KPMG

AIおよび生成AIの規制はどこへ向かうのか

「信頼されるAIシステム」とは

2023年8月

目次

「生成AIを含むAIがいっそう広く導入されるようになれば、イノベーションを起こしながら信頼性を保つために、リスク管理部門の役割が非常に重要となります。正式な法規制が存在しない場合（そうした規制が今後導入される可能性があっても）、企業はリスクとコンプライアンスに関わる適切なガードレールと「スピードバンプ」を事前に設定しなければなりません。規制当局は、アルゴリズム、AI、革新的なテクノロジーを含む「自動システム」に既存の権限や規制が適用されることを明確にしており、このことを忘れてはなりません」*

Amy Matsuo
Principal and National Leader
Compliance Transformation (CT) & Regulatory Insights
KPMG米国

「生成AIの導入は急速に進んでおり、組織は規制を遵守する方法を模索しています。生成AIをめぐる規制が策定され実施されるなか、経営幹部は警戒しながら推進する必要があります」

Emily Frolick
Partner
US Trusted Imperative Leader
KPMG米国

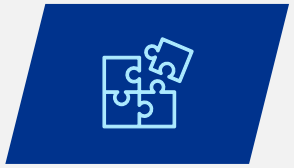
* 走行中の自動車の速度を減速させるために道路に設けられた突起物のこと

はじめに

企業は、規制が現在どのような状況となっているのか、今後どのように進展していくのかを注視しています。企業組織として、リスクを低減させながら自動化の進展を有利なものとするために、リスクガバナンスとリスク管理をどのように設計すべきでしょうか。

生成AI（GenAI）を含む人工知能（AI）がいっそう広く導入されるようになれば、イノベーションを起こしながら信頼性を保つために、リスク管理部門の役割が非常に重要となります。正式な法規制が存在しない場合（そうした規制が今後導入される可能性があっても）、企業はリスクとコンプライアンスに関わる適切なガードレールと「スピードバンプ」を事前に設定しなければなりません。

「AI規制」：現状および今後の展望



AI規制の複雑さを言い訳にはできない

さまざまな分野にまたがるAIリスク

すべてを管理する

KPMGはどのように支援できるか：

モダンデータ、アナリティクス、AIを促進

AIおよびデータ倫理規範

「AI規制」：現状および今後の展望

公共政策や立法においてAIが大きく注目されるなか、既存の規制がAIを含む「自動システム」に適用され、設計、開発、導入、継続的モニタリングのライフサイクル全体に及ぶことを規制当局は明確にしています。

法規制に関する重要な動き

自動システムにおける差別とバイアスに対する法執行に関する関係省庁の共同声明

現状存在する法的権限は、「自動システム」（すなわち、AIを含むソフトウェアやアルゴリズムによるプロセス）や「革新的な新テクノロジー」に適用されます。法的保護が市民権、反差別、公正な競争、消費者保護を促進。

ホワイトハウス AI権利章典：NIST AIリスク自主管理フレームワーク

AIリスクを管理するための資源と原則を確立し、信頼と、バイアスや利益相反の低減を含めてAIシステムの安全性と有効性についての信頼性、独立のレビューと報告を促進。

SECが「対象テクノロジー」と利益相反に関して規則を提案

投資家の意思決定を最適化、予測、ガイド、予想、指示する「対象テクノロジー」（AIやプレディクティブ・アナリティクスを含む）を企業が使用する際、利益相反に対処するための規制案を公表。

EU AI法（欧州連合人工知能法）

消費者が被る損害や消費者保護を視野に、AIアプリケーション、製品、サービスの設計、開発、導入、モニタリングにわたるリスクベースのフレームワークを確立する法案。適合性評価、技術的要件、監査要件、モニタリングなど、リスクレベルごとにプロバイダーに関する要件や義務を規定。

注視すべき重要領域：AI規制のテーマ

リスク管理

生成AIを含むAIの設計、使用、導入に関するリスク管理とガバナンス（以下を含む）

- 安全性と有効性（意図しない、または不適切なアクセスや使用に対する保護など）
- バイアスと差別の防止（バイアスに対する保護と継続的なテスティング）
- データガバナンスとデータプライバシー
- 透明性（使用される情報の内容や使用方法、企業や消費者への潜在的影響など）
- 説明責任と監督

既存の規制の下での公平性と消費者が被る損害

消費者および従業員保護に関する既存の法規制の下で、AIおよびその他の革新的テクノロジーの適用における公平性の監督および法執行

「政府一丸での取組み」
（複数の政府機関による協働アプローチ）

目的の制限とデータの最小化（プライバシー）

許可や同意、オプトイン／オプトアウト、承認などに基づいた、特定の目的や明示的目的に関する消費者データへのアクセスおよび使用の制限

データ保持の制限（所定の目的に限るなど）

データとシステムに関する保護措置（アクセスと使用に関するもの）

AI規制の複雑さを言い訳にはできない

AIや規制領域に対する当局のアプローチと監督上の重点が変化し、州、連邦、グローバルな法域にわたり乖離が生じる可能性があり、AIコンプライアンスはますます複雑になると予想されます。同様に、システムのインプットとアウトプットや顧客への影響（公平性、プライバシー、サイバーセキュリティなど）に関わる他の進化領域での規制当局の期待が、AIへの期待と重なる可能性があり、規制当局のモニタリングが強化され、複雑さが増す可能性があります。

複雑性が増す領域

AIの進化

AIの幅広いアクセシビリティとユーザーフレンドリーなインターフェースは、急速なテクノロジーの進化とイノベーションを促進し、州、連邦、そしてグローバルな規制の焦点は、AIがもたらす既存、新規、進化するリスクに当てられています。企業は、バイアス、差別、透明性、ガバナンス、一貫性、公平性とともに、データの収集、保護、質、所有権、保存、保持を含む（ただし、これらに限定されない）これらのリスクについて全社的な評価を実施する必要があります。

全社的理解

AIの説明可能性（透明性）と説明責任に関する規制当局のモニタリングに応えるには、適切なレベルの見識、経験、トレーニングが必要となります。企業がAIを設計・開発する際には、全社的な調整と連携が必要となるでしょう。AIのライフサイクルを通して社内のステークホルダーと連携し、メリット、リスク、限界、制約など、AIを理解するための全社的な能力を向上させ、コンテキストと使用に関する前提をチェックし、誤作動、誤情報、誤用を認識できるようにします。

AIに関する既知（および未知）のリスク

生成AIを含むAIテクノロジーが台頭するなか、新たな機会を活用しつつ規制上の落とし穴を回避するためには、効果的なリスク管理を優先することが欠かせません。AIシステムの設計、開発、導入、評価において、全社的なリスク管理の文化を醸成し、実践することを検討し、AIシステムの設計と開発の技術的側面を組織の価値観と原則に結びつけるようにします。

注視すべき重要領域：複雑性の増大

絶え間ない進化

ユーザーフレンドリーなAI製品やサービスの普及により、その適用や機能は急速に進化しています。こうした進化は、「規制当局がどのようにAIへアプローチするか」「企業がどのようにコンプライアンスを評価するか」の両方をますます複雑にしています。

期待の重複

公平性、データプライバシー、サイバーセキュリティ、レジリエンスに焦点を当てた法律や規制が現在急速に発展しているため、AIに対する省庁間または法域間を越えた取組みが強化され、複雑さが増しています。これらの規制の更新は、消費者への影響を含むAIの設計、開発、導入に対する規制上の期待と重なる可能性があります。

規制要件の乖離

AIの監督に対する規制当局間のアプローチや重点分野が乖離すれば、コンプライアンスをめぐる複雑性が大幅に増し、現在のコンプライアンス機能および目標とするコンプライアンス機能やコンプライアンス・リスク評価のアプローチを再評価する必要が生じます。影響評価、法域リスク、規制への認識、タイミングを検討しなければなりません。

さまざまな分野にまたがるAIリスク

AIのメリットとリスクは、オペレーション、製品およびサービス、顧客保護に関連するさまざまな側面を含む、組織の全領域にまたがることになります。 主な懸念領域としては、潜在的な利益相反（企業と顧客の間）、市場集中（AIベースモデルのプロバイダー）、マクロ・プルーデンス政策の介入などが挙げられます。

規制の影響を受ける可能性がある主な領域

プライバシー
データの収集、使用、保護、質、所有権、保存、保持

データ
データ漏洩、マルウェア、不正、なりすまし、その他の金融犯罪

セキュリティ
敵対的攻撃、データ・ポイズニング、内部脅威、モデル・リバース・エンジニアリングなどのAI利用に伴うセキュリティ・リスク

当該リスクは、レピュテーションを管理するために迅速な改善が必要

導入およびインテグレーション
サードパーティ・リスク管理、単一プロバイダーへの過度の依存、専門家への限られたアクセス、当該テクノロジーを効果的に活用するための従業員訓練の必要性など、AI導入に伴うオペレーショナルリスク

テスト、評価、検証、妥当性確認（TEVV）
効果的なAIの設計と開発には、AIのライフサイクルの各段階において、使用目的との整合性や適切なカリブレーションを確保し、ユーザーエクスペリエンスを評価し、関連する要件と期待を確実に遵守するための強固なTEVVプロセスが必要

保証と証明
AIの信頼性は、ユーザーエクスペリエンスの成功に不可欠であり、AIシステムの機密性、完全性、および可用性を維持するより広いシステムフレームワークを保証することで強化できる

知的財産
AIは、知的財産権をめぐる潜在的な法的問題（評価減の可能性など）を提起する可能性がある

注視すべき重要領域：影響

AIの「信頼性」
特に安全性、有効性、公平性、プライバシー、説明可能性、説明責任に関わるAIの信頼性に当局の関心が高まり、企業はデータの収集、インプットとアウトプット、使用、プライバシー、セキュリティなど、組織全体を通じてAIの目的と適用を総体的に見直すことが必要となります。

ビジネスリスク
プライバシーやサイバーセキュリティなど、AIや関連するトピックをめぐる新たな公共政策や規制上の課題や当局措置に基づき、現在の方針・手続を再評価または更新する必要があるかもしれません。

規制当局の動向や行動を監視し、事業の制約や制限など、ビジネスモデルの大幅な変更につながるかどうかを評価することが重要です。

AIリスク管理
不完全なAIやAIの誤用にかかわるリスクや、関連する規制当局の関心に注意を払い、積極的なAIリスク管理フレームワークを通じて、そのような潜在的リスクに対処します。

規制当局の求めるものは、以下のとおりです。

- 堅確なAIの開発、実装、使用（例えば、明確な目的の表明、健全な設計／理論／論理）
- AIの設計および開発から独立して実施される効果的な検証
- 健全なガバナンス、方針、統制

すべてを管理する

AIソリューションの設計、開発、導入、管理に関連するリスク管理に必要なのは、個々のAIの導入そのものを理解すること、新たなAIツールやトレンドを受け入れ、取り入れられるように既存のリスク・フレームワークを適応させること、そしてモニタリング結果、モデルリスクの脅威特定、包括的なモデルリスク管理にフォーカスしたリスク・マインドセットを持つことです。そのためにリスク管理部門が現在注力すべき4つの柱と代表的な活動は、以下のとおりです。

ガバナンスの確立

- AIガバナンス・フレームワークを確立する
- 役割と責任を明確に定義し、組織全体でAIの使用を管理する方針を策定する
- AIの使用、AIをめぐる新たなリスク、適切な使用方針についてステークホルダーを教育する
- 透明性の原則と方針を確立する
- 利用承認、継続的監視、リスクの評価などの分野をはじめとするモデルリスク管理（MRM）フレームワークにAIを組み込む
- AIモデルを、実証（内部利用）からビジネス上の意思決定、さらには実際の利用へ移行するに際して、MRM基準に沿った手順を確立する

コンプライアンスとリーガルリスク

- AI規制の動向を監視する
- 適切なステークホルダーが要件や統制を実施していることを確保する
- AIの導入とガバナンスの基準を適切な規制ガイドラインおよび要件に整合させる
- 全社的なAIの使用・導入基準に対する監督を検証する
- サードパーティに対する一貫した契約要件とAIの導入要件を確立する
- AIの脆弱性を特定・報告・管理する仕組みが確立されていることを確認する
- 計画されたAIの利用が及ぼす倫理的または社会的影響を評価する
- 市場への導入・適用での法的考慮をモニタリングする

AI戦略とロードマップの把握

- AIソリューションの現在のビジョン、戦略、運用モデルを調整する
- 取締役会レベルの監督を評価する
- 計画されているユースケース、モデル、ツールも含め、組織内のAIの在庫管理を網羅的に行う
- 各AIソリューションのユースケースとベンダーの状況を明確に理解する
- データ保護、データ保存、機密データへのアクセスに関連するサードパーティ・リスクを監視する
- データおよびAIパイプラインのセキュリティとプライバシーに関する懸念（ポイズンおよびドリフト*を含む）を継続的に監視するために取得したソフトウェアツールを評価する
- 年次リスク評価プロセスにAI評価を組み込む

使用と導入の監視

- コンプライアンス、ガバナンス、セキュリティ、公平性、バイアス、正確性、説明可能性などの領域について、AIリスク評価を実施する
- AI導入に特有のアクセス、API／インターフェース、データセキュリティ、プライバシー、変更管理統制を評価する
- AIのテスト、トレーニング、導入基準を評価する
- 財務報告への影響を評価する
- AIによりもたらされた成果を監視し、異常、不正、データ・ポイズニングを検知するためのKPIを特定する
- AIソリューションのレジリエンスと信頼性を評価する

* ポイズンとは、AI学習に用いるデータセットに不適切なデータが混入すること。ドリフトとは、何らかの要因によりAIの予測性能が低下すること。

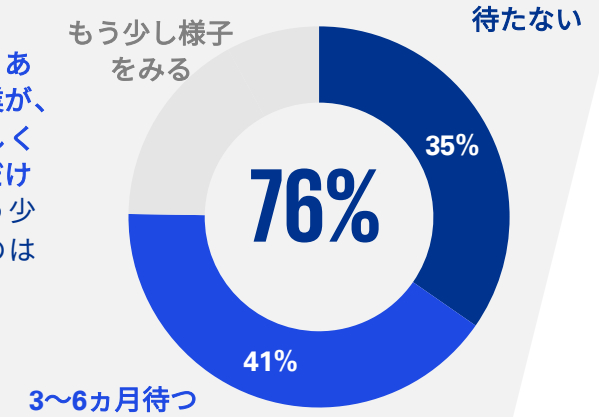
詳しくはこちらのサイトをご覧ください：
KPMG Speed to Modern Technology: Responsible AI

2023年KPMG生成AI調査

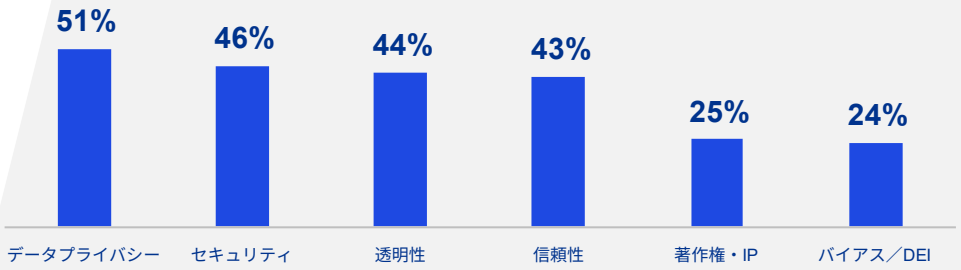
2023年生成AI調査報告書：KPMGは、米国のシニア・ビジネスリーダー200人を対象に、生成AIとこの新たなテクノロジーがビジネスにもたらす変革的影響について調査しました。回答者は、規制環境に関する不確実性が生成AIの導入における最大の障壁であると述べていますが、ほとんどの回答者はAIの導入を遅らせてはいません。

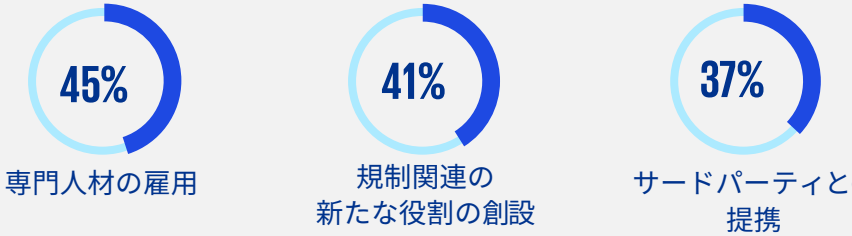
生成AIへの追加投資に関して、**10人に8人近く（77%）のビジネスリーダーが、規制の変化が意思決定に影響を及ぼしていると回答**しています。

規制の状況を見定めるにあたって、4分の3以上の企業が、AIの導入を待たない、もしくは、短期間（3〜6ヵ月）だけ待つと回答しており、もう少し様子をみると回答したのは4分の1だけです。



生成AIに関してビジネス・リーダーが予想する規制措置に関しては、**データプライバシーに関する規制措置が最も多く、**著作権やバイアスに関する規制措置は少なくなっています。

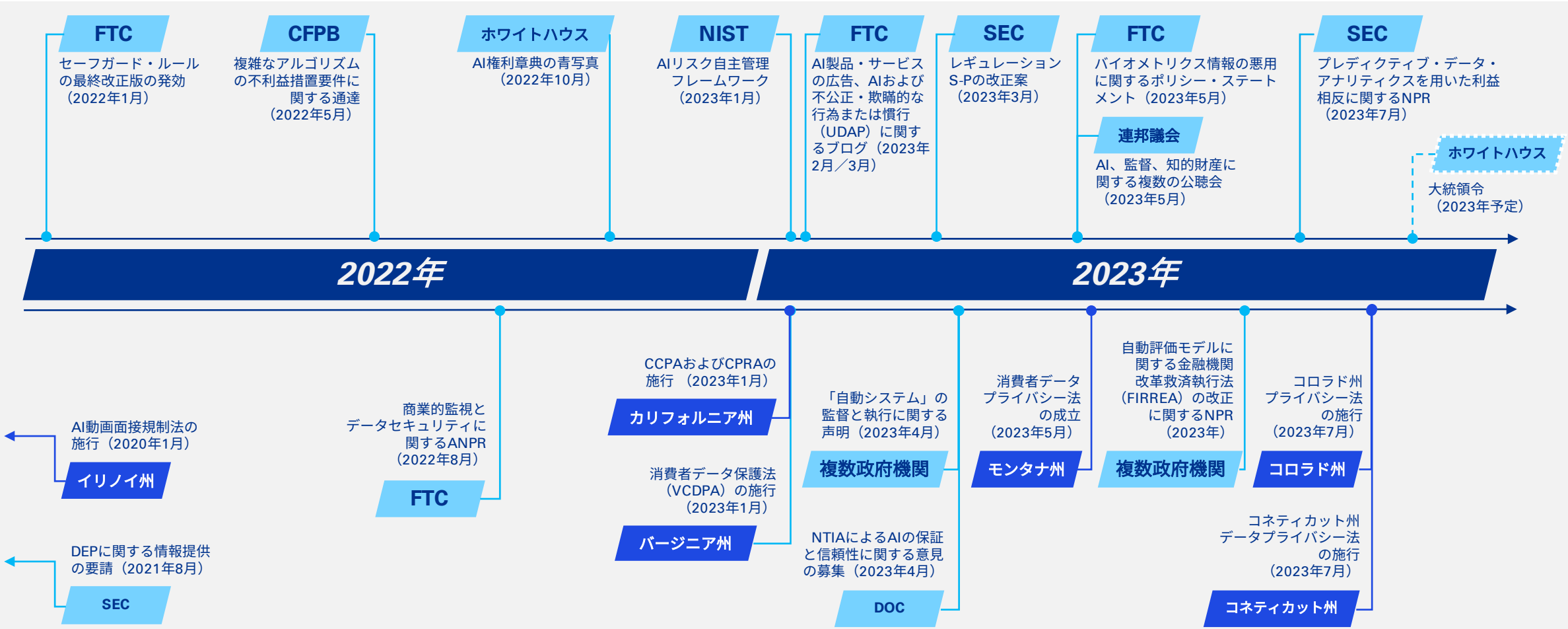




生成AIをめぐる規制の変化を見越して取られる最も一般的な**施策**には、**専門人材の雇用、規制関連の新たな役割の創設、サードパーティとの提携**などがあります。

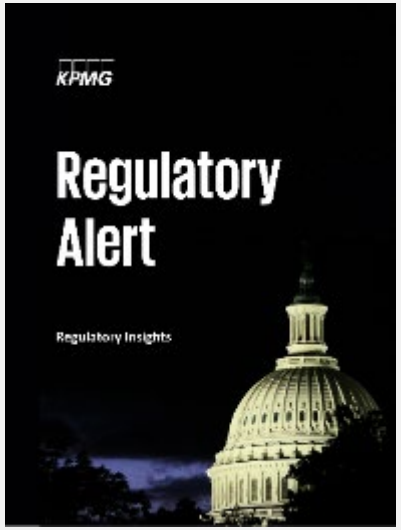
AI関連の法規制の動き

立法府や規制当局による州レベル、連邦レベル、世界レベルでのさまざまな動きにより、企業、消費者、その他のステークホルダーに対するAIテクノロジーの適切なガードレールが敷かれようとしています。以下の年表は、これらの動きの一部を抜粋したものです。



関連するThought Leadership

KPMG規制インサイト



- “Covered Technologies” and Conflicts of Interest: SEC Proposal
- Enforcement/Supervision to “Automated Systems”
- Ensuring Trust in AI: Commerce Department Request for Comment
- Focus on Tech: Cloud, AI, Personal Data

KPMGの他のサイト

KPMG Speed to Modern Technology: Responsible AI

Download the paper

Download the paper

Download the paper

Contact us

Amy Matsuo
Principal and National Leader
Compliance Transformation (CT) &
Regulatory Insights
KPMG米国

amatsuo@kpmg.com

Emily Frolick
Partner
US Trusted Imperative Leader
KPMG米国

efrolick@kpmg.com

Bryan McGowan
Principal
Generative AI Lead, Risk Services
KPMG米国

bmcgowan@kpmg.com

山﨑 千春
あずさ監査法人
マネージング・ディレクター
080-2108-1091
chiharu.yamazaki@jp.kpmg.com

秋場 良太
あずさ監査法人
ディレクター
080-2108-0958
ryota.akiba@jp.kpmg.com

KPMGジャパン
kpmg.com/jp/regtech
regtech@jp.kpmg.com

本冊子で紹介するサービスは、公認会計士法、独立性規則およ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。詳しくは有限責任 あずさ監査法人までお問い合わせください。

本冊子は、KPMG米国が2023年8月に発行した「Where will AI/GenAIregulations go?」を、KPMG米国の許可を得て翻訳したものです。翻訳と英語原文間に齟齬がある場合は、当該英語原文が優先するものとします。

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するよう努めておりますが、情報を受け取られた時点およ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。