

2018年4月9日

お客様各位

ポルシェ ジャパン株式会社
東京都港区虎ノ門一丁目23番1号
代表取締役社長 七五三木 敏幸

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調査結果の最終報告

2018年2月26日、弊社がお客様の個人情報の管理を委託している委託先（以下、当該委託先といいます）のサーバーに対し、第三者が不正なアクセスを行い、弊社がお預かりしているお客様の情報の一部が第三者に流出していたことを、初動調査に基づき公表いたしました。

弊社は、上記初動調査に引き続き、不正アクセスにより流出したお客様の情報の範囲を特定し、また再発を防止するために、データフォレンジック（※1）を専門とする外部機関を起用しての追加調査を行いました。

今般、上記の外部機関による調査が完了しましたので、当該追加調査の結果を踏まえて、今回の不正アクセスにより流出したお客様の情報の範囲、及び再発防止策について下記の通りご報告申し上げます。

お客様及び関係者の皆様に多大なるご心配とご迷惑をおかけしましたことを、改めて深くお詫び申し上げます。

※1 ここでは、電子機器に保存された電子データを分析・解析することにより証拠化を図る調査手法のことを指します。

記

1. 外部機関による調査

弊社は、データフォレンジックを専門とする外部機関に以下の事項の調査業務を委託し、2018年3月30日に調査結果を受領しました。

- 1) 不正アクセスにより流出したお客様情報の範囲を特定するための調査

- a) 調査対象機器：当該委託先において弊社のお客様の情報を保存していた各種サーバー（過去に交換されたものを含めて現存するもの全て）
 - b) 調査手続き：アクセスログ分析、脆弱性診断、その他のコンピュータフォレンジック
- 2) 不正アクセス判明後に当該委託先が実施した不正アクセス対策の妥当性及び網羅性の検証
- a) 調査対象機器：当該委託先において弊社のお客様の情報を保存する（現行の）サーバー
 - b) 調査手続き：当該委託先によるウェブアプリケーションを不正アクセス対策のために修正した作業の妥当性及び網羅性の確認

2. 流出したお客様情報の範囲

上記の外部機関による追加調査の結果、2018年2月26日に公表した際の初動調査によっては弊社にて確認できなかったお客様情報の流出が今回新たに確認されましたので、以下の通り、流出したお客様情報の範囲を修正いたします。今回修正した箇所は、下線で示しています。なお、今回新たに流出が確認されたお客様には個別にお知らせしております。

なお、今回新たに確認された流出情報も含めて、流出した情報又は流出した可能性のある情報には、クレジットカードに関する情報、信用情報、ポルシェの製品又はサービスに関するお取引履歴は含まれていません。

	該当するデータベース	流出した情報	流出した可能性のある他の情報 ※2	件数
1	2000年から2009年の間に、弊社WEBサイトを通じてカタログ請求をされたお客様のデータベース	電子メールアドレス、 <u>カタログ請求の際に設定をされたパスワード</u> ※3	カタログ請求の際にお申し出いただいた氏名、郵便番号、住所、電話番号、性別、生年月日、職業、年収、車の所有、台数、メーカー、車種、年式、トランスミッション、ポルシェ車購入予定の有無、購入予定時期、希望カタログ車種、販売店名称	23,151件

2	2015年7月に弊社が実施したEmail アドレスキャンペーンへご応募いただいたお客様のデータベース	電子メールアドレス	氏名	5,568件
3	2012年から2016年の間に、弊社WEBサイトを通じてポルシェスポーツドライビングスクール(PSDS)の資料請求をされたお客様、及び2017年4月から2018年1月の間に、弊社WEBサイトを通じてPSDSのメールマガジンに登録されたお客様のデータベース	電子メールアドレス、資料請求の際に設定をされたパスワードをハッシュ化したもの ※4		最大2,855件
合計 ※5				最大31,574件

※2 これらの情報は、流出した情報と同じデータベースに保存されていたことから、流出の可能性を完全に排除するには至りませんでした。もっとも、外部機関による今般の追加調査では、流出した痕跡までは検出されませんでした。

※3 本パスワードは、当時、カタログ請求されたお客様限定で公開されていたスペシャルコンテンツのページへのログインに用いられたものです。

※4 本パスワードは、任意で設定することにより、次回以降に資料請求をする際に、お名前やご住所の入力を省くために用いられたものです。ハッシュ化とは、入力した文字列をハッシュ関数という演算手法により固定長の文字列に不可逆的に変換することをいいます。

※5 前回公表時に調査中であった3件のメールアドレスは、テスト用のものであり、お客様からお預かりしたメールアドレスではないことが確認されました。

3. 再発防止策等

1) 不正アクセスへの対応

今回の不正アクセスにおいて確認された外部からの攻撃への耐性を備えるよう、当該委託先は、ウェブアプリケーションの修正を実施しました。そして、今回の外部機関による調査の結果、上記ウェブアプリケーションの修正により、当該攻撃への対策として独立行政法人情報処理推進機構が推奨する対策が実施されていることが確認されました。

不正アクセスを行った第三者は、不正アクセスのログをもとに調査をしておりますが、特定には至っておりません。引き続き警察と連携して対応いたします。

2) 再発防止への取組み

不正アクセスが判明して以降、当該委託先のサーバーを用いて弊社が運営しているウェブサイトにおいては、お客様情報を新たにお預かりすることを中止しているほか、これまでお預かりしているお客様情報は外部から物理的に遮断されたところに保存しております。こちらについては、今後、システムの再構築、及び不正アクセス攻撃への耐性に関する第三者によるセキュリティ診断の実施など、安全性を担保するために必要な措置を行ったうえで再開する予定です。

弊社は、お客様情報の取扱いに細心の注意を払ってまいりましたが、このたびの事態を防げなかったことを重く受け止め、深く反省するとともに、以下の取組みを含む、個人情報管理強化・徹底を図り、お客様からの信頼の回復に全力を尽くして参ります。

- 1) システム開発におけるセキュリティに関する審査手続きの厳格化
- 2) お客様情報を取り扱う新規又は既存のシステムに対する第三者によるセキュリティ診断の実施
- 3) お客様情報を取り扱う委託先のセキュリティ対策に対する監査

4. 本件に関するお問い合わせ

お客様からの本件についてのご不明点やご質問は、下記の専用フリーダイヤルにて承ります。

お客様情報に関する専用窓口 0120-950-290 (月～金 9:00-18:00)