

各 位

株式会社 JSOL

フロンティア AI 攻撃への備えを4領域で支援

～外部からの AI 攻撃と自社 AI 利用リスクの双方を見据え、攻撃の事前発見、AI リスク制御、外部リスク
予防、インシデント対応を体系化～

株式会社 JSOL(以下、JSOL)は、フロンティア AI 攻撃への備えを支援するため、「攻撃の事前発見」「AI リスク制御」「外部リスクへの予防」「インシデント対応」の4つの領域に対応するセキュリティソリューションを体系化し、提供を強化します。

対象となるのは、自律型ペネトレーションテストプラットフォーム「NodeZero」、AI 利用に伴うリスクを制御する「WITNESS AI」、外部露出リスクを把握する「CybelAngel」、組織的な対応を支援する統合 CSIRT「J'sARMOR」です。

【背景】

フロンティア AI は、最先端の高性能な汎用 AI モデルを指し、ソフトウェア解析、脆弱性の特定、攻撃手順の自動化など、サイバー領域でも高度な能力を発揮し得る技術として注目されています。こうした能力は防御側にも活用できる一方、攻撃者に悪用された場合には、これまで専門人材や時間を必要とした攻撃準備を高速化・自動化させる可能性があります。

昨今、生成 AI の業務利用が広がる一方で、AI エージェントのように自律的に計画・実行する技術の進展により、企業が備えるべきリスクは複雑化しています。外部から AI を悪用した攻撃を受けるリスクに加え、自社で利用する AI や AI アプリケーションを起点とした情報流出・不適切利用への対応も重要になっています。例えば金融機関などでは、資産管理や脆弱性管理、バッチ適用、監視対応、レジリエンスなどについて、迅速かつ適切に対応できる体制が整備されているかを至急点検し、必要な対策をとることが金融庁などから求められています。

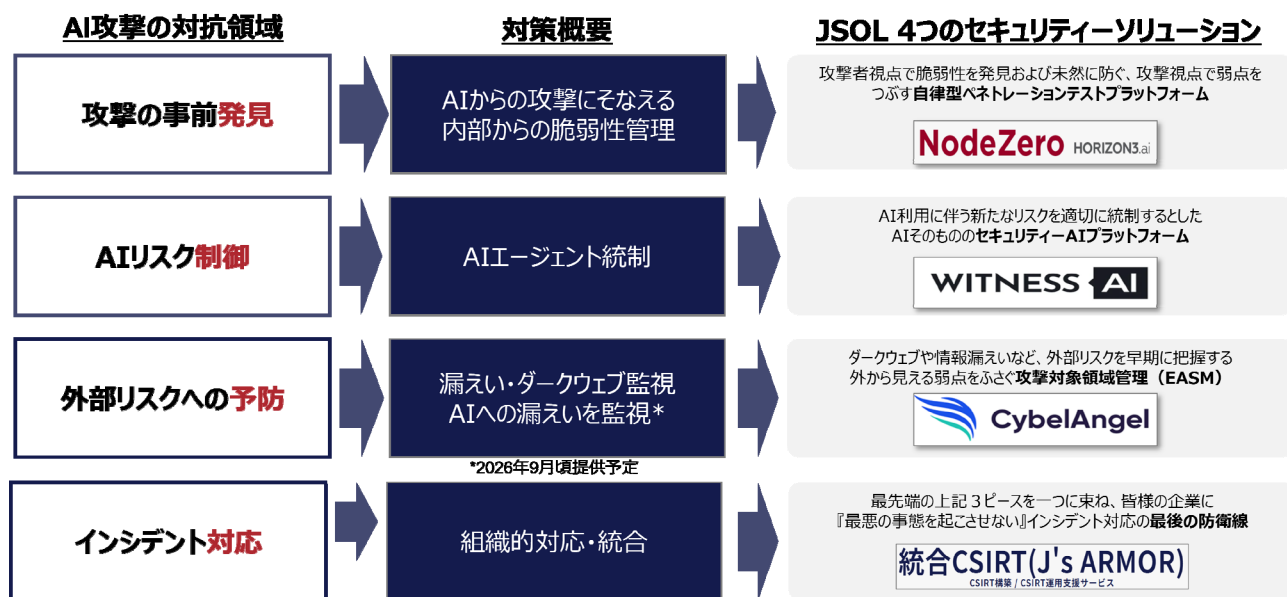
このように、企業にとって重要なのは、AI エージェントを活用した攻撃や AI 利用に伴う新たなリスクを、個別の論点としてではなく、サイバーセキュリティ全体の課題として捉えることです。攻撃対象領域の可視化、AI 利用の統制、外部露出リスクの把握、インシデント発生時の迅速な対応を一連の備えとして整えることが求められます。

【AI 攻撃・AI 利用に対する JSOL の4つのソリューション】

JSOL は、各ソリューションを単体で紹介するだけでなく、企業の業務、システム構成、AI 利用状況、セキュリティ運用体制に応じて、必要な対策を組み合わせで提案し、フロンティア AI 時代のセキュリティ強化を支援します。攻撃を受ける前の可視化、AI 利用時の統制、外部に露出したリスクの把握、発生後の組織的対応までを一連の流れとして捉えることで、企業が「どこから着手すべきか」「どの対策を優先すべきか」を判断しやすくします。

また、JSOL はシステムインテグレーターとして、業務システムの構築・運用で培った知見と、サイバーセキュリティ領域の専門性を生かし、製造、流通サービス、金融、公共など多様な業種の実情に即した対策を支援します。フロンティア AI の進展により攻撃のスピードや規模が変化する中でも、お客さまの事業継続と信頼性

確保に貢献します。



【今後の展開】

JSOL は、フロンティア AI 攻撃への備えに関する情報提供、セミナー、デモンストレーション、個別相談などを通じて、企業が自社のリスクを具体的に理解し、実効性ある対策を進められるよう支援していきます。今後も、AI を活用する企業が安心して技術の利点を享受できるよう、セキュリティ対策の高度化に取り組んでまいります。

関連サイト

<https://promotion.jsol.co.jp/SecAIOps/security-network/frontier-ai/index.html>

※本リリースに記載されている内容は予告無く変更することがあります。

※本リリースに記載されている製品名、会社名は各社の商標または登録商標です。

【お問い合わせ先】

株式会社 JSOL エンタープライズ&ソーシャルビジネス統括本部

サイバーセキュリティ&インテリジェント・オペレーション事業本部

E-Mail: hg_security_solutions_info@s1.jsol.co.jp

JSOL CORPORATION