



Nomura Research Institute Group

NEWS RELEASE

2026 年 10 月 15 日

NRI セキュアテクノロジーズ株式会社

NRI セキュア、AI 駆動開発のセキュリティ対策を支援するサービスを提供開始

～AI エージェント利用のルール整備から開発プロセスの設計、脆弱性対応までを包括的に支援～

NRI セキュアテクノロジーズ株式会社（本社：東京都千代田区、代表取締役社長：池田泰徳、以下「NRI セキュア」）は、生成 AI や AI エージェント¹を活用したソフトウェア開発（AI 駆動開発）を進める企業・組織を対象に、「AI 駆動開発向けセキュリティ支援サービス」（以下「本サービス」）の提供を本日開始します。

本サービスでは、AI 利用ルールの整備および AI エージェント利用時の統制、開発プロセスへのセキュリティ対策の組み込み、脆弱性対応の優先度付け（トリアージ）を支援します。これにより、AI 駆動開発の生産性を損なわずにセキュリティ対策を実現・推進します。

■ AI 駆動開発の普及に伴い、人手による管理は限界に

生成 AI や AI エージェントの活用は、要件定義、設計、実装、テスト、運用など、ソフトウェア開発の各工程に広がっています。これに伴い、例えば AI が生成したコードに脆弱性が含まれていないかどうかという成果物の品質や、AI エージェントに権限を過剰に付与していないかといった AI の制御の観点で、従来とは異なる管理が求められています。

AI 駆動開発により、確認すべき成果物や脆弱性情報が増えると、優先度を付けて対応するにしても、人手による確認だけでは対応が困難になると考えられます。また同時に、AI 技術そのものの急速な進化や開発プロセスへの組み込みが進む一方で、組織のセキュリティ施策が劣化する可能性も挙げられます。そのため、利用ルール、開発手順、技術面の対策を組み合わせた、AI 駆動開発のプロセス全体を包括的かつ継続的に管理する仕組みが重要です。

■ 本サービスの概要と特長

本サービスは、AI 活用に関するルール整備から脆弱性対応に至るまでの、以下の 4 つの支援メニューを提供します。

1. AI エージェント利用に関するガイドライン整備支援

AI エージェント利用時のリスクと運用ルールを整理し、組織全体で参照するガイドラインと、ツールごとの設定や利用方法を定めるガイドラインの整備を支援します。利用者と管理者それぞれに求められる役割を整理するとともに、AI 利用に伴う自組織のセキュリティリスクとその対策に関する判断基準を明確にすることができます。

2. セキュアな AI エージェントハーネスの整備・内製化支援

AI エージェントが参照すべきルール、利用できるツールや作業手順、想定される成果物などをあらかじめ定義した、指示ファイルや設定の一式（AI エージェントハーネス）を整備します。ハーネスには、組織が想定するセキュリティリスクを最小化できるよう、ルールやセキュリティ要件を最適な形で反映します。これにより、AI エージェントによる開発時のセキュリティリスクの低減も図ったハーネスを実現することができます。さらに、これらを自組織で見直し、改善していけるように、継続的な見直しや運用も支援します。

3. AI 組込型 セキュア開発プロセス設計構築支援

AI が生成した成果物に起因するリスクに対応するため、開発プロセス全体を設計・提案します。開発からリリースまでの工程の自動化を行う CI/CD²をベースに、AI が中心となって生成する成果物の中で品質基準を満たさないものを次の工程へ進ませない仕組みの構築も可能です。AI 駆動開発の開発速度を維持しながら、AI 特有のセキュリティリスクを考慮したセキュリティ対策を組み込んだ体制づくりを支援します。

4. 脆弱性トリアージ AI 自動化支援

開発の成果物や運用中のシステムに脆弱性が検知された際に、脆弱性情報、脅威情報、資産情報、組織のリスク許容度や選好度などを組み合わせて対応を検討する必要があります。本サービスでは、AI を活用した、対応すべき脆弱性の優先度付け（トリアージ）の仕組みを導入支援することで、トリアージ業務の自動化および効率化を推進します。人による最終判断を維持しながら、確認作業の負荷を減らし、優先度の高い脆弱性への早期対応を目指します。

本サービスの詳細については、次の Web サイトをご参照ください。

<https://www.nri-secure.co.jp/service/consulting/ai-development>

NRI セキュアは、セキュア開発、DevSecOps³、脆弱性管理の各領域で培ってきた知見を活かし、AI 駆

動開発時代に求められるセキュリティ対策の実現に向けて、企業・組織の開発体制に応じた取り組みを包括的に支援していきます。

- ¹ AI エージェント：与えられた目的を解釈し、外部／社内ツールを選択・連携させながら、自律的に目標を達成するソフトウェアのことです。
- ² CI/CD：Continuous Integration（継続的インテグレーション）と Continuous Delivery（継続的デリバリー）の略称で、ソフトウェアのビルド、テスト、リリースといった作業を自動化し、変更を短い周期で反映できるようにする仕組みのことです。
- ³ DevSecOps：開発（Development）と運用（Operations）が連携する「DevOps」に、セキュリティ（Security）を組み込んだ開発手法です。開発スピードを維持しながらセキュリティを確保することを目的とします。

【ニュースリリースに関するお問い合わせ】

株式会社野村総合研究所 コーポレートコミュニケーション部 日下部、西
TEL：03-5877-7100 E-mail：kouhou@nri.co.jp

【本件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
E-mail：info@nri-secure.co.jp

【ご参考】

開発プロセスにおける本サービスの位置づけと、DevSecOps に関する従来の支援サービスの一覧

