

各位

2026 年 10 月 22 日

株式会社 GRCS

**AI を悪用したサイバー攻撃には、AI で対策を
セキュリティ診断体験キャンペーン、好評につき期間延長を決定
事業継続を脅かす不正アクセスリスクへの対応を支援**

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、当社が提供する AI 駆動型ペネトレーションテストを特別価格で提供するキャンペーン（以下 本キャンペーン）について、好評につきキャンペーン期間を延長することをお知らせいたします。

<背景>

近年、不正アクセスや巧妙なサイバー攻撃による重大な情報漏えい事案が多発しており、企業の事業停止やブランド毀損、法的な賠償責任など、経営基盤そのものを揺るがすビジネスリスクが急速に高まっています。攻撃者が AI 技術を悪用して侵入手法を多様化・自動化させている現在、従来の形式的な脆弱性診断や年 1 回の定期診断だけでは、十分な対策とは言えないのが現状です。

サイバーセキュリティにおける課題は単なる IT 部門の業務ではなく、自社およびサプライチェーン全体を守る経営課題として、全社での的確な把握と迅速な意思決定が強く求められています。こうした情勢を受け、より多くの企業に経営リスク評価として最新のセキュリティ診断を体験いただくため、本キャンペーンの期間延長を決定いたしました。

<本キャンペーンについて>

本キャンペーンでは、AI 駆動型 CTEM※支援ソリューション「RidgeBot」を活用したペネトレーションテストを期間限定で特別価格にて提供します。テストの一連の流れを AI 駆動で実施することにより、企業のセキュリティリスクを短期間で、タイムリーに、かつ効果的に評価することが可能です。

<キャンペーン詳細>

- **キャンペーン価格：** 55 万円（税込）～
- **キャンペーン期間：** 実施中～2026 年 11 月末日までのご契約
※ 募集社数に達した場合、期間内でもキャンペーンを終了する場合がございます。
- **提供サービス：** インターネット上に公開されている企業の Web サイトや、外部からアクセスできるシステム（ネットワーク、サーバーなど）を対象に、疑似攻撃によるリスク検知・分析を行い、診断レポートを提供します。
- **お問い合わせ：** キャンペーン URL よりお問い合わせください

キャンペーン URL：<https://www.grcs.co.jp/promotion/penetrationtest>

<「RidgeBot」について>

攻撃対象領域の検出からペネトレーションテスト、レポーティングまでのプロセスを AI により自動化し、継続的にセキュリティ評価を実施する CTEM 支援ソリューション。ハッカーレベルのセキュリティテストによって重要資産を保護することを目的とし、管理すべき資産の検出からリスクの報告までの活動を自動かつ継続的に実施できる。

製品ページ URL : <https://www.grcs.co.jp/products/ridgebot>

※CTEM (Continuous Threat Exposure Management)

継続的な脅威エクスポージャ管理。Gartner 社が提唱した概念。従来の脆弱性管理では拡大する攻撃対象領域に対応できなくなるため、継続的に脆弱性とエクスポージャを認識、評価することで論理的に意思決定をするセキュリティリスクマネジメントのアプローチ。

<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 : 131 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 I R 担当
E-mail: ir@grcs.co.jp