NRI グループからのお知らせ
Notification from NRI Group

Nomura Research Institute Group

2026 年 8 月 6 日

NRI セキュアテクノロジーズ株式会社

NRI セキュア、自社の SOC 運用知見を組み込んだ AI で、セキュリティ監視サービスを強化

～独自開発の AI 統制基盤で、AI 活用時のリスクを抑制しながら分析品質と対応力を向上～

NRI セキュアテクノロジーズ株式会社（以下「NRI セキュア」）は、自社のセキュリティオペレーションセンター（SOC）[1]「NeoSOC（ネオソック）」に、独自開発の AI 統制基盤「AgenticBlue（エージェンティックブルー）」[2]を導入し、本日より運用を開始します。

AgenticBlue 上で、SOC 運用知見を組み込んだ AI が調査・分析プロセスを支援することで、NeoSOC が提供する「セキュリティログ監視サービス（共用 SOC）」および「SIEM 監視サービス」[3]における分析品質の向上と対応の迅速化を実現しました。

■ サイバー攻撃者による AI 悪用と SOC 運用における課題

サイバー攻撃者による AI の悪用が急速に進んでおり、偵察活動や攻撃準備などのプロセスが AI により自動化される事例も報告されるなど、攻撃成立までのスピードはこれまで以上に増しています。一方で、多くの SOC では、大量に発生するアラートに対する調査・分析・判定をアナリストが手作業で行っており、分析品質のばらつきや熟練アナリストへの依存、アラート増加に伴う運用負荷の増大といった課題が、昨今の攻撃の高速化に伴い深刻化しています。

■ AI 活用によりセキュリティ監視サービスの品質を向上

これらの課題を解決するため、NRI セキュアは、20 年以上にわたる SOC 運用で培った分析・対応の知見を AI に組み込み、NeoSOC の運用基盤として実装しました。AgenticBlue 導入のポイントおよび、AI 活用による「セキュリティログ監視サービス（共用 SOC）」と「SIEM 監視サービス」への効果は、主に以下の 2 点です。

1. AI による自動化で、分析品質向上と対応迅速化

従来、NeoSOC のアナリストが手作業で行っていたアラートのトリアージ（対応優先度の判定）から一次調査、分析、脅威の重要度判定、報告作成までのプロセスを自動化します。定型的な確認作業や情報収集を AI が担うことで、アナリストは高度な脅威分析や対応判断、インシデント対応といった専門性の高い業務に専念し、サイバー攻撃の検知から対応、お客様への報告までのスピードを向上させることができます。

さらに、利用企業ごとの運用要件やセキュリティポリシーに応じた調査・分析・通知にも柔軟に対応できるようになるため、カスタマイズ性の高いサービス提供が可能となりました。

2. AI 活用の効果と安全性を両立する SOC 運用

AgenticBlue は、アクセス制御や認証情報管理、機密データ保護といったセキュリティ機能に加え、AI の判断過程を記録・可視化する機能を備えており、複数の AI が相互検証することで、分析結果の信頼性を確保しています。また、取り扱うログや調査データは、安全に隔離された専用環境内で処理されるため、学習データとして外部に転送されることはありません。

利用企業は、AI による効率化や分析品質向上のメリットを享受しながら、AI 活用時に懸念される情報漏えいや誤判断などのリスクを抑えた、セキュリティ監視サービスを利用することができます。

図：AI を活用した 24 時間 365 日のセキュリティ監視

詳細については、次の Web サイトをご参照ください。

https://www.nri-secure.co.jp/service/mss/secureprotecht

NRI セキュアでは今後、AI の活用範囲を一次分析から攻撃を検知・防御するためのルールやパターンの自動適用をはじめとした対処の自動化など、より高度なレベルへ順次拡大し、SOC 運用全体の高度化を推進していきます。

---

[1] セキュリティオペレーションセンター（SOC）：企業などが所有する情報システムへの脅威を、24 時間 365 日体制で監視し、脅威情報の分析などを行い、対応策を示す専門組織を指します。

[2] AgenticBlue：SOC およびマネージドセキュリティサービスの運用で利用する複数の AI エージェントを、安全かつ高品質に運用するために NRI セキュアが開発した AI 統制基盤です（商標出願中）。詳細については、次の NRI セキュアブログをご参照ください。https://www.nri-secure.co.jp/blog/agenticblue

[3] サービスの詳細はそれぞれ次の Web サイトをご参照ください。
セキュリティログ監視サービス（https://www.nri-secure.co.jp/service/mss/log_monitoring）
SIEM 監視サービス（https://www.nri-secure.co.jp/service/mss/siem_monitoring）

【お知らせに関するお問い合わせ】
NRI セキュアテクノロジーズ株式会社　広報担当
E-mail：info@nri-secure.co.jp

【ご参考】

- 関連セミナーの開催について

AI を活用した SOC 高度化の取り組みを解説する、「Agentic AI×SOC 実践セミナー」を開催します。

開催日時：2026 年 9 月 7 日（月）13:05～13:50

開催方法：オンライン

参加費：無料

主催：NRI セキュアテクノロジーズ株式会社

講演者：NRI セキュアテクノロジーズ株式会社　セキュリティアナリスト　切上 太希

※セミナー内容は予告なく変更される場合があります。詳細については、次の Web サイトをご参照ください。https://www.nri-secure.co.jp/seminar/2026/0907ai-soc