KPMG

AIが生み出す価値と進化し続けるサイバー脅威の潮流



US Japanese Practice | October 2026

エグゼクティブ サマリー

生成 AI の急速な進化は、前例のないビジネスチャンスをもたらす一方で、重大なセキュリティ上の課題を突きつけています。AI の性能が 4 ヶ月ごとに倍増するなか、明確な AI 戦略の欠如や全社展開の停滞により、具体的なビジネス上のリターン（投資対効果）を具現化できていない企業が少なくありません。同時に、フロンティア AI の台頭はサイバー脅威の潮流を加速させており、企業には人手による従来の防御から、AI を活用した自動化された防御プロセスへの移行が求められています。本稿では、在米日系企業が直面する共通の課題について考察します。

1 AI の発展

生成 AI が一般公開されてから数年が経ち、新たに公表されるモデルは凄まじく進化しているが、どの程度の進化を遂げつつあるかを体感していない方も多いと思う。

例えば、自律的なタスク実行能力に関する外部機関のベンチマーク評価を見ると、その性能は極めて劇的な飛躍を遂げている。初期の 2022 年世代の大規模言語モデル（LLM）は、人間が 1 分未満で完了できるような簡易的なタスクしか実行できなかったのに対し、最新の 2026 年世代の推論型モデルは、人間が実施すると 16 時間程度を要するような高度で複雑なマルチステップのタスクを自律的に実行することが可能となっている。また、最近は性能が 4 ヶ月ごとに 2 倍になっていることが見て取れるようになっており、数年後には人が 1 ヶ月かけて実施するタスクを生成 AI ができるようになるとも予測されている。皆様の組織で 16 時間や 1 か月かけて実施しているタスクにはどのようなものがあるだろうか。それらが AI によって実施できるようになっていると考えると、以前の一問一答のような AI と比較して大幅な進化を遂げていることが分かるのではないだろうか。AI が何でもできるようになるとは言えないが、かなりの作業を担うことができるようになるだろう。

このような AI は多くの企業で導入されているが、実際に AI 利活用によるビジネス上のリターンを具現化している企業は少ないことも分かってきている。これには様々な理由が考えられるが、ここでは紙面上の制限もあるため筆者が日系企業への AI 案件やディスカッションを通じて良くあると感じた 2 つのポイントを挙げたい。

© 2026 KPMG LLP, a Delaware limited liability partnership, and its subsidiaries are part of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved. USCS044886-1A

2 AI 価値創出の主要課題

2.1 AI 戦略が存在しない

AI 活用を通じてビジネス上のリターンを具現化するためには、ビジネス戦略と紐づいた AI 戦略を策定し、どの領域に AI を導入することでビジネス上のリターンが具現化できるかを明確化しておく必要がある。各従業員任せ (自発的) で AI を利活用させたり AI エージェントを構築させることが必要なフェーズもあるが、それだけだとビジネス上のリターンが具現化できないケースが多いのも事実である。また AI 戦略の中でリターンの測定方法についても明示すべきであり、更には (当然だが) 定期的に ROI を測定し、必要に応じて方向性を修正することも重要となる。

2.2 AI を全社展開できていない

2025 年の MIT 調査になるが、タスクに特化した LLM を対象にした場合、全社展開できてている企業は 5%しかない、との報告も出ている[1]。これは「取りあえずパイロット導入」という考えで導入を進めて、データ、人、ガバナンス、業務プロセスといった、AI 以外の分野における重要な変革がおざなりになっているケースが多いことが背景にある。ここではデータ、人、ガバナンスの 3 つに絞って説明したい。なお、「取りあえずパイロット」が悪いのではなく、それ以外の側面に注意を払わないのが問題である点に留意していただきたい。

- **データ**

  データは AI を導入するにあたっての土台になるため、これを整備することは非常に重要である。パイロットは特定の部門に閉じて実装されることが多いため、全社展開時に部門を跨ぐ際には各部門でのデータ整備が重要となる。一方で、全社の全データを整備することを AI 導入の前提としてしまうと、AI 導入が進まなくなってしまう。特定の AI を導入するにあたって必要となるデータに絞って整備するなどの工夫も必要となる。

- **人 (ひと)**

  AI を導入したら人が不要になる訳ではない。人が AI を使って仕事を進める必要が出てくるため、人への投資が重要になってくる。トレーニングはもっとも分かりやすい点だが、それ以外にも幾つかポイントがある。

  - 心理的安全性の確保：AI の導入にはトライアル＆エラーがつきものなので、失敗することに対する心理的安全性を醸成する必要がある。
  - 評価制度：例えば、特定タスクを AI を使わずに長時間かけて完了する人材に比べて、AI を使って同じタスクを短時間で完了することができる人材の評価は高くなるべきだろう。従って人事評価をアウトプットベースに変更していくことも検討すべきである。

- **ガバナンス**

  多くのユーザーは AI が出してきた結果を信用していないし、他人が AI を使って作ったアウトプットについては更に信頼性が低いと感じている。KPMG では AI のアウトプットに対する信頼性を見える化する仕組みなどを用意しているが、このような仕組みを活用して AI の回答やアウトプット資料などに対する信頼性を見える化して共有することが重要になる。

---

[1] 出典：MIT Project NANDA『The GenAI Divide: State of AI in Business 2025』(2025 年 7 月)

© 2026 KPMG LLP, a Delaware limited liability partnership, and its subsidiaries are part of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved. USCS044886-1A

3 フロンティア AI を使ったサイバー攻撃

ここまではビジネス上のリターンに直結する AI を構築するために必要となる事項を簡単に記載してきたが、AI にはマイナス面もある。そのひとつがフロンティア AI を活用したサイバー攻撃である。ここではフロンティア AI がサイバー攻撃を活性化する理由や、どのようなサイバーの世界が待っていると考えられるのかを簡単に紹介したい。

フロンティア AI のサイバー攻撃能力については新聞などにも掲載されているので詳細は省くが、これからは脆弱性の調査から攻撃までの時間が急速に短縮化し、24 時間未満で攻撃を完結することができると想定されている。一方で、多くの企業は脆弱性を是正するためのパッチ適用に 60 日程度の時間をかけており、工場などの OT システムに至っては平均して 18 ヶ月かかっている。つまり守る側は穴を埋めるのに 60 日～18 ヶ月かかるのに、攻める側は穴を見つけてから攻撃まで 24 時間で完結させられるわけであるから、大変な状況になり得ることは自明であろう。

表：脆弱性対応タイムライン

主体	アクション	所要時間
攻撃者	脆弱性発見から攻撃実行まで	24 時間未満
一般的な企業・組織	修正パッチの適用	約 60 日
制御システム (OT)	工場等の製造現場におけるパッチ適用	約 18 ヶ月

出典：AI を活用した攻撃スピードの動向、ならびに企業の脆弱性修正および制御システム（OT）の保守サイクルに関する KPMG の知見・業界平均に基づく(2026 年)。

また AI エージェントを使って攻撃を並列化することも起きつつある。守る側を人間だけに頼ると複数の脆弱性を同時に突くような攻撃には耐えられないだろう。今のところサイバー攻撃能力を押さえたモデルのみが公開されているが、高性能で安価なオープンモデルも登場してきており、悪意を持った集団や個人がサイバー攻撃能力に制限を掛けないモデルを手にする日も遠くないと想定される。

4 防御プロセスの自動化

このような攻撃に対しては、防御プロセスを自動化することが求められる。ただ、「明日から防御用の AI エージェントを使って防御プロセスを自動化してください」と言っても実現は容易ではない。防御プロセスの自動化には幾つかの重要ポイントがある。(紙面の関係上、一部だけ記載)

- **攻撃対象となり得る IT 資産の一元管理**
  IT などの資産、ID、インターネットに面したサービスや依存関係を一元的に把握し管理する必要がある。一元的に管理・可視化されていないものを多層的に防御することはできない。

© 2026 KPMG LLP, a Delaware limited liability partnership, and its subsidiaries are part of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved. USCS044886-1A

- **重要な資産に対する迅速なパッチ適用の運用開始**
  パッチを適用することで脆弱性に対応することができるため、パッチが公開されてから 60 分以内程度にパッチを適用する運用を開始する必要がある。
- **封じ込めや緩和策の自動化**
  パッチが公開される前に脆弱性を突かれる可能性は十分にあるため、攻撃を受けた IT 資産を自動的に隔離するプロセスを準備する必要がある。ただ、現状では複数のステークホルダーが IT 資産の隔離に関する意思決定に関与していたり、簡単には止められないサービスや業務プロセスも多く存在したりする。よって、まずは IT 資産ごとに IT 資産の隔離やセグメンテーション対応プロセスを見える化し、AI エージェントを使った自動化に向けた準備を始める必要がある。

5 おわりに

AI はツールである。業務改革、顧客満足度向上や事業モデル変革のための非常に有効なツールにもなり得るし、サイバー攻撃にも防御にも使うことができる。一方で、これらを使わない選択肢は徐々に失われつつある。競争優位性の維持と強固なセキュリティ態勢の確立に向け、企業は事業の「攻め」と「守り」の双方において、AI を戦略的に組み込んでいくことが不可欠である。

お問合せ



Nobuhiro Tamura 田村 暢大
Senior Director, Advisory
KPMG LLP
ntamura1@kpmg.com

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

Learn about us: **kpmg.com**

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act upon such information without appropriate professional advice after a thorough examination of the particular situation.

© 2026 KPMG LLP, a Delaware limited liability partnership, and its subsidiaries are part of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved. USCS044886-1A

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