



Nomura Research Institute Group

2026 年 9 月 17 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 対応プロアクティブ脆弱性診断」 のデータ取り扱い体制を強化

～Amazon Bedrock を活用し、診断対象のソースコードを国外に出さずに分析～

NRI セキュアテクノロジーズ株式会社（以下「NRI セキュア」）は、「フロンティア AI 対応プロアクティブ脆弱性診断」サービス（以下「本サービス」）¹において、Amazon Web Services（AWS）が提供する生成 AI 基盤サービス「Amazon Bedrock」を活用することで、取り扱うデータの処理を日本国内で完結させる体制をこのたび構築しました。

診断対象のソースコードやシステム構成情報を日本国外に出さずに、フロンティア AI²を活用した診断サービスの提供が可能となったことで、金融分野や公共部門などの重要インフラをはじめとする厳格なデータ管理要件を持つ企業・組織においても、安心して本サービスを利用できます。

■ フロンティア AI で使用されるデータの国内保持・機密性への社会的要請

生成 AI の業務利用にあたっては、「データが国外のデータセンターへ送信されること」、「入力した情報が AI モデルの学習に利用されること」、「第三者に情報を閲覧されること」などの懸念点が指摘されています。特に重要インフラ事業では、データを国内に保持し、その取り扱いを自組織の管理下に置くことが、AI 導入の必須条件となる場合があります。NRI セキュアは、こうした社会的要請に応えるため、Amazon Bedrock の日本国内リージョンを活用したデータ取り扱い体制を新たに整備しました。

■ 強化したデータ取り扱い体制の概要

Amazon Bedrock は、AWS が提供する生成 AI 向けのクラウドサービスで、日本国内のリージョン（東京・大阪）でフロンティア AI を活用することができます。本サービスでは、Amazon Bedrock 上で米国 Anthropic PBC（以下「Anthropic」）の最新フロンティア AI モデルを用いた一次分析と、NRI セキュアの専門家による精査を組み合わせることで診断を実施します。診断業務は、厳格なアクセス管理・情報管理体制の

もとで実施し、さらに AI 活用におけるデータの取り扱いに関する懸念に対しては、以下の 3 点で対応します。

1. 国外へのデータ移転の防止

本サービスでは、ソースコードやシステム構成情報など、機密性の高い情報を取り扱います。診断対象のデータは、NRI セキュアが契約する Amazon Bedrock の日本国内リージョンで処理する構成とし、国外のデータセンターへ転送されることはありません。これにより、データの越境移転に関する規制や社内ポリシーに適合した形での運用が可能です。

2. 意図しない AI モデルへの学習利用の防止

Amazon Bedrock では、入力されたデータは、フロンティア AI モデルの学習・再学習には利用されません。そのため、診断対象のデータがフロンティア AI モデルに取り込まれて、外部に流出することを防止できます。

3. 基盤運用担当者による閲覧の防止

Amazon Bedrock では、クラウドサービス提供者のアクセスを制限する「Zero Operator Access (ZOA)」と呼ばれるアーキテクチャを採用しており、AWS の運用担当者による不必要なデータ閲覧を防ぐ保護構造となっています。これにより、第三者からのアクセスを防ぎ、情報漏洩のリスクを構造的に低減します。

NRI セキュアは、フロンティア AI の利用が防御目的かどうかを審査する、Anthropic の「Cyber Verification Program (CVP：安全な防御利用のための審査制度)」³の承認を受けており、フロンティア AI を活用したサイバーセキュリティ対策の強化に重点的に取り組んでいます。今後も、AI 活用の拡大に伴い、高度化・複雑化するサイバーリスクに対応するため、先進的な AI 技術と豊富なセキュリティ知見を融合したサービスを提供し、企業・組織が安全に AI を活用できる環境づくりに貢献していきます。

※本リリース内に記載されている会社名、製品名、サービス名は、各社の商標または登録商標です。

¹ 本サービスの詳細については、NRI セキュアの次の Web サイトをご参照ください。
<https://www.nri-secure.co.jp/service/solution/proactive-vulnerability-assessment>

² フロンティア AI：大規模なデータと計算資源を用いて開発された、極めて高度な能力を持つ最先端の生成 AI モデルの総称。従来の AI を大きく上回る汎用的な推論・分析能力を備え、セキュリティ診断のような専門的な判断を要する領域での活用が期待されています。

³ **Cyber Verification Program (CVP)** : Anthropic が提供する、防御目的のセキュリティ専門家・組織を対象とした審査・認定プログラム。認定を受けた組織は、脆弱性分析をはじめとする、通常は制限される高度なセキュリティ関連の用途において、Anthropic のフロンティア AI モデルを正当なサイバーセキュリティ防御活動のために利用できます。

【お知らせ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