2026年８月28日

各 位

会　社　名　株式会社トレジャー・ファクトリー
代 表 者 名　代表取締役社長　野坂　英吾
（コード番号：3093　東証プライム）
問 合 せ 先　執行役員経営企画室長　金坂　剛嗣
（ＴＥＬ．０３－３８８０－８８２２）

当社連結子会社における不正アクセスによる個人情報漏えいに関するお知らせ

当社の連結子会社である株式会社カインドオル（以下「当該子会社」といいます。）が運営するECサイトにおいて、第三者による不正アクセスにより、お客様の個人情報が漏えいしたことが判明いたしましたので、下記のとおりお知らせいたします。

お客様をはじめ、関係者の皆様に多大なご心配とご迷惑をおかけしますことを、深くお詫び申し上げます。

記

１．事案の概要

当該子会社が運営するECサイトで利用しているECプラットフォームのスタッフアカウントに対し、第三者による不正アクセスが行われました。

2026年８月24日、通常業務において注文情報のエクスポートを行った際、当該スタッフアカウントに登録されているメールアドレスが当該子会社で使用していないものに変更されていることを確認したことから、ECプラットフォームの運営会社へ調査を依頼しました。

その結果、2026年８月22日に第三者による当該スタッフアカウントへの不正アクセスが行われ、その後、８月23日に当該アカウントのメールアドレスが変更され、同日、お客様情報の一括エクスポートが2回実行されていたことが確認されました。

２．漏えいした個人情報

現時点で確認されている対象者は136,464名であり、このうち住所情報を含むものは109,311名です。

対象となった可能性がある情報は以下のとおりです。

カスタマーID・氏名・住所・電話番号・生年月日・メールアドレス・メールマガジン購読状況・合計注文回数・合計購入金額・ECプラットフォーム上で管理している顧客タグ情報・ポイント情報履歴（保有・失効・累計）

※　対象となる情報項目はお客様によって異なります。

※　今回エクスポートされたデータに、クレジットカード情報及びECサイトのログインパスワードは含まれていないことを確認しております。

※　現時点において、本件に起因する個人情報の不正利用その他の具体的な二次被害は確認されておりません。

３．原因

社内調査の結果、不正アクセスを受けたスタッフアカウントを利用する従業員に対し、ECプラットフォームの運営会社を装ったフィッシングメールが送信され、当該メールに記載されたリンク先において、当該スタッフアカウントの認証情報が入力されていたことを確認いたしました。

当該PCのログ等を調査した結果、認証情報が入力された直後に今回確認されている最初の不正アクセスが発生していることから、当社グループでは、当該フィッシングメールを通じてスタッフアカウントの認証情報が第三者に取得されたことが、本件不正アクセスの原因であると判断しております。

また、当該スタッフアカウントには二段階認証が設定されておらず、メールアドレスとパスワードのみでログイン可能な状態であったことに加え、設定されていたパスワードについても十分な強度ではありませんでした。

これらの認証管理上の不備も、不正アクセスを防止できなかった要因の一つであると認識しております。

４．対応状況について

本件の判明後、当該子会社では直ちに以下の措置を実施しております。

- 不正アクセスを受けたスタッフアカウントの削除
- その他すべてのスタッフアカウントにおける不審なアクセス・操作の有無の確認
- ECプラットフォームの全スタッフアカウントにおける二段階認証の必須化
- 不正な顧客情報のエクスポート後に当該アカウントからその他の操作が行われていないかについてのECプラットフォームの運営会社への追加調査依頼

また、当該子会社は、本件について2026年８月27日付で個人情報保護委員会への報告を行っております。

５．問い合わせ窓口について

対象となるお客様に対しては、順次、本件の内容及び注意事項等について個別にご案内いたします。また、本件に関する専用のお問い合わせ窓口については、現在設置準備を進めております。体制が整い次第、速やかに当社及び株式会社カインドオルのホームページにてご案内申し上げます。

６．今後の対応及び再発防止

当該子会社では、本件判明後、すべてのスタッフアカウントについて二段階認証を必須化するとともに、アカウント及びアクセス権限の管理状況について点検を実施しております。

また、今回の原因を踏まえ、フィッシングメールへの対策強化、従業員に対する情報セキュリティ教育及びフィッシング対策訓練の徹底、顧客情報へのアクセス権限及び一括エクスポート権限の見直し、不審なログインや重要なアカウント情報の変更、大量のデータ出力等を早期に把握するための監視・エスカレーション体制の強化等を進めてまいります。

当社においても、本件を当該子会社固有の事象として捉えることなく、当社グループが利用するシステム及びクラウドサービス等について、二段階認証の設定状況、アカウント・アクセス権限管理、情報の出力権限、セキュリティ監視体制等を改めて点検するとともに、グループ全体でフィッシング対策及び情報セキュリティ教育を強化し、再発防止に取り組んで

まいります。

７．業績への影響

本件が当社グループの連結業績に与える影響については、現在精査中です。

今後、業績に重要な影響を与えることが判明した場合、その他開示すべき事項が生じた場合には、速やかにお知らせいたします。

以 上