2026 年 4 月 27 日

報道関係各位

GMO サイバーセキュリティ by イエラエ株式会社

GMO サイバーセキュリティ by イエラエ、「AI エージェントペネトレーションテスト」を提供開始

～ホワイトハッカーが実攻撃手法で AI エージェントのリスクを検証～

GMO インターネットグループの GMO サイバーセキュリティ by イエラエ株式会社（代表取締役 CEO：牧田 誠　以下、GMO サイバーセキュリティ by イエラエ）(※1) は、2026 年 4 月 27 日、企業内で利用される AI エージェント・チャットボット・RAG（Retrieval-Augmented Generation）(※2) などを対象に、サイバー攻撃に悪用されるリスクを攻撃者と同等の手法で検証する「AI エージェントペネトレーションテスト」の提供を開始しました。

本サービスでは、ホワイトハッカーがお客様の業務フローやシステムの権限設定、外部アプリケーションとの連携などを踏まえて、AI を起点とした情報漏えい・不正操作・権限逸脱等につながるリスクの可視化と対策を提案します。これにより、企業は AI を業務で安全に利用することができます。

（※1）　GMO サイバーセキュリティ by イエラエ株式会社は GMO インターネットグループ株式会社の連結会社です。

（※2）　外部データを検索し回答生成に活用する技術のこと。

【サービス開始の背景】

昨今、様々な業種において、業務自動化および生産性向上を目的とした AI 活用が加速しています。その一方で、企業では AI を利用することで意図せず個人情報や業務上の機密情報が漏えいするリスクや、利用中の AI がサイバー攻撃の踏み台として悪用されるといったリスクへの懸念が高まっています。

このような背景から、GMO サイバーセキュリティ by イエラエが誇るホワイトハッカーのノウハウを活用し、AI をサイバー攻撃の起点とした場合の実践的なペネトレーションテスト（侵入テスト）を提供開始いたしました。

【「AI エージェントペネトレーションテスト」の概要】（https://gmo-cybersecurity.com/service/assessment/ai-agent/）

■お客様の業務環境におけるサイバー攻撃リスクを検証

お客様の AI 利用状況をホワイトハッカーがヒアリングし、オリジナルのテストシナリオを作成します。お客様からテスト用の社員向け業務用パソコンをお借りし、実際の攻撃者と同じ手法で業務利用中の AI に内在するリスクを検証します。

LLM（Large Language Model）（※3）に対するプロンプトインジェクション（※4）の動作検証のほか、AI が持つシステムの権限や、AI が取り扱うことを許可されたデータ、AI と連携するシステムを対象にすることで、情報漏えいや不正操作に直結する具体的なリスクを可視化します。

■AI の業務活用に伴うリスクの例

AI の業務活用では、以下のようなリスクが懸念されます。

意図しない情報漏えい	AI が業務データや機密情報にアクセスできる状態で、悪意のあるプロンプト混入操作により社外への情報流出が発生するリスクがあります。
権限逸脱	AI エージェントに付与された権限が、業務上必要な範囲を超えており、本来制限されるはずのデータへのアクセスや操作が可能になるリスクがあります。
不正操作と横展開	外部システムやワークフローとの連携を悪用し、AI を踏み台としてシステム全体に影響を及ぼすリスクがあります。

また、本サービスは、AI セーフティ・インスティテュート （AISI）が発行する、「AI セーフティに関するレッドチーミング手法ガイド（第 1.10 版）」に基づいた検証も可能です。（※5）

「AI セーフティに関するレッドチーミング手法ガイド（第 1.10 版）」とは、AI システムの開発者や提供者が、対象の AI システムに施したリスクへの対策を攻撃者の視点から評価するための手法をまとめた資料です。

（※3） LLM（Large Language Model：大規模言語モデル）膨大なテキストデータをディープラーニングし、人間のような自然な文章生成や理解を行う AI モデルのこと。

（※4） 生成 AI や LLM に対し、悪意のあるプロンプト（指示）を混入し、機密情報漏えいや不正操作などの意図しない動作を引き起こすサイバー攻撃のこと。

（※5） 「AI セーフティに 関するレッドチーミング手法ガイド（第 1.10 版）」を基に、お客様の環境や業務実態に合わせたペネトレーションテストを提案します。

■「AI エージェントペネトレーションテスト」の調査対象の例

・Microsoft 365 Copilot / Azure OpenAI 等のエンタープライズ AI サービス
・業務自動化・社内オペレーション支援を目的とした AI エージェント
・社内ナレッジ検索・回答生成を行う RAG システム

・チャットボット
・その他、社内ツール連携（ファイル、チケット、CRM、ワークフロー等）を含む AI 機能など

■本サービスのお問い合わせ先について

下記サービスお問い合わせフォームよりご連絡ください。
1 営業日以内(※6)に、担当者よりご連絡を差し上げます。

https://gmo-cybersecurity.com/contact/service/

（※6）　休業期間中にいただいたお問い合わせは翌営業日以降順次ご対応させていただきます。

【今後の展望】

AI 活用が急速に進む一方で、業務データや権限、外部連携を扱う AI エージェントには、従来の LLM 単体の評価では捉えきれないリスクが潜在しています。GMO サイバーセキュリティ by イエラエは、本サービスを通じて、企業が安全かつ円滑に AI を活用して業務を遂行できるよう支援するとともに、AI セキュリティ診断の知見を蓄積し、サービスの継続的な改善・拡充を進めてまいります。

今後も、世界トップクラスのホワイトハッカーの技術力を活かし、最先端の脅威に対応するセキュリティサービスの提供を通じて、安心・安全なデジタル社会の実現に貢献してまいります。

【GMO サイバーセキュリティ by イエラエについて】（https://gmo-cybersecurity.com/）

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。会社理念である「人を助ける信念を守るチカラに変えていく」ために今後も最先端の技術と実践的な教育を通じて、日本のサイバーセキュリティの強化に貢献していきます。また、「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。

以上

【報道関係お問い合わせ先】

●GMO サイバーセキュリティ by イエラエ株式会社
マーケティング部　広報担当　伊礼
TEL：03-6276-6045
E-mail：pr@gmo-cybersecurity.com

●GMO インターネットグループ株式会社
グループ広報部　PR チーム　望月
TEL：03-5456-2695
お問い合わせ：https://group.gmo/contact/press-inquiries/

【GMO サイバーセキュリティ by イエラエ株式会社】（URL：https://gmo-cybersecurity.com/）

会　社　名	GMO サイバーセキュリティ by イエラエ株式会社
所　在　地	東京都渋谷区桜丘町 26 番 1 号　セルリアンタワー
代　表　者	代表取締役 CEO　牧田　誠
事 業 内 容	■Web アプリ及びスマホアプリ脆弱性診断 ■ペネトレーションテスト ■不正利用（チート）診断　■IoT 脆弱性診断　■自動車脆弱性診断 ■フォレンジック調査　■CSIRT 支援　■クラウドセキュリティ診断 ■クラウドセキュリティ・アドバイザリー
資　本　金	1 億円

【GMO インターネットグループ株式会社】（URL：https://group.gmo/）

会　社　名	GMO インターネットグループ株式会社　（東証プライム市場　証券コード：9449）
所　在　地	東京都渋谷区桜丘町 26 番 1 号　セルリアンタワー
代　表　者	代表取締役グループ代表　熊谷　正寿
事 業 内 容	持株会社（グループ経営機能） ■グループの事業内容 インターネットインフラ事業 インターネットセキュリティ事業 インターネット広告・メディア事業 インターネット金融事業 暗号資産事業
資　本　金	50 億円