インターネット取引サービスにおける
不正取引等防止に関するガイドライン

令和 3 年 10 月 29 日

日本貸金業協会
Japan Financial Services Association

１．制定の目的

本ガイドラインは、貸金業において各社の Web サイト及びスマートフォンのアプリケーション等を通じたインターネット取引サービス（以下、「インターネット取引サービス」という。）を提供するにあたり、安全性及び信頼性を確保することにより、資金需要者等の利益の保護を図り、貸金業の適正な運営に資することを目的とする。

（１）不正取引等事案の発生

昨今、貸金業界において新たなサービスの提供や顧客利便性が向上する一方、各種システムへのサイバー攻撃が複雑化・巧妙化しており、メールや SNS、フィッシングサイト等を用いたサイバー攻撃が国内外問わず多数発生している状況にある。

その様な中、先般、悪意のある第三者が顧客情報を何らかの不正な手段で入手し、当該顧客になりすまして提携先のコンビニエンスストア内の ATM から借入金を出金するといった事案が発生した。

これは、カードローン・キャッシング用カードを用いることなく、スマートフォンのアプリを利用することで ATM から出金できるサービス（スマホ ATM）において、認証の脆弱性を突かれたものである。

（２）経緯

同様の事案が発生した場合、これまで長年かけて築いてきた業界全体に対する信用を失うリスクも考えられる。当協会では、利用者が安心してインターネット取引サービスを利用できるよう、協会員がインターネット取引サービスのシステムを構築及び運用するに当たっての留意事項等をガイドラインとして取りまとめることとした。

（３） 運用方針

本ガイドラインは、インターネット取引サービスにおける不正取引等を防止するために留意すべき基本的な事項を整理した具体例等であり、適用範囲は、インターネット取引サービスを提供及び提供しようとしている協会員とする。

協会員におかれては、インターネット取引サービスにおける本ガイドラインの趣旨を十分に踏まえ、各社の実情に応じてリスクベースで検討する等、実効性のある不正取引等防止対策を実施願いたい。

なお、本ガイドラインは適時、適切に見直しを行うものとする。

２．不正取引等の未然防止

協会員は、インターネット取引サービスを提供する場合並びにその内容及び方法を変更する場合は、サービス連携先を含む全体のリスクを評価した上で、不正取引等の未然防止策を講じる必要がある。

具体的な内容としては、申込み時の対応、サービス提供時の対応、システムのセキュリティ対応、顧客情報等の管理、不正検知モニタリング及び不正取引等を検知した際の対応に係る一連のプロセスに脆弱性がないか確認し、問題があると認められた場合は、リスクベースで不正取引等の防止策を講じた上で、その内容又は方法を変更する必要がある。

また、金融犯罪は日々、高度化及び巧妙化しているため、定期的かつ適時にリスクを再評価し、不正取引等防止策の継続的な改善を図る必要がある。

（１）申込み時の対応

本人確認は、犯罪による収益の移転防止に関する法律等に基づき的確に実施するものとし、非対面取引の場合は、次に掲げるいずれかの方法で本人確認を実施する必要がある。

① e-KYC（※1）

② 転送不要郵便又は本人限定郵便等を用いた郵便での KYC（Know Your Customer）

③ その他（公的個人認証サービス（※2）、犯罪による収益の移転防止に関する法律施行規則第 13 条第 1 項第 1 号に規定する方法等）

（※1）e-KYC（electronic Know Your Customer）
犯罪による収益の移転防止に関する法律施行規則に規定されている、オンラインで完結する自然人の本人特定事項の確認方法

（※2）公的個人認証サービス
オンラインでの申請や届出といった行政手続やインターネットサイトへのログインを行う際などに、他人による「なりすまし」やデータの改ざんを防ぐために用いられる本人確認の手段

ただし、既に取引時確認を行っている顧客等であることを確かめる措置をとった取引については、通常、犯罪による収益の移転防止に関する法律に基づく取引時確認は不要となる。既に取引時確認を行っている顧客等であることを確かめる措置に関しては、（２）サービス提供時の対応も参考にするものとする。

（２）サービス提供時の対応

インターネット取引サービスは、不正取引等のリスクを低下させた上で提供しなければならない。悪意のある第三者が不正に入手した認証情報等のみで不正取引等が行えないよう、次に掲げる例を参考に堅牢な認証方法及び認証後の対応を導入する必要がある。なお、ログイン時、出金時並びに顧客属性変更及び閲覧時にリスクに見合った多要素認証（※）を導入することが求められる。

（※）多要素認証

認証の３要素である「知識情報（ID＋複雑なパスワード等）」、「所持情報（ワンタイムパスワード等）」又は「生体情報（顔認証、指紋、声紋又は静脈等）」のうち、２つ以上を組み合わせて認証すること。

＜ログイン時＞

①　多要素認証の設定

ただし、出金時並びに顧客属性変更及び閲覧時に多要素認証を導入している場合は、「知識情報」、「所持情報」又は「生体情報」のいずれかによる認証に置き換えることも可能である。

②　ログイン通知又は通常と異なる端末でログインがあった際の通知

ログイン又は通常と異なる端末でログインがあった際は、身に覚えのない不正なログインを早期に検知するため、メール又はSMS等により利用者へ通知を行う。

③　ログインに複数回失敗した場合のアカウントロック（※）の設定

ログインに複数回失敗した場合、ログインを停止するアカウントロックの機能を設定する。

（※）アカウントロック

一定期間のログインの停止又は本人確認等の手続きを行うまでの間のログインの停止

＜出金時＞

①　多要素認証の設定

ただし、ログイン時に多要素認証を導入し、ログインから一連の流れで出金する場合は、「知識情報」、「所持情報」又は「生体情報」のいずれかによる認証に置き換えることも可能である。

②　出金完了通知

出金が完了した際は、身に覚えのない不正な出金を早期に検知するため、メール又はSMS等により利用者へ通知を行う。

＜顧客属性（※）変更及び閲覧時＞

① 多要素認証設定

ただし、ログイン時に多要素認証を導入している場合は、「知識情報」、「所持情報」又は「生体情報」のいずれかによる認証に置き換えることも可能である。

② 顧客属性変更完了通知

顧客属性変更が完了した際は、身に覚えのない不正な顧客属性変更を早期に検知するため、メール又はSMS等により利用者へ通知を行う。

（※）顧客属性

Webサイトやアプリ上で顧客自身が閲覧又は変更若しくは閲覧及び変更することが可能な自身の情報

＜備考＞

① 知識情報について、パスワードは複雑なものになるよう、文字数や組み合わせの条件等を設ける。

② 知識情報について、パスワードは推測しやすいパスワード（生年月日、電話番号及び一般的に使用されるパスワード等）の設定ができないように設計又は設定しないよう注意喚起を表示する。

③ ログイン時、出金時並びに顧客属性変更及び閲覧時の認証は都度行う。

④ 所持情報を入力する画面に注意喚起を表示することが望ましい。

例：当社はメール、電話等により、お客様のID・パスワードやSMS認証コード等をお問合せすることは一切ございません。

⑤ ワンタイムパスワードの有効期限を30秒～1分程度に設定することが望ましい。

（３）システムのセキュリティ対応

セキュリティ上の欠陥である脆弱性を解消し、顧客情報を外部及び内部の脅威から守るため、例えば次に掲げるセキュリティ対策を講じる必要がある。

① ファイアウォールの設置

② セキュリティのアップデートを行い、常に最新の状態に保つ

③ 顧客利用端末のマルウェア感染などに対して協会員側から対応可能な対策の検討

例：注意喚起、当該端末からのアクセス遮断、ログインの停止

④　カテゴリーに応じた脆弱性対策
例：脅威の情勢に応じたIPアドレスによるアクセスの制限
⑤　各種システムの脆弱性やセキュリティ上の抜け穴の有無の検証、必要な措置
例：脆弱性診断の実施
⑥　内部者犯行の検出、特定を可能にする管理態勢、内部統制の整備

（４）顧客情報等の管理

貸金業者は秘匿性の高い情報を保有しているため、常にサイバー攻撃及び情報漏えいのリスクがあることを認識し、例えば次に掲げる情報管理対策を講じる必要がある。

①　顧客属性等の匿名化又はマスキング
②　顧客情報等の保存、管理におけるデータの暗号化、ハッシュ化
③　顧客情報等の漏えい防止、管理強化策の実施
④　自社及び業務委託先でのデータアクセス制限、ログ取得
⑤　漏えい及び不正利用防止のための態勢整備状況の定期点検、強化策の実施
⑥　定期的な従業員教育を通じた情報取扱ルールの徹底及びルール順守状況の定期点検

（５）不正検知モニタリング

過去の不正取引等事案を分析し、その結果を反映させるなど、モニタリング機能の精度向上及び強化するため、例えば次に掲げる不正取引等の検知方法及び態勢整備を講じる必要がある。

①　アクセス推移の確認
②　ログ解析システムの導入
③　通常と異なるIPアドレスや地域等からのアクセス、取引パターン等の検知及び分析機能（振る舞い検知）の導入（不正検知関連の外部サービスの利用も可）

（６）不正取引等を検知した際の対応

不正取引等を防止するため、不正検知モニタリングによる評価（分析・検証の結果）に応じて、例えば次に掲げる対応等を実施する必要がある。

① 利用者への確認
② ID及びパスワード等の変更の案内
③ 不正と判断したアクセスを制限する機能の導入

３．不正取引等事案発生時の対応

（１）被害の拡大防止

不正取引等が発覚した際には利用者保護を最優先事項とし、事案の内容や規模等に応じて、次に掲げる被害の拡大防止措置を講じる必要がある。

① 取引の停止
(a) 不正取引等に利用されたID及びパスワード等の無効化又はアカウントロック
(b) サービスの停止

② 監督当局等及び協会への報告
(a) 障害発生等報告書（貸金業者向けの総合的な監督指針Ⅱ-2-4(2)②イ）
(b) 個人情報等漏えい等報告書（金融分野における個人情報保護に関するガイドライン第17条等）
(c) 警察への届出
(d) その他

③ 被害の公表
(a) ホームページ等にて事案の発生状況及び対応について公表
(b) 利用者への通知

④ 情報共有
(a) 他社との情報共有
(b) 関係団体との情報共有

（２）不正取引等への対応

次に掲げるとおり、不正取引等が判明した場合に備えて相談態勢を確立し、また不正取引等が判明した場合には事案解決に向けた対応を行う必要がある。

① 相談態勢の確立

被害者からの問い合わせや相談については、次に掲げる措置を講じ、真摯に対応する必要がある。

(a) 相談窓口の設置及び周知
(b) 相談者の不安を解消するための丁寧な説明や相談の実施
(c) 迅速かつ正確な事実関係の把握ができる態勢の整備
※　相談者に対して日本貸金業協会の相談・紛争解決センターの相談窓口やADR制度をホームページ等で周知すること。

② 事案解決に向けた対応

事案解決を迅速に行うためには、サービスの内容やリスクによって異なり得るものの、少なくとも次に掲げる事項について基準や手続き等を定めておく必要がある。

(a) 不正取引等による被害が発生した場合の緊急連絡ルート及び指揮命令系統の構築
(b) サービスの停止
(c) 不正取引等により発生した信用情報の抹消
(d) サービスの内容に応じた、具体的な場面ごとの被害者の責任の有無、内容及び要件がある場合にはその内容
(e) 不正取引等の公表（二次被害又は類似事案等の発生リスクが極めて軽微であると判断される場合を除く）

（３）被害者の保護方針

不正取引等が判明した事案において、被害者から当該不正取引等に係る債務を負担しない旨の意思表示があった場合、事前に定めた被害者の保護方針に従って、速やかに被害者に責任を負わせない対応を行う必要がある。

ただし、被害者側に過失がある場合等には個別対応を妨げるものではないが、その場合、提供するサービスの内容に応じた適切な方針を策定しておくことが重要であり、消費者契約法その他の法令の趣旨に照らし、被害者の保護に欠けるような方針は許容されるものではない点に留意が必要である。また、被害者に責任を負わせない場合とそうでない場合がある場合には、被害者にわかりやすく説明する必要がある。

（４）再発防止

不正取引等事案の発生後、速やかに次に掲げる例を参考に再発防止策を講じる必要がある。

① 原因分析等
(a) 不正取引等の事実の調査及び把握
(b) 把握した事実の原因分析
(c) 再発防止策の策定
(d) 再発防止策の有効性の検証及び改善
② リスクの再評価を行う
(a) サービス連携先と合わせたリスクの再評価
(b) サービス全体のリスクの再評価
③ 利用者への注意喚起等（ホームページ及び取引画面への掲載、アプリのポップアップ表示等）
(a) これまでに発生したサイバー攻撃や不正取引等の手口
(b) ID 及びパスワード等の適切な管理
(c) 身に覚えのない取引通知があった際の連絡
④ 社員教育
(a) 最近のサイバー攻撃や不正取引等の手口の周知
(b) 本人確認時に本人以外を見抜く方法等の研修
(c) 不審な取引への感知力向上の研修