2021 年 2 月 12 日

お客さま各位

SMBC コンシューマーファイナンス株式会社

弊社インターネット会員サービスでの不正ログインについて

このたび、弊社会員向けインターネット会員サービスにおきまして、第三者による不正ログインが判明いたしました。そのうち一部のお客さまについては、プロミスアプリを利用したスマホATMにより不正出金されたことが確認されております。不正ログインのありましたお客さまをはじめとする皆さまには、ご迷惑とご心配をお掛けしましたことを深くお詫び申し上げます。
なお、お客さまに安心・安全にスマホATMをご利用いただくため、現在スマホATMの利用（出金に限る）を停止しております。今後、より一層のセキュリティ強化と安全性の確保に努めてまいります。

1. 経緯

2020 年 11 月、弊社を騙った不審なSMSが配信されて、弊社の会員専用サービスへのログインページに酷似したフィッシングサイトに誘導する事態が発生、ログインするためのお客さま情報（IDやパスワードなど）が不正に取得されて、ログインをされた可能性があることを確認しました。
また、弊社会員向けインターネット会員サービスへ海外からの大量のアクセスがあり、調査した結果、2020 年 11 月 24 日から 12 月 3 日にかけて、当該アクセスにより不正ログインをされた可能性があることを確認しました。調査を進める中で、不正ログインに使用されたID・パスワードは弊社に登録されていないものが多数含まれており、「リスト型攻撃（※1）」による不正ログインと判明しております。
なお、使用されたID・パスワードが弊社から流出した証跡はございません。

※1 「リスト型攻撃」：悪意のある第三者が、他社サービスなどから不正に入手した可能性のあるID・パスワードを使用し、不正アクセスを試みる手法

2. 不正ログインの状況（2021 年 2 月 10 日現在）

（1）不正にログインされた可能性のある顧客数

826顧客（不正ログイン試行総数は約240万件）
なお、一部のお客さまが正常にログインされたものも含まれている可能性があります。
不正ログインされた可能性のあるお客さまに対して、ID・パスワードの無効化を行うとともに、電子メール等にて個別にご連絡しID・パスワードの変更をお願いしております。
また、リスト型攻撃に対する措置として、不正ログインと関連するアクセスを遮断し、現在定常的にモニタリングを実施し検視する対策を講じております。

（2）閲覧された可能性のある項目

お客さまの氏名、会員番号、自宅住所、自宅電話番号、勤務先名、勤務先住所、勤務先電話番号、携帯電話番号、Eメールアドレス、振込先金融機関口座、取引履歴情報、お借入残高、支払情報（支払期日、請求金額）

3. スマホATMによる不正出金の被害対応

リスト型攻撃またはフィッシングにより不正ログインされただけでは、プロミスアプリを利用したスマホATMにより不正出金することはできませんが、さらにスマホATMのご利用時に必要な「SMS認証コード」が第三者により不正に取得（※2）された結果、不正出金された可能性のあるお客さまを特定しております。

不正出金の被害に遭われたお客さまに対しては、個別に弊社から連絡をさせていただき、被害額を補償する手続きを進めております。

※2 ①お客さまにフィッシングサイトにて「SMS認証コード」を入力させる手口、または
②悪意のある第三者が当社社員を装いお客さまへ電話かけるなどしてお客さまから「SMS認証コード」を聴き出す手口

4. 公的機関への報告・相談

本事案につきましては、監督官庁に報告し、所轄の警察署へ報告及び相談をしております。

お客さまの安全なご利用のために、再度のお願い（2020年12月28日お知らせ）となりますが、他社のサービスで使用しているID・パスワードを流用していらっしゃる場合には、速やかに変更していただくようお願い申し上げます。

また、プロミスではSMSやEメール、電話などにより「ID・パスワード」、「SMS認証コード」をお問合わせすることは一切ございませんので、ご注意いただきますと共に、「身に覚えのない取引（出金・入金・各種手続き等）」がございましたら、プロミスコールまでご連絡いただきますようお願いいたします。プロミスでは、ご相談内容に応じて事実確認など丁寧に実施し、真摯に対応してまいります。

5. お客さまお問合わせ先

受付時間：平日9:00～18:00

プロミスコール 0120-24-0365

以上