報道関係者各位
プレスリリース

2026年5月27日

グローバルセキュリティエキスパート株式会社

GSXは生成AI時代のセキュリティリスクに備える「AIプロンプト診断」を提供開始
OWASP LLM Top 10準拠で企業の生成AI活用を安全に加速

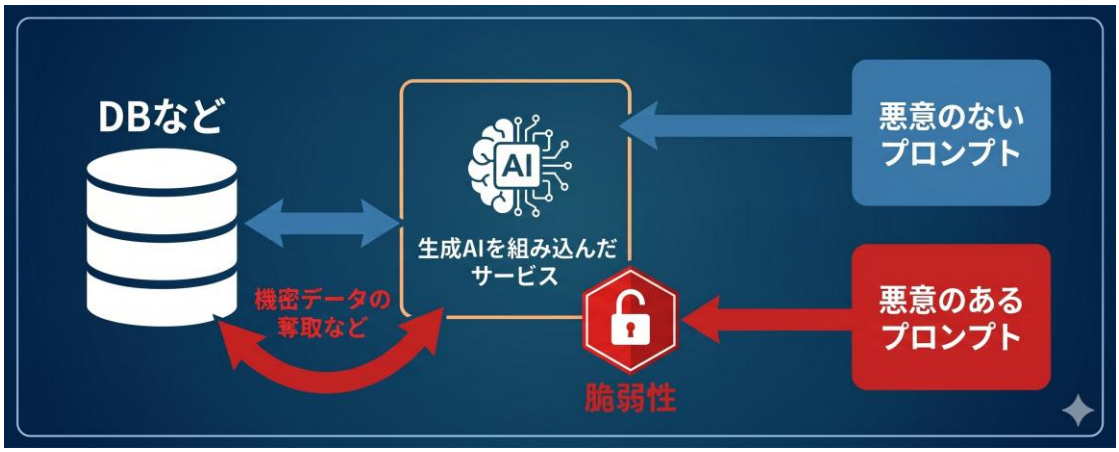
グローバルセキュリティエキスパート株式会社（本社：東京都港区海岸1-16-1、代表取締役社長：青柳 史郎、証券コード：4417、https://www.gsx.co.jp/、以下、GSX）は、生成AI活用の広がりを受け、生成AIをセキュアに活用するための「AIプロンプト診断(AI Prompt Security)」サービスの提供を開始しました。

生成AIは便利である一方、プロンプト（AIへの命令文）から攻撃を受ける（プロンプトインジェクション）ことで、生成AIを経由して情報を奪取されるといったリスクも起こりえます。

本サービスは、ChatGPT API等の生成AIを組み込んだWebアプリケーションに対し、プロンプトインジェクション・プロンプトリークなどAI特有の脆弱性を診断するもので、グローバル標準であるOWASP LLM Top 10に基づく8つの診断カテゴリにより、AI環境のセキュリティリスクを網羅的に可視化します。

生成AI時代に不可欠となる新たなセキュリティ基準を企業に提供することで、安心して生成AIを活用できる環境構築を支援します。

プロンプトインジェクション概念イメージ



生成AIを組み込んだサービスに脆弱性がある場合、悪意のあるプロンプトでデータを摂取されるリスクがあるため、診断を行うことでリスクを取り除く

■　生成AI活用の加速と企業が直面する新たな経営リスク

企業における生成AIの導入が急速に進む中、従来のセキュリティ対策では防ぎきれない新たな脅威が顕在化しています。OWASPが2025年版で発表した「Top 10 for LLM Applications」(*1)では、プロンプトインジェクションが第1位の最重要リスクとして位置づけられており、本番AIデプロイメントの73%超でこの脆弱性が検出されています。生成AIを業務に組み込む企業が増える一方で、AI固有のセキュリティ制御を導入済みの企業はわずか34%にとどまり、導入スピードとセキュリティ対策の整備に大きなギャップが生じています。機密情報の漏洩、著作権侵害、ハルシネーションによる誤情報拡散など、生成AI特有のリスクは企業の信用を揺るがす重大なインシデントにつながる可能性があり、適切な対策なしに利用することは経営リスクそのものとなっています。

(*1) Top 10 for LLM Applications
https://genai.owasp.org/resource/owasp-top-10-for-llm-applications-2025/

■　GSXの「AIプロンプト診断」が解決する価値

ChatGPT API等を自社のWebアプリケーションに組み込んで活用する企業にとって、プロンプト設計・入力制御・データ管理は自社の責任範囲となり、独自のセキュリティ対策と診断が必須です。本サービスは、従来のWebアプリケーションには存在しなかったAI特有の新たな攻撃ベクトルに対応し、LLMアプリケーションを取り巻く脅威ランドスケープを網羅的に検査します。20年以上の脆弱性診断実績に裏打ちされたGSXの実践的な検査手法とグローバル標準のOWASP LLM Top10を融合させることで、企業は生成AIの利便性を享受しながら、経営層が安心できるセキュリティレベルを確保することができます。

■　「AIプロンプト診断」3つの特長

1. OWASP LLM Top 10準拠の網羅的な診断

グローバル標準に基づく8つの診断カテゴリでAI特有のリスクを漏れなく検査し、プロンプトインジェクション、プロンプトリーク、データポイズニングなど最新の攻撃手法に対応します。

2. 経営視点と技術視点の両面からの報告

4段階の総合評価で経営層が現在のリスクレベルを直感的に把握でき、問題の原因と具体的対策を記載することで開発現場が即座に修正アクションへ移行可能です。

3. 多層防御フレームワークに基づく包括的対策

脆弱性の特定に加えてシステム全体でのDefense in Depthの確立を支援し、AIモデルのセキュリティ、権限管理、アクセスコントロール、データセキュリティまで一貫した対策を提案します。

■　診断カテゴリと対応するOWASP LLM Top 10

GSXのAIプロンプト診断では、OWASP LLM Top10の脅威分類と統合した8つの診断項目を提供しています。コア診断項目として、AIモデルへの直接的な攻撃ベクトルを検査する「プロンプトインジェクション(OWASP LLM01対応)」「プロンプトリーク(OWASP LLM02対応)」「データポイズニング(OWASP LLM04/LLM08対応)」、さらにシステムおよびデータへの波及的脅威を検査する「問題のある応答/アプリケーション脆弱性(OWASP LLM03/LLM05対応)」「サービス拒否(OWASP LLM10対応)」「問題のあるサードパーティの利用(OWASP LLM05対応)」「機微データ漏洩(OWASP LLM07対応)」を網羅的に診断します。これにより、生成AI環境の脆弱性を構造化して可視化し、実践的な対策を提供します。

診断カテゴリ	対応 OWASP 項目	主なリスク
プロンプトインジェクション	LLM01	AI モデルへの直接的な攻撃ベクトル
プロンプトリーク	LLM02	システムプロンプトや機密情報の漏洩
データポイズニング	LLM04/LLM08	学習データの汚染とモデルの信頼性低下
問題のある応答/アプリケーション脆弱性	LLM03/LLM05	システムおよびデータへの波及的脅威
サービス拒否	LLM10	リソース消費による可用性低下
問題のあるサードパーティの利用	LLM05	外部サービスに起因するリスク
機微データ漏洩	LLM07	個人情報や機密データの不正な開示
アプリケーション脆弱性	LLM03/LLM05	アプリケーションレベルのセキュリティリスク

■　3つの導入メリット

1. 「やらないリスク」の可視化により、生成 AI 活用を躊躇していた企業が具体的なリスクレベルと対策を把握し、安心して AI 活用を推進できるようになります。

2. 経営層向けの 4 段階総合評価と技術者向けの具体的対策レポートにより、経営判断と現場の修正アクションを同時に支援し、組織全体での迅速な対応が可能となります。
3. OWASP LLM Top10 という国際標準に準拠した診断により、グローバル展開を視野に入れる企業にとって説明責任とコンプライアンス要件を満たすことができます。

■ 「AIプロンプト診断」サービス概要

【診断対象】
ChatGPT API 等の生成 AI を組み込んだ Web アプリケーション（API 組み込み開発）

【診断項目】
OWASP LLM Top 10 に基づく 8 つの診断カテゴリ（プロンプトインジェクション、プロンプトリーク、問題のある応答、データポイズニング、サービス拒否、問題のあるサードパーティの利用、機微データ漏洩、アプリケーション脆弱性）

【成果物】
総合評価レポート（4 段階評価）、脆弱性診断報告書、具体的対策提案書

【サービス URL】
https://www.gsx.co.jp/services/findrisk/ai_prompt_security.html

【お問い合わせ】
https://www.gsx.co.jp/inquiry

◆グローバルセキュリティエキスパート株式会社

社名：グローバルセキュリティエキスパート株式会社
東京本社：〒105-0022 東京都港区海岸1-16-1 ニューピア竹芝サウスタワー10F
代表者：代表取締役社長　青柳 史郎
証券コード：4417
上場証券取引所：東京証券取引所グロース市場
資本金：546百万円（2026年3月末）
設立　：2000年4月（グローバルセキュリティエキスパートへの商号変更日を設立日として記載）
コーポレートサイトURL：https://www.gsx.co.jp/

【本リリース内容に関するお問い合わせ先】

グローバルセキュリティエキスパート株式会社　経営管理本部　マーケティング部
TEL：03-3578-9001　MAIL：mktg@gsx.co.jp