を創造している<sup>30</sup>。

量子ロボティクス（量子コンピューティングとAI搭載ロボティクスの組み合わせ）もまた、まだ非常に初期段階にあるものの、有望である。重ね合わせ、量子もつれ、量子アルゴリズム、その他の量子コンピューティングの

原理により、ロボットは今日の二進コンピューターでは不可能な速度で動作できるようになる可能性がある<sup>31</sup>。量子アルゴリズムは、処理・ナビゲーション・意思決定・フリートの調整を改善すると期待されており、量子センサーは知覚と相互作用を強化するだろう<sup>32</sup>。

有用な量子ロボットは、数十年先になると予想されている。ハードウェアの未熟さ、統合の課題、量子状態の極端な感度などは、量子コンピューティングが広く展開される前に解決しなければならない課題のほんの一部にすぎない<sup>33</sup>。

ヒューマノイドの執事は少なくとも10年先であり、変わった形のロボットや量子能力は依然として大部分が実験的なものである。しかし、それらは私たちがロボティクスについて考える方法における根本的な変化を表している。これらの画期的な技術が研究室から企業へ、そして家庭へと普及するにつれて、ロボティクスの分野は単に人間のタスクを自動化することを超えて、全く新しいカテゴリーの機械を創造する方向へと動いている。

---

# Endnotes

1. Nvidia, "What is physical AI?" accessed Nov. 6, 2025.
2. Anony, "Vision-language-action models for embodied AI: A survey overview," Medium, May 12, 2025.
3. Josh Schneider and Ian Smalley, "What is a neural processing unit (NPU)?" IBM, accessed Nov. 6, 2025.
4. Jiefei Wang and Damith Herath, "What makes robots? Sensors, actuators, and algorithms," *Foundations of Robotics* (Singapore: Springer, 2022); Bank of America Institute, "Humanoid robots 101," April 29, 2025.
5. *MIT Technology Review*, "Training robots in the AI-powered industrial metaverse," Jan. 14, 2025.
6. Automate, "NVIDIA on what physical ai means for robotics," Aug. 5, 2025.
7. Mark Osis, Raquel Buscaino, and Caroline Brown, "Robotics and physical AI: Intelligence in motion," Deloitte, Oct. 17, 2025.
8. Ibid.
9. Ibid.
10. Michael Grothaus, "What are physical AI and embodied AI? The robots know," *Fast Company*, July 19, 2025.
11. Scott Dresser, "Amazon launches a new AI foundation model to power its robotic fleet and deploys its 1 millionth robot," Amazon, July 1, 2025.
12. Brad Anderson, "Who needs factory drivers when cars drive themselves at BMW plants," *Carscoops*, Nov. 26, 2024.
13. Erica Salvato, Gianfranco Fenu, Eric Medvet, and Felice Andrea Pellegrino, "Crossing the reality gap: A survey on sim-to-real transferability of robot controllers in reinforcement learning," *IEEE Access* 4, 2016.
14. Ayanna Howard, interview with Deloitte, Sept. 18, 2025.
15. Standard Bots, "Industrial robot safety standards: What you need to know," April 23, 2025.
16. Jacob Otasowie, Alexander Blum, Mohamed El Sayed Ahmed, and Mathias Brandstötter, "Danger of AI in robotics: A systematic analysis of ethical, regulatory, and economic challenges," *Springer*, Sept. 2, 2025.
17. Osis, Buscaino, and Brown, "Robotics and physical AI."
18. Rexroth, "Efficient fleet management: How to successfully orchestrate heterogeneous vehicle fleets," Aug. 30, 2024.
19. Conor Hale, "Nvidia outlines new AI projects in robotic surgery, autonomous imaging," *Fierce Biotech*, March 21, 2025.
20. Rafael Blesa, interview with Deloitte, May 22, 2025.
21. Deloitte US, "Rust belt renaissance: Cincinnati's OptoAI story," YouTube video, Sept. 15, 2023.
22. Deloitte US, "Detroit gets moving on autonomous vehicles," accessed Nov. 6, 2025.
23. *Humanoid Robotics Technology*, "Top 12 humanoid robots of 2025," February 2025.
24. Jonathan Hurst, interview with Deloitte, Oct. 6, 2025.
25. Anabelle Yearsdon, "Humanoid robots guide (2025): Types, history, best models, anatomy and applications," Top 3D Shop, April 28, 2025.
26. Steve Goldstein, "300 million humanoid robots are coming - and here are the companies that will benefit," *Morningstar*, June 18, 2025.
27. BMW Group, "Humanoid robots for BMW Group plant Spartanburg," Nov. 9, 2024.
28. *News.am*, "Humanoid robot Fourier GR-1 has been introduced: What is it for?" July 14, 2023.
29. Goldman Sachs, "The global market for humanoid robots could reach US\$38 billion by 2035," Feb. 27, 2024; Bank of America Institute, "Humanoid robots 101."
30. Future Today Strategy Group, "2025 tech trends report," accessed Nov. 6, 2025.
31. Matt Swayne, "What is quantum robotics? Researchers report the convergence of quantum computing and AI could lead to Qubots," *The Quantum Insider*, May 9, 2025.
32. Fei Yan, Abdullah M. Iliyasa, Nianqiao Li, Ahmed S. Salama, and Kaoru Hirota, "Quantum robotics: A review of emerging trends," *Quantum Machine Intelligence* 6, no. 86 (2024).
33. Swayne, "What is quantum robotics?"

---

# About the authors

## **Jim Rowan**

jimrowan@deloitte.com

Jim Rowan is the US head of AI at Deloitte and collaborates with external technology organizations, clients, and Deloitte's business leaders to help our clients achieve their AI ambitions. Beyond his client work, Rowan is a principal in Deloitte Consulting LLP. His experience spans the life sciences, health care, and telecommunications industries, with a strong focus on applying analytics, planning, forecasting, and digital transformation to enhance finance functions.

## **Tim Gaus**

tgaus@deloitte.com

Tim Gaus is a principal and the smart manufacturing business leader with Deloitte Consulting LLP. He brings over 25 years of supply chain experience with a focus on value chain optimization using emerging technology. He has led multiple supply chain transformations, spanning supply chain strategy, manufacturing optimization, supply chain planning, inventory optimization, operating model design, and operational excellence for domestic and multinational corporations.

## **Franz Gilbert**

frgilbert@deloitte.com

Franz Gilbert is a managing director at Deloitte Consulting LLP, where he is the Human Capital Strategy and Innovation leader, and serves on the Human Capital Management Committee. He and his team are responsible for developing and driving the Human Capital Growth strategy, incubating new and emerging businesses, and stewarding alliances to bring innovative solutions and deliver more valuable outcomes for clients. Gilbert serves on the board of directors for the Human Resource Certification Institute.

## **Caroline Brown**

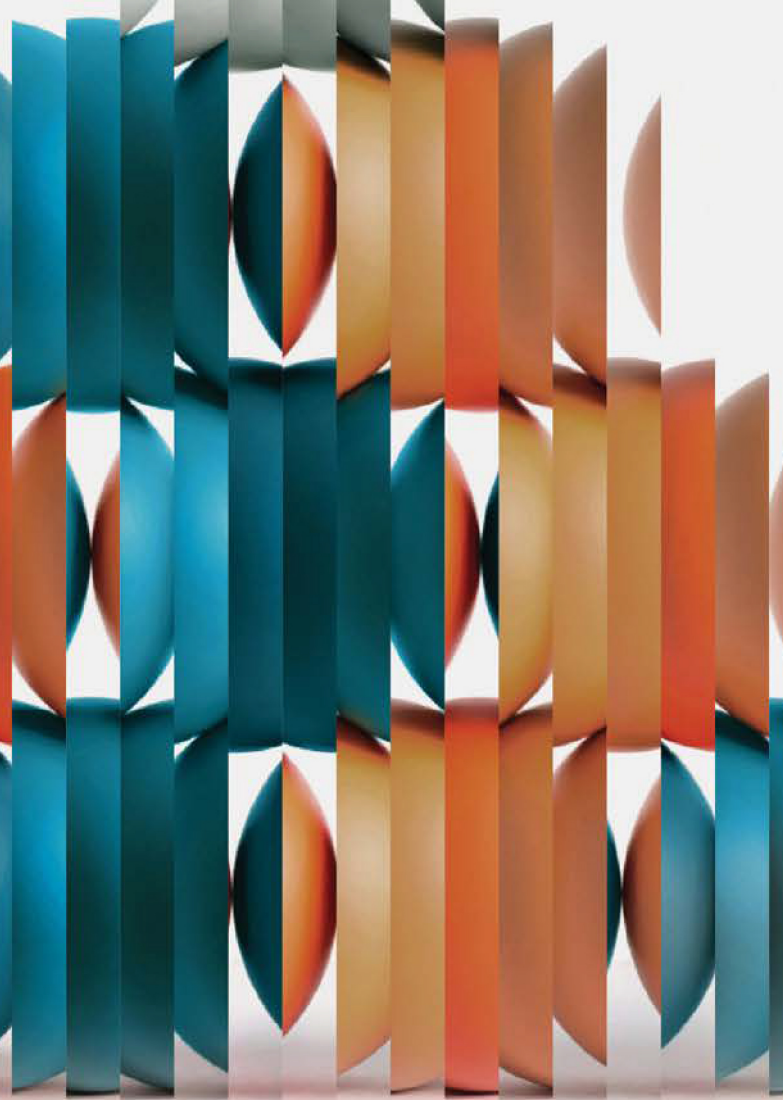
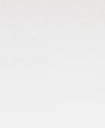
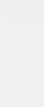
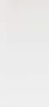
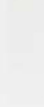
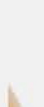
carolbrown@deloitte.com

Caroline Brown is a senior manager within Deloitte's Office of the CTO. She leads a cross-functional editorial and design production team in developing thought leadership. She serves as the editor of Tech Trends, Deloitte's flagship technology report. A writer and researcher, Brown earned undergraduate and graduate degrees in English and journalism from the University of North Carolina at Chapel Hill.

---

# Acknowledgments

Much gratitude goes to the many subject matter leaders across Deloitte who contributed to our research for this chapter: Mahesh Chandramouli, Ryan Kaiser, and Mark Osis.





# エージェント化のリアリティチェック： シリコンベースの労働力に備える

Agentic AIはその確信されている将来性にもかかわらず、多くの導入は失敗に終わっている。しかし先進的な組織では、業務を再創造し、エージェントを労働者として管理し成功を収めている。

Jim Rowan, Nitin Mittal, Parth Patwari, and Ed Burns



業はAgentic AIへと急速に移行しているが、その多くは壁にぶつかっている。彼らは、業務が実際にどのように行われるべきかを再検討することなく、人間のために設計された既存の業務プロセスを自動化しようとしている。一方先進的な組織では、全く異なる事実に関心し始めている。真の価値は、既存のワークフローにエージェントを配置するだけでなく、業務を再設計することから生まれるのだ。これは、エージェントを配置可能なアーキテクチャーを構築し、堅牢なオーケストレーションのフレームワークを実装し、これらデジタルワーカーのための新しい管理アプローチを用意することを意味する。

このことは同時に、我々が携わっている業務そのものを再考することも意味する。組織がエージェントの可能性を最大限に活用するにつれて、その業務プロセスだけでなく、労働者の定義も変わることになる。エージェントは、人間の労働力を補完し強化する、シリコンベースの労働力と見なされるようになるかもしれない。マイクロサービスベースのエージェントアーキテクチャーからシリコン労働力の管理まで、基本を正しく理解し実践することは、ワークフロー自動化の未来がどのような形をとろうとも企業側での準備を促し、エージェントネイティブなビジネス環境で効果的に競争を確保する効果をもたらす。

このことについてHenry Fordは完璧に表現している「多くの人々は、そもそも行う必要のないことをより良く行う方法を見つけようと忙しくしている。役に立たないことをより良く行う方法を見つけるだけでは、進歩はない」<sup>1</sup>。彼は1922年に自動車の製造について執筆していたが、その内容は2025年のエンタープライズ用途におけるAIについても同様に当てはまる。

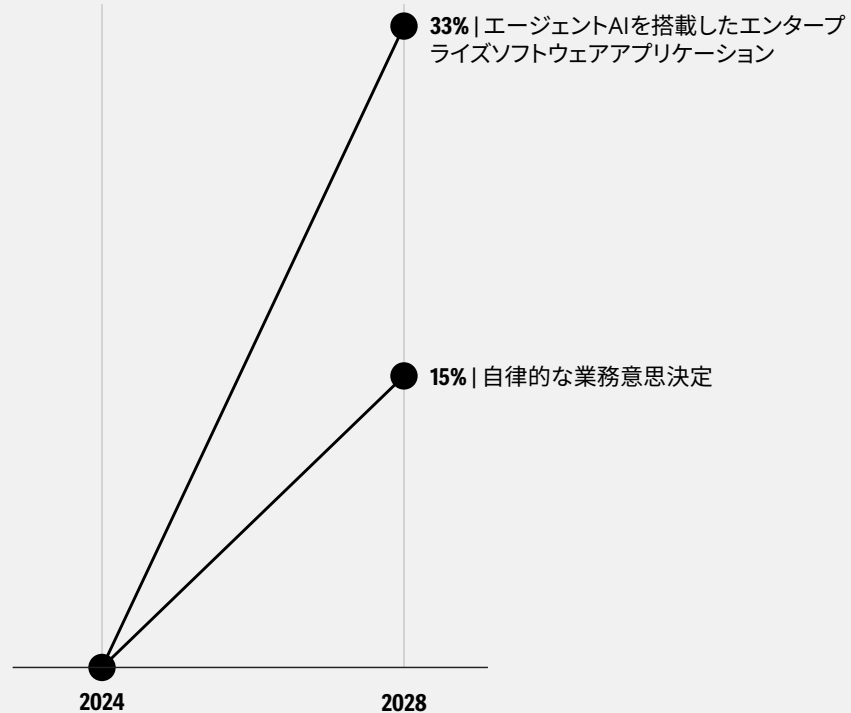
## エージェントのリアリティチェック

Agentic AIは、自律的な運用と知的なタスク実行という魅力により、企業の注目を集めている。その勢いは否定できない。Gartnerは、2028年までに日常業務の意思決定の15%がAgentic AIによって自律的に行われるようになる予測している。2024年ではこのような自律的な意思決定はゼロだった。さらには、同じ2028年までにエンタープライズソフトウェアアプリケーションの33%にAgentic AIが含まれるようになる予測されており、これは現在の1%未満と比較すると大幅な増加となる(図1)<sup>2</sup>。

しかし、この熱狂にもかかわらず、エージェントのパイロット運用を本番環境向けのソリューションに移行する上で、企業は大きな障害に直面している。デロイトグローバル(デロイト)の2025 Emerging Technology Trends in the Enterprise調査によると、調査対象組織の30%がエージェントの選択肢を検討し、38%がソリューションを試験運用している一方で、展開準備が整っているソリューションを持つ組織はわずか14%であり、これらのシステムを本番環境で積極的に使用している組織はわずか11%にすぎない。さらに、42%の組織がエージェント戦略のロードマップをまだ策定中であると報告しており、35%は正式な戦略を全く持っていないのである<sup>3</sup>。

図1

## 予測されるエージェントAIの導入率



出所：Gartner analysis. In January 2025, Gartner polled 3,412 webinar attendees about their companies' plans for agentic AI implementation.

### エージェントリアリティのギャップ

組織においてAgentic AIの可能性を最大限に引き出すことを妨げている、3つの基本的なインフラストラクチャーの障害があると考えられる。

**レガシーシステムの統合：**従来のエンタープライズシステムは、当然ながらエージェントとの相互タスクを想定して設計されていない。ほとんどのエージェントは依然として、API (Application Programming Interface、アプリケーションプログラミングインターフェース) や従来のデータパイプラインに依存してエンタープライズシステムにアクセスしており、これがボトルネックを生みエージェントの自律的な能力を制限してしまっている。Gartnerは、2027年までにAgentic AIプロジェクトの40%以上が、レガシーシステムが最新のAI実行要求をサポートできないために失敗すると予測している。これらのシステムには、真のエージェント統合に必要なリアルタイム実行能力、最新のAPI、モジュラーアーキ

テクチャー、および安全なID管理といったことが欠けている<sup>4</sup>。

**データアーキテクチャーの制約：**ETL (Extract・Transform・Load、抽出・変換・ロード) プロセスとデータウェアハウスを中心に構築された現在のエンタープライズアーキテクチャーは、エージェントの展開に摩擦を産み出してしまふ。問題は、組織におけるほとんどのデータが、ビジネスコンテキストを理解し意思決定を行う必要があるエージェントに上手に活用されるように配置されていないことだ。2025年のデロイトの調査では、組織のほぼ半数が、AI自動化戦略の課題としてデータの検索性 (48%) とデータの再利用性 (47%) を挙げている<sup>5</sup>。

解決策として、従来のデータパイプラインから、GoogleがWorld Wide Webを発見可能にしたのと同様に、組織内データ検索とインデックス作成と表現できるパラダイムシフトが必要になる。実施可能なアプローチは例

例えば、ナレッジグラフ上に構築されたコンテンツストアとインデックスストアを通じて組織内データを文脈化し、大規模なETLプロセスを必要とせずに情報を発見可能にすることである。

**ガバナンスと統制のフレームワーク：**企業は、自律的に動作するように設計されたシステムに対して、適切な監督メカニズムを確立するのに苦慮している。従来のITガバナンスモデルでは、独立した意思決定や行動を起こすAIシステムは考慮されていない。課題は技術的な統制を超えて、業務プロセス再設計にまで及ぶことは疑いが無い。現状では多くの組織は、エージェント環境向けにワークフローを再設計するのではなく、現行のワークフロープロセスを自動化しようと試みている。

さらに、いわゆるエージェントに関する取り組みで問題となるのは、実際には必要とされない自動化のユースケースである。企業は、より単純なツールでも十分な場合であってもエージェントを適用することが多く、結果としてROI (Return On Investment、投資収益率) が低くなる。この「エージェントウォッシング」は問題を悪化させ、ベンダーは既存の自動化機能を「エージェント」として再ブランディングしている<sup>6</sup>。さらに、設計の不十分なエージェントアプリケーションは、実際には追加で作業が発生する可能性がある。エージェントによるこのような「ワークスロップ」が業務プロセスをさらに非効率にすることがあることを一部の企業では認識し始めている<sup>7</sup>。

AIエージェントは、その核心部分では仕事の進め方における新しいパラダイムの代表となっているが、今日のほとんどの企業では、エージェントが提示する自動化の機会を活用する準備がまだできていない。一方先進的な組織では、戦略的なプロセス再設計、アーキテクチャーの近代化、および新しいガバナンスフレームワークに取り組むことで、これらの課題を克服できる兆しが見え始めている。

### 自律的運用のアーキテクチャー

先進的な組織は、パイロットプロジェクトを超えて、エージェント変革のための体系的なアプローチを実装することに移行している。こうした組織では個々のエージェントを展開するだけでは効果として不十分であることを認識している。代わりに、エージェントをシステムやワークフローに統合するために考え抜かれたアプローチと、展開後のエージェントを慎重に管理する取り組みを実践している。

### 業務プロセスをエージェントネイティブに再設計する

Agentic AIに先進的に取り組む企業では、単に既存のワークフローにエージェントを配置してはいない。代わりに、エージェントの独自の強みを活用するために業務プロセスを再設計している。つまり、一歩引いて現在の業務内で自動化の機会を見つけるのではなく、end-to-endの範囲で業務プロセスを検討する必要がある。エージェントは、さまざまなトランザクションを処理し、互いに通信し、協力してビジネスの成果を達成することができるが、それは基盤となる業務プロセスがこれらの能力をサポートするように構成されている場合に限られる。

「今は、ワークフローがどのように機能すべきか、対して、現在どのように機能しているかを理解するために、バリューストリームマッピングを実施する絶好の機会だ」と、IntelのグローバルSIアライアンス責任者であり、元AI戦略担当副社長のBrent Collinsは言う。「単に既存の非効率なプロセスを自動化する(牛が通ってきた道を舗装するだけ)のではなく、このAIの進化を活用して、エージェントがビジネスのために業務を最適に協力・サポート・最適化する方法を再創造すべきだ」<sup>8</sup>

ほとんどの企業の既存プロセスは、人間のスタッフを中心に設計されていた。これに対してエージェントは異なる方法でタスクを遂行する。彼らは休憩も週末も必要としない。継続的に大量のタスクを完了することができる。これを組織が認識すると、プロセス再設計の機会は魅力的なものになる。だからこそ、Agentic AIで成功している企業は、自社のプロセスをend-to-endで見ているのだ。

エンタープライズソフトウェアおよびサービス企業であるHPEは、まさにこの種のプロセス再設計を念頭に置いてAIエージェントを開発している。「私たちは、単一のペインポイントを解決するだけでなく、真に変革できるend-to-endのプロセスを選択したかった。私たちは異なる方法で運営したかったのだ」と、執行副社長兼最高財務責任者のMarie Myersは言う<sup>9</sup>。

彼女のチームは、社内の業績評価レビューの完了を支援するAlfredという名のAIエージェントの作成を主導した。Myersによると、レビューを実施するプロセスは非常に時間がかかるが、大規模なデータセットから作成されるため、エージェントによる自動化に適しているという。チームが開発したエージェントは、エージェントフロントエンドのユーザーインターフェースと、その下で動

作する4つの個別のエージェントで構成されている。これらのエージェントは、クエリを処理のために複数の要素に分解し、SQLデータに対してデータ分析を行い、データを提示するためのチャートやグラフを作成し、AIの洞察をユーザーフレンドリーな構造化レポートに変換する。エージェントは、同社のエンタープライズリソースプランニングおよび顧客関係管理システムの上にあるデータウェアハウスからデータを取得する。

Myersは、このプロジェクトが彼女のチーム外、さらにはHPEを超えても教訓となると信じていると言う。「このユースケースは、機能や業界を越えて適用できる。だからこそ、私たちはこのユースケースを選んだ。私たちは、組織のさまざまなレベルで変化を推進できるようにしたかったのだ」

## スキルをデジタル化しスケールさせる:JOHN ROESEが語る、AIエージェントを用いたビジネスプロセス変革

John Roeserは、Dell Technologiesのグローバル最高技術責任者兼最高AI責任者であり、同社のグローバル技術戦略とAI変革イニシアティブを主導している。エンタープライズテクノロジーにおける数十年の経験を持ち、厳格なガバナンスとセキュリティ基準を維持しながら、測定可能なビジネス価値を提供する実用的なAI実装の推進に注力している。

### Q:AIエージェントに関して、企業が見落としていることは何か

**A:** エージェントをデジタルスキルと考えるなら、その真の価値は、それらが集合体として機能し始めたときに現れる。チャットボットやコーディングアシスタントのような第一世代のAIツールは、販売情報の提示やコードの作成といった単次元のプロセスの処理に非常に優れている。しかし、プロセスが複合的、つまり単一のドメイン内に完全に存在するわけではないものになると、エージェントの方が優れたツールである。エージェントは、互いにコンテキストを渡し、境界を越えて推論し、エージェント間のようなプロトコルで対話する能力を持っている。

ほとんどの複合プロセスは、企業内にのみ存在するわけではない。サードパーティ・ソフトウェアベンダー・SaaSプロバイダーがそのワークフローの一部である。エージェント間の信頼できる安全な連携は不可欠である。そうでなければ、我々はそれらのプロセスの境界を越えてデジタル化することは決してできない。ほとんどの企業は、モノリシックな単

一プロセスにAIを適用することにほとんど着手していない。しかし想像してほしい。組織を運営する複合プロセスにAIを適用した場合に生産性がどれだけ向上するか。

### Q:これを社内でどのように実践しているか

**A:** 現在、我々は12のPoC (Proof Of Concept、概念実証) をエージェントで進めており、これらすべてが見積もり・権利・請求・物流を含むドメインを横断した顧客問題のend-to-endの修復といった複合的な問題に取り組んでいる。我々はROIに非常に注力しているため科学技術関連プロジェクトに対しては行っていない。販売・サービス・サプライチェーン・エンジニアリングといった会社の財務実績に重大な影響を与える分野でエージェント技術が登場している。

我々は20程度の大規模業務プロセスの自動化に着手している。2025年末までには、第一世代のツールとしてドメインを横断して機能する自律システムを稼働させる予定であり、これにより来年はエージェントの活用を大幅に拡大するための非常に良い一年になるだろう。

### Q:必要なコストとインフラ投資について、組織レベルでの検討をどのように支援したか

**A:** プロセスの初期段階で、財務パートナーとその事業部門の責任者によって署名された現実的なROIを求めている。その厳格な取り決めにより、確固たるROIが示された場合にのみ本番稼働が行われる。

またAIは、人・組織・企業などではなく、業務プロセスに適用されることにも気づいた。我々は、改善しているのはプロセスであることを意識している。

改善を続ける中で、我々はプロセスに対して非常に規律正しい態度で臨むようになった。例えば人々が独自のAIソリューションを設計することを許可するのをやめ、代わりに、AIへの投資とソリューションを評価・承認するアーキテクチャーレビューボードを設立した。

### Q:既存の業務プロセスをすでに文書化し、測定していたか

**A:** AIはプロセス改善技術なので、確固たるプロセスがなければ、進めるべきではない。まずそれを解決してほしい。さもなければ、この技術をどこに適用するかを推測することになる。

我々はデータを整理し、導入しているプロセスについて明確な定義を得た。それがなければ、定量化できず、正確でないかもしれない何かにAIを適用しようとしていただろう。

このアプローチを念頭に置いて、我々のサービス組織はすべてのプロセスをデジタル化した。我々はすべてのデータを単一のアシスタントにまとめ、すべてのデジタルおよびヒューマンチャネルに配置して、次の最善のアクションを予測した。その結果、コストと顧客満足度に関するすべての指標で2桁の改善が見られた<sup>10</sup>。

## レガシーシステムの置き換え

組織がend-to-endのプロセスを検討すると、レガシーソフトウェアを含む複数のシステムにまたがるワークフローを見出すことになる。これは、コアモダナイゼーション戦略に影響を与える。昨年の**Tech Trends 2025レポート**で議論したように、AIはビジネスの運営を定義する本質的なビジネスルールとワークフローを学習し、理解する能力をますます高めている。組織は、自社の真のコアシステムが何であるかを慎重に検討し、エージェントがレガシーシステムのギャップを効果的に埋めることができる場合に、従来のアプリケーションモダナイゼーションを使用するかどうかを決定する必要がある。

トヨタでは、チームがエージェントツールを使用して、ディーラーへの車両の到着予定時刻に関する可視性を向上させており、車両供給問題を解決するためにまもなくエージェントを使い始める予定だ。このプロセスは、以前は50から100のメインフレーム画面と、サプライチェーンチームメンバーによる大幅な手作業を伴っていた。現在では、エージェントが製造前からディーラーへの納車までの車両に関するリアルタイム情報をスタッフに提供しており、メインフレームと対話する必要はなくなった。

今後、チームはエージェントに車両輸送の遅延を特定し、問題を解決するためのメールを下書きする権限を与える予定だ。

「エージェントは、チームメンバーが朝出勤する前に、これらすべてのことを行うことができる」と、**トヨタのデジタルイノベーション担当副社長**であるJason Ballardは言う。「私たちは、この分野にもう少し投資するという重要な決定を下した。これが今後の差別化要因になると感じている」<sup>11</sup>

## シリコンベースとカーボンベースの混合労働力の管理

おそらく、AIエージェントを実装する際の最も重要な変化は、エージェントが新しい形態の労働力であり、人間の（カーボンベースの）労働力といくつかの類似点を共有する可能性があることを認識することだろう。一部の組織は、エージェントを単純な自動化ツールを超えた用途として使用することを考え始めており、それらを人間の労働力と統合する方法を模索し始めている。

この進化は、仕事は何を意味するのか、どのように実行されるのか、そして誰が実行するのかという、根本的な

再創造を表している。この変化の中心にあるのは、AIエージェントと人間の労働者が異なるスキルセットを持っているという認識だ。エージェントは定義されたプロセスに優れているが、人間はビジネス要件の変動する状況や複雑な問題解決シナリオを乗り切るために不可欠であり続ける。

この変革は、人間の労働者が今後向かうことになる2つの主要な領域を生み出す。

- **コンプライアンスとガバナンス:**人間はますます、エージェント運用の検証・監督・ガードレールの構築に焦点を当てるようになる。
- **成長とイノベーション:**人間はまた、業務を再創造し、エージェントの能力から生まれる新しい機会を特定することに集中する。

保険会社Mapfreでは、AIエージェントが組織全体で使用されており、損害査定のような定型的な管理タスクをエージェントが処理する保険金請求管理もそのひとつだ。そして、顧客とのコミュニケーションのようなデリケートなタスクに関しては、常に人がループに関与している。Mapfreのグループ最高データ責任者であるMaribel Solanas Gonzalezは、どのタスクをエージェントに委任するかを慎重に検討し、エージェントが安全かつ効率的に完了できるタスクであることを確認していると言う。リスクを伴う可能性のあるものはすべて、依然として人間の労働者を經由する。こうした取り組みは仕事の性質を変え始めている。同社は、適切に統治され、尊重され、安全なAIを優先するAIマニフェストを公表している。

「そもそもハイブリッドの設計である」と彼女は言う。「これらのエージェントの高い自律性をもってしても、人々に取って代わることはないが、人間の労働者が今日行っていることを変え、人間はより価値のある仕事に時間を投資できるようになるだろう」<sup>12</sup>

他の企業はさらに先を行っている。バイオテクノロジー企業Modernaは最近、初の最高人事・デジタル技術責任者を任命し、実質的にテクノロジー部門と人事部門を統合した。この動きは、人と技術を統合して仕事の進め方を加速させることで、Modernaの運用モデルを進化させるための戦略的な一歩だった。

「人事組織は労働力計画を非常に上手く作成し、IT部門は技術計画を上手に作成する。それが人であれ技術

であれ、業務計画について考える必要がある」と、Modernaの最高人事・デジタル技術責任者であるTracey Franklinは言う<sup>13</sup>。

### 特化型対広範な自動化

成功した導入は、企業全体の自動化を試みるのではなく、特定の、明確に定義されたドメインに焦点を当てている。広範な自動化は依然として可能だが、単一のモノリシックなソリューションではなく、オーケストレーションにて責務が分担された方法で動作する複数の特化型エージェントが必要となる。

組織は、技術的な成熟度や特定のユースケースの要件によって左右される、内製化または調達についての重要な決定を迫られる。調査によると、戦略的パートナーシップを通じて構築されたパイロットは、社内で構築されたものと比較して完全な展開に至る可能性が2倍高く、外部で構築されたツールの従業員使用率はほぼ2倍である<sup>14</sup>。

### マルチエージェントオーケストレーション

企業における生成AIの第一波は、汎用チャットボットであった。これらは生産性向上ツールとして有用であるものの、自動化の機会を必ずしも提供できなかったためビジネスの新たな効率性を推進するに至らなかった。今度はAIエージェントを使用することで、組織は特定のタスクを自動的に実行する高度に専門化されたツールを開発できる。スペシャリストのエージェントがオーケストレーションされた方法で展開されると、ワークフロー全体を自動化できる。このアプローチは、エージェントの相互作用を容易にさせる標準とプロトコルを深化させることによって可能になる。

**モデルコンテキストプロトコル (MCP) :** Anthropicによって開発されたMCPは、AIシステムがデータソースやツールに接続する方法を標準化し、エージェントがエンタープライズリソースにアクセスするためのユニバーサルインターフェースを提供する<sup>15</sup>。有望ではあるが、MCPは複雑なエンタープライズセキュリティ要件の処理やレガシーシステムの統合において限界に直面している。

**エージェント間プロトコル (A2A) :** Googleのプロトコルは、プラットフォームを越えた異なるAIエージェント間の直接通信を可能にし、エージェントの発見・タスクの委任・協調的なワークフローを取り扱う<sup>16</sup>。

**エージェント通信プロトコル (ACP) :** これはエージェントがRESTful APIを介して互いに通信できるようにするオープンプロトコルであり、エージェントが構築された環境に関係なく協業できるようにする<sup>17</sup>。ACPは、単一ネットワーク内でのエージェントの数に関する制限や、既存のエンタープライズツールとの統合の複雑さにより、ハードルに直面する可能性がある<sup>18</sup>。

これらのプロトコルは、専門家が「AIへのマイクロサービスアプローチ」と表現するものの基盤層を代表している。つまり、エージェントを、プラットフォームにて多数の小規模で専門化されたそれぞれの領域において、ワークフローの指示やデータが存在する場所の近くに配置することだ。このアプローチには、複雑さの軽減(小規模なエージェントはデバッグ・テスト・保守が容易である)、スケーラブルなオーケストレーション(複数の専門化されたエージェントを複雑なタスクのために組み合わせることができる)、およびエージェントが相互運用性を維持しながら異なるシステムで実行できるプラットフォームの柔軟性など、いくつかの利点がある。

### エージェントのためのFinOps

エージェントが継続的に動作するにつれて、不適切に構成されたエージェントの相互作用は、予測不可能なリソース消費やコストの急増などの連鎖的なアクションを引き起こす可能性があり、コスト管理が重要になる。組織は、エージェント主導の費用を監視および制御し、トークンベースの価格設定モデルを考慮に入れるための、専門の財務運用フレームワーク(つまりFinOps)を必要とする。これらのフレームワークは、リソースタギング・リアルタイム監視・自動スケーリングやライトサイジングを含む自動リソース管理、およびAI固有の支出を管理するための強力なガバナンスフレームワークを通じて、コストを詳細に追跡するのに役立つ<sup>19</sup>。

### Agentic AIの導入を推進するための5つの質問

組織がエージェントの活用を検討するにあたり、現在および将来にわたってその採用を推進するのに役立つ5つの戦略的な質問を検討することができる。

- どのようなエージェントが展開され、どのような機能を実行するのか
- 人間の従業員と比較したコストプロファイルはどのようなものか
- どのプロセスが、どの程度の効率で自動化されるのか

- 今後4年間で、人間とデジタルの労働力の最適な組み合わせはどうか
- 5年後には、エージェントが運用領域全体を引き継ぐことになるのか

今日AIエージェントを実装する準備ができていないほとんどの企業は、最初の3つの質問に対する準備された回答を持っている可能性が高い。しかし、後の2つを検討するにつれて、事態はより曖昧になる。多くは、エージェント技術と基盤となる生成AIモデルが将来どのように発展するか、そしてこの発展が労働力の構成と運用上の優先順位の変化をどのように推進するかにかかっている。

## 人間とデジタルの協業が差別化を推進する

未来の企業は、従来のカーボンベースの労働力を超えて、職務機能全体を自律的に処理するデジタルエージェントを含む、仕事の基本的な性質に大きな変化をもたらす可能性が高い。これまで議論したように、企業はすでにハイブリッドな人間とデジタルの労働力を開発し始めている。組織がこのバランスを正しく取ることができれば、それは今後、ほとんどの業界で主要な競争上の差別化要因になるだろう。

### 自律性のスペクトラム

組織は、適切な人間の監督トリガーを備えた、段階的な自律性レベルを通じて、エージェントの意思決定に対する明確な境界を定義する必要がある。自律性のスペクトラムは、3つの異なるフェーズを経て進行する。

- **拡張:** エージェントが人間の労働者の能力を向上させる今日の現実
- **自動化:** エージェントが人間によって定義されたプロセス内のタスクを自動化する新たな能力
- **真の自律性:** 人工汎用知能がエージェントに最小限の監督で作業させることを可能にする未来の状態

成功には、「エージェントスーパーバイザー」、つまり、例外を判断し処理するために要所となるポイントでワークフローに人間を配置することが必要だ。これは単にエージェントの仕事を確認することではなく、重要な意

思決定ポイントでの作業の戦略的な引き継ぎに関するものである。今後数年間で、AI技術が向上し、潜在的に人工汎用知能に達するにつれて、組織はエージェントにより独立して作業させることができるようになるはずだ。リーダーは、エージェントが処理するのに適した責任を委任していることを確認するために、AI能力の状態を継続的に評価する必要がある。

### エージェントのための人事

エージェントが職務機能内で成熟するにつれて、組織はこれらを管理するためのアプローチが必要になる。エージェントが人間の労働者と類似点を共有する領域については従来の人事管理の概念を適用することになる。しかしそれだけでなく、その独自の特性を考慮してエージェントを管理するための全く新しいフレームワークが必要になる可能性が高い。職場文化・従業員の忠誠心・労働者のモチベーションなど、人事のいくつかの焦点分野はエージェントには適用されないが、組織が人間のスタッフを管理する方法は主要な管理の柱として残り続ける。その他の労働者管理の方法は、拡張してエージェントに適用することができる。

**オンボーディング:** 人間の労働者と同様に、エージェントには企業の独自のデータと運用について訓練するオンボーディングプロセスが必要になる。同時に、人間の監督者は、新しいエージェントを活用する方法についてのトレーニングと教育を受ける必要がある。これは、エージェントと人間のスタッフが協業するための、デジタル労働力のオンボーディングに対する2方面からの新しいアプローチである。

**パフォーマンス管理:** これは、エージェントの管理が従来の人事管理と最も異なる領域の1つかもしれない。組織は、エージェントが何をしたか、なぜ特定の決定を下したか、そして誰の権限の下で行動したかを証明するシステムが必要になる。これには、デジタルIDシステム、トランザクションの暗号化された領収書、およびすべてのエージェントアクションの不変のログが必要だ。エージェントがビジネスの運営全体に展開されるにつれて、人間の管理者が評価するには多すぎるデータを生成するため、パフォーマンスを管理する追加のエージェントが必要になるかもしれない。

**ライフサイクル管理:** エージェントには、継続的なトレーニングの更新、優先分野への再配置、そして潜在的には退職計画さえも必要になる。組織は、デジタルワーカーが最終的に人間の従業員と同様に課税対象となる可能性があることを認識し、生産性の貢献を追跡

するためにエージェントに個別の名前を割り当て始めている<sup>20</sup>。

**ゼロトラストアーキテクチャー**：人間の労働者が企業リソースにアクセスするために定期的に認証タスクを完了する必要があるのと同様に、エージェントのアクションが継続的に検証および承認されることを保証するために、一時的な認証システムを実装する必要がある<sup>21</sup>。適切に調整されれば、エージェントを管理するためのフレームワークは、人間とデジタルの労働者間の協業を強力に促進する。しかし、エージェントをデジタルワーカーとしてのアナロジーを文字通りに捉えすぎると、エージェントの可能性を制限するかもしれない。人間のパフォーマンスを測定するために開発された基準にエージェントを留めておくことは、本来人間の労働者に任せた方が良い場合でも、誤ってエージェントを担当に置いてしまうリスクがある。

### デジタル排気ガスとしてのデータ

エージェントが働く環境では、システムは実行されたアクションと結果についての膨大な量のデータを生成される。今日、ほとんどのエージェントは自身の出力データで学習をしないが、将来的には、このシリコンワーカーによるデジタル排気ガスが、エージェントが学習し改善することを可能にする貴重な洞察の宝庫になる可能性がある。組織がこの副産物をどのように利用してエージェントの学習と能力を強化するかについては、今後の重要な差別化要因となり得る。

これは根本的な考え方の転換を表している。エージェン

トによる推論のすべての行為はトークンを生成し、それらのトークンは学習システムを強化できるデータを構成する。将来最も重要になる可能性が高いのは、この継続的なデータストリームの洗練された使用である。

### エージェントネイティブの未来

システムモダナイゼーションの未来を検討すると、初期段階での検証の結果では、ハイブリッドアプローチが最も普及する可能性が高いことを示唆している。このアプローチでは、エージェントがレガシーシステムの利用可能年数を延長する一方で、組織は特に重要な業務プロセスについてモダナイゼーションを追求することが可能になる。このアプローチにより、組織は将来の技術決定に対する戦略的柔軟性を維持しながら、エージェントの能力からただちに価値を実現できる。

Agentic AIへの移行は、技術的な進化に留まるものではない。それは、企業がどのように運営し、競争し、価値を創造するかを再形成するための組織的な変革である。エージェントネイティブなプロセス設計、マルチエージェントオーケストレーション、およびシリコン労働力管理の基本要素を習得した組織は、ますます自動化されたビジネス環境で成功する立場となるだろう。

成功の鍵は、エージェント変革で人間を機械に置き換えることではなく、人間とシリコンベースの労働者の両方の独自の強みを活用する協業を新たに創造することにあると認識することにある。この協業を効果的に推進する方法を見つけ出した組織が、仕事そのものの未来を定義するだろう。

---

## ギザギザのフロンティア:ETHAN MOLLICKが語る、労働力としてのAIエージェント

---

Ethan Mollickは、ペンシルベニア大学ウォートンスクールの教授であり、*Co-Intelligence: Living and Working with AI*の著者である。ビジネスと教育におけるAIの実用的な応用に関する第一人者として、組織がAIを効果的に採用し、業務に統合する方法に関する研究で知られている。

**Q:AIがツールから労働力へと移行するとは、実際にはどのようなことか**

**A:**多くの組織のリーダーは、これが何を意味するのかを明確に理解していない。「AIが何か

をやる」とか「たくさんエージェントを管理することになる」といった、漠然とした発言が多い傾向にある。しかし、それは組織の運営方法を再考し、やり直すことなしには起こらない。

私は、これは実際には技術的な問題ではなく、プロセスの問題だと考える。それは、ギザギザのフロンティアを理解しなければならないことを意味する。AIは数学とコーディングに非常に優れており、これは数学とコーディングのタスクに明らかな影響を与えるが、分析や人々との会議のようなタスクではその影響はそれほど明白ではない。労働者は、

仕事の中で時間を調整して、異なることを行う必要がある。AIエージェントがすべてを行うわけではないが彼らは基本的な単純作業を行ってくれるので、私は代わりにインタビューのためにより多くの相手に電話をかけることができる。リーダーはその未来を明確に説明できなければならない。

**Q:エージェントファーストのプロセス再設計に関して、組織は何を考慮する必要があるか**

**A:**AIの仕事をするには、リーダーシップ・ラボ・クラウドの3つが必要である。第一に、クラ

---

## ギザギザのフロンティア:ETHAN MOLLICKが語る、労働力としてのAIエージェント

---

ウド、つまり組織の全員がこれらのシステムを使用していることが必要である。第二に、24時間365日実験を積極的に行い、クラウドからのアイデアを実際の製品に変えるラボが必要である。そして最後に、連携したリーダーシップが必要である。リーダーは組織設計について考えなければならない。例えば、以前の10倍または100倍の速さでコーディングできるようになった場合でも、まだアジャイル開発を行っているのか、といったことである。このような速度ではアジャイル開発は機能しなくなるので行う必要はない。

### Q:最も重要な労働力のスキルは何か

A:「AIを使うスキル」だがこれは正確に測定したり訓練したりする方法がまだ分かっていない。それにはおそらく、自ら行動する主体的な姿勢や試行錯誤をいとわない意欲、それを後押しする適切なインセンティブ設計、そして自分の分野の専門分野に対する深い知見が含まれる。

### Q:エージェントが業務を引き継ぐのはいつ頃だと予想するか

A:分からないが、エージェントはすでに人々が思っているよりも優れている。真のエージェ

ントはすでにここにある。ただ、あなたがそれらを使っていないだけである。そして、あなたはそれらを構築しなければならない。しかし、それは今日でも実行可能である。いつ使用可能になるかという未来のタイムフレームは不要である。なぜなら、現在の技術で経済的に価値のあるエージェントを今すぐにでも構築可能で、先進的な企業では高い精度で自律的に多くの作業を行うエージェントワークフローを構築しているからである。エージェントによりすべての人間の仕事を置き換えられるのか。いいえ、私もそうは望んでいない。技術がもっと成熟するのを待っているのか。そうだとしたらあなたは困ったことになるだろう。なぜなら、それはすでにそこにあるからである<sup>22</sup>。

---

## Endnotes

1. The Henry Ford, “Henry Ford quotations,” accessed Nov. 6, 2025.
2. Gartner, Inc., “Gartner predicts over 40% of agentic AI projects will be canceled by end of 2027,” press release, June 25, 2025.
3. 2025 Deloitte Emerging Technology Trends in the Enterprise Survey, publication in process.
4. Gartner, Inc., “Gartner predicts over 40% of agentic AI projects will be canceled by end of 2027.”
5. 2025 Tech Value Survey by Deloitte Center for Integrated Research, fielded June 2025.
6. Gartner, Inc., “Gartner predicts over 40% of agentic AI projects will be canceled by end of 2027.”
7. Bruce Gil, “‘Workslop’: AI-generated work content is slowing everything down,” Gizmodo, Sept. 23, 2025.
8. Deloitte On Cloud podcast interview with Brent Collins, vice president of AI strategy, Intel, Aug. 27, 2025.
9. Marie Myers, executive vice president and chief financial officer, HPE, Deloitte interview, March 1, 2025.
10. John Roesse (chief technology officer and chief AI officer, Dell Technologies), interview with Deloitte, Sept. 29, 2025.
11. “Reimagining operations with agentic AI at Toyota,” *Deloitte Insights*, Dec. 3, 2025.
12. Maribel Solanas Gonzalez, group chief data officer, Mapfre Insurance, Deloitte interview, June 18, 2024.
13. Tracey Franklin (chief people and digital technology officer, Moderna), interview with Deloitte, Sept. 26, 2025.
14. Aditya Challapally, Chris Pease, Ramesh Raskar, and Pradyumna Chari, “The gen AI divide: State of AI in business 2025,” July 2025.
15. Anthropic, PBC, “Introducing the model context protocol,” Nov. 25, 2024.
16. Rao Surapaneni, Miku Jha, Michael Vakoc, and Todd Segal, “Announcing the Agent2Agent Protocol (A2A),” Google for Developers, April 9, 2025.
17. AgentCommunicationProtocol.dev, “Welcome,” accessed Nov. 6, 2025.
18. Saad Merchant, “ACP: Future of offline AI agent collaboration,” Alumio, Oct. 24, 2025.
19. Kearney, “FinOps for AI and AI for FinOps,” Jan. 28, 2025.
20. Jake Latimer, “Will AI be taxed? The debate over AI-powered businesses: The 2025 tech-tax tussle,” *Medium*, March 13, 2025.
21. Ken Huang, “Agentic AI identity management approach,” Cloud Security Alliance, March 11, 2025.
22. Ethan Mollick (professor, Wharton School of the University of Pennsylvania), Deloitte interview, Jan. 1, 2025.

---

# About the authors

## **Jim Rowan**

jimrowan@deloitte.com

Jim Rowan is the US head of AI at Deloitte and collaborates with external technology organizations, clients, and Deloitte's business leaders to help our clients achieve their AI ambitions. Beyond his client work, Rowan is a principal in Deloitte Consulting LLP. His experience spans the life sciences, health care, and telecommunications industries, with a strong focus on applying analytics, planning, forecasting, and digital transformation to enhance finance functions.

## **Nitin Mittal**

nmittal@deloitte.com

Nitin Mittal is a principal at Deloitte and leads Deloitte's global AI program. He advises organizations on AI applications and the implications of emerging technologies on the strategy and competitive positioning of businesses. At Deloitte, Mittal is responsible for shaping the AI market and creating new business opportunities by harnessing emerging technologies. He is also leading Deloitte's own effort to be a global AI-fueled organization and transform how they deliver professional services.

## **Parth Patwari**

ppatwari@deloitte.com

Parth Patwari leads Deloitte's AI and Data practice across all industries in the United States. He has extensive experience working with capital markets and payments institutions to architect, design, and implement large-scale systems that support mission-critical customer, finance, risk, regulatory, and compliance functions. Patwari drives efficiency agendas using AI, analytics, and data management capabilities.

## **Ed Burns**

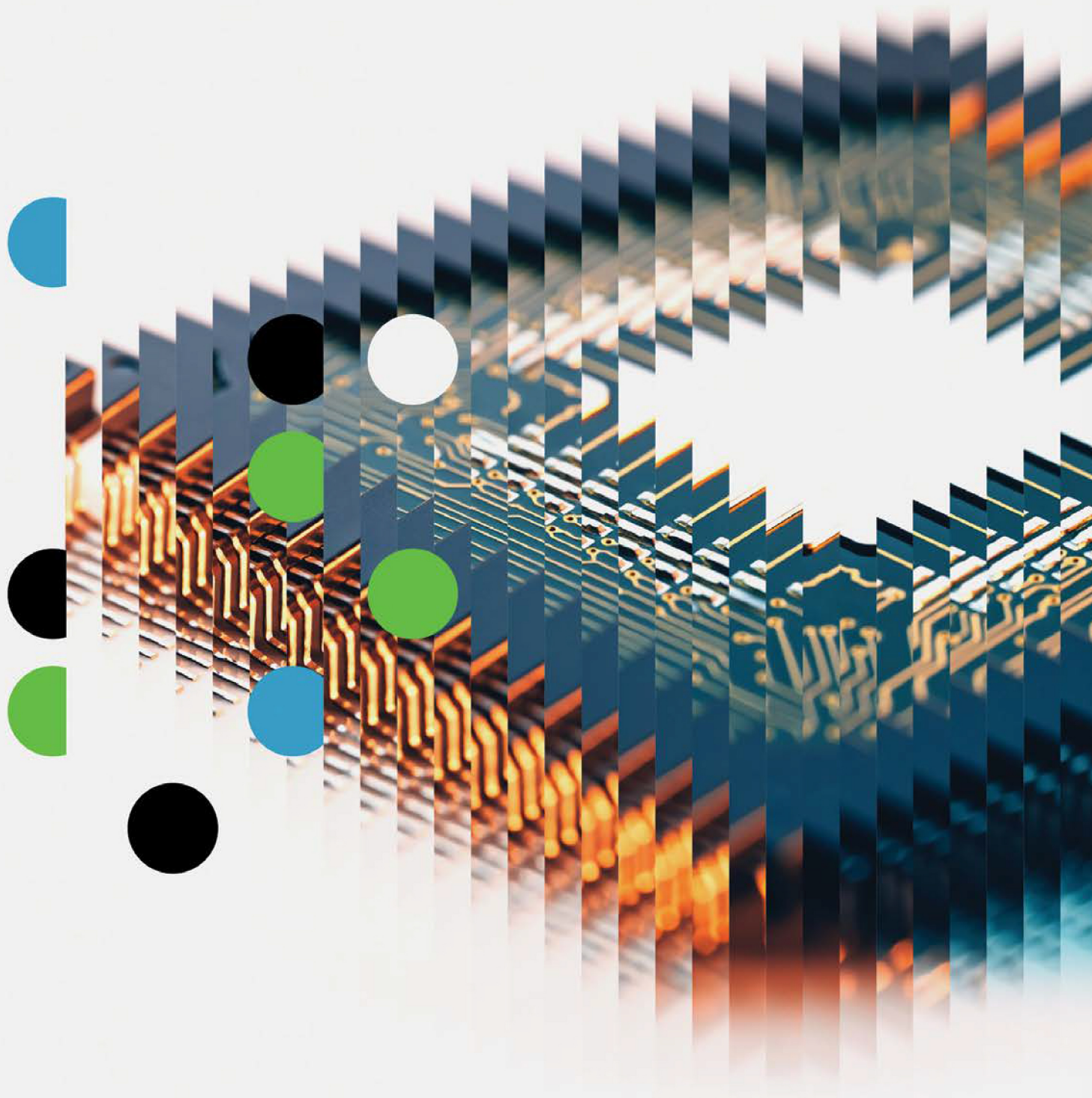
edburns@deloitte.com

Ed Burns leads the client stories initiative within the Office of the CTO known as Trend Lines. This project serves as a key research input to Tech Trends and other eminence. Prior to his current role he led a tech news publication that covered all things AI, analytics, and data management.

---

# Acknowledgments

Much gratitude goes to the many subject matter leaders across Deloitte who contributed to our research for this chapter: **Jinlei Liu, Baris Sarer, Kate Fusillo Schmidt, Prakul Sharma, Akash Tayal, and Ashish Verma.**





# AIインフラの転換点：推論エコノミクスの時代におけるコンピューティング戦略の最適化

AIがPoCから本番展開へと移行する中で、組織は既存インフラがAI特有の要件と乖離していることに気づき始めている。

Nicholas Merizzi, Chris Thomas, and Ed Burns

**生**成AIが急速に注目を集めた当初、組織は次世代の製品やサービスの構想に注力していた。現在、AIは成熟期に入りつつある。しかし、PoC段階から本番規模の展開へと進むにつれ、多くの組織は、既存のインフラ戦略がAIの要求に適合していないことを認識し始めている。

反復的なAIワークロードは、ほぼ常時推論を実行すること、すなわち、AIモデルを実世界の業務プロセスで利用することを意味する。クラウドベースのAIサービスを利用する場合、API (Application Program Interfaces、アプリケーション・プログラム・インタフェース) 呼び出しが頻発し、コストが急激に増大する可能性がある。このため、一部の組織では、AIワークロードを実行するためのコンピュート資源の見直しを迫られている。

しかし、課題はコストだけではない。データ主権、レイテンシー、知的財産の保護、レジリエンスといった観点も重要である。解決策は、単にクラウドからオンプレミスへ、あるいはその逆へとワークロードを移行することではない。重要なのは、各ワークロードに最適なコンピュート基盤を選択し、それを組み合わせたインフラを構築することである。

AI活用に最適なインフラを検討する過程で、組織はチップセット、ネットワーク、ワークロードオーケストレーションの進화가、全社的な重要課題に対応し得ることに気づくだろう。インフラのモダナイゼーションと人材の準備を同時に進める組織は、来たるべきコンピューティングのルネサンスにおける競争環境を定義する存在となる。

## 推論エコノミクスが鳴らす警鐘

AI利用に関する計算構造は、組織に前例のない速度でインフラ再計算を迫っている。推論コスト自体は過去2年間で約280分の1に急落した<sup>1</sup>一方で、AI関連支出の総額は爆発的に増加している<sup>2</sup>。その理由は単純である。推論という形での利用量が、コスト低下をはるかに上回るペースで増加しているからである。

APIベースのLLM (Large Language Model、大規模言語モデル) ツールは、PoC用途には適しているが、全社業務へ展開するとコスト面で持続不可能となる<sup>3</sup>。すでに一部の組織では、AI利用に関する月額請求額が数千万ドルに達している。最大のコスト要因は、継続的な推論を前提とするエージェント型AIであり、トークンコストが急増する要因となっている。

## 企業がコンピュート戦略を再考する理由

AI利用に伴う請求額の増加は、組織にAIワークロードの配置先や実行方法を再考させる直接的な要因となっている。ただし、見直しの背景はコストだけにとどまらない。

**コスト管理：**一貫して高ボリュームなワークロードにおいては、オンプレミス展開の方がクラウドよりも経済的となる転換点を迎えつつある。具体的には、同等のオンプレミス環境を構築する総コストに対して、クラウドコストが60~70%を超え始めた段階で、予測可能なAIワークロードについては運用費よりも設備投資の方が魅力的となる可能性がある<sup>4</sup>。

**データ主権：**規制要件や地政学的懸念を背景に、一部の組織はコンピューティングサービスの国内回帰を進めている。重要なデータ処理やAI機能を自国管轄外のサービス事業者に全面的に依存することを避ける動きが広がっている。特に米国以外の地域では、主権型AI（ソブリンAI）の取り組みが進展し、インフラ投資を加速させている<sup>5</sup>。

**レイテンシーへの感度：**リアルタイム性が求められるAIワークロードでは、データソースへの近接性が不可欠となる。特に製造現場、石油掘削施設、自律システムなどでは、ネットワーク遅延がリアルタイムの意思決定を阻害する。応答時間が10ミリ秒以下であることが求められるアプリケーションでは、クラウドベース処理に内在する遅延は許容できない。

**レジリエンス要件：**中断が許されないミッションクリティカルな業務では、クラウド接続が遮断された場合に備え、オンプレミス基盤を主系またはバックアップとして確保する必要がある。

**知的財産保護：**多くの組織データはいまだオンプレミスに存在している。このため、機密性の高い情報を外部のAIサービスに移動するのではなく、AI機能をデータのある場所に持ち込むことをより好むようになっている。これにより、知的財産の統制を維持し、コンプライアンス要件を満たすことが可能となる。

こうした要因を背景に、多くの国でデータセンター容量の拡張が前例のないペースで進んでいる。デンマークの不動産管理企業であるThylanderは、国内で**新たなコロケーション型データセンターの整備を進めており**、AIワークロードで利用される最先端のGPUなどに必要なラックスペース、ネットワーク、電力、冷却設備を提供している。

Thylander Data CentersのCEOであるAnders Mathiesenによれば、現在デンマーク国内に存在するハイパースケール規模のデータセンターは、すべて外国企業によって所有されているという。一方で、国内企業が所有・運営する事業者によってデータを保管・処理できる選択肢を求める声が、企業の間で高まりつつある。

「データ主権を考え、実際に誰がデータセンターを所有しているのかを見つめ直すことが、デンマーク企業のために、同時に、デンマーク市場に価値を見出す国外企業のためにも、デンマークらしい取り組みを行いたいと考える出発点となった」とMathiesenは述べている<sup>6</sup>。

## インフラのミスマッチ

組織は前述の要因を踏まえて将来の方向性を検討することができる一方で、現行インフラの状態そのものが新たな障壁となる場合がある。既存のデータセンターは、床上げ構造、標準的な冷却方式、プライベートクラウド仮想化を前提としたオーケストレーション、従来型のワークロード管理を特徴としており、いずれもラックマウント型の空冷サーバーを前提に設計されている。一方で、AIインフラに求められる技術要件は、GPU間的高速ネットワーク通信からInfiniBandのような高度な相互接続技術に至るまで、従来のエンタープライズ環境には存在しなかったアーキテクチャー上のアプローチを必要とし、この構造的な乖離が、AI活用を拡大する上での障壁となり得る。

## AIに最適化されたデータセンター

先進的な組織は、クラウドかオンプレミスかという選択を迫られるのではなく、それぞれの強みを活かしたハイブリッドアーキテクチャーの構築を進めている。このアプローチは、過去10年にわたり支配的であったクラウド対オンプレミスという二元論的な考え方からの転換を意味する。

この物理的なインフラのミスマッチは、組織がAI活用を拡大するにつれて、主要なボトルネックとなる可能性がある。しかし、先進的な組織はすでに、将来のデータセンターの姿を描き始めている。

## 3層ハイブリッドアプローチ

先進的な組織は、三層構造のハイブリッドアーキテクチャーを導入し、利用可能なあらゆるインフラ基盤の強みを活かしている。

**伸縮性を担うクラウド：**パブリッククラウドは、変動する学習ワークロード、突発的なキャパシティ需要、実験フェーズ、既存データの所在や移動コストを踏まえ、クラウド展開が合理的なケースを担う。ハイパースケラーは最先端のAIサービスへのアクセスを提供し、急速に進化するモデルアーキテクチャーの管理を簡素化する。

**一貫性を担うオンプレミス：**プライベートインフラは、高ボリュームかつ継続的なワークロードに対する本番推論処理を、予測可能なコストで実行する。組織は、性能・セキュリティ・コスト管理に対する統制を確保しながら、AIインフラ運用に関する内部知見を蓄積することができる。

**即時性を担うエッジ：**ローカル処理は、最小限のレイテンシーで時間制約の厳しい意思決定を担う。特に製造現場や自律システムでは、瞬時の応答が運用の成否を左右するため、エッジ処理は不可欠となる。

AI分野の思想的リーダーであるDavid Linthicumは次のように述べている。

「クラウドは特定の用途においては理にかなっている。AIにおけるいわば「イージーボタン」のような存在である。しかし重要なのは、用途に応じて最適なツールを選択することである。組織は多様で異種混在のプラットフォーム上にシステムを構築し、コスト最適化の観点から最善となる選択を行っている。ある場合はクラウドであり、ある場合はオンプレミスであり、また別の場合にはエッジとなる」<sup>7</sup>

## ハイブリッドの実現性チェック:AIインフラの適正規模に関するDAVID LINTHICUMの見解

David Linthicumは、AI、クラウドコンピューティング、サイバーセキュリティ分野において国際的に認知された思想的リーダーであり、イノベーターであり、インフルエンサーである。グローバル2,000企業、新興のイノベーター企業、政府機関に対し、思想的リーダーシップ、アーキテクチャー設計、テクノロジーに関する指針を提供している。

**Q：企業がクラウドファーストからハイブリッドモデルへと進化する中で、どのような課題に直面し、その解決策は何か**

**A：**最大の課題は複雑さである。異種混在のプラットフォームを採用すると、信頼性を維持しながら複数の異なる基盤を同時に管理することになる。これはマルチクラウドの導入時にも見られた現象であり、組織は一夜にして5,000のクラウドサービス管理から10,000のサービス管理へと拡大し、それらを異なるプラットフォーム上で運用せざるを得なくなった。

各プラットフォームを個別に管理するのではなく、組織には統合的な管理アプローチが必要である。モバイル基盤がどのようにデータを保存しているのか、クラウド環境やデスクトップ環境とどう違うのかといったことを、いちいち意識したくない。そうした複雑性は、物理的な配置にかかわらず、リソースをグループやクラスターとして管理できる抽象化レイヤーへと押し下げるべきである。

そうしなければ、組織は専門チームを増員し、プラットフォーム固有のツールを購入することで複雑性に対処することになる。しかしそれは高コストかつ非効率であり、戦略的

に考えることなく場当たり的なプロセスで複雑性管理を拡張することになり、結果としてビジネス価値を損なう。本質は、運用上の頭痛の種を減らし、組織にとって本当に重要なことに集中できる状態をつくることである。

**Q：デロイトの調査では、クラウドコストが同等のハードウェアコストの60~70%に達した場合、組織は代替手段を真剣に検討すべきであると示唆している。クラウドファーストからハイブリッドモデルへの移行を検討する際、組織は他にどのような転換点を注視すべきでないと考えるか**

**A：**オンプレミス基盤とパブリッククラウドが同等の条件で比較できるのであれば、私は常にパブリッククラウドを選択する。理由は単純で、導入が容易であり、スケーラビリティと伸縮性を得られるからである。しかし、クラウドコストが同等のハードウェアコストの60~70%に達した段階では、コロケーション事業者やマネージドサービス事業者といった代替案を評価すべきである。これは、経済性を無視してクラウドファーストを前提とするのではなく、インフラ配置についてデータに基づいた意思決定を行うための、実務的かつ定量的な判断指標となる。

**Q：データセンターのサステナビリティという問題はどのように解決されると考えるか**

**A：**最終的に言えることは、データセンターの増加が止まることはないという点である。需要は極めて大きい。私が住んでいる北バージニアでは、今この場所から半径約16キロ圏内に100カ所ものデータセンターが存在している。そうである以上、この方向に進

むのであれば、クリーンな電源を活用することで環境への負荷をできるだけ抑えるしかない。その選択肢の一つが原子力である。多くの人にとって不安を感じさせる選択ではあるが、現実的には他に代替手段がほとんど存在しない。

今後は、データセンターが集積する地域に小型原子力発電所が設置され、現在と同様にそこから電力を供給する形になると考えている。私の近くにも、データセンターに電力を供給することだけを目的とした発電所があるが、それはクリーンエネルギーではない。ビジネスを維持しながら、より環境負荷の低い手段で同じことを実現することが、現実的に受け入れ得る唯一のトレードオフである。何らかの新たな電源を確保しない限り、意味のある速度で送電網を拡張することはできない。

**Q：このトピックについて、過激な意見や、間違っていると思う通説はあるか**

**A：**それは簡単である。すべてがGPU上で動作するわけではないという点であり、私たちはその思い込みから脱却する必要がある。数年前に見られたGPUの困り込みは、正直なところ非常に馬鹿げていた。現実には、組織に実質的な価値をもたらす形でAIを活用する大半のワークロードは、専用プロセッサを必要としない。CPU上で十分に動作する。もちろん、大規模言語モデルを用いた大規模学習を行うのであれば、専用プロセッサは必要となる。そうでなければ、数カ月で終わる処理に10年かかってしまうだろう。しかし、そのようなユースケースは極めて限定的であり、多くの組織がそのレベルのAI活用を行うことはない。

## コンピュータインフラ配置のための意思決定フレームワーク

コンピュータインフラの配置を判断するためのフレームワーク（図1）は一見すると単純に見えるが、実務においてその判断は決して容易ではない。誰もが、最新のモデルを最速のハードウェアで、できるだけ少ない障壁で立ち上げたいと考える。しかし、その選択は高コストになりがちである。

こうした背景から、Dell Technologiesは近年、アーキテクチャーレビューボードを設置した。このボードは、新たなAIプロジェクトを評価し、コスト・性能・ガバナンス・リスクの観点から、一貫したツールと最適なインフラが選択されているかを確認する役割を担っている。Dellは現在、4つの中核領域にわたってエージェント型AIのユースケース開発を進めており、経営層はこれらの高ROI領域におけるユースケース拡大を見据えている。プロジェクト数が増加する中で、それぞれが適切なインフラ上で実行されていることを担保することが極めて重要であると、リーダーは指摘する。場合によっては

AIサービス事業者のAPIを呼び出すことが最適となる一方で、別の場合には完全にオンプレミスのリソースを利用する判断が求められる。

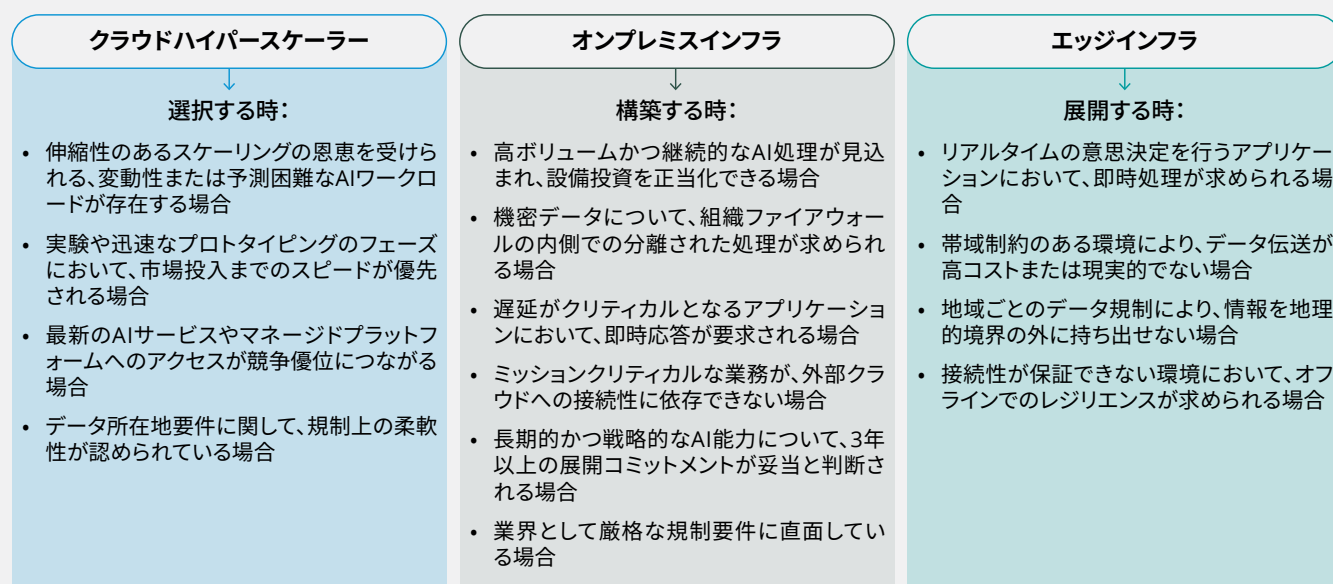
「これらのシステムはリソース集約度が非常に高いため、アーキテクチャーに対する厳格さはこれまで以上に重要になっている」とDellのグローバル最高技術責任者兼最高AI責任者であるJohn Rueseは述べる。「推論モデルやエージェント、そしてそれに伴うコストを議論し始めた瞬間から、こうしたアーキテクチャー上の規律が不可欠となる」<sup>8</sup>

## ハードウェアアーキテクチャーの革命

この局面は、組織に対し、中央処理装置（CPU）を中心とした従来の思考から脱却し、AI向けに最適化された専用ハードウェアアーキテクチャーへと移行する、前例のない機会をもたらしている。組織は、プロセッサ配置について深慮した意思決定を行い、汎用コンピューティングからワークロード特性に応じた最適化へと舵を切りつつある。

図1

## コンピューテーションワークロード配置のための意思決定フレームワーク



出所：Deloitte analysis.

この進化は、単一のシステム内に複数のプロセッサ種別を統合する形で進んでいる。具体的には、並列的なAI処理を担うGPU、オーケストレーションや従来型ワークロードを担うCPU、効率的な推論処理を担うNPU（ニューラルプロセッシングユニット）、特定の機械学習タスクに最適化されたTPU（テンソルプロセッシングユニット）である。現在のサーバー更改では、CPUとGPUを組み合わせた混在構成が一般的になりつつある。

かつては、1つのトレイに4～8基のGPUを搭載し、CPUがそれらを制御する構成が見られたが、現在ではCPU1基あたりGPU2基程度の構成が増加している。

**カスタム構築されたAIデータセンター：**これらの潮流は、いわばAIデータセンターと呼ぶべき形へと収束しつつある。そこでは、CPUに対して相対的にGPUの比率が高い構成、新たなサーバーモデルやハイブリッドワークロードに対応したオーケストレーションレイヤー、迅速な展開を可能とする進化したデータセンターのフォームファクターが採用される。また、レイテンシー低減を目的としたプロセッサ間の光ネットワーク接続や、GPUの能力を最大限に活用するためのワークロードの移行およびプラットフォームも含まれる。

## AIファクトリーの台頭

AIワークロードの拡大により、AIファクトリーと呼ばれる新たな形態が登場している。これは、AI処理に特化して設計された統合型インフラエコシステムであり、複

数の専門的コンポーネントを単一のソリューションとして統合する：

- **AI専用プロセッサ：**高帯域メモリと同一パッケージ化されたGPU、および汎用計算ではなくAIオーケストレーションに最適化された特別設計のCPU
- **オーケストレーションプラットフォーム：**異なるコンピュートタイプにまたがるマルチモーダルAIワークロードを統合的に管理できる基盤であり、さまざまなAI技術をシームレスに連携させることを可能にする
- **高度なデータパイプライン：**AIモデルが利用することを前提に、データの収集、クレンジング、前処理を行う専用システムであり、従来の抽出・変換・ロードに伴うボトルネックを解消する
- **高性能ネットワーキング：**データ転送の遅延を最小化するための高度な相互接続技術であり、光ネットワークの進化やGPU間専用通信プロトコルを含む
- **アルゴリズムライブラリ：**AI機能を特定のビジネス目的に整合させる形で事前最適化されたソフトウェアフレームワークであり、開発期間の短縮と性能向上を実現する

これらのAIファクトリーは、余剰となった計算能力をサービスモデルとして提供することも可能であり、重要なワークロードに対する戦略的な統制を維持しつつ、未使用の処理能力を収益化することができる。

## グリーンフィールドの利点：専用AIインフラに関するJOHN ROESEの見解

John Roeselは、Dell Technologiesのグローバル最高技術責任者兼最高AI責任者であり、同社のグローバル技術戦略とAIトランスフォーメーションのイニシアティブを主導している。エンタープライズテクノロジー分野で数十年にわたる経験を有し、厳格なガバナンスとセキュリティ基準を維持しながら、測定可能なビジネス価値を生み出す実践的なAI実装の推進に注力している。

**Q：AIインフラに関連する最大のボトルネックと課題は何か**

**A：**多くの組織が現在保有しているインフラ

は、AI登場以前の時代を前提に設計されたものであり、マルチクラウド時代の初期に下されたアーキテクチャー上の判断に基づいている。どのクラウドを使うか、ネットワークポロジをどうするか、オンプレミスとオフプレミスをどう切り分けるかといった判断は、おそらくパンデミック以前に行われたものである。当時存在していなかったものを前提にアーキテクチャーを設計できるほど、誰も賢くも幸運でもなかったというのが実情である。近い将来、ほとんどのインフラキャパシティは、従来型ワークロードではなくAIシステムのために使われるようになる。AIワークロードには、単なるデータではなく知識

レイヤーが必要であり、また高速化されたコンピュートが求められる。これらのワークロードは分散実行が可能であり、さまざまなアプローチが併存する高エンタロピーな産業環境の中にある。そのため、インフラの最も基礎的なレベルにおいて、これまでとは全く異なる種類のワークロードであると言える。

**Q：AIファクトリーという概念は、この文脈においてどのような位置づけになるのか**

**A：**AIファクトリーは、AIのためのグリーンフィールド環境である。従来のエンタープライズアプリケーションやサービスを前提に設計され

## グリーンフィールドの利点:専用AIインフラに関するJOHN ROESEの見解

たブラウンフィールド環境を改修し、適切にAI環境を動作させることは困難である。AIには、高速化されたコンピュートアーキテクチャーが必要であり、多くの場合、CPUだけでは不十分である。ネットワークの観点ではトポロジーは簡素化される一方で、極めて高速であることが求められる。ストレージ環境は、実質的には知識レイヤーであり、ベクトルデータベース、グラフデータベース、ナレッジグラフ、コンテキスト対応型チャットボット、データパイプラインなどで構成される。また、AIアプリケーションおよびその実行環境自体も、極めてモダンなものとなっている。こうした要素を既存のブラウンフィールドインフラに後付けで組み込むことも理論上は可能であるが、私たちは、AIに最適化されたインフラ、すなわちAIファクトリーを新たに構築することを推奨している。そうすることで、立ち上げスピードを大幅に高め、アーキテクチャー上のリスクを低減し、AIのために設計された専用環境を実現することができる。

### Q:それを立ち上げるのに通常どのくらい期間を要するか

**A:**実際には、既存環境を改修するよりも速い。私たちは、GPUと知識レイヤーを備えた並行環境を立ち上げ、既存インフラと接続してきた。すべてのデータはデータメッシュによ

って連携され、AIツールは従来ツールと同じデータメッシュを参照する。一方で、実際の物理トポロジー、すなわちそれらが稼働する基盤は、高速化されたサーバー、知識レイヤーのデータ管理、AIワークロード、可観測性、統制機能から構成される。これを独立した環境として構築する方が、既存環境に後付けで組み込むとするよりも速かった。エージェント型AIスタック全体を即座に稼働させるために、ストレージ、コンピュート、ネットワークを事前に組み上げたアプライアンスを導入することも可能である。ブラウンフィールドの外側に構築することで、多くの複雑性から切り離すことができ、その結果、迅速な展開が可能となる。

一見すると追加コストのように思えるかもしれないが、実際にはそうではない。既存のレガシー環境にAI機能を無理に組み込むとする運用コストは、新たに専用インフラを構築する場合よりも高くなる可能性が高い。

### Q:サステナビリティはインフラの意思決定プロセスにどのように関わってくるか

**A:**計画策定において、エネルギー効率は重要な判断要素である。高度な冷却システム、熱管理技術、サーバーの進化により、消費電力あたりの性能を最大化すると同時に、エネルギー使用量の可視化と削減が可能とな

る。特に重要な判断の一つが、液体冷却方式をいつ採用するかである。例えば、ダイレクト液体冷却はフリーエア冷却と比較して少なくとも2倍のエネルギー効率を実現できるため、ダイレクト液体冷却を採用した単一ラックであっても、コストおよび設置面積の削減に寄与する。

次に注目すべきは、既存インフラである。IT資産の低い利用率は、データセンターにおけるエネルギー浪費の最大要因である。レガシーインフラを最適化し、無駄を削減しつつ効率を高めることができれば、AI拡張に伴う追加的な環境負荷を抑制できる可能性がある。

最後に、多くのAIワークロードはクライアントデバイス側へと移行可能である。AI PCは、分散型でありながら非常にエネルギー効率の高いコンピューティング環境である。すでに電力網に組み込まれており、既存の環境フットプリントの中に存在している。相当量の計算処理をデータセンターからこれらのデバイスへ移行できる可能性があり、ワークロード特性に応じて機能の一部を高効率なAI PCへ分散させることで、全体としての環境負荷を低減することができる。

## データセンターの新たなフロンティア

現在進行しているAIインフラの変革は、より広範なコンピューティングの変革の始まりにすぎない。今後5年から20年の間に、新たなコンピューティングパラダイムが成熟するにつれ、データセンターは、用途ごとに高度に特化したツールを受け入れるため、継続的な進化を求められることになる。

### インフラの進化は続く

カスタムシリコンの統合は、汎用チップの枠を超え、特定のAIタスク向けに設計された専用プロセッサへと加速している。これには、パターン認識用途<sup>9</sup>に適したニューロモーフィックコンピューティングや、AI分野で注

目が高まりつつある、より高いエネルギー効率を実現する光コンピューティングが含まれる<sup>10</sup>。

量子コンピューティングが実用規模に達した場合、データセンターの設計要件は根本的に変化する可能性が高い<sup>11</sup>。量子システムは、冷却設備、高度なフォームファクター、極めて厳格なノイズおよび温度感度制御を必要とし、現在のAIインフラとは大きく異なる要件を持つ。

こうしたハイブリッドアーキテクチャーを運用するためには、新たな専門性と管理ツールが不可欠となる。将来的なオーケストレーションレイヤーは、従来型のソリューションに代わり、AIワークロードに特化して設計されたプラットフォームへと置き換わる可能性がある。それらのシステムは、従来の仮想マシンやコンテナだけでなく、

量子プロセッサ、ニューロモーフィックチップ、光コンピューティングアレイといった多様な計算資源を統合的に管理することになる。

## 人材変革に求められる要件

インフラ変革は、IT組織全体におけるリスクリングを必要とする可能性が高い。データセンターチームは、従来のサーバー管理から、AIに最適化されたインフラ運用、GPUクラスター管理、高帯域ネットワーク、専用冷却システムの運用へと移行していくことが求められる。

ネットワークアーキテクトは、従来のエンタープライズネットワークとは本質的に異なる、AIファーストのトラフィックパターンおよび高スループット要件を前提とした設計という課題に直面する。GPU間通信、大容量データ転送、超低レイテンシーといったAI特有のネットワーク要件は、多くの組織が十分に備えていない専門性を必要とする。

コストエンジニアには、ハイブリッドなコンピュートポートフォリオ最適化に関する専門性が求められる。単なるクラウド経済性の理解にとどまらず、インフラ方式ごとの複雑なトレードオフを把握する必要がある。これには、GPUの稼働率、推論経済性、ハイブリッドコスト構造を考慮した新たな財務モデルの習得が含まれる。

長年にわたるクラウド移行の結果、社内のデータセンター関連スキルが失われ、多くの組織ではAIインフラ要件を理解する人材の確保が困難になっている。この人材ギャップは、特に全面的にクラウドへ移行した組織にとっては大きな課題である一方、人材育成に投資する意思を持つ組織にとっては機会ともなり得る。

## AIインフラを管理するAIエージェント

AIインフラの複雑さが増すにつれ、従来型のIT運用ブロックは、AIワークロードが求める動的な最適化には不十分になりつつある。その結果、アラートの要約、原因仮説の提示、是正策の提案を行う、IT運用向けに設計されたカスタムAIコパイロットの登場が進んでいる<sup>12</sup>。

これらのエージェントは、キャパシティプランニングやベンダー選定の領域にも拡張されつつある。例えば、Amazon Web Servicesでは、キャパシティ予約を自動分析し、Amazon Bedrockエージェントを通じて推奨アクションを提示するAIパターンが公開されている<sup>13</sup>。これは、モデル選択、インスタンスタイプの最適化、ス

ロット価格とリザーブ価格の使い分け、さらにはマルチクラウドにおけるコストおよびカーボン最適化を動的に制御する、完全自律型エージェントへの前段階と位置づけられる。

調達プロセスもまた、定期的かつ手動的なものから、アルゴリズム主導で継続的に行われる形へと変化しつつある。今後、組織は、ワークロード需要・コスト変動・性能要件に基づき、リアルタイムでインフラに関する意思決定を行う主体として、AIエージェントへの依存を一層強めていくことになる。

## サステナブルなデータセンターのイノベーション

AIインフラが環境に与える影響の拡大を背景に、サステナブルなコンピューティングアプローチに関するイノベーションが進んでいる。政府および民間セクターでは、カーボン排出を伴わずにデータセンターへ電力供給を行う手段として原子力の活用が検討されているが、現時点での実装は、ハイパースケーラーや多額の資本を有する組織に限定されている。

マイクロソフトのProject Natickは、海水をヒートシンクとして利用する水中データセンターコンテナが、実用的かつ信頼性の高い計算基盤となり得ることを示した。ただし、同社は概念実証フェーズの完了をもって研究プログラムを終了した<sup>14</sup>。一方で、中国の海洋機器メーカーであるHighlanderは、商用の水中データセンターモジュールをすでに展開しており、政府の正式な支援のもとで事業拡大を進めている<sup>15</sup>。

再生可能エネルギーとの統合も加速している。テキサス州で計画されているData Cityのようなプロジェクトでは、将来的な水素エネルギーの統合も見据え、完全再生可能エネルギーによるデータセンター運営が構想されている<sup>16</sup>。これらの取り組みは、サステナブルなコンピューティングインフラに向けたより大きな潮流を示している。

さらに、新たな概念として、太陽光発電で稼働し、発生した熱を直接宇宙空間へ放射することで冷却水を一切必要としない軌道上データセンターも検討されている。Sophia SpaceやLonestarなどの企業が軌道上コンピューティングの開発を進めており、月面データセンター向けペイロードの初期飛行試験に成功した例もあるものの、実用化にはなお数年を要する<sup>17</sup>。

## コンピューテーション・ルネサンス：戦略的差別化要因としてのAIインフラ

このインフラ変革を成功裏に乗り越える組織は、AIの展開と運用において持続可能な競争上の優位性を得る可能性が高い。一方で、変化に適応できない組織は、AIが事業運営の中核を占めるにつれて、コストの増大、性能上の制約、さらには戦略的な脆弱性に直面することになる。

このAIインフラの変革は、一時的な市場調整にとどまるのではなく、組織が計算資源と向き合う姿勢そのものを

を根本から変える構造的転換である。過去10年にわたりクラウドコンピューティングがIT戦略を再定義してきたのと同様に、今後10年においては、ハイブリッドAIインフラがテクノロジーに関する意思決定の軸となる可能性が高い。

コンピューテーション・ルネサンスはすでに始まっており、その帰結が、AI主導のビジネス環境においてどの組織が成功するのかを左右することになる。

## Endnotes

1. Stanford Institute for Human-Centered AI, “The 2025 AI index report,” Stanford University, accessed Nov. 12, 2025.
2. Sarah Wang, Shangda Xu, Justin Kahl, and Tugce Erten, “How 100 enterprise CIOs are building and buying gen AI in 2025,” Andreessen Horowitz, June 10, 2025.
3. Chris Thomas, Akash Tayal, Duncan Stewart, Diana Kearns-Manolatos, and Iram Parveen, “Is your organization’s infrastructure ready for the new hybrid cloud?” *Deloitte Insights*, June 30, 2025.
4. Thomas, Tayal, Stewart, Kearns-Manolatos, and Parveen, “Is your organization’s infrastructure ready for the new hybrid cloud?”
5. Exasol, “The rise of cloud repatriation,” Nov. 6, 2024.
6. “A new asset class for Danish RE investment firm: AI-ready, sustainable data centers,” *Deloitte Insights*, Dec. 5, 2025.
7. David Linthicum (former chief cloud strategy officer, Deloitte) interview with Deloitte, Sept. 8, 2025.
8. John Roesse (chief technology officer and chief AI officer, Dell Technologies), interview with Deloitte, Sept. 29, 2025.
9. National Institute of Standards and Technology, “Introduction to neuromorphic computing, why is it so efficient for pattern recognition, and why it needs nanotechnology,” accessed Nov. 12, 2025.
10. Kazuhiro Gomi, “Optical computing: What it is, and why it matters,” *Forbes*, Sept. 10, 2024.
11. Christopher Tozzi, “Assessing the state of quantum data centers: Promises vs. reality,” *Data Center Knowledge*, Feb. 8, 2024.
12. ServiceNow, “Now Assist for IT operations management (ITOM),” Jan. 30, 2025.
13. Ankush Goyal, Salman Ahmed, Sergio Barraza, and Ravi Kumar, “Optimizing ODCR usage through AI-powered capacity insights,” Amazon Web Services, June 5, 2025.
14. Sebastian Moss, “Microsoft confirms Project Natick underwater data center is no more,” *Data Centre Dynamics*, June 17, 2024.
15. Peter Judge, “China’s Highlander completes first commercial underwater data center, looks for exports,” *Data Centre Dynamics*, April 4, 2023.
16. *Fuel Cells Works*, “Energy Abundance unveils Data City, Texas — World’s largest 24/7 green-powered data center hub with future hydrogen integration,” March 24, 2025.
17. Mandala Space Ventures, “Mandala Space Ventures launches Sophia Space: The world’s first scalable data center in space,” May 19, 2025; Lonestar Data Holdings, “Lunar data center achieves first success en route to the moon,” PR Newswire, March 5, 2025.

---

# About the authors

## Nicholas Merizzi

nmerizzi@deloitte.com

Nicholas Merizzi is a principal at Deloitte Consulting LLP and a recognized leader in digital transformation. He is Deloitte's Silicon2Service and AI Infrastructure leader, where he works with organizations to accelerate technology modernization, unlock cloud potential, and integrate AI-driven solutions. Merizzi blends deep infrastructure experience with strategic vision and cloud innovation, guiding clients through the complexities of digital change to achieve their technology goals.

## Chris Thomas

chrthomas@deloitte.com

Chris Thomas is a principal in Deloitte Consulting LLP and the US Hybrid Cloud Infrastructure leader. He has over 25 years of strategy consulting and hands-on cloud transformation experience across industries to lead Deloitte's US AI & Engineering business offering for hybrid cloud infrastructure to help clients optimize hybrid cloud strategies and build future-ready organizations. He has extensive experience working with senior executives to enable business outcomes through cloud-centric operating models, large-scale technology transformations, strategic cost optimizations, global outsourcing programs, and workforce of the future initiatives.

## Ed Burns

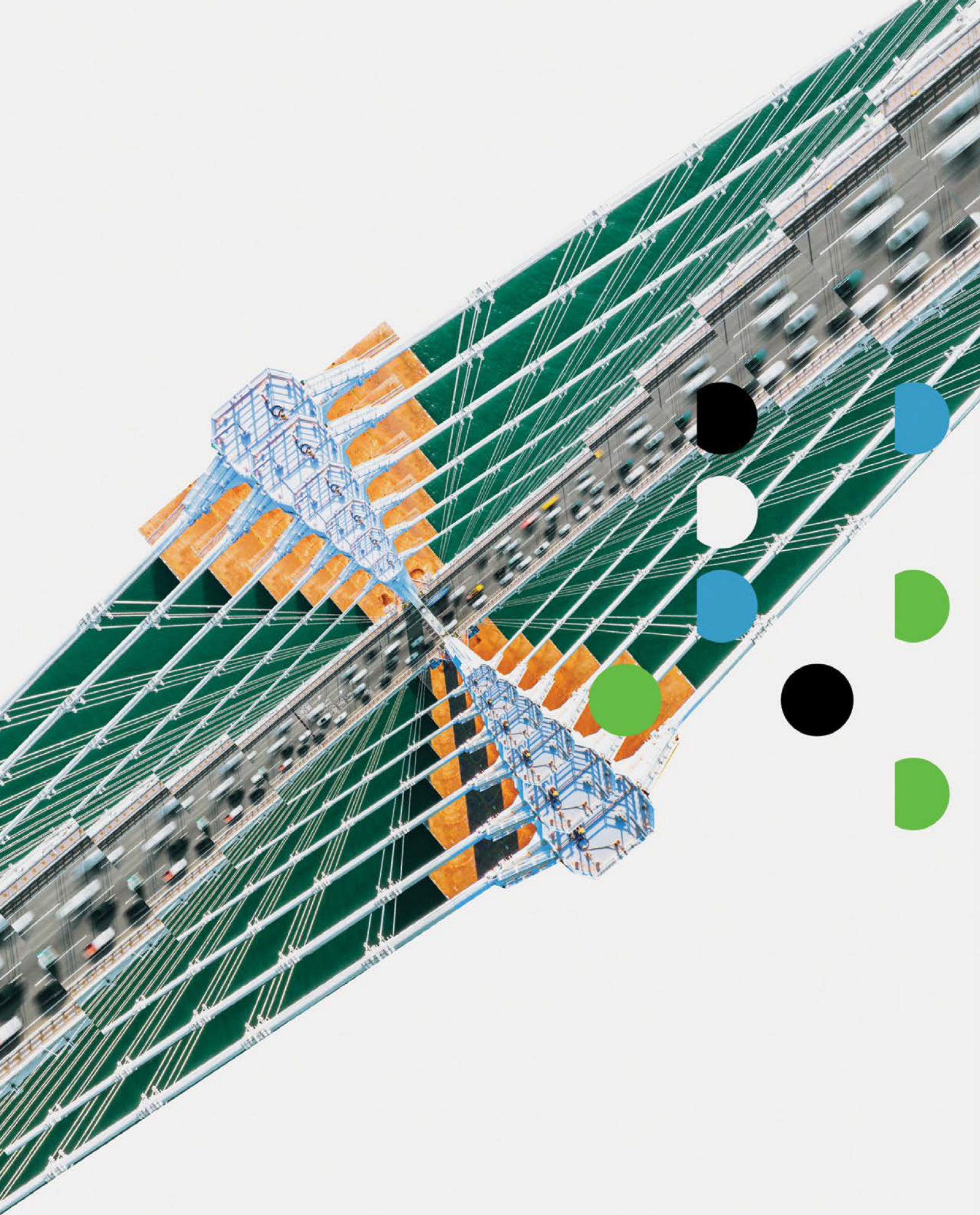
edburns@deloitte.com

Ed Burns leads the client stories initiative within the Office of the CTO known as Trend Lines. This project serves as a key research input to Tech Trends and other eminence. Prior to his current role, he led a tech news publication that covered all things AI, analytics, and data management.

---

# Acknowledgments

Much gratitude goes to the many subject matter leaders across Deloitte who contributed to our research for this chapter: **Bernhard Lorentz, Baris Sarer, Duncan Stewart, and Rohit Tandon.**





# テクノロジー組織の再構築: AIネイティブなテクノロジー組織の設計

未来のテクノロジー組織を定義するものとは何か、リーダーは今日からどのようにその構築を始めるべきか。

Lou DiLorenzo, Jr., Anjali Shaikh, Michael Caplan, and Erika Maguire

**テ**クノロジーが段階的に変化する時代は終わった。わずか数年で、人工知能はタスクの自動化から、テクノロジー組織の構造自体を解体・再構築する段階へと飛躍した<sup>1</sup>。デロイトの2025年 Horizon Architecture Surveyによると、テクノロジーリーダーの78%が、今後5年間で、AIエージェントがアーキテクチャーのワークフローに幅広く、または部分的に、あるいは変革的な形で統合されると予測している<sup>2</sup>。

これは単なるツールの入れ替えや人員数の変化以上のものである。AIは、テクノロジーチームの構成・ガバナンス・リーダーシップのあり方を再設計している。未来のモデルは、よりリーンで、より速く、アーキテクチャーからデリバリーに至るあらゆる層にAIが組み込まれ、テクノロジー組織を継続的に学習し最適化するダイナミックなエンジンへと変貌させるであろう。

「エージェントと人間は、仕事の進め方という点で間もなく完全に統合されるだろう。その統合は多くの企業の準備を上回る速さで起こりうる。「一度作ったら終わり」の時代は終わった。企業は、継続的なロードマッピングと反復改善を習得する必要がある<sup>3</sup>と、Modernaの最高人事・デジタル技術責任者であるTracey Franklinは述べている。

AI主導の世界に向けてテクノロジー組織を構築するための決定的な青写真はないが、進むべき道は見え始めている。未来のハイパフォーマーは、AIに歩調を合わせるだけでなく、AIを推進力として全く新しい領域へと進出するだろう。今日、すべてのリーダーにとっての問いは、AIがテクノロジー組織を変革するかどうかではなく、いかに迅速にAIの潜在能力を最大限引き出せるかである。

## AIはテクノロジー組織をどのように再構築しているか

デロイトのTech Spending Outlookによると、調査対象組織の64%が今後2年間<sup>4</sup>でAIへの投資を増やす計画である。これは、AIが企業全体にもたらしうる大きな価値と変革の可能性を、リーダーが認識している明確な兆候である。ほとんどの組織が生成AIとエージェントAIの探索段階にあることを認めつつ（図1）、データは、AIが優先事項、人材、そして目的に至るまで、多くの点でテクノロジー組織を再構築していることを示している。

**優先事項** デロイトの2025年Tech Executive Surveyにおいて、CIO（Chief Information Officer、最高情報責任者）が最も時間とエネルギーを費やしている分野として、AI・データ・アナリティクスの潜在能力の最大活用が挙げられた<sup>5</sup>。これまで多くの経営幹部にとってAIは最優先事項であったが、生成AIとエージェントAIの登場により、AIはテクノロジー組織の最重要課題となり、それに応じて投資が行われている。テクノロジー予算に占めるAIの割合は、今後2年間で平均8%から13%へと大幅に上昇すると予想されており、AIが実験段階からコア戦略へと移行していることを浮き彫りにしている<sup>6</sup>。

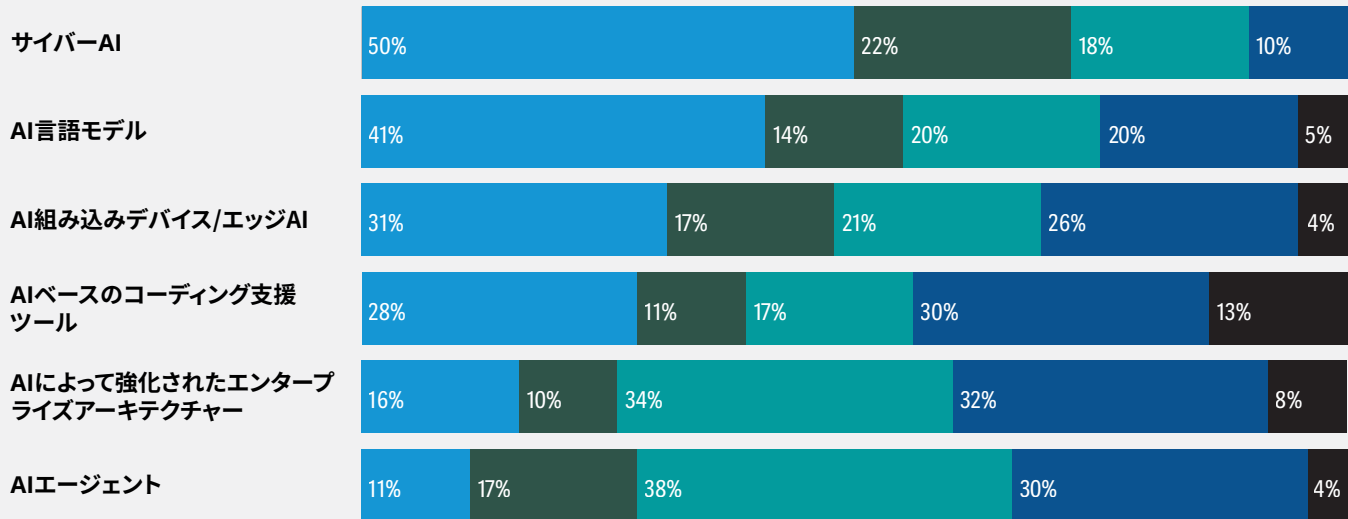
**人材** 同調査において、テクノロジーリーダーの70%近くが、生成AI<sup>7</sup>への直接的な対応としてチームを増強する計画を立てている。これは雇用喪失への懸念から、人材の増強と専門化という戦略への明確な転換を示している。AIの継続的な勢いは、Modernaの最高人事・デジタル技術責任者や前線配置エンジニアといった新しい役職を生み出すとともに、他の役職の存在感も高めている<sup>8</sup>。例えば、AIアーキテクトの役職数は、現在の30%から今後2年間で58%へと、ほぼ倍増すると予想されている<sup>9</sup>。AIは新しい働き方を推進しており、

図1

## 組織はまだAI技術を試験的に導入している段階だが、広範な実験のトレンドは、テクノロジー機能を再設計する強い勢いを示している

Q: 「以下の各テクノロジーについて、貴組織の現在の導入段階はどれか」

● 積極的に使用中 ● 導入間近 ● ソリューションを試験運用中 ● 選択肢を検討中 ● 検討していない



注：四捨五入のため、合計が100%にならない場合がある。

出所：Deloitte 2025 Emerging Technology Trends in the Enterprise Survey. Deloitte conducted an online survey of 500 US technology leaders between June and July 2025 to quantify the prevalence, engagement, and perceptions surrounding the adoption of emerging technologies across industries.

もはや「プラグアンドプレイ」のツールではなく、周到な設計・統合・ガバナンスを要するテクノロジーであり、専門的な知見を必要とする。

**目的** AIがCEOの現在および将来の戦略において重要な役割を果たすにつれて<sup>10</sup>、テクノロジー組織の使命は変化している。今日のCEOは、テクノロジーリーダーに対して、単なるITの運用ではなく、ビジネス戦略の推進を期待している。デロイトのTech Executive Surveyによると、多くの大企業（66%）が自社のテクノロジー組織をサービスセンターではなく収益創出源と見なしており、デロイトのTech Spending Outlookでテクノロジー組織がビジネスを形成する上での役割を尋ねたところ、最も多かった回答は「戦略的リーダー：テクノロジーに重点を置いて全体的なビジネス

戦略を実現する」であった<sup>11</sup>。CEOに直接レポートするCIOの数が増加していること（2025年<sup>12</sup>の65%に対し、2015年<sup>13</sup>には41%）は、テクノロジーとAIが単なる運用上の懸念事項ではなく、成長、イノベーション、そして競争力の中心であることをさらに示している。テクノロジー組織の目的は、「現状維持（keep the lights on）」から「未来への道を照らす（light the way forward）」ことへと拡大している。

### AI主導の未来に備えるための戦略

AIの勢いが増すにつれ、組織は自社のテクノロジーオペレーティングモデルを積極的に見直している。実際、進化するビジネスニーズに応えるためにテクノロジーオ

ペレーティングモデルをどのように変化させているかを尋ねたところ、調査対象のIT意思決定者のうち、「大きな変更はない」と回答したのはわずか1%であった<sup>14</sup>。

AI主導の未来に備えるための道のりは、組織の成熟度や優先事項などの要因によって異なるが、AIと自動化の導入を増やすことから始まる可能性が高い。その先で、組織が今日、AI主導の未来に向けてどのように計画しているかは以下のとおりである。

### モダナイゼーションはテクノロジーではなく、ビジネス課題から始まる

調査対象組織の71%が現在、AI導入をサポートするためにコアインフラをモダナイズしており、23%が年間収益の6%から10%をコアエンタープライズシステムのモダナイゼーションに投資している<sup>15</sup>。しかし、認識だけでは不十分である。重要なのは、単にテクノロジーをアップグレードするのではなく、実際のビジネス課題を解決することである。

「モダナイゼーションはテクノロジーのためのテクノロジーではなく、コスト、市場投入の問題など、根本的なビジネス課題に対処することである」と、BroadcomのCIOであるAlan Davidsonは言う。「AIは良い例。テクノロジーは非常に速いペースで進化しているため、今日AIについて行われている会話は6ヶ月前のものとは大きく異なる。したがって、戦術的な計画を持つことが重要である。特定のビジネス課題とそこから得たい価値に焦点を当てなければ、AIに投資してもリターンが得られないということになりかねない」<sup>16</sup>

### モジュール性とオブザーバビリティのために設計されたアーキテクチャー

AI主導で将来に対応できる企業は、継ぎはぎのレガシープラットフォーム上には構築できない。これが、調査対象組織の66%がAIで強化されたエンタープライズアーキテクチャーの試験的な導入や検討をしている理由だろう<sup>17</sup>。新しいテクノロジーを全社end-to-endの視点と組み合わせて活用すると、より大きな価値を生み出せる。新しいアーキテクチャーは、モジュール性とオブザーバビリティに対応する形で設計可能である<sup>18</sup>。オブザーバビリティの本質とは、システムの外部出力を分析することでシステムを可視化し、理解し、最適化する能力にある。

「Western Digitalでは、当社の技術環境を全体的に

管理するためのオブザーバビリティアーキテクチャーを開発している。我々は完璧なAIソリューションを待つのではなく、潮流を逃さないよう小規模なパイロットで早く失敗する方がましである」と、Western DigitalのCIOであるSesh Tirumalaは語る<sup>19</sup>。

The Coca-Cola Companyもモジュール型のアプローチを優先している。「グローバル企業にとって、一つの方がすべてに当てはまることは稀である。世界各地で働き方は同じではない。当社は、必要に応じてローカライズしながら迅速に動けるアジャイルチームに支えられ、モジュール型アーキテクチャーと指針となる基本原則を構築する、という方針を取ってきた」と、シニアバイスプレジデント兼CIOのNeeraj Tolmareは言う<sup>20</sup>。

### テクノロジー人材戦略の中心にある人間と機械のコラボレーション

最近のデロイトの調査は、テクノロジー人材ランドスケープの急速な進化を浮き彫りにしている。組織が新しいテクノロジーを導入するにつれて、最も期待される新しい役割には以下が含まれる。

- **人間とAIのコラボレーションデザイナー:**人間とインテリジェントシステム間のシームレスなインタラクションを設計する責任を負う
- **エッジAIおよび組み込みシステムエンジニア:**AI機能をデバイスや接続されたインフラに直接もたらす
- **合成データのためのデータ品質スペシャリスト:**AIシステムを動かすトレーニングデータが信頼でき、代表的であることを保証する
- **AIプロンプトエンジニアおよびモデルトレーナー:**AIの出力を最適化し、特定のビジネスニーズに合わせてモデルを調整する<sup>21</sup>

AIを実際に機能させるためには、AIがスキルアップのエンジンであり、知識のギャップを埋めるツールでもあることを考慮する必要がある。「たとえJavaScriptのエキスパートやプロダクトマネージャーのエキスパートでなくても、AIはそのギャップを埋める、あるいはそのギャップを完全に埋めるのに役立つ」と、研究者であり、The Phoenix Projectおよび新刊Vibe Codingの共著者であるGene Kimは言う<sup>22</sup>。組織がテクノロジー人材戦略を再考する際、AIができることを踏まえて、チームにどの程度の機能的専門知識が必要かを考える

ことが役立つ、と彼は付け加える。それは、スキルアップやリスクリングの取り組みにどこに焦点を当てるべきかを明らかにするのに役立つ。

AIは能力と専門知識を民主化することができるが、未来の競争優位性は、単にAIツールを導入することからではなく、人間と機械が協力する方法を設計、管理、進化させることができるチームを構築することから生まれる可能性が高い。未来は人間か機械かではなく、人間と機械なのである<sup>23</sup>。

### 新たなリスクを管理しつつ、スピードを可能にするガバナンス

これは容易なことではないが、航空宇宙・防衛企業RTXの最高デジタル責任者兼エンタープライズサービ

ス部門のリーダーであるVince Campisiは、AI時代におけるガバナンスを適応させるための自身の戦略を共有している。「ガバナンスを3つのM、すなわちマップ(map)、メジャー(measure)、モニター(monitor)に分解する。これは、チームが進捗を把握するために活動をマッピングし、望む成果を達成しているかを確認するために結果を測定し、当初の目標が実現されているかを確認するために品質を監視できることを意味する。次に、戦略的意図との整合性を維持するために設計された戦術に焦点を当てる。AIがよりエージェント的になるにつれて、組織はリーダーシップの意図から始まり、人間が結果を検証し信頼できるように説明可能性と監査可能性を組み込んだガバナンスを確立することができる」<sup>24</sup>

## VIBE SHIFT: GENE KIMが語る、エンタープライズITにおけるAIを活用したコーディング

Gene Kimは、ハイパフォーマンスなテクノロジー組織を研究する研究者であり、*Wall Street Journal*のベストセラー作家である。元CTOであるKimは、毎年開催されるEnterprise Technology Leadership Summitの主催者である。彼の著書は100万部以上を売り上げている。彼の最新刊であるVibe Codingは、Steve Yeggeとの共著である。

### Q: AIコーディングツールは、エンタープライズITの状況をどのように変えているか

**A:** AIは、私が「自律的」チームと呼ぶものを生み出している。そこでは、AIがギャップを埋めたり補ったりするのに役立つため、必ずしもすべての分野で深い機能的専門知識が必要というわけではない。あなたはデータベースのエキスパートでも、ビジネスのエキスパートでも、プロダクトマネージャーでもないかもしれないが、AIはこれらのドメインを横断してより独立して作業するのに役立つ。

営業、マーケティング、顧客サポートなど、あらゆるビジネスドメインのエキスパートが開発者と組むことで、多くの監督なしに素晴らしいことを成し遂げられるようになった。あるシニアテクノロジーリーダーは私にこう言った。「私はキャリアの20年間、成果が不十

分で、遅れ、約束を守れないと言われ続けてきた。今ではその逆だ。常に速すぎると言われ、減速する必要があると言われていた。それは我々全員が目指したい場所である。

### Q: ITリーダーは、単に「AIでコーディングを学べ」と言うだけでなく、チームをどのように準備させるべきか

**A:** 最も成功を収めているのは、多くの場合、よりシニアで技術志向のリーダーであり、彼らは限界を理解しつつも可能性を見出している。リーダーとして、時間は貯蔵も創造もできないのだから、時間を節約できるものがあればそれを使わなければならないというトーンを設定する必要がある。

興味深いことに、多くのシニアエンジニアは実際にAIコーディングツールに反発している。テクノロジーはまだ未熟で予測不可能であるため、古典的に訓練されたコーダーの多くは、自分たちが訓練された方法の方が優れていると考えて抵抗している。ツールが未熟であるからこそ、トレーニングが必要なのである。一度や二度試して諦めるわけにはいかない。ある程度の理論と、それらが内部でどのように機能するかを理解する必要がある。

AI支援ソフトウェア開発の現状に関する最近のレポートから得られた一つの重要な洞察が心に残っている。AIへの信頼は、使用頻度と期間に直接関連する。これらのツールを使えば使うほど、その癖や限界をよりよく理解できるようになる。より大きな問題を任せようになり、そこに大きな見返りがあるのだ。

### Q: この移行に直面しているCIOやITリーダーへのアドバイスは何か

**A:** 価値を見出すことに抵抗し、取り残されるリスクのあるシニアエンジニアを助ける上で、リーダーシップは極めて重要となるだろう。全体的に採用は減少しているが、行われている採用はAIを使用する開発者を優遇する可能性が高い。経済的な観点から見れば、すべての行を手で書くことに固執する人よりも、AIを活用して仕事を加速させる人を選ぶだろう。

リーダーはまた、誰が生産性余剰を獲得するかを決定する上で重要な役割を果たす。AIが公に議論されなければ、人々は1日の仕事を1時間で終えて誰にも言わないかもしれない。しかし、AIの実践が共有される文化では、そのエンジニアは「5日分の仕事を1時間で終えた。これがその方法だ」と言うかもしれない。

## VIBE SHIFT: GENE KIMが語る、エンタープライズITにおけるAIを活用したコーディング

い。その知識共有の価値は、節約された時間をはるかに上回り、組織がその利益を獲得するのである。

**Q: エンタープライズITでAIに関して起こっていることについて、何かホットな見解はあるか**

**A: 主流ではないかもしれない2つの点がある。第一に、手作業によるコーディングの時代**

は終わりつつあると私は信じている。誰も私を説得することはできない。

第二に、私はAIがこれ以上良くなるかどうかはあまり気にしていない。たとえAIのパフォーマンスが現在のレベルで凍結したとしても、私は非常に感謝するだろう。既存のAIから得られるレバレッジはすでに奇跡的である。それが有用であるために大きな進歩は必要ない。す

でに有用なのである。つまり、ソフトウェアエンジニアやリーダーが待つ理由はない。今すぐ飛び込むべきだ。

### 漸進的な変化よりも再創造を優先する大胆な野心

テクノロジー組織の変革には、一連の小さく安全なステップ以上のものが求められる。それは、何が可能かを再創造する勇気あるビジョンを必要とする。大胆な野心を掲げる組織は、戦術的な自動化をはるかに超えてAIを活用し、テクノロジー・人材・戦略が交差する方法を根本的に再構築する。

「永続的な概念実証のサイクルに行き詰まるのではなく、最大の問題に取り組み、大きな成果を目指すことを検討すべきだ」と、UiPathのCEO兼執行会長であるDaniel Dinesは言う。「大きな成功を手に入れば、ビジネスプロセスを再考する機会だけでなく、生産性向上の可能性や新たな収益源を発見する機会があることを証明できる。早く始めれば始めるほど、それらの目標に向けた道のりにおいて、より良いポジションを築くことができる」<sup>25</sup>

### CIOの役割の再定義

AIが定着するにつれて、CIOの使命はテクノロジーストラテジストからAIエバンジェリストへと拡大している。実際、Tech Executive Surveyに参加したCIOの70%が、自組織における生成AIに関する主な役割は、企業全体への生成AIの実装か、チームにテクノロジーの可能性を理解させるエバンジェリストとしての役割のいずれかであると述べている<sup>26</sup>。AI対応の機能が組織全体に組み込まれ、ITの集中化が緩和されるにつれて、CIOはインフラの所有者ではなく、オーケストレーター兼インテグレーターとなる。実際、CIOのほぼ3分の1が、今後18ヶ月間で中間のテクノロジーリーダーを調整することが不可欠であると述べている<sup>27</sup>。この役割は現在、ビジネス戦略と全社的な変革とのより深い統合を必要とし、CIOをチェンジエージェントであると同時に責任あるゲートキーパーにしている。

「かつてCIOは、SaaSや他のアプリケーションが効果的に連携することを確認することが任務の多くを占めていたため、最高統合責任者のようであった。今日、私は自分の役割を、従来のCIOに加えて、最高データ責任者・最高AI責任者・最高デジタル責任者を組み合わせたものだと考えている」と、Western DigitalのTirumalaは付け加える。「この時代は、テクノロジーリーダーがステップアップする機会である。我々はテクノロジー、データ、そしてプロセスを理解している。許可を待つのではなく、パートナーとして積極的に関与すべきだ。強力なデジタルへの野心を明確にし、トップラインの成長とビジネスモデルの転換を可能にするロードマップを、リスク管理戦略とともに策定する。スピード、アジリティ、成果、そして価値に焦点を当てる。正しいアプローチをとれば、後で許しを請う必要はなくなるだろう」<sup>28</sup>

### AIを活用したテクノロジー組織の指標

企業ごとにAI導入の歩みは異なるが、AIを活用して成功するテクノロジー組織には共通の特徴がある。ここで示す指標は、AI主導の時代に成果を上げるテクノロジー組織の新しい標準である。

### コアコラボレーターとしてのAI

未来のテクノロジーオペレーティングモデルは、AIを単なるアドオンツールや効率化策から、意思決定やオペレーション、製品開発に至るまで、あらゆる層に組み込まれたコラボレーターへと昇華させる。共同制作者としてのAIは、ロードマッピングを加速し、フィードバックループを自動化し、リアルタイムで作業の優先順位を見直すことができる。クラウドやモバイルがもたらした変革と同様に、このシフトはAIを競争優位性の厳選となる次のコア能力として位置づけられる。

このビジョンの実現には、クラウドネイティブなプラットフォーム型の基盤が不可欠である。Tech Spending Outlookの調査では、48%の組織が、テクノロジーをビジネスニーズにより良く整合させるために、クラウドネイティブとDevOpsの実践を拡大していると回答した<sup>29</sup>。クラウドはもはや単なるインフラではなく、スピード・柔軟性・イノベーションのエンジンである。モジュール化され、APIファーストのセルフサービス型プラットフォームは、インフラのオーバーヘッドを抑えながら迅速なスケーリングを可能にする。プラットフォームエンジニアリングとオーケストレーションは、製品ライン全体で一貫性、ガバナンス、再利用を保証する。このモデルでは、テクノロジー組織はエンタープライズAIのアーキテクトとなり、標準化され、安全で、スケーラブルなビルディングブロックを提供することで、チームが自信を持って一貫してAIを導入できるようにする。

### スピードのために再創造された仕事

今後数年間で、従来のプロジェクトチームは、製品やバリューチェーンに沿ったリーンで部門横断的なチームへと移行する可能性が高い。これにより、コンセプトから顧客へのループが短縮され、成果へのオーナーシップが組織に組み込まれる。すでに57%の組織が、ビジネスとITをより緊密にするため、プロジェクトからプロダクトへのモデルに移行していると報告されている<sup>30</sup>。このモデルでは、プロダクトラインが共有の顧客向けプラットフォームを介してユーザー中心の機能を提供し、アジャイルポッドは働き方やツール選定を管理し、フロントラインエンジニアはプロダクトチームや顧客側のチームと並行して価値創出までの道のりを短縮する<sup>31</sup>。その結果、より強いオーナーシップ、より速いイテレーション、そして現実世界への影響に対するより明確な見通しが生まれる。

AI・コグニティブツール・ロボティクスは、継続的な計画・デリバリー・実験を日常業務に組み込むことで、この構造を増幅できる。予測モデルとスマートオートメーションは手動の引き継ぎを置き換え、AI Opsリードのような新たな役割が登場するにつれて、従来型のプロジェクト管理の比重は低下していく。組織のアジリティはIT部門を超えて拡大し、チームレベルのスピードと説明責任を維持しながら、変化する優先順位に継続的に適応するオペレーティングモデルが形成される。

### 大規模な人間とエージェントのチーム

未来の労働力は、人間の創意工夫と機械の知能を融合させる。組織の3分の2が、AIエージェントを試験的に導入、積極的に使用、または導入間近である<sup>32</sup>。これらの未来のチームは、人間・AIエージェント・オーケストレーターがシームレスに融合したものになる可能性が

高い。そこでは、人間が創造性・監督・倫理的判断を提供し、AIがスピード・精度・パターン認識をもたらす。このモデルは、製品・サービス・オペレーション全体で、継続的な実験、迅速なプロトタイプング、スケーラブルなイノベーションを促進する。AIエージェントがより複雑なタスクを担うにつれて、デジタルフルエンシーはすべての役割にとってのコアスキルとなる。テクノロジー組織の将来の成功の鍵は、このコラボレーションを適切に調整し、人間と機械が共に学び、進化し続けられるようにすることにある。

### 組み込み型ガバナンス

現代のテクノロジー組織は、遅く、ポイントインタイムの監督を、適応的なガバナンスサイクルへと置き換えている。これは、安全性を犠牲にすることなくスピードを確保する、継続的でAI支援のメカニズムである。予測モデルとリアルタイムのシグナルは、意思決定を主観的な推測から、客観的で事実に基づく選択へと変革し、リスクをエスカレートする前に顕在化させ、状況が変化に応じて優先順位を示す。ポリシー・プロセス・コントロールは、生きた資産となり、コード化され、自動的に監視され、新技術の進化に追従するため短いサイクルで反復される。これにより、コンプライアンス・セキュリティ・倫理が、後付けではなく、仕事の流れに組み込まれる。これを大規模に実現するには、リーダー間の強力な協働が必要である。AIの成果は、サイロ化されたイノベーションからは生まれにくい。CIO、最高財務責任者(CFO)、最高戦略責任者(CSO)が三位一体の体制として機能し、ビジョン・実行・価値実現のバランスをとるときに効果が最大化される。このダイナミクスにおいて、CIOはテクノロジー統合を推進し、CFOは投資が測定可能なROIをもたらすことを保証し、CSOは戦略を企業の優先事項と整合させる<sup>33</sup>。彼らは共に、イノベーションとビジネス成果の間の結合組織を創造し、AIの成功が先進技術と同じく共有されたリーダーシップにかかっていることを示している。

### エコシステムのオーケストレーション

テクノロジー組織は、サービスプロバイダーからエコシステムオーケストレーターへと進化し、スタートアップ・ハイバースケーラー・規制当局・学界と連携してイノベーションを加速させる可能性が高い。デジタル能力が企業全体に拡散し、テクノロジーに精通した役割が標準となるにつれて、ITとビジネスの境界は溶解していくかもしれない。今後数年間で、企業は流動的なイノベーションネットワークで活動し、賭けのポートフォリオを運営し、うまくいくものに基づいて構築していく可能性が高い。成功は、すべてのテクノロジーを自社で所有することよりも、継続的に実験し、「早く失敗し、より速く学ぶ」文化を受け入れる適応的なエコシステムを調整することに依存するようになるだろう。

## 継続的な進化：設計による常時ベータ版

未来のテクノロジー組織の決定的な特徴は、永続的な進化であり、変化を一度きりのイベントではなく、コア能力として組み込む。適応性と常時ベータ版という考え方を構造・文化・戦略に組み込むことで、活用するテクノロジーの進化速度に合わせて学習する組織を創造する。

「これまでやってきたやり方が、明日も同じやり方である必要はない」とKimは言う。「AIから得られるものはすべて今すぐ活用すべきだ。なぜなら、たとえばパフォーマンスレベルが凍結したとしても、AIが今日あなたの組織やチームのためにできることは、依然として奇跡的だからだ。待っている時間はない。今こそ飛び込む時だ」

## ライターからディレクターへ：STEVE YEGGEが語るソフトウェア開発者の変革

30年以上の業界経験を持つソフトウェアエンジニアであるSteve Yeggeは、*Vibe Coding*の共著者である。Yeggeは、十数種類の言語で100万行以上の本番コードを書き、それぞれ最大150人のチームを複数率いてきた。彼は現在、Sourcegraphのエンジニアとして、AIコーディングアシスタントに取り組んでいる。

### Q: AIコーディングはテクノロジー機能にどのような影響を与えているか

**A:** ITは階層的な活動である。我々は最下層であるコード生成の領域を担わなくなりつつある。タスクや役割は順次ハードウェアやソフトウェアに移管され、人間は上位のレイヤーへと押し上げられる。多くのエンジニアリング活動には、設計、ワークストリームの統合、チームの指導が含まれる。AIがコードを記述するようになったため、重心がその方向へシフトしている。

それはまた、非プログラマーがIT機能に参入していることを意味する。AIで共有アーティファクトを生成できるようになった結果、プロダクトマネージャーやUXデザイナーのような役割もコーディングに関与し始めている。ビジネスとITの間には、これまでになかった翻訳レイヤーが存在する。我々は、エンジニア・財務アナリスト・マーケティング担当者などで構成される小規模なチームがソフトウェアを作成している。

### Q: これはソフトウェアエンジニアの役割をどのように変えるか

**A:** すべてをAIに任せることはできない。最終

的には人間が見る必要がある。それは、従来はエンジニアのチームを統括していたテクニカルプログラマージャーのような役割であったが、今ではAIエージェント群を管理している。しかし、エージェントがすべてを解決できるわけではない。彼らは人間よりもはるかに速く作業できるが、我々の目標のスケールはさらに大きくなるだろう。我々がこれまでやりたくてもできなかったすべてのプロジェクトは、今や実行可能になるだろう。それにはAIに対する絶え間ないコース修正、ケア、そして指導が必要となる。

AIツールが高度化するにつれて、今後数年間でより多くの非プログラマーがこの監督を行えるようになるだろう。しかし、現時点では、プログラマーとその神経可塑性、つまり本質的にAIを指示するという全く新しい働き方に適応する能力が鍵を握っている。

### Q: この環境で開発者の生産性をどのように測定するか

**A:** 2022年にAIを活用したコード補完が登場して以来、企業はこれを解明しようと試みてきた。コード補完では、AIがあなたの記述中のコード行を自動補完し、あなたはそれを受け入れるか無視するかを選択するため、生産性の指標は受入率であった。ところが、チャットベースのコーディングツールが登場すると、その生産性の尺度はほぼ一夜にして意味を失った。今ではチャットでリクエストするだけで、AIがコードを書き、それをコピー＆ペーストすればよく、改善が単純な受入率よりも多様で文脈依存となったため、良い指標の特定が難しくなった。

今ではコーディングエージェントが登場し、AIはツールを用いてコードを実行し、結果を評価し、手でコピー＆ペーストを介さずに反復することができる。コーディングエージェントを使用する人々は、使用しない人々と比較して、コード行数、コミット数、実際のビジネス成果など。どの指標を選んでも10倍生産性が高い。コーディングエージェントを使用していない人々と比べて明らかに桁違いに大きい。企業はそれを測定しようとさえしない。結果として、業績評価の場で、同僚よりも10倍生産性の高い人とそうでない人をどのように比較するかという議論に発展する。

### Q: AI時代の開発者採用についての考えは

**A:** この分野への新規参入者にとっては厳しい時期だが、私の見解では、企業は過度に慎重になり、採用を抑制する傾向にある。その結果、次世代のプロダクトを構築して企業をそのカテゴリーのトップに押し上げる可能性のある、優秀なジュニアプログラマーの人材プール形成を妨げている。

適応性が高く、神経可塑性のある人々は常に必要とされてきたが、今ではこれまで以上に重要になっている。固定観念や過度な制約にとらわれない、つまり「Xはしない、Yはしない」と言わない人々を雇うべきである。彼らに投資し、育成し、組織として試行錯誤を許容し、そこから学ぶ柔軟性を与える。こうした取り組みを行う企業は、大きな成功を収めるだろう<sup>34</sup>。

---

# Endnotes

1. Kelly Raskovich et al., “IT, amplified: AI elevates the reach (and remit) of the tech function,” *Deloitte Insights*, Dec. 11, 2024.
2. Deloitte 2025 Horizon Architecture Survey. From June to July 2025, Deloitte conducted an online survey of 250 US technology leaders across industries to understand the state of technology architectures today and how different approaches drive business value. All respondents were leaders within their organization’s IT functions (director level and above) and were from commercial companies with US\$1 billion or more in annual revenue.
3. Tracey Franklin (chief people and digital technology officer, Moderna), interview with Deloitte, Sept. 26, 2025.
4. Deloitte Tech Spending Outlook. From June to July 2025, Deloitte conducted an online survey of 302 IT procurement leaders, heads of IT, and non-IT executives with technology spending oversight to understand how US enterprises in key industries are managing technology budgets, making spend decisions, measuring value delivered by technology investments, and planning scenarios based on market dynamics. All respondents were from organizations with US\$1 billion or more in annual revenue; 66% of surveyed organizations were publicly owned, and 34% were privately owned.
5. Deloitte US, “New Deloitte Tech Exec Survey spotlights a moment of reinvention for the tech C-suite as need for gen AI skills, cross-functional collaboration becomes critical,” June 17, 2025. From March to April 2025, Deloitte conducted an online survey of 622 US technology leaders across industries to understand how senior technology leadership roles and responsibilities are evolving, as well as key challenges and priorities for 2025 and beyond. Survey respondent titles included chief information officer (33%), chief technology officer (18%), chief data analytics officer (25%), and chief information security officer or equivalent (24%).
6. Deloitte Tech Spending Outlook.
7. Deloitte 2025 Tech Executive Survey.
8. Isabelle Bousquette, “Why Moderna merged its tech and HR departments,” *The Wall Street Journal*, May 12, 2025; Lee Chong Ming, “An OpenAI exec said the company is using a new engineering role to get big customers’ projects going fast,” *Business Insider*, July 23, 2025.
9. Deloitte 2025 Horizon Architecture Survey.
10. Benjamin Finzi, Brett Weinberg, and Elizabeth Molacek, “Spring 2025 *Fortune*/Deloitte CEO Survey,” Deloitte, May 15, 2025.
11. Deloitte US, “New Deloitte Survey shows tech execs driving growth, shaping strategy, and eyeing the CEO seat,” Deloitte Tech Spending Outlook.
12. Deloitte 2025 Tech Executive Survey.
13. Deloitte CIO Program, “Many tech leaders’ influence in the C-suite is growing, new Deloitte research suggests,” *Deloitte Insights*, Sept. 26, 2024.
14. Deloitte Tech Spending Outlook.
15. 2025 Deloitte Emerging Technology Trends in the Enterprise Survey.
16. Katherine Noyes, “Broadcom CIO: ‘Modernization should be driven by the business,’” *The Wall Street Journal*, Sept. 10, 2025.
17. 2025 Deloitte Emerging Technology Trends in the Enterprise Survey.
18. Michael Caplan et al., “The technology operating model of the future: Rise of the agentic enterprise,” *The Wall Street Journal*, Aug. 23, 2025.
19. Katherine Noyes, “Western Digital CIO: In the AI era, ‘play offense or get left behind,’” *The Wall Street Journal*, Sept. 6, 2025.
20. Katherine Noyes, “Coca-Cola CIO on scaling AI: From ‘what can we do?’ to ‘what should we do?’” *The Wall Street Journal*, Jan. 18, 2025.
21. 2025 Deloitte Emerging Technology Trends in the Enterprise Survey.
22. Gene Kim (researcher and coauthor of *The Phoenix Project* and the newly released book, *Vibe Coding*), interview with Deloitte, Sept 15, 2025.
23. Kyle Forrest, Brad Kreit, Abha Kulkarni, Roxana Corduneanu, and Sue Cantrell, “AI, demographic shifts, and agility: Preparing for the next workforce evolution,” *Deloitte Insights*, Aug. 25, 2025.
24. Katherine Noyes, “RTX CDO on AI: ‘Value beats volume every time,’” *The Wall Street Journal*, Sept. 13, 2025.
25. Katherine Noyes, “UiPath CEO: Agentic automation will ‘usher in a new era of work,’” *The Wall Street Journal*, Feb. 22, 2025.
26. Deloitte 2025 Tech Executive Survey.
27. Ibid.
28. Noyes, “Western Digital CIO: In the AI era, ‘play offense or get left behind.’”
29. Deloitte Tech Spending Outlook.
30. Ibid.
31. Gergely Orosz, “What are forward deployed engineers, and why are they so in demand?” *The Pragmatic Engineer*, Aug. 12, 2025.
32. 2025 Deloitte Emerging Technology Trends in the Enterprise Survey.
33. Lou DiLorenzo et al., “AI’s ROI triumvirate: CIO, CFO, and chief strategy officer,” *The Wall Street Journal*, May 10, 2025.
34. Steve Yegge (coauthor of *Vibe Coding* and software engineer, Sourcegraph), interview with Deloitte, Oct. 1, 2025.

---

# About the authors

## **Lou DiLorenzo Jr.**

ldilorenzocr@deloitte.com

Lou DiLorenzo Jr. leads Monitor Deloitte's US Technology, AI, and Data Strategy practice. With over 25 years of experience across various sectors, DiLorenzo excels in bringing key stakeholders together to drive change, develop new capabilities, and achieve positive financial results for both large corporations and startups. DiLorenzo is a prominent voice in the technology community, frequently quoted in leading publications such as *Forbes*, *Fortune*, and *The Wall Street Journal*.

## **Michael Caplan**

mcaplan@deloitte.com

Michael Caplan is a principal in Deloitte Consulting's Strategy practice and leader of Deloitte's Technology Operating Model Design and Enablement capability. Caplan brings over 20 years of experience advising companies in complex technology and business model transformations with a focus on aligning technology and the broader corporate enterprise to forge future-ready technology strategies, operating models, and ways of working that enhance value and drive organizational growth.

## **Anjali Shaikh**

anjalishaikh@deloitte.com

Anjali Shaikh leads Deloitte's technology executive programs, serving as an advisor to CIOs, CDAOs, and tech leaders and providing strategic direction for program development. Shaikh leads a team of skilled practitioners responsible for creating customized experiences and developing valuable insights that help executives navigate complex challenges; shape the tech agenda; build and lead effective teams; and excel in their careers.

## **Erika Maguire**

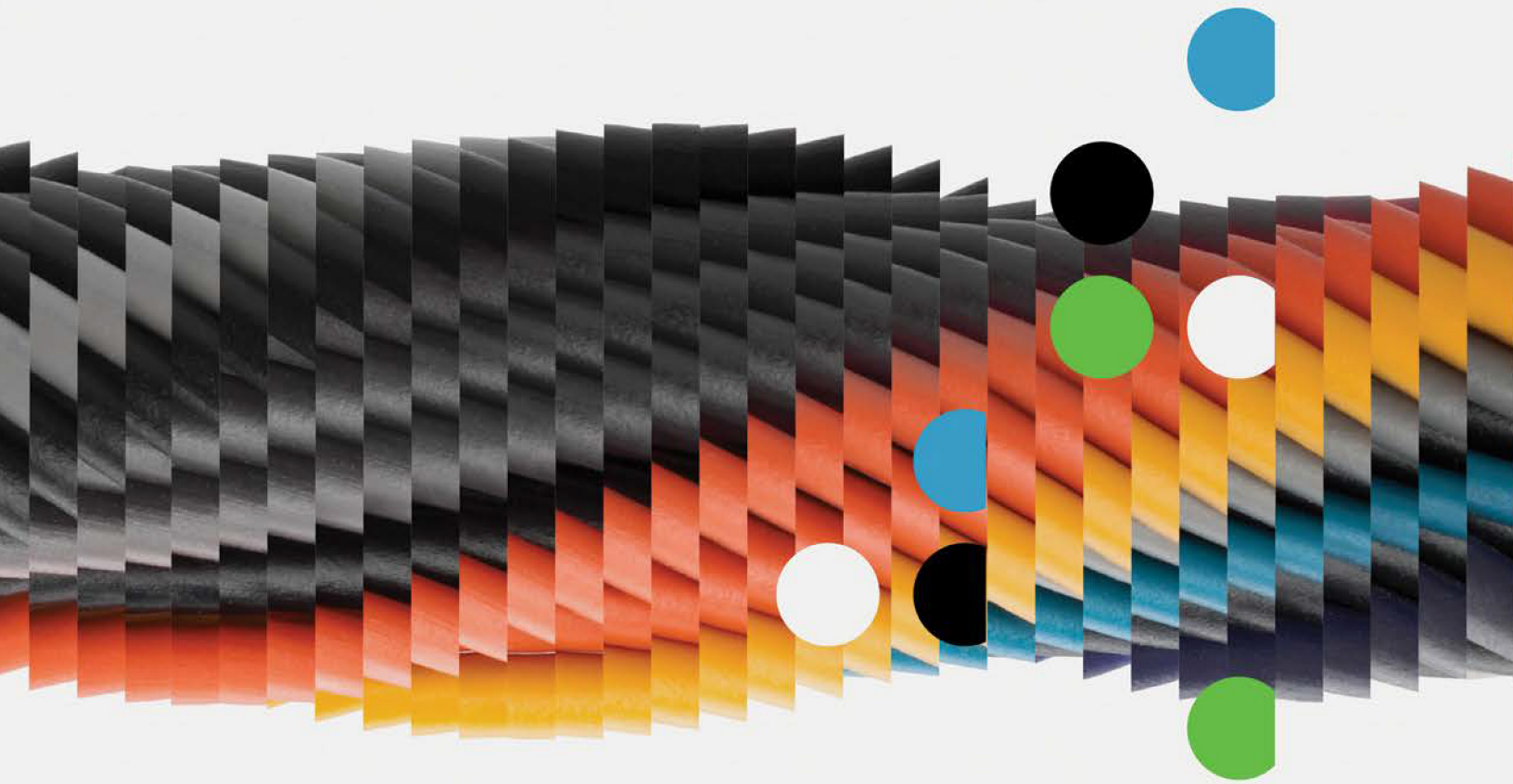
ermaguire@deloitte.com

Erika Maguire is a researcher and editor focused on uncovering what's new and next in tech. As part of Deloitte's CIO program, she leads key thought leadership initiatives, including Deloitte's Global Technology Leadership Study, and provides clients with actionable insights to build better teams and better businesses. She previously spent nine years at *Forbes* creating data-driven content for today's biggest brands.

---

# Acknowledgments

Much gratitude goes to the many subject matter leaders across Deloitte who contributed to our research for this chapter: **Ryan Casden**, **Nate Paynter**, **Tarun Sharma**, **Tim Smith**, and **Michael Wilson**.





# AIのジレンマ：サイバー防御のためのAIの確保と活用

組織は、AIがもたらす脅威に先手を打ちつつ、その強力な防御能力を認識し活用するという、サイバーセキュリティのパラドックスをどのように乗り越えることができるだろうか。

Sunny Aziz, Adnan Amjad, Naresh Persaud, Mark Nicholson, and Ed Burns

**A**Iを大規模に導入している組織は、そのパラドックスを発見しつつある。競争力の向上に役立つAIの能力が、新たなセキュリティリスクをもたらす可能性もあるのだ。さらにパラドックスに拍車をかけるように、AIは自らが生み出す脆弱性に対抗するための強力な新機能を提供することも認識され始めている。

企業は、シャドーAIの展開、AIによって加速される攻撃、AIシステム固有のリスクなど、AIに関連する複数の脅威に直面している<sup>1</sup>。しかし、AIが新たな脅威ベクトルを生み出す一方で、従来のサイバーセキュリティの原則は不変であり、マシンスピードで学習、適応、運用する自律システムに適用されるべきである。これらの技術の多くには、大幅な適応が必要である。なぜなら、ほとんどのサイバー組織はデジタルインテリジェンスを活用するように設計されていなかったためである。

事後的なセキュリティ対応の機会は狭まりつつある。昨年、多くの組織はAIの活用とその可能性の探求に注力した。現在では、統制されていない導入のリスクを認識するにつれて、新たな脅威をカタログ化し、イノベーションのスピードとセキュリティのバランスを取るためのガバナンスフレームワークを導入している。

## 内なる脅威

外部からの脅威は依然として存在する。[Tech Trends 2024](#)で議論したように、ディープフェイク、合成ペルソナ、AIを活用したソーシャルエンジニアリングは進化し続けている。しかし、今日の最も差し迫ったAI関連リスクの多くは、組織内部から発生している。そのようなリスク

の2つが、シャドーAIとエージェントAIガバナンスに対する不適切な管理である。

シャドーAI、すなわち企業内の個々のチームによって導入される未承認のAIデプロイメントは、ガバナンスの死角を生み出し、機密データへのアクセス、重要な選択、他のシステムとの連携が可能な自律的な意思決定システムを導入することになる<sup>2</sup>。各デプロイメントは、データ漏洩、モデル操作、モデルドリフト、または不正アクセスの潜在的な原因となる。企業が過去数年間にシャドーITの展開に対応するために開発したアプローチの多くには、ネットワークの監視によりすべてのアプリケーションを発見し、新規導入がプライバシーとセキュリティ基準に準拠していることを保証するためのポリシーを策定することが含まれる<sup>3</sup>。

過去1年間、企業はAIを業務プロセスのワークフローに効果的に統合することに注力してきた。現在、業務全体でAIの利活用を拡大するにつれて、AI導入の新たな一連のリスク及びそれらに関する緩和の戦略が存在することを認識しつつある。

## リスクの特定からリスクの緩和へ

AIのセキュリティリスクは、データ・AIモデル・アプリケーション・インフラの4つの領域にわたり顕在化する。組織は脅威の全容を発見し続けている一方で、事後的なセキュリティ対応の機会は狭まりつつある。既存のセキュリティプラクティスの多くは、これらのAI固有のリスクに対処するために適応させることができる。

**データセキュリティリスク：**大規模言語モデル（LLM）やその他のAIシステムは、膨大な量の情報を単一の場所に集中させるため、追加の保護が必要となる。デー

セキュリティの懸念は、トレーニング、テスト、検証、およびデプロイメント後の推論時にAIモデルが処理する情報を包含する(図1)。

**AIモデルのセキュリティリスク**：モデルセキュリティは、モデルのアーキテクチャーと独自のトレーニングパラメータ、およびトレーニング、テスト、検証プロセスを含む(図2)。透明性の要件はモデルの種類によって異なることが多く、重要な規制上の考慮を必要とする。

図1

## AI関連のデータセキュリティリスクと緩和戦略

リスク	緩和策
<p><b>機密性とデータプライバシー</b>：AIツールは機密データを意図せず公開する可能性がある。</p> <p><b>トレーニングデータポイズニング</b>：攻撃者はトレーニングデータを改ざんして、出力の正確さと有用性を損なう可能性がある。</p> <p><b>モデルの歪曲</b>：バックドアやシステムのバイアスを作成するためのトレーニングデータの意図的な操作が含まれる。</p>	<p><b>安全なデータ管理プラクティス</b>：AIデータソースをカタログ化し、人間が生成した高品質なトレーニングデータを維持し、合成データを慎重に管理する。</p> <p><b>データ完全性の監視</b>：データが改ざんされていないことを継続的に監視し、異常を検出する。</p> <p><b>堅牢なアクセス制御</b>：最小権限の原則を実装し、許可された担当者だけにトレーニングデータまたはサポートサービスへのアクセス権を付与する。</p>

出所：Deloitte analysis.

図2

## AIモデルのセキュリティリスクと緩和戦略

リスク	緩和策
<p><b>モデル崩壊</b>：合成データでトレーニングされたAIモデルは、時間とともに徐々に劣化する。</p> <p><b>モデル窃盗</b>：独自のモデルへの不正アクセスにより、攻撃者は脆弱性の特定や機能の複製ができる。</p> <p><b>モデルインバージョン</b>：モデルの出力を使用して、機密性の高いトレーニングデータを再構築し、抽出することができる。</p> <p><b>過剰なエージェンシーの乱用</b>：生成AIアプリケーションが過剰な権限を取得して、意図しないアクションを実行する。</p>	<p><b>モデルの分離</b>：トレーニングとデプロイメントにわたって、データと環境の明確な分離を実装する。</p> <p><b>特権アクセス管理</b>：包括的なIDおよびアクセス管理を通じて、学習済みモデルへのアクセスを制御および監視する。</p>

出所：Deloitte analysis.

**アプリケーションセキュリティリスク：**アプリケーションリスクは、モデルをホストインフラ上に位置する外部レイヤーに関連する。これらのレイヤーは、ユーザーやシステムがAI機能と対話するためのユーザーインターフェースとして機能する（図3）。

**インフラセキュリティリスク：**インフラセキュリティは、AIシステムの開発とホスティングに使用されるハードウェアとネットワークコンポーネントを包含し、AI機能が動作する基盤レイヤーを表す（図4）。

図3

## AIアプリケーションのセキュリティリスクと緩和戦略

リスク	緩和策
<p><b>倫理的な使用に関する懸念：</b>モデルは人間の行動を模倣するため、AIの決定は不正確さやバイアスの影響を受けやすい。</p> <p><b>入力インジェクション：</b>悪意のある入力制御を上書きしたり、モデルの動作を変更したりする。</p> <p><b>不正アクセス：</b>許可されていないユーザーがAIアプリケーションまたはデータにアクセスする。</p>	<p><b>ネットワークとユーザーのアクセス管理：</b>大規模言語モデルには、許可されたユーザーのみがアクセスできる安全なエンクレープが必要である。</p> <p><b>包括的なアクセス制御：</b>トレーニングデータ、学習済みモデル、またはサポートサービスへのアクセスを制御および監視する。</p> <p><b>サードパーティサービスプロバイダーの評価：</b>潜在的なパートナーリスクを特定し、ベンダーエコシステム全体にセキュリティ要件を拡張する。</p>

出所：Deloitte analysis.

図4

## AI関連のインフラセキュリティリスクと関連する緩和戦略

リスク	緩和策
<p><b>安全でないインターフェースとAPI：</b>脆弱性が悪用され、モデルへの攻撃やシステム・データに関する情報取得が行われる可能性がある。</p> <p><b>モデルのサービス拒否：</b>巧妙に細工された入力リソースを大量に消費する処理を引き起こし、システムを利用不能にする、またはコストを増加させる。</p> <p><b>サプライチェーンの脆弱性：</b>サードパーティのデータセット、事前学習済みモデル、およびフレームワークの使用は、AIシステム全体に伝播するリスクをもたらす可能性がある。</p> <p><b>デプロイメントの設定ミス：</b>ホスティング環境の設定ミスは、不正アクセス、データ漏洩、またはシステムの侵害につながる可能性がある。</p> <p><b>ラテラルムーブメント攻撃：</b>攻撃は、システム横断的なサービスまたは侵害されたアカウントを使用してAIシステムにアクセスする。</p>	<p><b>仮想ネットワークでの安全なデプロイメント：</b>安全なサンドボックスは、テスト時にAIワークロードを本番環境から分離する。</p> <p><b>境界とワークロードの強化：</b>ファイアウォール、ネットワークセグメンテーション、トラフィック検査などの厳格な制御により、侵害リスクを低減する。</p> <p><b>セキュアな機械学習運用の統合：</b>機械学習運用にセキュリティを統合する。</p>

出所：Deloitte analysis.

## AIのためのセキュリティ: AIシステムの基本的なセキュリティ課題

Sanmi Koyejojはスタンフォード大学の助教であり、AIの安全性とセキュリティのためのエンタープライズソリューションを開発するVirtue AIの共同創設者である。彼のAI評価、敵対的堅牢性、および安全性評価に関する研究は、主要なテクノロジー企業の本番システムに実装されている。

### Q:従来のコンピューティングシステムと比較して、AIシステムの保護が難しいのはなぜか

**A:** AIシステムは、過去に見てきた多くのコンピューティングインフラとは、挙動、ユースケース、範囲が大きく異なる。

最大の違いは、AIが従来のコンピューティングシステムと比較して、はるかに柔軟で文脈的であることだ。これは、従来のセキュリティのために開発、完成されたツールセットの多くが、AIシステムにはあまり効果的ではなく、エージェントシステムのような新しいフレームワークにはさらに効果が薄いことを意味する。

また、従来のコンピューティングでは、データと計算は分離されていたため、従来のサイバーセキュリティ技術を使用して、データを攻撃するものとインフラを攻撃するものを分離し対処することができた。しかし、AIシステムでは、データと計算が結合されているため、一方を攻撃することは両方を攻撃することを意味する。

新たなAIのユースケースと脅威領域の複雑さは、コンピューティングシステムのセキュリティの在り方を再考する必要がある。AIシステムは、標準的なトラフィックに溶け込み、人間が生成した情報のように見せることに非常に長けているため、多くの従来の検出戦略は通用

しなくなっている。

言語を超えて、視覚、音声、その他のマルチモーダルシステムへの移行には多くの期待が寄せられている。音声や動画はテキストよりもはるかに人々の関心を引くため、物事をより容易に信じてしまう。

モダリティ種類の拡大と多様なモードへの対応能力により、利害関係者及びコンピューティングシステムインフラに対するリスクは増大する。

### Q: AIのためのセキュリティに関して、どのようなアプローチが登場しているか

**A:** エコシステムの観点では、非常に興味深いことが起こっている。主要な2つのタイプの企業があり、互いに補完的だが異なるアプローチを取っている。

一方は、従来のサイバーセキュリティ企業が、AIのためのセキュリティ (Security for AI) とセキュリティのためのAI (AI for Security) の両方の分野でAIを導入している。これらの企業は従来のセキュリティ課題を解決するためにAIに投資してきたが、最も興味深いのは、データサニテーション、ガードレール、プロンプトインジェクションやその他のエージェント展開の問題に対するAIファイアウォールのようなAIのためのセキュリティ機能を追加していることだ。

他方は、AIネイティブの企業がAIセキュリティに取り組んでいるケースだ。これは非常に対照的なアプローチである。セキュリティを出発点としてAIの脅威に対処するための足場を組む方法を模索するアプローチと、AIネイティブ

のインフラを出発点として、これらのシステムを構築し、その脆弱性を把握するとともに、その知識を活用してセキュリティインフラを設計するアプローチでは、見え方が異なる。

私は、AIネイティブの企業のアプローチの方が、AI向けのセキュリティアプリケーションにはるかに効果的であると考えている。AIネイティブの企業は、システムをより深く理解しており、従来のセキュリティ企業に比べて、よりの絞った対応が可能であるため、特別な強みとなっている。

### Q: 2~4年先を見据えて、他にどのような攻撃や攻撃ベクトルが予想されるか。あるいは、この進化のスピードから予測は不可能なのか

**A:** 私の経験と知見からすると、リスクと能力は非常に密接に連動している。システムができるが増えるほど、我々はそれにアクセス権と裁量 (エージェンシー) を与え、それに伴い新たなセキュリティ面をカバーする必要が生じる。したがって、リスクがどこに向かっていくかを知りたければ、能力がどこに向かっているのか、つまり人々が何をしようとしているのか、どのようなユースケースに注目が集まっているのか、将来の投資がどこに向かっているのかを見るべきだ。

AIでは、テクノロジーに対する熱狂により、セキュリティや安全性の問題を無視し機能面に焦点を当てることで、後になりギャップがあったことに気づく。もう一度見直し、どのようなセキュリティリスクが生じるかを把握したうえで、セキュリティや安全性もモデルの機能の一部として扱うべきである<sup>4</sup>。

### 古いものが再び新しくなる

AIのデプロイメントを保護するために必要なプラクティスのほとんどは新しいものではなく、AIのリスクに対処するために更新されているだけである。AT&Tのシニアバイスプレジデント兼最高情報セキュリティ責任者であ

るRich Baichは、AIリスクを緩和するためのアプローチは、既存のサイバーセキュリティの主要なプラクティスに大きく依存していると述べている。特に、彼は強固なソフトウェア開発ライフサイクルの実施に注力している。ツールが自社開発かベンダー提供かにかかわらず、それぞれについてテストやレッドチームによる評価がな

され、アーキテクチャー要件を満たし、アクセス制御を実施していることが必要である（「高度なAIネイティブの防御戦略」のセクションを参照）。このアプローチにより、彼のチームは、新たな問題を生み出さないようにしつつイノベーションや業務推進のために必要なAIツールを導入できる。

彼は「私たちが今日経験していることは、過去に経験したことと大差はない」と述べている。

「AIとの唯一の違いは、スピードとインパクトだ」<sup>5</sup>

加速する攻撃のタイムライン、シャドーAI、および自律エージェントの管理の複雑さによって、データのカタログ化からエージェント監視まで、基本的なセキュリティ対策は喫緊の課題となっている。しかし、次のセクションで示すように、AIはサイバー、リスク、コンプライアンスの各チームにおいてもより大きな役割を果たしており、これらの新たな課題への対応を支援している。

## AI軍拡競争の激化

AIは新たな脆弱性をもたらす一方で、同時に強力な防御能力も提供する。先進的な組織は、AIを活用し、マシンスピードで活動しつつ進化する脅威にリアルタイムで適応する方法を模索している。AIを活用したサイバーセキュリティソリューションは、人間が見逃すパターンの特定、ランドスケープ全体の監視、脅威対応の迅速化、攻撃者の動きの予測、反復的なタスクの自動化を支援する。これらの能力は、組織のサイバーリスク管理のアプローチを変えている。

### 高度なAIネイティブの防御戦略

サイバーセキュリティチームがAIを活用している分野の1つがレッドチームである。これは、AIシステムに対し敵対的攻撃をシミュレートし、厳格にストレステストすることで、攻撃者が悪用する前に脆弱性と弱点を特定することを含む。このプロアクティブなアプローチは、組織が自社のAIシステムの故障モードとセキュリティ境界を理解するのに役立つ。

ブラジルの金融サービス会社Itau Unibancoは、レッドチーム演習のためにエージェントを導入した。同社は、人間の専門家とAIテストエージェントを全社的に展開する洗練されたアプローチを採用している。これらの「レッドエージェント」は、反復的なプロセスを使用して、倫理、バイアス、不適切なコンテンツなどのリスク

を特定し、緩和する。「規制された業界であるため、信頼が我々の最優先事項だ」とItau Unibancoの先進技術責任者は述べている。「そのため、モデルを破綻させるさまざまな方法をテストおよび再テストし、シミュレートすることに多くの時間を費やした」<sup>6</sup>

AIは敵対的トレーニングでも役割を果たしている。この機械学習技術は、モデルをだましたり攻撃したりするように設計された敵対的サンプルでモデルをトレーニングし、操作の試みに気づき抵抗できるようにすることで、攻撃に対するシステムの堅牢性を高める。

### ガバナンス、リスク、コンプライアンスの進化

AIを活用する企業は、新たなコンプライアンス要件に直面している。特にヘルスケアや金融サービスでは、意思決定プロセスの説明責任がたびたび求められる<sup>7</sup>。このプロセスは一般に読み解くのが難しいものの、いくつかの戦略は、AIのデプロイメントのコンプライアンス遵守を確保する上で有効である。

一部の組織では、誰がAIのデプロイメントを監督するかを見直している。従来は取締役会がこの分野を監督してきたが、監査委員会に責任を移管する動きが強まっている。監査委員会は、AI関連の活動を継続的にレビューおよび評価するのに適した立場にある<sup>8</sup>。

国境を越えたAI実装のガバナンスは今後も重要である。「AIインフラの清算」で議論されているように、規制に従って現地でデータを管理するために、データ主権の取り組みが求められる場合がある。

### 高度なエージェントガバナンス

エージェントは設計上、高い自律性を持って動作する。組織全体でエージェントが急増する中、企業はエージェントの意思決定パターンやエージェント間の通信をリアルタイムで分析し、基本的なアクティビティログに加えて異常なエージェントの行動を自動的に検出するための洗練されたエージェント監視が必要になる。この監視により、セキュリティチームは、重大な損害を引き起こす前に、侵害の疑いがある、もしくは不正挙動を示すエージェントを特定できる。

動的な特権管理は、エージェントガバナンスの側面のひとつである。このアプローチにより、チームはセキュリティ境界を維持しながら、ユーザーごとに数百〜数千のエージェントを管理できる。特権管理ポリシーは、エージェントの自律性とセキュリティ要件のバランスを取り、

コンテキストや挙動に基づいて特権を調整する必要がある。

ガバナンスポリシーには、エージェントの作成、変更、無効化、および継承計画を制御するライフサイクル管理を組み込む必要がある。これは、「エージェント的現実のチェック」で論じられているように、従業員の人事管理に類似しているが、デジタルワーカー向けに最適化されている。これは、オフボーディング後でも主要システムへのアクセスを保持する孤立したエージェント（ポット）の問題を抑止するのに役立つ。

AIエージェントが自ら新たなエージェントを立ち上げる権限を与えられるようになると、ガバナンスは企業にとってより差し迫ったものになる。この能力は、プライバシーやセキュリティの管理に関する重大な課題を提起する。特に、企業がこれらのエージェントの活動内容やアクセスできるシステムを把握していない場合、攻撃者の格好の標的になる可能性がある。

### フォースマルチプライヤー効果

多くのサイバーセキュリティ組織は、複雑な脅威を克服するためのフォースマルチプライヤーとしてAIを使用している。AIモデルは、強化された防御機構として、現在のセキュリティ対策に統合できる。

AIは、リスクスコアリングと優先順位付け、サードパーティリスク管理、自動化されたポリシーのレビューとオーケストレーション、サイバーセキュリティ成熟度評価、および規制遵守を支援できる。これらの分野でAIを活用することで、セキュリティチームはリソース配分についてより迅速かつ十分な情報に基づいた意思決定を下すことができる。

AIはまた、統制のテストと自動化、安全なコード生成、脆弱性スキャン、システム設計の最適化、およびモデルコードのレビュープロセスにも活用されている。これにより、セキュリティの弱点の特定と修正が迅速化される。

### AIブループリントの必要性

サイバーセキュリティチームの運用はAI向けに設計されていなかったが、組織全体でAIを実装しようとするビジネスの取り組みは、現在のサイバーセキュリティのプラクティスを再考する機会となる。企業が業務全体でAI（特にエージェント）を展開するにつれて、多くの企業は人材、運用モデル、ガバナンスモデル、およびテクノロジーアーキテクチャーを完全に再構築することを選択し

ている。AIエージェントを活用するために運用を再設計する際、セキュリティの考慮事項は後付けではなく、設計段階から組み込むべきである。この新たなサイバーリスクに対処するためのプロアクティブなアプローチは、企業が今日の脅威に備えるとともに、2~5年後に発生する可能性が高い危険への備えとしても役立つ。これが次のセクションの主題である。

## AIサイバーリスクは進化するが、解決策も進化する

今後を見据えると、新たなトレンドがサイバーセキュリティ、物理的セキュリティ、さらには地政学的安定性に関する基本的な前提に挑戦する可能性がある。一部のシナリオは依然として推測の域を出ないが、潜在的な複数の可能性を理解することで、組織は脅威の進化に適応できるアーキテクチャーとガバナンスフレームワークを準備できる。

### すべてが武器になるとき：AIと物理的現実の融合

AIが電力網・水処理施設・交通網・サプライチェーン・ヘルスケア提供システムなど、あらゆる**物理システム**に普及し、AIの能力が向上するにつれて、物理的リスクは指数関数的に増加する。AIと物理インフラの融合は、前例のない混乱につながる可能性のあるアタックサーフェスを生み出す。

将来の脅威には、交通・ヘルスケア・公益事業を含む複数のセクターにわたるAIシステムを同時に破壊する単一の攻撃が含まれる可能性がある。相互接続されたAIシステムにアクセスを得た攻撃者は、重要なインフラセクター全体における連鎖的障害を画策する可能性がある。

洗練された攻撃は、「茹でガエル」の戦術を用いる可能性があり、AIシステムが数か月にわたってシステムのパフォーマンスを徐々に低下させ、重大な損害が蓄積されるまで検出を困難にする。

組織は、いくつかのアプローチを通じてAIと物理的現実の融合リスクに備えることができる。

- **サプライチェーンの脆弱性の自動検出**: 組織は、サプライチェーンのリスクを常時監視するツールを導入し、侵害の兆候に対する早期警告システムを実装すべきである。

- **物理システムのレジリエンス:**組織は、重要な物理システムのための手動によるバックアップ制御を整備し、必要に応じて人間のオペレーターが自動化された意思決定を上書きできるようにすべきである。
- **カスケード防止アーキテクチャー:**組織は、接続されたシステム全体に問題が広がるのを防ぐ障壁を設け、障害を封じ込める分離境界を実装すべきである。

## 自律型サイバー戦争

自律型サイバー戦争への進化、すなわち、人間の介入なしにマシンスピードで動作する完全に自動化された攻撃および防御システムによるAI対AIの戦闘は、サイバーセキュリティにおけるパラダイムシフトを表す。

将来の攻撃能力には、以下が含まれる可能性がある。

- **スウォーム攻撃の連携:**AIシステムは、防御側の対応にリアルタイムに適応する協調的な行動を通じて、防御システムを圧倒する可能性がある。
- **適応型持続的脅威:**攻撃は防御策に応じて進化し、各防御行動から弱点を学び、戦術を継続的に調整する可能性がある。
- **地政学的側面:**サイバー戦争のためのAIの兵器化は、新たな地政学的リスクを生み出す。[Tech Trends 2024](#)で説明されているように、改ざんまたは捏造されたメディアによる世論操作などが含まれる。
- **経済戦争のリスク:**株式市場は、取引・リスク評価・市場分析のためにますますAIに依存している。一部の専門家は、次の金融危機は従来の経済的要因ではなく、AIによって引き起こされる可能性があるとして示唆している<sup>9</sup>。

## 新たなフロンティア：宇宙と量子セキュリティ

AIセキュリティが進化する中、宇宙インフラと量子コンピューティングという2つの新たな分野が、発展途上であるものの見過ごせないものとなっている。

**宇宙インフラの脆弱性:**商業宇宙産業は新たなアタックサーフェスを生み出した。すべての衛星は本質的に悪用されやすいコンピューターである。攻撃者が衛星に侵入する能力を高めるにつれて、混乱の可能性はGPS、

通信、気象監視、および国家の安全保障システムにまで及ぶ。

**量子通信チャネル:**量子通信は理論的に破られない暗号化を約束するが、同時に現在の暗号化方法を時代遅れにする脅威でもある。[Tech Trends 2025](#)で述べられているように、組織はこの移行に備える一方で、攻撃者による侵害や妨害から量子通信インフラを守る必要がある。

## バランスの取れたイノベーションの必要性

組織は、AIに関する取り組みの初期段階からセキュリティを組み込む戦略的フレームワークを通じて、イノベーションとセキュリティの両立を追求すべきである。企業は、基本的なセキュリティコントロール（データセキュリティ・アクセス管理・モデル保護・インフラ強化）を実装することから始めることができる。迅速なAIデプロイメントを優先してこれらの基本を省略すると、最終的に競争上の地位を危うくする脆弱性が生じる可能性がある。

そのうえで、企業は高度なAIを活用した防御能力への投資を検討することが考えられる。AIの脅威への対抗には、マシンスピードで動作し、微妙な攻撃パターンを特定し、進化する攻撃者の戦術に適応できるAIを活用したセキュリティシステムが必要である。AIセキュリティをコストセンターではなくフォースマルチプライヤーとして扱う組織は、持続的な防御上の優位性を構築する可能性が高い。

最後に、中長期を見据え、新たな脅威に対するアーキテクチャーやガバナンスフレームワークを準備することがより重要になる。自律型サイバー戦争やAIと物理的現実の融合は遠い未来のように思えるかもしれないが、今日、適応可能なセキュリティアーキテクチャーを構築することは、脅威のランドスケープが進化する中で、明日の組織のレジリエンスを高めるのに役立つ。

AIのジレンマは、結局のところジレンマではなく、行動への呼びかけである。AIセキュリティに戦略的にアプローチし、複数の防御層を実装しつつ迅速にイノベーションを進める組織は、資産をより良く保護し、主要なリスク管理能力を通じて競争優位性を確立できる可能性がある。セキュリティをAI導入の制約ではなくイネーブラーとして扱い、このバランスを習得する企業が未来を手にする。

---

# Endnotes

1. Gartner, “Gartner survey reveals gen AI attacks are on the rise,” press release, Sept. 22, 2025.
2. CybSafe, “STUDY: Almost 40% of workers share sensitive information with AI tools, without employer’s knowledge,” press release, Sept. 26, 2024.
3. Dana Raveh, “What is shadow IT?” CrowdStrike, July 10, 2024.
4. Sanmi Koyejo (assistant professor, Stanford University), interview with Deloitte, Sept. 26, 2025.
5. “A no-nonsense approach to secure AI enablement at AT&T,” *Deloitte Insights*, Nov. 21, 2025.
6. Roberto Frossard (head of emerging technologies, Itau Unibanco), interview with Deloitte, Sept. 17, 2025.
7. Pat Niemann, “Cyber and AI oversight disclosures: What companies shared in 2025,” Harvard Law School Forum on Corporate Governance, Oct. 28, 2025.
8. Deloitte US, “Artificial intelligence: An emerging oversight responsibility for audit committees?” accessed Nov. 11, 2025.
9. John Divine, “How AI could spark the next financial crisis,” *US News & World Report*, June 30, 2023.

---

# About the authors

## **Sunny Aziz**

saziz@deloitte.com

Sunny Aziz is a principal in Deloitte's Cyber and Strategic Risk services with over 25 years of experience in helping clients manage, implement, and operate complex cyber programs. He advises clients on cyber strategies and executing large cyber transformation initiatives. Aziz also serves as Deloitte's Financial Services Industry Insurance sector lead for Cyber, specializing in managed security services, cyber strategy and assessments, identity and access management, and more.

## **Adnan Amjad**

aamjad@deloitte.com

Adnan Amjad serves as the US Cyber Leader at Deloitte, overseeing the growth and strategy of Deloitte's Cyber offerings, including Cyber Defense & Resilience, Cyber Operate, Cyber Strategy & Transformation, Digital Trust & Privacy, and Enterprise Security. In this role, Amjad advises clients in navigating the evolving threat landscape through powerful cyber solutions and managed services that aim to simplify complexity and protect and enable businesses to succeed, build resilience, and supercharge transformation—helping them to secure the enterprise of the future.

## **Naresh Persaud**

napersaud@deloitte.com

Naresh Persaud is a principal in Deloitte Risk and Financial Advisory focused on cyber risk across industries. He has over 20 years of experience in identity and access management through multiple roles. Persaud has strong domain knowledge in both identity management and relational database security and experience leading large security implementations and operations across sectors.

## **Mark Nicholson**

manicholson@deloitte.com

Mark Nicholson is a principal in Deloitte Advisory with 25 years of experience in cybersecurity. Prior to its acquisition by Deloitte, Nicholson was the cofounder of the cybersecurity firm Vigilant, Inc. He is currently the AI leader for Deloitte Cyber.

## **Ed Burns**

edburns@deloitte.com

Ed Burns leads the client stories initiative within the Office of the CTO known as Trend Lines. This project serves as a key research input to Tech Trends and other eminence. Prior to his current role, he led a tech news publication that covered all things AI, analytics, and data management.

---

# Acknowledgments

Much gratitude goes to the many subject matter leaders across Deloitte who contributed to our research for this chapter: Giri Saravanan Chandramohan, Edward Guerrero, Kieran Norton, and Abhishek Sekhri.



## ノイズを切り裂く：AIの進展に伴い 追跡すべき技術シグナル

地殻変動の前触れとなる小規模なテクノロジートレンドとは何か。ニューロモーフィックコンピューティングからエッジAIまで、これらは注目すべき分野である。

*Raquel Buscaino, Kelly Raskovich, Bill Briggs, and Caroline Brown*

# 通

信理論では、シグナルとはノイズをカットする情報、すなわちそれを送信するシステムについて意味のある何かを明らかにするパターンのことである。テクノロジーにおいて、シグナルとは方向性の変化を示す初期の指標、すなわち大規模な変化に先立つ微震のようなものだ。シグナルは予測ではない。すでに動き始めている力の観察であり、本レポートで前述した複利的な効果から現れるパターンである。

本レポートでは、今後1年半～2年にわたって組織を再構築する5つの新たなテクノロジートレンド、物理的な人工知能とロボティクス、エージェントAI、AI インフラ、

テクノロジー機能の変革、そしてAI時代のサイバーセキュリティを取り上げた。しかし、新たなテクノロジーの展望には5つ以上のトレンドが存在する。我々のレポートにどれを含めるかを決定することは、科学的な裏付けだけでなく、編集上の判断や多少の直感も必要とされる。

この後に続くシグナルは、我々の中核的なトレンドに直接関連するものもあれば、並行して進行しているものもあるが、いずれもテクノロジーリーダーが追うべき新たな動向である。これらが各章として取り上げられなかったのは、重要性が低いからではなく、我々の中核テーマの周縁に位置しているか、まだ発展途上にあるためだ。いずれも注目に値する。

そのほとんどは、憶測に基づいた未来ではなく、いま起きている現象だ。すでに業界を再構築しているものもあれば、ようやく定量的な影響が現れ始めたものもある。「新興」と「主流」の間の距離が縮まりつつある状況において、リーダーはどこに注意とリソースを向けるべきか、すなわち、投資に値するものはどれか、監視にとどめるべきものはどれか、そして無視するとリスクになり得る依存関係はどれか、を見極める必要がある。

**基盤モデルはプラトーンに達しつつあるか** 大量のデータセットでトレーニングされた大規模AIシステムである基盤モデルは、重大な問いに直面している。指数関数的な改善をこの先も続けるのか、それともその能力が頭打ちになるのか。新しいモデルは依然として改善されているが、いくつかの指標では、初期の世代で見られたような劇的なパフォーマンスの飛躍が示されていない<sup>1</sup>。さらに、モデルが大きくなるほど、エネルギー消費とコンピューティングコストが増大する。複雑な問題を処理するためにモデルにより多くの時間を与えるといった<sup>2</sup>、新たなスケールアップアプローチは、「モデルが大きいほどパフォーマンスが優れている」という考え方から我々を転換させる可能性がある。これは、現行モデルでもプロンプトや実装戦略を最適化することで改善できることを意味する。企業がAIをいかにうまく展開し、ファインチューニングし、再設計されたプロセスに統合するかが、最新の基盤モデルを持つことよりも重要になる可能性が高い。

**新しいデータ > 合成データ > 古いデータ** 基盤モデルが同様の公開データセットで学習するにつれ、データそのものは競争優位ではなくなっていく。世界が変化するにつれて、古いデータは価値を失う。合成データ（他のAIをトレーニングするために使用されるAI生成コンテンツ）はギャップを埋めるのに役立ち、AIツールが使用するデータの80%が2028年までに合成データになると予測されている（2024年の20%から増加）<sup>3</sup>。しかし、合成データにはパフォーマンスの天井があり、通常、実データの品質の90%から95%にとどまる<sup>4</sup>。さらに悪いことに、主にAI生成コンテンツでトレーニングされたAIは、モデル崩壊を引き起こす可能性がある<sup>5</sup>。これは、モデルがまれなパターンに関する情報を失い、概念を混同し、最終的に単調で反復的な出力を生成するようになる退行的な過程だ。新鮮な情報（リアルタイムのユーザーインタラクション、独自のビジネスデータ、最新の研究）にアクセスできる者が優位に立つ。言い換えれば、インタラクションレイヤー（検索エンジン・ソーシャルプラットフォーム・AIアシスタント・スマートデバイス）を握る企業が勝者となる。

**ニューロモーフィックチップがコンピューティングを飛躍的に向上させる** ニューロモーフィックチップは、特定のAIタスクにおいて従来のGPU（画像処理装置）よりもエネルギー効率が高い、脳にヒントを得たプロセッサである。GPUはメモリと処理の領域が分離されているが、ニューロモーフィックチップは両方を同じ場所に組み合わせている。ニューロモーフィックチップはイベント駆動型であり、何かが起こった時のみ情報を処理するのに対し、GPUは常にフルスピードで動作する。これは、ニューロモーフィックチップが、センサーデータの分析や自動運転車での情報処理など、散発的な信号を扱うAIタスクにおいて、80~100倍少ないエネルギーしか使用しないことを意味する。一方で、連続的で高スループットな計算ではGPUが依然として優れている<sup>6</sup>。AIがデータセンターから何十億ものエッジデバイスへと広がるにつれ（次のシグナルを参照）、このエネルギー効率の優位性は極めて重要になる。ニューロモーフィックコンピューティングの広範な採用は2030年までに進むと期待されている<sup>7</sup>。

**エッジAIとオンデバイス処理の台頭** データを遠くのクラウドサーバーに送信するのではなく、エッジAIはスマートフォン、スマートウォッチ、防犯カメラ、または産業用ロボットなどのデバイス上で直接動作する。重要な理由は、レイテンシー（自動運転車はサーバーの応答を待たない）、プライバシー（データはデバイスから離れない）、爆発的なコスト（クラウドの請求書が月々数千万ドルに達する）、そしてインターネットへの依存である。エッジAIの可能性は、生成AI対応スマートフォンの市場に表れており、2024年には前年比で約364%成長し、年間販売台数は2億3,420万台に達し、2028年には9億1,200万台に向かう見込みだ<sup>8</sup>。実世界の応用例には、ローカルでリアルタイム認識を行うスマートカメラ、機器の故障を予測する産業用センサー、医療データを外部送信することなくバイタルを監視するヘルスケア向けウェアラブルなどがある。これはすでに動き出している根本的なシフトである。

**AIネイティブのパーソナルデバイスやウェアラブルは主流になるか** 企業は、スマートフォンを超えたAIネイティブのウェアラブルデバイスを試している。会話を録音・文字起こしするペンダント、リアルタイム翻訳機能を備えたスマートグラス、画面のない音声対話型ピンなどが挙げられる。世界のウェアラブルテクノロジー市場は2026年までに2,654億米ドルに達すると予測されており、テック大手は次世代フォームファクターに多額の投資を行っている<sup>9</sup>。しかし、市場への浸透は依然として非常に不確実で、この市場には失敗したメガネ、ピン、その他のウェアラブルやポケットサイズのフォーム

ファクターが散乱している<sup>10</sup>。消費者が実際に別のAIデバイスを望んでいるのか、それともすでに使用しているスマートフォンやイヤホンにAIが統合されることを好むのかという疑問はなお残る。勝利を収めるフォームファクターはまだ定まっておらず、成功はプライバシー懸念への対応と、追加のデバイスを持ち歩くに値する機能を提供できるかにかかっている。

**次世代サイバーセキュリティとしての生体認証** AIは声を複製し、文書を偽造し、行動パターンを模倣できるため、物理的な存在と本人性を確認するために生体認証が重要になっている。ディープフェイクやAIを利用した詐欺がより巧妙になるにつれて、組織は急速に生体認証システムを導入している。最高情報セキュリティ責任者を対象としたある調査では、92%がパスワードレス認証をすでに導入済み、導入中、または導入予定だと答えた<sup>11</sup>。しかし、生体認証が唯一の解決策というわけではない。漏洩した生体データはパスワードのように変更できず、プライバシーに関する懸念も依然として大きい。今後は、生体認証が主要ではあるが排他的ではない検証手段として用いるハイブリッド型アプローチが有力視される。

**AIエージェントのプライバシーに関するトレードオフ** 真に有能なパーソナルAIアシスタントは、前例のないレベルで個人データへのアクセスを必要とするが、そのアクセスはすでに許可されつつある。レストランの予約、スケジュール管理、メールのフィルタリングを効果的に行うために、パーソナルAIエージェントは、何年分ものメッセージ履歴、カレンダーの予定、閲覧データ、保存されたパスワード、クレジットカード情報、そして極めて私的な嗜好までを必要とする<sup>12</sup>。しかし、そのトレードオフは厳しい。個人データがAIモデルに組み込まれると、消去権はほぼ不可能になる<sup>13</sup>。そしてもちろん、セキュリティ上の懸念も大きい。世間の反応はすでに二分して

おり、機能性のために積極的に許可を与える人もいれば、抵抗する人もいる。とはいえ、同意のパラドックスは残る。AIアシスタントを有用なものにするためには広範な権限付与が必要だが、ほとんどのユーザーは、自分が共有に同意している内容の範囲や恒久性を十分に理解していない。

**GEOがSEOを凌駕する** ユーザーは従来の検索エンジンよりもAIチャットボットを利用するようになってきている。AIが生成する回答に登場することを巡る競争が始まっている。これは検索エンジン最適化（SEO）から生成エンジン最適化（GEO）へのシフトである。AI生成の回答はすでに主要な検索エンジンの検索結果を席巻しており、従来ウェブサイトへのクリック率を3分の1以上低下させている<sup>14</sup>。AIプラットフォームは現在、オーガニックトラフィックの6.5%を占めており、1年以内に14.5%に達すると予測されている<sup>15</sup>。GEOはSEOとは根本的に異なり、キーワードよりも意味的な豊かさを、バックリンクよりも著者の専門知識を、ページビューよりもAIの回答で引用されることを優先する<sup>16</sup>。2000年代が有料検索、2010年代がソーシャルメディア広告によって特徴づけられたように、2020年代はAI生成の回答が最も重要なマーケティングチャネルになりつつある。

これらのシグナルの中には、支配的な力に成熟するものもあれば、消えていくものもあるかもしれない。しかし、それらすべてが同じ根底にある現実を反映している。テクノロジーの変化のペースは根本的に変わったのだ。そして、予測の確からしさよりも適応のスピードがほうが重要だ。成功する組織は、どのシグナルがトレンドになるかを予測する組織ではなく、現れたものを感じし、評価し、迅速に対応する能力を構築した組織であろう。明確さが得られるまで待つ者は、競合他社がすでに活用している変化に後追いで適応することになるだろう。

---

# Endnotes

1. Casey Newton, “AI companies hit a scaling wall,” *Platformer*, Nov. 14, 2024.
2. Matthias Bastian, “AI progress in 2025 will be “even more dramatic,” says Anthropic co-founder,” *The Decoder*, Dec. 25, 2024.
3. Grant Gross, “Synthetic data takes aim at AI training challenges,” *CIO Magazine*, Feb. 19, 2025.
4. Emmett Fear, “Synthetic data generation: Creating high-quality training datasets for AI model development,” *RunPod Inc.*, July 31, 2025.
5. IBM, “Examining synthetic data: The promise, risks and realities,” accessed Nov. 11, 2025.
6. TokenRing AI, “Neuromorphic computing: The brain-inspired revolution reshaping next-gen AI hardware,” *WRAL News*, Oct. 7, 2025.
7. Research and Markets, “Growth opportunities in neuromorphic computing 2025-2030: Neuromorphic technology poised for hyper-growth as market surges over 45x by 2030,” press release, *GlobeNewswire*, April 18, 2025.
8. IDC Research, “Worldwide generative AI smartphone shipments forecast to reach 70% of the market by 2028 with more than 360% growth in 2024, according to IDC,” press release, July 30, 2024.
9. *PR Newswire*, “AI-powered wearables transform how consumers interact with everyday technology,” Sept. 15, 2025.
10. Amanda Yeo, “Three Products that Flopped in 2024,” *Mashable*, November 28, 2024.
11. Janna Bureson, “Passwordless hits the tipping point in enterprise security,” *Portnox*, Oct. 20, 2025.
12. Mark McCarthy, “The privacy challenges of emerging personalized AI services,” *Tech Policy Press*, May 28, 2025.
13. Zack Whittaker, “For privacy and security, think twice before granting AI access to your personal data,” *TechCrunch*, July 19, 2025.
14. Ryan Law and Xibeijia Guan, “AI overviews reduce clicks by 34.5%,” *Ahrefs*, April 17, 2025.
15. Jake Stainer, “Generative engine optimization (GEO): Complete 2025 guide,” *Skale*, Sept. 30, 2025.
16. Leigh McKenzie, “Generative engine optimization (GEO): How to win in AI search,” *Backlinko*, Oct. 23, 2025.

---

# About the authors

## Raquel Buscaino

rbuscaino@deloitte.com

Raquel Buscaino leads Deloitte’s Novel & Exponential Technologies (NExT) team where she and her team sense, and make sense of, emerging technologies that are likely to change the way we work and live. The NExT team uses this research to create world-class thought leadership, such as Deloitte Tech Trends and xTech Futures. Buscaino is also the host of the Deloitte TECHTalks podcast where she interviews industry leaders about what’s new in tech.

## Kelly Raskovich

kraskovich@deloitte.com

Kelly Raskovich is a senior manager and lead within Deloitte’s Office of the CTO, and serves as the executive editor of Tech Trends, Deloitte’s flagship report on emerging technologies. Her mission is to educate clients, shape the future of Deloitte’s technology brand and offerings, cultivate talent, and enable businesses to achieve future growth. She is responsible for technology eminence, client engagement, and marketing/PR efforts.

## Bill Briggs

wbriggs@deloitte.com

As the chief technology officer, Bill Briggs helps clients anticipate the impact that emerging technologies may have on their business in the future and how to get there from the realities of today. He is responsible for research, eminence, and incubation of emerging technologies affecting clients’ businesses and shaping the future of Deloitte Consulting LLP’s technology-related services and offerings. Briggs also serves as executive sponsor of Deloitte’s CIO Program.

## Caroline Brown

carolbrown@deloitte.com

Caroline Brown is a senior manager within Deloitte’s Office of the CTO. She leads a cross-functional editorial and design production team in developing thought leadership. She serves as the editor of Tech Trends, Deloitte’s flagship technology report. A writer and researcher, Brown earned undergraduate and graduate degrees in English and journalism from the University of North Carolina at Chapel Hill.

---

# Acknowledgments

## Special thanks

**Ed Burns, Preetha Devan, Makarand Kukade, Erika Maguire, Heidi Morrow, and Sarah Mortier** for being the engine powering Tech Trends. Ed, your continued dedication to editorial excellence and ability to deftly weave research and insights into compelling narratives have truly elevated our work. Erika, what a great first-time effort—we're so grateful for your research and writing skills, business instinct, sense of humor, and ability to roll with the punches. Heidi, your leadership in design and creative vision have set a standard for visual excellence, bringing our ideas to life in ways that captivate and inspire. Makarand, thank you for jumping in during your first year on Tech Trends and bringing fresh perspective to our supplemental assets and visual materials. Sarah, your leadership in managing the production process has been instrumental in keeping us on track. Your organizational prowess, attention to detail, and collaborative spirit have navigated us through challenges and kept the editorial moving forward. Preetha, we appreciate you bringing your publishing expertise to Tech Trends this year and helping us refine our processes and workflows. We're lucky and thankful that the six of you are part of the team.

**Caroline Brown**, for leading the Tech Trends editorial and production with steady guidance, strategic insight, and unwavering support. Your leadership has been essential in navigating the complexities of this year's report, and we're grateful for your partnership in bringing Tech Trends to life.

**Catarina Pires and Haley Gove Lamb** for championing Tech Trends and delivering exceptional client experiences. Your dedication to bringing Tech Trends to life for our clients and creating meaningful engagements ensures the report reaches and resonates with the audiences who need it most. Thank you for being such effective ambassadors for our work.

**Katarina Alaupovic, Alison Cizowski, Deanna Gorecki, Ben Hebbe, Bri Henley, Abria Perry, Mikaeli Robinson, and Madelyn Scott** for your tireless dedication and innovative strategies in promoting Tech Trends. Your creativity in marketing, communications, and outreach significantly amplifies our reach and impact year after year. Thank you for your passion and commitment to spreading the value of Tech Trends far and wide.

**Amanpreet Arora and Nidhi John** for the breath of fresh air you brought to the Tech Trends process by pitching in with research, data, and insights. We appreciate your enthusiastic and cheerful willingness to tackle whatever came your way throughout the entire life cycle of the report, from identifying trends to bringing the numbers that back our work.

**Raquel Buscaino and Mark Osis** for being our collaborators as we identified trends and signals and for helping us hone our research craft. Thank you for generously sharing your knowledge and expertise with us.

**Diana Kearns-Manolatos and Duncan Stewart** for your expertise and willingness to share knowledge across teams. Your collaboration has enriched our work and strengthened the connections between our research efforts. Thank you for your generosity and partnership.

**Hannah Bachman, Aditi Rao, Elisabeth Sullivan**, and the entire **Deloitte Insights team** for your continued partnership and support as we evolve Tech Trends together. We appreciate your flexibility, strategic guidance, and commitment to excellence as our collaboration deepens and our practice continues to grow.

**Sylvia Chang, Jim Slatton, Manya Kuzemchenko, Melissa O'Brien, Molly Piersol, Natalie Pffaf, Harry Wedel, Jaime Austin, Govindh Raj, Megha Priya, and Naveen Bhusare** for your creativity and dedication in developing the visual assets that bring Tech Trends to life. Your artistic vision and attention to detail create the captivating imagery and graphics that make our report not just informative but truly engaging. We're grateful for your commitment to collaboration and creative excellence.

---

# Continue the conversation

Our insights can help you take advantage of emerging trends. If you're looking for fresh ideas to address your challenges, let's talk.

## The Office of the CTO

The Deloitte US Office of the CTO is a team centered on engineering technology futures. We identify, research, and incubate emerging technology solutions to shape demand for future markets, cultivate talent, and enable businesses for future growth.

If you'd like to connect and discuss more, please feel free to contact us at [OCTO@deloitte.com](mailto:OCTO@deloitte.com).

---

# Executive editor



**Kelly Raskovich**

Client & Marketing Lead, Office of the CTO  
Deloitte Consulting LLP  
kraskovich@deloitte.com

Kelly Raskovich is a senior manager and lead within Deloitte’s Office of the CTO (OCTO), and serves as the executive editor of Tech Trends, Deloitte’s flagship report on emerging technologies. Her mission is to educate clients, shape the future of Deloitte’s technology brand and offerings, cultivate talent, and enable businesses to achieve future growth. She is responsible for technology eminence, client engagement, and marketing/PR efforts. Prior to her leadership role, she led several data and analytics projects for global Fortune 500 organizations across the oil and gas industry.

---

# Executive sponsor



## **Bill Briggs**

Global chief technology officer  
Deloitte Consulting LLP  
wbriggs@deloitte.com

As chief technology officer, Bill Briggs helps clients anticipate the impact that emerging technologies may have on their business in the future and how to get there from the realities of today. He is responsible for research, eminence, and incubation of emerging technologies affecting clients' businesses and shaping the future of Deloitte Consulting LLP's technology-related services and offerings. Briggs also serves as executive sponsor of Deloitte's CIO Program, offering CIOs and other technology executives insights and experiences to navigate the complex challenges they face in business and technology.

Bill earned his undergraduate degree in computer engineering from the University of Notre Dame, and his MBA from the Kellogg School of Management at Northwestern University. He proudly serves on the board of directors for the Kids In Need Foundation, partnering with teachers and students in under-resourced schools and providing the support needed for teachers to teach and learners to learn.

---

# 日本版発行責任者



## 中川 貴雄 パートナー

Tech Strategy and Transformation

多様な業界で、IT・DX戦略立案、IT組織・ガバナンス、アーキテクチャ、IT M&Aなど、テクノロジー戦略領域のコンサルティングに従事。グローバル案件に強みを持ち、システム実装の知見を活かして、戦略・構想策定から変革実行までを一貫して支援し、CIOに対してアドバイザーサービスを提供している。

---

# 日本版発行担当者

イントロダクション

## イノベーションの複利効果

武野 淳            李 作鵬

インタラクション

## AIは物理世界へ：AIとロボティクスの融合がもたらす新たな可能性

高橋 直之          戸辺 諒太  
大地 宏明          西村 咲映  
川上 秀之

インフォメーション

## エージェント化のリアリティチェック：シリコンベースの労働力に備える

穴倉 剛            米島 慎二  
河原 弘宜          ウエイレン 由子

コンピューテーション

## AIインフラの転換点：推論エコノミクスの時代におけるコンピューティング戦略の最適化

南野 香澄          中澤 雄馬  
傳田 拓真          田中 玖留美

ビジネスオブテクノロジー

## テクノロジー組織の再構築：AIネイティブなテクノロジー組織の設計

斉藤 宏樹          近藤 正堯  
植木 成実          吉田 晃大  
篠塚 竣            塩見 遥

サイバーとトラスト

## AIのジレンマ：サイバー防御のためのAIの確保と活用

大場 正士          坂井 星児

コンクルージョン

## ノイズを切り裂く：AIの進展に伴い追跡すべき技術シグナル

武野 淳            李 作鵬

---

# 国内のお問い合わせ先

中川 貴雄 / Takao Nakagawa

Technology Strategy & Transformation

Partner

合同会社デロイト トーマツ

taknakagawa@tohatsu.co.jp

# Deloitte.

## Insights

Sign up for Deloitte Insights updates at [www.deloitte.com/insights](http://www.deloitte.com/insights)

### Deloitte Insights contributors

**Editorial:** Aditi Rao, Hannah Bachman, Debashree Mandal, Pubali Dey, and Cintia Cheong

**Creative:** Manya Kuzemchenko, Sylvia Yoon Chang, Natalie Pfaff, Molly Piersol, Harry Wedel, and Govindh Raj

**Deployment:** Atira Anderson

**Cover artwork:** Manya Kuzemchenko and Sylvia Yoon Chang; Getty Images, Adobe Stock

デロイト トーマツ グループは、日本におけるデロイト アジア パシフィック リミテッドおよびデロイトネットワークのメンバーである合同会社デロイト トーマツ グループならびにそのグループ法人（有限責任監査法人トーマツ、合同会社デロイト トーマツ、デロイト トーマツ税理士法人およびDT弁護士法人を含む）の総称です。デロイト トーマツ グループは、日本で最大級のプロフェッショナルグループのひとつであり、各法人がそれぞれの適用法令に従いプロフェッショナルサービスを提供しています。また、国内30都市以上に2万人超の専門家を擁し、多国籍企業や主要な日本企業をクライアントとしています。詳細はデロイト トーマツ グループWebサイト、[www.deloitte.com/jp](http://www.deloitte.com/jp)をご覧ください。

Deloitte（デロイト）とは、Deloitte Touche Tohmatsu Limited（“Deloitte Global”）、そのグローバルネットワーク組織を構成するメンバーファームおよびそれらの関係法人（総称して“デロイトネットワーク”）のひとつまたは複数指します。Deloitte Globalならびに各メンバーファームおよび関係法人はそれぞれ法的に独立した別個の組織体であり、第三者に関して相互に義務を課しまたは拘束させることはありません。Deloitte Globalおよびその各メンバーファームならびに関係法人は、自らの作為および不作為についてのみ責任を負い、互いに他のファームまたは関係法人の作為および不作為について責任を負うものではありません。Deloitte Globalはクライアントへのサービス提供を行いません。詳細は[www.deloitte.com/jp/about](http://www.deloitte.com/jp/about)をご覧ください。デロイト アジア パシフィック リミテッドは保証有限責任会社であり、Deloitte Globalのメンバーファームです。デロイト アジア パシフィック リミテッドのメンバーおよびそれらの関係法人は、それぞれ法的に独立した別個の組織体であり、アジア パシフィックにおける100を超える都市（オークランド、バンコク、北京、ベンガルール、ハノイ、香港、ジャカルタ、クアラルンプール、マニラ、メルボルン、ムンバイ、ニューデリー、大阪、ソウル、上海、シンガポール、シドニー、台北、東京を含む）にてサービスを提供しています。

Deloitte（デロイト）は、最先端のプロフェッショナルサービスを、Fortune Global 500<sup>®</sup>の約9割の企業や多数のプライベート（非公開）企業を含むクライアントに提供しています。デロイトは、資本市場に対する社会的な信頼を高め、クライアントの変革と繁栄を促進することで、計測可能で継続性のある成果をもたらすプロフェッショナルの集団です。デロイトは、創設以来180年の歴史を有し、150を超える国・地域にわたって活動を展開しています。“Making an impact that matters”をバース（存在理由）として標榜するデロイトの約46万人の人材の活動の詳細については、[www.deloitte.com](http://www.deloitte.com)をご覧ください。

本資料は皆様への情報提供として一般的な情報を掲載するのみであり、Deloitte Touche Tohmatsu Limited（“Deloitte Global”）、そのグローバルネットワーク組織を構成するメンバーファームおよびそれらの関係法人（総称して“デロイトネットワーク”）が本資料をもって専門的な助言やサービスを提供するものではありません。皆様の財務または事業に影響を与えるような意思決定または行動をされる前に、適切な専門家にご相談ください。本資料における情報の正確性や完全性に関して、いかなる表明、保証または確約（明示・黙示を問いません）をするものではありません。またDeloitte Global、そのメンバーファーム、関係法人、社員・職員または代理人のいずれも、本資料に依拠した人に関係して直接または間接に発生したいかなる損失および損害に対しても責任を負いません。Deloitte Globalならびに各メンバーファームおよび関係法人はそれぞれ法的に独立した別個の組織体です。

Member of  
**Deloitte Touche Tohmatsu Limited**

© 2026. For information, contact Deloitte Tohmatsu Group.