

訪問販売代理店でのお客さま情報の不正取得について

2015年から2018年までの期間、主に訪問販売代理店などにおいて、当社の携帯電話サービスなどの契約手続きを行ったお客さまの情報6,347件が、不正に取得されたことが判明しましたので、お知らせします。

これは、複数の携帯電話会社のブランドを扱う併売店において、訪問販売やブース販売などの形で当社の代理店業務を行っていた人物が、当社のルールを遵守せず、不正な方法でお客さまの情報を取得していたものです。当該人物は、すでに別件に関する電子計算機使用詐欺などの容疑で警視庁に逮捕されており、取り調べを受けています。当社は捜査当局からの捜査協力依頼により本件を知得し、これまで捜査に全面的に協力してきました。なお社内調査の結果、当社の顧客データベースからはお客さま情報が一切流出していないことを確認しています。

このたびは、お客さまに多大なご不安およびご迷惑をおかけしましたことを深くお詫び申し上げます。本件を厳粛に受け止め、当社の代理店に対する管理・監督責任を再度徹底するとともに、全社を挙げて再発防止を図ってまいります。

1. 経緯

捜査当局によると、当該人物は、2015年から2018年までの期間、当社のお客さまの契約手続きを行う際に、当社の顧客システム以外に情報を登録・記録してはならないというルールを遵守せず、「お客さま控え」を写真撮影やコピーをすることで情報を不正に取得していました。当社は従来、このような行為を一切禁じており、代理店の研修でも禁止行為として指導しています。

2. 不正取得された情報

以下は、捜査当局からの情報を当社で精査して判明した内容です。

- ・件数：6,347件
- ・内容：氏名、住所、生年月日、連絡先電話番号、携帯電話番号、携帯電話機の製造番号（IMEI）、交換機暗証番号※、料金支払い用の金融機関名および口座番号
- ・対象：2015年から2018年の期間、当該人物が関わった訪問販売代理店などで、「ソフトバンク」「ワイモバイル」の携帯電話サービス、SoftBank 光、SoftBank Air の契約手続きを行ったお客さまの一部

※ 交換機暗証番号とは、一般電話から留守番・転送電話の再生・消去などを行う場合や、一部の設定変更の際に入力する4桁の番号です。設定変更後、SMSで契約者ご本人の携帯電話に通知が届くため、万が一第三者による変更が行われても検知が可能です。また、携帯端末の暗証番号とは異なります。

捜査当局からは、上記のうち一部のお客さまにおいて、金融口座からの不正引き出し被害に遭われた事案が62件発生し、金融機関による補填が行われたと伺っています。なお、当社は金融機関の口座暗証番号は取得しておらず、今回、当該人物による不正取得も確認されていないと捜査当局から伺っています。改めて、多大なご不安とご迷惑をおかけしたことを深くお詫び申し上げます。

3. 対象となるお客さまへの対応

情報不正取得の対象となったお客さまについては、書面で個別にご連絡を行ってまいります。なお、交換機暗証番号についてはすでにリセットを完了しています。

4. 再発防止策

再発防止策として、販売代理店の管理体制の見直しを下記の通り行っています。

- ・販売代理店における業務の定期的な監査
- ・販売代理店における個人情報に関わる事故・不正行為への厳罰化
- ・販売代理店における個人情報取り扱いに関する教育の再徹底

以上

- SoftBank およびソフトバンクの名称、ロゴは、日本国およびその他の国におけるソフトバンクグループ株式会社の登録商標または商標です。
- その他、このプレスリリースに記載されている会社名および製品・サービス名は、各社の登録商標または商標です。