

2026年8月28日

不正アクセスによるお客様情報漏えいに関するお詫びとお知らせ

このたび、当社が運営する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第三者による不正アクセスがあり、登録されているお客様の個人情報が入力されたことが判明いたしました。

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することとなりましたことを、心より深くお詫び申し上げます。

本件の概要及び当社の対応について、下記のとおりお知らせいたします。

1. 事案の概要

2026年8月24日、当社が通常業務として注文情報の出力を行った際、ECプラットフォームの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ました。

直ちにECプラットフォームの運営会社へ調査を依頼した結果、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た後、2026年8月23日にお客様情報の一括エクスポートが2回行われていたことが確認されました。

2. 漏えいしたお客様情報

今回、漏えいした可能性があるお客様は、現時点で136,464名であることを確認しております。

漏洩し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
- メールマガジンの購読状況
- 合計注文回数
- 合計購入金額
- 当社が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）

なお、上記のすべての情報がお客様全員について漏洩したものではなく、登録状況等により対象となる情報が異なります。また、今回漏洩したデータに、クレジットカード番号、セキュリティコード及び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。

3. 原因について

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使用していた従業員宛に、当社が利用する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の偽サイトにおいて、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のログ等を確認した結果、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、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

これらの認証官理が十分でなかったことも、第三者による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. 現在までの対応

本件の判明後、直ちに以下の対応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を削除し、アクセスできない状態としました。
- 当該アカウント以外のすべてのスタッフアカウントについて、不審なアクセス及び操作の有無を確認しました。
- ECプラットフォームの全スタッフアカウントについて、二段階認証を必須化しました。
- 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、ECプラットフォームの運営会社へ追加調査を依頼しております。

また、本件については、個人情報保護法に基づき、個人情報保護委員会への報告を実施しております。対象となるお客様に対しては、本件の内容及びご注意いただきたい事項について、個別にご案内しております。

5. 二次被害の状況およびお客様へのお願い

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。しかしながら、漏えいした情報を悪用し、当社や配送事業者、金融機関その他の事業者を装った不審なメール、SMS、電話等が行われる可能性があります。身に覚えのないメール、SMS、電話等を受けた場合には、記載されたURLへのアクセス、添付ファイルの開封、個人情報やパスワード、クレジットカード情報等の入力・回答を行わないよう、十分にご注意くださいますようお願いいたします。

当社が本件への対応を理由として、メールやSMS等により、お客様のパスワード、クレジットカード番号、セキュリティコード等の入力・回答をお願いすることはありません。

不審な連絡を受けた場合や、ご不明な点がございましたら、下記お問い合わせ窓口までご連絡ください。

6. 再発防止について

当社は今回の事態を重く受け止め、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を改めて点検しております。

今回の原因がフィッシングメールを通じた認証情報の取得であったことを踏まえ、今後、以下の対策を進めてまいります。

- フィッシングメールを含む不審な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
- 二段階認証を含む認証管理の強化
- 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
- アカウントの追加、変更及び削除に関する管理手続の見直し
- 不審なログイン、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

これらの対策を着実に実施するとともに、情報セキュリティ管理体制全体について継続的な見直しを行い、再発防止に努めてまいります。お客様の大切な個人情報をお預かりする事業者として、このような事態を発生させましたことを改めて深くお詫び申し上げます。

7. 本件に関するお問い合わせ先

対象となるお客様に対しては、順次、本件の内容及びご注意いただきたい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、速やかに当社ホームページにてご案内申し上げます。





Sell
売る

Buy
買う

Store
店舗



Work
働く

JP / EN



2026年9月2日追記

本件に関する専用お問い合わせ窓口を公開いたしました。

詳細は『不正アクセスによるお客様情報漏えいに関する専用お問い合わせ窓口開設のお知らせ』をご確認ください。

Kindal Official SNS



Sell 売る

店頭買取
宅配買取
出張買取
法人買取

Buy 買う

カインドオールオンライン

Search 探す

Shop
店舗一覧
現在地から店舗を探す

Brand
ジャンルから探す
ブランド名で探す

Read 読む

ショップコラム
買取コラム
ショップブログ
サステナビリティ
よくある質問

Work 働く

採用情報

会社概要 | プライバシーポリシー | 利用規約 | 取材依頼 | 電子公告 | お問い合わせ

古物商許可番号：大阪府公安委員会 第621131100169号

Copyright © 2012-2020 Kindal All right reserved.



ブランド古着の買取 / 販売