AI利用時のセキュリティ脅威・リスク調査
調査報告書

2024年07月04日発行
独立行政法人情報処理推進機構
セキュリティセンター　企画部　調査グループ

IPA Better Life with IT

7月5日修正版

目次

- 調査概要
- 調査項目
- 回答者属性情報
- 調査結果
  1. AIサービスの利用状況
  2. セキュリティの脅威認識
  3. セキュリティ対策の必要性
  4. セキュリティ対策状況
  5. 生成AI利用の課題と対策状況
  6. AIサービスを利用しない理由
- 調査まとめ
- 提言

本資料に掲載しているグラフ内の数値の合計は、小数点以下の端数処理のため100%にならない場合があります。

調査概要

- 目的

生成AIの登場により、業務でのAI利用機会が増えているが、一方AI利用の脅威やリスクについては十分な検討がされておらず、今後悪用や誤用によるサイバー攻撃やインシデントが懸念される。

本調査ではAIの業務利用の浸透具合やセキュリティ上の脅威・リスクの認識について、企業・組織の実務担当者に対してアンケートを実施した。

調査期間　２０２４年３月１８日～２１日

調査方法　ウェブアンケート

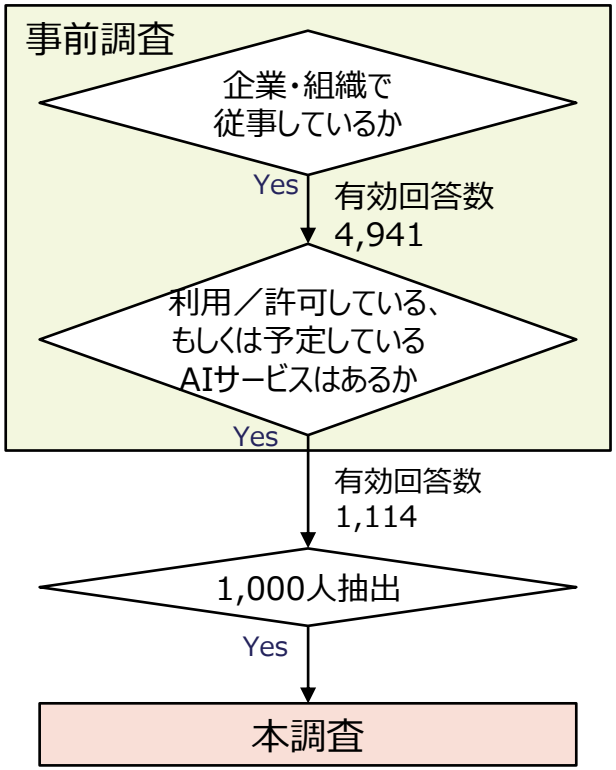
調査委託先　株式会社アスマーク

回収数　事前調査　企業・組織で従事する人　4941人

本調査　予備調査の回答者の中でAIを業務で利用している人　1000人

調査項目

- 事前調査
  - 基本情報（5問）
    - 年代、職業、業種、役職、従業員数
  - 設問（6問）
    - AI利用状況、AI利用上の立場、最重要AI、AIを利用／許可しない理由、担当業務、AI理解度
- 本調査（12問）
  - AIの業務利用時の検討項目と重要度
  - AI利用における管理コストの負担
  - AI利用に関する組織の対応手順や体制
  - AIのセキュリティに関する脅威
  - 生成AIの利用・評価における課題
  - 生成AIで生成したコンテンツの課題　　等
    - 詳細は別紙参照
    - 本調査においては、生成AIと分類AIに分けた設問と分けない設問があります。

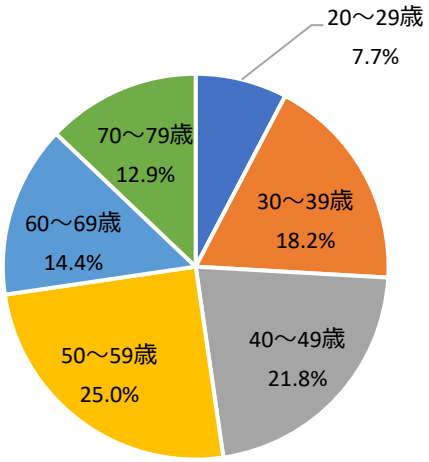


生成AI：入力したプロンプト（質問）に基づいて最もマッチするコンテンツを検索あるいは生成します。
応用分野は、チャット・質問回答サービス、音声・画像合成、文書作成、文書チェック、プログラム生成・チェックなどです。代表例がChatGPT。
分類AI：入力データを学習済みのモデルに基づいて分類し、分類結果を判定・診断・予測・制御等に用いります。応用分野は、音声・画像認識、状態監視、異常検知、市場予測、自動制御、自動走行などです。従来のAI。

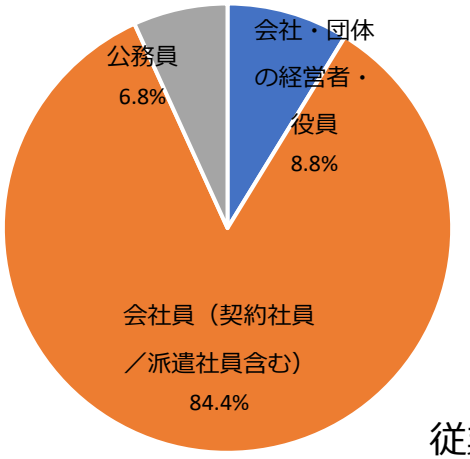
回答者全員に聞きました

回答者属性情報

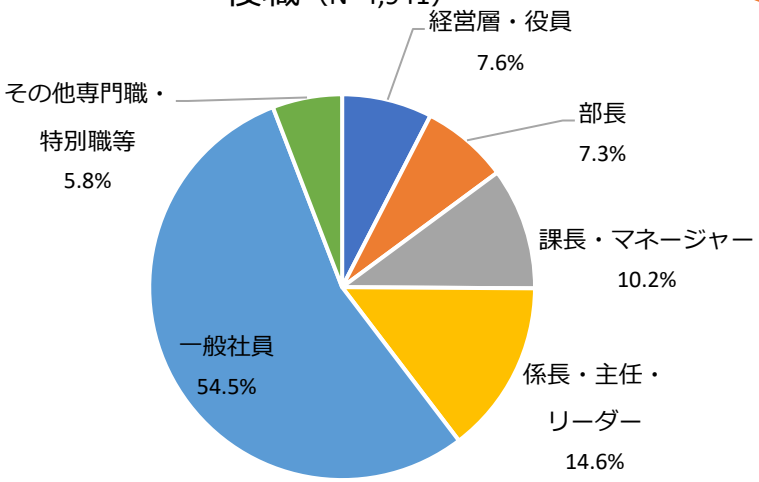
年代（N=4,941）



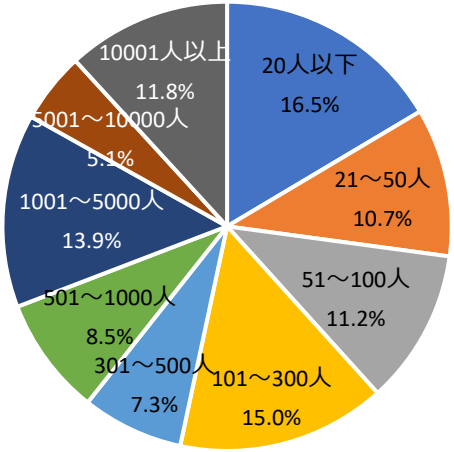
職業（N=4,941）



役職（N=4,941）



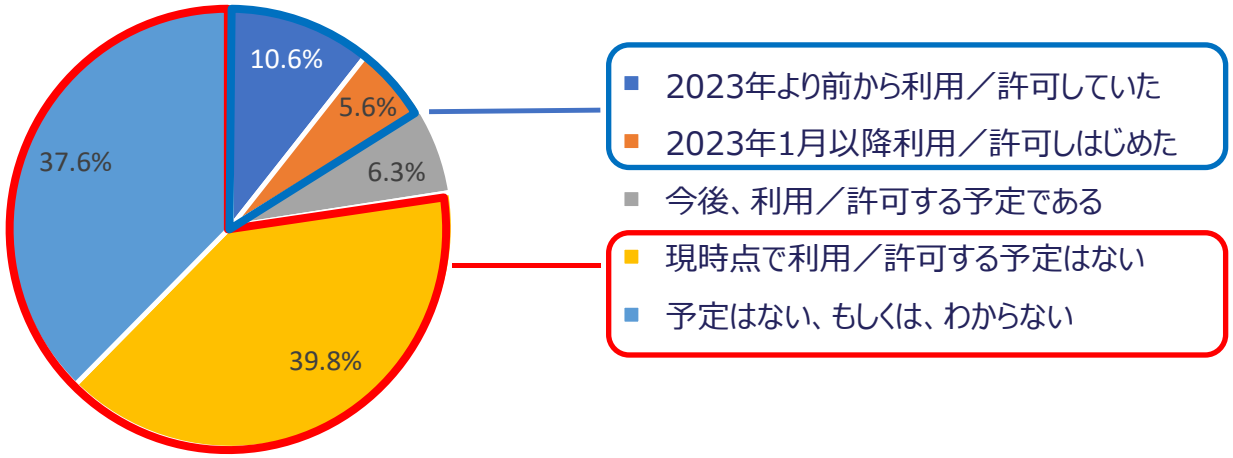
従業員数（N=4,941）



回答者全員に聞きました

AIの利用状況

質問：あなたの所属する組織では
業務でのAI利用、あるいは、職員の業務での**AI利用許可**を
していますか？



2024年3月時点の
AIの利用

している	16.2%
予定あり	6.3%
していない	77.4%

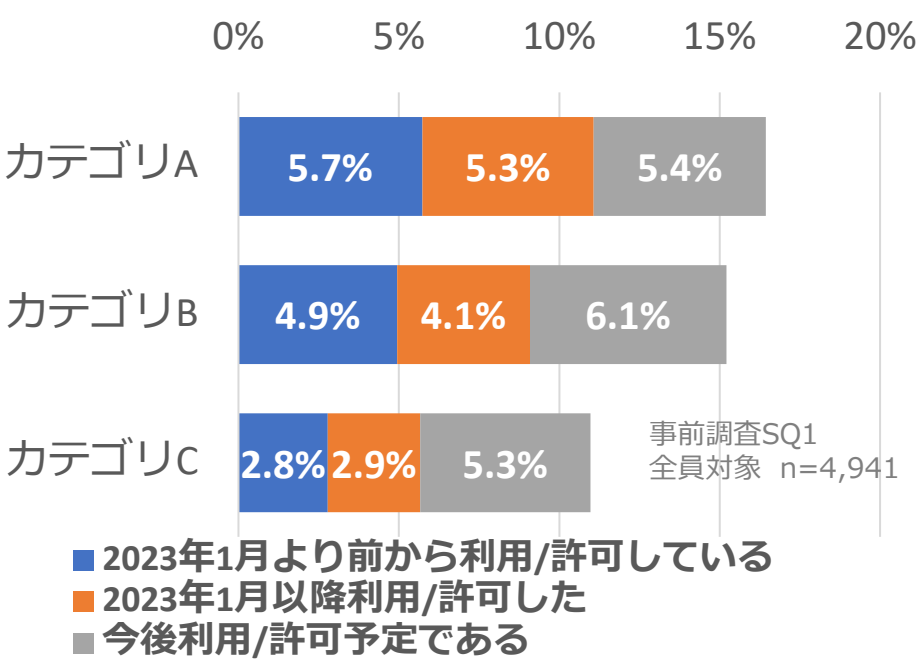
事前調査SQ1　全員対象　n=4,941

2024年3月時点で業務でAIを利用/許可しているのは16.2%、
予定ありを合わせても**22.5%（回答者4,941人中1,114人）**とまだ十分浸透はしていない。
しかし、個々のサービスを見る利用が加速していることがうかがえる。詳細は別冊参照

回答者全員に聞きました

生成AI登場によりAIの業務利用は加速している

- 質問：**いつから業務で**AIを利用あるいは利用許可していますか？

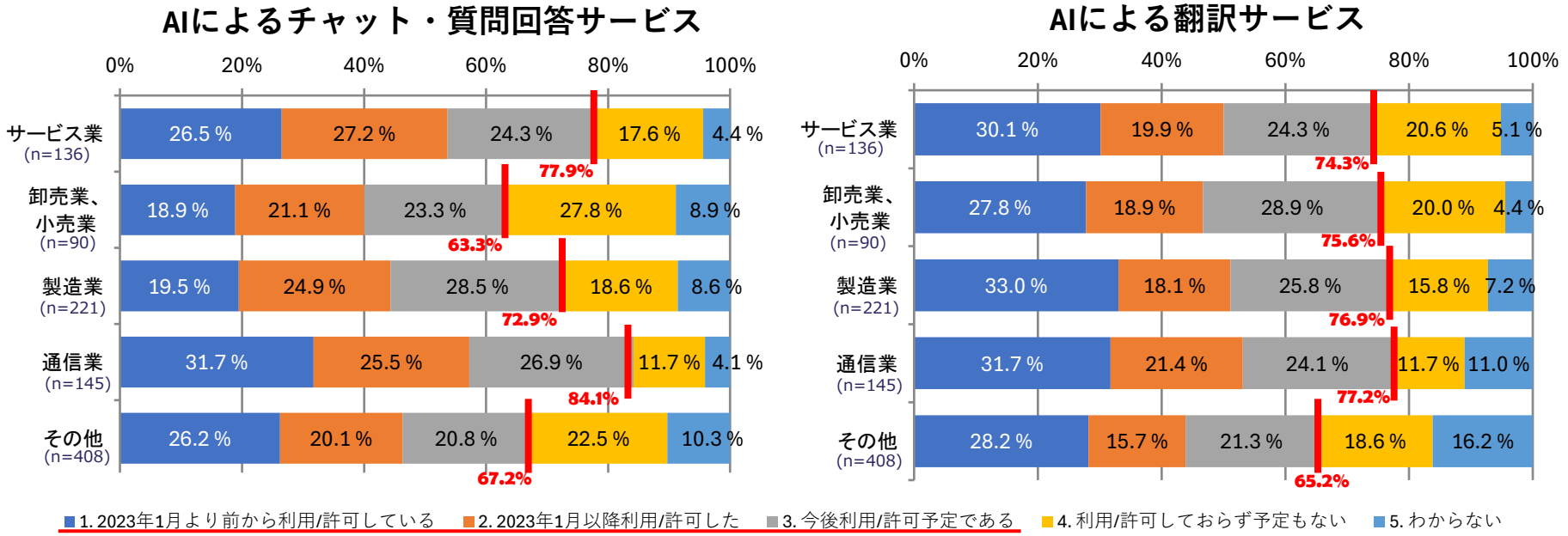


特徴		サービス例	カテゴリ
業種共通	顧客向けサービス改善	チャット・質問回答	A
業種共通	社内業務効率化	翻訳、文案作成、文章チェック、効率化、自動化	B
業種・業務の専門性が必要		法務文書作成・チェック、仕様書作成支援、ソフトウェア開発支援、学習支援、画像生成、リスク分析、カスタマサービス、セキュリティ監視、トレンド予測、運用監視等	C

業種共通的に利用可能なサービスから利用が進んでいる。
その中でも、チャット・質問回答といった**顧客向けサービス改善**に有効と考えられるAIサービスの利用が先行しており、**社内業務効率化**に有効と考えられる翻訳や文案作成などのサービスが続く。
業種・業務の専門性が必要と考えられるサービスも含むすべてのカテゴリにおいて、2023年だけで、**それ以前と同程度に利用率が増加**しており、今後はさらに**利用が加速すると考えられる。**

AIを利用/許可している、
予定がある人に聞きました

導入率の高いサービスの業種別利用状況



導入率トップ２の業種別利用状況(事前調査SQ1　AIを利用/許可している、予定がある人n=1,000)

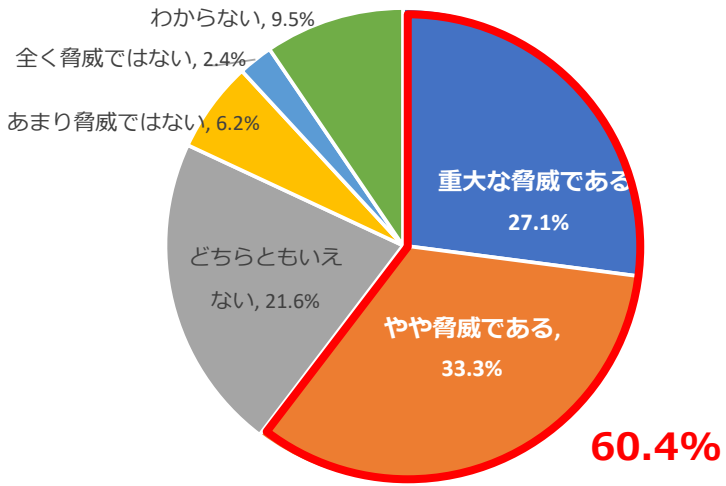
回答数が90件を超えていた4業種以外はその他としている。

<u>第1位のチャット・質問回答サービス</u>は、特に**<u>通信業、サービス業</u>**で導入が進んでいる。
導入率にばらつきは見られるのは、業種の特性によるところが大きいと思われる。
<u>第2位の翻訳サービスは</u>2023年より前から導入されてきており、
その他の業種を除くと**<u>導入率に業種の差はあまりない。</u>**
2023年間や今後の予定から見ても企業での代表的な利用方法として定着しつつある。

AIを利用/許可している、
予定がある人に聞きました

6割がセキュリティ脅威を感じ 7割がセキュリティ対策が重要であると回答

質問　あなたの組織にとって、AIのセキュリティに関する脅威はどの程度？



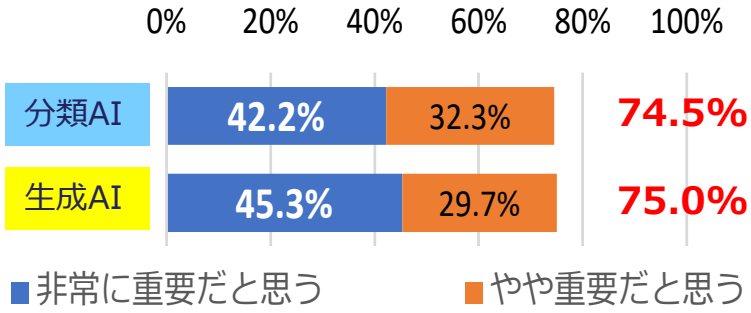
AIのセキュリティに関する脅威の度合い

（本調査　Q10　全体平均
対象　AIを利用/許可している、または予定があると回答した1,000人）

調査項目では、虚偽拡散、検証不備による事業トラブル、攻撃激化、詐欺、システム障害、情報漏えい等の脅威について個別に回答を得た。詳細は別冊参照。

回答者の**約6割はAIのセキュリティに関して脅威を感じている。**

質問　AIの導入・利用に「セキュリティ対策」はどれくらい重要？



AIの導入・利用可否における セキュリティ対策の重要度の度合い

（本調査　Q1Q2　「セキュリティ対策」抜粋
対象　AIを利用/許可している、または予定があると回答した1,000人）

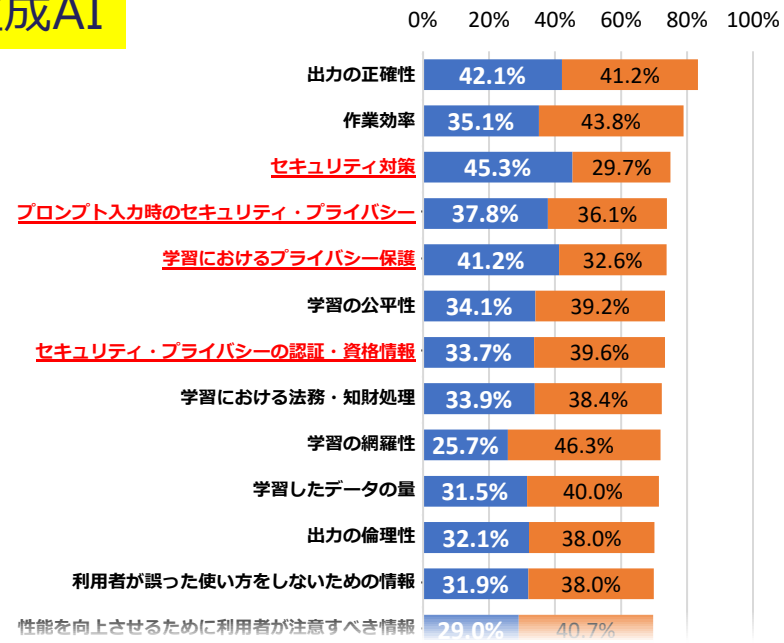
AIの導入・利用に**セキュリティ対策は重要である**という回答者は分類AI、生成AIともに**7割を超えている。**

AIシステムの堅牢性や個人情報の適切な取り扱いを重要と考えている

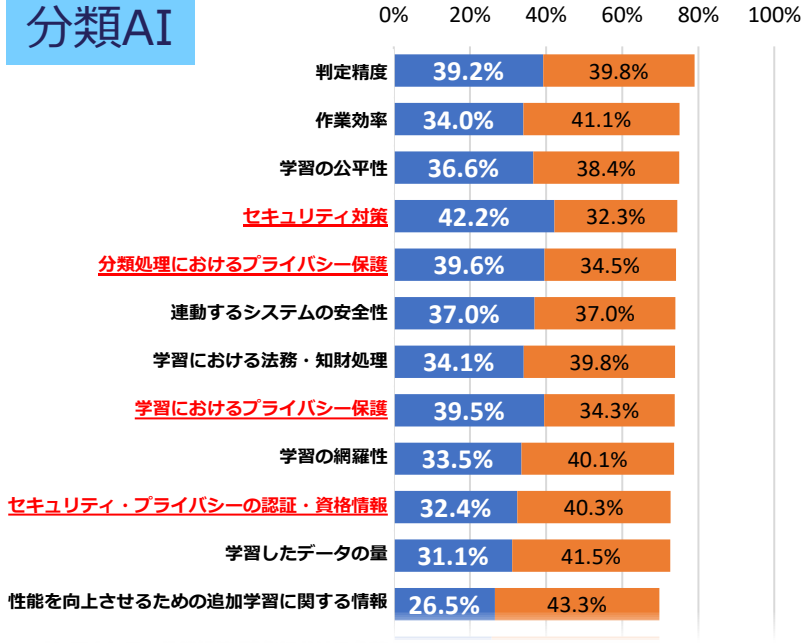
AIを利用/許可している、予定がある人に聞きました

- 質問：次の尺度はAIの導入・利用可否にどれくらい重要ですか？

生成AI



分類AI



セキュリティやプライバシーに関する項目は上位にあり、特に、**セキュリティ対策が「非常に重要だと思う」**と回答している人は**生成AI（45.3%）、分類AI（42.2%）とともに最も多い。**
AIの導入・利用検討において、AIシステムの堅牢性や個人情報の適切な取り扱いを重要と考えていることがわかる。

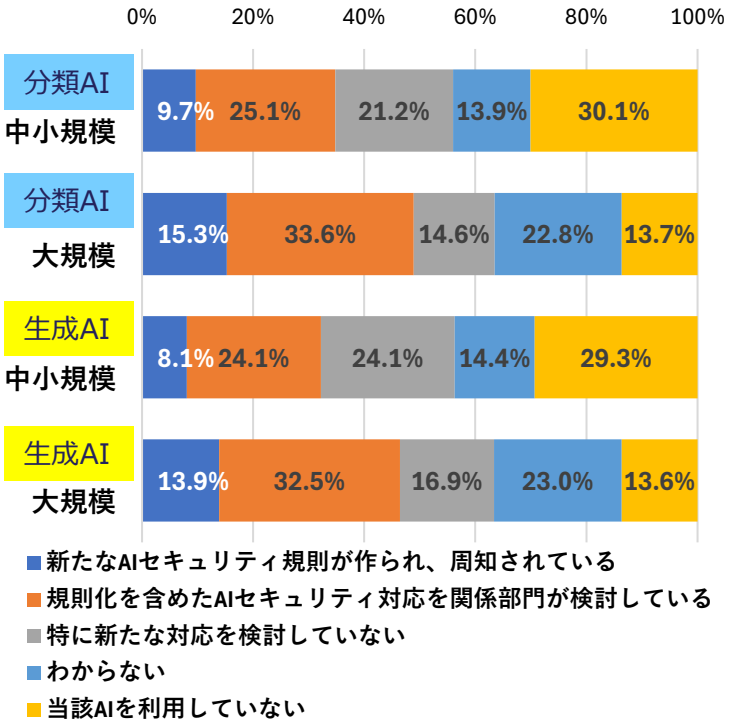
詳細は、別冊参照

（本調査Q1,Q2
対象　AIを利用/許可している、または予定があると回答した1,000人）

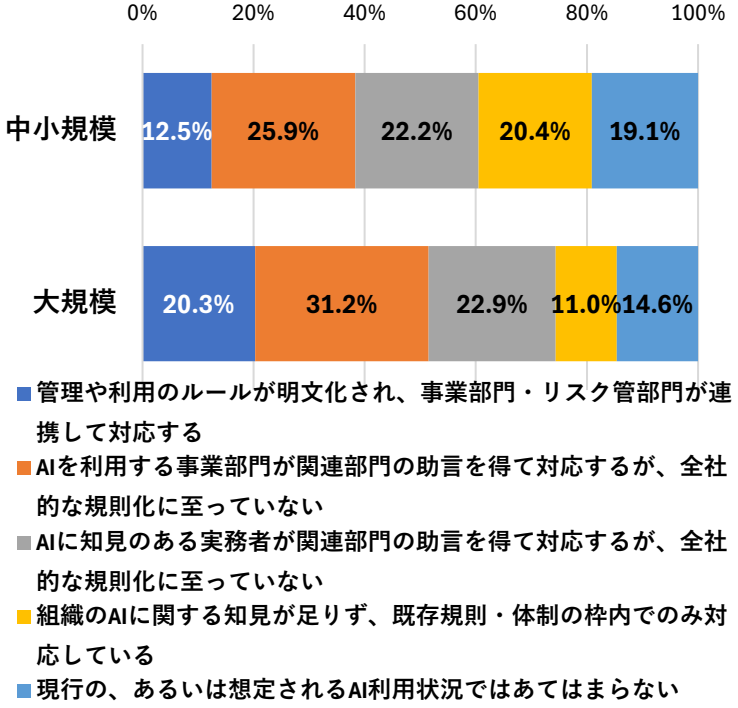
AIの対策状況(規則や体制整備)は規模によりに差がある

AIを利用/許可している、予定がある人に聞きました

質問　AIサービスの利用に関するセキュリティ規則は作成、周知されているか



質問　AI利用に関するマネジメントについて対応手順や体制は整っているか



セキュリティ規則の対応の度合い

（本調査　Q7 分類AI、生成AIの回答結果を規模別に集計
対象　AIを利用/許可している、または予定があると回答した1,000人）

AI利用に関するマネジメント手順・体制

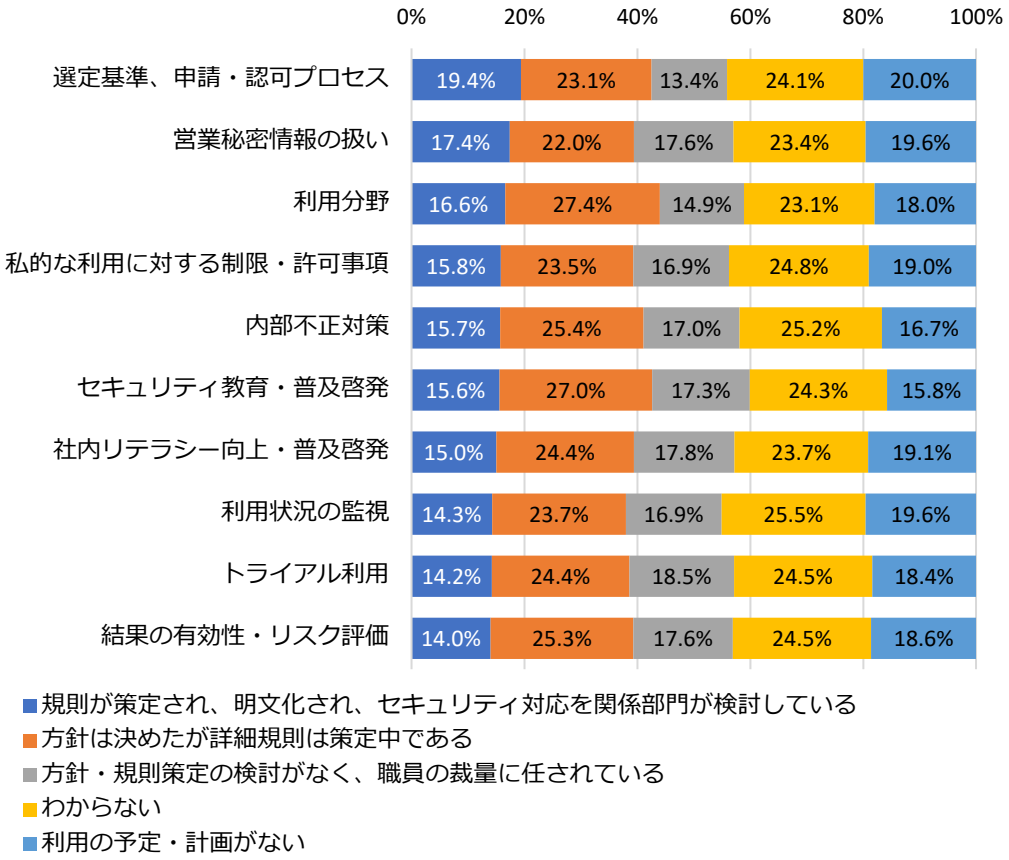
（本調査　Q5 規模別の回答結果を集計
対象　AIを利用/許可している、または予定があると回答した1,000人）
（中小規模312、大規模688）

以下の業種については101人以上を大規模、それ以外の業種については301人以上を大規模としています。
通信業のうち情報サービス業・インターネット附随サービス業・映像・音声・文字情報制作業。
運輸業・郵便業、卸売業・小売業、金融業・保険業、不動産業・物品賃貸業、学術研究・専門・技術サービス業、
教育・学習支援業・医療・福祉・複合サービス事業等を含むサービス業。

AIを利用/許可している、
予定がある人に聞きました

生成AIの規則、体制整備状況

質問　生成AI利用時のセキュリティに関連した規則・体制は整備されていますか



課題認識は60%を超えていたにも関わらず、
規則の策定、明文化、組織的な検討がされているのは**20%未満**で、詳細規則策定中を合わせても**40%前後しか整備が進んでいない。**

個人任せの状態では課題の解決は難しく、事業への影響が懸念される。

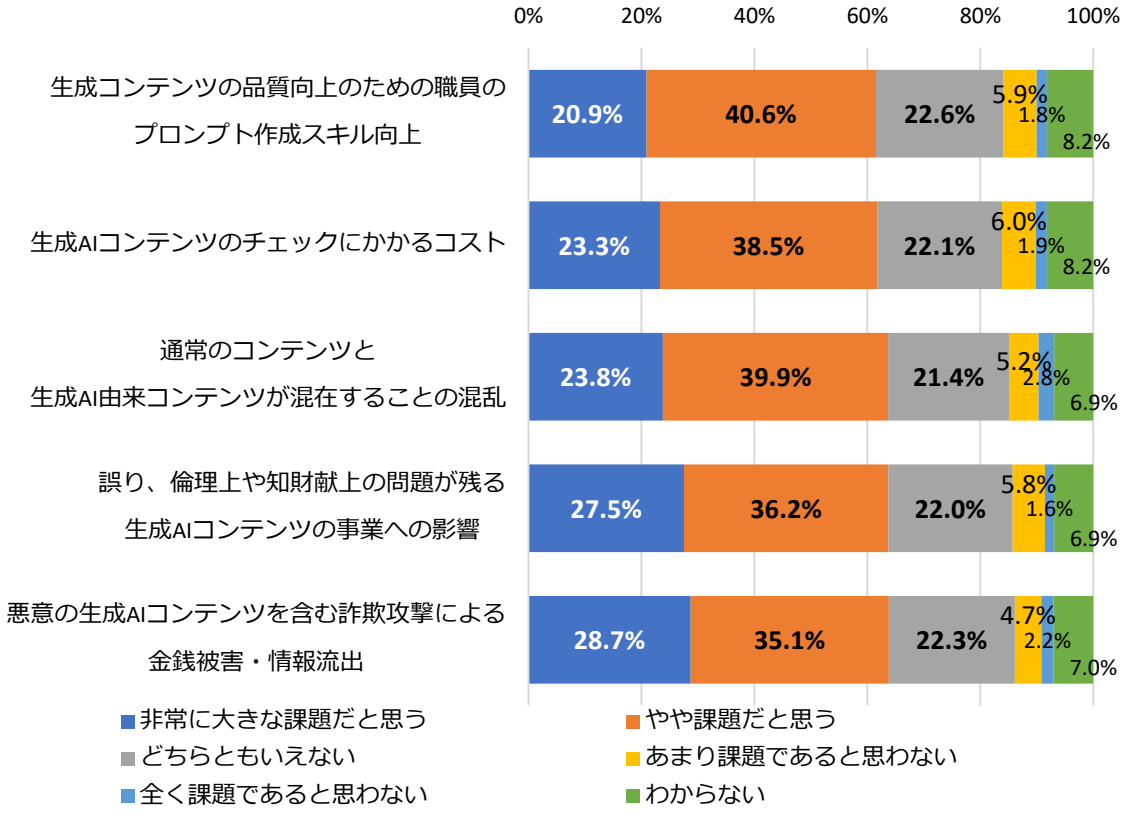
生成AIの利用規則・体制の整備状況

（本調査　Q9
　対象　AIを利用/許可している、または予定があると回答した1,000人）

AIを利用/許可している、
予定がある人に聞きました

生成AIの利用、普及における課題

質問　生成AIの利用、普及において次の事象は事業に影響するほど大きい課題ですか



「非常に大きな課題である」、「やや課題だと思う」を合わせた結果、最も多いのは詐欺による金銭被害・情報流出であったが、
いずれの事象も60%以上が課題と考えており、差は大きくない。

優先度がつけられてないため対応の遅れが懸念される。

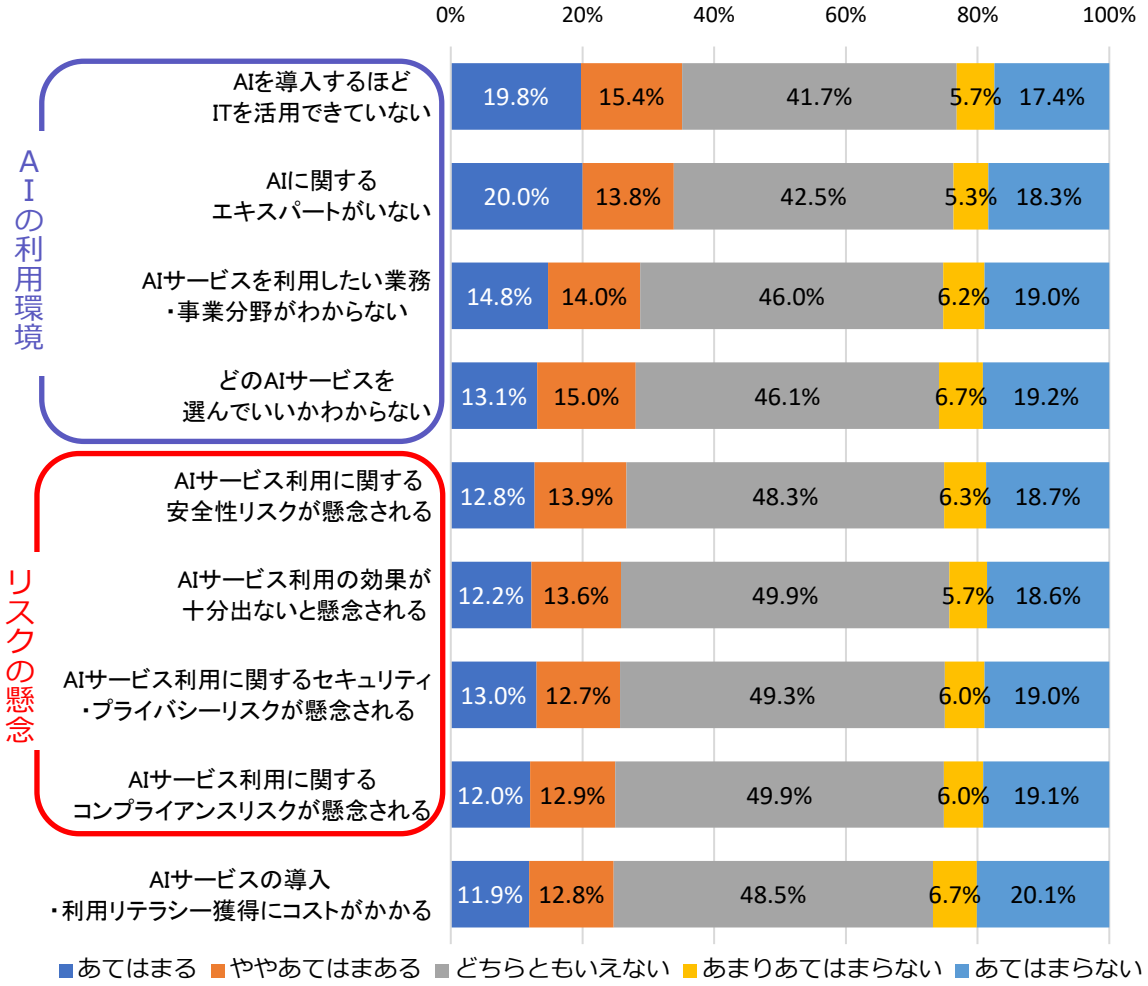
生成AI利用・評価・普及の課題

（本調査　Q11,12を分析し、類似項目は統合
対象　AIを利用/許可している、または予定があると回答した1,000人）

業務にAIを利用しない理由

まだAIを利用/許可していない、予定もない人に聞きました

質問　あなたの組織がAIサービスを利用/許可しておらず、導入予定もない理由？



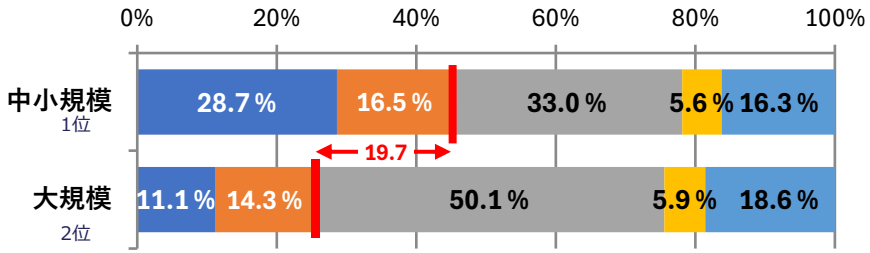
（事前調査　SQ4　対象　AIを利用/許可していない、予定もないと回答した3,827人）

- AIを利用する環境が整っていないことが、利用/許可しないことの**一番の要因**。
- セキュリティや安全に対する**リスクを懸念するとの回答が**4分の1程度あった。

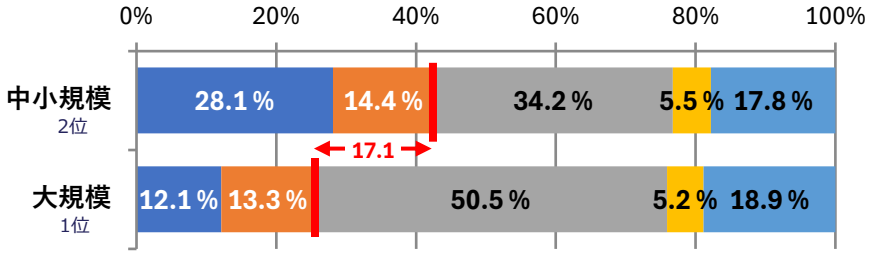
AI利用を促進するには 業務におけるITの活用とエキスパートの確保が課題

まだAIを利用/許可していない、予定もない人に聞きました

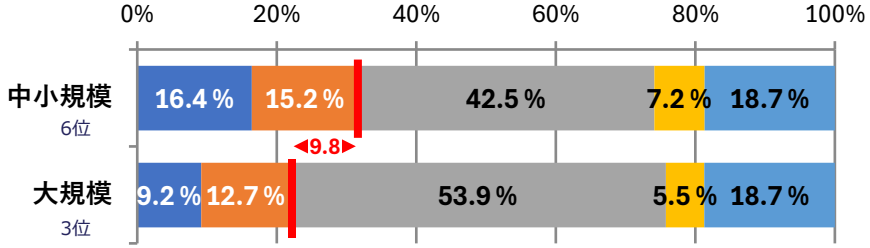
AIを導入するほどITを活用できていない



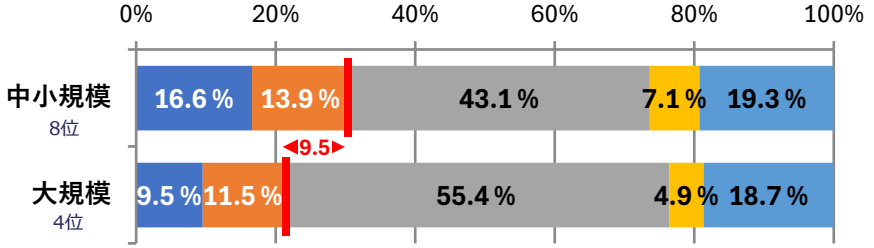
AIに関するエキスパートがいない



安全性リスクが懸念される



セキュリティ・プライバシーリスクが懸念される



1. あてはまる　2. ややあてはまある　3. どちらともいえない　4. あまりあてはまらない　5. あてはまらない

AIを利用しない理由　規模別集計結果

（事前調査SQ4　対象　AIを利用/許可していない、予定もないと回答した3,827人（大規模1,939、中小規模1,888））

「ITを活用できていない」「エキスパートがいない」は規模によらず利用促進阻害となっているが特に中小規模の方が大きな課題と考えられる。
大規模では、「安全性リスク」「セキュリティ・プライバシーリスク」が続く要因に挙がっている。

調査まとめ

- １．**AI利用している人は16.2%**、**予定あり6.3%**を合わせても22.5%とまだ多くはない。個別のサービスでは、**業務共通的**に利用でき、**顧客サービス改善や業務効率化**に役立ちそうなサービスから利用が進んでおり、**専門性の高いサービス**の利用も加速が期待される。
- ２．**AI利用者の6割はセキュリティ脅威を感じて**いる。AIサービスの導入において**セキュリティ対策、プライバシー保護**を重視している。
- ３．セキュリティの脅威や重要性の認識はあるもののAI利用規則や体制は検討中で、**明文化の遅れや利用者個人任せ**になっている組織が多い。特に**中小規模の組織では対応が遅れ**ている。
- ４．AI利用していない理由としては、**セキュリティや安全性のリスクを懸念**しているとの回答が25%前後見られたが、それ以前に、何に**AIが利用できるのか理解と検討が十分ではない**可能性がある。