Deloitte.
デロイト トーマツ

最高情報セキュリティ責任者（CISO）のための生成AIガイド

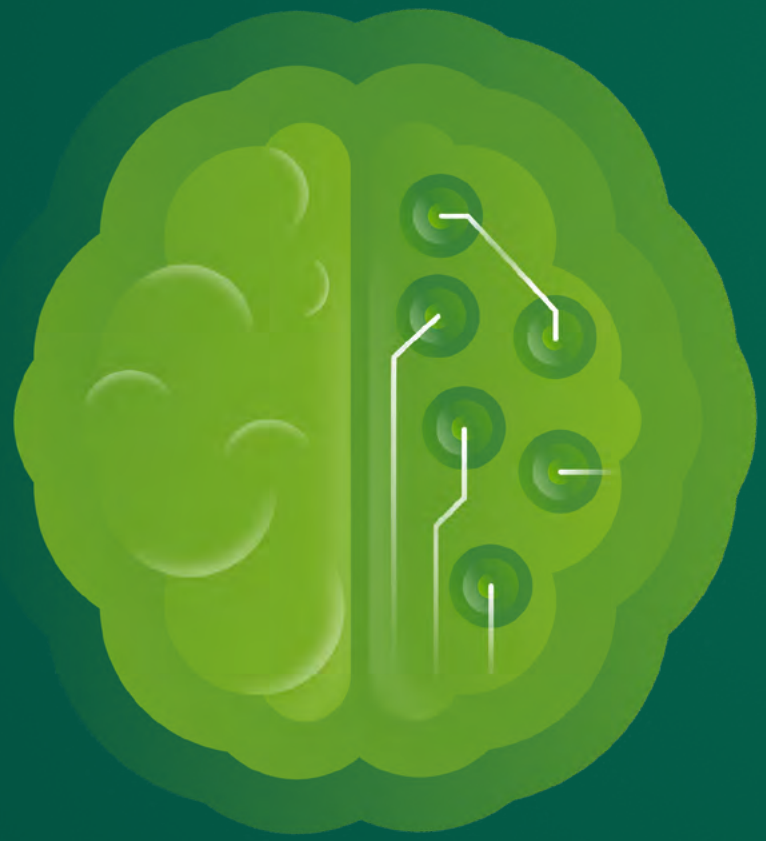
今日における緊急性と、これまでの成果、将来の可能性

生成AIは、次のどれに活用できるでしょうか 正しいものをすべて選択してみてください

- **組織のサイバーセキュリティの取り組みにおける、新たな機会と価値の創出**
- **コスト削減、報告とインテリジェンス製品の強化**
- **高度なフィッシング攻撃に対する迅速な保護**
- **過去の活動に基づいた、重要情報の特定**
- **規制と法遵守の指針の理解**
- **現在および将来の状況に対応したサイバーセキュリティにかかわるロードマップの構築**

上記の項目がすべて正しいと回答された方は、
生成AI技術について正しく理解していることになります。

本ガイドを読み進めて、生成AIを自組織のサイバーセキュリティの
変革にどのように活用できるかを確認していきましょう。



生成AIは、人々にどのような メリットをもたらすのでしょうか

ジェネレーティブAI（生成AI）は至る所で話題になっています。
この新しい人工知能（AI）が自組織や所有するデータ、セキュリティに
どのようなメリットをもたらすのかを皆が知りたがっています。
しかし、これは容易には答えが見つからない複雑な問題なのです。

AIの一部である生成AIでは、機械によってテキスト、コード、音声、画像、動画、プロセスといった形で新しいコンテンツが作成されます。当該技術によって、人々の仕事や生活にまさに大変革がもたらされる可能性があります。サイバーセキュリティに関していえば、生成AIは、組織と政府の両者にとって有望な技術であり、自らの保護、報告とインテリジェンスを自動化するツールの作成、コスト削減、より効率的な成長、変化し続ける多様な規制環境の中での整備などにおいて活用が期待されています。

しかし、生成AIは、このような強力な技術を悪用して負の結果をもたらし、個人的利益を得ようとする悪意のある攻撃者の新しいツールにもなり得ます。サイバー攻撃は、発生件数と戦術の両面で増加し続けています。実際のところ、デロイトの2023年 Global Future of Cyber Surveyでは、90%を超える回答者が少なくとも1件の侵害が発生したと報告しています。

サイバーセキュリティにかかわる事象が従来の人的なセキュリティオペレーションセンターの能力を凌駕してから長い時が経った一方で、AIがサイバーインフラと検出・対応能力の強化に大きな影響を与えています。ディープラーニングモデルは攻撃の検出によく適しています。

しかし、サイバーリーダーたちは依然として次のような疑問を抱いているかもしれません。「AIによって自社の防御能力や防御態勢が強化されたが、生成AIでさらに強化させることができるのだろうか。攻撃があった際の被害の範囲の制限、データ損失からの保護、脅威への対応能力の拡張を予算・期限内に行うために、生成AIをどのように利用できるのか。言い換えれば、生成AIによって、攻撃者の先を行き、その状態を保てるのか」と。

生成AIは、人々にどのようなメリットをもたらすのでしょうか

生成AIは、先述した各疑問に対応することができます。そして、侵害を見つけ出し防御を行う組織に、サイバー関連のより良い成果をもたらす大きな可能性を秘めています。また、生成AIは、高速かつ論理的で、処理できる知識量がどの人間よりも優れているだけでなく、コスト削減、セキュリティ調査の強化、サードパーティーのリスク評価の迅速化も実現し得るのです。

より確立されたAI能力（機械学習やディープラーニングなど）ではパターンの識別や推論を行うことができる一方、生成AIはそのようなデータをまとめ上げ、人間に近い回答を生成し、桁違いに速いスピードで作業を行うことができます。また、生成AIにより、セキュリティアナリストがほぼリアルタイムのインシデント分析を基に脅威を拡散前に特定して抑え込められるよう支援する、新しい種類の脅威インテリジェンスを作成することができます。

悪意のある攻撃者が生成AIをどのように悪用し得るのだろうとサイバーリーダーが懸念するのは当然のことです。しかし、楽観的な見解も持つべきです。なぜなら組織は、適切なアプローチとガバナンスを確立することで、サイバー態勢の強化、人材に関連する課題の克服、脅威の検出と対応のための新しいロードマップの構築に生成AIを活用することができるからです。

生成AIの可能性を引き出すにあたり、サイバーにかかわるリーダーが最初に行うべきことは、生成AIを活用できる領域、必要なデータの種類に加え、安全性やレジリエンス、信頼性に対する考慮事項を含む行動計画の策定方法を理解することです。

覚えておくべき2つのことがあります。すなわち、生成AIは完全に新しい概念ではなくAIの進化形であること、そして、当該技術に合わせて導入計画とリスク管理体制も進化し得ることです。また、これまでの真の進化に至る過程と同様、このような技術にも長期的な変革の努力が求められます。生成AIのサイバーセキュリティへの導入は、能力を構築するための取り組みとなるとお考えください。

本ガイドでは、生成AIをどのように活用できるのか、そして、
どのようなサイバー関連の考慮事項が存在し得るのかを探っていきます。
組織が生成AIを利用してより良い成果を生み出すことができるか否かは、
人間と機械が補完し合うコラボレーティブ・インテリジェンスについて想像し、
適切な問いかけを行えるかにかかっていることを忘れてはいけません。
生成AIが組織に真の影響を与えられると信じるためには、
まず生成AIが持つ力と可能性を理解する必要があります。

それでは、始めていきましょう。

生成AIは攻撃と防御両面で サイバーセキュリティに影響を与えます

生成AI×サイバーセキュリティには、①AI自体に対する攻撃、②AIを悪用した攻撃、③AIを利用した防御の3つの観点が挙げられます。今、これらの観点を踏まえ、サイバーセキュリティ戦略を見直す転換点を迎えています。

生成AI× サイバーセキュリティ

1	**AI自体に対する攻撃** (Security for AI)	
a	**開発者・提供者への攻撃** (構築・提供時の攻撃)	• 学習データのポイズニング・インジェクション • 学習データの漏えい／推測 • サービス停止 • モデルバックドア・不正アクセス 等
b	**利用者への攻撃** (利用時の攻撃)	• 入力データのポイズニング・インジェクション • 入力データの漏えい／推測 • サービス停止 • モデルバックドア・不正アクセス 等
2	**AIを悪用した攻撃** (Attack using AI)	• 偽画像・偽音声の生成・なりすまし • パスワードクラッキング • フィッシングメールの作成 • ランサムウェアの開発 • 漸弱性・不具合の探索（ファジング） • 攻撃の自動化・24/365化 等
3	**AIを利用した防御** (AI for Security)	• マルウェアの検知 • ログ・トラフィックの解析 • リスクベース認証 • ペネトレーションテストの高度化 • 脅威インテリジェンスの高度化 • 原因究明・復旧支援 等

攻撃者によるAIの活用を促す動機・メリット

新たな攻撃手法の開発	全く新しい攻撃手法が登場し、従来のセキュリティ対策の有効性が損なわれる
生産性・効率性の向上	攻撃者のスキルが拡張される（スキルを持った者はより高度な攻撃を、またスキルをあまり持たない者でも容易に攻撃を行うようになる）
コンテンツの品質の向上	フィッシング、フェイクサイト、ニュースなどのコンテンツの品質が向上してしまう
なりすましの高度化	画像、音声、動画など多様なコンテンツでの認証機能が無効になってしまう
攻撃の多様化	新たなコードの生成・攻撃を繰り返すことで、検知がより困難になる
攻撃の自立化	簡単な指示による自動的・継続的な攻撃が行われる

サイバーセキュリティに対する生成AIの計り知れない価値

人間には太刀打ちできない著しい速さで、人間が行うような作業ができる生成AIには、価値を乗数的に高める力があります。

機械学習は長年、サイバーセキュリティ上の脆弱性を検出し、脅威を監視するために大規模に利用されてきたものですが、組織モデルを錬磨してパターンの理解とデータの異常検出を行うには、高度な技術的熟練と投資が必要となります。言い換えると、ルールベース型のAIは、既知の攻撃のみを検出し、また特定のユースケースでの使用に限定されているのです。

しかし、生成AIと大規模言語モデル（LLM）を利用することで、大きな変革がもたらされます。生成AIは、膨大な量のデータを基にトレーニングが実施された基礎的なニューラルネットワークモデルを使用することから、データサイロを横断し、データセット間の橋渡し役として機能します。アナリストはこのような技術を利用することで、洞察の特定、統合、要約を行うためのより自然な手法を用いることができるようになります。

用語の説明

予測：アセットインベントリ、セキュリティログ、脅威インテリジェンスなどを分析し、リスクスコアの予測や予防策の推奨に役立てる。

解釈：アラート受信、構文解析など、大量のテキストデータを要約し、処理することで、一貫性のある実用的な要約を作成する。
文脈や知識ベースを考慮し、論理的分析（推論、演繹、説明）を行う。

シミュレート：知識ベースから情報を抽出することで、自然言語での質問に対する回答の生成およびテストケースやサンプルシナリオの作成に役立てる。

自動化：アラートのトリアージ、イベントの関連付け、インシデント対応のプレイブックに基づく対応担当者への指針提供など、インシデント対応活動を作成する。

検出：アラートデータと脅威インテリジェンスレポート間の相関関係を特定し、インフラに対する影響判断に役立てる。修復・リカバリ活動においてセキュリティアナリストの指針となる具体的な対応策を更新する。

やり取り：規制文書、法規制、データ、基準を分析し、迅速に行動を通知する。従業員の役割、責任、職務要件に基づく、個別化され、的を絞った脅威・危機対応トレーニングを実施する。

作成：一連の入力データ、事例、特定のテーマやトピックに基づき、様々な様式のためにコンテンツを新しいフォーマットやスタイルに変換することで、コンテンツ生成を実施する。

サイバーセキュリティにかかわる活動の変革に生成AIを活用することができます。

サイバーリスク管理とコンプライアンス

リスクのスコアリングと優先順位付け
アセットインベントリ、セキュリティログ、脅威インテリジェンスを分析し、リスクスコアの予測や予防策の推奨を実施

サードパーティーリスク管理
ベンダーが提出した文書と外部文書内のデータを分析し、サードパーティープロバイダのセキュリティ態勢を評価

ポリシーのレビューと整理の自動化
コンプライアンス要件を満たすため、標準的な業界・規制フレームワークに照らして、現行のポリシー、基準、手順をマッピングする

サイバーセキュリティの成熟度評価
組織がサイバーリスクに係る成熟度を自ら評価することで、サイバー戦略におけるギャップを特定し、改善のための適切な提言を行う

脅威の検出と対応

実行可能かつ正確な脅威インテリジェンス
過去のトレンドや公開されているデータを基に、アクティブな脅威に関する要約レポートや経営陣向けのブリーフィングを生成

脅威の相関関係と検出
アラートデータと脅威インテリジェンスレポート間の相関関係を特定し、インフラに対する影響を判断

セキュリティインシデントへの対応
アラートのトリアージ、イベントの関連付け、インシデント対応のプレイブックに基づく対応担当者への指針提供など、インシデント対応活動を自動化

リカバリと修復強化
修復・リカバリ活動においてセキュリティアナリストの指針となる具体的な対応策を作成

生成AI対応のフィッシング検出
生成AIを利用し、LLMによって生み出された脅威やフィッシングの試みを検出

脆弱性の管理とセキュリティのテスト

統制テストと自動化
テストケースやサンプルシナリオの作成、結果の予測、証拠文書の策定

セキュアコードの生成
最新のセキュリティ上の考慮事項（セキュアコーディングガイドラインの川上統合）に準拠し、アプリケーションコードと関連する補足的なテストケースを開発

脆弱性スキャンの強化
行動計画の優先付けのため、脆弱性データ（スキャンデータ、外部情報、修復計画）の関連付けを実施

システム設計／設定の強化
予備的な技術仕様の作成や最適な設定の推奨を行うことで、システムやセキュリティアーキテクチャの設計を強化

その他

ロールマイニング
アクセス制御を柔軟に行うため、生成AIを利用して、ユーザーの属性に基づいた役割の割り当てを推奨

データの分類と監視
構造化されていないテキストベースのデータを分類し、監視することで、データの抽出（Exfiltration）に対する保護を強化

トレーニングと啓発
従業員の役割、責任、職務要件に基づく、個別化され、的を絞った脅威／危機対応トレーニングを実施

注記：上記は網羅的なリストではありません。また一部のユースケースの実現可能性は、データの可用性やその他の制約に基づいて評価する必要があります。

AIと生成AIの組み合わせで生まれる力

AIをサイバー脅威の検出や対処に利用している組織は、そうしていない組織の一歩先を既に進んでいます。生成AIを何層にも重ねることで、自組織のモデルをさらに複雑で強力なものにすることができます。

従来のAIモデルでも脅威を検出できますが、そこに生成AIを追加することで、インシデントの要約、文書の作成、対応行動計画の策定が可能になると考えられます。

生成AIの活用により、組織は、ルールベース型の分析だけでなく、より高い複雑性と能力を備えた出力も行えるようになるのです。

	要件の提案	セキュリティ侵害インジケーター（IOC）と署名生成	インシデント対応とセキュリティオペレーションセンター（SOC）の自動化のためのコパイロット	対応プロセスの自動化
生成AIの応用	複雑なアプリケーションのためのプロトタイプを開発することで、要件収集のフェーズを簡素化。アナリストと顧客間でのより直感的なやり取りを実現させ、開発に役立てる。	明瞭な署名生成機能を使用したIoCの分類（例えば、特定のセキュリティ侵害に関する情報によって、攻撃が行われた場合にセキュリティチームへの通知が行われる）。	トリアージシグナルと予測ガイダンスを利用することで、隠れたパターンの検出、防御の強化、インシデントへの迅速な対応を実現する。複数のソースのデータを迅速に統合し、実用的な洞察を提示する。	対応プロセスの一環として、サイバー防御戦略、業界への通知、将来に向けた緩和戦略などを自動化する。
メリット	誤解を招くリスクを軽減させる（つまり、アナリストと顧客は、構築フェーズに進む前に、プロトタイプについて意見を整合させることができる）。	サイバー攻撃を迅速に特定し、トリアージすることで、攻撃の可視性を向上させ、セキュリティチームの対応を効率化させる。	インシデント対応、脅威ハンティング、セキュリティ報告のための堅牢かつ信頼性の高いアプローチを導入する。	自動化を行い、インシデント対応計画と緊急時対応計画に対する組織の遵守率を向上させることで、効率化と実行の合理化を図る。
従業員のスキル	• 顧客エンゲージメント（例：レビューサイクル） • ストーリーボード	• 情報の収集 • 任務に対する専門知識／セキュリティクリアランス	• SOC • 脅威の検出と対応	• サイバーセキュリティのためのSOC • 脅威への対応

中核となるAIスキル　データサイエンス、AI／MLエンジニアリング、ディープラーニング、UI／UXデザイン、ハイパフォーマンスコンピューティング、プロンプトエンジニアリング、デジタルオペレーションとデリバリー、学際的な協業、コンピュータビジョン、NLP

生成AIに対する
サイバー脅威の考慮事項

組織は、生成AIが持つ力を理解するにあたり、テクノロジー固有の考慮事項を十分に認識する必要があります。

前述したように、生成AIは組織がサイバー攻撃に備え、防御を行うための新たな機会を切り開くものです。ただし、他のあらゆる新興テクノロジーと同様、生成AIにもリスクがあり、既存のリスクを増大させる可能性もあります。

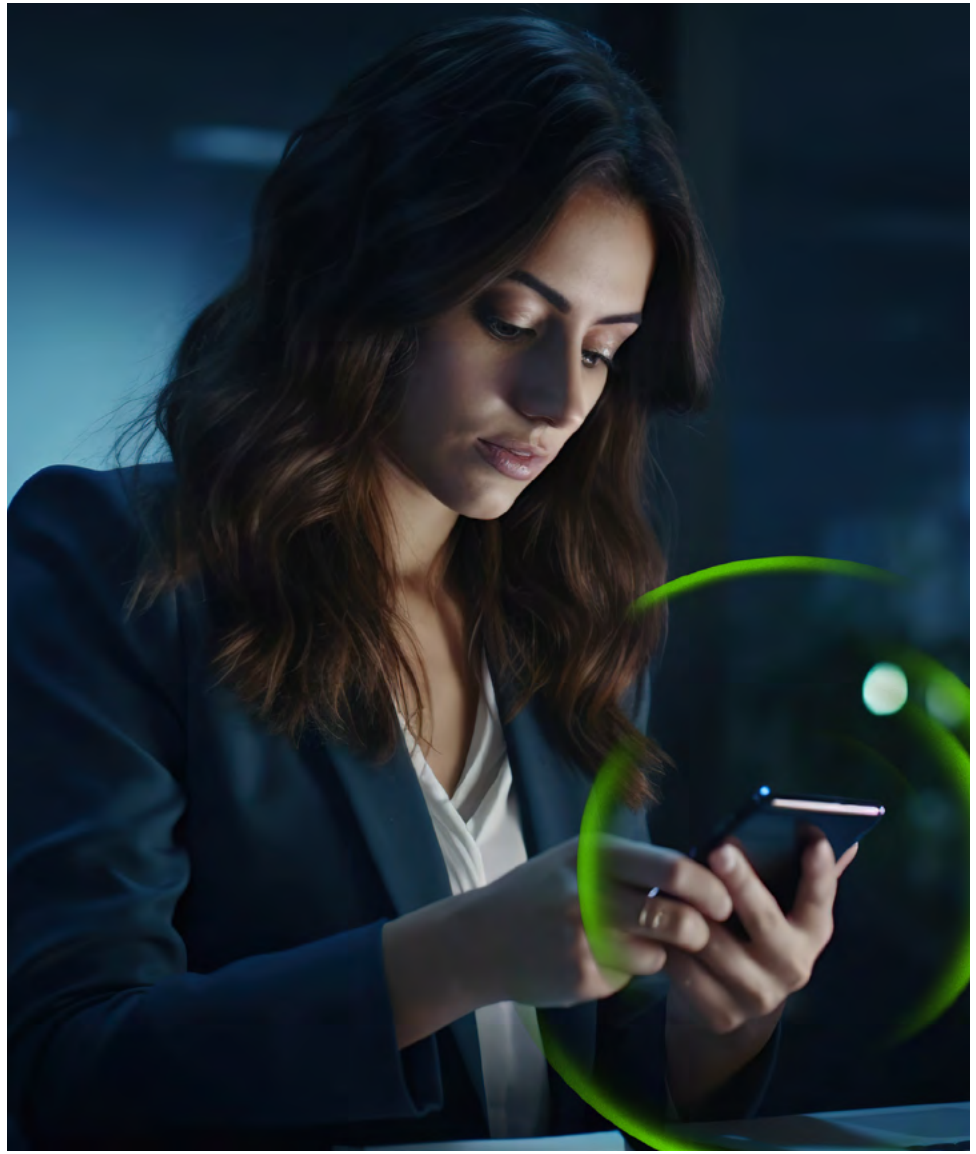
初期のAIシステムは追跡可能であり、そのデータを通じて特定の出力を理解することができました。しかし、生成AIについては、複数のパラメーターによって出力の追跡が困難になる可能性があるため、状況が異なってきます。また、生成AIは従来のAIよりもはるかに大規模なデータセットを用いてトレーニングされているため、データがどこでどのように変更された可能性があるのか、あるいは品質上の懸念がどこに存在し得るのかを把握することがさらに困難になっています。絶え間ない進化を遂げるリスクプロファイルにおいては、新しい視点が求められます。

高まる懸念と世界各地で取られる行動

2023年秋、バイデン政権は、安全性と信頼性の高いAIの利用に関する大統領令を発表しました。この発表は、新しい規制や基準に将来的な影響を与え、規制環境をさらに複雑化させる可能性があります。

一方、欧州連合（EU）はAI関連の規制の厳格化を進めており、場合によっては使用を禁止する方向に動いています。生成AIの利用がより一般化するにつれ、各国政府は潜在的なリスクの軽減に向けてより多くの措置を取ると予想されます。

また、日本では総務省・経済産業省より「AI事業者ガイドライン」が発表されています。同ガイドラインでは、不正操作によってAIの振る舞いに意図せぬ変更または停止が生じることのないように、セキュリティを確保することが重要とされています。



変化を続ける生成AIのサイバーリスク

データの侵害

モデルのトレーニングのため、またはプロンプトを通じて、機密データを外部の生成AIベンダーと共有することは、機密情報や個人情報の漏えいの原因となり得ます。また、敵対的攻撃（Adversarial attacks）は、入力データを変更することでMLモデルを騙すために悪用されます。

セキュリティ保護されていない統合

生成AIツールと組織が使用するその他のシステムを適切に統合し損ねた場合、潜在的な脆弱性（例えば、セキュリティ保護されていないデータチャネル）やバックドアが生み出される可能性があります。

風評リスク

悪意のある攻撃者が生成AIツールを悪用して誤情報やディープフェイクを素早くかつ広範に拡散すると、世論や信頼性、セキュリティに悪影響が及ぶ可能性があります。

規制上のリスク

懸念の高まりが新しい法規制や指針に影響を与えていることを受け、生成AIを利用する組織では、米国立標準技術研究所（NIST）が提案したAIリスクマネジメントフレームワーク[1]やEUによる汎用AIシステムに関する新規制[2]など、新しいコンプライアンス要件への適合が必要になる可能性があります（詳細はこちら）。

各国の関連する機関も、生成AI×サイバーセキュリティのリスクについて度々言及しています

今後2年間におけるAIによるサイバー攻撃の有効性と脅威（英国 国立サイバーセキュリティセンター）

英国 国立サイバーセキュリティセンターは、2024年1月24日に今後2年間におけるAIによるサイバー攻撃の有効性と脅威について、その影響を評価したレポートを公表しました。

The near-term impact of AI on the cyber threat - NCSC.GOV.UK

AIセキュリティに関する研究動向について（日本 内閣サイバーセキュリティセンター）

NISCは、AIセキュリティに関する研究動向について、「AIを活用したサイバーセキュリティ対策（AI for Security）」「AIを使ったサイバー攻撃（Attack using AI）」「AIそのものを守るセキュリティ（Security for AI）」の動向をまとめています。

15shiryou0202.pdf (nisc.go.jp)

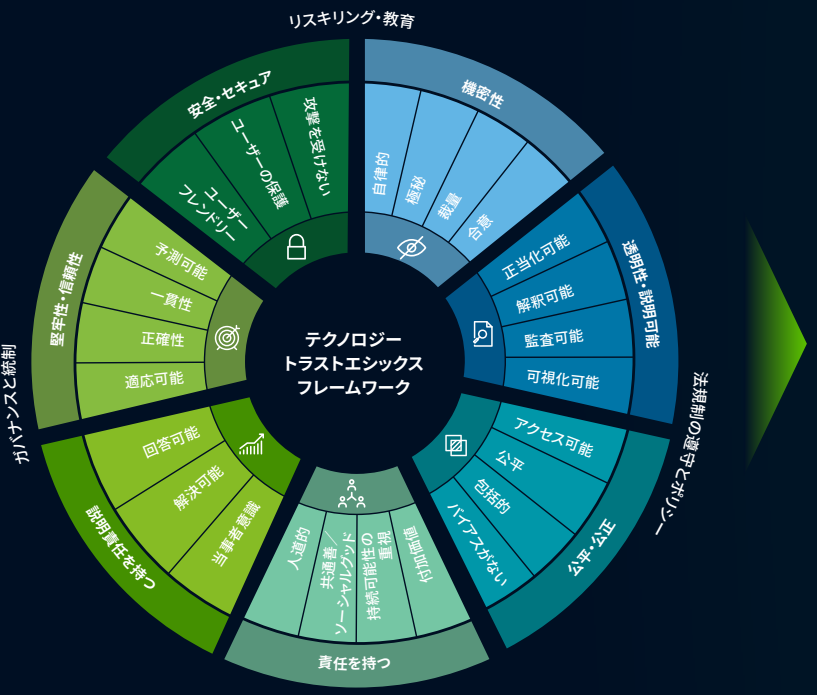
他の有益な情報

Open Worldwide Application Security Project（OWASP）は、学習データのポイズニングやサプライチェーンの脆弱性など、大規模言語モデルを利用するアプリケーションにおけるリスクの上位10位を発表しました[3]。

生成AIに関連するリスクと限界に対応するフレームワーク

新興テクノロジーには固有のリスクが存在します。そこで、AIアプリケーションの構築、展開、商業化に向けてデロイトのテクノロジートラストエシックス（TTE）のフレームワークを活用することができます。

デロイトのTTEフレームワーク



デロイトのTTEフレームワークを基本的な能力や生成AI固有の能力に活用することができます。

基本的な能力

AI戦略

- 包括的なAI戦略と管理フレームワークを定義し、導入する
- 法規制の遵守：進化する規制環境を調査し、新規の要件の登場に備える

AIリスクの管理

- AIに関する統制の設計と実行：AI固有のリスク（例えば、バイアス）に対処するため、規制と業界基準に基づき統制を設計し、実行する
- 統制の監視：統制の有効性を評価し、修復を実行する

AI技術／サイバーセキュリティ

- コード評価とモデル検証：AIの独立テストができるようになる
- 脅威の監視と検出：AIモデルと基盤技術を標的とした特定のテクノロジー脅威（悪意による脅威と環境による脅威）の監視

生成AI固有の能力

ハルシネーションと誤情報の管理

- 適切なガバナンスの仕組みを導入することで、生成AIによる誤情報を特定し、管理する（例えば、従業員のスキルアップ、監視体制の構造化、普遍的な文書化）
- 法規制の遵守：進化する規制環境を調査し、新規の要件の登場に備える

情報源・著作権の管理

- 情報源の帰属の評価と検証を行い、またモデルの使用による盗用や著作権の違反がないことを確認する

生成AIに係る説明責任と説明可能性

- 生成AIについて、また、生成AIの限界、能力、関連するリスクについて、専門的な用語を使わずに明確に説明することに注力する
- 生成AIと基盤技術の利用における説明責任、信頼、倫理に係る実行可能な方法を構想する

どのように備えるか

サイバーリーダーが事前に検討し熟慮を重ねることで、自組織は生成AIが持つ能力やリスクに備えることができます。

組織が持つ特定のニーズにかかわらず、主要な成果を定義し、ガードレールを設置することは、リーダー層が生成AIに関連するリスクへの準備態勢を改善し、レジリエンスを高め、新しいビジネスチャンスを見つけるうえで役立ちます。

リーダー層は、生成AIにおいて技術やトレーニング、各種プロセスに対する新しいアプローチが求められることを認識する必要があります。とはいえ、生成AIに関連するリスクは既存のリスクが進化したものにすぎません。そのため、生成AIには完全に新しいロードマップやトレーニングは必要ないかもしれません。組織の既存のリスク管理体制やサイバー構造でも、生成AIに対処できる可能性があります。

重要になるのは、こうした体制を進化させ、生成AIやAIシステムを標的とし得る微妙なリスクや脅威に対応することです。組織固有のリスクは、SaaS（サービスとしてのソフトウェア）やプライベートLLMなど、どの導入モデルを選択するかによって異なってくる可能性があります。

組織は導入戦略を選択する際、1つや2つの活動を自動化するよりもエンド・ツー・エンドで変革を行うことの効果や必要性を認識する必要があります。

チェックリストの例

- 生成AIに関連する新しい種類のバイアス、法規制、プライバシー、知的財産、データリスクに対応するためのポリシーや統制を更新する。
- 新しいコンプライアンス要件と、既存の法規制に対するコンプライアンス活動への影響を特定する。
- 生成AIのユースケースを入念に評価することで、組織が際立った成果を獲得し、導入に係るあらゆる抵抗に対処するうえで役立てる。
- セキュリティや共有情報の利用について生成AIベンダーが果たすべき契約上の義務を導入し、ベンダーが利用するデータの共有チャネルを監視する。
- 生成AIツールのモデル開発とトレーニングを実施する際のプライバシーとデータ保護に関する基準と統制を導入する。
- バックドアと脆弱性に対応するため、既存のコードレビュープロセスを強化し、生成AIが作成したコードのテストに活用する。
- アクセス制御を実施し、生成AIツールの利用状況を監視することで、不注意な使用や不適切な使用によるリスクを制限できるようにする。
- 企業とクラウドでホストされた生成AIツール間でデータを転送するためのセキュアなチャネルと仕組みを確立する。
- サードパーティーに関する統制を見直し、契約上の義務を確立することで、生成AIベンダーと共有する機密データの保護に役立てる。
- 新たな攻撃（例えば、プロンプトインジェクション）を監視し、生成AIツールの適切な利用を促すことで、脆弱性を防ぐ。
- 組織内で生成AI技術を利用できる「場所」および「時」の境界を明確にする。
- 生成AIアプリケーションをエンタープライズアーキテクチャに統合する際に、セキュリティ・バイ・デザインの原則を取り入れる。
- 誤情報の監視を行うことで組織ブランドの保護を促進し、誤情報の拡散活動に対応し、影響を軽減するためのコミュニケーション戦略を明確化する。
- 敵対的で悪意のある生成AIの使用がもたらすリスクに早急に対処する。

どのように備えるか

何よりも忘れてはならないことがあります。それは、生成AI導入のロードマップにおいては、リスクの理解と予測に役立てるため、サイバーリーダー、リソース責任者、組織の法務チームなど、リスクに関連するステークホルダー間での緊密かつ継続的な協業を考慮する必要があるということです。また、テストの実施や監視についても忘れずに考慮に含めることも重要です。

組織による生成AIの導入を左右する6つの要因

1. **コストと効率性：**生成AIベースのシステムを利用するメリットが関連コストを上回るかどうかを評価する能力。この評価は、大規模なデータセットの処理と保存を行うことで、インフラとコンピュータ資源に関連するコストが増加する可能性があるために必要となる。
2. **知識とプロセスに基づく作業：**現場での物理的な作業のみではなく、高度な知識とプロセスに基づく作業があること。
3. **高レベルなクラウド導入：**インフラ要件を考慮した、中～高レベルのクラウド導入。
4. **規制やプライバシーに関する作業負荷の低さ：**規制の監視やプライバシー上の懸念、倫理的バイアスを伴う職務や業界。
5. **専門的な人材：**技術的な知識と新しい能力を備える強力な人材と、迅速な適応のために職場の変革を促す能力。
6. **知的財産、ライセンス供与、利用契約:**ライセンス供与や利用契約と制限事項の評価、関連するコンプライアンス要件の確立・監視、関連するベンダーと個別の契約について交渉を行う能力。

サイバー攻撃が止むことはありませんが、セキュリティ向上のための生成AIの進化も止まることはありません

生成AIによって、サイバー攻撃とサイバー脅威対応能力の両方が強化される可能性があります。企業はこうした生成AIをめぐる状況の両面を認識する必要があります。

ここで問題となるのは、サイバーリーダーが現在までに作られた中で最も強力な人工知能の能力を活用しながら、混乱の中でどのように自分のチームや組織を先導できるかということです。
多くの組織では、現在抱える問題に対処することで精一杯になっており、開発、運用、新しい人材、進化したプロセスが必要になり得る新しい生成AIエコシステムの構築を検討することは困難となっています。

サイバーリーダーは、生成AIの導入プロセスの手始めとして、組織に固有の問題に対応することが重要です。生成AIは、セキュリティを向上させ、次のレベルの協業を可能にする、新しい種類のコラボレーティブ・インテリジェンスを実現させるかつてないチャンスとなっています。では、リーダーは何から始めることができるのでしょうか。

「もしこうしたらどうなるだろうか」という1つの問いから、すべての可能性が開かれます。

特に日本企業は、先行する海外の事例を踏まえ、リスクが顕在する前に、サイバーセキュリティの施策をアップデートすることが求められます。

欧米やアジア等の国々においては、既にAIによるサイバーセキュリティの脅威が顕在化しており、今後はその流れが日本にも及ぶことが想定されます。特に日本企業においては、そのような海外の企業におけるインシデントの事例や当局の見解、専門家による研究、ITソリューション等の動向を把握して、自社であらためて脅威分析・リスクシナリオの検討を行い、サイバーセキュリティの施策を見直すことが重要になります。

デロイトでは、サイバー分野における豊富な経験、提携関係、将来を見据えた現実的な視点を駆使することで、組織が最も差し迫ったサイバーセキュリティの現在の課題に対処するだけでなく、今後直面していくあらゆる事項に対処していくための支援を提供しています。
詳細については、私たちにご相談ください。

参考資料

1. AI Risk Management Framework | NIST
2. https://www.europarl.europa.eu/news/en/press-room/20231206IPR15699/artificial-intelligence-act-deal-on-comprehensive-rules-for-trustworthy-ai
3. https://www.meti.go.jp/press/2024/04/20240419004/20240419004-1.pdf
4. OWASP Top 10 for LLM Applications Version 1.1, October 16, 2023
5. https://www.ncsc.gov.uk/report/impact-of-ai-on-cyber-threat
6. https://www.nisc.go.jp/pdf/council/cs/kenkyu/dai15/15shiryou0202.pdf

私たちとともに始めましょう

著者

David Caswell, Sabthagiri Saravanan Chandramohan, Deborshi Dutt, Chris Knackstedt, Vikram Reddy Kunchala, David Mapgaonkar, Mike Morris, Abdul Rahman, Kate Fusillo Schmidt, Niels van de Vorle

貢献者

Sanmitra Bhattacharya, Edward Bowen, Ben Bressler, Suzanne Denton, Eric Dull, Lena La, Sajin Mathew, Nirmala Pudota, Stephanie Salih, Colin Soutar

連絡先（グローバル）

Emily Mossburg
Global Cyber Leader
emossburg@deloitte.com
+1 571 766 7048

Adnan Amjad
Cyber & Strategic Risk Offering Leader, Deloitte US
aamjad@deloitte.com
+1 713 982 4825

Amir Belkhelladi
Cyber Leader, Deloitte Canada
abelkhelladi@deloitte.ca
+1 514 393 7035

Ian Blatchford
Cyber Leader, Deloitte Asia Pacific
iblatchford@deloitte.com
+61 474 288 278

Vikram Reddy Kunchala
Cyber & Strategic Risk Solutions Leader, Deloitte US
vkunchala@deloitte.com
+1 713 982 2807

David Mapgaonkar
Cyber & Strategic Risk Industries Leader, Deloitte US
dmapgaonkar@deloitte.com
+1 408 704 4481

César Martín Lara
Cyber Leader, Deloitte Spain
cmartinlara@deloitte.es
+34 91438 1416

Mike Morris
Strategy and Innovation Leader, Deloitte US
micmorris@deloitte.com
+1 303 312 4773

Niels van de Vorle
Cyber Leader, Deloitte North and South Europe
nvandevorle@deloitte.nl
+31 88 2882186

Peter Wirnsperger
Cyber Leader,
Deloitte Central Europe
pwirnsperger@deloitte.de
+49 40 320804675

連絡先（日本）

岩本 高明
パートナー／サイバー戦略担当
takaaki1.iwamoto@tohmatsu.co.jp
+81 70 1552 4899

大場 敏行
マネージングディレクター
toshiyuki.oba@tohmatsu.co.jp
+81 90 9833 4463

Deloitte.
デロイト トーマツ

デロイト トーマツ グループは、日本におけるデロイト アジア パシフィック リミテッドおよびデロイトネットワークのメンバーであるデロイト トーマツ合同会社ならびにそのグループ法人（有限責任監査法人トーマツ、デロイト トーマツ リスクアドバイザリー合同会社、デロイト トーマツ コンサルティング合同会社、デロイト トーマツ ファイナンシャルアドバイザリー合同会社、デロイト トーマツ税理士法人、DT弁護士法人およびデロイト トーマツ グループ合同会社を含む）の総称です。デロイト トーマツ グループは、日本で最大級のプロフェッショナルグループのひとつであり、各法人がそれぞれの適用法令に従い、監査・保証業務、リスクアドバイザリー、コンサルティング、ファイナンシャルアドバイザリー、税務、法務等を提供しています。また、国内約30都市に約2万人の専門家を擁し、多国籍企業や主要な日本企業をクライアントとしています。詳細はデロイト トーマツ グループWebサイト、www.deloitte.com/jpをご覧ください。

Deloitte（デロイト）とは、デロイト トウシュ トーマツ リミテッド（“DTTL”）、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（総称して“デロイトネットワーク”）のひとつまたは複数を指します。DTTL（または“Deloitte Global”）ならびに各メンバーファームおよび関係法人はそれぞれ法的に独立した別個の組織体であり、第三者に関して相互に義務を課しまたは拘束させることはありません。DTTLおよびDTTLの各メンバーファームならびに関係法人は、自らの作為および不作為についてのみ責任を負い、互いに他のファームまたは関係法人の作為および不作為について責任を負うものではありません。DTTLはクライアントへのサービス提供を行いません。詳細はwww.deloitte.com/jp/aboutをご覧ください。
デロイト アジア パシフィック リミテッドはDTTLのメンバーファームであり、保証有限責任会社です。デロイト アジア パシフィック リミテッドのメンバーおよびそれらの関係法人は、それぞれ法的に独立した別個の組織体であり、アジア パシフィックにおける100を超える都市（オークランド、バンコク、北京、ベンガルール、ハノイ、香港、ジャカルタ、クアラルンプール、マニラ、メルボルン、ムンバイ、ニューデリー、大阪、ソウル、上海、シンガポール、シドニー、台北、東京を含む）にてサービスを提供しています。

Deloitte（デロイト）は、監査・保証業務、コンサルティング、ファイナンシャルアドバイザリー、リスクアドバイザリー、税務・法務などに関連する最先端のサービスを、Fortune Global 500®の約9割の企業や多数のプライベート（非公開）企業を含むクライアントに提供しています。デロイトは、資本市場に対する社会的な信頼を高め、クライアントの変革と繁栄を促し、より豊かな経済、公正な社会、持続可能な世界の実現に向けて自ら率先して取り組むことを通じて、計測可能で継続性のある成果をもたらすプロフェッショナルの集団です。デロイトは、創設以来175年余りの歴史を有し、150を超える国・地域にわたって活動を展開しています。“Making an impact that matters”をパーパス（存在理由）として標榜するデロイトの45万人超の人材の活動の詳細については、www.deloitte.comをご覧ください。

Member of
Deloitte Touche Tohmatsu Limited

IS 669126 / ISO 27001

BCMS 764479 / ISO 22301