各位

2026 年 11 月 25 日

株式会社 GRCS

AI ツールの認証情報漏えいリスクを調査する「無料診断キャンペーン」を開始

ドメインの入力だけで企業の AI アカウントの情報流出を特定

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・開発 AI ツールの急速な普及に伴い急増している認証情報の漏えいリスクに対処するため、法人・団体向け「AI 認証情報漏えい診断 無料ドメイン診断キャンペーン」（以下 本キャンペーン）を開始いたします。

＜背景＞

ChatGPT や Claude をはじめとする対話型 AI や AI コーディングアシスタントの業務利用が急速に広がるなか、AI アカウントへのログインは、シングルサインオン（SSO）や多要素認証（MFA）によって安全性が確保されていると思われがちです。しかし近年、端末から情報を盗み出すマルウェア（インフォスティーラー※）が悪用され、ブラウザ内のログイン状態や API キーを窃取されることで、パスワードや多要素認証を使わずに AI アカウントへ不正侵入される手口が頻発しています。

AI アカウントに不正アクセスされると、従業員が入力した内部情報の閲覧・窃取に加え、組織のクラウド環境の無断利用による高額なサーバー利用料の請求や犯罪行為への悪用など、深刻な被害に直結します。当社は、こうした認証情報が流出している状態を早期に発見し有効な対策につなげるため、本キャンペーンを実施いたします。

＜本キャンペーンについて＞

本キャンペーンでは、対象の企業ドメインに関連する認証情報が、情報窃取型マルウェアによって流出していないかを無料で診断します。特別なシステム導入は不要で迅速に現状を把握でき、診断結果は指定された社用アドレスにのみ配信されます。情報の漏えい、またはその疑いが検知された場合は、不正アクセスの連鎖を早期に遮断するために推奨される初期対応の手順をご案内します。

さらにご希望に応じて、脅威動向を常時監視し、新たな流出をいち早く察知する継続的な監視ソリューションの導入・運用など、企業の状況に合わせた支援をご提案します。

受付期間： 2026 年 11 月 25 日より受付開始（期間限定）

対　　象： 自社の AI ツール利用状況や認証情報の漏えいリスクに懸念を持つ企業・団体

内　　容： 情報窃取型マルウェアによって流出した自社の認証データの検索・特定

費　　用： 無料

お申込み・お問い合わせ：以下のお問い合わせフォームよりお問い合わせください

https://www.grcs.co.jp/contact-airisk

AI の業務活用が企業の競争力を左右する時代において、利便性の追求と強固なセキュリティの両立は重要な経営課題です。当社は今後も、最新のサイバー脅威に対応したソリューションの提供を通じ、組織の安全な AI 利活用と持続可能な成長を支援してまいります。

※ インフォスティーラー（情報窃取型マルウェア）：パソコン等に感染し、ブラウザに保存された ID・パスワードや認証データなどを数秒で盗み出して外部へ送信する不正プログラムの総称。

＜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　ＩＲ担当
E-mail: ir@grcs.co.jp