News Release
2020年7月22日
ジュピターショップチャンネル株式会社

リスト型攻撃による通販サイトへの不正ログイン発生について

ジュピターショップチャンネル株式会社（以下「当社」）は、当社が運営する通販サイトにおいて、当社以外の外部で不正に取得されたと思われる情報を使った不正なログインが発生し、お客様の情報が第三者に閲覧された可能性があること（以下「本件」）を確認しました。
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しましたことを、深くお詫び申し上げます。現時点で確認している事実と当社の対応は次のとおりです。

1. 経緯

2020年7月15日（水）、当社が定常的に行っているモニタリングで、海外から不正なログインが試行されていることを探知したため、直ちに海外からのアクセスを遮断し、これ以上の不正なログインを防ぐとともに、調査を実施いたしました。
調査の結果、不正ログインに使われたお客様の個人情報が当社内から流出した証跡はなく、今回の不正ログインは第三者が外部で不正に取得した情報を利用した「リスト型アカウントハッキング（リスト型攻撃）※1」の手法で行われたものと推測されます。

※1「リスト型アカウントハッキング（リスト型攻撃）」は、何らかの手段により他者のID・パスワードを入手した第三者が、これらのID・パスワードをリストのように用いて様々なサイトにログインを試みることで、個人情報の閲覧等を行うサイバー攻撃

2. 対象となるサイト

当社が運営する「ショップチャンネル」の通販サイト（https://www.shopch.jp）

3. 不正ログインの状況

(1) 不正ログインが確認された件数：
264件

(2) 不正ログインにより第三者に個人情報が閲覧された可能性のある件数：
22件

(3)　第三者に閲覧された可能性のあるお客様の個人情報：

・氏名（姓名・フリガナ）
・郵便番号
・住所
・電話番号
・メールアドレス
・生年月日
・クレジットカード情報（カード番号の下 4 桁・有効期限）※2
・ご本人以外へのお届け先として登録されている情報（氏名・郵便番号・住所）

なお、現在までに情報の不正利用等の二次被害に関するご報告はありません。

※2 カード番号の下 4 桁以外とセキュリティコードはマスキングされているため閲覧された可能性はありません。

4.　現在までの対応

本件発覚後、当社は現時点までに以下の対応を行っております。

(1)　不正にログインされたお客様のパスワードを 7 月 16 日（木）に初期化いたしました。対象のお客様にはメールとお電話で個別にご連絡し、他社サービスとは異なるパスワードを推奨した上で、パスワードの再設定をお願いしております。

(2)　不正ログインの試行を行った通信元からのアクセスを遮断するとともに、その他のアクセスについても監視強化を行っています。

5.　今後の対応

当社では、お客様の個人情報保護は最優先事項と認識しており、今回の事態を厳粛に受け止め、再発防止に向けて不正ログインの監視強化やセキュリティレベルの向上に努めてまいります。

以上

【報道関係者からのお問い合わせ先】
マーケティング部　広報担当　佐藤、上田
TEL：03-6667-2316