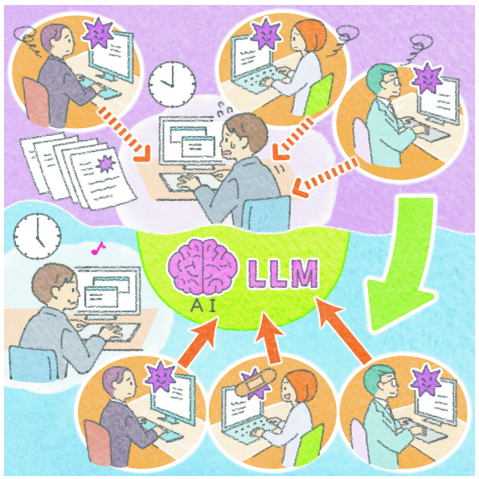
P08

サイバーセキュリティ対応の知見を学習したAIが、高度な知識を求めないオペレーションを可能にします

tsuzumiの未来の提案：サイバーセキュリティオペレーション技術

IOWN Pick Up　NTT版大規模言語モデル



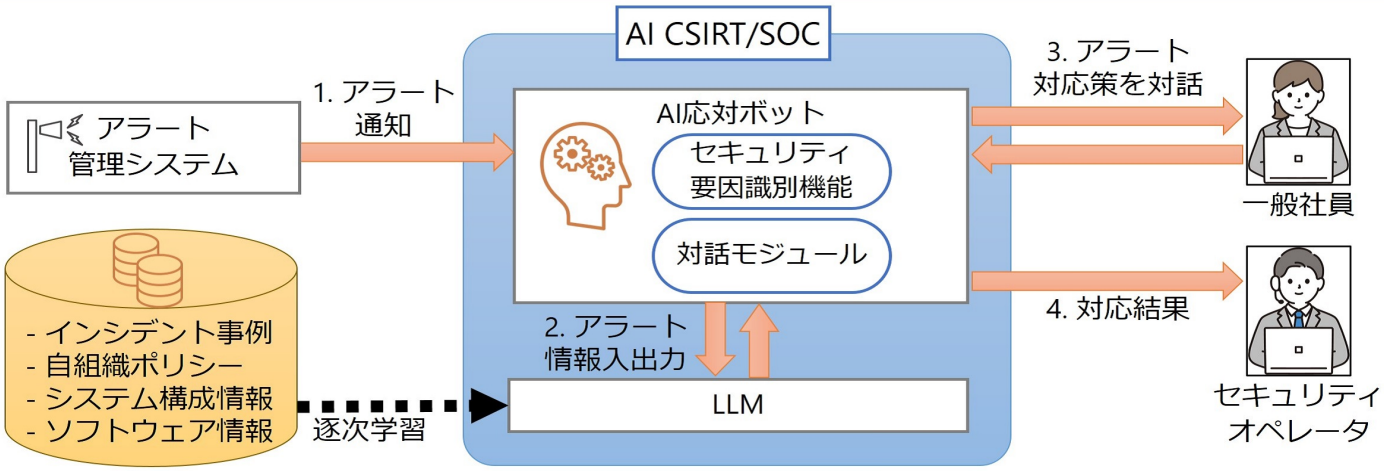
背景

世界中で470万人がセキュリティ業務に従事していますが、それでも人材不足と言われています。経験の蓄積に時間がかかり、常に新たな情報を扱うため、雇用・育成にコストがかかることが要因です。経験や知見をどう扱うかはセキュリティを維持するために必要な経営課題です。

成果の概要

LLM（大規模言語モデル）の特徴を生かしサイバーセキュリティ対応の知見である脅威インテリジェンスや組織ごとのルールなどを学習することで、多様なセキュリティオペレーションを代行・補助し、高度な知識を求めないオペレーションを可能にします。

サイバーセキュリティの知見をAIが学習　⇒　セキュリティ人材の確保・育成に関する課題を解決



技術のポイント

- 長年の運用で蓄積した多種多様なセキュリティインテリジェンスに加え、日々更新される情報に対しても追加学習することで最新情報に基づくオペレーションを実現
- ソフトウェアの依存関係や安全性などを分析することにより得られた情報を学習することで自社・自組織に固有の影響調査や対策検討を実施
- セキュリティインテリジェンスとオペレーションノウハウを詰め込んだAIがインシデント対応の事前・事後のセキュリティ業務を高効率化・自動化

この研究がもたらす未来

複雑かつ高度なセキュリティ業務を簡易化し、脅威に対する24・365のオペレーションから人々を解放することで、生産性の向上をもたらす、サステナブルなセキュリティを実現します。

出展企業

日本電信電話株式会社

問い合わせ先

rdforum-exhibition@ml.ntt.com