2026 年 10 月 23 日

各　位

会 社 名　パーク２４株式会社
代表者名　代表取締役社長 CEO　西川 光一
（コード：4666、東証プライム市場）
問合せ先　取締役常務執行役員 CFO　實貴 孝夫
（TEL：03-6747-8120）

不正アクセスに関する調査結果および今後の対応に関するお知らせ

2026 年９月 28 日に公表いたしました「連結子会社における不正アクセスの発生および個人情報漏えいに関するお知らせ」のとおり、当社の連結子会社であるタイムズモビリティ株式会社（以下、タイムズモビリティ）が運営するカーシェアリングサービス「タイムズカー」の Web システムにおいて、第三者による不正アクセスが確認され、当社グループの保有する個人情報が外部に漏えいしたこと（以下、本事案）が判明いたしました。

本事案に対して、外部専門機関によるフォレンジック調査を進めておりましたが、この度、フォレンジック調査が完了し報告書を受領いたしました。フォレンジック調査によって判明した事実や影響範囲、発生原因等に関するご報告とともに、今後の対応等についても本日決定いたしましたので、以下のとおりお知らせいたします。

お客様、お取引先様をはじめ、関係者の皆様に多大なるご迷惑とご心配をおかけしておりますことを、心より深くお詫び申し上げます。

記

１．本事案発生から現在までの経緯

当社は、2026 年９月 25 日、タイムズカーの Web システムにおいて異常なアクセスを検知し、直ちに調査および封じ込め対応を開始いたしました。

不正アクセスの可能性を確認した後、影響を受けたシステムの隔離、アクセス経路の遮断、ログ分析および外部専門機関によるフォレンジック調査を実施するとともに、個人情報保護委員会への報告、対象となるお客様への通知および公表を順次実施してまいりました。

また、お客様からのお問い合わせに対応するための専用窓口を設置し、被害防止策や対応方針の検討を進めるとともに、実害の有無に関する継続的な確認を実施しております。

主な経緯は以下のとおりです。

日付	主な対応
2026/9/25　（金）	第三者による不正アクセスを検知し、直ちに調査を開始
	対象サーバーを隔離
	不正アクセス経路を遮断
	外部専門機関によるフォレンジック調査を開始
	問い合わせ窓口を開設
	個人情報保護委員会へ報告
	個人情報漏えいの可能性があるとして、HP にて第１報を公表
2026/9/26　（土）	侵害を受けた環境および関連環境の切り離し完了
	第１報に情報を追記
2026/9/28　（月）	既存会員の方へのご案内を開始
	「連結子会社における不正アクセスの発生および個人情報漏えいに関するお知らせ」適時開示
	HP にて第２報を公表

	警察への相談を開始
	国土交通省へ一報
2026/9/29 （火）	HP にて第３報を公表
	個人会員の方へのご案内を開始
2026/10/1 （木）	退会された方へのご案内を開始
2026/10/2 （金）	法人会員の方へのご案内を開始
2026/10/16（金）	HP にて第４報を公表
2026/10/23（金）	外部専門機関によるフォレンジック調査を終了
	調査結果および対応方針を公表

２．調査結果

外部専門機関によるフォレンジック調査を進めた結果、以下のことが判明いたしました。

(1) 発生原因

本事案は Web システムに存在した脆弱性が悪用されたことにより発生したものと判断しております。攻撃者は当該脆弱性を悪用してシステムへ侵入した後、システム内の情報を探索し、取得した情報を利用してデータベースおよびファイル領域へアクセスしていたことを確認しております。

なお、攻撃手法の詳細やシステム構成等については、二次被害防止の観点から公表を差し控えます。

(2) 漏えいまたは漏えいのおそれが確認された情報および影響範囲

本事案に関連してタイムズクラブ Web システムへの不正アクセスが確認されました。

また、当社はこれまで、本人確認書類画像データ約 160 万件について漏えいのおそれがあるとお知らせしておりました。その後の詳細調査の結果、外部送信の痕跡が確認された本人確認書類画像データは約 146 万件であることが判明しました。なお、外部送信の痕跡は確認されなかったものの、攻撃者によるアクセスの痕跡が確認された暗号化データが存在することも判明しております。

現時点で確認されている対象件数および対象情報は以下のとおりです。

【タイムズカーWeb システムからの漏えい状況】

①	攻撃者により、右記のデータにアクセスされ、外部送信された痕跡が確認されたもの	・氏名※1 ・住所 ・生年月日 ・電話番号※1 ・メールアドレス※1 ・運転免許情報	6,628,007 件

※１ タイムズビジネスサービスに「カンタン入会」を通じて入会された方のご契約情報をタイムズカーWeb システムで管理しているため、駐車場のみ（クレジットカード払い）をご契約されているお客様の情報が含まれております。

＜①に該当するアカウントの「属性・識別情報」の漏えい状況＞

②	攻撃者により、「属性・識別情報」データにアクセスされ､外部送信された痕跡が確認されたもの	法人会員様の所属部署名	3,677 件
		タイムズカー会員番号（IC 管理番号）	8 件

		タイムズビジネスカード番号	113 件
		連携サービス ID※2	4 件

※２ 2026 年 9 月 28 日公表の「連結子会社における不正アクセスの発生および個人情報漏えいに関するお知らせ」において、連携サービス ID の漏えいは 9 件としておりましたが、調査の結果 4 件であることが判明いたしました。なお、「連結子会社における不正アクセスの発生および個人情報漏えいに関するお知らせ」にて漏えい対象としておりました「JR 西日本グループの会員サービス WESTER ID」は 0 件でした。

＜①に該当するアカウントの「認証情報」の漏えい状況＞

③	攻撃者により、ハッシュ化された「認証情報」データにアクセスされ、外部送信された痕跡が確認されたもの	パスワード	4 件

＜①に該当するアカウントの「本人確認書類の画像」の漏えい状況＞

④	攻撃者により、暗号化された「本人確認書類の画像」データにアクセスされ、外部送信された痕跡が確認されたもの※3	1,464,800 件
⑤	攻撃者により、暗号化された「本人確認書類の画像」データにアクセスされたものの、外部送信された痕跡が確認されなかったもの	891,602 件
	計	2,356,402 件

※３ 本人確認書類画像データは暗号化した状態で保管していたため、攻撃者によるアクセスや外部送信を示す痕跡が確認された場合であっても、直ちに画像内容が閲覧可能な状態になったことを意味するものではありません。一方で、外部送信された暗号化データについては、将来的な復号の可能性を完全に否定できるものではありません。

【タイムズクラブ Web システムからの漏えい状況】

⑥	攻撃者により､右記のデータにアクセスされ、 外部送信された痕跡が確認されたもの	・氏名 ・住所 ・生年月日 ・運転免許情報	5 件
		タイムズクラブカード番号	19,510 件
		タイムズビジネスカード番号	12 件
		連携サービス ID※4	135,436 件
		クレジットカード番号の下 4 桁※5	28 件

※４ タイムズクラブで提供している他社提携サービスと連携するための識別番号です。
※５ 当社は決済情報の非保持化に対応しており、クレジットカード番号全桁およびセキュリティコードは一切保持していないため、不正に利用されるおそれはございません。

その他、会員管理およびシステム運用のための識別情報についても、攻撃者によりアクセスされ、外部送信された痕跡がありました。

なお、外部専門機関による調査の結果に基づく最終件数については上記のとおりであり、現時点で追加の対象範囲は確認されておりません。

(3) お客様への影響および想定されるリスク

当社は、外部専門機関の協力のもと、漏えいした情報の内容、外部送信の状況および二次被害の有無について調査を継続しております。

現時点において、当社が把握している範囲では、本事案で漏えいした情報が売買・公開されたことを示す事実は確認されておりません。しかしながら、漏えいした情報には氏名や住所等の個人情報に加え、本人確認情報が含まれていることからも、以下のようなリスクが想定されます。

- フィッシングメールやフィッシングサイトによる詐欺
- なりすましによる各種申込みや問い合わせ
- 不正勧誘
- 個人情報の悪用

当社は引き続き、外部専門機関と連携してダークウェブを含む情報流通状況の監視を継続するとともに、実害発生状況の確認を行ってまいります。

なお、当社は決済情報の非保持化に対応しており、クレジットカード番号全桁およびセキュリティコードは一切保持していないため、不正に利用されるおそれはございません。

３．今後の対応等

(1) お客様への対応

当社は、お客様の被害防止および不安軽減を最優先に考え、以下の対応を実施しております。

A) 対象となるお客様へのご案内

影響を受けたお客様に対し、個別通知を実施しております。

B) 専用お問い合わせ窓口の設置

本事案に関する専用窓口を設置し、お客様からのお問い合わせやご相談を受け付けております。

C) お見舞金のお支払い

当社は、本事案により暗号化された運転免許証等の本人確認書類画像データへのアクセスおよび外部送信を示す痕跡が確認されたお客様に対し、多大なるご心配とご負担をお掛けしていることを重く受け止め、お見舞いとして 3,000 円相当の現金または金券をお渡しすることといたしました。

当該画像データは暗号化した状態で保管していたため、外部への送信を示す痕跡が確認された場合であっても、直ちに画像内容が閲覧可能な状態となったことを意味するものではありません。しかしながら、外部送信された暗号化データについては将来的な復号の可能性を完全に否定できるものではないこと、お客様への影響およびご負担を踏まえ、暗号化された運転免許証等の本人確認書類画像データへのアクセスおよび外部送信を示す痕跡が確認されたお客様を対象とさせていただきました。

なお、お見舞いの内容およびお渡し方法については現在検討中であり、決定次第、対象となるお客様へご案内いたします。

D) 継続的な対応

今後、新たな事実が判明した場合には、対象となるお客様への追加のご案内を行うとともに、必要な対応策を検討いたします。

(2) 本人確認書類の画像保有について

A) タイムズカーにおける本人確認書類の画像保有ルールの見直し

当社は、タイムズカーへの会員ご登録時にお客様からご提出いただいた運転免許証等の本人確認書類の画像を、暗号化した状態で会員期間中および退会後 7 年間保有しておりました。会員ご登録時のご本人確認手続きの実施に加え、不正利用が疑われる事案への対応、お問い合わせ対応および各種ご本人確認業務に利用することを目的として保有しておりました。

また、本人確認書類の画像は社内ルールに基づき保管・管理しており、保有期間についても当社が定めた基準に則って運用しておりました。

本事案を受け、本人確認書類の画像保有に伴うリスクおよび管理のあり方を総合的に勘案した結果、運用方法等の変更を行い、会員登録完了後は画像を保有しない社内ルールに変更いたしました。

	現行	変更後
現　会　員	会員期間中は保有	登録確認完了後、即時削除
退 会 会 員	退会後７年間保有	―

B) 本人確認書類の画像削除について

従来、本人確認書類の画像につきましては、社内ルールで保有不要となったものを削除する他、ご本人様からのご請求に基づき削除しておりました。

このたびの社内ルール見直しに伴い、現在当社が保有している本人確認書類の画像データにつきましては、ご本人様からのお申し出の有無にかかわらず、2026 年 10 月末までに削除いたします。

なお、画像データは削除いたしますが、将来お客様からのお問い合わせ対応等のために必要となった際に、当社において保存していた画像との同一性を確認するための情報は、適切に保全しております。

(3) 現時点での対応状況

本事案については、侵入経路、攻撃者行動および影響範囲の調査を実施するとともに、確認された侵害経路に対する対策を完了しております。

また、同一構成システムへの点検および脆弱性対策を実施し、監視・検知強化の追加対策を実施しております。

現時点において、確認された侵害経路に対する必要な対応は完了しておりますが、当社は引き続きセキュリティ対策および監視体制の高度化を進めてまいります。

(4) 今後の対応

当社は、本事案を重大な経営課題として受け止め、再発防止および信頼回復に向けた取り組みを進めてまいります。

情報セキュリティに関する外部専門家の助言も踏まえながら、情報セキュリティ強化策を策定し、順次実施してまいります。

あわせて、当社社外取締役を中心とし、外部専門家を加えた調査委員会にて、本事案にかかる当社グループの内部統制およびガバナンスの観点からの検証を行います。

具体的な情報セキュリティ強化策およびガバナンス強化策については、年内を目処に公表いたします。

４．業績への影響

本事案への諸対応費用等を踏まえ、2026 年 10 月期通期連結業績予想を修正することといたしました。詳細は本日公表の「特別損失の計上および通期連結業績予想の修正に関するお知らせ」をご覧ください。

５．本事案の対象となる方のお問い合わせ窓口

■フリーダイヤル：0120-25-8924（24 時間）　※おかけ間違いにご注意ください

■お問い合わせフォーム：https://share.timescar.jp/inquiry.html

以　上