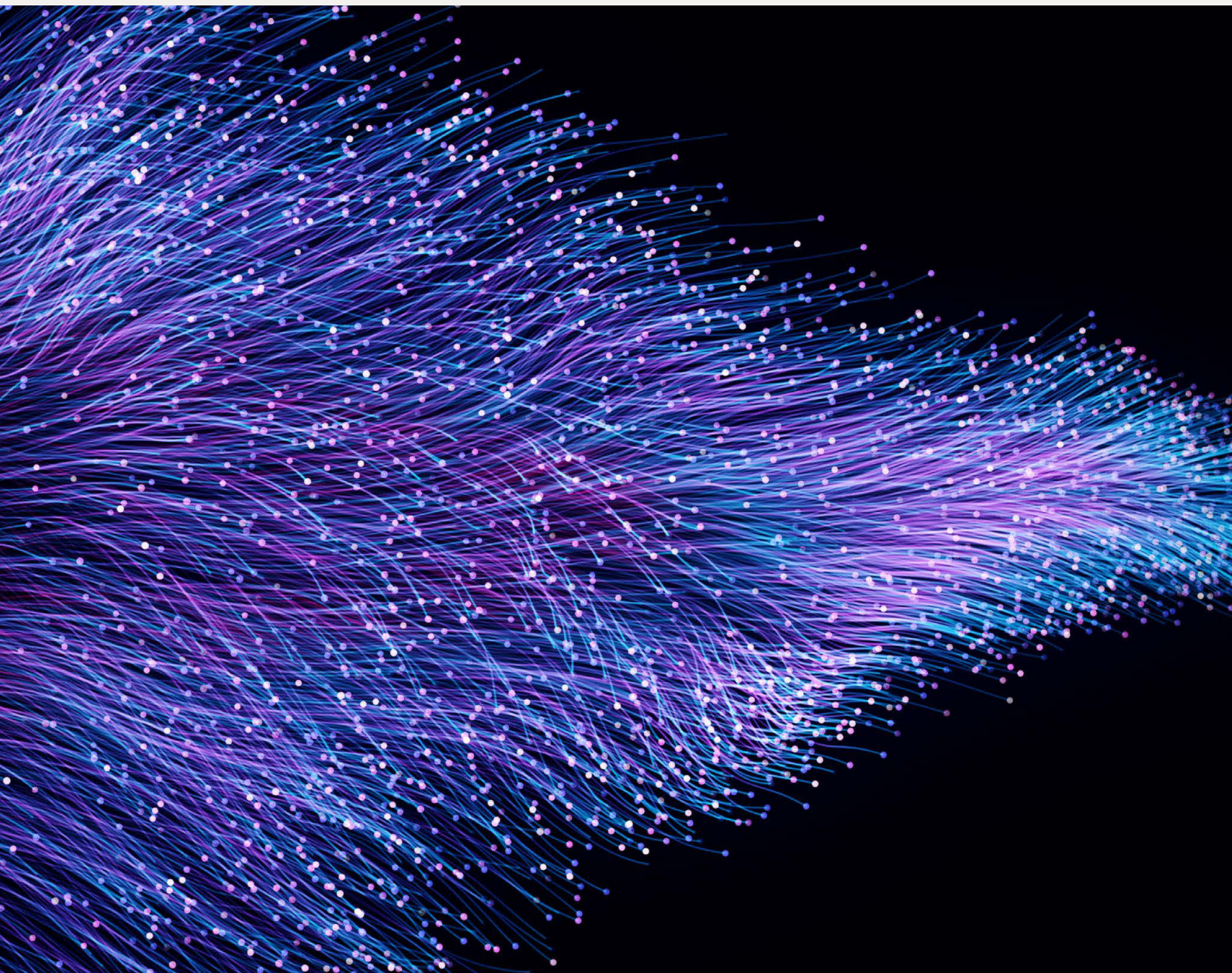


テクノロジーの真価と代償が 問われるとき

この1年のAI、量子技術、サイバーリスク、
インフラの制約から見てきた、
企業経営の次なる時代

クリス・ラブジョイ (Kris Lovejoy)

ストラテジー グローバル責任者、キンドリル



はじめに

2025年、私はテクノロジーリスクの次の局面は、単一の画期的な技術やプラットフォーム、あるいは脅威アクターによって決まるものではないと論じました。それを特徴づけるのは「融合」です。すなわち、AIが業務上のインフラとなり、量子技術が科学的な可能性から戦略的なリスクへと変化し、データセンターがエネルギーや水資源の制約に直面し、デジタルシステムが現実世界へとさらに深く入り込んでいくということです。

それから12か月を経て振り返ってみると、この見立てはおおむね正しかったといえます。テクノロジー戦略はもはや資本戦略、地政学戦略、人材戦略、サステナビリティ戦略、オペレーショナルレジリエンスと切り離して考えることはできません。最も優れた業績を上げている企業は、この「融合」を最も適切に管理している企業です。

この新しい時代が本格的に始まるなか、次のテクノロジーの変革期は、企業が「テクノロジー変革で最も難しいのは技術そのものではなく、それをいかに統制するかである」と気づき始めることで生まれる連鎖的な影響によって形作られていくでしょう。

第一部：2025年の予測を振り返る

予測は、後から事実にもとづいて検証してこそ意味があります。テクノロジーの未来予測では、後から検証されることを前提とした分析よりも、自信に満ちた大胆な主張が評価されがちです。しかし、より規律ある検証では、次の3つの問いを立てる必要があります。「予測したトレンドは実際に起きたのか」、「想定した時期に起きたのか」、そして、「当初の見立ては、適切な戦略的示唆を導き出していたのか」という問いです。

この観点から振り返ると、的中したものもあれば、見直すべき点もあり、多くの示唆を含んでいます。企業のテクノロジーリスクが、よりシステム全体に及び、より物理的なものとなり、政策や経済と一層密接に絡み合うようになるという見方は、おおむね正しかったといえます。また、AIが生産性と脅威の進行速度の双方を加速させるという点も予測どおりでした。一方、予測の精度が十分でなかったのは、その変化がどのような形で現れるかという点です。一部のリスクは、個別の大きな衝撃としてではなく、予算超過、許認可の遅延、インフラ不足、ガバナンスの欠如、新たな依存関係といった、事業運営上の制約として現れました。

この違いは重要です。以下の評価は、予測が当たったことを誇示するためでも、間違いを認めるためだけのものでもありません。新たな予測を示す前に、重要なシグナルとノイズを見極めるための試みです。

評価

2025年の5つの予測を評価すると、3つは方向性が正しく、想定より早く進展しました。1つは依然として可能性はあるものの、まだ立証されていません。そしてもう1つは、テーマとしては正しかったものの、捉え方が狭すぎました。重要な教訓は、重心が「テクノロジーの導入」から「テクノロジーがもたらす結果」へと移ったということです。



01 自律化する攻撃者 評価:おおむね的中、 想定より早く進展

- 予測したこと:
AIを活用したサイバー攻撃は、エンド・ツー・エンドの自律化へ向かい、2027年までに企業に大きな影響を及ぼす。
- 実際に起きたこと:
予測はおおむね正しく、想定より早く進展しました。AIを活用して実行されるサイバー攻撃に関する公表情報を見ると、攻撃者はおもはや、助言を得る、フィッシングメールを作成する、コードを生成するといった用途だけにAIを利用しているわけではありません。偵察、脆弱性の発見、攻撃の実行、ラテラルムーブメント（ネットワーク内での横展開）、認証情報の窃取、データ分析など、一連の攻撃プロセスでエージェンティックAIの能力を使い始めています。
- 見直すとなれば:
「完全に自律化した攻撃」か「人間主導の攻撃」か、という二分法で捉えるべきではありません。より重要なリスクは、戦術的な実行主体が人間から機械へと段階的に移っていることです。部分的な自律化であっても、速度、規模、持続性が高まることで、攻撃者側のコスト構造や攻撃効率は大きく変わります。
- リーダーへの示唆:
人間の対応速度を前提とした検知、チケットのトリアージ、手作業による対応を中心に構築されたセキュリティ運用モデルでは、今後ますます攻撃に追いつけなくなります。企業には、防御の自動化、AIを活用した一連の攻撃を想定した攻撃者シミュレーション、そしてID、API、ソフトウェアパイプラインが機械の速度で悪用されることを前提とした統制が必要です。



02 大きな変化に直面する サイバーセキュリティ人材 評価:可能性はあるが、 まだ立証されていない

- 予測したこと:
テクノロジー人材を取り巻く経済環境の変化により、一部の高度なスキルを持つ人材がサイバー犯罪へと流れ、ランサムウェアやサイバー犯罪組織の巧妙化が進む。
- 実際に起きたこと:
テクノロジー業界の労働市場をめぐる大きな前提には、依然として一定の妥当性がありますが、その前提と実際の変化との因果関係を証明することは困難です。サイバー犯罪は、より専門化、自動化され、サービスや製品のように組織的に提供される傾向が強まっています。しかし、その変化を技術者の失業や人材流動化と直接結び付けるには、現時点で利用可能な証拠だけでは不十分であり、より強力な裏付けが必要です。
- 見直すとなれば:
人材の移動ではなく、「能力の拡散」という観点から捉え直します。より重要なのは、高度なツール、クラウドネイティブの手法、AIコーディング支援ツール、商用レベルの運用モデルを、より幅広い攻撃者が利用できるようになっていることです。
- リーダーへの示唆:
企業は、高度な人材を組織内に抱えていなくても、攻撃者が高性能な自動化ツールやソフトウェアエンジニアリング手法、さらにはカスタマーサービスまで備えた犯罪インフラを利用できる世界を前提に、脅威モデルを見直す必要があります。

03 地政学的な「スプリンターネット」 評価:的中したが、影響を過小評価

- 予測したこと:
データローカライゼーションとデジタル主権が、経済的な影響力を高める手段となり、地政学的な競争にも利用される。
- 実際に起きたこと:
この予測は正しかったものの、その影響は想定より広範囲に及んでいます。主権はもはや、法的要件やデータの保存場所だけの問題ではありません。アーキテクチャー設計の原則、調達基準、市場参入の条件、さらには国境を越えたテクノロジーをめぐる関係における交渉材料にもなりつつあります。
- 見直すとなれば:
私は「スプリンターネット」という捉え方を、「デジタル主権を重視した運用環境」へと広げます。企業が直面しているのは、単に分断されたインターネットへの対応ではありません。各国・地域がデータ、コンピューティング、ID、クラウド運用、AIガバナンスを自国内・域内で管理するよう求めるなか、企業はそれぞれ異なる規制や要件に対応しながら、複数の法域にまたがって事業を展開しています。
- リーダーへの示唆:
地政学的な分析を、より上流のITアーキテクチャーを設計する段階から組み込む必要があります。データの保存場所、モデルのトレーニング、サポート時のアクセス権限、暗号化、クラウドのコントロールプレーン(管理基盤)、事業継続性は、もはや実装時の細かな検討事項として扱うことはできません。

04 暗号技術に迫る量子の脅威 評価:方向性は正しいが、 長期的な課題

- 予測したこと:
「今収集し、後で解読する(HNDL: harvest now, decrypt later)」攻撃のリスクを踏まえ、企業は、現在の暗号方式を脅かす能力を持つ量子コンピューターが公に実証されるよりもはるかに前から、量子対応を戦略的なセキュリティ課題として捉えるようになる。
- 実際に起きたこと:
この予測は方向性として引き続き正しいと考えます。公に認められるようなブレークスルーはまだ起きていませんが、暗号技術の移行の難しさはより明確になっています。耐量子暗号(PQC)は、もはや学術的な議論にとどまるテーマではありません。現在使用している暗号技術の棚卸し、ベンダーへの依存、組み込みシステム、ID基盤、規制対象データ、長期にわたって保護すべき機密情報など、企業全体に関わる長期的な移行の課題となっています。
- 見直すとすれば:
量子コンピューターによって暗号が解読可能になる「時期」よりも、移行に要する「期間」に焦点を当てるべきでした。リスクは、明日突然、量子コンピューターによって暗号が破られることではありません。企業が、自社のどこで暗号技術が使われているのかを把握するまでに時間をかけすぎることです。
- リーダーへの示唆:
暗号技術に対する俊敏性は、単なるセキュリティパッチではなく、予算を確保した全社的な変革プログラムとして扱う必要があります。取締役会は経営陣に対し、現在使用している暗号技術を継続的に把握し、重要性の高いデータを優先したうえで、ベンダーの製品ロードマップや規制当局の要件と連動した移行計画を策定するよう求めるべきです。

05 電力網の脆弱性 評価:的中し、 今や取締役会レベルの課題に

- 予測したこと:
データセンターの拡大、AIワークロード、老朽化したエネルギーインフラといった状況が重なり合うことで、ハイパースケーラーのインフラに依存する企業にとっては、可用性とレジリエンスのリスクになる。
- 実際に起きたこと:
この予測は的中し、想定より早く進展しました。電力供給力、送電網への接続に要する期間、水使用量、冷却要件、変圧器不足、地域社会からの反対などが、AIインフラ拡大の制約となっています。ボトルネックは、意欲や資本から物理的なインフラへと移っています。
- 見直すとすれば:
これは「電力網の脆弱性」ではなく、「デジタル戦略の物理化」と表現した方が適切です。デジタルの成長は今や、電力、水、土地、許認可、サプライチェーン、そして地域社会からの支持に左右されます。
- リーダーへの示唆:
クラウドとAIの戦略に、物理的資源へのリスクを組み込む必要があります。ベンダー選定時の比較・検討では、電力調達、水使用量、地域の許認可リスク、電力網への依存、サステナビリティへのコミットメント、供給能力が制限された場合の緊急時対応計画まで確認すべきです。



第二部：今後12カ月を方向づける テクノロジートレンド

今後12カ月は、まったく新しいテクノロジーを発見するというよりも、すでに導入されたテクノロジーがもたらす影響に対応する期間となるでしょう。AIは試行段階から運用モデルへと移行します。量子技術は将来のケイパビリティであり続ける一方、今対応すべきガバナンス上の課題となります。データセンターは、政治・環境の両面で議論の焦点となるでしょう。ロボティクスや自律システムによって、サイバーリスクは物理的なリスクへと変わります。そして企業は、テクノロジー変革で最も難しいのは「発明」ではなく「統制」であることに気づくでしょう。

トレンド 1: AIは「試行・検証」から「経済規律」へ

生成AIの第一段階では、探索的な取り組みを前提に投資が行われていました。企業は、長期的な戦略価値によって初期投資が正当化されるとの期待から、パイロット、生産性向上に向けた試行・検証、コーディング支援ツール、概念実証(PoC)などを進めてきました。

今、その段階は終わろうとしています。AIは今や、継続的に発生する運用コストとなり、事業運営上の依存度も高まり、場合によっては予算変動の要因にもなっています。

ここでの経済的な問題は、トークンの利用にはコストがかかるということだけではありません。エージェントックAIが「消費」の性質を変えることにあります。1回のユーザーリクエストが、計画立案、ツールの呼び出し、情報の検索、再試行、モデル間のやり取り、コード実行、検証ループなどのプロセスを次々に引き起こす可能性があります。企業からはたった1回のビジネス上のやり取りに見えても、その背後では、何十回、何百回ものモデル処理が実行されているのです。

トークンの消費に加えて、最近、議論になっているのが「オープンウェイトモデル」です。これは、AIの利用をすべて「従量課金制」サービスで行うべきか、という問いを投げかけるもので、戦略的な検討が必要です。議論のポイントが、「どれだけのトークンが必要か」から、「必要な成果に基づき、このワークロードに最も効率的なモデルは何か」へと移行しているのです。

これにより、新たな管理手法である「AI FinOps」が必要になります。

従来のクラウドFinOpsは比較的成本を可視化しやすく、帰属先も特定しやすいインフラ単位を基準に設計されていました。AIの消費はもっと流動的です。アプリケーションに組み込まれていたり、エージェントによって起動されたり、ワークフローの中に隠れていたり、あるいは従業員が正式な調達プロセスを経ずに利用するツールから発生する場合もあります。そのため、単位当たりの経済性は改善しても、総支出が増加する可能性があります。

予測: 今後12カ月以内に、少なくとも大企業の1社が、AIの利用コストが測定可能な価値創出を上回ったことを理由に、AIプログラムの見直しを公表するでしょう。こうした事態を回避したい企業は、エージェントックワークフローを広範に展開する前に、トークン利用のリアルタイムな可視化、複数モデルの適切なルーティング、セマンティックキャッシング、そして明確な価値測定指標を確立することになります。

トレンド 2: 企業内にガバナンスの 及ばないAI資産群が生まれる

従業員がAIで多くのことを試行するなか、最大のリスクは、企業の監視やガバナンスが及ばないエージェント、コパイロット、ローコードの自動化、スクリプト、プラグイン、モデルとの接続、AI搭載アプリケーションといった新たなAI資産群が生じることです。

この資産群は、シャドーITとはひとつ決定的な違いがあります。多くのAI搭載システムは、単に情報を保存したり、定型的なワークフローを自動化したりするだけではありません。状況を踏まえて推論し、データを取得し、APIを呼び出し、認証情報を使用し、取引を開始し、コードを生成し、他のエージェントと対話することもできるのです。それは企業環境の中で実際にアクションを実行する「主体」といえます。しかし、キンドリルの最近の調査によると、「自社環境で運用するすべてのAIを一元的に登録し、監視している」と回答した経営層は、わずか27%でした。

こうしたガバナンスの欠如は、リーダーが本来なら容易に答えられるはずの基本的な問いを投げかけた時に明らかになります。たとえば、「どんなエージェントが存在するのか」、「誰が責任を持っているのか」、「どのデータにアクセスできるのか」、「どのようなアクションを取ることができるのか」、「どのモデルに依存しているのか」、「今も必要とされているのか」、「想定外の動きをした場合、何が起きるのか」などです。

従来のソフトウェア資産群	新たなAIエージェント資産群
アプリケーションは通常、正式なプロセスを通じて登録、責任が決められ、導入される。	エージェントや自動化は、事業部門、開発者、またはベンダーによって、短期間で作成される場合がある。
動作は、ほぼ確定的で、事前定義されたワークフローの範囲内に限定される。	動作は、プロンプト、文脈、ツール、モデルのアウトプット、エージェント間のやりとりによって変わる場合がある。
コストとリスクは、一般にインフラ、ライセンス、アプリケーションオーナーを通じて可視化される。	コストとリスクが、トークン消費、APIの呼び出し、認証情報、自律的な実行経路に隠れる場合がある。

予測: 今後12カ月以内に、企業で重大な影響を及ぼすインシデントが発生し、その原因は基盤モデルの欠陥ではなく、未登録あるいはガバナンスの不十分なAIワークフローにあることが判明するでしょう。このインシデントを契機に、企業全体のエージェントやAI対応アプリケーションを検出、登録、保護、監視し、不要になったものを廃止するためのガバナンス基盤、すなわち「エンタープライズAIコントロールプレーン」への需要が高まるでしょう。

トレンド 3: デジタル成長は物理的資源の制約を受ける

AIブームによって、「**デジタルインフラは物理的インフラである**」という以前からある事実が改めて浮き彫りになりました。AIモデルにはデータセンターが必要であり、データセンターには、電力、水、土地、冷却設備、変圧器、変電所、光ファイバー、専門技能を持つ人材、許認可、そして地域社会の理解と支持が必要です。AI導入の制約は、アイデアや資本ではなく、クラウドを支える物理的なインフラへと移りつつあります。

これによって、企業のテクノロジー調達方法も変わります。企業はかつて電力事業者や環境担当部門、地方自治体が扱っていたような問いを、これからは企業のバイヤーがクラウドやAIプロバイダーに投げかけるようになるでしょう。「設備はどこにあるのか」、「電力源は何か」、「その地域は、送電網の混雑、水不足、許認可の遅れ、地域社会からの反対といったリスクにどの程度さらされているのか」、「地域的な電力や水の供給制限やインフラ整備の遅延が生じた場合でも、プロバイダーは契約上のサービスを維持できるのか」といった問いです。

企業は今後、インフラが地域社会から受け入れられるかどうかを、戦略上の重要な判断要素として捉える必要があります。また、事業を継続するには、地域社会の理解と支持が重要になります。データセンターを、税収を生み出す存在と捉える地域社会は、その拡張を支持するかもしれません。一方、電気料金の上昇、水不足、土地利用をめぐる対立の要因になると考える地域社会は、拡張に反対する可能性があります。

予測: 今後12カ月以内に、企業のクラウドおよびAIの調達判断には、電力供給、水の使用効率、地域の許認可リスク、プロバイダーが事業を行うための社会的受容性に関する明確な評価が必要になってくるでしょう。こうした基準は、従来サステナビリティ報告書に記載されていたものですが、今後は調達時の評価項目として扱われるようになるでしょう。

トレンド 4: 量子技術はコンピューティング上の利点をもたらす前に、ガバナンス上の課題となる

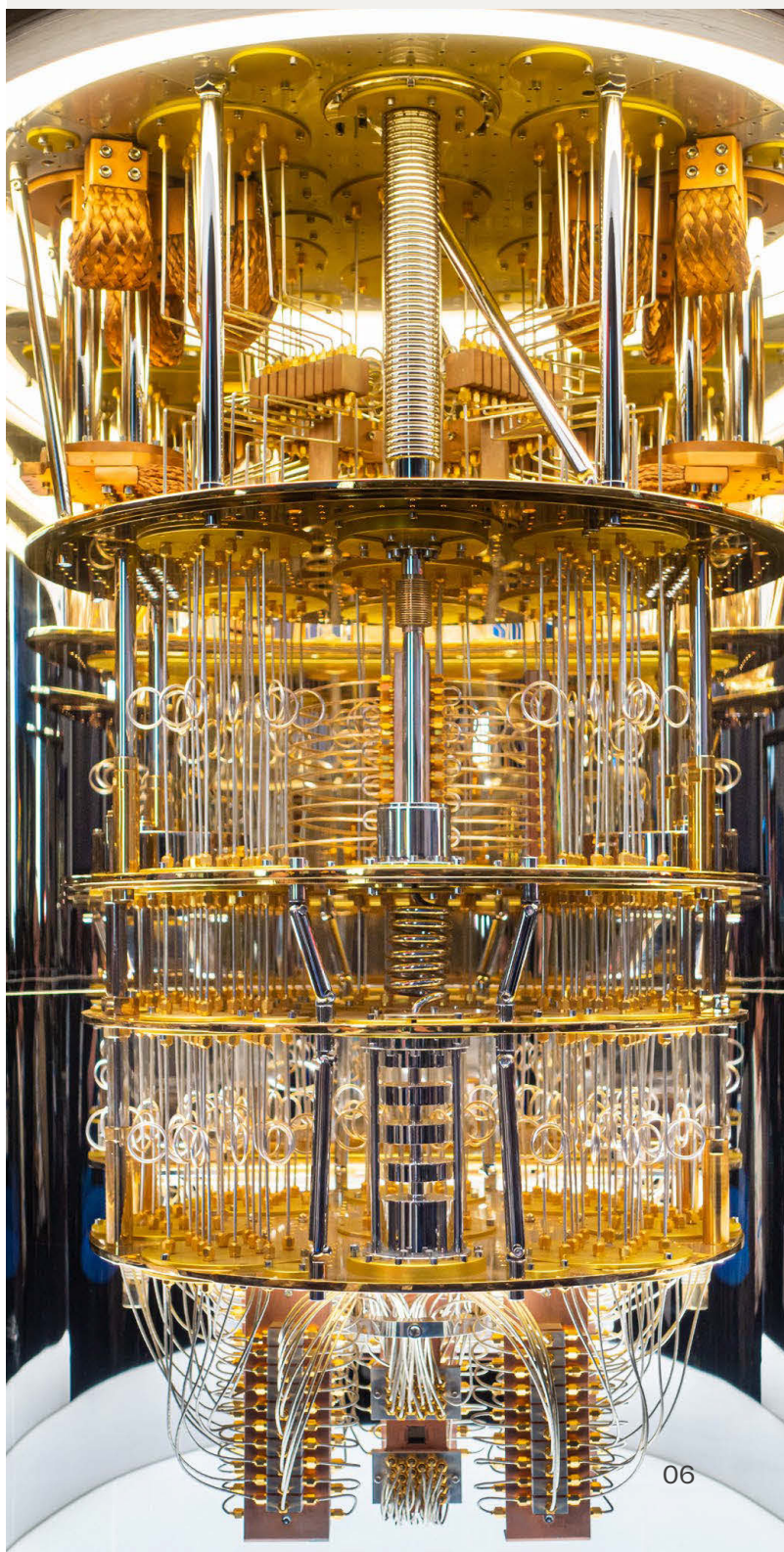
量子コンピューティングは今後1年の最も重要なテクノロジートレンドであり続けるでしょう。しかし、当面の課題はガバナンスです。

組織は、暗号技術に関する前提が変化し、最適化技術が進歩し、さらには業界特有の量子コンピューティング活用事例が研究段階から実際の業務プロセスへの導入段階へ移行していく未来に備える必要があります。

量子技術の劇的な進展が起きるまで、対応を先送りにすべきではありません。暗号技術は、アプリケーション、デバイス、証明書、ID管理システム、ネットワークプロトコル、サードパーティー製品、組み込みシステム、バックアップ、アーカイブ、長期保存が必要な規制対象データセットなど、企業内のあらゆるところに使用されています。そのため、新たな暗号技術への移行には時間がかかります。多くの企業は、脆弱性のある暗号技術が、自社のどこで使われているかをまだ把握できていません。

同時に、量子技術は競争戦略にとってはますます重要になってきます。製薬、材料科学、金融サービス、物流、エネルギー、先端製造業などの業界では、今後も量子技術と古典的なコンピューティング技術を組み合わせたハイブリッド方式の模索が続くでしょう。先行者利益は、現在の暗号方式を脅かす能力を持つ量子コンピューターを保有することから生まれるとは限りません。むしろ、価値の高い活用事例に関するデータ、ワークフロー、人材、知的財産を保有することから生まれる可能性があります。

予測: 今後12カ月の間に、先進的な企業は量子技術導入の準備を二本立てで行うようになるでしょう。一つは、耐量子暗号の移行を主眼とするもの、もうひとつは量子コンピューティングと、量子と古典コンピューティングを組み合わせたハイブリッド型の活用事例を通じてビジネス価値を見出すものです。前者はリスク低減策として、後者は将来の選択肢を創出する取り組みとして推進されます。



第三部:経営層が取り組むべき課題

この1年で得られた教訓は、リーダーがテクノロジーに対してより慎重になるべきだということではありません。より規律を持って取り組むべきだということです。AI、量子技術、自動化、クラウドインフラから最大限の恩恵を得るのは、それらを適切に管理するためのマネジメントシステムを構築した企業です。経営層が取り組むべき5つの課題を以下に示します。



1. AIをツール群としてではなく、オペレーティングモデルとして扱う

AIガバナンスは、単にモデルの承認や利用規定だけではなく、さらに広範囲にわたります。仕事のあり方をどう変えるか、エージェントワークフローに誰が責任を持つのか、価値をどう測定するのか、実行中にどのように制御するのか、例外にどう対応するのかを定義する必要があります。

- AIツールだけでなく、AIを活用したワークフロー全体の責任者を明確にする。
- パイロット単位ではなく、業務プロセス単位で価値を測定する。
- データアクセス、ツールの利用、モデルの選択、エスカレーションに関する実行時の統制を必須とする。



2. エージェントワークフローを大規模展開する前にAI FinOpsを確立する

AI導入が加速する前に、AIの経済性を可視化しておく必要があります。財務、テクノロジー、調達、リスク管理、ならびに事業の責任者は、トークン消費量、複数モデルのルーティング、価値の実現、例外管理を共通して把握する仕組みが必要となります。

- ワークフロー、責任者、モデル、事業成果ごとにトークン消費量を追跡調査する。
- マルチモデルルーティングを使用し、単純な日常業務に最も高価なフロンティアモデルが初期設定として使われないようにする。
- セマンティックキャッシング、コンテキストの適切な管理、利用制限を適用し、無駄を削減する。



3. 企業向けAIコントロールプレーンを構築する

企業には、エージェント、コパイロット、AIを活用したアプリケーション、モデル接続、ツールの権限、データの利用権限、ライフサイクルの状況などを一元的に管理する棚卸しが必要です。この棚卸しがなければ、リーダーはリスク、コスト、説明責任を管理できません。

- すべてのエージェントとAI活用ワークフローを登録し、責任者を明確にする。
- 各エージェントを、データへのアクセス、アクション権限、依存するモデル、業務上の重要度に基づいて分類する。
- 異常な動作、ポリシー違反、トークンの過剰消費、不要になったまま残存している権限などを監視する。



4. 物理的資源への依存とリスクをデジタル戦略に組み込む

取締役会や経営陣は、今後のテクノロジー戦略において、それを支える物理的なインフラ資産も含めて検討する必要があります。クラウドリジョン、AI処理能力、データセンターパートナー、エッジ環境などについては、電力供給、水資源、許認可、そして地域社会への影響やリスクといった観点から評価すべきです。

- クラウドとAIベンダーのデューデリジェンスに、地域のエネルギーと水資源への依存とリスクを含める。
- 供給能力の制限や許認可の遅延に関する緊急時対応計画を、プロバイダーに求める。
- サステナビリティへのコミットメントを、AIの成長を支えるために必要なインフラと整合させる。



5. 量子技術への備えを複数年の取り組みとして予算化する

量子技術への備えは、緊急の課題が危機へと発展する前に、計画的に進めておく必要があります。まずは、現在使用している暗号技術のどこにリスクがあるのか、また将来、量子技術がどの事業領域で競争優位につながる可能性があるのかを把握することです。

- アプリケーション、インフラ、製品、サードパーティーへの依存関係全体にわたる公開鍵暗号の一覧を最新に保つ。
- 長期保存が必要なデータ、規制対象データ、戦略的に機密性の高いデータの移行を優先する。
- 早期の学習によって、持続的な競争優位性を生み出すことのできる業界固有の量子技術の活用事例を特定する。

成功するリーダーは、すべてのトレンドを完璧に予測できる人ではありません。迅速に学び、慎重にガバナンスを行い、意図を持って投資し、予測が変わった時に適応できる組織を構築する人です。その意味で、今後1年のテクノロジー課題は、テクノロジー自体の進化以上に、それを管理する仕組みを十分な速さで進化させられるかどうかにかかっています。



kyndryl.

© Copyright Kyndryl Inc. 2026

Kyndryl は、米国もしくはその他の国における Kyndryl Inc. の商標または登録商標です。他の製品名およびサービス名等は、それぞれ Kyndryl Inc. または他社の商標である場合があります。

本書および本書に含まれる情報は、情報提供およびKyndrylのマーケティング活動を目的としてのみ提供されるものであり、助言または推奨として依拠されるべきものではありません。