elastic

Elasticを使用して AIコンプライアンスの 取り組みを拡大する方法

エグゼクティブサマリー

世界中の政府がサービスやツール内での人工知能（「AI」）の開発と使用を管理する法律や規制を導入する中、組織はAIシステムの透明性、リスク管理、それぞれの法的要件への準拠を確保するための適切な対策を採用しています。Elasticsearch Platformは、エンタープライズ顧客がAIの導入を監視し、影響評価を実行し、より信頼性の高いエコシステムを維持するための包括的な制御を実装するのに役立ちます。本ホワイトペーパーでは、透明性の義務の理解からモデルトレーニングのためのデータの倫理的な活用まで、AIガバナンスの主要領域について説明します。当社は、企業が規制の要求に対応し、自信を持ってイノベーションを推進できるようにするためのロードマップを提供します。また、Elasticの強力なプラットフォームが、適用されるAI法に基づく独自の要件へのコンプライアンスの追跡と管理にどのように役立つかについても説明します。

注意：*このホワイトペーパーは情報提供のみを目的としており、法的助言を構成するものではありません。法的助言については、ご自身の法律顧問にご相談ください。*

世界のAI関連法の背景と入門

過去数年間で、AIに関する世界的な規制環境は大きく変化し、世界中でAIの開発、適用、監視に関する新しい法律が制定されました。生成AIと大規模言語モデル（LLM）の急速な出現により、組織や消費者はデータを全く新しい、変革的な方法で活用できるようになりました。この進歩に伴い、これらのテクノロジーの動的な性質により、当然ながら、その法的、倫理的、実際的な影響についての疑問が生じています。

世界のAI法には重要な違いがありますが、多くの共通する原則を共有しています。注目すべき例としては、EUのAI法、韓国のAI基本法、ブラジルのAI法、コロラド州のAI法、カリフォルニア州のAI透明性法、カリフォルニア州の既存のCCPAプライバシー法に基づく自動意思決定技術に関する規制、ユタ州のAI政策法などが挙げられます。このような現行の法制化に加え、OECDのAI原則、オーストラリアのAI安全スタンダード、シンガポールのモデルAIガバナンスフレームワークなどの国際的・国内的な自主的枠組み、あるいは顧客やエンドユーザーとの契約により、データの利用や処理活動によっても、データの使用および処理活動に関する追加の義務が課される場合があります。

組織はこれらの要件と期待に応えるために、Elasticを戦略的に活用し、AI法の遵守を効果的に追跡、管理、改善することができます。Elasticはパートナーとして、責任あるAIイノベーションの未来の構築をお手伝いします。

人工知能と機械学習

AIは過去数十年で劇的に進化しました。初期のAIシステムは、明示的な指示に従って厳密に定義されたタスクを実行するように設計されたルールベースのプログラムに依存していました。時間の経過とともに、機械学習（コンピュータシステムが統計的手法を使用してデータから「学習」し、明示的にプログラムすることなくパフォーマンスを向上させる AI のサブセット）の登場により、この分野は自然言語処理、画像認識、自動意思決定などの複雑なタスクを実行できる高度なモデルへと進歩しました。

AIの定義は法律や業界のガイダンスによって異なりますが、EUのAI法は有用な出発点を提供しており、AIシステムを、機械学習、ロジックベース、または統計的手法を使用して開発され、人間が定義した一連の目的に対して、予測、推奨、決定など、現実環境または仮想環境に影響を与える出力を生成するソフトウェアと定義しています。このような環境の中で大きく発展しているのが生成AIです。これは、テキスト、音声、またはビジュアルコミュニケーションを通じてユーザーと対話し、そうしたコミュニケーションを処理して特定のターゲットを絞った出力を生成するシステムを指します。厳格でルールに縛られたプロセスから動的なデータ駆動型の学習システムへの進化により、AIでデータを使用する可能性は根本的に変わりました。

開発者と導入者

AIシステムの開発者と導入者は、急速に進化するAIエコシステム内で、それぞれに異なるものの相互に関連した役割を果たします。EU AI法や米国のいくつかの州法に見られるような規制提案や法定フレームワークでは、一般的に「開発者」はAIシステムを設計、作成、トレーニング、保守する個人または団体と定義されています。その責任には通常、アルゴリズムの設計やモデルのトレーニングなど、システムの技術的および理論的な基盤が含まれます。

対照的に、「導入者」は、一般に、AIシステムの意図された目的を決定し、それらを製品、サービス、運用ワークフローに統合する個人または組織を指します。多くの場合、導入者は、実装したAIシステムが公平性、透明性、安全性、説明責任に関する確立された標準に準拠して動作することを保証する責任を負います。

*開発者と導入者*は協力して概念設計と開発から実際のアプリケーションに至るまでのAIのライフサイクルを定義し、AIシステムの実装全体にわたる明確な説明責任の重要性を強調します。

自動化された意思決定とプロファイリング

AI技術を特別に規制する法律に加えて、違法または不当な差別につながる可能性のある方法で（そのような差別が意図的でない場合でも）AIを含む自動意思決定技術の使用を禁止する法律が増えています。例えば、イリノイ州の法律では、人材の採用と維持において保護された特性に基づく差別につながる可能性のあるAIの使用に制限を設けています。同様に、ニューヨーク市の地方法144は、雇用決定に大きな影響を与える特定の「自動化された雇用決定ツール」を規制し、バイアス監査などの要件を義務付けています。

さらに、他に提案されているさまざまな法律や規制は、スコアリング、分類、推奨など、人間の裁量的な意思決定を支援または置き換えるために使用される単純化された出力を生成するAIシステムを対象としています。

さらに、これらのシステムで個人データが使用される範囲において、最も有名なEU GDPRなどの特定のプライバシー法は、個人の特性、行動、経済状況、健康、個人的嗜好や関心の側面を評価、分析、または予測することを目的とした自動処理に制限と義務を課しています。

リスクベースのAI立法アプローチ

新しいAI法の多くは、リスクベースのフレームワークを採用して、AIアプリケーションを潜在的な損害に応じて分類しています。例えば、EUのAI法では、許容できないリスク、高いリスク、限定的なリスク、最小限のリスクのアプリケーションを区別しており、職場の感情や感情分析などのシステムは禁止されています。同様に、コロラド州や米国の他の規制案では、特定のAI導入に関連するリスクの評価に重点が置かれています。これは、特に決定がグループや個人に大きな影響を与える可能性がある場合に、AIの特定のアプリケーションを規制する傾向が高まっていることを示しています。

AIの基本原則

AI法が制定される前は、責任あるAIの開発と導入の指針となる業界標準とベストプラクティスが有機的に形成されていました。これらの自主規制措置は、業界関係者、標準設定機関、学術研究者によって導入され、いずれも、AI技術とその導入の急速な進歩に関連する倫理的および運用上の懸念に対処することを目的としています。これらの初期の取り組みから、AIシステムが理解可能で、公平で、説明責任を果たす方法で運用されることを保証するための重要な原則が浮かび上がりました。

1

透明性

この原則は、データソース、方法、意思決定プロセスの開示を含む、AIシステムの設計および運用方法に関する情報を公開して共有し、ユーザーと利害関係者がシステムの機能を理解して信頼できるようにするための取り組みです。

2

説明可能性

これは、AIシステムが出力や決定に対して明確で、理解しやすく、解釈可能な根拠を提供する能力を指し、それによって開発者、規制当局、ユーザーがシステムの結論の背後にある根拠を追跡し評価することを可能にします。

3

AIのバイアスやアルゴリズムによる差別からの保護

この原則は、AIシステムにおけるデータや設計の選択における違法または不当なバイアスから生じる可能性のある不公平な結果を認識しています。この技術が特定のグループや個人に不公平または違法な方法で体系的に不利益を与えないようにすることの重要性を強調しています。

これらの原則は、AIの責任ある統合のための倫理的必須事項を強調することで、後の法的フレームワークの基礎を築きました。

AI法への不遵守が企業にもたらすコスト

増え続けるAI法規制の不遵守は、単なるコンプライアンス違反にとどまらず、組織の財務の安定性、市場での地位、長期的な存続可能性に対する真の脅威となる可能性があります。規制は拡大と進化を続けていますが、現行規制における罰則は、規制されていないAIシステムがもたらす可能性のある重大な社会的、経済的損害を反映して、意図的に厳しくなっています。例：

- **EU AI法は**、ハイリスクまたは許容できないリスクのAIシステムに関連する違反に対して、企業のグローバル売上の最大7%と3,500万ユーロのいずれか高い方の罰金を科します。数十億ユーロの収益を上げている多国籍企業にとって、このような罰金は数億ユーロ、場合によっては数十億ユーロに上る可能性があり、収益性、投資家の信頼、時価総額に重大な脅威をもたらす可能性があります。この法律に基づくその他の違反には、最大3%、誤情報の提供に関しては最大1.5%の罰金が課せられます。EU AI法はまた、EU市場でAIシステムを提供するプロバイダーは物理的な拠点に関係なく遵守しなければならないという治外法域的効力も有します。

- **ブラジルのAI法案草案**は最大5,000万レアル（約900万米ドル）の罰金を想定するだけでなく、規制当局に非準拠のAIサービスの停止を命じる権限やシステム調整を義務付ける権限を付与することが提案されています。

- **コロラド州AI法**は、高リスクAIシステムにおけるアルゴリズム的差別を避けるための「合理的な注意」を怠ることを不当な取引慣行と見なし、違反ごとに最大20,000ドル、高齢者に対して行われた違反の場合は最大50,000ドルの罰則を科します。

- **カリフォルニア州AI透明性法**は、対象となるプロバイダーに対して違反1件あたり1日最大5,000ドルの課徴金を科し、場合によっては差止命令を発動することもあります。「1日単位」の課徴金により、対応の遅れや継続的な違反が壊滅的な経済的負担へと急速に発展する可能性があります。

- **ユタ州AI政策法**は、違反1件につき最高2,500ドルの罰金を課し、差止命令や法律違反で得た金銭の没収など、その他の救済措置も認めています。継続的な違反の場合は1回の違反につき5,000ドルの罰金が科される場合があります。企業は、たとえAIが違反の出力に直接責任を負う場合であっても、生成AIアプリケーションによって引き起こされた違反に責任を負います。これにより、コンプライアンス負担は導入組織に完全に移行します。

AI規制法に違反すると、定量化可能な金銭的罰則に加え、無形であっても同様に大きな影響を与えるコストが発生します。ブランドの評判の低下、顧客や利害関係者の信頼の喪失、業務の非効率性は長期的な市場不利益につながり、成長と革新を妨げる可能性があります。

さらに、金銭的罰則や差止命令だけでは不十分な場合、米国の連邦取引委員会（FTC）などの執行機関は、違法に取得したデータだけでなく、そのデータに依存するアルゴリズムやモデルも削除するよう組織に要求する「アルゴリズム廃棄」を追求することができます。AIが事業運営に不可欠になるにつれ、コンプライアンス違反の財務的および戦略的な影響はますます大きくなっていっています。

Elasticが企業のAI法遵守を効率化する方法

Elasticは、コミュニティとの透明性と直接的な関わりを持ち、オープンな開発プロセスに取り組む革新的なAIソリューションのリーダーとして、透明性、責任、説明可能性に優れたシステムの構築にも注力しています。この取り組みにより、お客様は進化するAIの法的基準に確実に準拠しながら、自信を持ってデータを管理できるようになります。Elasticは、新しい規制環境によってもたらされる主要なコンプライアンスの課題に直接対応する包括的な機能スイートを提供します。Elasticを使用すると、複雑なコンプライアンス要件を合理化された自動プロセスに変換できます。

ここ数年で出現したAI法には、透明性の欠如、アルゴリズムによる違法または不当な差別や偏見に関する懸念、あるいは自動化された意思決定全般に関係するAIによる潜在的な危害に対する保護を志向する傾向が見られます。AIソリューションによって処理される基礎データ

は既に多くの法的フレームワークによって規制されていますが、技術自体や、そのようなソリューションを設計・使用する企業を規制しているものはほとんど（あるいは全く）ありません。

したがって、グローバルなAI法を遵守するには、組織のデータが存在するエコシステム全体と、そのデータが移動し、処理される方法を理解する必要があります。そこで、Elasticはお客様のコンプライアンスフレームワークをサポートしながら、これらのプロセスを簡素化・自動化できるよう支援します。

次の表は、Elasticがさまざまなコンプライアンスのユースケースで組織をどのようにサポートできるかを示しています。

AIコンプライアンスの課題	コア規制のニーズ	Elasticの機能	主な利点
透明性	通知と開示	一元化されたログ、メトリクス、監査証跡	データフローと意思決定を実証し、調査を簡素化
文書化とデータインベントリ	データインベントリ	データマッピングと分類	データガバナンスを自動化し、正確なレポートを保証
リスクの特定	継続的な監視	リアルタイムのアラートと分析	プロアクティブなリスク調整と動的制御の実施
影響評価の実施	アルゴリズムによる差別防止	検索機能、データ系統の追跡	評価を効率化し、基礎的なコンプライアンスを確保
AIリテラシーとポリシー	トレーニング	包括的なトレーニングプラットフォーム	AIの知識を運用化し、スタッフの監視を支援
ユーザーへの選択肢の提供	個別のリクエスト	データのマッピングと分類	リクエストに迅速に対応し、個人の権利管理を合理化

透明性：Elasticを使用して通知および開示義務を充足

AI システムは本質的に複雑であり、透明性の確保は、法的、規制的、または契約上の義務のいずれに関してもユーザー、規制当局、利害関係者との信頼関係を構築するための基本となります。EU AI法などの規制では、組織はデータの使用状況と意思決定モデルに関する洞察を提供する必要があります。例えば、EU AI法など法律に基づく通知関連の要件は、関連する業界やAIの種類によって異なりますが、これらの法律のほとんどには、エンドユーザーがAIと対話している際に通知する一般的な義務が含まれており、特定の状況下では、ユーザーに明確な通知を提示し、モデルのトレーニングに使用されたデータのインベントリを維持する義務が含まれます。一般的に、カリフォルニア州やコロラド州などの新しいフレームワークの一部では、使用前に通知が必要になる場合があり、場合によっては、エンドユーザーに関する重大な決定が行われる前に通知が必要になることもあります。多彩な法律が複雑に進化していく中、関連するデータと処理内容を理解し、通知する義務は、米国とEUの法律を通じて一貫して維持されています。

Elasticsearch Platformは、ログ、メトリクス、監査証跡を環境間で一元管理し、リアルタイムのモニタリングと過去のトレーサビリティを可能にします。これは、お客様がAIシステムを通じてデータがどのように流れるか、そしてそのようなデータに基づいてどのように決定が下されるかを示すのに役立ちます。具体的には、Elasticを活用して、これらの透明性義務の遵守を促進する対策を実施できます。

例えば、Elasticのお客様は次のことが可能です。

- 多様なデータソースを業務、AIアプリケーション、ユーザーインタラクション全体で統合し、データインベントリへの理解を深められるようにすることで、ユーザーはトレーニング、テスト、検証（その他多数）に使用されるデータを識別、分類、評価可能に
- フォレンジック分析とコンプライアンスレポートのためにデータ系統とモデルアクティビティを記録するログを維持して監査証跡を実施
- Kibanaなどのツールを使用してダッシュボードを作成し、AIが特定の決定をどのように行うかを検索、集約、視覚化することで、ユーザーがデータ調査を簡素化できるように

Elasticのお客様は、自社のAIアプリケーションから詳細なログを取り込み、格納できます。これにはLLMのプロンプトや対応、エラーや例外などが含まれ、AIシステムの動作を理解するために不可欠なデータです。

Elasticの強力な検索機能により、技術文書、トレーニングデータの詳細、運用ログなど、膨大な量の構造化データおよび非構造化データをインデックス化して検索可能にすることができます。

Elasticのお客様は、Kibanaのカスタムダッシュボードでリアルタイムのモニタリングにアクセスし、AIシステムのパフォーマンスを追跡することができます。ログ分析、異常検出、パターン分析などのKibanaの機能は、AIシステムの動作を追跡するのに役立ちます。これにより、開示が必要となる可能性のある異常や予期しない動作を特定できます。

詳細を確認：ComcastはElasticを使用してデータの傾向と異常を視覚化し、チーム間で分析情報を共有しています。

文書化とデータインベントリ：ElasticでAIシステムの適切な使用を開発・促進

透明性に関連して、EU AI法およびカリフォルニア州などの米国の特定の州法では、特定のAIシステムに関する特定の文書の維持と公開が義務付けられています。例えば、2026年1月1日以降、カリフォルニア州のAB 2013は、AI開発者が生成AIシステムを消費者に提供する前に、Webサイトに文書を掲載することを義務付けています。カリフォルニア州法に基づく開発者とは、AIシステムを「設計、コーディング、製造、または実質的に修正する」企業を指します。特に、生成AIシステムの開発に使用されたデータセットの概要（データセットのソース、データセットがどのようにAIシステムの目的を促進するのか、データセットが集合情報を含むのか、個人情報を含むのか、などを含む）を文書化する必要があります。

上述の通り、Elasticはお客様のデータを評価するための効果的なデータマッピングを可能にします。これには、お客様のエンドユーザーにより適したソリューションを提供するために、お客様が当社の検索エクスペリエンスを変更する方法も含まれます。さらに、お客様がデータを一元管理し、タグ付けし、理解できるようにすることで、当社はお客様が特定のデータに適用される義務（法律上の義務、契約上の義務、受託者責任、機密保持義務）を理解できるようにします。

詳細を確認 ：SitecoreがElastic Securityを使ってデータを一元化し、最大96%のセキュリティワークフローを自動化している方法を紹介します。

データに関連するリスクや潜在的なAIユースケースの特定

新たなAI法では、データの種類やユースケースに基づいてさまざまな要件が規定されているため、データを理解、管理、保護することがこれまで以上に重要になっています。

Elasticの継続的な監視機能により、顧客はデータとその潜在的な使用に関連するリスクを評価できるため、経時的なリスクレベルの変化に応じて、より効果的に制御を調整できます。例えば、適用法の下では、高リスクAIシステム（医療や法的決定を行うために使用されるものなど）はより厳格な管理の対象となります。Elasticは、リアルタイムアラート、カスタマイズ可能なダッシュボード、詳細な分析を提供することで、お客様のリスク管理フレームワークの実装をサポートします。これにより、ユーザーは、検索機能を含むAIシステムの使用から生じる潜在的な損害に対処（および是正）するためのルールとパラメーターを設定できます。

詳細を確認：Ernst & YoungはElasticsearch Relevance Engineを使用して、コンプライアンスとイノベーションに不可欠な非構造化データから重要な洞察の精度を向上させ、検索を高速化しています。

影響評価の実施

既存のプライバシー法におけるデータ保護影響評価の実施義務と同様に、EUやコロラド州などの新たなAI法では、AIの導入者に影響評価の実施が求められており、これは特に高リスクのアプリケーションで顕著です。これらの評価では、一般的にAIのユースケースに関する主要な詳細を文書化する必要があります。これには、システムに関するさまざまな詳細、その目的、使用されるデータ、意図された利点、アルゴリズム的差別のリスク、セーフガード、導入後のモニタリングが含まれます。

Elasticは、顧客がこれらの影響評価をいつ、どのように実施すべきかを理解できるようにします。特に、データがどこにあり、どのように処理され、どこに流れているかを知ることで、個人データの使用を理解するためにこれまで事業部門全体で多面的なサポートが必要だった影響評価を効率的に完了できます。これらの影響評価は、基本的なコンプライアンスを実証すると同時に、組織がデータの処理を適用法で許可されている範囲に制限できるようにします。

詳細を確認：製薬会社がElasticを利用して研究者やコンプライアンスチームがインジェストから検索までの利用レポートを作成できるよう支援し、規制機関への報告義務を効率化している事例を紹介します。

AIリテラシーとリスク管理のポリシーと手順の実装

EU AI法に基づき、AIプロバイダーと導入者は、AIの運用および使用に関わるスタッフ（特に人間の監視機能を果たす個人を含む）が十分なレベルのAIリテラシーを持っていることを確保するための措置を講じる必要があります。さらに、AIリテラシーの目標では、組織がスタッフにAIシステムの導入によって生じる機会、リスク、制限を理解させ、潜在的な害を認識し軽減できるようにするためのトレーニングプログラムを開発および実施することが期待されています。この期待は、コロラド州など他の地域での、アルゴリズムによる差別の可能性に対処するためのリスク管理ポリシーとプログラムの実装要件と連動しています。

Elasticは、お客様が想定するユースケースにおいて十分なAIリテラシーをスコープ設定、決定、そして文書化できるよう支援します。Elasticは、包括的なトレーニングプラットフォーム、技術的専門知識、そして統合データソリューションを活用することで、これらの要件を満たすためのサポートも提供します。特に、機械学習とAIの高度な概念を網羅したオンデマンドトレーニングや講師主導のバーチャルコースなど、豊富なライブラリをご用意しています。トレーニングサブスクリプションでは、実践的な演習を通して理論的な概念を補強し、AI処理に関する抽象的な理解をより具体的なものにします。

ユーザーへの選択肢の提供

多くのAI法（および特定のAI導入に影響を与える法律）は、組織にユーザーに対してデータと意思決定の方法に関する明確な選択肢を提供することを義務付けています。例えば、規制によりプロファイリングや自動化された意思決定プロセスに関する透明性が求められる場合があり、ユーザーにはオプトアウトや人間による介入を要求する権利がある場合があります。

Elasticのデータマッピング機能は、組織がデータ主体の要求を処理するための中核的な基盤を形成します。具体的には、Elasticのデータマッピング機能とデータ分類機能を使用することで、組織はそのような要求の有効性を判断する方法を迅速に把握し、必要に応じて要求に応答できるため、コンプライアンスチームがこれらの法律で定められた短い期間内に応答するための貴重な時間を節約できます。

アルゴリズムによる差別の削減とバイアス監査の実施

AIシステムは大量のトレーニングデータに依存しており、そのデータの品質、多様性、ソースはAIの結果の公平性と信頼性に直接影響します。規制では、AIの倫理的な導入を確保するために、トレーニングデータの出所と偏りにますます重点が置かれるようになっています。

Elasticプラットフォームは、ログ、トレーニングデータ、機械学習モデルの出力など、多様なソースからデータを取り込み、インデックス化することができます。Elasticでは、データの移動やリハイドレートが不要であらゆるデータタイプの検索と分析が可能なため、組織は入力データから最終結果までの意思決定パイプライン全体からデータを1か所で収集できます。Elasticのプラットフォームにより、顧客はデータセットをクエリ、探索、可視化して、その構成を評価し、AIシステムのパフォーマンスと公平性に影響を与える可能性のある潜在的なバイアスやギャップを特定できます。

さらに、Elasticの強力なクエリDSLを使用することで、組織はデータをフィルタリングし、掘り下げて、異なる人口統計グループ間で結果を比較できます。例えば、アグリゲーションクエリを実行して、アルゴリズムの決定が特定の集団に不均衡に影響を与えているかどうかを検出できます。

お客様がデータとそのソースに関する詳細な記録を保持できるようにすることで、データの360度ビューを持つ能力を提供し、意思決定がブラックボックス化されないようにします。

まとめ

Elasticを使用してAIコンプライアンスの未来を管理

データを理解し、技術がどのように意思決定を行うかを理解することは、法的要件となると同時に、業界のベストプラクティスになりつつあります。増大するAI関連の要件に大規模に準拠する能力は市場での差別化要因となり、組織の戦略的成功を支えることが期待されます。Elasticは、このプロセスの重要なステップを合理化し、お客様がコンプライアンスの主導権を握れるようにします。Elasticは、規制上の課題を戦略的利点に変換することで、組織がリスクを軽減するだけでなく、責任を持って自信を持って革新できるようにします。