NTT AT

News Release

2026年9月29日
NTTアドバンステクノロジ株式会社

AIによる攻撃をAI×専門家が先回りする「AIハイブリッドWeb診断サービス」を提供開始

～フロンティアAIと専門家の知見で脆弱性発見から継続的な対策まで支援～

NTTアドバンステクノロジ株式会社（以下：NTT-AT、本社：東京都新宿区、代表取締役社長：伊東匡）は、生成AIの進展に伴い高度化・自動化するサイバー攻撃に対応するため、フロンティアAI[*1]と長年培ってきたセキュリティ技術を活用した新たなWebセキュリティ診断サービス「AIハイブリッドWeb診断サービス」（以下：本サービス）を2026年10月1日から提供開始します。

NTT-ATは、フロンティアAIの高度な解析能力と、長年にわたり培ってきたセキュリティ分野の知見を組み合わせることで、AI時代に求められる新たなセキュリティの実現をめざしており、その取組みの一環として、本サービスを提供します。

本サービスは、従来のセキュリティ診断では検出が困難であった脆弱性をAIの高度なソースコード解析により発見するとともに、AIにより抽出された大量の脆弱性候補のなかから対処不要な脆弱性を専門家の知見・データベース・専門ツールにより取除きます。これにより、実環境に影響のある真に対応が必要な内容を報告し、高セキュリティ水準の確保と現場の負担低減を両立します。また、継続的な診断により、日々変化する脅威動向や新たに発見される脆弱性に継続的に対応できる体制づくりを支援します。

1. 背景

近年、生成AIの普及・進化に伴い、AIを悪用したサイバー攻撃の高度化・自動化が進んでいます。なかでも、Claude Mythos（クロード・ミュトス）[*2]をはじめとする高度なAIの登場により、従来は発見が困難であった脆弱性の探索や悪用が容易になっています。そのため、企業・組織では、フロンティアAIを活用して早期に脆弱性を発見し、攻撃に悪用される前に対策を講じることが重要になっています。

一方で、フロンティアAIを活用して脆弱性を検出できても、自社システムにおける影響や対応の必要性を判断し、改修につなげるには専門的な知見が必要です。特に、限られた人員で脆弱性に対応する開発・運用現場では、すべての脆弱性候補に同等の対応を行うことは困難であり、実際の影響を踏まえて対応の優先度を判断することが重要となっています。

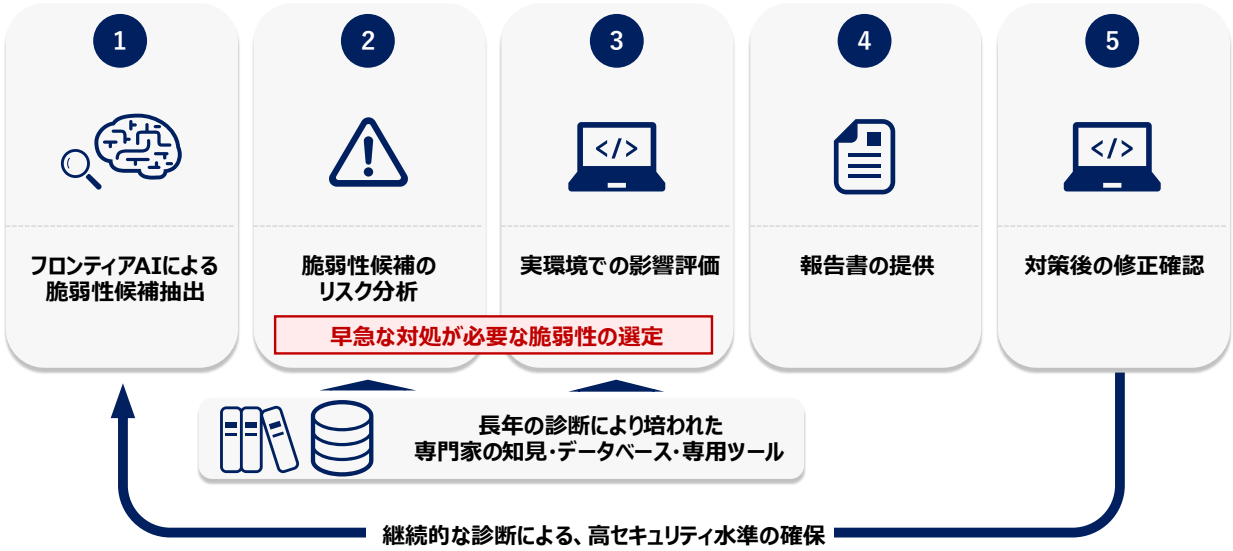
こうした背景を踏まえ、NTT-ATは、フロンティアAIによる高度な脆弱性発見能力と、25年以上にわたり培ってきたセキュリティ診断の知見・データベース・専用ツールを活用し、脆弱性候補の抽出からリスク評価、対応優先度の判断までを支援する本サービスを提供します。

2. 本サービスの概要

本サービスでは、お客さまからお預かりしたソースコードをフロンティアAIで解析し、脆弱性候補を洗い出します。その後、専門家の知見・データベース・専用ツールを活用した実環境での評価を行い、

AIにより抽出された大量の脆弱性候補のなかから対処不要な脆弱性を取除きます。これにより、対応が必要な脆弱性について、優先度や対策方法とともに報告します。
　主な実施内容は、以下のとおりです。

(1)フロンティアAIのソースコード解析による脆弱性候補抽出
(2)専門家およびフロンティアAIによる脆弱性候補のリスク分析
(3)専門家による実環境での影響評価
(4)影響度、対応優先度および対策方法をまとめた報告書の提供
(5)対策後の修正確認



3. 本サービスの特長

(1)AIで高度に解析し、専門家が実影響を見極めるハイブリッド診断

　フロンティアAIがソースコードから脆弱性候補を抽出し、専門家が実環境における再現性や影響を評価します。AIにより抽出された大量の脆弱性候補に含まれる誤検知や影響がない項目を、専門家の知見を活用した実環境への検査により取除き、実際に対応が必要な脆弱性を優先度とともに報告することで、開発・運用現場における判断負担を軽減します。

(2)改修判断に活用できるわかりやすい報告書

　脆弱性の内容だけでなく、実環境における影響、優先度や対策方法を整理して報告します。開発・運用現場における改修判断や、Webシステムのリリース可否判断に活用できます。

(3)最新の脅威動向に対応する継続型支援

　Webサイトの更新や機能追加など、お客さまが必要とするタイミングで診断を実施します。最新の脅威動向や検査手法を継続的に取入れることで、変化するサイバー攻撃に対応した診断を提供し、Webシステムのセキュリティレベルの維持・向上を支援します。

4. 対象のお客さま

本サービスは、次のような課題やニーズを持つ企業・組織を対象としています。

(1)AIを悪用した高度なサイバー攻撃への対応力を強化したい
(2)従来は高コストとなりがちだった高度なセキュリティ診断を、より手軽に活用したい
(3)対応すべき脆弱性と優先順位を明確にし、現場負担を抑えて効果的に対処したい
(4)一度きりの診断ではなく、継続的にセキュリティリスクを把握・管理したい

5. 提供開始

2026年10月1日

6. 提供価格

詳細は、下記「お問い合わせ先」までご連絡ください。

7. 今後の展開

NTT-ATは、フロンティアAIをはじめとする先進技術を継続的に取入れ、本サービスにおける検査・評価手法の高度化を進めてまいります。また、AIを活用したセキュリティサービスの拡充を通じて、お客さまのシステムにおけるリスクの早期発見と継続的な対応を支援し、あんしんしてデジタルサービスを利用できる社会の実現に貢献します。

*1 フロンティアAIとは、その時点で最先端にある最も高性能なAIモデルまたはAIシステムを示す言葉。
*2 Claude Mythos(クロード・ミュトス)は、Anthropicが2026年4月7日に発表した、サイバーセキュリティ・脆弱性発見に特化した最強クラスのAIモデル。

※本文中に記載されている会社名および製品名は、各社の商標または登録商標です。
※掲載のデータは発表日現在の情報です。予告なしに変更されることがございますので、あらかじめご了承ください。

■本件に関するお問い合わせ先
NTT アドバンステクノロジ株式会社
【商品に関するお問い合わせ先】
ソーシャルプラットフォーム・ビジネス本部
セキュリティビジネス部門
トータルセキュリティソリューション担当
https://www.ntt-at.co.jp/product/netprotect-ai-hybrid/

【報道関係のお問い合わせ先】
経営戦略室　経営企画部門
広報担当
後藤・根本
https://www.ntt-at.co.jp/inquiry/koho/