

2024 年 11 月 28 日

三菱総研 D C S 株式会社

GMO サイバーセキュリティ by イエラエ株式会社

報道関係者各位

三菱総研 D C S と GMO サイバーセキュリティ by イエラエが生成 AI 活用支援で協業 ～生成 AI 利用システム向けのセキュリティ診断サービスを提供～

三菱総研 D C S 株式会社（本社：東京都品川区、代表取締役社長：亀田 浩樹、以下 D C S）と、GMO サイバーセキュリティ by イエラエ株式会社（本社：東京都渋谷区、代表取締役社長：牧田 誠、以下 GMO サイバーセキュリティ by イエラエ）は、生成 AI 活用におけるセキュリティ強化を図るため協業します。

その取り組みとして D C S は「生成 AI 利用システムセキュリティ診断」の提供を 2024 年 11 月 28 日（木）より開始します。これは、GMO サイバーセキュリティ by イエラエが提供する、GPT 等の大規模言語モデル（Large Language Model、以下 LLM）対応の「LLM セキュリティ診断」を用いた、初のサービスです。



■ 背景と概要

近年、OpenAI 社の ChatGPT などの生成 AI が API を通じて気軽に利用できるようになったことで、生成 AI を活用したシステムやサービスが加速度的に普及しています。一方で、攻撃者が AI に対し不正な命令を入力することで不適切な出力の生成や、機密情報を窃取など、新たなセキュリティリスクが発生しています。このような AI システムに対する新たな脅威に対しセキュリティを確保するため、生成 AI を組み込んだシステム特有のリスクを可視化し、対応策を提示するサービスが「生成 AI 利用システムセキュリティ診断」です。

金融業界をはじめとしたセキュリティ対策に知見を持つ三菱総研 D C S と、攻撃者の手法を熟知したホワイトハッカーが多数在籍する GMO サイバーセキュリティ by イエラエがタッグを組むことで、最先端のセキュリティ対策をお客様に提供します。

■ 「生成 AI 利用システムセキュリティ診断」の特長

「生成 AI 利用システムセキュリティ診断」は、GPT 等の LLM を利用して構築したアプリケーションに対し、敵対的プロンプト (Adversarial Prompting) を用いた擬似攻撃を行い、アプリケーションに内在するセキュリティリスクを調査するサービスです。

■ サービスページ

https://www.dcs.co.jp/solution/ai_diagnostic/

■ 対応可能な言語モデル

GPT-3.5、GPT-4、Gemini、Claude3、Claude 3.5 Sonnet 等

※その他の LLM、ChatGPT プラグイン等をご利用の際にも気軽にご相談ください。

■ 今後の展開

両社は今回の協業をきっかけに、AI 技術の進展に伴い発生する新たなセキュリティリスクへの対策を図り、お客様の生成 AI 活用を支援します。他分野でも連携を広げ、増大するサイバーリスクに対し柔軟に対応できる環境を創出することで、皆様に安心という価値を提供してまいります。

■ 三菱総研DCS株式会社について

1970 年の創業以来、銀行・クレジットカードなど金融関連業務で豊富な実績を有する IT 企業です。2004 年からは三菱総研グループの中核企業として、コンサルティングから運用まで、高品質なソリューション・サービスを幅広いラインナップでご提供し、お客様の課題解決に貢献しています。近年は、AI・データ分析技術を用いた分野など時代の先端をいく技術を積極的に取り入れ、新たな価値の創出に努めています。

会社 HP : <https://www.dcs.co.jp/>

■ GMO サイバーセキュリティ by イエラエについて

GMO サイバーセキュリティ by イエラエは、国内最大規模のホワイトハッカーで組織されたサイバーセキュリティのプロフェッショナルカンパニーです。GMO サイバーセキュリティ by イエラエは、「世界一のホワイトハッカーの技術力を身近に」を目指して、各種脆弱性診断、ペネトレーションテスト、セキュリティコンサルタント、SOC サービス、フォレンジック調査まで包括的にサイバーセキュリティ対策サービスをご提供します。

会社 HP : <https://gmo-cybersecurity.com/>

※本プレスリリース内の会社名、商品名は各社の商標、または登録商標です。

■ 問い合わせ先

三菱総研DCS株式会社

〒140-8506 東京都品川区東品川四丁目 12 番 2 号

・当サービスに関して マネージドソリューション開発部 E-mail: security-biz@dcs.co.jp

・当リリースに関して 広報部 TEL:03-3458-8214 E-mail:kouhou@dcs.co.jp

GMO サイバーセキュリティ by イエラエ株式会社

〒150-8512 東京都渋谷区桜丘町 26 番 1 号セルリアンタワー 7F

・当リリースに関して マーケティング部 広報・伊礼 E-mail: irei@gmo-cybersecurity.com