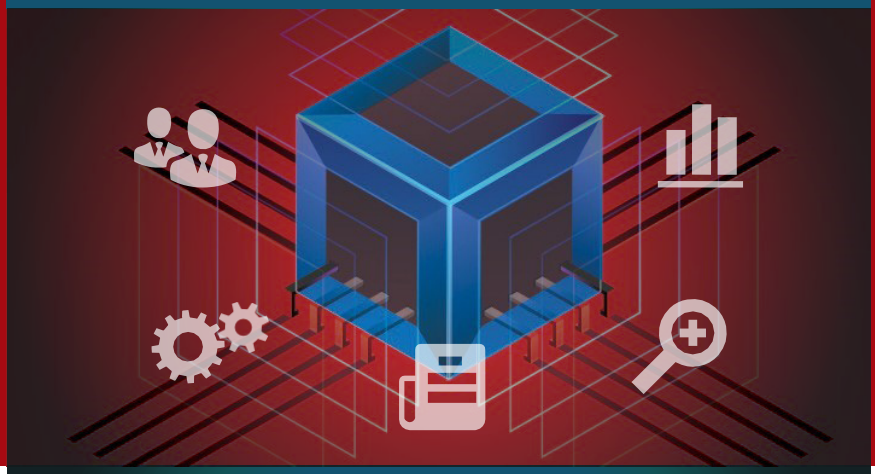
COSO

トレッドウェイ委員会支援組織委員会

全社的リスクマネジメント



人工知能の可能性を最大限に実現する

ＣＯＳＯフレームワークと原則を適用した人工知能の導入と拡張の支援

デロイト社

ケリー・カラーニャ | ブライアン・キャシディ | エイミー・パーク

2021 年 9 月

著　者

デロイト＆トウシュ社
リスク・ファイナンシャル
アドバイザリー部門プリンシパル
ケリー・カラーニャ

デロイト＆トウシュ社
監査・保証部門パートナー
ブライアン・キャシディ

デロイト＆トウシュ社
監査・保証部門パートナー
エイミー・パーク

謝　辞

本稿の作成に当たり、技術的なご意見や助言をいただいたデロイト＆トウシュ社のシニアマネージャー ジョン・フォガティ氏、マネージャーのヘマン・デンガン氏、シニアマネージャーのメアリー・シュミードリン氏およびマネージングディレクターのエドワード・ボーウェン氏に謝意を表したい。

ＣＯＳＯ理事会は、デロイト＆トウシュ社の支援に感謝する。

トレッドウェイ委員会支援組織委員会（ＣＯＳＯ）理事

序　文

本プロジェクトは、トレッドウェイ委員会支援組織委員会（ＣＯＳＯ）から委嘱されたものである。ＣＯＳＯは、組織のパフォーマンスや監督を改善するとともに、組織における不正を減らすために立案された内部統制、全社的リスクマネジメントおよび不正抑止に関する包括的なフレームワークとガイダンスの開発を通じて先進的な考え方を提供することに取り組んでいる。ＣＯＳＯは、次の団体の協賛と資金提供によって運営されている民間部門主導の団体である。

米国会計学会（American Accounting Association）

米国公認会計士協会（American Institute of Certified Public Accountants）

国際財務担当経営者協会（Financial Executives International）

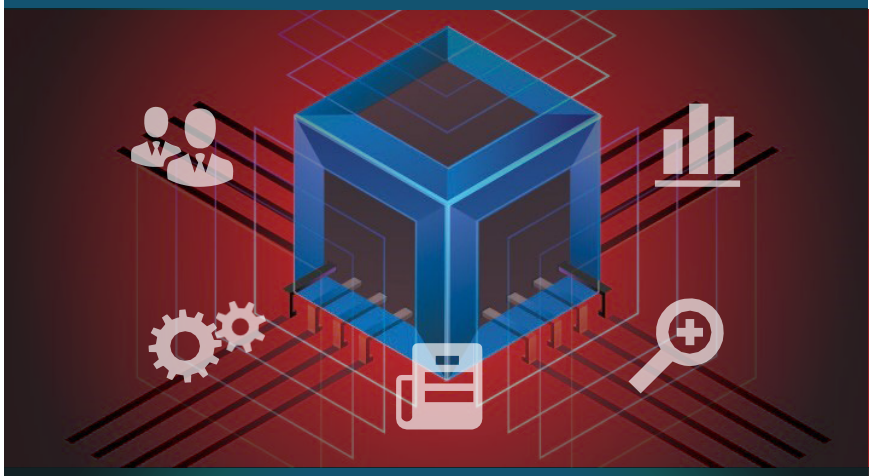
管理会計士協会（Institute of Management Accountants）

内部監査人協会（Institute of Internal Auditors）

COSO
トレッドウェイ委員会
支援組織委員会

coso.org

全社的リスクマネジメント



人工知能の可能性を最大限に実現する

ＣＯＳＯフレームワークと原則を適用した人工知能の導入と拡張の支援

調査委嘱者

COSO

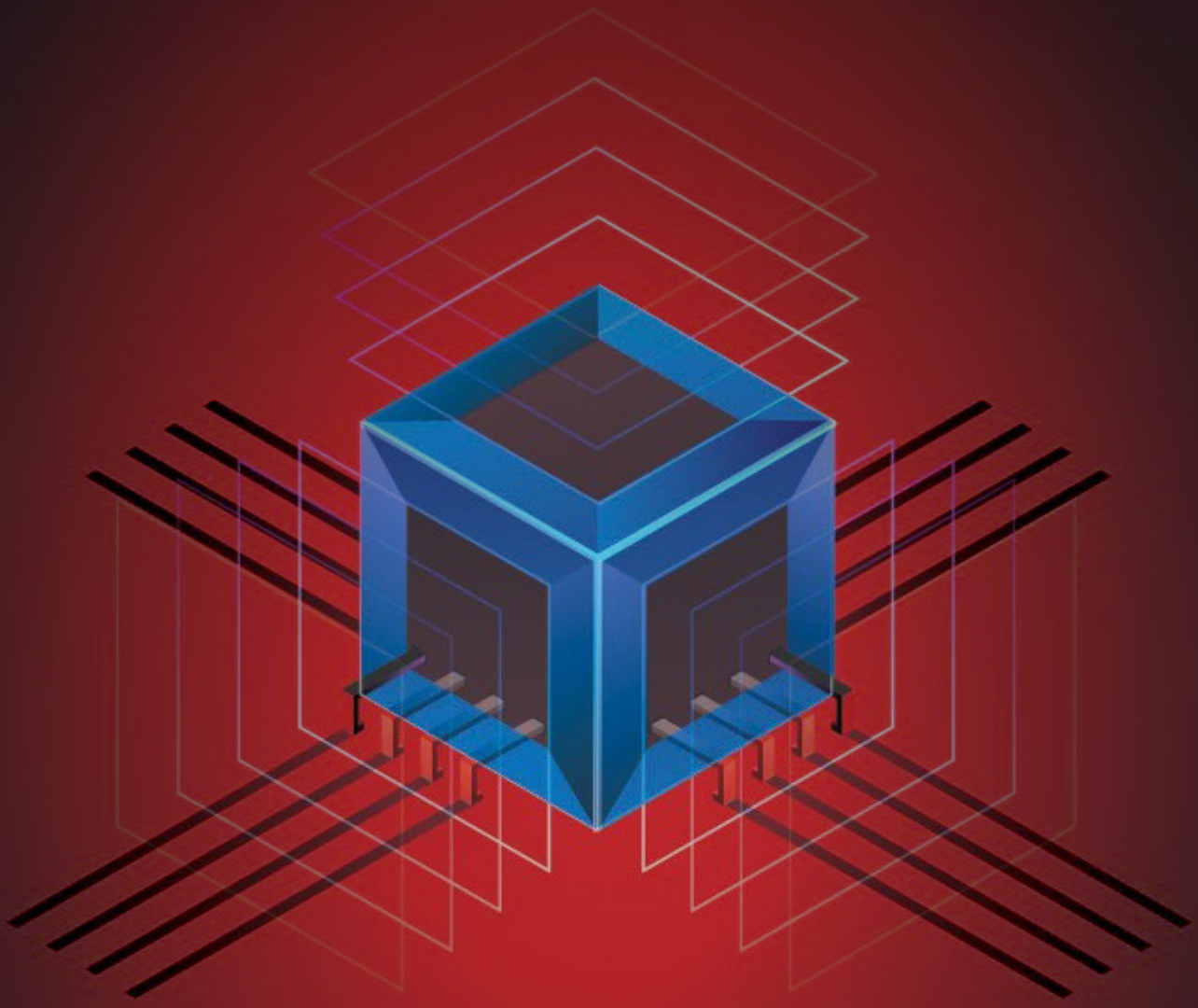
トレッドウェイ委員会支援組織委員会

2021 年 9 月

Design and production: Sergio Analco.

coso.org

目　次



はじめに

人工知能（ＡＩ）は、事業戦略、ソリューションおよび業務を変革しており、今後も変革し続けるであろう。組織がＡＩアプリケーションを採用して拡張し、ＡＩの可能性を最大限に実現するためには、ＡＩ関連のリスクを最優先に考えて重要な優先事項とする必要がある。全社的リスクマネジメント（ＥＲＭ）の原則をＡＩ施策に適用することで、組織はＡＩの統合的なガバナンスを確立し、リスクを管理し、戦略目標の達成を最大化するためのパフォーマンスを向上させることができる。５つの構成要素と 20 の原則からなるＣＯＳＯ ＥＲＭフレームワークは、総合的かつ包括的なフレームワークを提供し、リスクマネジメントとＡＩの戦略およびパフォーマンスを整合させ、ＡＩの可能性が実現できる。

図１.『ＣＯＳＯ 全社的リスクマネジメント―戦略およびパフォーマンスとの統合』

出典：2017 *COSO Enterprise Risk Management – Integrating with Strategy and Performance*（邦訳は、一般社団法人日本内部監査協会・八田進二・橋本　尚・堀江正之・神林比洋雄監訳、日本内部統制研究学会ＣＯＳＯ - ＥＲＭ研究会訳『ＣＯＳＯ全社的リスクマネジメント－戦略およびパフォーマンスとの統合』、同文舘出版、2018 年）

ＡＩ革命：ビジネスとイノベーションの変革

ＡＩは現代生活のほぼすべての面に拡大しており、ビジネス上必要な能力になりつつある。顧客との関係管理、サイバー脅威の識別と対応、あるいは医療診断の支援など、ＡＩは幅広い経営課題に取り組んでいる。ＡＩの急速な普及により、組織のデータに対する知見が高まり、それが意思決定を支援するインテリジェンスとなる。そのため、組織はＡＩ施策に大規模な投資を行うようになった。ＡＩへの支出は、2020 年の 501 億ドルから 2024 年には 1,100 億ドル超へと倍増すると予測されている。この期間の複利の年平均成長率（ＣＡＧＲ）は約 20%と予測されている[1]。さらに、ソフトウェア、ハードウェアおよびサービスを含むＡＩ市場の全世界の収益は、2021 年に 3,275 億ドル、2024 年には 5 年間のＣＡＧＲは 17.5%で 5,543 億ドルに達すると予測されている[2]。

何が変革を促しているのだろうか。組織は、ビジネスプロセス、タスクおよび動作を自動化して、コストを削減し、効率を上げ、結果の予測可能性を向上させるために、変革の可能性を求めてＡＩを適用している。ＡＩによって、より優れたデータの知見が得られ、より多くの情報に基づいた経営判断、事業や業務の好結果およびイノベーションの拡大につながっている。

組織はどのようにＡＩを利用して価値を高めているか

コスト削減
ＡＩを利用して、業務プロセス、タスクおよびやり取りを知的に自動化することで、コストを削減し、効率を高め、予測可能性を向上させる。

実行の加速
ＡＩを利用して遅延を最小限に抑えることで、業務や事業の成果を得るまでの時間を加速させる。

予測分析
ＡＩを利用して組織のデータに対する知見をもたらし、複雑さを増すデータソースからパターンを解読し、点と点を結びつけ、結果を予測することで、理解と意思決定を向上させる。

デジタルとの関わり方
ＡＩを利用して、音声、視覚、文字およびタッチといった操作手段を拡大することで、人間とスマートシステムとの関わり方を変える。

イノベーションの加速
ＡＩを利用して、新製品や新規市場の機会と新たなビジネスモデルのための知見を創出する。

最近の調査によると、組織はＡＩへの短期的な投資によって、これらのメリットを活用する方向に進んでいる。

- 回答者の 75%が、2024 年末までにＡＩの試験運用から実用化へと移行すると予測している[3]。
- 調査対象ＡＩ導入企業の 75%が、３年以内に組織が変革すると予測している[4]。
- 調査対象ＡＩ導入企業の 61%が、同じ期間内に業界が変革すると予測している[5]。
- 調査対象ＡＩ導入企業は多額の投資を行っており、53%がＡＩ関連のテクノロジーと人材に 2020 年に 2,000 万ドル以上を投じている[6]。
- 調査対象ＡＩ導入企業の 71%が、来年度の投資を平均 26%増加させると予測している[7]。

[1] International Data Corporation (IDC), "Worldwide Spending on Artificial Intelligence is Expected to Double in Four Years, Reaching $110 Billion in 2024, According to New IDC Spending Guide," August 25, 2020. https://www.idc.com/getdoc.jsp?containerId=prUS46794720（訳注：翻訳時点の 2022 年 8 月にはこのサイトは見つからなかった。）

[2] International Data Corporation (IDC), "IDC Forecasts Improved Growth for Global AI Market in 2021," February 23, 2021. https://www.idc.com/getdoc.jsp?containerId=prUS47482321（訳注：翻訳時点の 2022 年 8 月にはこのサイトは見つからなかった。）

[3] Gartner, Accelerating AI Deployments – Paths of Least Resistance, July 2020.

[4] Deloitte, State of AI in the Enterprise, 3rd Edition, 2020. Figure 2, page 7.（邦訳は、次の URL からダウンロード可。デロイト「グローバルＡＩ活用企業動向調査 2020」https://www2.deloitte.com/jp/ja/pages/technology-media-and-telecommunications/articles/et/state-of-ai-2020.html）

[5] 前掲、８頁、図 1-2。

[6] 前掲、７頁。

[7] 前掲、７頁。

組織や業界の変革を視野に入れて、多くの企業が事業戦略の転換に向けてＡＩ機能に投資をしている。一部の金融テクノロジー企業が従来のＦＩＣＯスコア[i]から脱却し、ＡＩを活用した複数のパラメータやモデルを用いて融資審査を行っているように、ＡＩがビジネスモデルを下支えしているケースもある。このプロセスは自動化されているため、取り組みが効率化され、さらなる審査が必要な事案にはユーザに警告が出される。意思決定が改善され、既存のサービスや顧客の体験を向上させる可能性がある。

ＡＩと機械学習：実用的な導入

ＡＩに関連するリスクを適切に識別して管理するためには、ＡＩに関連するアルゴリズムとその構築方法についての理解が不可欠である。実際には、ＡＩは人間がソフトウェアプログラミング（コード）を使って開発するものである。財務報告やソフトウェア開発において人的要素があるためにガバナンスや統制が必要であるのと同様に、組織にはＡＩに対するガバナンスや統制も必要である。しかし、ＡＩが何を行い、どのように構築されるかについて、取締役会や経営幹部[ii]に基本的な理解がなければ、効果的に統制のモニタリングを支援することはできない。

アルゴリズムが行うこと

機械学習のアルゴリズムには、非深層学習、深層学習および強化学習の３つの一般的な分類がある。これらのＡＩモデルのゴールは、分類、予測または新規データの生成である。

- **非深層学習は、分類、パターンの発見および結果の予測を行う。**一般的なモデルには、回帰、クラスタリング、決定木（ディシジョンツリー）およびサポートベクターマシン[iii]などがある。これらのモデルは、需要予測、クロスセリング傾向およびリスク分類など、多くの有用かつ一般的な問題を解決するのに役立つ。
- **深層学習アルゴリズムは、ゲームチェンジャーとなった。**分類と予測を行うこれらの手法は、過去 10 年のＡＩ革命を牽引してきた。画像処理、自然言語処理および異常検出は、ディープニューラルネットワークを使用して最先端の結果を達成した。ウェブサイト上で顧客サービスをナビゲートしてくれる会話型ボットは、このＡＩテクノロジーから生まれたものである。単純な自動化は、携帯電話の音声の文字起こしなど、より広範囲に適用できるし、データを活用して手書きの文字を認識して変換することも可能である。
- **強化学習モデル**は、環境を調査し、最適なプラスの経路を見つけることを目的とした一連の決定を行う能力を開発する。このようなモデルは、チェスや囲碁のトーナメントで人間の名人に勝つための学習ができる。実用的な応用例には、経路の最適化、工場の最適化およびサイバー脆弱性テストなどがある。

アルゴリズムの構築方法

すべてのアルゴリズムは、事業戦略とリンクすべきである。アルゴリズムは、意図した事業価値を生み出すための情報に基づいた意思決定に寄与するように、人間によって設計される。機械学習モデルの構築には、６つの重要なステップがある。

1. **問題定義－**ビジネス上の問題と、それを機械学習で解決する方法を考える。
2. **データプロファイリング－**問題解決に必要なデータソースと、必要な追加データを特定する。ＡＩにおける新たな傾向として、ＡＩのパフォーマンスを向上させることのみを目的とした新しいセンサーの開発とデータ収集が挙げられる。組織は、データが倫理とパフォーマンスの観点から公正でバランスが取れていることを確認する必要がある。
3. **データの準備－**データの変換、正規化およびクレンジングに必要なものを決定し、テストと検証のアプローチを作成する。
4. **アルゴリズムの評価－**問題解決に必要なアルゴリズムを選択するために、先進事例を活用する。多くの場合、データサイエンスチームは複数のアルゴリズムを並行して開発し、最もパフォーマンスの良いモデルを決定する。その際、正しいパフォーマンス評価規準を設定することが重要である。
5. **モデルの開発－**特定されたすべてのアルゴリズムをデータで研修、テストおよび検証し、正則化のようなアプローチを導入する。
6. **モデルの展開、モニタリングおよび保守－**機械学習業務（ＭＬＯｐｓ）およびモニタリング構造を、モデルドリフト[iv]に対応するプロセスとともに組み込む。環境内の活動が時間とともに変化すると、モデルのパフォーマンスが低下する可能性がある（例えば、電力消費を予測するモデルは、ソーラーパネルが消費者に普及するにつれて、時間の経過とともに更新する必要がある）。

---

[i] 訳注：米国で広く利用されているクレジットスコア（個人のデータを収集し、数値化して、個人の信用度合いを明示的にしたもの）。ＦＩＣＯスコアでは、借入金残高、クレジットカード使用状況、返済、支払の状況などといった情報を基にして、300 点から 850 点の数値で個人の信用度を表現する。

[ii] 本稿では、「senior management」「executive management」「senior executive」「top executive」「senior leadership」「leadership」「leaders」「executive」を経営幹部と訳し、「management」を経営者と訳した。

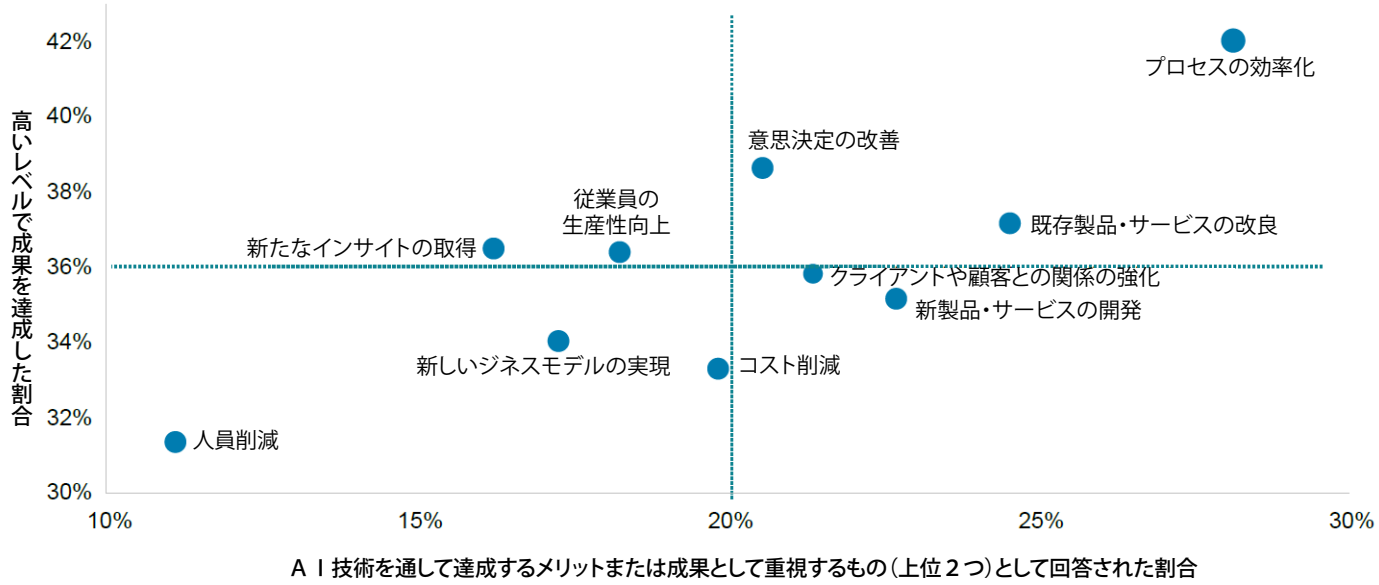
[iii] 訳注：教師あり学習による２クラス分類の機械学習手法のこと。

[iv] 訳注：何らかの「予期せぬ変化」によって、モデルの予測性能が時間経過とともに劣化していくこと。

ＡＩは素晴らしい世界を提供する ... 不幸な結末を迎えるまでは

ＡＩと機械学習の導入が進む中、調査対象ＡＩ導入企業が挙げる導入効果の上位２つは、プロセスの効率化と既存製品・サービスの改良である（図２参照）。また、ガートナー社の調査によると、組織がＡＩ機能に投資する理由の上位２つは、収益増加やコスト削減の達成と、競合他社や新興企業に対する脆弱性への対応である[8]。

図２．ＡＩ導入により改善される企業活動



青い点線は各項目の平均値

出典：*State of AI in the Enterprise, 3rd Edition, Deloitte*

ＡＩは、データを利用して予測や提案を行い、分類を生成し、新しい構造を考案するコンピュータ・アルゴリズムによって効率化を推進する。今日導入されている多くのＡＩユースケースは、人間ができることをより速くより効率的に行っている。ＡＩは人間が感知できない微妙なニュアンスを感知できるため、今後 10 年間は、人間ができないことをＡＩに実行させることに重点が置かれるようになりそうである。例えば、製薬会社では、人間の科学者が検知できない顕微鏡画像のニュアンスをＡＩで解釈することができる。この大規模な画像ベースの細胞プロファイリングにより、健康な細胞と病気の細胞の大規模なデータセットの違いを迅速に把握し、病気を治療するための特異性の高い新薬の化合物が設計できる。理論的には、研究者は目で見て比較できるが、わずかだが一定の違いがある何千もの細胞を比較することは、ＡＩを使用しなければ非常に難しい。要するに、ＡＩは変革的なイノベーションを推進している。こうした傾向は、今後さらに加速したり進化したりする可能性がある。

ＡＩはビジネス変革の万能薬のように思われるが、そのテクノロジーと適用には、組織に深刻な問題をもたらすリスクがないわけではない。それらのリスクは、ＣＯＳＯ ＥＲＭフレームワークを慎重に先手を打って検討することで軽減が可能である。しかし、まず、リスクについて説明する。ＡＩ関連のリスクは多岐にわたり、以下のようなものがあるが、これらに限定されるものではない。

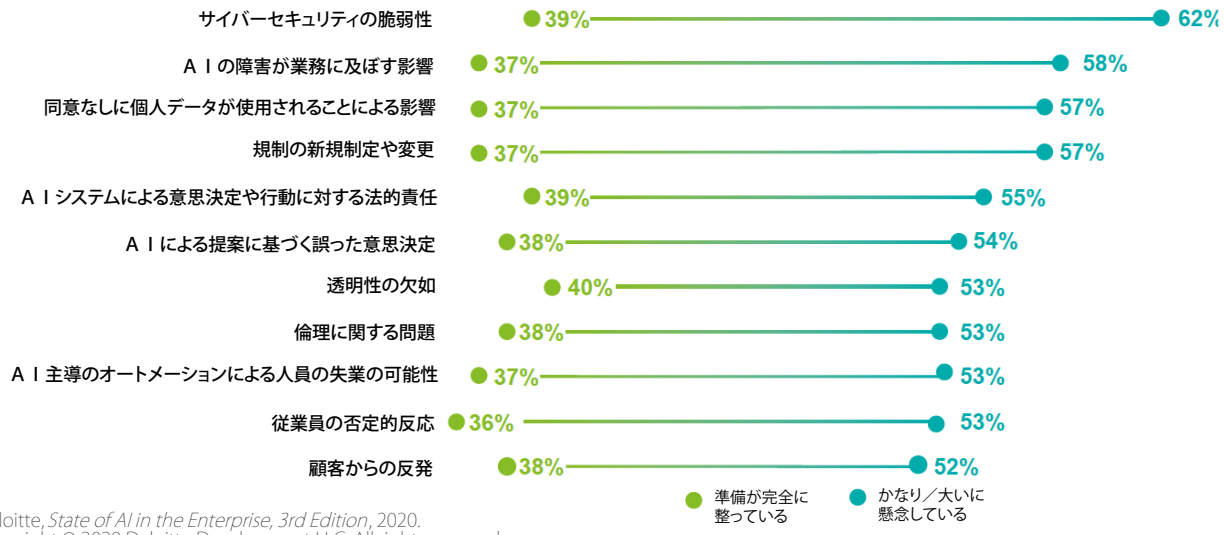
- 不適切または典型的でないデータによるバイアスや信頼性の破綻
- ＡＩモデルからのアウトプットの理解不足や説明不足
- データの不適切な使用
- データの入手やＡＩモデルの操作を目的とした敵対的な攻撃に対する脆弱性
- ＡＩテクノロジーの急速な適用と変革による社会的ストレス

[8] 2019 Gartner, AI in Organizations Survey. 735439_C.

これらのリスクによる潜在的な影響には、風評被害、株主価値の毀損、規制当局の罰金および訴訟などの可能性がある。このような新たなリスクが生じるため、調査対象ＡＩ導入企業の 56%が、自らの組織はＡＩテクノロジーの導入を遅らせていると回答している[9]。しかし、組織が競争力を維持しようとするならば、それは長くは続かない可能性がある。ブレーキを踏むよりも関連するリスクをより適切に管理することが、より賢明な戦略かもしれない。組織はＡＩのリスクや予期せぬ結果を無視することはできない。

デロイト社の「グローバルＡＩ活用企業動向調査」では、ＡＩの導入企業や採用企業は、バイアスの他にもさまざまなリスク領域にまたがるＡＩの活用について、深刻な懸念を抱いていることが示されている（図３参照）。さらに、この調査の回答者は、これらの懸念に対応するための組織の現在の能力に大きなギャップがあると指摘している。ガートナー社が実施した別の調査結果では、ＡＩ導入の障壁として、セキュリティやプライバシーに関する懸念と、ＡＩソリューションと既存インフラとの統合の複雑性を上位に挙げている[10]。

図３．ＡＩ関連リスクへの懸念と準備の比較



出典：Deloitte, *State of AI in the Enterprise, 3rd Edition*, 2020.

（邦訳は、デロイト「グローバルＡＩ活用企業動向調査 2020」）

規制の不確実性の影響

規制要件も重要な検討事項であるが、規制の遵守とは、現在の法律に従うだけでなく、将来必要となり得る安全なＡＩ実務へのコミットメントを示すことを意味する。組織は、ＡＩと関連データに関するガバナンスのフレームワークを評価する際に、懸案となっている規制要件の適用範囲を検討すべきである。

図４．法規制の遵守

プレーヤーの例	基準、方針および法令の例	
	規制の例	ビジネスへの影響
世界経済フォーラム「ＡＩとロボティクスの未来」協議会	製造物責任法は、ＡＩ搭載製品を使用した際に負傷した個人に適用される	企業は人間の社員と同じようにＡＩをモニタリングしなければならない（デジタルは完全無欠ではない）
ＡＩ NOWイニシアティブ	不法行為法修正条項は、ＡＩの設計・製造の欠陥および警告の不履行に関するものである	ＡＩを搭載した製品の警告ラベルの作成には特に注意しなければならず、例えば、「この製品はＡＩで監査された」など
スタンフォード大学のＡＩに関する 100 年研究	公正な信用報告法およびＡＩ談合に対する公正取引委員会の取締り	ＡＩの手法に透明性がなければ意図しない結論に至る可能性があるため、企業には強力な統制が必要
マサチューセッツ工科大学メディアラボ、ＡＩ、倫理およびガバナンスプロジェクト	ＥＵで業務を行っている米国企業に影響を与えるＥＵ一般データ保護規則	企業は最も規制の厳しい市場でも期待に応えられるようなＡＩに関する方針を設計する必要がある
ＡＩに関するパートナーシップ	言論法がボットと人間とのコミュニケーションに適用された	会話型ＡＩのユースケースについては、言論法を組み込むために、特別な統制を導入しなければならない
データ＆ソサエティのインテリジェンスとオートノミーイニシアティブ	ニュースボットを規制する「2018 年ボッドの開示と説明責任に関する法律（Bot Disclosure and Accountability Act of 2018）」を制定	ソーシャルメディアボットはすでにＡＩで業務を行っていることの開示が必要、今後の規制はソーシャルボットにとどまらない可能性がある
人工知能および自律システムの倫理的課題について検討する米国電気電子技術者協会のグローバルイニシアティブ		
ケンブリッジ大学生存リスク研究センター		

[9] 前掲、「グローバルＡＩ活用企業動向調査 2020」、14 頁。
[10] 2019 Gartner, AI in Organizations Survey. 729419_C.

ＣＯＳＯ ＥＲＭフレームワーク：総合的な事業戦略やＩＴ戦略と整合したＡＩリスクへの対応

ＡＩがビジネスや日常生活に浸透するに従い、組織はもはやＡＩ導入に伴う特有のリスクを無視したり回避したりする選択肢を持たなくなりそうである。それどころか、これらのリスクを効果的に認識して管理することを学ばなければならない。この問題をさらに深刻にしているのは、ＡＩがＩＴなどの特定の機能に限定されず、むしろ組織内の複数の機能に影響を及ぼすことが多いという事実である。組織は、人間がＡＩと協働する可能性を実現するために、ガバナンス、リスクマネジメントおよび統制の戦略と構造を設計して導入する必要がある。幸い、ＡＩは組織の他のテクノロジー要素と同様に、効果的なＥＲＭによってうまく管理できる。

1985 年以来、民間の任意団体であるトレッドウェイ委員会支援組織委員会（ＣＯＳＯ）は、内部統制、リスクマネジメント、ガバナンスおよび不正抑止を強化するソートリーダーシップを発揮して、組織のパフォーマンス向上を支援することに注力している。2017 年に改訂されたＣＯＳＯ ＥＲＭフレームワークの最新版では、次の５つの重要な構成要素において、このフレームワークを組織全体に定着させることの重要性を強調している。

- ガバナンスとカルチャー
- 戦略と目標設定
- パフォーマンス
- レビューと修正
- 情報、伝達および報告

図５．『ＣＯＳＯ 全社的リスクマネジメント―戦略およびパフォーマンスとの統合』フレームワーク

ガバナンスとカルチャー

1. 取締役会によるリスク監視を行う
2. 業務構造を確立する
3. 望ましいカルチャーを定義づける
4. コアバリューに対するコミットメントを表明する
5. 有能な人材を惹きつけ、育成し、保持する

戦略と目標設定

6. 事業環境を分析する
7. リスク選好を定義する
8. 代替戦略を評価する
9. 事業目標を組み立てる

パフォーマンス

10. リスクを識別する
11. リスクの重大度を価する
12. リスクの優先順位けをする
13. リスク対応を実施する
14. ポートフォリオの視点を策定する

レビューと修正

15. 重大な変化を評価する
16. リスクとパフォーマンスをレビューする
17. 全社的リスクマネジメントの改善を追求する

情報、伝達および報告

18. 情報とテクノロジーを有効活用する
19. リスク情報を伝達する
20. リスク、カルチャーおよびパフォーマンスについて報告する

出典：2017 *COSO Enterprise Risk Management – Integrating with Strategy and Performance*（邦訳は、『COSO 全社的リスクマネジメント―戦略およびパフォーマンスとの統合』）

ＣＯＳＯ ＥＲＭフレームワークを活用することで、組織はＡＩ特有のリスクを識別して管理し、意図せぬバイアスや透明性の欠如といったリスクへのエクスポージャーを管理しながら結果を最適化するための実務が確立できる。フレームワークの導入によって、組織内外のステークホルダーの信頼を向上させ、ＡＩ関連の新たなリスクに先見的に対応できるようになる。

ガバナンスとカルチャー

ガバナンスとカルチャーは、ともにリスクマネジメントの全構成要素の基礎を形成している。ガバナンスはＥＲＭの重要性を強調し、カルチャーは組織内の全階層での意思決定に反映される。ＣＯＳＯ ＥＲＭフレームワークによると、ガバナンスとカルチャーという構成要素には、組織のビジョン、ミッションおよびコアバリューに対する組織のコミットメントが組み込まれなければならない。コアバリューは、組織の戦略と事業目標の達成を支援するために、ＡＩ施策やＡＩモデルを適切に監督するための重要な基盤となる。ＣＯＳＯ ＥＲＭフレームワークの「ガバナンスとカルチャー」の構成要素と以下の原則は、本稿のこの章の基礎となるものである。

1. **取締役会によるリスク監視を行う**
2. **業務構造を確立する**
3. **望ましいカルチャーを定義づける**
4. **コアバリューに対するコミットメントを表明する**
5. **有能な人材を惹きつけ、育成し、保持する**

組織の取締役会は、ＡＩ施策に関与していないことが多く、また、経営者に適切なリスク関連の質問ができるほどＡＩを十分に理解していない場合もある。経営幹部や取締役がＡＩとその意味を理解して積極的に関与すれば、リスクマネジメントの重要性についてトップが姿勢を示すことになる。そのような関与は不可欠である。

調査対象ＡＩ導入企業のうち、ＡＩ関連のリスク管理を１人の経営幹部が担当する体制を取っているのは約 26％に過ぎない[11]。事業の他の中核的要素と同様に、取締役はＡＩ施策に関連するリスクを評価するために組織が用いるフレームワークを理解し、経営幹部による監督が必要なリスクの閾値を判断する必要がある。施策の中には、少数の単純なＡＩモデルに限られ、リスクプロファイルの低いものがあるかもしれない。しかし、複雑なＡＩモデルが多数存在する場合や、患者への医療の提供、顧客の安全確保または製造活動の統制のような重要な事業活動に関わる場合は、リスクプロファイルが高くなる。リスクの高いＡＩ施策は、最高リスク管理責任者[v]または同等のリスク管理責任者と連携する経営幹部による徹底した監督が求められる。組織は、ＡＩ施策を適切に監督するためにＡＩ開発やデータ分析に精通した人材を獲得するか、必要なスキルセットが組織内にない場合は、関連する経験を持つ外部のアドバイザーに依頼する必要があるかもしれない。これらの人材は、取締役会に助言し、リスクと見返りに関する知見をもたらし、リスク情報に基づく意思決定を促進することができる。このような関与は、ＡＩの効果的な採用や導入と、組織にとって危機的な出来事の防止に不可欠である。

ガバナンスの重要性

ＡＩが組織内でより広範に導入されるようになると、ＡＩ施策や関連モデルを適切に監督するために、ガバナンスが重要な役割を担うようになる。組織は、ＡＩに対する監督が不十分であると認識されていることもあり、さまざまなステークホルダー（例えば、規制当局、顧客、ユーザなど）からの厳しい監視に直面している。

ガバナンスは、以下の主要な領域で重要な役割を果たす。

1. ＡＩモデルの開発と運用を支援するために、組織はかつてないほどの量のデータを収集している。調査参加者は、自分のデータがどのように使用されているのか、他の誰が自分のデータにアクセスできるのか、などの懸念を持っている。組織は、データの使用、収集、保持およびアクセスに関して明確な規則を設け、これらの懸念への対応の一環として、組織全体で一貫してこれらの規則を適用する必要がある。これらの問題に適切に対応できなければ、人々に害を与えたり企業の評判や株主価値を損ねたりすることになりかねない。
2. 組織では、より多くの判断を必要とし、参加者に大きな影響を与える可能性がある状況にＡＩを適用することが増えている。参加者に大きな影響を与える重要な判断（例えば、引受判断、各種給付の受給資格、医療診断および推奨治療など）を実行または通知するＡＩモデルには、倫理的な問題が生じる可能性がある。組織は対応の一環として、ＡＩがいつ、どこで、どのように使用されるか、または使用される予定か、また、そのような使用が組織の価値観や設計と整合しているか、さらに、必要に応じて、組織の監督機構がより大きな社会的関心事にどのように関わっているかを評価する必要がある。

[11] 前掲、「グローバルＡＩ活用企業動向調査 2020」、16 頁、図 1-9 の平均に基づく。

[v] 訳注：本稿では、「Chief Risk Officer」を「最高リスク管理責任者」と訳した。

さらに、経営幹部は、ＡＩの開発、導入、モニタリングおよび保守を行う際に、成功をどのように定義し、それが企業の目的とどのように関連するかを理解する必要がある。成功を定義する上で重要なのは、どの測定基準や評価基準が最も適切かを判断することと、組織が費用対効果をどのように識別して評価するかという点である。これらの側面は、行動に対する説明責任を強化し、リスクを意識した行動と意思決定をパフォーマンスに合わせるための基礎を提供することにより、ＡＩ施策を組織のコアバリューへの幅広いコミットメントと結びつけるような経営を行うことに密接に結びついている。そのため、組織には、アルゴリズムの目的や組織のニーズとゴールを文書化するための厳格で統制のとれたプロセスが必要である。これは、組織のＡＩアーキテクチャ文書や関連するソフトウェア開発プロセスに含めるべきである。

経営幹部や取締役のための明確な見通しとともに、基盤となるデータのガバナンスは、効果的なＥＲＭフレームワークの鍵となる。導入を成功させるためには、組織はＡＩを開発するために必要なデータを評価しなければならない。ＡＩアルゴリズムは、データを使用して学習し、新規モデルを作成する。モデルが新しいデータを受け取ると、将来の結果を予測する。コアバリューから導き出される、データガバナンスに必要な検討事項には、１）ＡＩのユースケースに適した母集団の代表とバイアスの低減、２）データ収集においてプライバシーだけでなく使用と廃棄の開示など、データの使用と配付に関する明確な規則、３）データ資産を保護する方法、などがある。

ＡＩとそれを機能させるモデルもまた、組織全体で徹底してモニタリングしなければならない。ＡＩの設計と導入において、６つの重要な側面は、倫理を守り、人々が受け入れることのできる、企業にとって信頼できるＡＩ戦略を構築する一助となり得る。現在、ＡＩの倫理に関する権威あるフレームワークはないが、デロイト社の「信頼できるＡＩフレームワーク（Trustworthy AI™ Framework）」は、ＡＩに特有のリスクや倫理的配慮を理解して評価する手段となり、特にガバナンスとパフォーマンスに関連するＣＯＳＯ ＥＲＭフレームワークを補完する貴重なレンズとなり得る。組織は、これを継続的なリスクの判断とモニタリングに役立てることができる。

図６．デロイト社の「信頼できるＡＩ™フレームワーク」

デロイト社の「信頼できるＡＩフレームワーク」（図６参照）には、以下が含まれている。

- **公正不偏－**ＡＩシステムが、全参加者に対する公正な適用を可能にするのに役立つ内部と外部のチェックを含んでいるかを評価する。
- **透明性と説明可能性－**参加者が、自分のデータがどのように使用され、ＡＩシステムがどのように意思決定を行うかを理解できるようにする。アルゴリズム、属性および相関関係は自由に検証できる。
- **責任と説明責任－**ＡＩシステムの判断のアウトプットの責任を誰が負うかを明確に判断できるような組織構造と方針を確立する。
- **堅牢性と信頼性－**ＡＩシステムが、一貫性があり信頼できる結果を生み出すために、人間や他のシステムから学習する能力を備えていることを確認する。
- **プライバシー－**データのプライバシーを尊重し、意図した用途や明示された用途以外に顧客データを活用するためにＡＩを使用することを回避する。顧客がデータの共有についてオプトイン[vi]またはオプトアウト[vii]できるようにする。
- **安全かつ確実－**ＡＩシステムを、物理的およびデジタル的な損害を引き起こす可能性のある（サイバーリスクを含む）リスクから保護する。

考慮すべきポイント

- 組織には、統合されたＡＩガバナンスプログラムがあるか。
- ＡＩの導入において倫理的配慮はどのように織り込まれているか。ＡＩの継続的なモニタリングを管理する最高倫理責任者を置くべきか。
- 組織には、全社的なＡＩ施策に関連するリスクに対応するための最高リスク管理責任者、最高データ責任者または同等のリスク責任者がいるか。
- 取締役会には、テクノロジーやＡＩの専門家がいるか。
- ＡＩの導入や導入後の変更について、取締役会レベルでどのような承認や協議が行われているか。

[vi] 訳注：加入や参加、許諾、承認などの意思を相手方に示すこと。個人が企業などに対し、電子メールなどのメッセージの送信や、個人情報の収集や利用などを承諾する手続きを指すことが多い

[vii] 訳注：企業が個人に行うさまざまな活動や措置、行為などに対し、対象者がこれを拒否したり、（登録などの）解除・脱退、（情報などの）抹消などを申し出たりすること。

戦略と目標設定

すべての組織は、自らのミッションとビジョンを実現し、価値を高めるための戦略を持っている。組織はＥＲＭを戦略設定と統合させ、組織の戦略と事業目標に関連するリスクプロファイルに対する知見を得るべきである。ＣＯＳＯ ＥＲＭフレームワークの「戦略と目標設定」の構成要素と以下の原則は、本章の基礎となるものである。

6. **事業環境を分析する**
7. **リスク選好を定義する**
8. **代替戦略を評価する**
9. **事業目標を組み立てる**

組織は、ＡＩに関連する戦略と事業目標を確立すべきである。デロイト社の「2020 年最高戦略責任者調査（2020 Chief Strategy Officer Survey）」によると、回答者の 51%はＡＩが組織の戦略にとって重要であると回答しているが、組織にＡＩ関連の戦略を実行する能力があると感じているのは 17%であった[12]。事業と戦略の状況を理解すれば、組織の経営幹部はＡＩ施策のリスクに影響を与える内部と外部の要因が把握できる。重要な要素は、ＡＩと関連データの現在や将来の用途の分類と、ＡＩ使用に対する潜在的なエクスポージャーの評価である。

組織の価値観と整合しないＡＩモデルを使用すると、戦略目標が損なわれる可能性がある。組織がＡＩモデルを使用した結果、保護された特性（例えば、性別、人種など）に基づいて参加者の扱いが異なったり、不平等になったりするようなアウトプットが得られた例は数多く存在する。これらの事例は、ＡＩの開発と継続的なモニタリングの両方において、公正さと透明性に関連する問題の識別と対処に十分な焦点が当てられていないことを示唆している。

リスク選好を定義することで、組織はリスクの識別、評価および対応を事業戦略と整合させることができる。リスク選好の定義に関するより深い議論については、ＣＯＳＯの「リスク選好は成功に不可欠：変化する世界で成功するためにリスク選好を利用する（Risk Appetite - Critical to Success: Using Risk Appetite to Thrive in a Changing World）」を参照されたい[13]。リスク選好の策定においてさらに考慮すべきことは、同業他社とのベンチマーキングである。組織のリスク選好は、ＡＩに関連して、リスク情報に基づく意思決定を促進するための重要な考慮事項でもある。リスクを完全に取り除く方法はないため、組織はリスク選好を決定し、ＡＩへの投資を特定して評価する際にどの程度のリスクが許容されるかを評価しなければならない。リスクと見返りのバランスを考慮すべきである。ＡＩを導入した組織は、開発と導入に多大な投資を行っているため、ＡＩのリスクマネジメントをより広範なリスクマネジメントの取り組みと調和させなければならない。デロイト社の最新レポート「グローバルＡＩ活用企業動向調査」によると、調査対象ＡＩ導入ベテラン企業の 43%が、このような整合性を追求している[14]。

より低いリスクで成果を上げる

ＡＩは、組織に大きな効率と利益をもたらすことができる。組織は、さまざまな製造プロセスの部品をモニタリングするためにＡＩを使用している。例えば、製造業では、コンベヤーベルトが故障しそうな時期を予測するためにＡＩが使用できる。ベルトの現在の故障データを使用する代わりに、温度測定、ビデオカメラの映像およびその他の新しい変数を通じてＡＩを使用して故障箇所を特定し、有用なモデルを構築するための新しいデータが作成できる。学習データとモデル自体のデータは、製造業者のプロセスの効率化を促進するのに役立つ可能性がある。このＡＩの例は、リスクを低減した比較的一般的なＡＩの使用例を示している。

[12] Deloitte, 2020 Chief Strategy Officer Survey, a Monitor Deloitte and Kellogg School of Management study.

[13] Committee of Sponsoring Organizations of the Treadway Commission (COSO), "Risk Appetite - Critical to Success: Using Risk Appetite to Thrive in a Changing World," May 2020. https://www.coso.org/Shared% 20Documents/COSO-Guidance-Risk-Appetite-Critical-to-Success.pdf（訳注：原文に記載されていたＵＲＬは翻訳時点で存在しなかったが、こちらのＵＲＬが正しいと思われる。）

[14] 前掲、「グローバルＡＩ活用企業動向調査 2020」。（訳注：原文には Figure 2 on page 7 と記載されているが、Figure 9 on page 15（邦訳では、16 頁、図 1-9）が正しいと思われる。）

戦略策定とリスク選好の間の関係は、組織のリスク評価への重要なインプットである。リスク評価の情報に基づき、組織は識別されたリスクへの対応を決定する。組織の対応には、識別したリスクを管理するための統制活動（例えば、記録作成、ベンチマーキングおよび傾向分析）の設定を含めるべきである。導入後は、事業目標がより低いリスクで達成されたか否かを判断するために、成果を測定することが重要である。調査対象ＡＩ導入企業のうち、導入したすべてのＡＩの正式な記録を維持しているのは約 34%に過ぎない[15]。このような記録を維持しなければ、ＡＩのユースケースから生じる潜在的なリスクをモニタリングして評価することは難しい。

ＣＯＳＯ ＥＲＭフレームワークの重要な部分の１つであるリスク許容度の定義は、アルゴリズムのパフォーマンスを長期的にモニタリングするための、ＡＩに関する主要なパフォーマンス指標とリスク指標を設定するのに役立つ。アルゴリズムの開発中に主要なパフォーマンス指標とリスク指標および許容度を設定することは、信頼を明確にするためのパフォーマンスの基準値を作り上げるのに役立つ。このような指標の報告は、ステークホルダー間の透明性をもたらし、アルゴリズムのパフォーマンスと基礎となる入力データの完全性を向上させるのに役立つ可能性がある。

考慮すべきポイント

- 組織は、ＡＩプログラムにシナリオプランニングや仮定テストのような戦略的リスク評価手法を用いているか。
- ＡＩ機能は、新たなリスクを識別して、製品、サービスおよびブランドに関するステークホルダーのフィードバックを求めるために使われているか。
- ＡＩ施策は、リスクをモニタリングするためのリスクアナリティクスを支援しているか。
- ＡＩリスク評価は、各ＡＩユースケースに関連するリスクと見返りを考慮し、これらのバランスを実行・不実行の決定や関連するＡＩモデルの設計と目的の両方に織り込んでいるか。

[15] 前掲、16 頁、図 1-9 の平均に基づく。

パフォーマンス

リスクを識別し、評価し、対応することは、組織の戦略や事業目標の達成を支援するために行うべき重要な活動である。リスク、特にＡＩ関連のリスクは、さまざまな原因から発生するため、組織は組織全体と全階層でさまざまな対応を行う必要がある。ＣＯＳＯ ＥＲＭ フレームワークの「パフォーマンス」の構成要素と以下の原則は、本章の基礎となるものである。

10 **リスクを識別する**
11 **リスクの重大度を評価する**
12 **リスクの優先順位づけをする**
13 **リスク対応を実施する**
14 **ポートフォリオの視点を策定する**

組織は、信頼性に対応せずにＡＩアプリケーションを導入すべきではない。潜在的な価値を最大限に引き出すためには、信頼性の高いＡＩを念頭に置いてＡＩモデルを構築し、プライバシーを維持しつつ、ＡＩの堅牢性、信頼性、安全性およびセキュリティを高めるためのパフォーマンスに関する配慮を盛り込むべきである。

すべてのＡＩモデルのリスクプロファイルが同じであるとは限らない。組織は、それぞれのビジネスケースを強固にするためにリスク評価を行う必要がある。ＡＩ施策に関連するリスクの識別は、エクスポージャーの評価と、価値創造に向けたＡＩ導入拡大の機会の特定のためにも必要である。また、組織はＡＩモデルを評価することによってリスクに優先順位をつけ、関連するユースケースに必要な精度、信頼性および透明性のレベルを決定する必要もある。成功するために高いレベルの精度、信頼性または透明性を必要とするＡＩモデルは、より高いリスクプロファイルである可能性が高い。さらに、影響度の低い判断（例えば、次に再生する曲）を提案するために使用されるＡＩモデルは、これまで人間が行っていた判断（例えば、保険契約の引受条件の決定）を自動化するために使用されるＡＩモデルよりもリスクプロファイルが低い。

組織は、リスク対応を選択して展開する際に、リスクの重大性と優先順位ならびにＡＩモデルの事業環境、事業目標およびパフォーマンスのターゲットを考慮すべきである。ＡＩモデルに関連するリスク対応は、通常、以下のカテゴリーに分類される。

- **受容：**リスクの重大度を変える措置は講じない。この対応は、戦略や事業目標に対するリスクが、すでにリスク選好の範囲内に収まっている場合には適切である。組織のリスク選好から逸脱したリスクを経営者が受容しようとする場合、通常、取締役会やその他の監督機関の承認が必要となる。
- **回避：**ＡＩモデルを使用しない、ＡＩモデルの使用範囲を限定する、またはＡＩモデルの機能を変更して複雑性を抑制するなど、リスクを取り除くための措置を講じる。
- **活用：**パフォーマンスを向上させるために、リスクの増加を許容する措置を講じる。これには、ＡＩモデルの使用範囲を拡大したり、ＡＩモデルの機能を変更して複雑性を高めたりすることが含まれる場合がある。リスクを活用することを選択する場合、経営者は、容認できるリスク許容度の境界を超えないようにしつつ、望ましいパフォーマンスを達成するために必要な変更の性質と程度を理解する。
- **低減：**リスクの重大度を下げるための措置を講じる。これには、組織のリスクプロファイルとリスク選好に見合った許容レベルまで残存リスクを低減する、業務プロセスと統制の確立が含まれる。（ＡＩモデルに関連するリスクを低減するために組織がとり得る措置は、以下で説明する。）
- **共有：**リスクの一部を移転または共有することにより、リスクの重大度を下げるための措置を講じる。一般的な例としては、ＡＩモデルの開発、導入またはモニタリングを専門のサービスプロバイダに委託することが挙げられる。

ＡＩリスクを完全に回避するのは不可能であるが、リスクを低減するために組織がとり得る措置はある。１つは、開発や導入されたＡＩソリューションのテスト体制を構築し、ＡＩソリューションのライフサイクル全体にそのテスト体制を適用することである。調査対象ＡＩ導入企業の約40%は、現在、ＡＩ導入の内部監査とテストを実施している[16]。

人工知能は意図せぬ結果をもたらすことがある

アルゴリズムのパフォーマンスは、公正性、透明性および堅牢性を総合的に評価しなければならない。アルゴリズムがより多くのデータを取り込むことで、当初の戦略的意図から外れてしまう可能性がある。

- **公正不偏：**特定の集団にバイアスがないか、集団の差別的扱いが正当化されていないか、関連する集団を公正に代表しているか。
- **透明性と説明可能性：**モデルのアウトプットに影響を与える主な要因は何か、また、各インプット要因は結果にどのような影響を与えるか。
- **堅牢性と信頼性：**将来にわたってモデルが安定し、未知のデータに対してもうまく一般化できるか、あるいは、モデルが新しいデータを受け取ることによって将来的にバイアスが生じるリスクがあるか。

ＡＩモデルのパフォーマンスを評価する際の主要な活動は以下のとおりであるが、これらに限定されるものではない。

- **リスクレビュー**は、サイバーセキュリティ、データリスク、バイアスおよび倫理など、ＡＩ導入の成功という目標を妨げたり最適化を阻害したりする可能性のあるリスク要因を識別するのに役立つ。すべてのＡＩプロジェクトに関連するリスクのポートフォリオの視点は、経営幹部や取締役会とレビューすべきである。このレビューの重要な側面はリスク対応の実施であり、それぞれの対応と残存リスクのレベルは、リスク選好の定義に照らして慎重に評価すべきである。
- **データレビュー**は、データの品質と完全性およびＡＩモデルやその結果への影響を評価するのに役立つ。データレビューは、変数間の相関関係を特定するのにも役立つ。例えば、年齢および／または肥満度は、癌の発症と相関があるか。組織は基礎となるデータの多変量解析を行うことによって、アルゴリズムのインプットとして使用される可能性のあるバイアスの履歴ソースを特定することができる。
- **モデルレビュー**では、以下の作業で結果をテストする。
  1. アルゴリズムの機能形式とパラメータを分析し、意思決定プロセスで起こり得る問題点を理解する。
  2. 実データを用いたアルゴリズムのパフォーマンスの評価により、複雑な相関関係やその他の予期せぬ実世界のエラーソースから生じる隠れたバイアスをテストする。相関関係は、保護対象変数（例えば、性別、人種など）と、モデルで使用する保護対象変数の潜在的なプロキシとして機能する可能性がある変数の間の関連性の存在を識別するのに役立つため重要である。そのような関連性が存在する場合、モデルにはバイアスが含まれている可能性がある。統計的有意性は、これらの変数間の関連性が無作為の偶然によって引き起こされたものではないことを示す。
- **導入レビュー**は、ＡＩアルゴリズムが正しく動作していることを確認するのに役立つ。このレビューは、アルゴリズムが将来にわたって堅牢で、効果的かつ公正であり続けるかを評価し、潜在的なリスクを識別するのに役立つ。
- **導入後レビュー**では、アルゴリズムを繰り返し検証する。導入後も定期的にモデルのパフォーマンスと公正性を評価することが必要である。この評価には、モデルの基礎データと機能を継続的にテストするモニタリングの仕組みが必要だと考えられる。

ＡＩモデルがテスト環境外で動作する場合の問題点

ＡＩモデルのパフォーマンスとアウトプットのテストには、ＡＩモデルから得られる結果の信頼性を評価するために、予期しないデータや動作、あるいはデータ内の変更を考慮することが含まれる。ＡＩモデルの設計方法によっては、予期しないデータや動作、あるいはデータ内の変更の発生により、ＡＩモデルが不正確なアウトプットや有害なアウトプットを出したり、まったく機能しなくなったりする可能性がある。堅牢でなく信頼性のないＡＩモデルを導入した組織には、重大な結果がもたらされる可能性がある。

[16] 前掲、「グローバルＡＩ活用企業動向調査 2020」、16 頁、図 1-9 の平均に基づく。

ＡＩプログラムは、他のデータソースや企業と同様にハッキングされる可能性があることに留意してほしい。デロイト社の調査によると、回答者の 62%がサイバーセキュリティの脆弱性に大きな懸念を抱いているが、これらのリスクに対応しているのは 39%に過ぎない[17]。ＡＩアプリケーションと関連データの安全性とセキュリティ、つまり信頼できるＡＩの支柱を保つために、組織は、ＡＩモデルの監査可能性、透明性および再現性を可能にすべく、基になるバージョンの維持や、その後の各バージョンとそれに対する変更の追跡などのモデル・バージョン管理の方法を導入して維持しなければならない。データのバージョン管理の方法論が、その基礎を提供する。組織は、不正な変更や悪意のある変更を防止および検出するために、モデルやモデル内の基礎的なアルゴリズムを学習するために使用されるデータに関する予防的、発見的およびモニタリング的な統制を段階的に確立すべきである。これらのモデルの多くを動作させるためにはコンピューティング能力が必要なため、処理はクラウドで行われることから、第三者の信頼性とプライバシーに関する懸念も生じる。

さらに、個人データの安全な保持（暗号化、匿名化など）とデータの廃棄や、何を取得し、どのように使用し、どのように維持しているかというコミュニケーションに対応した方針が求められている。デロイト社の調査によると、回答者の 57%は同意なしに個人データを使用した場合の結果に大きな懸念を抱いているが、こうしたリスクに対応しているのは 37%に過ぎない[18]。プライバシーは、信頼できるＡＩを実現するための重要な支柱である。

さらなるレビューが必要な場合についてのルールを確立しなければならない。組織は、さらなる調査やより厳格なレビューが求められる欠陥、パフォーマンス指標および閾値を定義すべきである。これらのルールは、「パフォーマンス」に加えてＣＯＳＯ ＥＲＭフレームワークの「ガバナンスとカルチャー」と「戦略と目標設定」の構成要素も支える。主要なインプットには以下の項目が含まれるが、これらに限定されるものではない。

- ＡＩ施策や関連するＡＩモデルに対する、組織の（単に財務上や業務上だけでない）成功の定義
- その成功を達成するために識別されたリスク
- それらのリスクを管理するために設計され導入された統制

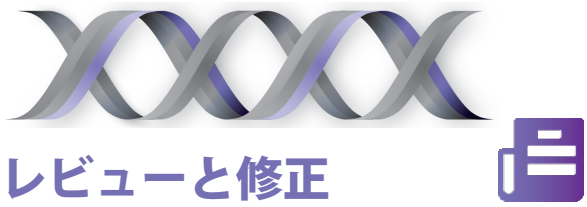
信頼できるＡＩの支柱の１つである責任と説明責任の一環として、組織は継続的な成功をモニタリングするプロセスを定めて実行する必要がある。また、成功が得られない場合の改善策も定めて実行すべきである。これらの活動には、具体的な責任者が必要である。責任者を補佐するために、モニタリングや上申を支援するために必要なアーキテクチャをＡＩプラットフォームに組み込むことができる。自動化によってモニタリングが容易になり、リアルタイムで指定された人にレビューを上申することができる。

考慮すべきポイント

- ＡＩモデルのパフォーマンスレビューには、結果を改善するためのリスクの評価と管理が含まれているか。
- ＡＩアプリケーションの主要なリスク指標とパフォーマンス指標は、エグゼクティブダッシュボード[viii]を通じてモニタリングされ、権限を与えられたデータ利用者に報告されているか。
- ＡＩアプリケーションと関連する業務が意図したとおりに運用され、意思決定のための正しい情報を生成していることに、どの程度の自信があるか。

[17] 前掲、「グローバルＡＩ活用企業動向調査 2020」、15 頁、図 1-8。
[18] 前掲、15 頁、図 1-8。

[viii] 訳注：会社のデータを整理し、図式化して表示するカスタマイズされたインターフェイスのことであり、特に経営幹部を意識してカスタマイズされている。



レビューと修正

刻々と変化する事業環境下では、組織の戦略や事業目標およびＥＲＭの実務や能力は、時とともに変化する可能性がある。特にＡＩの分野では、能力の変化と用途の拡大が進んでいるため、組織には、ＥＲＭの実務と能力を継続的に評価して必要に応じて修正することが求められる。ＣＯＳＯ ＥＲＭフレームワークの「レビューと修正」の構成要素と以下の原則は、本章の基礎となるものである。

15 **重大な変化を評価する**
16 **リスクとパフォーマンスをレビューする**
17 **全社的リスクマネジメントの改善を追求する**

本稿で前述したように、組織は次第にＡＩを採用するようになり、ＡＩへの投資による組織や業界全体の変革が期待されている。さらに、規制当局や政府は、ＡＩや関連データの利用に関わる追加的な規制を制定し、審議している。これらの進展は、ＡＩモデルの機能性を含む大幅な変化を引き起こし、新たなリスクや変化をもたらす可能性がある。このような進展は、戦略や事業目標の達成だけでなく、ＥＲＭにも影響を及ぼす可能性がある。ＥＲＭのいくつかの構成要素に影響を及ぼす可能性のある反復プロセスには、実質的な変化とその影響を特定し、それらの変化に対応することが含まれる。

ＥＲＭの実務と能力を、目標に対する組織のパフォーマンスと合わせてレビューすることで、組織は、ＡＩアプリケーションがどのように価値を高め、今後も高めるかをモニタリングできるようになる。経営者は、ＡＩや機械学習のアプリケーションをテストしてモニタリングすることによって、アプリケーションが意図したとおりに機能することを確認する必要がある。パフォーマンスとリスクの継続的なモニタリングは、ＡＩが意図した目標を達成しているかを評価し、リスク情報に基づく意思決定のサイクルを確立するのに役立つ。

ＡＩリスクの対象領域に対応するために、ＡＩモデルと関連する施策に焦点を当てたリスク分類法を開発すべきである。リスクマネジメントチームは、リスクの識別と評価の取り組みの指針となる分類法の開発を支援しなければならない。組織はＣＯＳＯ ＥＲＭフレームワークやその他のガイダンスを利用して、ＡＩ関連リスクの識別、評価、優先順位づけおよびモニタリングが支援できる。ＡＩモデルの目標達成度を評価することで、リスクマネジメントの価値を実証し、改善の機会が明らかにできる。

アルゴリズムは学習によって変化し、将来的に意図せぬ結果を生む可能性があるため、主要なパフォーマンス指標とリスク指標は長期的に維持することが重要である。さらに、どんなに優れたアルゴリズムであっても、バイアスや信頼性に関わる問題が発生する可能性はある。人種や性別など、個人を特定できる情報（ＰＩＩ）を単に省くだけでは十分でない場合もある。特に、アルゴリズムが使用するデータやデータの傾向は時間とともに変化するため、アルゴリズムの継続的なモニタリングとテストが必要である。

各ステークホルダーは、ＡＩアプリケーションとそのパフォーマンスのレビューと修正において、3 ラインモデル[ix]を使用して役割が果たせる。ＥＲＭの指導を受ける第１ラインは、ＡＩのリスク要因を先見的に識別して対応することができ、ＥＲＭ（第２ライン）は第１ラインと連携して、リスク評価を効果的、動的かつ実行可能なものにできる。また、ＥＲＭは第１ラインのステークホルダーとも連携し、洞察に満ちたリスクレポートと提言を経営幹部に提示できる。内部監査は、リスクベースのアプローチを用いて独立したレビュー者の役割を果たし、ビジネスパフォーマンスとリスクマネジメントのゴールについてＡＩアプリケーションを批判的に評価できる。

[ix] 訳注：原文は「The three lines of defense model」となっているが、内部監査人協会（ＩＩＡ）は 2020 年７月にこのモデルを改訂した「The IIA's Three Lines Model（ＩＩＡの３ラインモデル）」を公表している。邦訳は、『月刊監査研究』2020 年８月号（日本内部監査協会）掲載。

パフォーマンスのレビューとモニタリングを怠ると、深刻な問題が発生する可能性がある

例えば、医療機関では、病状の診断や医療上の助言を支援するために、ＡＩモデルの使用が増えてきている。医療機関や医療従事者がこれらのモデルのパフォーマンスを適切にモニタリングしない場合、ＡＩモデルが不正確な診断や医療上の助言を行ったケースを識別して修正することができない可能性がある。不正確な結果を識別して修正することができなければ、医療被害、患者の不安および関連するＡＩモデルの構築プロセスへの疑問を招きかねない。

考慮すべきポイント

- 組織は、すべてのＡＩプログラムに対してポートフォリオのレビューを行い、総体的なレベルでの相乗効果とリスクを理解しているか。
- 最高リスク管理責任者は、ＡＩのパフォーマンスレビューに参加してリスクマネジメントの視点を共有しているか。
- そのようなレビューで得られた発見事項は、肯定的なものも否定的なものも含めて経営幹部や取締役会と共有されているか。
- 経営幹部は、否定的な発見事項に対して適切な是正措置を講じているか。
- ＡＩモデルのリスク軽減計画を支援できる学際的なリスクマネジメントチームがあるか。

情報、伝達および報告

組織は、データのプライバシーやセキュリティおよび関連するＡＩモデルの透明性に対する懸念が高まる中、生成される膨大な量のデータの活用に継続的に取り組んでいる。このような環境では、組織が適切な情報を、適切な形式で、適切なレベルの詳細さで、適切な人に適時に提供することが重要である。ＣＯＳＯ ＥＲＭフレームワークの「情報、伝達および報告」の構成要素と以下の原則は、本章の基礎となるものである。

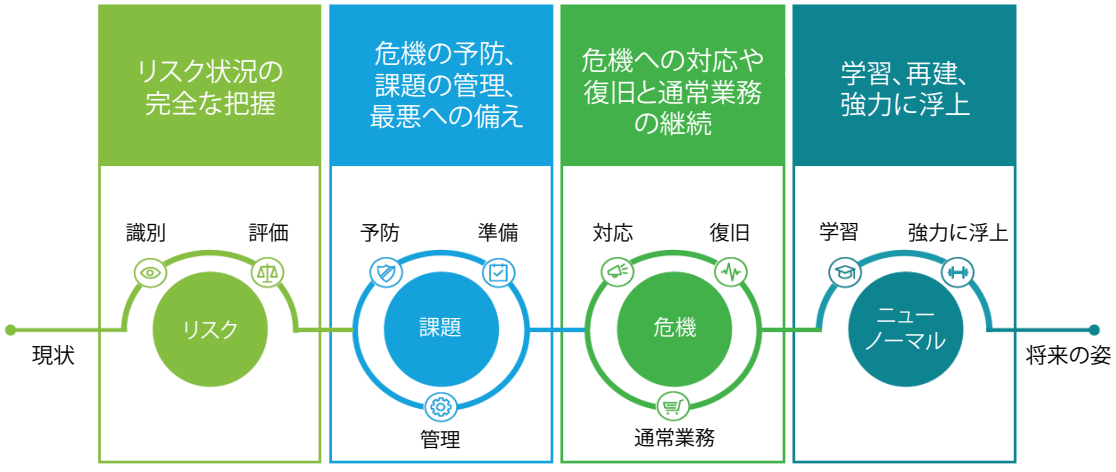
18 **情報とテクノロジーを有効活用する**
19 **リスク情報を伝達する**
20 **リスク、カルチャーおよびパフォーマンスについて報告する**

リスク、カルチャーおよびパフォーマンスに関する報告書は、ＩＴシステムを使用してデータや情報を取得、処理および管理している。経営者は、ＡＩモデルに関連するリスクマネジメントを含むリスクマネジメントに情報を提供して支援するために、その情報を使用する。ＡＩモデルのパフォーマンス、メリットおよび潜在的なリスクについて、社内外のステークホルダーに通知するためには、報告プロセスが必要である。報告プロセスでは、ステークホルダーが情報を受け取る方法、時期および頻度も考慮する。組織のレジリエンスを高めるには、リスクの状況を理解する必要があり、経営幹部と取締役向けに統一したＡＩリスク報告書を作成して監督活動を支援すべきである。この報告書には、組織のＡＩモデルのパフォーマンスに関する主要なパフォーマンス指標とリスク指標の最新情報とともに、主要な監督とモニタリングのプロセスの結果も含める場合がある。予期せぬ発見事項を含む結果の適時な伝達は、問題が大きくなる前に特定して解決するために不可欠である。

危機を予防し、課題を管理し、ＡＩ施策に関連する望ましくないパフォーマンスやインシデントから起こり得る最悪のシナリオに備えるには、危機時のコミュニケーション対応のフレームワークと手順がガイドとして機能するはずである（図７参照）。このような危機時のコミュニケーションの台本は、事業を継続させながらインシデントによる影響とエクスポージャーを抑制するために組織がとるべき対応策を明文化したものである。これには、復旧を支援するための手順も含めるべきである。

ステークホルダーの反応に関するデータは、危機後に再建してより強力に浮上するための重要な要素である。これらの対応は、ＡＩの戦略や導入の伝達に役立ち、組織が透明性に対する期待に応えるための一助となる。

図７．レジリエンスの向上



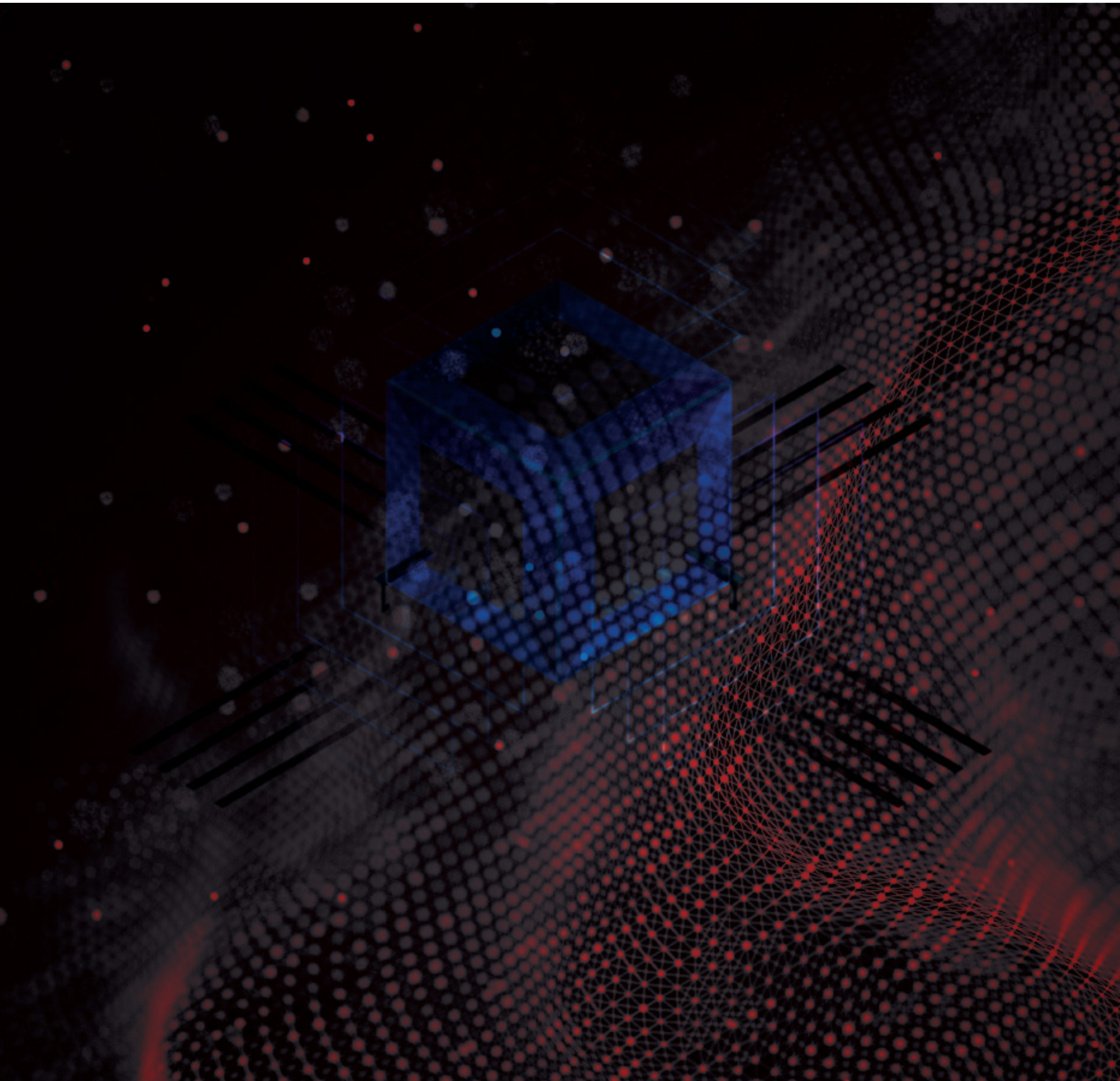
注目されるＡＩの活用

ＡＩは、組織の業務にますます大きく関わるようになりつつある。ＡＩ利用に対する投資家の関心が高まっていることを受け、テクノロジー関連の大企業数社は、ＡＩモデルが現在どのように業務に影響を与えているか、また将来的にどのような影響を与える可能性があるかを概説する情報開示を10-K 書類[x]に盛り込んでいる。

考慮すべきポイント

- 危機対応計画はあるか。
- ステークホルダーや一般市民に対して、どのようなＡＩプログラムのパフォーマンス報告を行っているか。
- 組織内の経営幹部や監督機関は、ＡＩプログラムに関する適切なパフォーマンス情報を受け取っているか。

[x] 訳注：米国証券取引委員会が公式的に作成を義務づけている年次報告書の開示様式。日本の有価証券報告書に相当する。



総　括

ＡＩの価値を実現し、その可能性を活用するために、組織はリスクマネジメントを戦略およびＡＩ施策の実行と整合させなければならない。ＣＯＳＯ ＥＲＭフレームワークは、組織がＡＩに関する統合的なガバナンスを構築し、リスクを管理し、戦略目標を達成するためにパフォーマンスを向上させるのに役立つ。ＡＩに関する統合的なガバナンスを導入することで、組織は関連するリスクについてより良い情報が得られる。これは、計算された戦略的リスクを取るための機会の範囲と柔軟性を高め、ＡＩ施策の計画や実行においてより機敏かつ適応的になれることを裏付けているのかもしれない。権威あるものではないが、デロイト社の「信頼できるＡＩフレームワーク（Trustworthy AI™ Framework）」は、組織がＣＯＳＯのＥＲＭフレームワークをＡＩに適用する際に、リスクを熟考する一助となり得る。

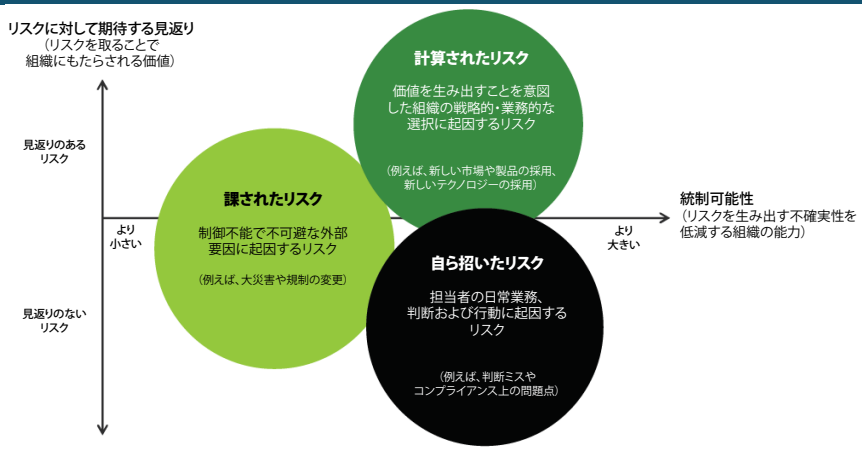
図８.『ＣＯＳＯ 全社的リスクマネジメント―戦略およびパフォーマンスとの統合』フレームワーク

出典：2017 *COSO Enterprise Risk Management – Integrating with Strategy and Performance*（邦訳は、『COSO 全社的リスクマネジメント－戦略およびパフォーマンスとの統合』）

ＣＯＳＯ ＥＲＭ フレームワークに基づくＥＲＭを通じて、組織はパフォーマンスの変動を抑え、ＡＩ施策を成功させる可能性が高められる。軌道修正の合図を早期に識別することで、組織はプラスの成果を上げ、マイナスの驚きを減らし、リスクへのレジリエンスを高められる。また、リスクに応じた資源配分も改善され、リスクを理解することで組織は投資収益率を高めてステークホルダーの期待に応えられるようになるかもしれない。さらに、組織はＥＲＭを導入することで、急速に変化する事業環境の中で戦略を支えるために、イノベーションの取り組みを改善して適応させることができる。

リスクマネジメントの適切な導入は、組織が高い見返りのある計算されたリスクを活用し、内在するリスクを管理し、自ら招いたリスクを大幅に減少させるのに役立つ（図９参照）。

図９. ＥＲＭプログラムは組織のＡＩ施策の成功を支援する



ＡＩソリューションは、信頼され、テストされ、正しいものである必要がある。信頼されるーＥＲＭは本質的に透明性があり、組織がリスクと機会を常に把握するのに役立つからである。テストされるーモデルは意図したとおりに動作していることを確認するために、継続的にテストされ精査されるからである。正しいーガバナンス、リスクマネジメント、テストおよびモニタリング体制は、組織の価値観を反映し、組織の評判を保護する形でモデルが運用される支援をする。ＣＯＳＯ ＥＲＭフレームワークを適切に考慮すれば、信頼され、テストされた、正しいＡＩが実現できる。

行動喚起：ＣＯＳＯ ＥＲＭフレームワークに基づいて検討すべき５つの次のステップ

ＣＯＳＯフレームワークおよびその基礎となる構成要素と原則を使用して、信頼性の高いＡＩプログラムを確立する。ここでは、その方法を紹介する。

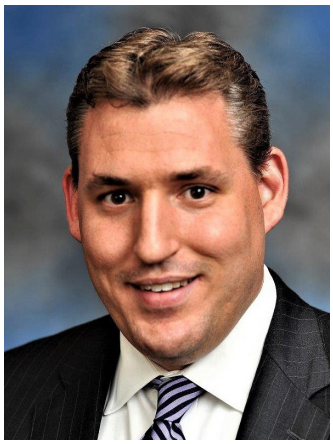
1. **ＡＩプログラムのガバナンス構造を確立する。**組織がいつ、どのようにＡＩを使用するかを決定し、提案されたＡＩ施策の目的と目標を定義する。これには、該当する倫理的配慮の評価も含まれる。組織内のさまざまなＡＩ施策を、全体的なＡＩプログラムとガバナンス構造の下に置くことで、経営幹部と取締役会に見通しを提供する。ＡＩプログラムをリードし、リスクとパフォーマンスのモニタリングを行う経営幹部を特定する。
2. **ＡＩリスク戦略をまとめる。**ステークホルダーと連携して、ＡＩの戦略リスク、技術リスク、規制リスクおよび運用リスクを管理するための組織全体の戦略を立案する。ＡＩリスク戦略を実行するためのＡＩの技術的な経験を組織に備えるようにする。戦略では、役割、責任、統制および緩和手続を定めるべきである。
3. **ＡＩリスク評価を率先して行う。**組織が使用する各ＡＩモデルについて、最適でない戦略的成果、運用上の失敗またはバイアスの可能性の影響を測定する。また、アルゴリズムがどのようにデータを管理し利用しているか、意図しないバイアスが生じていないかを評価する。ＡＩと統合するビジネスプロセスについては、脆弱性を探し、それらの発生可能性を確認し、既知のリスクとそれに対応する統制を記録する。
4. **ＡＩ施策のリスクと機会に関するポートフォリオの視点を養う。**最高リスク管理責任者とＡＩ責任者が連携することで、バイアス、改ざんおよびモデルの誤動作に関連するリスクについて、ＡＩモデルが先見的にレビューできる。彼らは、ＡＩリスクのポートフォリオの視点を経営幹部や取締役会に報告し、認識や意思決定の支援をすべきである。
5. **ＡＩのリスクを管理するためのアプローチを策定し、ステークホルダーに報告して透明性を確保する。**これには、ＡＩ施策のリスクと見返りのバランスの評価や資源配分も含まれる。先進事例、客観性およびリスク対応方法を提示する、ＡＩモデルのリスクの専門家のチームを編成することを検討する。各モデルの有効性、公正性および透明性などの目標を測定するための主要なパフォーマンス指標とリスク指標を確立する。各指標について、定例外のモデルレビューと是正措置を行うきっかけとなる閾値を設定する。経営幹部や取締役会向けの報告用ダッシュボードを作成するとともに、ＡＩのパフォーマンスとリスクマネジメントの取り組みを外部のステークホルダーに開示して認識を高める。

著者について

デロイト＆トウシュ社リスク・ファイナンシャルアドバイザリー部門プリンシパル、ケリー・カラーニャ

ケリーは、デロイト社のサイバー・戦略リスク部門のリーダーである。リスクに関して 25 年以上の経験を持ち、組織がカルチャー、能力およびプロセスを進化させ、事業の成長、パフォーマンスの加速、レジリエンスの向上および戦略目標の達成に役立つ統合リスクプログラムを構築できるよう支援している。キャリアを通じて、財務、業務、風評、規制、全社、戦略およびテクノロジーのリスクなど、さまざまなリスクの評価、管理およびモニタリングを支援してきた。また、全社レベルのリスクガバナンス、モニタリングおよびレポーティングの設計と展開について、取締役会と経営幹部チームに助言を行い、組織にとっての最大のリスクについて経営幹部の連携と団結を支援している。

レンセラー工科大学ラリー経営技術学部で起業家精神の理学士号と経営学修士号を取得している。



デロイト＆トウシュ社監査・保証部門パートナー、ブライアン・キャシディ

ブライアンは、米国の監査・保証部門の人工知能・アルゴリズム担当リーダーで、フォーチュン 500 企業に監査やアドバイザリーのサービスを提供した多様な経験がある。技術、リスクマネジメント、コミュニケーションおよび組織に関する強力なスキルを持つリーダーとして、金融サービス部門の上場・非上場企業に対する監査、会計およびアドバイザリーのサービスの提供を中心に行っている。ブライアンの経験は、銀行（ブローカー・ディーラー）、投資会社、事業開発会社ならびにプライベートエクイティ、ヘッジおよび不動産などのオルタナティブファンド等、金融サービスセクターの幅広い業界にわたっている。また、新たなテクノロジーが顧客や市場に影響を与え続ける中、アルゴリズム・ＡＩの保証分野においてデロイト社の取り組みを主導している。

米国公認会計士協会（ＡＩＣＰＡ）、ペンシルバニア州公認会計士協会（ＰＩＣＰＡ）、ニューヨーク州公認会計士協会（ＮＹＳＳＣＰＡ）の会員である。ヴィラノバ大学で会計学と経営学の学士号を取得している。

デロイト＆トウシュ社監査・保証部門パートナー、エイミー・パーク

エイミーは、デロイト社の会計アドバイザリー・トランスフォーメーションサービス部門のアイデア開発リーダーを務めている。この役割において、ＡＩ、アルゴリズム、ブロックチェーンおよびデジタル資産などの新興テクノロジーや保証の拡大の分野を含む、デロイト社が市場にもたらす価値を高めることができる新しいサービス提供の可能性へのアイデア開発を主導している。また、デロイト社の米国国内事務所の会計・報告サービスのパートナーであり、連結、金融商品およびデジタル資産取引の会計における技術的な会計事項を専門としている。

米国公認会計士協会（ＡＩＣＰＡ）の会員であり、ＡＩＣＰＡのデジタル資産タスクフォースでデジタル資産に関連する会計事項を中心に活動している。米国財務会計基準審議会での特別研究員を含め公開企業の会計に関して 17 年以上の経験があり、銀行、証券およびデジタル資産業界の公開・非公開企業にサービスを提供している。

ＣＯＳＯについて

1985 年に設立されたＣＯＳＯは、５つの民間団体の共同イニシアティブであり、全社的リスクマネジメント（ＥＲＭ）、内部統制および不正抑止に関するフレームワークとガイダンスの開発を通じて、先進的な考え方を提供することに取り組んでいる。ＣＯＳＯの支援団体は、内部監査人協会（ＩＩＡ）、米国会計学会（ＡＡＡ）、米国公認会計士協会（ＡＩＣＰＡ）、国際財務担当経営者協会（ＦＥＩ）、管理会計士協会（ＩＭＡ）である。

デロイト社について

本稿には一般的な情報のみが含まれており、デロイト社は本稿を通じて、会計、ビジネス、金融、投資、法律、税務またはその他の専門的なアドバイスやサービスを提供するものではない。本稿は、そのような専門的なアドバイスやサービスの代用となるものではなく、ビジネスに影響を与える可能性のある意思決定や行動の根拠として使用すべきではない。ビジネスに影響を与える可能性のある意思決定や行動をとる前に、関連する有資格の専門アドバイザーに相談していただきたい。

当社は、本稿に依拠した者が被った損失について、いかなる責任を負わないものとする。

Deloitte（デロイト社）とは、英国の保証有限責任会社であるデロイト トウシュ トーマツ リミテッド（「ＤＴＴＬ」）と、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の１つまたは複数を指す。ＤＴＴＬと各メンバーファームはそれぞれ法的に独立した別個の組織体である。ＤＴＴＬ（「Deloitte Global とも呼ばれる」）は、顧客に業務を提供していない。米国では、デロイト社は、ＤＴＴＬの米国メンバーファーム、米国で「デロイト」の名称を使って業務を行っているその関連会社、およびそれぞれの関連会社の１つまたは複数を指す。一部の証明業務は、公開会社に関する会計の規則上、顧客に提供できない場合がある。　メンバーファームのグローバルネットワークの詳細については、About the network (deloitte.com) を参照されたい。

一般社団法人日本内部監査協会

内部監査および関連する諸分野についての理論および実務の研究、ならびに内部監査の品質および内部監査人の専門的能力の向上を推進するとともに、内部監査に関する知識を広く一般に普及することにより、わが国の産業、経済の健全な発展に資することを目的に活動。

また、国際的な内部監査の専門団体である内部監査人協会（The Institute of Internal Auditors：ＩＩＡ）の日本代表機関として世界的な交流活動を行うとともに、内部監査人の国際資格である“公認内部監査人（Certified Internal Auditor：ＣＩＡ）”等の認定試験を実施している。1957（昭和 32）年創立。

公益財団法人日本内部監査研究所

内部監査に関する研究調査を推進するとともに、わが国の内部監査の普及発展に貢献することにより、わが国経済、社会の健全な発展に資することを目的として、2020 年７月に設立。2021 年６月に公益財団法人としての認定を受け「公益財団法人日本内部監査研究所」となった。

監訳者

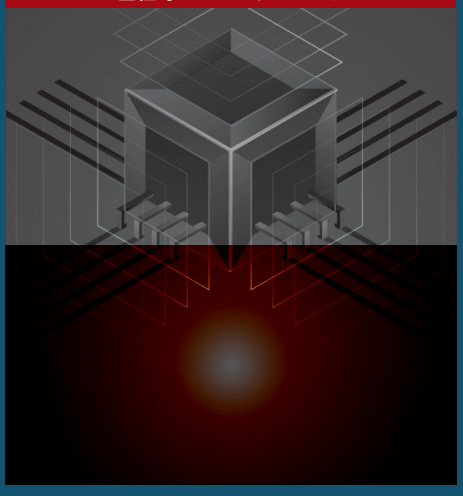
八田　進二　（大原大学院大学　会計研究科　教授　／　青山学院大学　名誉教授）

橋本　　尚　（青山学院大学大学院　会計プロフェッション研究科　教授）

訳　者

堺　　咲子　（内部監査人協会（ＩＩＡ）国際本部　北米外地域筆頭理事　／　インフィニティコンサルティング　代表　／　プレミアアンチエイジング株式会社　社外取締役　／　ＣＩＡ，ＣＲＭＡ，ＣＣＳＡ，ＣＦＳＡ）

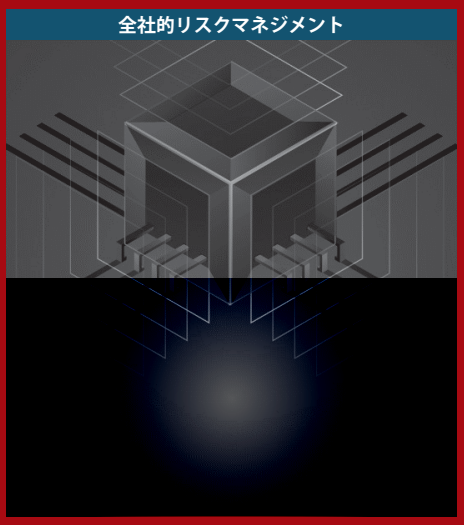
全社的リスクマネジメント



COSO

トレッドウェイ委員会
支援組織委員会

coso.org



人工知能の可能性を
最大限に実現する

ＣＯＳＯフレームワークと原則を適用した
人工知能の導入と拡張の支援

COSO

トレッドウェイ委員会支援組織委員会

coso.org