サイバーセキュリティ最前線

生成ＡＩに潜む情報漏洩リスクが国内外のビジネスシーンで顕在化!!

最近、「生成ＡＩ」という言葉をテレビや新聞などで目にすることが増えてきた。パソコンやスマートフォンさえあれば、誰でも無料または少額で使用することができるとあって、ビジネスシーンでも急速に普及しはじめている。しかし、そこに情報漏洩リスクがあることを忘れてはならない。

生成ＡＩの落とし穴

生成ＡＩの代表的なツールとしては、文章や資料を自動で作成してくれる「ChatGPT」や表計算やメールの下書きを手伝ってくれる「Copilot」などがある。ビジネスシーンでも「人間の代わりに作業をしてくれる便利なツール」として使われはじめている。日本でも急速に普及しつつあり、企業によってはすでに日常業務で積極的に活用している。

その利用にあたっては、情報を入力する際の情報漏洩リスクなどがあることを忘れてはならない。たとえば、請求データや顧客との取引内容を整理する資料をＡＩに作成してもらう過程で、不注意で社外秘の情報をそのままインプットしてしまうことが間々あるのだ。また、ＡＩに翻訳業務をしてもらう場合も注意が必要だ。従業員が社内の機密資料や契約書草案などをＡＩに不用意に入力して翻訳させていたという事例もあるという。これらのチョッとした不注意で、企業外への〝情報の持ち出し〟が発生する可能性があるのだ。

こうした事態を警戒し、一部の大手企業では生成ＡＩをクラウド経由ではなく、社内専用環境（いわゆるオンプレミス）で構築するといった事例が増えている。海外のある調査ではそうしたＡＩ環境が社内に用意されているにもかかわらず、従業員が個人的に外部のＡＩサービスを利用しているケースが頻繁に確認されているという。そしてもうひとつ、誰が、何を目的に、どのような情報を入力しているのかを社内で共有、把握し会社として管理、制御していくことが重要だ、と。こうした点について、セキュリティ専門企業の㈱ブロード（東京都千代田区）は「見えないものは守れないので、〝利用しているＡＩ〟と〝利用されている情報〟の両方を可視化する必要がある」と忠告する。だが、この点については日本においても海外においてもその対応はやや後手に回っているようだ。

安全に活用できる環境づくり

世界的に商用サービスとして一定の信頼性と知名度を持つ生成ＡＩツールは１００種を超えるとされ、さらに研究・個人開発ベースのサービスを含めると、その数は１０００を超えるともいわれている。今後、それらの日本語対応がすすめば、企業が把握していないあらたなサービスを従業員が〝先取り〟して使いはじめることもあるだろう。

かといって、新しいＡＩサービスを使用禁止にするわけにもいかないし、使ったからといって即座に情報漏洩につながるわけではない。だが、これだけはハッキリしている。たとえＡＩサービスの提供側がサイバー攻撃などで情報漏洩を起こしたとしても「入力された情報の取り扱いについてはユーザー責任」とする利用規約があることを忘れてはならない。つまり、利用した側、すなわち企業や従業員がその責任を問われる場合が多いのだ。

実際、海外ではこの種のリスクが顕在化しつつある。２０２３年には韓国のSamsung（サムスン）の技術者がChatGPTにソースコード（プログラミング言語などで書かれたコンピュータへの指示）を入力したことで、同社はＡＩツールの使用を一時禁止する事態になったことも。それに対し、前出のブロードの担当者は「〝安全に活用できる環境〟の整備が第一」と話し、「近々、そういったことに対応できる強力なソフトもわれわれから紹介できる予定だ」と。ＡＩの活用がますます活発なってきている今日、こうした事態への対応策が急務に。