

最新セキュリティマネジメント(第38回)

AI利用におけるセキュリティ対策

2024.07.18



生成AIの登場以来、業務におけるAI利用への関心は急速に高まり、実際に利用されるシーンも増えている。しかし、AIを利用する際の誤用、悪用に対する懸念も常に取り沙汰されている。業務でAIを利用している企業はセキュリティについてどう捉え、どのようなプロセスで検討し、どのような体制で臨んでいるのか。独立行政法人情報処理推進機構(IPA)が、2024年7月4日に発表した調査結果の概要を紹介する。

IPAがAI利用者に対してアンケート調査を実施

IPAは7月4日に「AI利用時のセキュリティ脅威、リスク調査」という調査報告書を公開した。これは、事前調査で「AIを利用／許可している、予定がある」と回答した約1000人を対象にWebアンケートを行い、結果をまとめたものだ。AIの利用に関心が高まっている今、タイムリーな調査といえるだろう。

事前調査は企業や組織に従事している5000人弱を対象に実施。AI利用をしている(予定を含む)人は22.5%であり、個別のAIサービスでは、チャット・質問回答など顧客向けサービス改善、翻訳など社内業務効率化などの業種共通サービスが多かった。

AIサービスのうち導入率第1位の「AIによるチャット・質問回答サービス」を最も導入しているのは、通信業、次いでサービス業だ。企業などに問い合わせをする際、チャットへ誘導されたという経験を持つ人は多いだろう。特に通信業では2023年1月以前から利用されていたケースが多い。

第2位の「AIによる翻訳サービス」は業種に関係なく導入が進み、こちらも2023年1月以前から導入されている。翻訳という専門性の高い業務を行う企業は以前からAIを利用しており、すでに定着しつつあると見られる。

興味深いのは、AIを利用している人の多くが、セキュリティに不安を抱いている点だ。約6割がAIのセキュリティに関して脅威を感じ、7割を超える人がセキュリティ対策は重要であると回答している。不安を抱きながら利用している人たちは、どのような対策をとっているのだろうか。

組織的な対応が遅れがちなAI利用のセキュリティ対策… 続きを読む