日本証券業協会
Japan Securities Dealers Association

資料４

インターネット取引における
不正アクセス等防止に向けたガイドライン

2021年3月17日

10/4は証券投資の日

1. ガイドライン制定の目的

1. 制定の目的

- 昨今、インターネット取引サービスを顧客に提供する会員のシステムに悪意のある第三者が不正にアクセスし、顧客の有価証券を売却し、登録していた銀行口座とは別の口座に不正出金された事象や顧客情報が漏えいする事象が複数発生。このような不正行為を防止し、顧客が安心して証券取引を行うために、これまで以上にインターネット取引システムのセキュリティ水準の向上を図る必要がある。

- 証券業界としては、インターネット取引における口座開設時から出金に至る各段階における不正防止、脆弱性対策や情報管理、不正利用時の対応等についての具体的な留意事項をガイドラインとして取りまとめた。

- 会員各社においては、本ガイドラインにおいて対応が必要とされている留意事項（スタンダード）を着実に実行すべきであり、さらに対応することが望ましいとされている留意事項（ベストプラクティス）については各社の顧客特性などを勘案してリスクベースで検討、実施することが望まれる。

- なお、日々手口が変化する不正行為に対応すると同時に、進歩するインターネット技術を活用してセキュリティ水準を高める必要があることから、本協会は適時これらの変化に応じて本ガイドラインの見直しを行う。

2. 具体的な留意事項

- インターネット取引における不正アクセス等の防止を図るため、現行の法令・諸規則等を遵守するほか、次の事項について留意【詳細は次ページ以降】
  (1)口座開設、ログイン、取引、入出金等、(2)脆弱性対策及び情報管理、(3)モニタリング、(4)顧客情報（個人情報）に係る安全管理措置、(5)不正アクセス発生時の対応、(6)公表対応等、(7)その他

- 実施されていない項目がある場合は、各社の顧客特性などを勘案してリスクベースで検討し、着実に実行

※ 不正アクセス等防止の実効性を高めるためには会員間の情報共有や出金時における他業界との連携も重要な課題であることから、これらのガイドライン化等に向けて検討を行っていく。

2. 具体的な留意事項①

1．口座開設、ログイン、取引、出金等

	スタンダード			ベストプラクティス
(1) 口座開設時の本人確認	①eKYCの導入 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の導入			①公的個人認証サービスの導入 ②本人確認証跡の確保
(2) ログイン	①複雑なパスワード ‣文字数・組合せの制限 ‣推測可能なパスワードの抑止 **【上記の方法が取れない場合】** ①多要素認証	②ログイン通知 （顧客選択制も可）	③アカウント・ロック （複数間違えた場合のログイン停止）	①多要素認証 ②顧客固有の利用端末やIPアドレスを認証して限定的にアクセスを許可する手法の検討
(3) 取引	①複雑なパスワード ‣文字数・組合せの制限 ‣推測可能なパスワードの抑止 **【上記の方法が取れない場合】** ①多要素認証	②取引通知 （顧客選択制も可）	③アカウント・ロック （複数間違えた場合の取引停止）	○多要素認証
(4) 出金	①複雑なパスワード ‣文字数・組合せの制限 ‣推測可能なパスワードの抑止 ②多要素認証（顧客選択制も可）	③口座変更時通知 ④出金通知 （顧客選択制も可）	⑤アカウント・ロック （複数間違えた場合の出金停止）	
(5) その他（顧客属性）	①個人情報のマスキング ②重要な顧客属性が変更された場合の顧客への通知			

2. 具体的な留意事項②

2. 脆弱性対策及び情報管理

	スタンダード	ベストプラクティス
(1) 脆弱性対策	① カテゴリーに応じた脆弱性対策を行う。例えば、 （ア）脅威の情勢に応じたIPアドレスによるアクセスの制限 （イ）テレワークを導入している場合はサーバーへの遠隔接続サービスやVPNサービス、オンライン会議システム等のネットワーク環境の脆弱性対策や外部侵入経路の特定と不正アクセスを検出する手法や態勢の整備 ② 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 ③ 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	○ 顧客利用端末のマルウェア感染などに対して証券会社側から対応可能な対策の検討
(2) 情報管理	① 顧客の機密情報の保存・管理におけるデータの暗号化・ハッシュ化 ② 取引記録・保有資産残高情報の漏えい防止・管理強化策の実施 ③ 口座開設時の本人確認書類の返却又は廃棄等による記録媒体からの完全削除の実施を適時・確実にする事務管理態勢の整備 ④ 特定個人情報の厳重管理、漏えい・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	

3. モニタリング

スタンダード
① 顧客の属性情報やログイン時及びログイン後の挙動を分析して不正アクセスを検知（振る舞い検知を実施）、不正アクセスの評価に応じて追加の本人確認を実施、当該不正アクセスの適時遮断対応 【振る舞い検知の具体例】 ‣ログイン時：普段とは異なるデバイス、IPアドレス、及び地域からのアクセス ‣ログイン後：普段とは異なるページ遷移、入力操作、及び取引パターン（出金指示・出金状況及び出金先口座の追加・変更状況の分析を含む） ② 上記①の分析・検証を可能にする記録（ログ）の作成方法・有効保存の実施、そのための態勢整備

2. 具体的な留意事項③

4. 顧客情報（個人情報）に係る安全管理措置

スタンダード
法令等に規定する技術的安全管理措置の中でも特に以下の①から⑤について重点的に対応 ① 情報資産保護に関する社内規程の整備状況の確認 ② 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 ③ 情報を取り扱う区域の適正な管理の実施、情報を取り扱う機器・電子媒体等の盗難等の防止のための対策 ④ 社外からの不正アクセス対策としてのファイヤーウォール設置、自社及び業務委託先でのデータアクセス制限・ログ取得 ⑤ⅰ）外部委託した業務について、委託元として委託業務が適切に行われていることの定期的なモニタリング ⅱ）外部委託先への不正アクセス等により顧客情報が漏洩することのない措置が取られていることの確認 ⅲ）外部委託先における顧客データの運用状況を、委託元として監視、追跡できる態勢の構築

5. 不正アクセス発生時の対応

	スタンダード	ベストプラクティス
（1）顧客への対応	① 利用者からの問い合わせや相談を受け付ける窓口の取決め、利用者の不安を解消するべく真摯な姿勢での迅速かつ丁寧な対応 ② 被害状況を十分に精査し、顧客の態様やその状況等を加味したうえで、顧客との被害補償を含め、被害解決に向けての誠実かつ迅速な対応 ③ 一顧客が被害に遭った場合には、他の顧客にも被害が及んでいないか、その状況の調査	
（2）関係機関との連携強化		以下の対応をどのように行うのか整理しておく ① 銀行への連絡（被害発生時における出金停止等） ② 捜査当局への連絡 ③ 金融ISACへの情報提供による関連情報の還元・検知能力の相互強化 ④ 会員各社との情報連携

2. 具体的な留意事項④

6. 公表対応等

スタンダード
① 迅速な被害顧客への通知、二次被害の防止・類似事案の発生回避等に有用な情報の公表のための社内体制の整備 ② 各種届出義務（個人情報の漏えい、疑わしい取引、システム障害報告等）の確実な履行のための社内体制の整備

7. その他

	スタンダード	ベストプラクティス
（1）社内教育	例えば、本人確認時において本人以外を見抜く方法や最近の金融犯罪の手口に関する講座等の実務的な研修の実施	
（2）利用者への周知		例えば、Webサイト上又はメール等で利用者に対してログインパスワード及び取引パスワードの設定方法に関するお知らせなどの実施