各位

2025 年 6 月 19 日

株式会社 GRCS

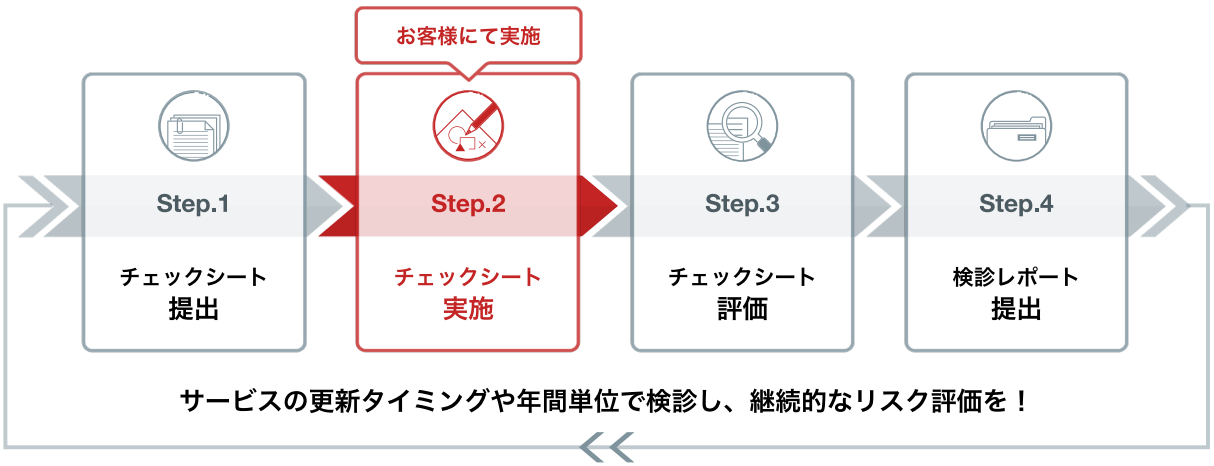
AI 活用サービスのリスク検診サービスをリリース

生成 AI 利用のセキュリティリスクを多角的に評価

株式会社 GRCS（本社：東京都千代田区、代表取締役社長：佐々木 慈和、以下 当社）は、生成 AI を活用する企業や組織が抱えるリスクを専門家が評価し、可視化するサービス「AI 活用サービスリスク検診」（以下 本サービス）の提供を開始しました。

近年、急速に発達した生成 AI 技術は、文書の自動生成やプログラムコード生成の補助、クリエイティブ業務の支援など、企業活動の生産性向上に大きく貢献しています。しかしその一方で、生成 AI の活用には企業情報の漏洩やモデル悪用、不正アクセスといったリスクが潜んでおり、企業はこうした新たなセキュリティリスクへの対応を求められています。

本サービスは、生成 AI を活用する企業が直面する脅威情報を洗い出し、セキュリティ体制の評価を行うことで、現状の潜在的なリスクを明確にする専門的な診断サービスです。国際的な脅威動向※1 を参照した評価を行い、モデルや API、プロンプト、出力など、生成 AI を活用したサービスに見られる脅威を複数の視点から分析します。



＜特長＞

・AI とセキュリティの専門家によるリスク評価

・生成 AI を活用したサービスに潜む脅威の多角的な評価

・スコアリング、対策一覧、評価結果を検診レポートとして提供

本サービスの利用により、生成 AI を活用したサービスを開発する企業や、業務等で生成 AI を利用している企業は、生成 AI サービスの脅威箇所を把握し、評価結果を自社の施策の策定やサービスの安全性を説明する根拠とすることができます。
サービス URL: https://www.grcs.co.jp/consulting/airs

当社は今後も、企業における高いセキュリティレベルの維持と生成 AI の安全な利活用による業務効率向上に寄与してまいります。

※1　国際的な脅威動向として、「OWASP Top 10 for LLM Applications※2」および「MITRE ATLAS™※3」は、それぞれ OWASP® Foundation および MITRE Corporation により策定・提供されているものであり、本サービスはこれらの団体による認定・承認を受けたものではありません。
当社ではこれらのガイドライン・知見を参考に、独自の評価と対策方針を策定しています。
※2　OWASP Top 10 for LLM Applications
https://owasp.org/www-project-top-10-for-large-language-model-applications/
※3　MITRE ATLAS™（Adversarial Threat Landscape for Artificial-Intelligence Systems）
https://atlas.mitre.org/

＜会社概要＞

会 社 名 ： 株式会社 GRCS
代 表 者 ： 代表取締役社長　佐々木慈和
所 在 地 ： 東京都千代田区丸の内 1-1-1 パレスビル 5F
設　　立 ： 2005 年 3 月
資 本 金 ： 50 百万円
上場市場 ： 東京証券取引所グロース（証券コード：9250）
事業内容 ： GRC・セキュリティ関連ソリューション事業
U　R　L ： https://www.grcs.co.jp/

本プレスリリースに関するお問い合わせ先
株式会社 GRCS　ＩＲ担当
E-mail: ir@grcs.co.jp