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

2025 年 10 月 15 日

Ⅰ．ガイドライン制定の経緯

証券業界においては、法令・諸規則等に則り、顧客情報及び資産の厳格な管理に努めていたが、2020 年に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、顧客の証券取引口座にある有価証券を売却し、預り金と合わせて、顧客があらかじめ登録していた銀行口座とは別の銀行口座に不正出金された事象や顧客の個人情報が漏えいする事象が複数発生した。

証券業界としては、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という認識に基づき、2021 年３月に本協会はインターネット取引における証券取引口座の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「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」（以下、「ガイドライン」）として取りまとめた。

また、2021 年７月には、会員の外部委託先の従業員による不正アクセス・出金が発生したこと等を踏まえ、ガイドラインにおける外部委託先の顧客情報に係る安全管理措置等について、より具体的な事項を定めるための改正を行った。

Ⅱ．ガイドライン改正（2025 年 10 月）について

今般、公的個人認証サービス利用や多要素認証の普及・定着などインターネット技術の利活用に係る環境の変化に加え、昨今、フィッシング及びマルウェアにより、顧客情報（ID、パスワード等）が窃取され、インターネット取引において不正アクセス・なりすまし取引等により、従来の不正出金ではなく、不公正取引に悪用されている事案が発生したことを踏まえ、ガイドラインを改正することとした。

インターネット取引サービスを顧客に提供する会員においては、常日頃から不正アクセス等の防止を図るため、法令・諸規則等に基づき、適切な業務運営に努めているが、より一層、顧客が安心して証券取引を行うことができる環境を提供するため、ガイドラインの改正内容を踏まえて、各社が提供するサービスの内容に応じた対応策を改めて見直し、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に努めることが求められる。

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、本協会では、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ものとする。

Ⅲ．内部管理態勢の整備

インターネット等の不正アクセス・不正取引等の犯罪行為に対する対策等について、犯罪手口が高度化・巧妙化し、被害が拡大していることを踏まえ、最優先の経営課題の一つとして位置付け、取締役会等において必要な検討を行い、セキュリティ・レベルの向上に努め、以下の態勢を整備する。

- インターネット取引利用時における留意事項等について、顧客に説明する態勢
- インターネット取引の健全かつ適切な業務の運営を確保するため、金融商品取引業者内の各部門が的確な状況認識を共有し、金融商品取引業者全体として取り組む態勢

なお、上記態勢整備においては、金融 ISAC や JPCERT／CC 等の情報共有機関等を活用して、犯罪の発生状況や犯罪手口に関する情報の提供・収集を行うとともに、有効な対応策等を共有し、自らの顧客や業務の特性に応じた検討を行った上で、今後発生が懸念される犯罪手口への対応も考慮する。

また、リスク分析、セキュリティ対策の策定・実施、効果の検証、対策の評価・見直しからなるいわゆる PDCA サイクルを機能させる必要がある。

Ⅳ．インターネット取引における不正アクセス等の防止に向けた対応

本ガイドラインにおける、スタンダードとベストプラクティスは以下の考え方とする。

【スタンダード】
会員各社において、対応が必要とされる事項
【ベストプラクティス】
会員各社の規模・サービス内容や顧客特性、並びに犯罪手口の巧妙化・複雑化を踏まえた上で、対応することが望ましいとされる事項

１．不正ログイン・不正売買等を防止するための対応について

（１）口座開設時における本人確認

【スタンダード】

口座開設時における本人確認においては、「犯罪による収益の移転防止に関する法律[1]（犯収法）」等に沿って以下のいずれかの方法を用いた本人確認を実施する。

① 本人確認書類等を用いた以下のいずれかの方法

- 「写真付き本人確認書類の画像」＋「容貌の画像」を用いた方法
- 「写真付き本人確認書類の IC チップ情報」＋「容貌の画像」の送信
- 「本人確認書類の画像又は IC チップ情報」＋「銀行等への顧客情報の照会」を用いた方法

[1] 2027 年（令和9年）以降に施行が予定されている「犯罪による収益の移転防止に関する法律施行規則の一部改正」があることに留意が必要である。

・ 「本人確認書類の画像又は IC チップ情報」＋「顧客名義口座への振込み」を用いた方法

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 電子証明書を用いた以下のいずれかの方法

・ 「公的個人認証サービス[2]の署名用電子証明書（マイナンバーカードに記録された署名用電子証明書)」を用いた方法

・ 「民間事業者発行の電子証明書」を用いた方法

（2）ログイン・取引・出金時

【スタンダード】

第三者による、不正ログイン及び顧客の口座での不正売買等を防止するため、以下の機能・仕様を実装する。

なお、ウェブサイトやアプリケーションなど、複数の取引ツールでインターネット取引を提供している場合においては、各取引ツールで同じ水準の機能・仕様を実装する必要がある。

① フィッシングに耐性のある多要素認証の実装及び必須化

ログイン時、出金時、出金先銀行口座の変更時など、重要な操作時[3]におけるフィッシングに耐性のある多要素認証[4]（例：パスキーによる認証、PKI（公開鍵基盤）をベースとした認証）の実装及び必須化（デフォルトとして設定）する。

なお、内外の環境変化や事故・事件の発生状況を踏まえ、定期的かつ適時にリスクを認識・評価し、必要に応じて認証方式等の見直しを行うこと。

【フィッシング耐性のある多要素認証を実装することができない顧客への対応】
フィッシングに耐性のある多要素認証の実装及び必須化以降、顧客が必要な機器（スマートフォン等）を所有していない等の理由でやむを得ずかかる多要素認証の設定を解除する場合には、代替的な多要素認証を提供するとともに、解除率の状況をフォローした上で、認証技術や規格の発展も勘案しながら、解除率が低くなるよう多要素認証の方法の見直しを検討・実施する。

【フィッシングに耐性のある多要素認証を実装及び必須化するまでの対応】
フィッシングに耐性のある多要素認証を実装及び必須化するまでの暫定的な対応と

[2] 公的個人認証サービスとは、インターネットを通じて行政手続などやインターネットサイトにログインを行う際に、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。「電子証明書」と呼ばれるデータを外部から読み取られるおそれのないマイナンバーカード等の IC カードに記録することで利用が可能になる。

[3] ログイン等に複数の経路がある場合には、各取引ツール間で脆弱性がないかなど、相互に影響を確認する必要があることに留意する。

[4] 多要素認証とは、認証の三要素である「知識情報」、「所持情報」、「生体情報」のうち、二つ以上を組み合わせた認証をいう。なお、「フィッシング耐性のある多要素認証」には、ガイドライン上の例示であるパスキーによる認証や PKI（公開鍵基盤）をベースとした認証のほか、認証技術についての知見を有する CISA（米国 国土安全保障省サイバーセキュリティ・インフラストラクチャセキュリティ省）等の団体等が「フィッシング耐性のある多要素認証」であると認めている認証や一定の利用実績によりフィッシング事案が確認されていない認証などが考えられる。

して、代替的な多要素認証を提供する場合には、具体的なスケジュールについて顧客に周知するとともに、それまでの期間においても、振る舞い検知やログイン通知等の検知機能を強化する。

② 顧客への通知

身に覚えがない第三者による不正なログイン・取引（売買注文もしくは約定）、出金、出金先口座変更について、顧客自らが早期の被害認識を可能とするため、通知先として登録されている電子メールや SMS[5]等に対して、通知を送信する機能を提供する。

なお、顧客自らが通知（する・しない）を設定する機能を設けることができるものとする。

③ 認証に連続して失敗した場合のアカウント・ロック[6]

認証に連続して失敗した場合、アカウント・ロックの自動発動機能を実装及び必須化。

④ 重要な顧客情報[7]の窃取や改ざん防止

第三者が不正にアクセスし、重要な顧客情報の窃取や改ざんが行われないよう、重要な顧客情報のマスキング、容易に情報が変更できない仕組みや変更時において、上記（２）②と同様に、通知を送信する機能を提供する。

【ベストプラクティス】

第三者による、不正ログイン及び顧客の口座での不正売買等を防止するため、以下の機能・仕様を提供することが望ましい。

① フィッシングに耐性のある多要素認証の提供

取引時において、フィッシングに耐性のある多要素認証を提供することが望ましい。

② 取引等の制限

顧客が使用しない取引ツール・アプリについては、ウェブサイト上などで使用有無を選択できるようにする。また、取引可能な商品や取引金額の上限を制限できるようにすることが望ましい。

（３）不正売買、不正出金等を防止・検知するための設定等の利用状況確認等

【スタンダード】

不正売買、不正出金等を防止・検知するための設定（上記（２）①・②・④及び、各社において重要だと考えられる設定）について、顧客の利用状況を確認し、経営層に対して定期的な報告を実施する。

また、これらの設定を普及させるための追加的な施策を講じる必要がある（下記7.（２）顧客の被害拡大・二次被害等を防止するための注意喚起等 ② 参照）。

---

[5] SMS とは、携帯して使用する通信端末機器（携帯電話、スマートフォン、タブレット端末等）の電話番号宛てによりメッセージを送信できるサービス

[6] アカウント・ロックとは、一定時間のログインの停止又は本人認証等の手続きを行うまでの間のログインを停止すること。

[7] 重要な顧客情報とは、メールアドレスや電話番号等の連絡先、出金先銀行口座など

【ベストプラクティス】

不正売買、不正出金等を防止・検知するための設定の利用状況については、指標値（期限と目標値）を設けて確認を行うことが望ましい。

2．自社システムにおける脆弱性対策及び情報管理

（1）脆弱性対策

【スタンダード】

自社システムにおける脆弱性対策については、金融庁が公表する「金融分野におけるサイバーセキュリティに関するガイドライン」に記載の内容に準拠した対応を行う。

（2）情報管理

【スタンダード】

自社システムにおける情報管理については、特に以下の①から④について各社重点的に対応する必要がある。

① 顧客の機密情報（暗証番号、パスワード等、顧客に損失が発生する可能性のある情報）は当該データを保存・管理する基幹システムやデータベースにおいて、データの暗号化・ハッシュ化[8]等を施して保護し、内部関係者による顧客情報の窃取を否定できる措置を講じる。

② 不正アクセスによって顧客の取引状況が把握されることにより、例えば発覚を遅らせるために取引の少ない顧客を狙う等がないよう、取引記録・保有資産残高情報の漏えい防止・管理強化策を実施する。

③ 口座開設時の本人確認書類の確認後の本人への返却又は廃棄・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を整備する（本人確認書類又はその写しを犯収法で規定する本人確認記録としている場合は除く）。

④ 特定個人情報（マイナンバーを含む個人情報）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・強化策を実施する。

3．顧客情報（個人情報）に係る安全管理措置

（1）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については各社重点的に対応する必要がある。

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の実施

---

[8] ハッシュ化…元のデータから一定の計算手順に従ってハッシュ値と呼ばれる規則性のない固定長の値を求め、その値によって元のデータを置き換えること。

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の実施

④　社外からの不正アクセス対策として、侵入可能経路の特定、ファイアウォール設置、データアクセス制限・ログ取得の実施

⑤　顧客情報の社外移転状況（クラウド・サービス等の利用を含む）及び移転先での利用・管理状況の把握、顧客説明・同意取得状況の確認、状況に応じた監督及び安全管理措置の実施

（2）外部委託先における顧客情報（個人情報）に係る安全管理措置

【スタンダード】

外部委託先において適切な情報管理を担保するため、外部委託した業務（二段階以上の委託を含む）についての管理として、以下の対策を実施する必要がある。

① 外部委託先に対して、委託元として委託業務が適切に行われているか、定期的なモニタリングの実施

② 外部委託先への不正アクセス等によりログイン ID 、パスワードを含む顧客情報が漏洩することのない措置が取られているかの確認

③ 外部委託先における顧客データへのアクセス制限またはその運用状況を、委託元として監視、追跡できる態勢の構築

④ 外部委託先に設置する「開発環境」と顧客情報を管理する「本番環境」間の適切な情報管理及びデータ転送における手続きの整備・転送状況の適切なモニタリングの実施

⑤ 外部委託先に付与するアクセス権限について使いまわしを防止する等、権限管理の適切な実施

⑥ 外部委託先を含めた情報セキュリティリスク及び情報管理の運用状況について、経営層に報告する体制の確立

⑦ 二段階以上の委託が行われた場合、外部委託先が再委託先等の事業者に対して十分な監督を行っているかの確認

4．フィッシング詐欺等被害未然防止のための措置

【スタンダード】

フィッシング詐欺被害未然防止の観点から、以下の（1）から（5）について実施する。

また、フィッシング詐欺対策の情報の収集に当たっては、金融関係団体や金融情報システムセンターの調査等、金融庁・警察当局等から提供された犯罪手口に係る情報などを活用することが考えられる。

（1） 顧客へ送信する電子メールのドメインを特定し、DMARC 等の送信ドメイン認証技術の計画的な導入を行う。また、DMARC レポート等の確認等を行った上で、ポリシーは「reject」にする。

（２） 共通ショートコード[9]を利用し、Web サイト上又はアプリケーション上等で当該共通ショートコードを公開する。

（３） 自社を騙るフィッシングサイトについて、そのアクセス制限のためのテイクダウン（閉鎖）活動を行う。

（４） ドメインは自己のブランドと認識し、以下の①から③を中心に適切に管理する。

① 自組織に割り当てられているドメイン名を把握・管理する。

② ドメイン名のライフサイクルを管理する。また、ドロップキャッチやサブドメインテイクオーバー等の攻撃に対する対策を実施する。

③ 顧客に対し、サービスで使用するドメインに関する周知を行う。

（５） メールや SMS（ショートメッセージサービス）内にパスワード入力を促すページの URL やログインリンクを記載しない（法令に基づく義務を履行するために必要な場合など、その他の代替的手段を採り得ない場合を除く）。

【ベストプラクティス】

顧客が各社からの正規のメールだと判断できるように、以下を実施することが望ましい。

（１）電子メールにブランドのロゴや公式マークが表示されるよう、BIMI への対応を行う。

（２） 顧客へ何らかの通知を行う場合のメールについて、S／MIME による電子署名を付与する。

５．モニタリング

【スタンダード】

（１）ログイン時における不正アクセスの検知等

ログイン時の挙動の分析による不正アクセスの検知（ログイン時の振る舞い検知）及び事後検証に資するログイン・取引時の情報（位置情報、端末情報、接続元 IP アドレス、接続元ポート番号等）の保存を実施する。

（２）不正アクセスの評価（リスクベース評価）に応じた追加の本人認証・遮断対応等

不正アクセスの評価に応じて追加の本人認証を実施するほか、当該不正が疑われるアクセスの適時遮断、不正アクセス元からのアクセスのブロック等の対応を行う。

【ベストプラクティス】

上記（１）・（２）に加えて、ログイン後の挙動の分析による不正アクセスの検知（ログイン後の振る舞い検知）を実施することが望ましい。

[9] 共通ショートコード…共通ショートコードは、「0005」から始まる８～10 桁の SMS の送信元表示名。共通ショートコードは SMS 配信企業向けに、MNO４社（ドコモ、ソフトバンク、KDDI、楽天モバイル）の審査により発行されるため、共通ショートコードの SMS は正規メッセージと判別可能である。

6．不正アクセス発生時等の対応

（1）被害を受けたあるいは被害を受けた疑いが生じた顧客への対応

【スタンダード】

不正アクセスが発生した場合及びその疑いが生じた場合に、被害を受けたあるいは被害を受けた疑いが生じた顧客に対して以下の対応を行い、顧客の被害を最小限に抑制するための措置を講じる。顧客の不安を解消するべく、真摯な姿勢で丁寧に対応する必要がある。

① 顧客への迅速な連絡（被害発生時における出金先金融機関への出金停止依頼を含む）
② 顧客のログイン状況の確認
③ 顧客のアカウント（口座）の一時凍結
④ 顧客へのログイン情報（ログイン ID、ログインパスワード等）変更依頼
⑤ 顧客の取引及び出金の制限（顧客から申告が行われた場合の即時の取引及び出金停止措置を含む）

また、不正取引により顧客に被害が発生した場合には、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、顧客の被害補償を含め、被害回復に向けて誠実かつ迅速に対応する。

（2）顧客のアカウント（口座）の一時凍結、取引及び出金の制限後の再開手続き

【スタンダード】

アカウント(口座)の一時凍結、取引及び出金の制限後の再開手続きを行うにあたっては、二次被害の発生防止するため、改めて本人確認を行う。

（3）関係機関への報告・連携強化

【スタンダード】

不正アクセスが発生した場合及びその疑いが生じた場合を想定し、あらかじめ以下関連機関との連携等の対応を行い、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態勢を整備する。

① 金融当局への報告
不正アクセス・不正取引を認識次第、金融当局に対して当局指定の様式により、速やかに報告を行う。

② 捜査当局との連携
不正アクセス等により被害を受けたあるいはその疑いが生じた顧客のアクセス履歴(接続時刻、接続時間、アクセス元 IP アドレス、接続端末など）等の情報について、捜査当局や被害を受けた顧客から開示要請があった場合には、迅速に対応を行う必要がある。

③ その他市場関係者（取引所、日本証券業協会等）との連携・報告

④ 銀行との連携(下記7.(3)銀行口座との連携サービス 参照)

【ベストプラクティス】

金融 ISAC、JPCERT／CC 等の情報共有機関等を活用して、犯罪の発生状況や犯罪手口に関する情報の提供・収集を行うとともに、継続的に不正アクセス等の手口や対策に関する情報を共有し、関連情報の還元・検知能力の相互強化を行うことが望ましい。

また、自らの顧客や業務の特性に応じた検討を行った上で、今後発生が懸念される犯罪手口への対応も考慮し、必要な態勢の整備に努める。

7．その他

（1）社内教育

【スタンダード】

社内教育においては、最新の金融犯罪の手口・対策に関する講座等の実務的な研修を実施する。

【ベストプラクティス】

フィッシング等による不正アクセス・不正取引が発生したことを想定した、対応演習や訓練を実施することが望ましい。

（2）顧客の被害拡大・二次被害等を防止するための周知・注意喚起等

【スタンダード】

顧客の被害拡大及び二次被害の防止・類似事案の発生を防止するため、自社のウェブサイトやアプリケーション等において、以下の顧客への周知・注意喚起等を実施する。

① 顧客が、不正アクセスの事例や被害に関する情報を取得し、適切なセキュリティ対策を講じることができるよう、例えばインターネット上での ID・パスワード等の個人情報の詐取の危険性、類推されやすいパスワードの使用の危険性（認証方式においてパスワードを利用している場合に限る。）といった、フィッシング及びマルウェアによる不正アクセス防止の具体的なセキュリティ対策の周知を含めた情報発信や手口・危険性並び被害拡大の恐れがある場合には、その旨等についての注意喚起を行う。

② フィッシング及びマルウェアによる不正アクセス防止に関する対応について、顧客が各社において推奨される利用環境・設定を利用しない場合のリスクについて明示する。特に、それらを利用しない顧客に対しては、強く働きかける。

③ 不正アクセスが発生した場合及びその疑いが生じた場合の公表内容（顧客被害状況や不正アクセスの手口など）の整理、被害拡大の可能性がある場合に顧客が速やかにかつ容易に理解できる形で情報公開を行うための社内態勢を整備する。

④ 顧客が各社からのお知らせ・注意喚起等を確実に確認するための措置（お知らせ・注意喚起を確認しないと、ウェブサイトやアプリケーション等で次の動作・画面に進めない機能など）を行う。

⑤ 顧客からの届出を速やかに受け付ける体制を整備し、顧客からの問い合わせや相談受付窓口の設置などについて、顧客への周知を行う。

⑥　正規のウェブサイトのブックマークや正規のアプリケーションからログインすることについて、顧客への周知を行う。

（3）銀行口座との連携サービス

【スタンダード】

銀行口座との連携サービスを提供している場合には、攻撃者が証券口座への不正アクセスにより、銀行預金を証券口座に移し株式を購入する被害も想定されることから、連携する金融機関との対応について整理する。

①　連携サービス全体を見た対応

銀行口座、証券口座を連携する際は、預金口座からの出金に係る認証強度を確認する。

新規に預金口座と連携する顧客は、銀行口座における認証を経て新規に連携登録を完了した後において証券口座の認証のみで預金引き出しが可能である。

認証情報を窃取された場合は、預金に被害が生じうることの注意喚起を行うとともに、既存の口座連携している顧客に対しても、現在生じている手口や対策、確認すべき事項について注意喚起を行う。

②　顧客被害発生時の連携元・連携先の間の被害拡大防止に向けた協力体制を確立するとともに、連携元・連携先における責任・役割分担を明確化する。

【ベストプラクティス】

・ フィッシングに耐性のある多要素認証の提供

他の銀行口座との連携サービス提供時にフィッシング耐性のある多要素認証機能を提供することが望ましい。

以　上

付　　則

この改正は、2025 年 10 月 15 日から施行する。