

2026年10月9日

各 位

株式会社アドベンチャー
東京都渋谷区恵比寿 4-20-3
恵比寿ガーデンプレイスタワー4F
代表取締役社長 中村 俊一
(コード番号：6030 東証グロース)
問い合わせ先 取締役 中島 照
ir@adventure-inc.co.jp

不正アクセスによるお客様情報の流出に関するお詫びとお知らせ

このたび、当社が運営する比較予約サイト”skyticket”のシステムが第三者による不正アクセスを受け、お客様の個人情報外部に流出したこと、または流出したおそれがある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るご迷惑とご心配をおかけいたしますことを深くお詫び申し上げます。

当社は本件を確認した後、直ちに不正アクセスの経路を遮断し、調査と対策を進めております。現時点で判明している内容を、以下のとおりご報告いたします。

記

1. 事案の概要

本件は、それぞれ異なる経路による次の3件の不正アクセスです。

(1) 当社サーバーへの不正アクセス

- ・ 発生期間：2026年10月2日～10月4日
- ・ 発覚日：2026年10月5日
- ・ 原因：skyticketの一部の管理機能を不正に操作され、そこから当社の他のサーバーおよびクラウド上に保管していたデータに不正にアクセスされたもの
- ・ 対象となるお客様：skyticketにご登録・ご入力いただいたお客様 約1,464万件（このうち、会員様のログインパスワードを含むもの 約413万件）
- ・ 流出した情報：氏名（パスポート表記を含む）、生年月日、メールアドレス、電話番号、郵便番号・住所、お振込み時のご依頼人名義、会員様のログインパスワード（ハッシュ化した状態のもの）
- ・ なお、パスポート番号は流出していないことを確認しております。

(2) skyticket の業務管理システムへの不正アクセス

- ・ 発生日：2026 年 9 月 20 日
- ・ 発覚日：2026 年 9 月 28 日
- ・ 原因：業務管理システムの脆弱性を悪用されたもの
- ・ 対象となるお客様：17,780 件（重複を含みます。このほか件数を調査中のものがあります）
- ・ 流出した、または流出したおそれのある情報：氏名、電話番号、返金先の口座情報（金融機関名・支店名・口座種別・口座番号・口座名義）など。一部のお客様については、メールアドレス・生年月日（68 件）、住所（18 件）なども含まれます。
- ・ パスポート番号については、現時点で流出の事実は確認されておりませんが、流出がなかったかどうかを引き続き確認しております。
- ・ このほか、2026 年 9 月 9 日に、会員様 1 名のアカウントへの不正ログインを確認しております。

(3) バス予約サービスにおける予約情報の閲覧

- ・ 発生期間：2026 年 8 月 3 日～10 月 1 日
- ・ 発覚日：2026 年 10 月 1 日
- ・ 原因：バスの予約完了ページがログインをしなくても表示できる状態になっており、第三者に機械的に閲覧されたもの（10 月 1 日に修正済み）
- ・ 対象となるお客様：ご予約 約 12,000 件（ご同行者様を含むと人数はこれより多くなります）
- ・ 閲覧された、または閲覧されたおそれのある情報：ご予約お客様の氏名（カナ）、年齢、性別、生年月日（ご登録がある場合）、メールアドレス、電話番号、会員 ID、ご予約に使われた端末の種類、お支払方法・金額、ご予約日時、ご乗車便の情報（日時・乗降地・運行会社・便名・運行会社の予約番号）、ご同行者様の氏名・年齢・性別
- ・ なお、パスポート番号は流出していないことを確認しております。

また、当社はおお客様のクレジットカード番号とパスポートの画像を保存しておらず（クレジットカード情報は当社ではなく決済代行会社が保管しております。）、いずれの案件でもクレジットカード情報とパスポートの画像は流出しておりません。

2. 二次被害の有無について

現時点で、上記 1 (2) に記載の会員様 1 名のアカウントへの不正ログインを除き、本件で流出した情報が悪用されたことによる二次被害は確認されておりません。ただし、流出した情報が悪用され、次のような被害が生じるおそれがあります。

- ・ 詐欺メール等（全ての案件）：氏名、メールアドレス、電話番号、住所などを悪用し、当社、金融機関、航空会社、バス運行会社などを装った詐欺メール（フィッシングメール）・SMS・電話・郵便物が届くおそれがあります。
- ・ 不正ログイン（上記 1 (1) の会員様）：ログインパスワードは、元のパスワードに戻すことが困難な形（ハッシュ化）に変換して保存しておりましたが、解析によりパスワードが判明し、skyticket や、同じパスワードをお使いの他のサービスへの不正ログインに悪用されるおそれがあります。
- ・ 口座情報の悪用（上記 1 (2) のお客様）：口座番号などの情報だけで直ちに預金が引き出

されるものではありませんが、返金手続きなどを装って、口座の暗証番号やインターネットバンキングの ID・パスワードを聞き出そうとする連絡が行われるおそれがあります。

- ・ 予約情報の悪用（上記 1（3）のお客様）：ご乗車便の情報や予約番号などを知った第三者が、当社や運行会社を装って、予約の変更・キャンセルや追加料金の支払いを求める連絡を行うおそれがあります。

二次被害を防ぐため、下記「4. お客様へのお願い」とあわせて、次の点にご注意ください。

- ・ 本件に関する返金・補償などを名目に、振込みや手数料の支払い、アプリのインストールを求める連絡には応じないでください。当社から、本件に関してお客様に金銭のお支払いをお願いすることはございません。
- ・ 口座に身に覚えのない入出金があった場合は、お取引の金融機関にご相談ください。
- ・ バスのご予約内容に身に覚えのない変更・キャンセルがあった場合は、下記の窓口までご連絡ください。
- ・ 不審な連絡を受けた場合には、記載されたリンクや電話番号にはアクセス・連絡せず、下記の窓口までご連絡ください。

3. 当社の対応

- ・ 不正アクセスの経路を遮断し、脆弱性への対策を実施しております。
- ・ skyticket にクレジットカード情報を保存されている会員様のアカウントに不正ログインされ、保存済みのクレジットカードを使って skyticket 上で不正に購入されることを防ぐため、2026 年 10 月 7 日 18 時ごろをもって、保存済みクレジットカードによるお支払いと、カード情報の保存機能を停止いたしました。
- ・ 対象のお客様には、電子メールで順次ご連絡しております。ご連絡が届かないお客様については、本お知らせをもってご案内に代えさせていただきます。
- ・ 個人情報保護委員会に報告しております。

4. お客様へのお願い

- ・ skyticket の会員様は、パスワードの変更をお願いいたします。他のサービスで同じパスワードをお使いの場合は、そちらも変更してください。
- ・ マイページの予約履歴と、クレジットカードのご利用明細をご確認ください。身に覚えのないご予約があった場合は、下記の窓口までご連絡ください。
- ・ 当社や金融機関などを装った不審なメール・SMS・電話・郵便物にご注意ください。当社から、パスワード、クレジットカード番号、口座の暗証番号などをお尋ねすることはございません。
- ・ 当社からお送りするご連絡メールに、パスワードの入力を求めるリンクは記載しておりません。パスワードの変更は、公式サイトまたは公式アプリから直接お手続きください。

5. お問い合わせ窓口

skyticket 個人情報流出に関するお問い合わせ窓口

- ・ メール：info@skyticket.com

6. 今後について

引き続き調査を進め、新たな事実が判明した場合は速やかにお知らせいたします。

お客様の大切な情報をお預かりする立場にありながら、このような事態を招きましたことを、重ねて深くお詫び申し上げます。全社を挙げて再発防止と情報管理体制の強化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業績に与える影響について現在精査中であり、今後、開示すべき事項が判明した場合には、速やかに開示いたします。

以上