タイムズモビリティ株式会社

2026年10月1日
最終更新日：2026年10月6日

タイムズカーWeb サイトへの不正アクセスに関する ご質問と回答

Q1 どのような個人情報が漏えいしているのか？

A. 以下の情報の漏えいを確認しています。

・氏名
・法人会員様の所属部署名
・住所
・生年月日
・電話番号
・メールアドレス
・運転免許情報
・本人確認書類情報 ※1
・パスワード ※2
・連携サービス ID

※1 運転免許証画像、現住所確認書類画像、学生証画像（学生プランの場合）、家族確認書類画像（家族プランの場合）
※2 パスワードは復元できない形式で保管しており、当該情報を用いてお客様アカウントが不正に利用される恐れはありません。

Q2 クレジットカード情報は漏えいしていないか？

A. 当社ではクレジットカード情報を保有していないため、今回の漏えい対象には含まれておりません。

Q3 自分の個人情報が漏えいの対象になっているか？

A. 漏えいが確認されたお客様には、個別にお知らせいたします。
運転免許証画像等の本人確認書類情報の漏えいが確認されたお客様には、9月29日より順次メールにて個別にご案内を開始しております。

Q4 届いたメールに記載のない個人情報は漏えいしていないということか？

A. メールには、現時点で漏えいを確認した情報を記載しております。

© TIMES MOBILITY CO., LTD.

Q5 退会済みだが個別通知が来るか？

A. 退会済みのお客様にも、10月1日より順次個別にご案内を開始しております。なお、退会済みのお客様については、ご登録いただいている連絡先情報が現在も有効とは限らないことから、慎重に対応を進めております。
大変お手数ですが、現在のご連絡先を確認するため、ご退会時のご登録情報をお問い合わせフォームよりご連絡※お願いいたします。

※お問い合わせフォームより、タイトル『退会済み会員様の個人情報漏えいについて』を選択の上、「ご意見・お問い合わせ内容」欄に表示された項目について、ご記入ください。
ご記入いただいてから、2週間程度を目処に順次ご案内いたします。

Q6 漏えいに伴う補償はあるか？

A. 現在実施しております外部専門機関による調査の結果を踏まえて、全体方針を決定する予定です。
新たにご連絡できる事項が発生した際は、速やかに対象となる関係者の皆様へご連絡するとともに、当社Webサイト等を通じてお知らせいたします。

Q7 今すぐ行う必要がある手続きや対策はあるか？

A. 不審なメール、SMS、電話、郵便物等には十分ご注意いただき、心当たりのない連絡には応答せず、記載されたリンクや添付ファイルを開かないようお願いいたします。

Q8 退会後も個人情報を保管しているのはなぜか？

A. 氏名、住所、生年月日については、税法等に基づき 7 年間保管しています。
運転免許情報および画像については、なりすまし対策やお問い合わせ対応のため、7 年間保管しています。

Q9 運転免許証画像に関する本人確認制度について

A. 運転免許証画像が流出した場合の本人確認制度や第三者による不正利用の可能性について、多くのお問い合わせをいただいております。
金融機関、クレジットカード会社等では、法令や業界ルールに基づき本人確認が行われています。
本人確認書類の画像情報を用いた非対面での本人確認においては、本人確認書類の画像だけでなく、本人の容貌画像との照合、本人名義口座による確認といった、追加の確認手続が用いられます。
ただし、第三者による不正な申込みの試みや、上記以外の契約に関する「なりすまし」、その他の情報・手段を組み合わせた不正行為等の可能性を完全に否定するものではありません。
当社は、本件に関する対応を継続しております。今後、お客様にお知らせすべき事項が確認された場合には、速やかにご案内いたします。

（2026年10月6日追加）

© TIMES MOBILITY CO., LTD.

Q10（お客様ご自身で）注意すべきことはあるか？

A. 本件に関連して、当社や金融機関、携帯電話会社、公的機関等を名乗り、SMS認証コード、ID・パスワード、口座情報、クレジットカード情報、各種暗証番号等を聞き出そうとする連絡には十分ご注意ください。
当社から、お客様に対してお電話やメール等でSMS認証コード、インターネットサービスのパスワード、運転免許証やマイナンバーカードの暗証番号等をお聞きすることはありません。
不審な連絡を受けた場合には、その場で情報を伝えず、各事業者の公式窓口へご確認ください。
本事案については、警察庁に相談しております。本件のような事案に関連して注意が必要な特殊詐欺対策として、警察になりすまして電話をしてくる「ニセ警察詐欺」への注意喚起とともに、
特殊詐欺の被害防止対策として有効な無料のアプリをご紹介いただきました。
このアプリは、犯行に利用されることの多い国際電話番号や犯行に利用された電話番号などの発着信をブロック・警告する機能※があります。スマートフォンをご利用のお客様は、必要に応じてご活用をご検討ください。
[アプリ] 詐欺対策 by NTTタウンページ（NTTタウンページ株式会社）
[アプリ] 詐欺バスター Lite（トレンドマイクロ株式会社）
[Webサイト] 警察庁・SOS47 特殊詐欺対策特設ページ
※AndroidとiPhoneで機能が異なります。詳細は警察庁・SOS47 特殊詐欺対策特設ページをご確認ください

＜参考法令・公表資料＞

記載の内容は、2026 年 10 月 5 日現在、関係法令および行政機関の公表資料を確認のうえ作成しています。法令改正、行政解釈の変更、本人確認制度の見直し等により、今後内容が変更される場合があります。

法令

・犯罪による収益の移転防止に関する法律（平成 19 年法律第 22 号）
金融機関等に対し、取引時の本人確認等を義務付ける法律
・犯罪による収益の移転防止に関する法律施行規則（平成 20 年内閣府、総務省、法務省、財務省、厚生労働省、農林水産省、経済産業省、国土交通省令第 1 号）
具体的な本人確認の方法等を定める規則

行政機関公表資料

・金融庁「犯罪収益移転防止法におけるオンラインで完結可能な本人確認方法に関する金融機関向けQ&A」
・金融庁「犯罪収益移転防止法におけるオンラインで完結可能な本人確認方法の概要」
上記Q&Aページ内の参考資料として公表

※本記載は、お客様から多く寄せられているご質問に対し、現時点の法令および公表資料に基づく一般的な制度の内容をご説明するものです。個別の事案や将来発生し得るあらゆる可能性について保証または否定するものではありません。制度や各事業者の運用によって取り扱いが異なる場合があります。

（2026年10月6日追加）

© TIMES MOBILITY CO., LTD.