セキュリティ監査への生成AI活用 ー現状と今後の応用可能性

サプライチェーンへのサイバー攻撃が相次ぎ、セキュリティ監査対象を拡大せざるを得ない状況にある。セキュリティ人材の慢性不足もあり、監査業務の品質維持が難しくなりつつある。その解決手法として注目されているのが生成AIの活用である。

セキュリティ監査業務の変革が求められる背景

金融機関における監査業務には様々な種類があるが、セキュリティの文脈でも監査業務が欠かせない。定期的に自社に関連するシステムに対して、脆弱性や設定不備がない状態かを調査するために、内部的な監査を行っている。

また、昨今、金融機関各社から「内部のセキュリティ監査業務に、生成AIを活用する検討を進めている」という声をよく聞く。こうした生成AI活用の動きの背景には、セキュリティ監査業務におけるより効率的で抜本的な改革へのニーズがあるからだと思われる。その最大の背景となっているのが深刻化しているサプライチェーンへのサイバー攻撃への対応である。

サプライチェーンや委託先を狙ったサイバー攻撃は、情報処理推進機構（IPA）セキュリティセンターが発表する「情報セキュリティ10大脅威 2025」[1)]における組織向けの情報セキュリティ脅威の2位に位置づけられている。また、サプライチェーンのシステムへの攻撃が主因となったランサムウェアによる他社インシデントのニュースは連日のように報道され、もはや対岸の火事とは言えない状況である。

攻撃者は、データ、システム、物理資産、あるいは人的資産といった組織のあらゆる側面におけるセキュリティの「弱い箇所」を標的とする。セキュリティ監査業務はこの「弱い箇所」を洗い出すための有効的な取り組みの一つだが、セキュリティ人材の慢性的な不足という事情がある。リスクの拡大とリソースの不足という乖離がセキュリティ監査業務上の大きな課題となっている。

セキュリティ監査の現状と生成AI活用の妥当性

サプライチェーンの拡大は、セキュリティ監査業務の需要そのものを増大させている。そもそも、監査担当者が自社のシステムに対して、自らすべての対象を1つ1つチェックすることは極めて困難である。そのため従来、管理主体が収集したシステム構成図やチェックシートに基づき監査を実施するアプローチで対処してきた。しかし、このようなセキュリティ監査の一般的なアプローチも、サプライチェーンの拡大にともない、自社を超えた更なるセキュリティ監査対象の拡大という問題に直面している。

対象が拡大するだけでなく、システム構成図のフォーマットの違いや他社ヒアリング調整等の追加のタスクという課題もある。多くの会社のセキュリティ監査は、監査プレイヤーを増やして対応しているが、それだけでは不十分であるため、より効率的な手法を模索している。

生成AIが注目されるのは、監査業務に求められる「効率化」のニーズと、生成AIが持つ「要約」や「読解」といった技術的強みが強く適合するためであると考えられる。「既存の膨大な証跡文書を入力情報とし、あらかじめ決められた監査基準に沿って評価を行う」といったルールに基づき文書を読み解くタスクにおいては、生成AIは比較的高い精度が期待できる。

生成AIによる業務変革の3段階

セキュリティ監査業務に限らないが、生成AIを活用した業務変革は、3つの成熟度モデルで整理できると考

NOTE

1) 情報処理推進機構（IPA）「情報セキュリティ10大脅威2025」（2025年1月）。

えられる。（1）コンテンツを生成する「コンテンツ・オートメーション」、（2）決められた手順を実行する「ワークフロー・オートメーション」、（3）自律的に目標を遂行する「エージェンティック・オートメーション」の3段階だ。

セキュリティ監査業務において、我々が現在把握している生成AI活用は、「監査対象システムの担当者ヒアリングの文字起こし」や「膨大なヒアリング証跡の内容の充足度チェック」「セキュリティ規程とヒアリング証跡の突合処理」「社内セキュリティ規程のリサーチと要約」といったタスクの効率化に留まっており、これは第1段階の「コンテンツ・オートメーション」に相当する。これらの生成AIの活用方法は一般的にどの業務でも活用が試行錯誤されている。

今後、実装や検討が進むと考えられる次なるステップとしては、「準拠すべきセキュリティ規程やガイドラインから監査項目の洗い出しを行う監査準備業務」「委託先へのヒアリングと監査調書の作成までの一連の監査の実施業務」、あるいは「自社セキュリティ基準での外部システムのリスク評価と改善提案といったセキュリティ監査結果のまとめ業務」等の複数タスクの連鎖からなるワークフローの“自動化”である。これらは第2段階の「ワークフロー・オートメーション」に位置づけられるが、実装にはシステム構成図等のセキュリティ評価を行うためのデータの格納箇所の分散や各社におけるセキュリティ監査フォーマットが異なることによる例外処理などの課題があり、連鎖するタスク間のデータの標準化や異常事象が発生したときに人がすぐに代替できる対策機能の具備が必要となる。こうした課題への対応が成熟することにより、監査業務においても単一タスクの“効率化”から、一連のタスクプロセスの“自動化”へと段階が進むだろう。

究極の姿：エージェンティック・オートメーション

一方で、第3段階の「エージェンティック・オートメーション」への移行には高いハードルが存在する。ステークホルダーを超えてセキュリティ監査に必要なデータを、網羅的かつリアルタイムに集約することが難しいといったデータ観点での課題や、生成AIによるセキュリティ監査業務の品質が人間の専門性を超えることが困難といった精度面での課題も存在する。

しかし、仮にセキュリティ監査業務が人手を介さず高度に自動化されれば、高品質なセキュリティ監査を従来よりも格段に早いサイクルで実施することが可能となる。これによりセキュリティ監査業務自体を、従来のシステムに関連する多人数を巻き込む受け身の定期作業から、生成AIによる品質の安定化と効率化を通じて高速かつ網羅的にセキュリティの「弱い箇所」を炙り出せるようになる「戦略的な未然防止の仕組み」へとパラダイムシフトさせる可能性を秘めていると考える。

このように、セキュリティ監査業務と生成AIの技術的親和性の高さに着目し、現在のセキュリティ監査業務の課題を鑑みると、生成AIを活用した業務効率化の取り組みは今後ますます加速していくと考えられる。

Writer's Profile

松本 寛正 Kansei Matsumoto
セキュリティソリューション事業開発部
セキュリティコンサルタント
専門は AI ガバナンス
focus@nri.co.jp