Nomura Research Institute Group

NEWS RELEASE

2026 年 6 月 23 日

NRI セキュアテクノロジーズ株式会社

NRI セキュア、フロンティア AI モデルに対応したプロアクティブな脆弱性診断サービスを提供開始

～独自の検証基盤を用いて、未公表の脆弱性を検出し対応策を提示～

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、企業・組織が所有する外部公開サーバや基幹システム、ソフトウェア製品を対象に、未公表の脆弱性を検出し、対応策を提示する「フロンティア AI 対応プロアクティブ脆弱性診断（以下「本サービス」）」を、本日より提供します。本サービスは、最先端の大規模 AI モデル（フロンティア AI）と NRI セキュアが独自に開発した検証基盤（ハーネス）[1]を組み合わせることで実現したもので、脆弱性を悪用したサイバー攻撃へのプロアクティブ（予防的）な対策実行を支援します。

■ フロンティア AI によるサイバー脅威と脆弱性対応の変化

2026 年 4 月、米国 Anthropic（アンソロピック）社は、脆弱性を発見するフロンティア AI モデル「Claude Mythos Preview（クロード・ミュトス・プレビュー、以下「Mythos」）」を発表しました。同社は、主要 OS・ブラウザ・オープンソースソフトウェア（OSS）において、これまで見逃されていた不具合も含め、多数のゼロデイ脆弱性を発見したと公表しています [2]。

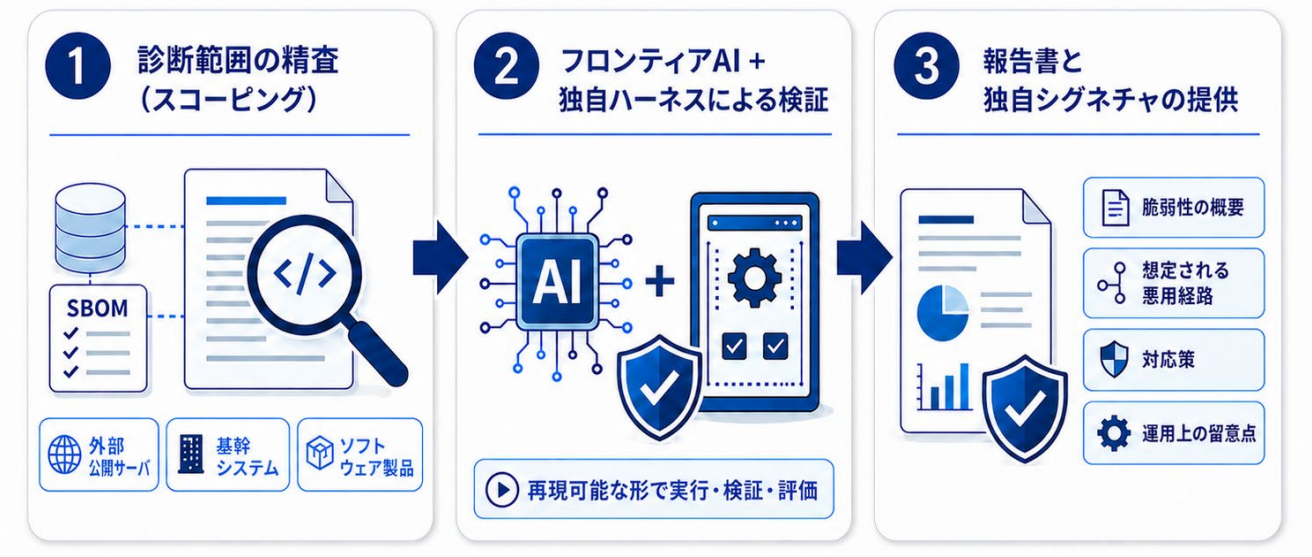
フロンティア AI モデルの登場により、脆弱性の発見・解析・検証が自動化されることで、脆弱性を突いたサイバー攻撃のスピードが大きく変わります。そのため、サイバー攻撃にさらされる防御側においても、悪用される前の段階で脆弱性を把握し、対応策を迅速に講じるための取り組みがますます重要になります。

■ 本サービスの概要と特長

本サービスは、企業・組織の外部公開サーバ・基幹システム・ソフトウェア製品（ファームウェア、組込みソフトウェア）を対象に、一般に利用可能なフロンティア AI と NRI セキュア独自のハーネスを組み合わせて、危険度の高い未公表の脆弱性の有無を検証し、対応策を提示するものです。

まず NRI セキュアの専門家が、対象のシステム・製品等で利用されているソースコードおよび OSS のソフトウェア部品表（SBOM）[3]情報をもとに、診断の範囲を精査します。診断の結果、危険度の高い脆弱性が検出された場合には、応急処置として NRI セキュアが作成した「独自シグネチャ（攻撃を検知・防御するためのルールやパターン）」を提供します（図を参照）。

図：本サービスの提供プロセス



本サービスの主な特長は、以下の 2 点です。

1. 再現検証に基づく、高い脆弱性検出能力

NRI セキュアは 2026 年 5 月、Mythos が発見したとされる代表的な脆弱性について、一般に利用可能なフロンティア AI と NRI セキュア独自のハーネスを用いて再現検証を実施しました。その結果、Mythos と同等のレベルで未公表の脆弱性を検出できることを確認しました。これは、独自開発したハーネスを使用することで初めて高い検出能力を発揮できるものです。そのため、本サービスはプロアクティブな脆弱性対策を推進するうえで、多くの企業にとって有用であると考えます。

2. 独自シグネチャの提供と対応策の提示

検出した未公表の脆弱性に対し、実際の修正プログラムが公開・適用されるまでの空白期間を埋めるため、侵入防御システム（IPS）や Web アプリケーションファイアウォール（WAF）などで利用可能な NRI セキュア独自のシグネチャを含む対策案を提示します。また、脆弱性の概要、想定される悪用経路、運用上の留意点を報告書にまとめ、修正プログラムが適用されるまでのリスクを低減しながら、迅速な対策の実行を支援します。

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/solution/proactive-vulnerability-assessment

NRI セキュアは、さまざまな取り組みを通じて AI のセキュリティに関する知見を培ってきました。今後も、フロンティア AI を含む最新の技術動向を踏まえ、攻撃者に先行して脆弱性を検証し、未公表の脆弱性への対応力向上に取り組むことで、安全・安心な情報システム環境と社会の実現に貢献していきます。

■ Anthropic Japan 合同会社 代表執行役社長　東條 英俊 氏からのコメント

この度、NRI セキュアテクノロジーズ株式会社がフロンティア AI を活用した新たな脆弱性診断サービスの提供を開始されることを歓迎いたします。AI の能力が高まるほど、その力を防御側の安全確保に役立てることの重要性は増していきます。NRI セキュアテクノロジーズは、AI セキュリティに関するガイドライン策定や書籍執筆を通じて知見を重ねてこられ、責任ある AI 活用を実践されている企業です。攻撃者に先んじて脆弱性を検出し、対策につなげる本サービスは、まさに AI を社会の安全のために役立てる取り組みだと考えます。Anthropic Japan として、NRI グループとのパートナーシップをより一層深めてまいります。

---

[1] 検証基盤（ハーネス）：システムや AI の動作を再現可能な形で実行・検証・評価するための統合的な実行環境・仕組み。

[2] Anthropic 社からの発表（2026 年 4 月 7 日）に基づきます。

[3] SBOM：Software Bill of Materials の略称で、製品に含まれるソフトウェアを構成するコンポーネントや互いの依存関係、ライセンスデータなどの一覧表です。OSS のライセンス管理や脆弱性の管理、ソフトウェアサプライチェーンのリスク管理等の用途で利用されます。

【ニュースリリース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