Press Release

2024 年 12 月 17 日

生成AIの業務利用をリスクとして認識している組織は98.4%、65.7%が生成AIの普及が外部からの攻撃リスクへの増大に繋がると認識

～生成AIとセキュリティに関する意識調査～

トレンドマイクロ株式会社（本社：東京都新宿区、代表取締役社長 兼 CEO：エバ・チェン　東証プライム：4704）と特定非営利活動法人 CIO Lounge（所在地：大阪府大阪市北区、理事長：矢島孝應）は、国内の法人組織（従業員 500 名以上）の経営者、セキュリティやリスクマネジメントの責任者（部長以上）300 人を対象に「生成 AI とセキュリティに関する意識調査」を実施しました※1。

※1 調査結果のパーセンテージは、小数点以下第二位を四捨五入した数値です。合計が 100%にならない場合があります。

生成 AI の業務利用とセキュリティに関する調査レポート全文はこちら

■調査結果トピックス

- 77.6%の組織で生成 AI を業務利用、従業員規模が大きくなれば業務利用率も上がる傾向
- 生成 AI を利用している業務は文書・資料の作成が 75.5%で最多
- 生成 AI の業務利用をリスクとして認識している組織は 98.4%、 65.7%が生成 AI の普及が外部からの攻撃リスクへの増大に繋がると認識
- 生成 AI の業務利用に際し特段セキュリティ教育は実施していない割合は 27.1%

● 77.6%の組織で生成 AI を業務利用、従業員規模が大きくなれば業務利用率も上がる傾向

生成 AI の業務利用について聞いたところ、業務利用を認めていると回答した割合は、77.6%でした。従業員規模が大きくなるにつれて、業務での利用を認める傾向が出ており、5000 人以上の規模では 8 割以上の割合で業務利用を認めているという結果になっています。組織が大きくなるにつれて、投資余力の観点から生成 AI サービスを導入できる予算が確保しやすいことや、部署間のコミュニケーションや情報共有の機会が多く生成 AI による効率化による恩恵が大きいことなどが、この理由として考えられます。

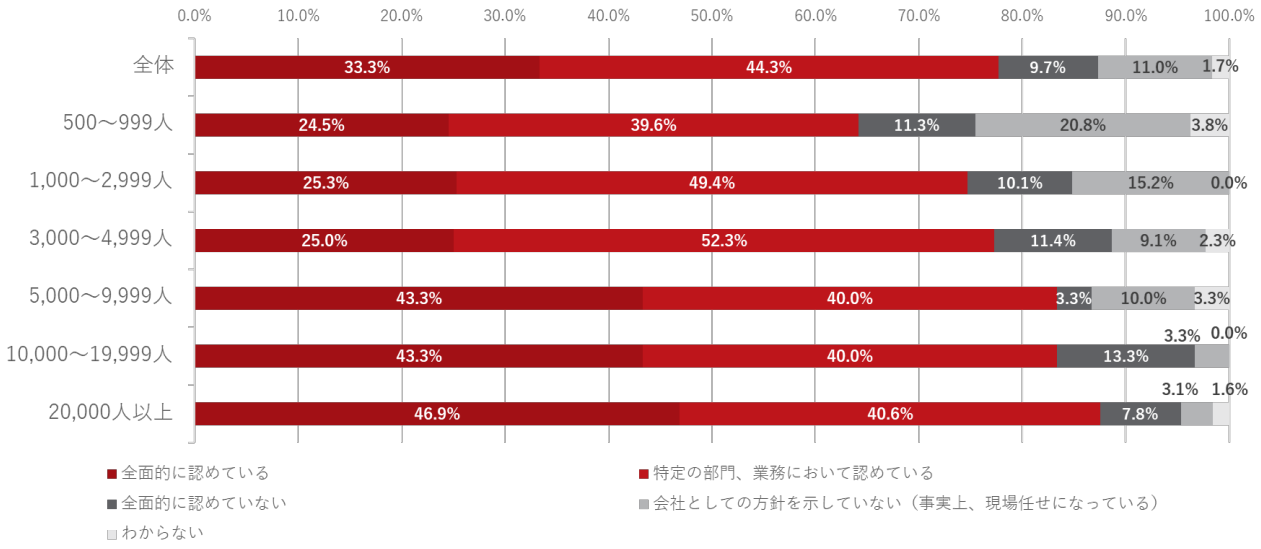

図1：生成AIの業務利用度合い（n=300）
質問「お勤め先の会社では、生成AIを業務で利用することを認めていますか」（単一回答）

● 生成 AI を利用している業務は文書・資料の作成が 75.5%で最多

生成 AI をどのような業務で利用しているのかを聞いたところ、文書（メールや報告書）・資料の作成が 75.5%で最多となっています。また、プログラムの作成、生成 AI を活用した独自サービスの開発も 3 割を超えており、作業効率化以外にも技術的な側面でのニーズがあることが明らかになっています。

一方で、技術的な側面での業務利用においては、AI が提案したコードの品質や安全性の検証が不十分になる危険性などもあり、適切なリスク管理と運用ルールの整備が不可欠になります。特に大規模なシステムや個人情報などを取り扱うサービスの開発では、慎重なアプローチが求められます。

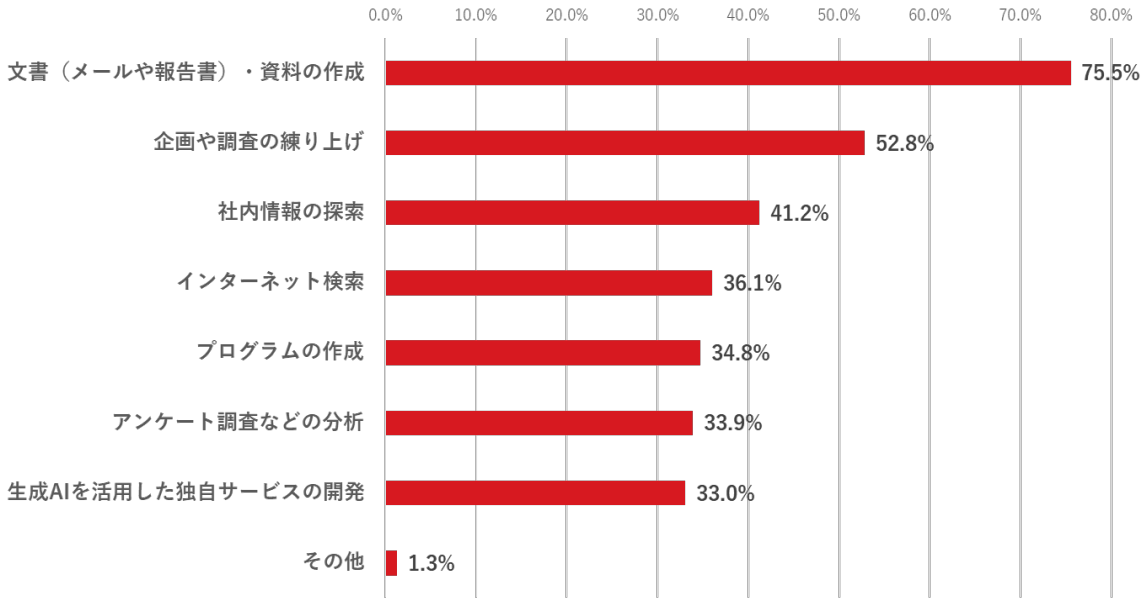

図2：生成AIの業務利用の内容（n=233：業務利用を認めている回答者に限定）
質問「お勤め先の会社では、どういった業務で生成AIを利用していますか」（複数回答）

● 生成 AI の業務利用をリスクとして認識している組織は 98.4%、 65.7%が生成 AI の普及が外部からの攻撃リスクへの増大に繋がると認識

生成 AI の業務利用におけるリスクの認識について聞いたところ、「特に懸念しているリスクはない」「わからない」の回答を除く 98.4%の組織が何らかのリスクを認識していることがわかっています。リスクの内容については、著作権や肖像権など法的権利の侵害が 63.7%で最多、機密情報などの入力による情報漏洩が 61.3%で次点となっています。実際に、著作権侵害については訴訟問題へ発展しているケース、情報漏洩についても機密情報を入力したことで誤って外部に送信してしまったケースが、それぞれ報道されています。

生成 AI 特有の課題として、プロンプトの入力をシステムだけで制限することが難しいため、従業員の判断に依存する部分が大きいことが挙げられます。そのため、生成 AI の業務利用を行っている組織は、ガイドラインの制定や従業員教育などの人的・組織的な対応が重要になっています。

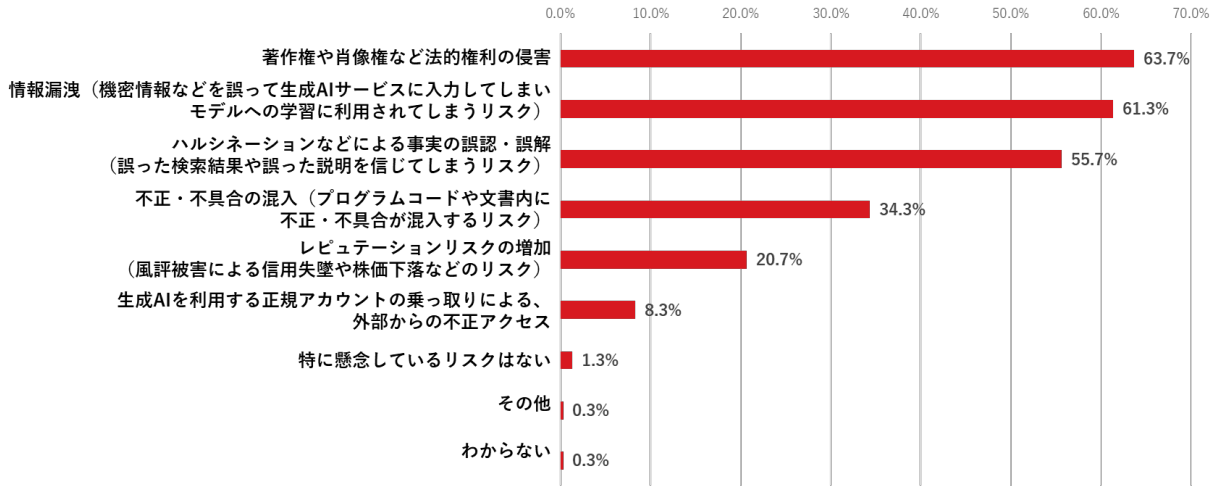

図3：生成AIの業務利用におけるリスク（n=233：業務利用を認めている回答者に限定）
質問「生成AIを業務で利用する際、リスクとして認識しているものを
上位３つまでお答えください」
（3つまで回答：「特に懸念しているリスクはない」「わからない」と他の選択肢は排他）

生成 AI の普及で外部からの攻撃リスクが増大するかを聞いたところ、65.7%が増大すると思うと回答しています。生成 AI がサイバー攻撃者にとっても多くのメリットをもたらすツールであり、フィッシングメールの生成や、マルウェアの作成において利用されるケースが想定されます。実際に日本でも生成 AI を悪用してランサムウェアを作成したとして逮捕まで至った事例が発生しており、そのリスクが現実のものとなっています。今回の調査結果では、生成 AI によるサイバー脅威の増大を認識している割合が過半数を超えており、生成 AI の悪用に対する懸念が広がっていることが分かります。

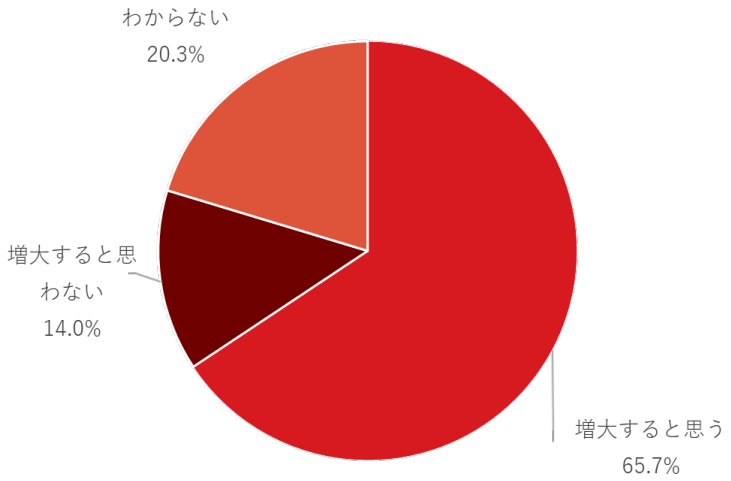

図4：生成AIによる外部からの攻撃リスク（n=233：業務利用を認めている回答者に限定）
質問「生成AIの普及により、外部からの攻撃リスクは増大すると思いますか」（単一回答）

● 生成 AI の業務利用に際し特段セキュリティ教育は実施していない割合は 27.1%

ルールやガイドラインの整備状況、セキュリティ教育の実施状況について聞いたところ、ガイドラインを整備している割合は 93.6%に上る一方で、セキュリティ教育を実施していない割合は 27.1%となっています。

この結果から、一定数の割合の組織が、コンプライアンス上の要請から形式的なルール化は行っているものの、それを従業員に伝える体制が構築できていないのではないかと考えられます。この状況を放置すると、ルールが形骸化してしまい、インシデントが発生する可能性が増大することが想定されます。そのため、組織においては従業員教育の機会を設けるとともに、定期的なフォローアップの機会を作っていくことが求められます。

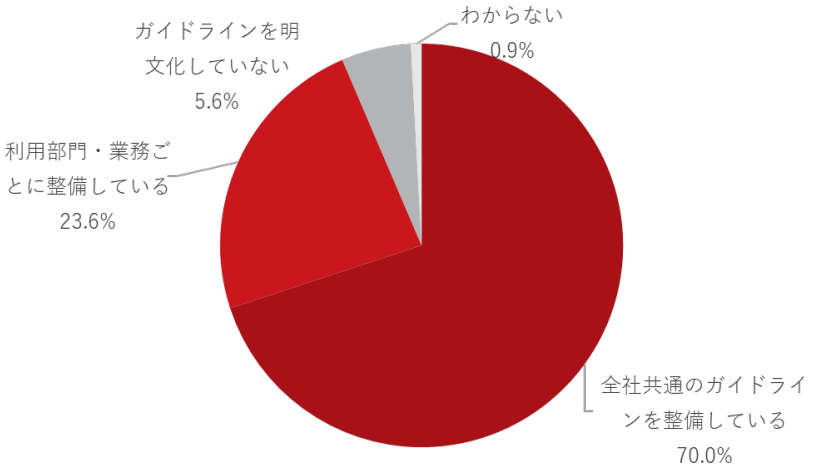

図5：ガイドラインの整備状況（n=233：業務利用を認めている回答者に限定）
質問「生成AIの利用に関しガイドラインの整備や教育を実施していますか」（単一回答）

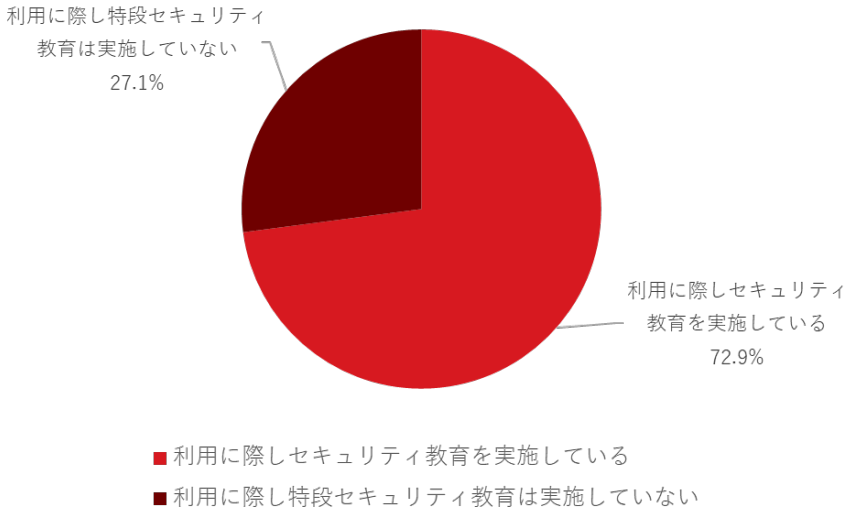

図6：生成AIの業務利用に際したセキュリティ教育の実施状況
（n=218：業務利用を認めている・ガイドラインを整備している回答者に限定）
質問「生成AIの利用に関しガイドラインの整備や教育を実施していますか」（単一回答）

■調査概要

調査手法（サンプリング）	インターネット調査
調査地域	日本国内
調査対象者	従業員規模500名以上の法人組織の経営者、セキュリティやリスクマネジメントの責任者（部長以上）
回答者数	300
調査時期	2024年9月
調査主体	トレンドマイクロ株式会社、特定非営利活動法人 CIO Lounge

※ 2024年12月17日現在の情報をもとに作成したものです。今後、内容の全部もしくは一部に変更が生じる可能性があります。

本件に関するお問合せ先
マーケティング本部 広報グループ
成田・高橋・中村・牧野
e-mail：pressweb@trendmicro.com
Web ページ:https://www.trendmicro.co.jp

商品に関するお問合せ先
営業 TEL　　：03－4330－7601
紙誌面掲載用 TEL：03－4330－7601