「フロンティアAIを巡る現状と今後 ― 大局からの 6 つの提言」

生成 AI により、脆弱性の発見やサイバー攻撃の**「速度」は上がる可能性が高い。しかし、脅威の本質と、企業が取るべき備えの基本は、これまでもこれからも変わらない。**特定の生成 AI モデルをめぐる過熱した議論に振り回されず、大局から次の 6 点に取り組むことを提言する。

1.「振り回されない」 AI を個別事象ではなく構造の変化として捉える

特定モデルをめぐる個々の事件に一喜一憂せず、「攻撃が速く・安くなる時代」が来たという構造変化を受け入れ、組織の戦略と投資を決める。騒ぎに振り回されるのではなく、平時の備えを粛々と見直し、システムやセキュリティの優先順位を立て直すことが出発点となる。

2.「止める勇気と止まる覚悟」 システムやサービスが止まる事態を想定する

フロンティア AI の活用有無によらず、自社の製品・サービスに重大な脆弱性が見つかり、提供停止や出荷見送りに追い込まれることがある。提供側は、顧客が負うリスクを踏まえ、重大な脆弱性を放置せずに、自ら急ぎ止める決断を下す勇気が求められる。一方、利用側も、提供側の判断によって、製品・サービス、あるいは AI そのものの提供が止められることがあり、それを受け入れざるを得ない事態に備える覚悟が、利用側には求められる。

3.「かかる費用の理解」 AI 時代の人材・体制・予算を見込む

AI は脆弱性発見・アラート・ソフトウェアの構造分析・コードレビューの件数を激増させ、人が判断すべき情報量はむしろ増える。AI は人を代替するだけでなく判断対象を増やすため、検証・トリアージの工数も含め、必要な人材・体制・予算をソフトウェア開発者側も、発注者側も経営として見込む必要がある。また、AI によって増える脆弱性対応は、すべてが無償の作業ではない。AI による新たな脆弱性の発見や対応にかかった工数は、別途請求の対象とする場合がある。

4.「やるべきことをやる」 基本のセキュリティを徹底する

AI が見つけるゼロデイより、放置された既知の脆弱性の方がはるかに多く悪用される。CISA KEV が示すとおり、攻撃の大半は既知の脆弱性とパッチ未適用であり、まずはここを徹底する。また、適用できない環境を考慮したうえで、組織としてのリスクの受容や緩和策を検討することが必要である。なお、組織は情報資産とアタックサーフェスを把握し、ソースコード等の重要資産の流出を防ぐことに努め、脆弱性情報は CVE／NVD単一に依存せず、CISA KEV・EPSS・ベンダー情報等を組み合わせ、悪用可能性で優先順位を付ける。

5.「不可欠な集団防御」 中小企業の「防御能力格差」を埋める

サイバー攻撃はもはや大企業だけの問題ではなく、中小企業にも及ぶ。いま広がっているのは、高性能AI・専門人材・脅威情報・演習環境・脆弱性対応支援といった防御能力全体への“アクセスの格差”であり、さらに、アクセスを得てもスキャンや AI の実行そのものに費用がかかる“利用コストの格差”である（高性能 AI の個別審査・申請制はその一例）。これを埋めるには、行政の補助・共同利用・伴走支援に業界の知見も組み合わせ、官民連携も含めた「集団防御」で、アクセスと利用コストの両面から防御能力を裾野まで届かせる必要がある。

6.「使う人があってこそ」 人への投資を継続する

AI を使いこなす人材と、セキュリティ人材を継続的に育成する。リスク判断と投資判断ができる経営層を育て、AI の指摘・判断を検証して鵜呑みにしない能力を組織に根づかせる。AI はあくまでも人間が使う一つのツール に過ぎず、最終的な判断や責任を担うのは人間であることは変わりえない。AI が高度化するほど、人間の判 断力が重要になる。騒がず基礎を固め、人に投資する。それが、最も確かな備えである。

一般社団法人ソフトウェア協会（SAJ） サイバーセキュリティ委員会／AI セキュリティワーキンググループ

委員長：萩原健太（SAJ副会長/ＧＯＦＵ株式会社）

ＷＧリーダー：飯田朝洋（理事/トレンドマイクロ株式会社）／サブリーダー：倉持浩明（理事/株式会社LAC）