EG Secure Solutions News Release

報道関係者各位

2025 年 9 月 17 日

EG セキュアソリューションズ株式会社

サイバーセキュリティ企業【EG セキュアソリューションズ】
生成 AI に悪影響を与えるデータポイズニング対策に！
「LLM 脆弱性診断サービス」を提供開始
～AI 技術の急速な普及に伴う新たなセキュリティリスクに対応～

イー・ガーディアン株式会社（https://www.e-guardian.co.jp/ 東京都港区 代表取締役社長：高谷 康久　以下、「イー・ガーディアン」）のグループ会社である EG セキュアソリューションズ株式会社（https://www.eg-secure.co.jp/ 東京都港区 代表取締役：高谷 康久　以下、「EG セキュアソリューションズ」）は、生成 AI や大規模言語モデル（LLM）を活用したサービスに潜む脆弱性を専門的に診断する「LLM 脆弱性診断サービス」の提供を開始しました。

EG Secure Solutions

イー・ガーディアングループは、安心・安全なインターネット環境の実現に向け、ネットパトロール、カスタマーサポート、デバッグ、脆弱性診断などネットセキュリティに関わるサービスを一気通貫で提供しております。特に EG セキュアソリューションズは、ネットセキュリティにおける課題解決を目的としたサービスを幅広く展開しております。

近年、生成 AI の活用が企業活動に急速に広がる一方で、従来のセキュリティ対策では検出が困難な新たなリスクが顕在化しています。例えば生成 AI は特性上、膨大なデータを学習、保有するためこれを悪用した情報漏洩や、学習データやプロンプトに含まれる機密情報が意図せず漏洩するリスクがあります。また、意図的に誤った情報や、悪意のある情報などを学習データに混入させて誤情報を生成・拡散させる「データポイズニング」などといった新たなセキュリティリスクがあります。

このような状況を受け、EG セキュアソリューションズは、新たなセキュリティリスク対策として「LLM 脆弱性診断サービス」の提供を開始する運びとなりました。

本サービスでは、LLM を活用したチャットボットや業務支援ツールに潜むプロンプトインジェクション、機密情報の漏洩、不適切な出力生成（ハルシネーション）などといった LLM 特有の脅威に対して、OWASP Top 10 for LLM Applications 2025 をベースに EG セキュアソリューションズの豊富なナレッジを加えてセキュリティリスクを専門的に診断いたします。これにより、導入企業が安全かつ確実にサービス運用できるようになり、企業の信頼性とブランドイメージ向上に貢献いたします。

今後も、イー・ガーディアングループは、専門性と質の高いサービスを提供し、ミッションである「We Guard All」の実現に向け、人々の生活をより便利に、豊かにするサービス・製品の開発に尽力して参ります。

【「LLM 脆弱性診断サービス」について】

詳細 URL：https://www.eg-secure.co.jp/service/llm-inspection

■サービスの特徴

1. LLM の特性を踏まえたリスク評価

単に一般的な脆弱性を洗い出すのではなく、LLM の構造や用途に応じて、システムごとの固有リスクまで丁寧に診断します。

2. 想定されるユースケースに応じた診断設計

利用されている LLM の運用形態や対話設計を考慮し、プロンプト構造や出力形式に即したリスク項目を抽出することで、より実態に即した検証を実施します。

3. モデル固有の潜在リスクにも対応

対象となる LLM モデルの仕様や学習特性に基づき、標準的な攻撃手法だけでなく、特定モデルに依存する挙動や潜在的リスクまで網羅的に分析します。

■主な診断項目

- 個人情報や機密情報の漏洩有無
- 誤情報生成（ハルシネーション）の傾向評価
- システムプロンプト・学習データ由来情報の漏洩リスク
- プラグイン・外部連携機能の脆弱性検証

■比較表

項目	従来の脆弱性診断サービス	LLM脆弱性診断サービス
診断対象	Webアプリ、OS、NW機器など	LLMアプリケーション、LLMモデルなど
検出対象	SQLインジェクション、 XSSなど	情報漏洩、誤情報生成（ハルシネーション）など
アプローチ	診断ツール、手動	LLMの特性、形態、設計に即した検証
診断項目	攻撃に対する脆弱性、設定ミスなど	個人情報の漏洩有無、連携機能の脆弱性など
攻撃	不正アクセス、DDoSなど	プロンプトインジェクションなど

【導入事例：弁護士ドットコム株式会社】

「LLM 脆弱性診断サービス」は、弁護士ドットコム株式会社が提供するリーガル特化型 AI エージェント「Legal Brain エージェント」に初導入いただきました。法律実務においては、誤った情報出力による影響が極めて大きく、加えて日々扱う情報には守秘義務の対象となる機密性の高いデータが数多く含まれます。そのため、設計段階から厳格な品質基準と情報管理体制が求められており、生成 AI の導入に際しても、一般的な業務用 AI とは異なるセキュリティ水準が必須となっていました。こうした背景を踏まえ、より高度な生成 AI セキュリティ対策として、本サービスが採用されました。

今回の本サービスの導入は、単なるセキュリティチェックにとどまらず、機密性・正確性・信頼性という 3 つの観点から、生成AIの実用化における新たな基準づくりを後押しする重要な取り組みになると期待されています。

■弁護士ドットコム株式会社　会社概要

代表者　　：代表取締役社長 兼 CEO　元榮 太一郎
所在地　　：東京都港区六本木四丁目 1 番 4 号 黒崎ビル
設立　　：2005 年 7 月 4 日
資本金　　：545 百万円（2025 年 6 月現在）
業務内容　　：「プロフェッショナル・テックで、次の常識をつくる。」をミッションとして、人々と専門家をつなぐポータルサイト「弁護士ドットコム」「税理士ドットコム」「BUSINESS LAWYERS」、契約マネジメントプラットフォーム「クラウドサイン」を提供
URL　　：https://www.bengo4.com/corporate/

【イー・ガーディアングループ 概要】

1998 年設立。2016 年に東証一部上場。2022 年に東証プライム市場へ移行。イー・ガーディアンはネットパトロール、カスタマーサポート、デバッグ、脆弱性診断などネットセキュリティに関わるサービスを一気通貫で提供する総合ネットセキュリティ企業です。センターは、提携先を含めてグループで国内 8 都市海外 3 都市 19 拠点の業界最大級の体制を誇ります。昨今は Fintech・IoT 業界への参入や RPA 開発による働き方改革への寄与など、時代を捉えるサービス開発に従事し、インターネットの安心・安全を守っております。

■EG セキュアソリューションズ株式会社 会社概要

代表者　　：代表取締役　高谷 康久
所在地　　：東京都港区虎ノ門 1-2-8 虎ノ門琴平タワー8F
設立　　：2008 年 4 月
資本金　　：1,000 万円（2025 年 3 月末日現在）
業務内容　　：1. 情報セキュリティ、情報システムに関する監査、コンサルティング
2. 情報セキュリティに関する調査、研究、執筆
3. 情報セキュリティ関連の教育及びコンテンツ制作
4. セキュリティ製品の開発、販売、サポート
URL　　：https://www.eg-secure.co.jp/

■イー・ガーディアン株式会社 会社概要

代表者　　：代表取締役社長　高谷 康久
所在地　　：東京都港区虎ノ門 1-2-8 虎ノ門琴平タワー8F
設立　　：1998 年 5 月
資本金　　：1,967 百万円（2025 年 3 月末日現在）
業務内容　　：ブログ・SNS・掲示板企画コンサルティング/リアルタイム投稿監視業務/ユーザーサポート業務/オンラインゲームカスタマーサポート業務/コンプライアンス対策・風評・トレンド調査業務/コミュニティサイト企画・サイト運営代行業務・広告審査代行サービス業務/人材派遣業務
URL　　：https://www.e-guardian.co.jp/

【本件に関するお問い合わせ先】
イー・ガーディアン株式会社　広報担当
TEL：0120-665-046　E-mail：info@e-guardian.co.jp