

AIリスク管理体制構築・ 内部監査実施支援

DX推進により拡大する新たなリスクの発見と改善に向けて

デジタルトランスフォーメーション（DX）の推進により、企業のあらゆる業務プロセスにおいて人工知能（AI）の利活用が進む一方で、AI特有の不確実性や新規性に起因するビジネス・技術面の新たなリスクが高まっています。KPMGは、長年の内部監査支援の経験を活かし、AIの活用に潜むリスクの発見および、改善に向けた管理体制の構築を支援します。

AIの活用に伴う新たなリスク

AIによる予測や分類などのデータ処理の精度は完全ではないため、AIのリスク管理体制が不十分だと、ビジネスに悪影響をもたらす可能性があります。たとえば、AIの評価モデルに不備があり、特定の顧客、社員、取引先に対して不公平な判断を下していたことが判明した場合、取引や業務の中断、企業イメージの低下などを招く恐れがあります。特に、新規性の高いAIの利活用においては、ルールやノウハウが十分でないことが多いため、内部監査部門には、独立した立場でリスク管理体制の不備を発見し、改善策を提言することが期待されています。

AIに関する法規制・ガイドラインへの違反リスク

EU一般個人データ保護規則（GDPR）や中国個人情報保護法等の海外の個人データ保護法令では、AI等のアルゴリズムを用いた個人データの自動処理が規制されています。また、EUでは高リスクのAIを対象とする包括的な規制案も検討されています。これらの法規制は日本企業に対しても域外適用され、違反した場合には数十億～数千億円規模の罰金が課される恐れがあります。一方、日本においても、法的拘束力はないものの海外諸国の法規制を参考にガイドラインの整備が進んでいます。そこでは、全社的なAIポリシーやAI品質管理体制の整備など、さまざまなAIリスクへの対応が求められています。

AIリスクの観点（例）	AIリスクシナリオ（例）	リスク顕在化時の影響（例）
透明性・公平性	AIによる顧客や社員・取引先等の評価モデルの不備により、被評価者に不公平な判断が行われる	顧客や社員・取引先の離反、係争や訴訟の発生、評判低下
安全性	自動運転車、産業用ロボット、医療診断機器等で利用されるAIの誤作動により、事故が発生する	人命の喪失や環境汚染の発生
プライバシー	行動履歴データを用いたAIによる個人属性推定（プロファイリング）の結果が外部に漏洩する	法令違反による行政指導、高額な罰金、評判低下
セキュリティ	AIを構成する学習データ、モデルや入力データへの攻撃によりAIの誤作動が発生する	経済的損害、情報漏洩、事故発生による安全性侵害
契約・利用規約	AIを利用したサービスの事故発生時における責任分担が、顧客やベンダーとの間で明確化されていない	顧客やベンダーとの係争や訴訟の発生
保険	AIを利用した業務やシステムでの事故発生時の損失額が、既存の保険契約内容で補填されない	経済的損失の発生
知財	自社のAIに関する秘密保持が不十分なことにより、開発委託先や第三者に無断で再利用される	自社の競争力低下

AIリスク管理体制に関する監査テーマ・対象

AIリスク管理体制の内部監査では、契約や社内規程、利用規約等に基づくビジネス面と、データやアルゴリズムの品質管理をはじめとした技術面の管理体制が対象となります。また、既存の全社リスク管理（ERM）や委託先管理、個人データ管理などにおけるAIリスクの管理状況も対象となります。

AIリスク管理体制構築における課題

AIリスクはさまざまな観点からの管理が必要となりますが、内部監査部門内にAIの専門知識を有する人材は少ないため、独立した立場でリスク管理を担う人員の確保が難しく、特に部門間の牽制関係が機能しにくい傾向が見られます。AI導入による効果とリスク管理を、限られた人材でどのように両立するかが課題です。

監査テーマ・対象（例）	監査要点（例）	発見事項（例）
全社的なAI活用状況の管理	AIを利用している業務やシステムが全社的に特定されているか（委託先による利用を含む）	AIを利用している業務やシステムがグループ内で網羅的に把握されていない
ERM体制におけるAIリスク管理	AIのさまざまなリスクを管理する部門や手順が全社的なリスクの調査を経て定義されているか	各部門がどのような種類のAIリスクの管理を担当するかが明確化されていない
全社的なAI活用ポリシーの運用状況	全社的なAI活用ポリシーやAI倫理ガイドラインが各部門のAI取扱い業務に反映されているか	全社的なAIポリシーと各部門におけるAIの運用実態が整合していない
個別のAI利用業務・システムでのリスク管理	AIを利用する各業務やシステムにおいて、リスク管理の手順が適切に整備されているか	AI活用に伴うリスクとその管理責任や役割分担が規程等で定義されていない
AI品質管理体制	AIが利用するデータやモデルの品質リスクが定期的かつ客観的に管理されているか	AIの開発・利用担当者以外の第三者による定期的な品質管理が実施されていない
AIによる個人データ処理プロセス	AIによる個人データ処理へのデータ提供者の同意が十分な説明を実施したうえで取得されているか	個人データのAI利用に関する同意取得にあたってのデータ提供者への説明が十分でない
委託先でのAIリスク管理体制	法令や企業方針に基づくAIリスク管理義務が委託先の業務においても遵守されているか	委託先との契約に法令や企業方針に基づくAIリスク管理義務が反映されていない

KPMGによる支援

KPMGは、AI活用やリスクマネジメント、内部監査に関する豊富な知識・経験を持つ人材を有しています。これらの領域における多数の支援実績を活かし、企業のAIリスク発見のための内部監査計画策定から監査の実施、課題改善に向けた管理体制の構築まで網羅的に支援します。

1. 内部監査計画策定支援

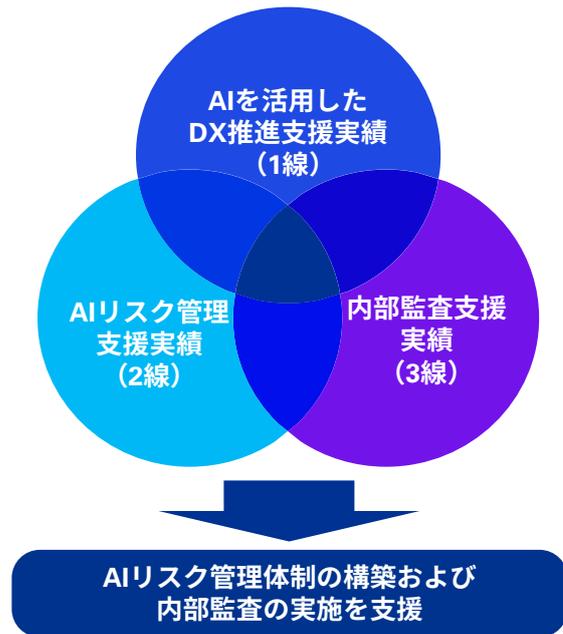
- AI利用業務・システムの運用状況と管理体制の可視化
- 高リスクのAI利用業務やシステムの選定

2. 内部監査実施支援（アウトソース／コソース）

- 監査テーマ、対象範囲、項目の選定、監査手続きの策定
- 往査実施、発見事項の検討、監査報告書の作成

3. 被監査部門の改善計画の実行支援

- AIリスク管理に関する規程・マニュアル等整備
- AI利用業務・システムの改善計画に関する要件定義



本リーフレットで紹介するサービスは、公認会計士法、独立性規則及び利益相反等の観点から、提供できる企業や提供できる業務の範囲等に一定の制限がかかる場合があります。詳しくはKPMGコンサルティング株式会社までお問い合わせください。

KPMGコンサルティング株式会社

T: 03-3548-5111

E: kc@jp.kpmg.com

home.kpmg/jp/kc

ここに記載されている情報はあくまで一般的なものであり、特定の個人や組織が置かれている状況に対応するものではありません。私たちは、的確な情報をタイムリーに提供できるよう努めておりますが、情報を受け取られた時点及びそれ以降においての正確さは保証の限りではありません。何らかの行動を取られる場合は、ここにある情報のみを根拠とせず、プロフェッショナルが特定の状況を綿密に調査した上で提案する適切なアドバイスをもとにご判断ください。

© 2022 KPMG Consulting Co., Ltd., a company established under the Japan Companies Act and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved. 22-5059

The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organization.