日本証券業協会
JSDA Japan Securities Dealers Association

News Release

情報解禁日時
10月15日(水)14時30分

2025 年 10 月 15 日

報 道 関 係 者　　各 位

日 本 証 券 業 協 会

「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」の改正について

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いたしました。

また、今般のガイドライン改正に当たり、2025年７月15日から８月18日までの間にパブリックコメントの募集を行い、お寄せいただいたコメント及びこれに対する本協会の考え方を取りまとめましたので、併せて御報告いたします。

以　　上

○　本件に関するお問い合わせ先：　会員本部 会員部（TEL：03-6665-6768）

日本証券業協会
東京都中央区日本橋２丁目 11 番２号　〒103-0027
http://www.jsda.or.jp

情報解禁日時
10月15日(水)14時30分

「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」の改正について

2025 年 10 月 15 日
日 本 証 券 業 協 会

１．改正の趣旨

本協会では 2021 年３月に、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てきたところである。

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、ガイドラインの改正を行うこととする。

２．主な改正箇所

（１）ログイン時、出金時、出金先銀行口座の変更時など、重要な操作時における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（ガイドライン Ⅳ．１．（２）①）

（２）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（ガイドライン Ⅳ．１．（３））

（３）フィッシング詐欺等被害未然防止のための措置（ガイドライン Ⅳ．４．（１）～（５））

（４）社内教育、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（ガイドライン Ⅳ．７．（１）・（２））

（５）その他所要の改正を行う。

３．施行の時期

この改正は、2025 年 10 月 15 日から施行する。

○　本件に関するお問い合わせ先　日本証券業協会 会員部　（TEL 03-6665-6768）

以　上

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。

「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」の改正案に関するパブリックコメントの結果について

2025 年 10 月 15 日
日 本 証 券 業 協 会

本協会では、「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」の改正案について、2025 年７月 15 日（火）から 2025 年８月 18 日（月）までの間、パブリックコメントの募集を行いました。

この間に寄せられた意見・質問（44 先、115 件）及びそれらに対する考え方は、以下のとおりです。

なお、下記の「該当箇所」に記載の項番は、2025 年７月 15 日公表のガイドライン改正案に準拠したものとなります。

Ⅰ．ガイドライン制定の経緯

項番	該当箇所	ご意見	考え方
１	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	・ 今回の対策が実際に発生した被害の実像を経緯とするのであれば、攻撃者が利得を得る手段によって対象の業態に応じたリスクが異なるということを勘案すべきではないでしょうか。 ・ 今回の被害の中心は薄商いの板取引による不公正取引に類似した新たな利得の獲得手法であるということを考慮する必要があり、流動性の高い FX 業者や CFD 業者は対策の優先度や期限は、日本株または外国株の板取引を中心とした証券業者とは大きく異なるのではないかと思います。 ・ また、業態に応じて個人投資家の取引の頻度も大きく異なり、一律での利便性をトレードオフとした認証方式の導入の形態は特定の取引形態に対してセキュリティ上の効果に対して釣り合いの取れない機会損失を課す事とな	貴重なご意見ありがとうございます。 本ガイドラインは現時点でフィッシングによる不正アクセス等が行われている中、不正アクセス等による脅威・リスクへの対策として、証券界としての一定のセキュリティを確保するための水準を示しているものであり、証券界全体の対応力強化を図りたいと考えます。

項番	該当箇所	ご意見	考え方
		り、日本の証券市場への参加形態を大きく変えてしまう恐れがある他、海外の証券会社への流出や、特定の取引形態の一方的な衰退を招く恐れもあると思います。 ・ 規制当局は一連の被害について業態やリスクポイントへの傾向や知見を有しているはずであり、それに応じた段階的な対策の導入を推奨すべきではないでしょうか。	

Ⅲ. 内部管理態勢の整備

項番	該当箇所	ご意見	考え方
2	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	・ 認証におけるセキュリティ対策は、利便性とセキュリティ効果のトレードオフであることは広く周知されており、完全には防ぐことが出来ないということを前提とした多層防御と、その利用者やサービス提供者の特性に応じたコスト効果の高い対策を複数導入していくべき、というのは基本的な考え方だと思います。 ・ 今回、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、従来は２段階認証という脆弱な手法が一般的だったことが主因であり、その後緊急的な対策としてメールや電話による多要素認証が広く導入された経緯を取った上での更なる強化という位置づけとなると考えています。 ・ 一方、PDCA サイクルを回すにあたり、この緊急的に導入された多要素認証の効果について十分な精査が行われないまま、パスキーのような新しい技術仕様を実質的に強制となるような標準にするという事は個人投資家にとっても大きな負担となる他、導入のハードルが高い相場参	貴重なご意見ありがとうございます。 現在、「フィッシングに耐性のある多要素認証」については、例として、パスキーによる認証、PKI（公開鍵基盤）をベースとした認証を挙げています。 当該例は、現時点においてフィッシングに耐性があると考えられる認証方式であります。一般論として申し上げれば、今後の認証技術の進展や不正アクセスの動向を鑑み、必要に応じて対応を検討する必要があると考えられます。

項番	該当箇所	ご意見	考え方
		加者にとって代替案や実装面での軽減策を検討することが難しい状況を作り出してしまうのではないでしょうか。 ・ フィッシング耐性が低い多要素認証であっても、攻撃をしづらくする、被害にあう確率を軽減するといった効果そのものは認められるべきであり、フィッシング耐性が無ければ被害に遭うといったミスリードを想定させる他、フィッシング耐性さえあれば被害に遭わない、といった誤った主観を植え付けてしまう恐れもあるかと思います。 ・ 業界全体での PDCA サイクルを機能させる為にも、現時点で効果の高かった対策等についての情報の開示や、選択肢として考慮を可能とするような指針とすべきではないでしょうか。	

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

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

項番	該当箇所	ご意見	考え方
３	【スタンダード】 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	・ 現実の各証券会社の取引システムの実情と、広く普及している取引端末の OS やブラウザの標準仕様から、セキュリティ機能の実装の難易度はそのプラットフォームによって大きく異なるものだと考えられます。 ・ 特に Windows 端末のブラウザによるアクセスに対しての、パスキーを代表する「フィッシング耐性のある多要素認証」の提供は広範に安定的な運用実績が乏しい技術領域であり、モバイル端末のネイティブアプリケーション	貴重なご意見ありがとうございます。 ご意見のとおり、各証券会社では、インターネット取引において、様々な取引ツールをお客様に提供しております。 本ガイドラインでは、インターネット取引において、顧客に提供している各取引ツールで「フィッシングに耐性のある多要素認証」を実装することを求めております。

項番	該当箇所	ご意見	考え方
		と比べると、それを実際に導入しようと考えた時のロードマップは、モバイルのネイティブアプリとは大きく異なることが予想されます。 ・ この記述では、モバイル端末と同じ技術標準、同じスケジュールで統一すべき、という過剰な制約と受け取られる可能性があり、例えば「各取引ツールでスタンダードを下回る水準とならないこと」のような、是々非々での検討が行われるような記述にすることを検討してもよいのではないかと思います。	一方で、各取引ツールへの実装を同一の技術や同一のスケジュールで行うことは想定しておりませんが、顧客の取引ツールの利用状況やセキュリティレベルを考慮しながら、適切に対応する必要があると考えられます。

（１）口座開設時における本人確認

項番	該当箇所	ご意見	考え方
４	①　本人確認書類等を用いた以下のいずれかの方法	本人確認という文言は、身元確認と当人認証を混同した、もしくはあえて区別しない場合に使用する単語であるため、本ガイドラインでは適切でないように思います。以下の方法は、十分に脆弱であると考えられるため、認めない方針に変更すべきではないでしょうか。 ・写真付き本人確認書類の画像 →運転免許証などの紙面偽造は十分に横行していることから、紙面画像は十分に信頼足りうる情報源ではないと考えます。 ・本人確認書類の画像又は IC チップ情報 →同上 ・容貌の画像	本ガイドラインでは、口座開設時における本人確認について、現行の「犯罪による収益の移転防止法に関する法律」に基づいた記載としております。 なお、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法に関する法律施行規則の一部改正」に伴い、口座開設時における本人確認方法については一部改正されることが予定されており、本ガイドラインの記載も改正と併せて見直しを行うことを予定しております。

項番	該当箇所	ご意見	考え方
		→十分な精度でリアルタイムでディープフェイク動画を生成することは容易であるため、容貌の静止画や動画は十分に信頼足りうる情報源ではないと考えます。 ・銀行等への顧客情報の照会 →銀行等への顧客情報の紹介の際に使用される、銀行等側の認証が十分な否認防止性を持ったものであり、アクセス権付与までの連携処理においてもその否認防止性が維持されることが保証できる安全なプロトコルを用いた場合のみ、銀行などへの顧客情報の照会が認められるべきであると考えます。 ・顧客名義口座への振込み →同上 ・写真付き本人確認書類の IC チップ情報 →IC チップ情報があれば何でもよいのではなく、その情報が十分な否認防止性を持って取り出されたことが仕組み上保証できる場合に限ると考えます。	
５	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』は、昨今の偽造身分証の精巧さを考えると安全性が低いと考えられます。ＩＣチップ・電子証明書を活用する方式に一本化するべきと考えます。	
６	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	郵便によるＫＹＣではＩＣチップ・電子証明書の利用はないと考えられるので、前述の通り、資産のような重要な本人確認の方法としては不適切と考えます。	
７	③電子証明書を用いた以下のいずれかの方法	「民間事業者発行の電子証明書」を用いた方法 →どの民間事業者でもよいように読み取れますので、日本証券業協会が定期監査を行っている民間事業者に絞るべきと考えます。	本協会において、電子証明書を発行する民間事業者を指定することは想定しておりません。証券会社各社において、選定されるものと考えられます。

項番	該当箇所	ご意見	考え方
８	―	口座開設時における身元確認しか記述されておらず、以下のケースについても分けて行うべきと考えます。 ・アカウントリカバリー時(当人認証手段の紛失時など)に求められるべき身元確認 →口座開設時の身元確認手段の実施に加え、口座開設時に行った連絡先(SMS、e-mail、対面)での医師の再確認が必要と考えます。 ・口座を構成する重要な属性情報の更新時に求められるべき身元確認 →口座開設時の身元確認手段の実施に加え、その重要な属性情報が当人のものであるか、身元確認書類との再照合が必要と考えます。	貴重なご意見ありがとうございます。 本ガイドラインでは、口座開設時における本人確認について、現行の「犯罪による収益の移転防止法に関する法律」に基づいた記載としております。 なお、「Ⅳ．５．モニタリング（２）」に記載がございますとおり、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の実施が求められております。

（２）ログイン・取引・出金時

項番	該当箇所	ご意見	考え方
９	【スタンダード】 ① 多要素認証	出金時および出金先銀行口座の変更が不正取引に関わるため重要であることは明らかですが、ログイン時についてはなぜ重要な操作例として挙げられているのでしょうか。どのような脅威やリスクを想定しているのでしょうか。例えば、ログイン時にすべての個人情報等をマスキングし、出金時・出金先銀行口座の変更時にフィッシング耐性のある多要素認証を実装・必須化するとともに、マスキングを解除する際に同じ認証方式を要求すれば、本ガイドラインが想定しているリスクは解消されますか。あるいは、取引と同等に、ログインが大きなリスクという整理でしょうか。	今般、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サービスへの不正アクセス（不正ログイン）が行われてしまうことで、第三者による、不正な売却・買付が行われる被害が多発しました。 それらの状況を踏まえて、不正アクセスを防止するために、ログイン時におけるフィッシングに耐性のある多要素認証を必須化することを想定しています。 なお、その際、顧客の利便性の観点から取引時にフィッシングに耐性のある認証を実装することはベス

項番	該当箇所	ご意見	考え方
			トプラクティスとし、ログイン時においてフィッシングに耐性のある認証を実装することをスタンダードとすることとしました。 ご指摘事項である、ログイン時にすべての個人情報等をマスキングし、出金時、出金先銀行口座の変更時にフィッシングに耐性のある多要素認証を実装・必須化するとともに、マスキングを解除する際に同じ認証方式を要求するという方式では、本ガイドラインが想定している、不正アクセス等のリスクを解消するには不十分であることも考えられます。
10	【スタンダード】 ① 多要素認証	「フィッシングに耐性のある多要素認証(例: パスキー, PKIをベースとした認証)」の、「フィッシングに耐性のある」を「リアルタイムフィッシングに耐性のある」に修正すべき。 理由: 一般的に多要素認証はフィッシング対策技術である。しかしリアルタイムフィッシングには破られており、実被害が多発しているのでこれを防御する趣旨を明示すべき。なお、AitM まで含めると(中間者攻撃はリアルタイムフィッシングと AitM に大別できる)過剰対策となる。利便性やコストを下げるため、現実的にはリアルタイムフィッシングに絞るべき。証券業界における大規模攻撃はリアルタイムフィッシングによるものであり、AitM は確認されていない。 「フィッシングに耐性のある多要素認証(例: パスキー, PKIベース認証)」の、例示を削除すべき。 理由: 例示は事実上の強制力を持ち、同等以上の効果を持つ他技術導入を妨げる。また「PKI ベース認証」は範囲が不明瞭で混乱を招く。さらに、パスキーは厳密にはリアルタイムフィ	貴重なご意見ありがとうございます。 本ガイドラインにおける「フィッシングに耐性のある多要素認証」は、リアルタイムフィッシングに耐性を持つものが含まれていると考えられます。 なお、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は、現時点においてフィッシングに耐性があると考えられる認証方式であり、今後の認証技術の進展を踏まえて、その他の技術を用いた認証の実装を妨げるものではありません。 また、「国民を詐欺から守るための総合対策 2.0」（令和７年４月 22 日犯罪対策閣僚会議決定）において、次世代認証技術の一つである、「パスキーの普及促進」が掲げられています。

項番	該当箇所	ご意見	考え方
		ッシング耐性を有しておらず、単なるパスワード代替に過ぎない。 以下にパスキーやFIDO系の課題例を示す。 【リアルタイムフィッシングが可能】 WebAuthnの脆弱性がある。攻撃者がPCのログイン用QRを偽装サイトに表示し、フィッシングメールで誘導。利用者がスマホでQRを読み取りパスキー認証すると、攻撃者PCで即座にログインが成立する。これは典型的なリアルタイムフィッシングである。 【海外プラットフォーム依存】 Googleアカウントが不正アクセスされるとパスキーが不正登録され、複数の金融機関へ不正侵入が可能となる。Googleアカウントは二段階認証未設定の利用者が多数おり、既に大量のID漏洩が発生している。FIDO UAFも導入ハードルが高く、高齢者や非スマホ利用者を排除し、金融包摂に反する。実質的に国産技術を排除し海外依存を強制することは、国防・国益・金融安定性の観点から不適切である。海外事業者従業員の属性や地政学リスクを考慮せず国民資産の鍵を「単一貸金庫」に預けることは危険である。 注記４）の「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」ですが、「一定の利用実績により大規模なフィッシング事案が確認されていない認証など」とすべき。上述のように全ての技術は、一定の利用実績があると、必ず何かしらの攻撃にあうため「大規模な」をいれ条件を緩和すべき。そうしないと、例示にあるパスキーのみになり、単一技術	

項番	該当箇所	ご意見	考え方
		化による一斉攻撃のリスクを高めてしまう。セキュリティ技術は、多様性・中立性が重要で、相互補完しあう技術を併用・選択制で導入すべき。また国産技術を一つ以上入れることにより、地政学リスクを最小化すべき。	
11	【スタンダード】 ① 多要素認証	・ パスキーによる認証について、特に Windows 端末でのパスキーの管理は社会的に広く受け入れられているわけではなく、ユーザー側のリテラシーを求める手法であることへの考慮が必要ではないでしょうか。特に高齢者がパスキーを自身で運用することの難易度は非常に高い、という点にも十分に留意した記述にすべきではないかと思います。 ・ パスキーを利用するということは、ユーザー側が従来の ID とパスワードを覚えておくといった管理手法からのパラダイムシフトが要求される手法であり、ユーザー自身が責任をもって保存されたデバイスを管理し、そのデバイスのセキュリティに依存する、ということは未だ広くに普及された認知とは言えないのではないでしょうか。この認知には、証券業界だけでなく、先進的な金融以外のアプリケーションでの活用の標準化といった下地も必要ではないでしょうか。 ・ また、普及にあたって多量に作成したパスキーが単一のデバイスに集中することでの紛失時に何もできなくなることのリスクや、デバイス間での連携方法、普及することによって新たな非推奨な使い方による脆弱性等、も十分に考えられると思います。 ・ 急ぎ、セキュリティを向上させる必要がある現状に対して、「スタンダード」として過剰にパスキーへの依存性を	貴重なご意見ありがとうございます。 本ガイドラインの改正は、今般、フィッシング等により窃取された顧客情報により、インターネット取引サービスでの不正アクセス・不正取引（第三者による取引）の被害が急増したことを踏まえて、フィッシングへの対策を強化するために、「フィッシングに耐性のある多要素認証」の実装を【スタンダード】とすることとしています。 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は、現時点においてフィッシングに耐性があると考えられる認証方式であり、今後の認証技術の進展を踏まえて、その他の技術を用いた認証の実装を妨げるものではありません。 また、パスキーによる認証等の導入にあたり、顧客に対する十分な説明や準備期間が必要であると考えられます。

項番	該当箇所	ご意見	考え方
		強制してしまうのは、各証券会社の実装ロードマップを歪ませると共に、稚拙な実装による認証外の部分による脆弱性を誘引することにもなりかねないのではと危惧します。フィッシング耐性とはゼロヒャクではない、といった点を考慮した慎重な言及をすべきとも考えられ、他の業界や大手の認証ベンダーによる国民全員への普及度合いについても十分に勘案すべき技術ではないかと思います。	
12	【スタンダード】 ① 多要素認証	・ パスキーという言葉は技術的に多くの要素を含んでおり、一般的には広義のパスキーと狭義のパスキーという形で分けて説明されることが多いかと思います。 ・ 今回、フィッシング耐性を有するという文脈から、必然的にドメインの検証が行われる FIDO2 の規格に準じた「狭義のパスキー」を指し示していると考えられますが、明示されていない以上事業者が実装を検討するにあたり混乱や、「広義のパスキー」の拡大解釈といったことが懸念されるかと思います。 ・ 実装を検討するにあたって、不要な確認や要件の不明確化によって生じるコミュニケーションコスト増を避ける為にも、ガイドラインとして「広義のパスキー」を意図していないのであれば、その旨は明示すべきではないでしょうか。	貴重なご意見ありがとうございます。 本ガイドラインでは、フィッシングに耐性のある多要素認証の例として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を挙げていますが、一方で、本ガイドラインにおいては、実装するべき仕様の詳細を定義するものではありません。
13	【スタンダード】 ① 多要素認証	・ 多要素認証の実装例のパスキーとは、FIDO Alliance が策定した FIDO2 の仕様の一部であり、現在 W3C によって標準化された Web Authentication(WebAuthn)のことを指しているという理解は正しいでしょうか？	

項番	該当箇所	ご意見	考え方
		・ その場合、『パスキー』という表記よりも、米 CISA Implementing Phishing-Resistant MFA で説明されている『FIDO/WebAuthn authentication』の表記の方が適切だと思いました。(PKI をベースとした認証の表記に合わせるため) ・ 多要素認証の実装例のパスキーには、複数デバイス間で同期される Synced Passkey と、特定のデバイスに紐づけられた Device-bound Passkey が存在しますが、プラットフォーマが実装するパスキーは、Synced Passkey であり、クラウド環境等を通じて、複数デバイスで同一パスキーが同期されたり、別デバイスにパスキーを転送したりすることが可能です。そのため多要素認証でパスキーを導入使用する場合の、安全性の担保、推奨される運用方針、その他制約事項について、監督当局としての見解を示してください。 ・ 多要素認証の実装例のパスキーとは、オペレーティングシステム等を提供しているプラットフォーマー（主に、Apple 社, Google 社, Microsoft 社等）が実装しているパスキーに加えて、FIDO Alliance が策定した CTAP に準拠した外部セキュリティキーを含んでいるという理解は正しいですか？ ・ 多要素認証の実装に、パスキー等を導入検討する際、FIDO Alliance が策定したモバイルアプリ向けの規格 FIDO1.1UAF(Universal Authentication Framework) も含まれているという理解は正しいですか？	

項番	該当箇所	ご意見	考え方
		・　多要素認証の実装に、パスキー等を導入検討する際、FIDO Alliance の認定を受けている製品を採用することが望ましいと考えていますが正しいですか？	
14	【スタンダード】 ① 多要素認証	●「パスキー」には 2 つの種類があります。「パスキー」 はデバイス間で同期する、またはデバイスに固定して紐づける（バインドする）ことができます。 ・同期パスキー：クレデンシャル・マネージャーに安全に保存され、デバイス（携帯電話、タブレット、コンピュータ）間でアクセス可能 ・デバイス固定パスキー：単一のデバイス（セキュリティキー）にバインドされ、そのデバイスとしてのみ使用可能 （「パスキー・セントラル」 https://www.passkeycentral.org/ja/introduction-to-passkeys/passkey-types より） どちらの 「パスキー」も利用者やサービス提供者のニーズなどに応じて、あんしんして便利にお使いいただくことができるので、補足説明として追記していただいてはいかがでしょうか？ ●また、下記のとおり、補足等をしてはいかがでしょうか？ ・p.3 （２）ログイン・取引・出金時 【スタンダード】の記載で、「①多要素認証」と記載があり、p.4 【ベストプラクティス】の記載で、「①フィッシングに耐性のある多要素認証の提供」と記載があります。p.3【スタンダード】においても本文では 「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	貴重なご意見ありがとうございます。 本ガイドラインでは、フィッシングに耐性のある多要素認証の例として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を挙げていますが、一方で、本ガイドラインにおいては、実装するべき仕様の詳細を定義するものではありません。 なお、（２）ログイン・取引・出金時 【スタンダード】の記載で、「①多要素認証」の表記につきましてはご指摘を踏まえ修正いたしました。

項番	該当箇所	ご意見	考え方
		実装及び必須化（デフォルトとして設定）する」とあるので、「①多要素認証」→「①フィッシングに耐性のある多要素認証の提供」としてはいかがでしょうか？	
15	【スタンダード】 ① 多要素認証	今回の「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」の改正案は被害が急増した証券口座乗っ取りで、リアルタイムフィッシング攻撃等により従来の多要素認証の主流であった SMS やメール、認証アプリを用いたワンタイムパスワードでは防げないという認識が広がり、「フィッシング耐性のある多要素認証」で防御できると判断しての改正案だと推察します。具体的には FIDO2 認証やパスキー認証を各社が採用していくと考えます。しかしながら、スマートフォンの生体認証を用いたパスキー認証（FIDO 認証）にはいくつかの脆弱性があり、「パスキーハイジャック」と「生体ハイジャック」という２つの攻撃方法でハッキングのスキルが高くなくても容易にパスキー認証を乗っ取ることが可能であることを確認しています。これらの攻撃方法と対策について以下に解説します。 ・パスキーハイジャック 公開鍵暗号方式を使うパスキー認証では秘密鍵はデバイスのセキュリティチップに保存され奪うことが出来ないため安全だとされています。しかしながら、同期パスキーで秘密鍵がクラウド経由で同期されるシステムを悪用すると、犯人が遠隔から秘密鍵を犯人のスマートフォンにダウンロードすることが可能です。同期パスキーは複数のデバイス間で秘密鍵をクラウド経由で共有することにより、機種変更時などにパスキー認証を再設定することなく使用可能とし利便性とセキュリ	貴重なご意見ありがとうございます。

項番	該当箇所	ご意見	考え方
		ティを両立する方式として広く使われています。しかしながら同期パスキーの秘密鍵が紐づいているアップルアカウントやグーグルアカウント等が乗っ取られると以下のような状態が発生します。 iPhone 所有者のＡ氏のアップルアカウントのサインイン情報（ID・パスワード等）を犯人Ｂが何らかの方法で入手し、犯人ＢのiPhoneにＡ氏のアップルアカウントでサインインした場合、アップルアカウントに紐づいたパスキーの秘密鍵やID・パスワード等の認証情報が自動的に犯人Ｂのスマートフォンのセキュリティチップにダウンロードされます。セキュリティチップに保存された秘密鍵は取り出すことはできませんが、犯人Ｂのスマートフォンには犯人Ｂの生体情報が登録されており犯人ＢがFace IDやTouch IDを使ってＡ氏のパスキーの秘密鍵を用いてパスキー認証が成功します。 従って、アップルアカウントやグーグルアカウント等をリアルタイムフィッシングで乗っ取ればパスキー認証も乗っ取ることができます。パスキー認証も必要な対策を行わないとフィッシング耐性が十分でない場合があるということになります。パスキーハイジャックは完全に遠隔からの攻撃が可能で、物理的に攻撃対象のスマートフォン等を入手する必要がありません。同期パスキーが提案された時点ではデバイスごとにパスキーを設定する煩雑さや機種変更時の再設定などの問題を解決する方法として利便性が高く、例え秘密鍵を同期してもセキュリティチップに保存すれば秘密鍵の窃取は出来ないし、生体認証が第三者では拒絶されるので安全だと考えられ	

項番	該当箇所	ご意見	考え方
		ていたのだと推察します。しかしながら、実際には対象のスマートフォンに登録されている生体情報とスマートフォンのセンサで検出した生体情報を比較し比較結果が一致していればセキュリティチップに保存された秘密鍵を使ってチャレンジコードを暗号化してFIDOサーバーに送信されパスキー認証が完了します。スマートフォンの生体認証のハードウェアでは誰の生体情報と比較したかについては不明のまま比較結果が一致している アップルアカウントの保護策としては SMS 認証を使った二要素認証を設定できますが、リアルタイムフィッシングでワンタイムパスワードを突破できることが当たり前となっている現在では有効な保護策とは言えません。アップル社ではiOS16.3 以降で FIDO 対応のセキュリティキーをアップルアカウントの二要素認証に設定できるようにしています。この設定を行った場合にはアップルアカウントの二要素認証は SMS 認証からFIDO対応のセキュリティキーに切り換わり、アップルアカウントにサインインする場合にFIDO対応のセキュリティキーが必須になります。FIDO 対応のセキュリティキーは秘密鍵をセキュリティキー内に保存するため遠隔からの攻撃に対して非常に強く、例えアップルアカウントの ID・パスワード等が漏洩していてもリアルタイムフィッシングで攻撃してもFIDO対応のセキュリティキーがなければ遠隔からアップルアカウントにサインインすることはできません。 アップルアカウントの二要素認証を回避する方法として、メールやメッセージ、電話等で二要素認証を OFF に設定するよ	

項番	該当箇所	ご意見	考え方
		う誘導する例もあるので、二要素認証を OFF に設定しようとした場合に強く警告表示を行うなどの改善も今後検討するべきです。アップルアカウント以外にグーグルアカウントやマイクロソフトアカウントのようにパスキーの秘密鍵に紐づけられるアカウントではアップルアカウントと同様に二要素認証としてFIDO対応のセキュリティキーを設定できます。それぞれのアカウントでセキュリティキーを紛失した場合の回復手段やセキュリティキーがなくてもサインインできる方法の有無などが異なるので実際に対策を行う際にはそれぞれのアカウント毎に検証する必要があります。 証券口座乗っ取りではリアルタイムフィッシングだけでなくインフォスティーラーによる認証情報の窃取の可能性が議論されていますが、アップルアカウントやグーグルアカウント等を乗っ取るだけでインフォスティーラーで奪える ID・パスワードだけでなくパスキー認証も乗っ取られるリスクがあること及びその対策を周知徹底する必要があります。 ・生体ハイジャック スマートフォンに搭載されている生体認証は認証精度が高く、殆どのスマートフォンに搭載されているので追加のデバイス及び追加コストを必要としないためロック解除用としてだけでなくセキュリティ用としても広く使用されています。しかしながら、スマートフォンに搭載されている生体認証は登録された生体情報とスマートフォンのセンサで検出した生体情報を比較し判定結果のみをシステムに送り、誰の生体情報と比較したかについてはシステムでは不明のまま比較結果	

項番	該当箇所	ご意見	考え方
		が一致していれば正常に生体認証が完了したものとして動作します。スマートフォンに搭載されている生体認証はスマートフォンの正規の所有者が自身の生体情報のみを登録することが前提で設計されていますが、iPhone の場合であればパスコードを知っていれば誰でも生体情報の登録・追加・削除が可能です。パスキーの秘密鍵をスマートフォンごと物理的に入手し生体情報を追加すればパスキー認証も正常に行えるのでパスキー認証も簡単に乗っ取ることが可能です。生体ハイジャックでは秘密鍵を保存したスマートフォンを物理的に入手する必要がありますが、同期パスキー以外に秘密鍵を同期しない アップル社では iOS17.3 以降で盗難デバイスの保護機能を追加しました。この機能を ON にすることで生体情報を登録・追加・削除する場合には本人の生体認証が必須となり、本人以外が生体情報を登録・追加・削除することを防いでいます。この機能はかなり強力ですがアップルアカウントにサインインして盗難デバイスの保護機能を ON にしたデバイスを初期化することで盗難デバイスの保護機能を無効化することができます。従って生体ハイジャックを防ぐためにもアップルアカウントの二要素認証として FIDO 対応のセキュリティキーを設定することは重要です。Android OS にも同様の盗難保護機能がありますが、生体情報を保護する機能は高いセキュリティレベル（クラス３）の生体認証に対応しているデバイスのみで対応との記述があるので対応機種に注意が必要です。 ・結論	

項番	該当箇所	ご意見	考え方
		【スタンダード】 フィッシング耐性のある多要素認証という表記だけでは認証を突破される可能性のあるものが含まれています。より具体的に認証方式について詳しく分類し、セキュリティの弱い認証においてもセキュリティレベルを上げる対策を含めて明示した方が良いと考えます。また、同じ公開鍵暗号方式を使うFIDO 認証（パスキー認証）でも同期パスキーや秘密鍵を同期しないFIDO2、スマートフォンの生体認証を使うパスキー、秘密鍵を物理デバイスに保存するFIDO対応のセキュリティキー等の種類があり、それぞれでフィッシング耐性を含めたセキュリティの強度に差があります。名称についてもパスキーという名称が使われ始めた当初は同期パスキーの事をパスキーと呼び、同期しないものを FIDO2 と呼んでいましたが、現在は FIDO2 でもパスキーと呼ぶ例もあり混乱しております。仕様ごとに「パスキーType〇」等の分かり易い表示に統一しメリット・デメリット・可能な対策を明示すべきだと考えます。 【スタンダード】 スマートフォン以外の物理デバイスに秘密鍵を保存するFIDO対応のセキュリティキーではパスキーハイジャックや生体ハイジャックのリスクはなく、スマートフォンの生体認証を使ったパスキー認証よりはるかに安全です。スマートフォンの生体認証を使ったパスキー認証とFIDO対応のセキュリティキーはFIDOサーバーとの信号のやり取りは基本的に同じであり両方に対応する際の負担は大きく変わらないので、高いセキュリティが要求される場合にはFIDO対応のセキュリティキーを使ったFIDO認証を選択可能なように認証システムを構築し	

項番	該当箇所	ご意見	考え方
		ておくことが望ましいと考えます。SBI 証券の発表によれば本年秋ごろに導入予定の FIDO2 認証ではセキュリティキーにも対応予定で顧客側で選択可能です。 【ベストプラクティス】 ログイン時、出金時、出金先銀行考査の変更時など、重要な操作時における FIDO 対応のセキュリティキーを使った多要素認証の実装及び必須化する。 【スタンダード】 パスキーハイジャック及び生体ハイジャックの対策については、どのような認証方法を採用するかにかかわらず設定を強く推奨すべきです。具体的にはアップルアカウントやグーグルアカウント等の二要素認証の設定と盗難デバイス保護機能の設定です。アップルアカウントやグーグルアカウント等の二要素認証については少なくとも SMS 認証等の設定を最低限とし、できる限り FIDO 対応のセキュリティキーの設定を促すべきです。現状ではセキュリティの専門家でも FIDO 対応のセキュリティキーの設定可能であることが知られていませんので、周知を徹底すべきです。 【ベストプラクティス】 FIDO 対応のセキュリティキーによるアップルアカウントやグーグルアカウント等の二要素認証の設定を必須化し、盗難デバイス保護機能の設定と合わせてこの２つの設定が出来ないスマートフォンについては使用を推奨しないか補償対象外とすべきだと考えます。	

項番	該当箇所	ご意見	考え方
		今後の検討課題として、FIDO 対応のセキュリティキーは NFC 専用になりますが、タッチ決済付きのクレジットカードやマイナンバーカードのハードウェアにJAVAプログラムを載せることでセキュリティキーとして動作します。もちろん既存のJAVA プログラムとの競合等で動作しない可能性も否定できませんが、マイナンバーカードにセキュリティキーの機能を追加できれば多くの国民がFIDO対応のセキュリティキーを持つことが可能でマイナンバーカードの普及も促進できます。クレジットカードやキャッシュカードにセキュリティキーの機能を追加することもセキュリティキーを広く普及させることが可能となります。JAVA プログラムの追加だけであればカードのコストアップも少なくて済みます。カード形状のセキュリティキーは評価用として提供可能です。 いずれにしろパスキー認証にも脆弱性があり完璧ではありません。不正アクセス・不正取引の被害を減らせるように実効性のある認証方式や不正防止策の強化の参考になればと考えております。	
16	【スタンダード】 ① 多要素認証	１.「認証技術についての知見を有する団体」について フィッシングに耐性のある多要素認証について、認証技術についての知見を有する団体として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)が例示されていますが、外国の機関に基準を委ねるのではなく、国内の認証技術について知見を有する団体を選定すべきであると考えます。 ２.「一定の利用実績」について フィッシングに耐性のある多要素認証の要件として、「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」	貴見のとおり、フィッシングに耐性のある多要素認証が実装できない顧客に対しても、フィッシングによる被害を低減する一定の実績がある、あるいは効果的であると想定される多要素認証を実装することが必要であると考えられます。それらの多要素認証を利用するにあたっての留意事項については、顧客に十分に周知する必要があると考えられます。

項番	該当箇所	ご意見	考え方
		と定義されていますが、「一定の利用実績」との表現が曖昧であると思います。 目安となるような基準が大まかにでも示されるべきと考えます。 ３.「代替的な多要素認証」について① 【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】において、「代替的な多要素認証」を提供することが求められております。 この「代替的な多要素認証」について、犯罪被害を軽減するために、少しでもフィッシングに強い多要素認証の導入を推奨することが望ましいと考えます。 ４.「代替的な多要素認証」について② 【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】において、「代替的な多要素認証」を提供することが求められております。 この「代替的な多要素認証」について、「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」と認められた場合は、これを以って「フィッシングに耐性のある多要素認証」になり得、対策として十分であることを明記すべきであると考えます。	
17	【スタンダード】 ① 多要素認証	●専用のアプリを利用しモバイル端末で完結する（一般的なブラウザから利用できない）スマホ証券サービスにおいては、端末認証を必須とすることで、「フィッシングに耐性のある多要素認証」と同等の対策を講じていると評価してよいでしょうか。 ●ここで言う「ログイン」はログイン後に追加の認証なしで取引・出金・登録変更などの「重要な操作」が行えるものを指し、	ご質問の趣旨が必ずしも明らかではありませんが、証券会社が提供するアプリケーションを用いてインターネット取引サービスが提供されている場合、フィッシングに耐性のある多要素認証をログイン時、出金時、出金先銀行口座の変更時などに実装することが求められます。

項番	該当箇所	ご意見	考え方
		ログイン時の認証だけでは参照しか行えないものは必ずしも含まないと考えてよいでしょうか。 ●必ずしも操作の都度多要素認証を行うことが求められるものではなく、一度認証をした同一セッション内で一定時間は再度の認証を行わないことも許容されると考えてよいでしょうか。 なお、監督指針のガイドラインの改正案にも同様の記載があるため、同様の意見提出を行っています。	
18	【スタンダード】 ① 多要素認証	・ 顧客が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、というケースの想定はスマートフォンの非所有以外にも、高頻度ではないアルゴリズムトレード等の自動売買をしているケースも考えられると思います。 ・ ガイドライン全体として、個人投資家の取引様式を旧来の対面取引の延長にある Web 取引のみを想定しているような文脈となっていますが、既に多くの個人投資家は様々な自動化手法によって自動売買を実現しており、その取引量は相場全体の多くを占めるようになっているはずだと思います。 ・ 今回、被害が拡大した経緯においても、そういった顧客に対してセキュリティ的に不完全な取引ルートを提供していた証券会社の存在も一因となっていることは周知の事実ではないでしょうか。 ・ API の提供やその場合のセキュリティの施策等についても考慮し、実質的に自動売買が不可能なスタンダードとしてしまうことで、よりセキュリティが低い証券会社や、	貴重なご意見ありがとうございます。 本ガイドラインの改正は、今般、フィッシング等により窃取された顧客情報により、インターネット取引サービスでの不正アクセス・不正取引（第三者による取引）の被害が急増したことを踏まえて、フィッシングへの対策を強化するために、「フィッシングに耐性のある多要素認証」の実装をスタンダードとすることとしています。今般の事象を防止することを前提としつつ、引き続き、必要に応じて検討してまいります。

項番	該当箇所	ご意見	考え方
		海外の証券会社に日本の個人投資家が流出しないような考慮も必要ではないかと思います。	
19	【スタンダード】 ① 多要素認証	多要素認証の導入を前提として、 ・ログインパスワードと取引パスワードの区別を禁止すべき 理由：そもそもパスワードレスが要求されている時代にパスワードを２つ持つこと自体がセキュリティリスクであり、ユーザが簡易なパスワードを設定する原因になる。 ・共通化したパスワードに対するパスワードポリシを定め、特に文字種を制限せず数十文字以上の ASCII 文字列を許容できるようにすべき 理由：パスワードの長さは強さである。短いパスワードを２つ持つくらいならば長い１つのほうが良い。 ・パスワードの定期的な変更の要求を禁止すべき 理由：パスワードの定期的な変更は簡単で予測しやすいパスワードを生む。	本ガイドラインにおいては、フィッシングに耐性のある多要素認証として例示されてい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は、いわゆるログインパスワードの利用を想定しておりません。
20	【スタンダード】 ① 多要素認証	多要素認証としてワンタイムパスワードが広く利用されていますが、最近は精巧な偽サイトやフィッシングが蔓延しております。この状況では人の手で作業を行う方法は安全性が低いと言うほかなく、フィッシング耐性がある多要素認証はもはや必須と考えます。その点において、こちらは是非推進していただきたいです。	貴重なご意見ありがとうございます。
21	【スタンダード】 ① 多要素認証	ログイン時の KPI 導入について，例示としてマイナンバーカードを使用しての JPKI を記載してはどうか	貴重なご意見ありがとうございます。
22	【スタンダード】 ① 多要素認証	【意見】 フィッシングに耐性のある多要素認証として、パスキーによる認証、PKI（公開鍵基盤）をベースとした認証が挙げられて	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は、現時点においてフィッシングに耐性があると考えられる認証方式であり、今後の認証技術

項番	該当箇所	ご意見	考え方
		いるが、これら以外でも該当する方式について具体的に記載していただきたい。 【理由】 原則としてフィッシングに耐性のある多要素認証を採用することの重要性を認識しているが、各社において採用した方式が本ガイドラインのなかでどのような位置づけになるかについて明確になることが不正ログインに対するお客様の信頼確保につながるものと考えており、「フィッシングに耐性のある多要素認証」に該当する方式についての記載をより充実化していただきたい。	の進展を踏まえて、その他の技術を用いた認証の実装を妨げるものではありません。
23	【スタンダード】 ① 多要素認証	・ 例以外の方法の場合、フィッシングに耐性があるか否かの判断は各社で行うことになるか。その場合、「フィッシング耐性のある多要素認証か否か」はどう客観的に判断するのか。世の中で耐性があると言われている、以上の判断根拠を明示して欲しい。 ・ 例以外の代替的な多要素認証をやむを得ず提供する場合もフィッシングに耐性がある多要素認証が求められているか。	認証方式の安全性・リスクについては、技術の進展等により適宜変化するものであると想定されますが、現時点では、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は、フィッシングに耐性があると考えられます。 なお、例示以外の認証方式の利用を妨げるものではありません。また、世の中で耐性があると言われている認証を導入したのち、犯罪手口の巧妙化等により、不正アクセスされたことだけをもって、速やかにガイドラインの違反を問うものではないと考えられます。
24	【スタンダード】 ① 多要素認証	「代替的な多要素認証」として容認される方式として現時点で想定される方式について具体的に記載していただくとともに、それらに対する評価も併せて記載いただきたい。 例えば、代替的な多要素認証として様々な方式の中には、採用しないことが望ましい方式や短期的な採用であるならば許容される方式などはあるのかなど、評価に幅があるのではない	本ガイドラインにおいて、代替的な多要素認証（認証方式）についての評価などについての記載は行いません。認証方式の安全性・リスクについては、流動的であり、技術の進展等により適宜変化するものであると想定されます。それらを考慮しながら、不正

項番	該当箇所	ご意見	考え方
		かと考えており、ガイドラインにおいて認証方式に対する評価や補足的な説明について記載していただきたい。 【理由】 フィッシングに耐性のある多要素認証を必須化していくまでには暫定的な対応として「代替的な多要素認証」を採用せざるを得ない証券会社は相当程度生じることになると思われるが、暫定的な対応としてであっても、よりお客様に安全に取引をしていただけるようにすることが重要であり、貴協会より更なる情報提供をいただけると、どの方法を採用するかの検討が各社において充実化するとともに、お客様にも安心いただけるかと考えるので、ガイドラインの記載をより充実化していただくようお願いしたい。	アクセスのリスクを低くする認証方式を提供する必要があると考えられます。
25	【スタンダード】 ① 多要素認証	「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」との記載について、「代替的な多要素認証」には”フィッシングへの耐性”が必ずしも求められるものではない、との理解で合っているか、確認したい。 【理由】 ”フィッシング耐性のある多要素認証”については、「パスキー」もしくは「PKI（証明書認証）」による実装が想定される。当社は現在「パスキー」による”フィッシング耐性のある多要素認証”の導入を進めている。⇒ガイドラインにあるとおり、「非所有」を理由に「パスキー」をお使い頂けないケースにおいては、同様に「PKI」もお使い頂けないことが想定されるため。	フィッシングに耐性のある多要素認証の提供が困難な顧客に対しては、実装が可能な多要素認証を提供する必要があると考えられます。代替的な多要素認証については、認証技術の進展や認証強度、利用実績などを考慮しながら、不正アクセスのリスクを低くする認証方式を選択する必要があると考えられます。
26	【スタンダード】 ① 多要素認証	【1】現状の課題認識 現在提示されている「フィッシングに耐性のある多要素認証」は、概念としては重要であるものの、実装とユーザー保護につ	貴重なご意見ありがとうございます。

項番	該当箇所	ご意見	考え方
		いては各証券会社に委ねられており、具体性に欠ける懸念があります。また、FIDO2／パスキー／Authenticator 等の方式であっても、「クロスデバイス認証時に中間者攻撃（リアルタイム・フィッシング）」を受けるケースが現実に存在しており、ユーザーが騙される設計を前提にした対策では限界があると感じています。 【2】提案①：ブラウザとの連携による認証支援 ブラウザ自体が「現在アクセスしている URL を QR コード等で明示」し、認証アプリ側でその正当性を検証するような仕組みのガイドライン化を検討していただきたいです。現在の Passkey や QR 認証では、ユーザーは「その認証要求が誰から来ているか」を視覚的に確認する手段がなく、これが中継攻撃による突破の原因となっています。 【3】提案②：証券会社任せにせず、業界横断の共通インターフェース／認証基盤の検討を 「フィッシング耐性のある多要素認証」の提供義務は証券会社側に丸投げするのではなく、日証協として共通ガイドラインや API、UI 設計のベストプラクティス（例：認証ドメイン明示・再確認インターフェース）を業界横断で整備することをご検討いただきたいです。ユーザーは複数の証券会社に口座を持つことも多く、UX がバラバラでは混乱を生み、結果的にセキュリティリスクを増やす可能性があります。 【4】補足・まとめ 一般ユーザーや高齢者も含めた全体のセキュリティ底上げを図るためには、「ユーザーが騙されても成立しない設計」と「ユーザーが直感的に確認できる支援表示（ブラウザ UI）」の両方が必要だと考えます。また各証券会社には、ブラウザからのア	

項番	該当箇所	ご意見	考え方
		クセスの場合は、アクセスしているＵＲＬを確認する仕組みを導入するべきと考えます。尚、一部企業が導入しているCookie/LocalStorageによる”疑似的デバイス登録”は、リアルタイム・フィッシングには脆弱であります。 【5】最後に ガイドラインの抽象化だけでなく、実装指針レベルまで踏み込んだ議論・整備をお願い申し上げます。	
27	【スタンダード】 ① 多要素認証	今回の口座乗っ取りの大きな原因の一つは、利用者がフィッシング詐欺サイトに導かれたのかもしれませんが、テスタ氏に限らず、十分フィッシング詐欺サイトを踏まないように注意していた利用者も被害にあっているところから、インフォスティーラー攻撃や RTPP,AiTM 攻撃の可能性も大きいと思います。 そんな中、ガイドラインを読むと パスキーを導入すれば、大丈夫だという印象を与えがちですが、パスキーはパスワードレス本人認証を堅牢化する技術であり、セッションハイジャック対策を保証するものではありません。 - パスキーや多要素認証の導入だけでは、依然としてセッション ID を奪取される攻撃への防御はできません。 - ガイドラインでは、ログイン時、出金時、フィッシングに耐性のある多要素認証（例：パスキーによる認証、PKI（公開鍵基盤）をベースとしとありますが、上述に記しましたが、フィッシングに耐性のある多要素認証を導入しても、セッション ID を奪取される攻撃には効果がありません - また、ガイドラインでは、ログイン時、出金時、フィッシングに耐性のある多要素認証（例：パスキーによる認証、PKI（公開鍵基盤）と書かれていますが、パスキーは PKI 機能を活用	貴重なご意見ありがとうございます。

項番	該当箇所	ご意見	考え方
		するソリューションなので、以下のようにしゅうせいすべきかとおもいます。（例：PKI（公開鍵基盤）による認証） - パスキー導入だけで「ガイドライン適合→責任を果たした」という安易な認識が組織現場に広がる危険性を指摘します。 - 全面施行前に、認証のところを強化しても効果が薄い可能性がある事を、事例分析も含めて周知しておくべきだと考えます。実際、パスキーも今年になってからでも被害報告が始まっています。 - 現行パスキーは ECC や RSA 等の従来型公開鍵暗号に依存しており、量子耐性が将来課題であることも頭に入れておくべき情報だと考えます。 - 最後に、ガイドラインでは、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。となっていますが、以下のように改めるべきではないでしょうか？ 年に２回かつ適時にリスクを認識・評価し、担当役員に報告する事。役員は必要に応じて自身の責任と権限で、認証方式等の見直しを行い、適宜導入運用し、運用効果を測定し社長に報告する事。	
28	【スタンダード】 ① 多要素認証	**＜同様のご意見、ほか５件＞** これらの理由より、二要素認証の実装、利用に関しては、証券会社の自主的な判断にゆだね、努力義務にとどめるべきだと考えます。利用ユーザーも、二要素認証を利用するか否かは自分で判断できることを原則としてほしいと思います。 不正ログイン、売買、出金など、標的にされやすいような大手証券会社はすでに、こういった高度な二要素認証を導入しており、改訂せずとも、自主的に対応を行っている現状を踏ま	フィッシングに耐性のある多要素認証の実装については、原則、全ての顧客が対象となります。 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多要素認証を実装することができないなどのケースは想定されますが、顧客からの利便性に関する要望に応じて実装の可否を判断するものではないと考えられます。

項番	該当箇所	ご意見	考え方
		え、一律全ての証券会社に強制するようなことは控えるべきだと思います。 さらに、二要素認証を利用しない設定にしたユーザーへの対応について、各証券会社は大きく分かりやすく、例えば「当社はこういった認証方法を提供しているがユーザーによる利用は自由で、解除も可能です。ただし、利用しない場合に不正などの被害が発生した場合、原則補償しない」などと表示する必要があります。この表示は義務化すべき箇所です。	
29	【スタンダード】 ① 多要素認証	**＜同様のご意見、ほか１件＞** 利便性を追求し、代替的なものも含めたすべての多要素認証の適用を拒否する顧客も存在する。当該顧客に対しては、多要素認証の適用を行わないことのリスクを説明の上適用しないような措置が可能であることを確認したく、その点を明記頂きたい。その際、何らかの追加の措置が必要であれば、考えられる措置についても確認したい。	
30	【スタンダード】 ① 多要素認証	以下のケースを「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」の一類型と整理して問題ないか。 ① IT リテラシーが著しく低い等、複雑な端末の設定や操作が困難な顧客 ② フィッシング耐性のある多要素認証を選択するも、複数の取引端末を利用する等、必ずしもフィッシング耐性ある認証方式を利用できない顧客 ③ 高頻度取引を行うため、自身のリスクにより多要素認証の解除要請があった顧客 ④ 出金時においてのみ二要素認証の解除要請があった顧客（解除に際しては二要素認証を適用）	顧客がフィッシングに耐性のある多要素認証を設定するにあたっては証券会社には丁寧な対応が求められますが、それらの対応を行った上で、複雑な端末の設定や操作がどうしても困難な顧客に対しては、代替的な多要素認証を提供する必要があることが考えられます。 また、ご質問の趣旨が必ずしも明らかではありませんが、例えば複数の取引端末を利用する、高頻度取引を行う顧客であってもログイン時、出金時、出金先銀行口座の変更時などはフィッシングに耐性のある多要素認証が求められます。

項番	該当箇所	ご意見	考え方
31	【スタンダード】 ① 多要素認証	【意見】 （重要な操作時における多要素認証の）「必須化」の対象者について教えていただきたい。必須化の対象となるお客様は、すべてのお客様の意味か。この場合、新規のお客様に向けた導入スケジュールと既存のお客様に向けたものとを異ならせることは許容されていると考えてよいか。 【理由】 新規のお客様については、口座開設時に新しい認証方式のご案内やサポートが比較的容易である一方、既存のお客様の場合、これまでの認証方式が全く利用できなくなると、大きな混乱（ログインができない、取引ができない、入出金ができないなど）が想定される。既存のお客様が安心して取引ができるような認証方式の導入は当然進めていくものの、既存のお客様において取引ができなくなるような不利益が発生しないようにするには、丁寧なコミュニケーションの中で新しい認証方式への移行を促すことが重要であり、そのためには導入スケジュールは柔軟性があることが必要であると考えている。	フィッシングに耐性のある多要素認証の設定については、原則、全ての顧客が対象となります。 一方で、顧客への影響を鑑みながら、新規顧客と既存顧客への対応について、異なるスケジュールを設定することも考えられます。
32	【スタンダード】 ① 多要素認証	【意見】 （重要な操作時における多要素認証の）「必須化」の具体的な内容について補足いただきたい。 重要な操作を行う場合には、その操作ごとに、フィッシング耐性を持つ多要素認証を経なければ操作が完了しないようにしなければならないということか。（従来の ID・パスワードによる認証で操作を完了させることは不可能なのか。また、操作の「都度」認証が必要であるということか（例えば連続した操作の場合も都度認証が必要ということか）） 【理由】	ご理解のとおり、本ガイドラインⅣ．１．（２）①多要素認証では、ログイン時、出金時、出金先銀行口座の変更時を「重要な操作時」としています。それに加えて、各社において重要な操作であると判断した場合には、多要素認証を実装することが考えられます。

項番	該当箇所	ご意見	考え方
		特に既存のお客様の場合、これまでの認証方式が全く利用できなくなると、大きな混乱（ログインができない、取引ができない、入出金ができないなど）が想定されるため、お客様に対する説明を丁寧に行い、理解を得ることが重要であると考える。そのため、必須化の具体的な内容についてガイドラインの記載をより充実化していただきたい。	
33	【スタンダード】 ① 多要素認証	【意見】 フィッシング耐性のある多要素認証の必須化は、新ガイドライン施行と同時に完了することまでは求められておらず、お客様の負荷にならないような形で導入していくことが許容されており、従来の認証方式との併用や段階的な導入も許容されるか。 【理由】 「必須化」により、お客様に対しても大きな影響と負荷があること（お客様において新しい認証方式による手続を理解・習熟していただく必要がある）を踏まえ、十分に移行期間を確保することが必要と考えている。移行期間を適切に設けることにより、お客様に対する丁寧な周知を徹底すること（特にITリテラシーが高くない方にはサポート体制を整備することが必須）が可能となるので、お客様への影響・負荷を踏まえた導入が可能であることをガイドラインで示していただきたい。	本ガイドラインに基づいた内部管理態勢の整備、並びにスタンダードとされている事項に対応するための機能・仕様の構築には時間を要することが考えられることから、本ガイドラインの施行日と同日に対応の完了を求めるものではありません。 また、新しい認証方式の導入にあたっては、顧客への周知や対応期間が必要になると想定されます。証券会社の態勢整備の状況や顧客の負担を考慮した上で、従来実装していた認証方式との併用や段階的な導入を行うことも考えられます。
34	【スタンダード】 ① 多要素認証	【意見】 各証券会社がお客様への周知や啓発に努めることは当然として、貴協会においても継続的、積極的に利用者への周知やサポートをお願いしたい。 【理由】	貴重なご意見ありがとうございます。 本協会においても、不正アクセス等の防止に向けた対応・取組みについての周知を行ってまいります。 また、本協会のウェブサイト・SNS等を活用した安全にインターネット取引を行うための注意喚起・情報発信についても継続的に行ってまいります。

項番	該当箇所	ご意見	考え方
		セキュリティの高い認証方式をお客様が迷うことなく快適に利用いただくためには、お客様への周知や啓発が不可欠であると考えており、お客様の安全性確保のためには、業界全体として行動する必要があると考えている。	
35	【スタンダード】 ① 多要素認証	ログイン時、出金時、出金先銀行口座の変更時などに、「フィッシング耐性のある多要素認証」の必須化が要請されていますが、口座利用プロセス全体を見た場合、最も重要なのは入口である「ログイン時」だと考えています。ログイン時に安全な対策が講じられていれば、その後のプロセスにおける被害の可能性は大きく低減されると認識しています。すべての段階に「フィッシング耐性のある多要素認証」を導入すると、プロジェクトの複雑さが増す一方で、防犯上の効果は限定的（コスパが低い）だと考えています。そのため、ログイン時のみに「フィッシング耐性のある多要素認証」を導入し、出金時や出金先銀行口座の変更時などは、リスクベースの観点から OTP のような多要素認証で対応する、という運用は可能でしょうか。	ログイン時において、フィッシングに耐性のある多要素認証が実装されている場合には、不正アクセスのリスクは低減されることが想定されます。 しかしながら、その他のタイミングにおいてフィッシングへの耐性が相対的に低いと考えられる認証方式を用いることは望ましくないと考えられます。
36	【スタンダード】 ① 多要素認証	ログイン時に多要素認証が一度正常に完了したデバイスに対して、「このデバイスを 7 日間記憶する」などの形で、一定期間内に多要素認証を省略できる機能の提供は可能でしょうか。	ログイン時の都度、多要素認証を行う必要があると考えられます。
37	【スタンダード】 ① 多要素認証	多要素認証に関して、「（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）」が例示されておりますが、これらはフィッシングに耐性のある認証方法の例示であると思われます。この点、顧客が記入のうえ届出印を押印し金融商品取引業者に郵送した書面に基づく取扱いは第三者による改ざんの恐れがなく、「フィッシングに耐性のある」ものと考えら	本ガイドラインの記載をもって、出金先銀行口座の変更に関する書面による手続きを妨げるものではありません。インターネット取引を行うシステムに出金先口座変更を行う機能がなく、システム外での対応を行われている場合には、当該出金先銀行口座の変更は本ガイドラインの対象外となります。

項番	該当箇所	ご意見	考え方
		れます。つきましては、出金先銀行口座の変更について、書面に基づく手続きについてもお認めいただきたい。	
38	【スタンダード】 ① 多要素認証	フィッシングに耐性のある方法により出金先口座の指定が行われ、かつ、ログイン時に多要素認証を行っている場合には、顧客の意図しない出金がなされることはないと思われます。このように不正ログイン及び不正な手続きを防止できる場合には、利用者利便性を確保するために、出金時に多要素認証を行わないことをお認めいただきたい。	ログイン時において、フィッシングに耐性のある多要素認証が実装されている場合には、不正アクセスのリスクは低減されることが想定されます。 一方で、証券会社が複数の取引ツールを保有しており、その中に不正アクセス対策の水準が劣る取引ツールが含まれている場合には、ログインが行われてしまう場合が想定されます。それらの取引ツールによりログインが行われた場合でも、出金時に改めてフィッシングに耐性のある多要素認証が実装されていれば、仮に不正取引が行われた場合でも、出金が行われることは防げると考えられます。
39	【スタンダード】 ① 多要素認証	フィッシングに耐性のある多要素認証導入までの経過措置として、共通ショートコードもしくはRCS によるワンタイムパスワード等の導入し、認証強化を行うことを提案いたします。 【修正案】 「共通ショートコードや RCS によるワンタイムパスワード等を導入し、認証強化を行う。」を追加。 ・ 【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】 【理由】 パスキーをはじめとした認証手段導入までの経過措置・代替措置の不足しているため。	貴重なご意見ありがとうございます。
40	【スタンダード】 ② 顧客への通知	現代では多く使用される以下の手段も加えるか、より汎用的な記載に改めたほうが良いと考えます。 ・ Web Notifications API を用いたブラウザへの Push 通知	貴見のとおり、ブラウザやスマートフォンのアプリケーションへの通知についても、顧客への通知の送信先として考えられます。

項番	該当箇所	ご意見	考え方
		・　スマートフォンアプリケーションへの Push 通知 これらの設定機構が追加導入された際には、利用者への設定誘導を行うべきと記載すべきと考えます。	
41	【スタンダード】 ② 顧客への通知	顧客通知の対象が「不正なログイン・取引」「出金」「出金口座先変更」とあるが、下記のような事柄も対象に含めてよいのではないでしょうか。 ・多要素認証設定の変更・解除 ・通知先の変更（変更前の連絡先に変更されたことを通知する） ・アカウント・ロックの発生　など	貴見のとおり、顧客が自ら早期の被害認識を可能とするために、多要素認証の設定を変更・解除した場合や通知の送信先の変更、アカウント・ロックが発生した場合に、顧客への通知を行うことが考えられます。
42	【スタンダード】 ② 顧客への通知	「② 顧客への通知」 の対象として 「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」がありますが、こちらに「認証設定の変更」を加えてはいかがでしょうか？攻撃者が不正なログイン後に認証設定を変更した場合、その変更された認証設定を無効化しないと再度不正ログインが発生してしまう恐れがあるため、その他の通知対象と同様に重要な操作と考えております。	
43	【スタンダード】 ③ 認証に連続して失敗した場合のアカウント・ロック	**＜同様のご意見、ほか１件＞** ・　一定期間後に自動復旧しないアカウントロックを行ってしまうことは、フィッシングへの誘導として使用されかねないため避けるべきと考えます。 ・　ブルートフォースやそれに類するリスト型、スプレー型などの亜種での攻撃が現実的でない当人認証手段のみを利用者が行えるように設定したアカウントにおいては、当人認証失敗によるアカウントロック機構は不要であると考えます。	貴重なご意見ありがとうございます。 アカウント・ロックの解除については、不正アクセスの評価（リスクベース評価）に応じて行われるべき事項であると考えられます。 認証に連続して失敗した場合に、一定時間経過後に再度認証が行うことができるようにする仕様を設けることは妨げられない一方で、ログイン時の挙動に応じて、追加の本人確認を行うなどの対応が求められることになると考えられます。

項番	該当箇所	ご意見	考え方
		・　アカウントロックは、スプレー型攻撃などに無力であるため、Proof of Work を認証試行への予防策として用いるなど別の対策のほうが望ましいと考えます。 〈記載のない内容〉 ・　認証時だけでなく、その後の利用においても継続的に同一クライアントであることを保証するため、送信者照明が行えるセッション管理やアクセストークン管理を義務付けるべきであると考えます。(Device Bound Session Credentials や Demonstration of Proof-of-Possession といった仕様の採用を意図しています) ・　取引内容やその一部を用いた、トランザクションサイニングの実装やそれが利用者によって必須設定できる機構についても記載すべきと考えます。 ・　構成証明付きのアプリケーションでの取引を必須化するなどの、暗号学的な不正検出の仕組みを導入することを義務付けるべきと考えます。	
44	【スタンダード】 ④ 重要な顧客情報の窃取や改ざん防止	「重要な顧客情報」の対象として「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」と記載されているが、現行ガイドライン上は「メールアドレスや電話番号、出金口座、住所等」と記載されている。記載事項を変更している意図を確認させていただきたい。現行ガイドライン上は「電磁的方法により交付された法定書面に記載する情報を除き」とされているが、今回改正後のガイドラインでも考え方に変更がないことを確認させていただきたい	「住所」の変更については、犯罪収益移転防止法の本人確認に基づいて確認されるべき事項であり、当該箇所においては、それ以外の「重要な顧客情報」であると考えられるものを示しています。
45	【ベストプラクティス】	資産の重要性を考慮すれば、パスキー等による認証はそこまでの手間ではありません。また、長期的なスパンで取引するユーザーにとっては、認証に要する時間の間での価格の変動は	ご指摘のとおり、顧客の属性やフィッシングへのより強い防止策を求める顧客に対しては取引時におい

項番	該当箇所	ご意見	考え方
	①　フィッシングに耐性のある多要素認証	大きな問題ではありません。従って、重要な操作に限らず、個別の取引においても多要素認証の機能を提供すること自体は必須とするべきです。非常に迅速な取引を必要とするユーザーのみが、リスクを理解した上でオプトアウトできるようにすることが望ましいです。	てフィッシングに耐性のある多要素認証を設けることが考えられます。
46	【ベストプラクティス】 ①　フィッシングに耐性のある多要素認証	「①　フィッシングに耐性のある多要素認証の提供」において、「取引時において」 の記載については、【スタンダード】との違いをわかりやすくするための補足をしてはいかがでしょうか？「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に加えて、その他の取引時においても」など	貴重なご意見ありがとうございます。
47	【ベストプラクティス】 ①　フィッシングに耐性のある多要素認証	【ベストプラクティス】として、フィッシングに耐性のある多要素認証の実装化及び必須化に対する本人確認強化としての追加措置として、通信キャリアが提供する認証サービス等、確実な本人確認を実施している事業者との認証連携を提案いたします。通信キャリアが提供する認証サービスは、強固な所有物認証により、リアルタイム型フィッシング攻撃への耐性があり、安心・安全な多要素認証を実現いたします。 ■修正案 ・【ベストプラクティス】①フィッシングに耐性のある多要素認証の提供に以下を追加。 ログイン時、出金時、出金先銀行口座の変更時など、重要な操作時における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（デフォルトとして設定）にあたり、確実な本人確認を実施している事業者との認証連携（通信キャリアが提供する認証サービス等）を追加的措置として導入することが望ましい。 【理由】	ご指摘のとおり、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などのフィッシングに耐性のある多要素認証を導入するにあたり、厳格な本人確認が必要になると考えられます。

項番	該当箇所	ご意見	考え方
		パスキー等フィッシング耐性の高い認証方式を採用する場合には、確実な本人確認が重要です。そのため、パスキーでの新規初期登録・再設定（アカウントリカバリー）等に通信キャリアが提供する認証サービス等を連携して活用することが望ましいと考えます。	
48	【ベストプラクティス】 ② 取引等の制限	**＜同様のご意見、ほか１件＞** ・ 口座登録時に使用したWeb、取引ツール、アプリについて、デフォルトで使用しないに設定しておき、明示的に使用する設定に変えさせるようにすべきと考えます。 ・ 取引可能な商品やその金額についても、初期登録時には取引不可能な設定にしておくべきと考えます。 ・ これらの設定機構が追加導入された際には、利用者への設定誘導を行うべきと記載すべきと考えます。	貴重なご意見ありがとうございます。 ご指摘のとおり、顧客が提供を希望するサービスの範囲に応じた設定とすることが考えられます。 また、個社の状況に応じて、口座登録時に使用したWeb、取引ツール、アプリについて、デフォルトで「使用しない」に設定しておき、顧客が明示的に「使用する」設定へ変更するよう促す仕様とすることも考えられます。

（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

項番	該当箇所	ご意見	考え方
49	【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。とあるが、経営層への報告だけでは不十分であり、日本証券業協会が定めた項目＋αについては、日本証券業協会や監督省庁（金融庁）、マスメディアへの報告、利用者への情報開示も行うべきと考えます。	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の確認等について、外部への公表（マスメディアへの報告、利用者への情報開示）を行うことについては、フィッシング・不正アクセス等を行う者のターゲットになる可能性を排除できないため、各社における、これらの取扱いについては、各社の判断に委ねられると考えられます。
50	【スタンダード】	・ 今回の板取引を経由して攻撃者が利得を得る為の不正取引は、１つの証券会社が単独で把握可能な個人投資家の振る舞いだけではなく、板取引によって相対する別の証	貴重なご意見ありがとうございます。

項番	該当箇所	ご意見	考え方
	不正売買、不正出金等を防止・検知するための設定	券会社の注文状況と合わせた取引所全体の振る舞いから検知していく必要があるのではないでしょうか。 ・ また、実際に不正な利得を得ようとし、出口となりうる注文を待ち構えている犯罪者が多く参加している取引所は、その取引所の健全性そのものの信頼性が低く、グローバル市場においてマネーロンダリングが容易な市場と認知されかねないとも思います。 ・ 攻撃者から狙われにくくする、攻撃者へのインセンティブに対するコストを増やすということは、重要なセキュリティ対策の一環であり、一方的に入口となり得る証券会社の認証部分のみに対策を絞ることは、足並みを揃えられない抜け道を常に攻撃者が探索するというモチベーションにもなりかねないと思います。 ・ 不正売買を検知する仕組みについては、証券会社だけでなく取引所も含めた業界全体での情報のやり取りや、薄商いとなりやすい上場企業の基準の見直し等、トレードライフサイクル全体を俯瞰した対策に繋がるような対策を検討すべきではないでしょうか。	
51	【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）	・ 不正売買、不正出金等を防止・検知するための設定の例示として「上記（２）①・②・④」が挙げられる中で「③（認証に連続して失敗した場合のアカウント・ロック）」が明示的にスタンダードから抜かれている、ということの根拠が不明確かと思います。 ・ 認証に連続して失敗した場合のアカウント・ロックというのは、証券口座に限らず一般的な認証システムとしては標準的な機能であり、また他の ① ② ④と比較しても実装難易度は低いと考えられます。	「認証に連続して失敗した場合のアカウント・ロック」については、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していることから、本ガイドラインにおいて顧客の利用状況の確認を行う対象ではないと考えられます。

項番	該当箇所	ご意見	考え方
		・　この記述において「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」の明示的な対象外となることへの合理性が低く、混乱を招く要因であると考えられる為、この整理については見直すべきではないでしょうか。	
52	【ベストプラクティス】	一般的に指標値は、期限と目標値ではなく、集計粒度と期間と上限下限と目標値を設けて設計すべきものと考えます。また、これらの目標値監視は、通常の KPI の考え方と同様に、上位団体や組織が定めたものを、現場に近づくにつれてより厳しくなるように段階的に設定していき、関係するすべての階層で適切であることを確認すべきものと考えます。 （厳しさが、監督省庁（金融庁）＜日本証券業協会＜証券銀行経営層＜証券銀行現場層となるような姿をイメージしています）	貴重なご意見ありがとうございます。 各社においてインターネット取引の利用状況・顧客数が異なるため、一律の指標値を設けることは難しいと考えられます。 また、指標値の設計についても、各社の規模・顧客数などの状況に応じた任意のものとすることが適当であると考えられます。
53	【ベストプラクティス】	顧客が自身の希望に応じて、任意に適用するセキュリティ対策については目標を定める必要はないという理解でよいか。 （Ⅳ．１．（２）①はパスキー必須化のため目標を設定する意義はあると考えるが、（２）②・④はあくまで機能の提供であるため。）	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の指標値については、各社で判断の上、確認を行うことが適当であると考えられます。

２．自社システムにおける脆弱性対策及び情報管理

（２）情報管理

項番	該当箇所	ご意見	考え方
54	【スタンダード】 ①	・　暗証番号、パスワードがあたかも暗号化すれば扱ってよいように読み取れてしまうため、記載を改めるべきと考えます。クレデンシャルとそうでない機密情報は明確に分けて記載すべきと考えます。	貴重なご意見ありがとうございます。

項番	該当箇所	ご意見	考え方
		・ 暗証番号、パスワードなどクレデンシャルはそもそもできるだけシステムで扱わないことが基本であると考えます。 ・ 暗証番号、パスワードについては、単にハッシュ化すればよいのではなく、暗号学的に十分にソルト、ペッパー、ストレッチングを行う必要があるためその旨の記載が必要であると考えます。	
55	【スタンダード】 ②	・ 取引記録・保有資産残高情報の漏えい防止・管理強化策の具体的な例を記載していただきたいです。 ・ 現代では、家計簿アプリなどを用いた、個人や家族の出納管理を行うことは一般的になりつつあると考えます。これらのような外部のアプリに渡す権限の制御が利用者によって行えないことは、当該情報の漏洩の温床になりかねないと考えます。	貴重なご意見ありがとうございます。
56	【スタンダード】 ②	当社の商品は株式や債券のように日常的な取引が発生するほどの流動性がありません。また、商品を購入できるタイミングも限定的です。このような商品特性やリスク状況を考慮すると、本件をスタンダードとして示されていても対応しない判断は可能でしょうか。なお、取引状況の把握という脅威への対策以外の目的（例：個人情報管理、災害対策など）での管理は実施しており、あくまでも「不正アクセスによる顧客の取引状況の把握」に関するスタンダードについて対応不要か確認しています。	本事項については、スタンダードとされており、対応が求められる事項であることから、各社の状況に応じた適切な情報管理を行うことが求められます。
57	【スタンダード】 ③	流出による外部での悪用（ディープフェイクの基にするなど）を利用者が避けるため、流出時には身元確認書類として意味をなさない暗号学的に安全な手段のみを用いて、身元確認が	貴重なご意見ありがとうございます。

項番	該当箇所	ご意見	考え方
		行えるように利用者が選択できる手段の提供を義務付けるべきと考えます。	

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

項番	該当箇所	ご意見	考え方
58	__	顧客の機密情報（暗証番号、パスワード等）がインターネットで公開されていないかの確認（脅威インテリジェンス）なども、ベストプラクティスとして追加してもよいかと考えます。	貴重なご意見ありがとうございます。

（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

項番	該当箇所	ご意見	考え方
59	【スタンダード】	・ そもそも多段階での委託を原則として制限すべきと考えます。共同利用型システムを利用してサービス提供するなど、正当な理由が存在する場合でも、何段階まで許容するか明示することを義務付けるべきと考えます。 ・ 脆弱性対応状況、新たな脅威に対するセキュリティ対策の追加実施状況など、経年劣化の要素を含むものの包括的なサプライチェーンマネジメントの実施も義務付けるべきと考えます。	貴重なご意見ありがとうございます。
60	【スタンダード】	・ 追加で最小権限の原則に触れてもよいかと考えます。外部委託先には運用に必要な最低限のシステム権限しか与えないことなど。	貴重なご意見ありがとうございます。

４．フィッシング詐欺等被害未然防止のための措置

項番	該当箇所	ご意見	考え方
61	【スタンダード】 （１）	DMARC ポリシーは「reject」に設定することが必須となるのでしょうか。また、「quarantine」に設定した場合、法令遵守上の懸念が生じるという意味でしょうか。DMARC の進捗状況は公表する必要がありますでしょうか。	DMARC ポリシーは、最終的に「reject」に設定することが求められます。 一方で、DMARC ポリシーは段階的な強化が行われることが一般的であることから、ポリシーが「quarantine」に設定される状況もあることが考えられ、その状況において法令遵守上の懸念が生じるということはありません。 なお、DMARC の進捗状況についての公表は必ずしも求められるものではありませんが、各社の判断で、自社で行うフィッシング対策について公表することは、問題がないと考えられます。
62	【スタンダード】 （１）	送信ドメイン認証「DMARC」のポリシーは「拒否」が必須となっていますが、「拒否」必須化となれば DKIM の公開鍵暗号は非常に長い鍵長の RSA 暗号が有力となります。DKIM で RSA 暗号以外の公開鍵暗号を設定すると、メールを受ける側も、その新しい公開鍵暗号を購入する必要があるため。現在は、いろいろ新しい公開鍵暗号を試している段階なので、とても全員が全部を購入しきれません。オープンソースだから問題ないという意見もありますが。 フィッシング対策にパスキーは高い効果がありますが OS を起動不能にする攻撃に非常に弱い。Yahoo! Japan でもパスキーを喪失した場合、SMS となり原則禁止のワンタイムパスワードを利用しています。OS 起動不能は CPU のバグや OS のアップデートミスで一斉に発生する場合もあり警戒すべきだと思われます。	貴重なご意見ありがとうございます。

項番	該当箇所	ご意見	考え方
		一般人がパスキーで安全に運用することは難しいため、パスキーではオンライントレードの市場が無くなる可能性もあります。そこで各社専用の認証ハードを必須とすべきです。運用が簡単でしかも安全です。 認証専用ハードの必須化の指針を出して、メーカーが安心してハードを開発できるようにする政策を考えていただければと思います。そして次期マイナンバーカードや、DKIM アクセラレータの開発コスト低減を考えた総合的な政策となるように。認証ハードの半導体製造メーカーに株価下落のタイミングで認証専用ハードが起動しないなどの問題が起きないように抑える必要があります。 １台のハードで複数社に対応する認証ハードより、各社専用の認証ハードになれば、半導体チップの数が出るので製造コストが下がるように思います。また運用が簡単であるメリットも大きいと思われます。電卓型アイドル認証端末は電池不要のため製造コストが安く、対応年数も 10 年以上にできる可能性があり、トータルコストでは安くなります。 また７セグ文字「錦」の発明により、液晶ディスプレイを安価な７セグ液晶にできるだけでなく、液晶のドライバチップの削減効果もあります。基板の部品点数が少なくなる効果もあるので、製造コストが下がると思います。 認証ハードの音声 I/F はオプションです。実際のハードでは無くてもフィッシング耐性はあります。ただし SSL サーバ証明書をコピーされた偽サイトには効果がありません。これは音声 I/F オプションの実装で対策されます。 認証ハードが販売されるまでの間は、オンライントレードを控えることが良いと考えますが、Windows のパスキーと無料のア	

項番	該当箇所	ご意見	考え方
		イドル認証アプリを併用する方法もあるように思われます。アイドル認証アプリにフィッシング耐性はありますが、余ったWin10 PCにWin10をクリーンインストールできない人も、多くいそうです。ただしアイドル認証アプリで被害を被っても、一切の責任を負わないこと、予めご了承下さい。	
63	【スタンダード】 （２）	**＜同様のご意見、ほか１件＞** 共通ショートコードの利用を求めるのは、SMS 認証を利用する場合に限定すべきではないか。フィッシング対策協議会の月次レポートでも、以下のように利用方法を限定した記載をしており、これと同様の記載がよいのではないか。″「SMS 認証併用の際にはスミッシング対策として、「0005」で始まる国内モバイルキャリア共通の SMS 発信用の共通番号（共通ショートコード）等を使う、正規メッセージには URL は記載しない、認証コードのメッセージにその用途や本物の入力画面照合のためのキーワードを記載する等を検討」″ 【理由】 共通ショートコードは主にスミッシング対策と考えており、URLのないログイン通知等のみに利用する場合には、必要性が低いと考える。	ご指摘のとおり、共通ショートコードの利用がスタンダードとして求められるのは、SMS を利用する会社に限定されます。SMS の利用実績あるいは利用予定がない場合には、共通ショートコードを取得する必要はありません。
64	【スタンダード】 （２）	【意見】 共通ショートコード利用は、【スタンダード】ではなく、【ベストプラクティス】に位置付けるのが適切ではないか。 【理由】 共通ショートコードはスミッシング対策として一定の効果が期待できる手段ではあるものの、現時点でこれを【スタンダード】の位置づけとして全証券会社に標準的対応として求めることに	ご指摘のとおり、共通ショートコードの利用がスタンダードとして求められるのは、SMS を利用する会社に限定されます。SMS の利用実績あるいは今後も利用予定がない場合には、共通ショートコードを取得する必要はありません。 また、証券会社各社がウェブサイト又はアプリケーション等で共通ショートコードを公開し、顧客

項番	該当箇所	ご意見	考え方
		は疑問を感じる。共通ショートコード（0005 で始まる送信元番号）がフィッシング対策に有効であるためには、受信者がその番号を確認し、正規メッセージであると判断する行動様式の定着が前提だが、現時点でその仕組みを理解している一般消費者は非常に限定的であり、短期的な実効性は乏しいのではないか。中長期的に普及や啓発を進めたとしても、「送信元番号からメッセージの信頼性を判断する」という行動様式は一般に定着しづらく、十分に理解・活用できない利用者が一定数存在することが想定されるため、期待どおりの効果が得られない可能性も高いと考える。共通ショートコードの取得・運用には金銭的負担および導入・運用にかかる工数的コストが発生するが、期待される効果に対してコストが過大である懸念もあり、現段階で全証券会社に対してスタンダードとして求めることは時期尚早ではないかと考えている。	に対して周知・普及を行うことで、顧客への認知を広める必要があると考えられます。
65	【スタンダード】 （２）	【スタンダード】として、共通ショートコード照会サイトへの掲載を提案いたします。 ■修正案 ・【スタンダード】(2) を修正 （２） 共通ショートコードを利用し、通信キャリアが公開した Web サイト（https://japansms.com/）に当該共通ショートコードを必ず公開し、Web サイト上又はアプリケーション上等にも公開する。 【理由】 共通ショートコードの認知訴求媒体が追加され、受信者は安全な送信元の判別がしやすい状態となるため。	貴重なご意見ありがとうございます。 共通ショートコードを利用する証券会社は、通信キャリア４社（KDDI／docomo／SoftBank／楽天モバイル）が公開しているウェブサイト「SMS 共通番号/共通ショートコード情報」に通信キャリア審査済である共通ショートコードを掲載することも考えられる対応の一つになると考えられます。
66	【スタンダード】 （３）	自社を騙るフィッシングサイトについてのパトロールも義務化すべきと考えます。	「アクセス制限のためのテイクダウン（閉鎖）」を行うために、顧客や外部等からの報告による受

項番	該当箇所	ご意見	考え方
			動的な対応のみならず、自社においてテイクダウンのアプローチ方法（自社、社外事業）を定めることも考えられます。
67	【スタンダード】 （４）	可能な限り一社もしくは一ブランドで一つのドメインのサブドメインを使用し、キャンペーンなどで不用意な eTLD+1 の取得を行ってはならない旨記載すべきと考えます。	ご質問の趣旨が必ずしも明らかではありませんが、各社が用途に応じたドメインの取得を行うこと自体は妨げられるものではありません。 一方で、ドメインの不適切な管理は、フィッシングサイトへの転用など悪用につながる恐れがあることから、適切な管理が求められます。
68	【スタンダード】 （５）	**＜同様のご意見、ほか２件＞** かつて利用されていた「EV 証明書」の無効性や弊害が指摘されている中で、「真正なウェブサイトを証明する方法」で想定される方法を具体的に例示いただきたい。以前は EV 証明書が利用されていたが、現在では、以下を理由として主要ブラウザのアドレスバーでの EV 証明書の組織表示は行われていない ・EV 証明書が利用者に対するセキュリティに効果がないこと ・EV 証明書の表示により安全だと誤認させることの弊害やそれを悪用した攻撃が可能であること ・スマホブラウザの少ない表示領域に表示するものとしてドメイン名の方が適切であるとの判断 また、フィッシング対策ガイドライン（フィッシング対策協議会）でも、2023 年度版から「EV 証明書」の記載は削除され、より具体的な施策としては、４.（４）に含まれる以下を挙げるに留められている ・ドメイン名の適切な管理 ・サブドメインテイクオーバーやドロップキャッチの対策 ・利用者へのドメイン名の周知	ご指摘のとおり、利用者が正規の証券会社のウェブサイトとフィッシングサイトを判別するための対策としての EV SSL 証明書の表示は、現在においては、ウェブサイトの真正性の判断とは異なるアプローチであると想定されます。ご指摘を踏まえて、削除することといたします。 一方で、利用者が正規の証券会社のウェブサイトからログインしていただくための対策は必要であり、利用者にはドメイン名などを使ってあらかじめ正規のウェブサイトであることを確認いただいた上でブックマークしていただくこと、スマートフォンの場合には、正規のアプリをオフラインなど偽装されにくい手段で案内し、必ず利用いただくことなどの対策が考えられることから、「７．その他（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」に当該事項をスタンダードとして追記いたします。

項番	該当箇所	ご意見	考え方
69	【スタンダード】 （６）	「(法令に基づく義務を履行するために必要な場合等を除く)」とあるが、ログイン画面へ直接遷移をさせない URL の記載（例えば、ログインボタンを有するビジターページの URL 記載など）は問題ないとの理解で良いか。	ご質問の趣旨が必ずしも明らかではありませんが、インターネット取引を行うツールにパスワードを入力するページに遷移するログインリンクを記載することはできないと考えられます。
70	【スタンダード】 （６）	メールや SMS 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ことがルールとされ、その例外として、法令に基づく義務を履行するための場合など代替手段をとり得ない場合と記載がされていますが、多要素認証を導入済の金融機関の場合、万一パスワードを取得されたとしても、ログインされることはない認識のため、例外事項の対象に『多要素認証を導入済のログインリンクを送付する場合』を追加いただきたい。	ご質問の趣旨が必ずしも明らかではありませんが、フィッシングに耐性のある多要素認証の実装が完了した場合でも、インターネット取引を行うツールにログインを行うことができるパスワードが存在する、あるいはパスワードの取得ができる状況にある顧客がいる場合には、URL・ログインリンクを記載することはできないと考えられます。
71	【スタンダード】 （６）	メールや SMS 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ことがルールとされ、その例外として、法令に基づく義務を履行するための場合など代替手段をとなり得ない場合と記載がされていますが、例外事項の対象に『お客さまが取引先の金融機関からログインリンクが送付されてくることを認識済の状況で送付する場合』を追加いただきたい。 ＜具体的なシチュエーション＞ ・お客様と有価証券の募集について電話で会話し、目論見書交付のためのログインリンク（目論見書交付ページへのリンク）を送付する旨を伝えたうえで送付。 ・お客様とサービスの申込、住所や氏名の届出事項の変更といったお客様が必要な手続きについて電話で会話し、その意向を確認したうえで、手続きを行うための Web ページへのログインリンクを送付。	ご指摘の事項である、目論見書交付については、法令に基づく義務を履行する行為に該当すると考えられます。また、顧客の状況に応じてサービス提供にあたり代替的手段を採り得ないと判断されている場合には、URL・ログインリンクを記載することは問題がないと考えられます。

項番	該当箇所	ご意見	考え方
72	【スタンダード】 （６）	SMS への URL 記載を禁止するのではなく、URL 記載方法の指針を提示することを提案いたします。次に記載する修正案は、現在総務省及び通信４キャリアで策定中の SMS 配信ガイドライン（案）より引用しております。 ■修正案 ・【スタンダード】(6) を修正 （６）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する場合は、アクセス先が識別可能なものとすること。例として、ドメイン名から利用企業を識別できるなどがある。また、短縮 URL を利用する場合は、アクセスが安全なものであることを担保すること。 【理由】 SMS への URL 記載を禁止した場合、電子通知の代替手段がないため。	ご質問の状況が必ずしも明らかではありませんが、本ガイドラインにおいては日常業務において SMS への URL の記載そのものを禁止しているわけではなく、特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こととしています。
73	【スタンダード】 （６）	営業やアンケートなど日常業務に必要なリンクがなくなった場合、投資家からの要望や質問を受け付けられなくなるなど、顧客本位の観点からも大きな影響が懸念されます。不正アクセス対策は必要ですが、リンクを掲載しつつ「※フィッシング等にご懸念がある場合は、ログイン後の〇〇＞〇〇からご確認ください」と併記して注意喚起するなどの代替的措置は可能でしょうか。あるいは、フィッシング耐性のある認証方式をデフォルトにすることで、代替的措置とすることは可能でしょうか。	ご質問の状況が必ずしも定かではありませんが、営業やアンケートなど日常業務において、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方法で対応いただくことを求めております。

項番	該当箇所	ご意見	考え方
74	【ベストプラクティス】②	現時点でS/MIMEの普及度・認知度が高いとは言えず、これから改善する見込みも薄いです。現時点ではS/MIMEに頼るしかないとしても、別の手段の検討を急ぐべきと考えます。たとえば、取引アプリに一本化し、あらゆる通知・連絡はアプリでのみ行い、メールは一切使わないという選択肢を検討していただきたいです。	貴重なご意見ありがとうございます。 今後、検討を行う際の参考とさせていただきます。
75	【ベストプラクティス】②	現状、S/MIMEをサポートしていないメールサービス、メールアプリ、メーラーが多く存在すると考えます。また、デフォルトでは使えないメーラーもあります。 そういった方々がメールを受信した場合、メールが安全であると根拠なく思いこまれたり、誤解する可能性があり、フィッシング攻撃者がこの状況を利用して、偽のメールを送信することも考えられます。 例えば、攻撃者がS/MIMEを使用していると偽って、受信者に対して「このメールは安全です」と主張することで、リンクをクリックさせたり、個人情報を入力させたりすることが考えられます。 従って、S/MIMEについてのリテラシー向上を伴った施策や広く利用できるような働きかけが望めない場合は逆にリスクになると考えました。 リテラシーの問題はとても大きいと思い、その点を強く補記頂く等して頂きたく、コメントさせて頂きました。	
76	—	【ベストプラクティス】として、RCSを利用して送信元が安全であると判別できる状態とすることを提案いたします。 ■修正案 ・【ベストプラクティス】に新規追加	

項番	該当箇所	ご意見	考え方
		RCS（リッチコミュニケーションサービス）を利用し、メッセージ画面の認証済み表記により送信元が安全であると判別できる状態とする。 【理由】 RCS を利用することで、メッセージ画面に表示される企業ロゴや認証済み表記により送信元が安全であると受信者が判別可能となるため。	
77	―	【ベストプラクティス】として、メール/SMS への URL 記載禁止の代替手段として、RCS のボタンを利用することを提案いたします。 ■修正案 ・【ベストプラクティス】に新規追加 RCS（リッチコミュニケーションサービス）を利用し、パスワード入力を促すページの URL やログインリンクは、本文に直接記載するのではなく、メッセージ内のボタンからアクセスできる状態とする。顧客に対し、RCS のボタンから Web サイトにアクセスするよう周知を行う。 【理由】 メール/SMS への URL 記載を禁止する場合、電子通知の代替手段を用意すべきと考えます。受信者に対し、RCS のボタンから Web サイトにアクセスするよう周知を行うことで、不審な URL のクリックを抑止することが可能となります。	

５．モニタリング

項番	該当箇所	ご意見	考え方
78	【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	・　DBSC や DPoP などを用いた暗号学的な不正挙動の検出についても記載すべきかと考えます。 （記載のない内容） ・　取引に関するふるまい検知も行うべきと考えます。 ・　システム全体での各種メトリクスを用いたふるまい検知も行うべきと考えます。	貴重なご意見ありがとうございます。 今後、検討を行う際の参考とさせていただきます。
79	【スタンダード】 （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た追加の本人認証については、以下のような対応で十分という理解で良いか。 ・　モニタリングの結果､不正アクセスが疑われるケースでは、本人に電話し不正アクセスの有無を確認。電話でのコンタクトができなかった場合はログイン規制等を実施、規制解除にはコールセンターに電話するようにメールで案内 ・　コールセンターに電話があった際に､発信電話番号や氏名、住所、生年月日等により本人確認を実施の上、ログイン規制を解除、不正アクセスの有無を確認	電話による「追加の本人認証」を想定されている場合に、それらが適切な方法であるかは個別の事象により判断されることとなりますが、顧客の本人確認及び本人自身の行為であるかを十分に確認する必要があると考えられます。
80	【ベストプラクティス】	「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」という表記になっていますが、実際は検知した後の対応が必要なこともガイドラインに記載すべきと考えます。例えば、ログイン後の挙動の分析について、リスクの高い振る舞い（高額の銀行口座からの入金、特定株式の高額購入、認証情報の変更等）を検知した場合は操作を受けつつ処理を「保留」とし、別途本人に意図した操作か確認した後に処理を「実行」できる運用をとるなど。	貴重なご意見ありがとうございます。 なお、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対応については、本ガイドライン「Ⅳ．６．不正アクセス発生時等の対応」に記載しております。

項番	該当箇所	ご意見	考え方
81	【ベストプラクティス】	本件の起因であろう情報詐取型のマルウェア検知を証券企業側からの提供機能にて行うことも加えるのが好ましいです。その理由は次の通りとなります。 パブリックコメントへの記載にもあります不正なログインの要因となるフィッシングに関しては、フィッシングに耐性のある多要素認証の提供やフィッシングサイトのテイクダウン、DMARC等の送信ドメイン認証技術の計画的な導入を行うとありますが、マルウェアに関しては利用者に対応を任せる注意喚起にとどまっているように見受けられます。利用者側による対応はコントロールする事が難しいため、証券企業側からも可能な範囲で、情報詐取型のマルウェア検知を行えるようにするのが好ましいです。	貴重なご意見ありがとうございます。 今後、検討を行う際の参考とさせていただきます。

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

項番	該当箇所	ご意見	考え方
82	【スタンダード】	不正取引が発生した場合、このガイドラインのベストプラクティスに満たないセキュリティで運用されていた場合は、証券会社はセキュリティ上の落ち度につき責任を持つべきです。そのくらいの真剣度での対応をお願いします。	貴重なご意見ありがとうございます。

（３）関係機関への報告・連携強化

項番	該当箇所	ご意見	考え方
83	【スタンダード】	不正取引が発生した場合、このガイドラインのベストプラクティスに満たないセキュリティで運用されていた場合は、証券会	貴重なご意見ありがとうございます。

項番	該当箇所	ご意見	考え方
		社はセキュリティ上の落ち度につき責任を持つべきです。そのくらいの真剣度での対応をお願いします。	
84	【スタンダード】 ①　金融当局への報告	6（3）【スタンダード】①で、「速やかに当局に報告を行う」とあります。ここで言う「報告」が、同時に金融庁でパブコメされている監督指針（Ⅲ-2-8-2-3（1））で示す「犯罪発生報告書」を指すのか、それ以外のものなのか等が不透明と思われます。同じものであれば特定した方が明確でよろしいと思います。	ご認識のとおり、「金融商品取引業者等向けの総合的な監督指針」で示されている犯罪発生報告書については、金融当局へ速やかに報告を行うための様式の一つとなります。 当該箇所は、「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。」と記載を修正いたします。
85	【スタンダード】 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	フィッシング詐欺等被害未然防止策として、「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」による各社から日本証券業協会に報告された情報は、不正取引の発生状況・銘柄等、遅滞なくネット取り扱い証券会社に共有していただきたく、ご検討くださいますようお願い申し上げます。	ご指摘の事項である、不正アクセス・不正取引等に係る証券会社間での情報共有・連携については、必要に応じて今後の検討事項とさせていただきます。
86	【スタンダード】 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	今般の証券口座の乗っ取りと不正売買の多くは、複数の証券会社の証券口座を乗っ取った上で、それらの証券会社を跨った不正な売買が行われ不正に利益を獲得していると認識していますが、最も問題なのは証券会社の顧客である「真」の顧客が気付かない状況下で当該不正行為が行われていることです。 こうした状況への対処方法として、「身に覚えがない第三者によるログイン・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「真」の顧客への通知を求め、不正売買の有無を「真」の顧客に判断してもらうとされていること(Ⅳ.1.(2)②)は一定の効果があると考えられますが、これとは別に、各証券会社自らの「モニタリング」(Ⅳ.5.)として、身に覚えがない売買注文・約定等の不正売買等を抽出・検知・分析することが必要かつ適当であり、責務があるとの観点から、各証券会社自ら	貴重なご意見ありがとうございます。 現在、証券会社においては、日証協の自主規制規則である「不公正取引の防止のための売買管理体制の整備に関する規則」に基づき、売買審査等が行われております。 これらの規則とは別に、証券会社における規則・ガイドラインなどが必要であるというご意見がある場合には、その内容を精査し、必要に応じ、今後検討いたします。

項番	該当箇所	ご意見	考え方
		が取引所有価証券市場における各銘柄の売買注文・約定等が異常なものであるかどうかについて、できるだけ早い抽出・検知・分析を行い、「不正アクセス発生時等の対応」（Ⅳ.6.）として、異常性をベースに不正売買の疑いがあるなど必要な場合はできるだけ早く、当該「真」の顧客に報告するとともに、金融当局及び市場関係者（取引所、日本証券業協会等） にも報告し複数の証券会社からの報告を総合的かつ迅速に分析・審査するという監視体制の構築もスタンダードの対応として重要であると考えますが、どうでしょうか。	

7．その他

（1）社内教育

項番	該当箇所	ご意見	考え方
87	―	最近、ブルーチーム演習として、実際に攻撃を受けた際の SOC から経営層までの事故対応演習のご依頼をよくいただきます。内容としては、ペネトレーションテストやレッドチーム演習などで模擬的な攻撃テストを実施した際に合わせて SOC 側のブルーチーム演習も行うものから、机上でのシナリオベースの訓練までございますが、教育のベストプラクティスとして追加されるのはいかがでしょうか。	ご指摘のとおり、サイバー攻撃・予測される事故等について対応演習を行うことは、インターネット取引における不正アクセス・不正取引等の対策にとどまらず、自社システムに対する包括的なセキュリティ対策の一環として有効な手段であると考えられます。 ご指摘を踏まえて、攻撃を想定した演習の実施について、社内教育に関するベストプラクティスとさせていただきます。

（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

項番	該当箇所	ご意見	考え方
88	―	顧客へ周知・注意喚起するべき事項として、「利用する証券会社のウェブサイトへのアクセスは、事前に正しいウェブサイトのURL をブックマークに登録しておき、ブックマークやアプリからアクセスすること」を、スタンダードとして追加してはいかがでしょうか。	ご指摘のとおり、証券会社が顧客へ周知・注意喚起するべき事項であると考えられることから、「７．その他（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」においてスタンダードとして追加させていただきます。
89	【スタンダード】 ④	「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）」について、ログイン画面等の顧客が必ず遷移する画面において、画面上の面積を十分に大きく占める注意喚起バナーを表示し、強制的に視認させる対応で不足はないか。画面の遷移をシステム制御するような対応や、顧客の確認状況等を記録する機能までは求められていないことを確認したい。	本項目は、顧客が「お知らせ・注意喚起等を確実に確認する」ことが目的であり、「画面上の面積を十分に大きく占める注意喚起バナーを表示し、強制的に視認させる」という方法を取ることも、一つの手段であると考えられます。 なお、顧客の確認状況等を記録する機能の実装を想定するものではありません。
90	【スタンダード】 ④	ここで指す「次の動作・画面」が具体的に何を意図しているのか確認したいです。この措置は取引を行う利用者のリテラシー向上に役立つ可能性がありますが、「投資に興味だけを持っている利用者」が商品性を確認する際には障壁となるおそれがあります。科学的研究によれば、認知負荷が増えると活動の成功率が低下することが証明されています。 多くの事業者がこれを実装した場合、投資活動全体が低下し、貯蓄から投資への資金移動を抑制してしまう可能性があります。例:https://pubmed.ncbi.nlm.nih.gov/16646695/ 現在、「次の動作・画面」という表現は曖昧さが残りますが、これは例えば取引画面など投資家本人にとってリスクの高い行動	ご指摘の趣旨が必ずしも明らかではありませんが、証券会社からの重要なお知らせや注意喚起については、顧客に対して必ず確認を経る対応が必要であると考えられます。

項番	該当箇所	ご意見	考え方
		に入る前に確認を求めるということを意図しているという理解でよろしいでしょうか。	
91	【スタンダード】 ⑤	「顧客からの届出を速やかに受け付ける体制を整備」との記載について、「問い合わせに対して速やかに回答する体制」まで求めるものではないという理解で合っているか、確認したい。 【理由】 「顧客からの届出を受け付ける体制」の整備は課題と認識している。たとえば、24h/365d で顧客からの届出・問い合わせをチャットボット等によりまずは受け付け、システム的に回答・反映可能な事項等はシステム的に処理を行うことを想定している。このような対応で題意を満たすものであるか、為念確認したいもの。	「顧客からの届出を速やかに受け付ける体制」については、サービスの内容、顧客数や日々の問い合わせ状況等に応じて整備されるものであると考えられます。 なお、「問い合わせに対して速やかに回答する体制」については、問い合わせの内容ごとに回答に要する時間や対応内容は異なるものであると考えられることから、顧客からの問い合わせについては、その内容を踏まえて適切にご対応いただきたく存じます。

（３）銀行口座との連携サービス

項番	該当箇所	ご意見	考え方
92	―	（３）銀行口座との連携サービスにおいて、フィッシングに耐性のある多要素認証の提供をすることは、ベストプラクティスではなく、スタンダードのレベルではないか。 ＜背景・理由等＞ 金融庁からの要請においては、特にスイープ機能についての認証強化が証券・銀行の両方に求められています。銀行によっては仕組み上、認証追加が困難なケースが想定されており、証券側での対応が期待されております。	ご指摘のとおり、銀行との連携サービスにおいて、フィッシングに耐性のある多要素認証を提供することも対応の一つであると考えております。 一方、顧客によっては、現金を証券口座には預けず、取引の都度、自動で取引に必要な現金を銀行口座から入金したいというニーズがあります。 その際、予め定時定額で行う取引もありますので、例えば、証券口座へ入金する都度、認証を行うとした場合、不都合が生じることもあると考えられることから、ベストプラクティスとしました。

項番	該当箇所	ご意見	考え方
93	【スタンダード】 ①	「新規に預金口座と連携する顧客に対しては、証券口座の認証のみで預金引き出しが可能」と記載されているが、これは「銀行口座での認証を経て新規の連携の登録完了後は、証券口座の認証のみで預金引き出しが可能」という趣旨で相違ないか。明確化のために修正を検討いただきたい。	ご指摘の認識で相違ないと考えられることから、当該箇所の記載について、ご指摘を踏まえて修正いたします。
94	【スタンダード】 ①	「銀行口座との連携サービス」の具体的な定義について明確にしていただきたいです。例えば、 https://www.billingsystem.co.jp/service/quick/ のような「リアルタイム入金確認」サービスは該当するのでしょうか。あるいは https://www.sevenbank.co.jp/support/apiCollaboration/ のような「口座連携サービス」を指しているのでしょうか。 後続の項目を確認すると、「証券口座の認証のみで預金引き出しが可能」な機能が本文における「銀行口座との連携」を指していると考えられます。この場合、「口座連携サービス」のみが該当するという理解でよろしいでしょうか。前者（リアルタイム入金確認）については「銀行振込を 24 時間リアルタイムでご通知」するもので、投資家が直接的に連携していないので該当しないと考えておりますが、念の為確認です。また、具体的にどのように連携するのでしょうか。契約がある前提で、情報連携をするのでしょうか。	「他の銀行口座との連携サービス」について具体的には、取引時に自動で銀行口座から証券口座へリアルタイムで資金移動を行うサービスが考えられます。
95	【スタンダード】 ①	ここで言う「認証強度を確認する」とは何か。「認証強度」の定義と、「認証強度を確認する」としている確認内容を明確/具体的に示していただきたい。	「預金口座からの出金に係る認証強度の確認」とは、預金口座から証券口座への出金（資金移動）がどのような認証が設けられているか、その認証によって不正な資金移動がどの程度抑止できるかの確認を行うものと考えられます。

項番	該当箇所	ご意見	考え方
96	【スタンダード】 ②	「責任・役割分担を明確化する」は、銀行と証券会社との間で被害発生時の補償割合の詳細を事前に取り決めることまでを求めているものではない理解で良いか。また、今後も新たな手口などが発生し得ることを踏まえると、実際に被害が生じた場合には個別の発生事象に応じて対応が必要と想定されるため、現時点の手口を元に具体的な責任や役割分担を明確化することはかえって将来的な被害発生時の被害対応の足枷となり得る可能性が考えられる。そのため、現時点においては、被害発生時の連絡体制・協力体制を確立するに留め、具体的な責任・役割分担は個別の事象に応じて対応していくのが適切と考えるがいかがか。	本ガイドラインは補償について定めるものではなく、セキュリティ水準等について定めるものであり、銀行と証券会社との責任・役割分担についてもセキュリティホールができないようにそれらを明確化することを求めているものです。ご指摘のとおり、被害が発生した場合の対応は個別の事象に応じて対応していくことが適切であると考えられます。
97	【ベストプラクティス】	「他の銀行口座との連携サービス」とは、以下のいずれを指しているものか確認したい。 ①取引時に自動で銀行口座から証券口座へリアルタイムで資金移動を行うサービス ②口座振替契約を事前に締結し、都度、顧客の指示に基づいて銀行口座から証券口座へリアルタイムで資金移動を行うサービス ③口座振替契約を事前に締結し、月１回などの頻度で銀行口座から証券口座へ定期定額の資金移動を行うサービス（リアルタイムでの任意の預金の移動が行えないもの）	「他の銀行口座との連携サービス」について具体的には、取引時に自動で銀行口座から証券口座へリアルタイムで資金移動を行うサービスが考えられます。

○ ガイドライン全体に対するご意見など

項番	ご意見	考え方
98	インターネット取引の定義について教えて頂きたい。	本ガイドラインにおけるインターネット取引とは、インターネット等の通信手段を利用した非対

項番	ご意見	考え方
	具体的には、有価証券取引や入出金等が該当するのは疑いの余地はないと思うが、例えば、顧客が自身の残高情報をインターネットで確認できるようなサービスのみをオンラインで提供している場合、それはインターネット取引には該当しないという理解でよいか。 該当性の有無にかかわらず、ガイドラインを踏まえた対応を考えていきたいと考えているが、他方で、上記のような場合においても直接適用されるものかどうか整理したい。	面の取引を前提としており、それ以外のサービスを対象とするものではありません。
99	【スタンダート】とされている事項についてはいつまでに実装されることを想定して作成しているのか。 【理由】 各社ともお客様への影響を考慮しながら、セキュリティ強化に努めていると認識しており、内容によってはスタンダードであっても実装までに相応の期間を要するものもあると考えている。ガイドラインが「留意事項」を取りまとめた位置づけであることは十分理解しているが、証券業界にとって喫緊の不正アクセス事案への対応は大きな課題であることから、貴協会としてもガイドラインを発出する立場として、【スタンダード】が実装されることを目指している目線を示していただきたい。	本ガイドラインの性質上、施行日の概念はありませんが、本ガイドラインにおいて対応が求められる内容については、公表後、証券会社各社の状況等を踏まえながら、速やかに対応いただくことになると考えられます。
100	Ⅳ．１．（２）において【スタンダード】としている①多要素認証はその導入や運用に多額の費用を要します。ところで、このガイドラインは日本証券業協会の自主規制規則ではなく、また自主規制規則に根差したガイドラインでもないと理解することができました。このため、【スタンダード】として挙げられている内容と言えども、このガイドラインの内容については、インターネット証券評議会に加盟している証券会社における自主的な取組みが記載されているのであって、インターネット証券評議会に加盟していない証券会社が日本証券業協会から強いられるものではないという理解でよいでしょうか。	貴見のとおり、本ガイドラインは、本協会の自主規制規則に該当するものではありません。 一方で、本ガイドラインは、インターネット取引を提供する全ての会員証券会社を対象としたものであり、本協会のインターネット証券評議会に所属する証券会社に限定するものではありません。
101	インターネット犯罪が激化・高度化し、プロによる犯罪行為が蔓延している環境下で証券業での安全・安心を高いレベルで担保するには、インターネット等の外部に情報が流れないことを原理原則とし、電子署名等を活用したチャレンジ＆レスポンス認証を徹底することが必要です。具体的にはマイナンバーカードの IC チップやスマートフォンの	貴重なご意見ありがとうございます。 今後、検討を行う際の参考とさせていただきます。

項番	ご意見	考え方
	ハードウェアセキュリティモジュール（HSM）内に格納した秘密鍵を活用し認証を行う方法が考えられます。 これを踏まえて、今回のガイドライン改正案に関しては以下の４点が重要であると考えます。各点は相互に連関する側面もあり包括的視点で理由背景を述べておりますが当該ガイドラインでの該当箇所については各点の末尾に記載させていただいております。 1. 証券取引プロセス全域を対象としたセキュリティプラットフォームの導入 本件対応における「スタンダード」では、インターネット取引のステップごとにセキュリティモジュールを設定し安全・安心を担保する方針のように見受けられますが、セキュリティモジュール間のつなぎ部分にセキュリティホールが生じるリスクも想定されること、個別モジュールに依存する体制においてはセキュリティアップグレードや責任管理体制における整合性確保が課題となることなどが指摘できます。証券サービス全体のセキュリティを高度に担保するためには、エンドトゥエンドで、一気通貫で、機能するセキュリティプラットフォームの構築が望ましいと考えます。 セキュリティプラットフォームでは、蔓延するフィッシング対策として ID およびパスワードの活用を廃止し、電子署名に基づく認証を技術的中核とするのが望ましいと考えます。電子証明書のプロセス全域にわたる活用により、セキュリティホールを排除するだけでなくセキュリティレベルを高いレベルで整合させることが可能となります。 また、サービス利用開始に至るまでのセキュリティを考えた時、身元確認（JPKI）と当人認証（ログイン）のセキュアな連携は必須要件であり、双方において多要素認証を実践することが重要であると考えます。 例えば、「口座開設時における本人確認」で、既に不正が確認されているもの（例：写真付き本人確認書類の画像＋容貌の画像）や偽造の可能性が議論されているものはガイドラインから除外するか、あるいはあくまでも経過措置であることを明示することが重要であると考えます。 また、当ガイドラインに記載の「口座開設時における本人確認」では、証券総合口座の開設時のみに本人確認が必要と記載されているように読み取れますが、信用取引口座や	

項番	ご意見	考え方
	デリバティブ取引口座等の専門の口座開設においても同レベルの本人確認措置を開設都度実施することが必要であると考えます。 さらに、顧客属性の変更においても多要素認証を活用することにより、取引商品許可（特にハイレバレッジ商品）が不正に変更され、顧客の損失リスクが大きくなる可能性を避けることができます。「ベストプラクティス」においては、このようなプラットフォーム型のセキュリティ構造を採用し、総体としてのセキュリティレベルを高度に担保することが求められることが考えられます。 具体的には、最新の身元確認情報と連動した当人認証の運用（例えば、当人認証時に身元確認情報の有効性や最新の情報を合わせて確認することです。仮に、本人が死亡と断定されていた場合、有効性が確認されず、当人認証を拒絶しログイン等ができないため、本人名義の証券口座が他人に不正に使用されることを防ぐことが可能になります。）とシームレスな多要素認証の実行をその要件とすることが適切であると考えます。 該当箇所　ガイドライン IV.1.(1)、(2) 2. 本来の「高度な多要素認証」の実践 本件ガイドライン規定されるように、多要素認証はセキュリティ強化の重要な要素であると考えます。しかしながら、ID・パスワードに加えて、普及しつつあるスマートフォンを利用した SMS 等によるピンコードなどの確認は、ガラケーによる SMS 認証とは根本的に異なり、ハードウェア（スマートフォン）に紐づく要素による確認ではないことが知られております。したがって、多要素認証ではなく単なる多重認証であることを明示すべきであり、また「スタンダード」では、多重認証ではなく異なる認証根拠を組み合わせた多要素認証が必須であるべきと考えます。 さらに、フィッシング耐性のある多要素認証という観点において、多要素認証のうち、理論上フィッシングが不可能な「高度な所持情報」を一要素として含む認証方式の実践を推奨することが適切であると考えます。「高度な所持情報」とは、例えば、スマートフォン内の安全な領域である HSM で生成される秘密鍵を活用し、認証に必要な情報がインターネット上に露出しない方式などが考えられます。	

項番	ご意見	考え方
	該当箇所　ガイドライン IV.1.(1)、(2) 3. 社会実装に耐えうる利便性とコストの確保 一般に、高度なセキュリティの実現とコストや利便性は相反するものといわれていますが、証券事業の健全な発展を実現するためには合理的なコストと高い利便性を前提とした高度なセキュリティの実装が必須要件であると考えます。 そのための具体的なアプローチとして、携帯電話に秘密鍵を生成させ、外部インフラに重く依存しないセキュリティ構造が重要と考えます。電子署名そのものは安価なオペレーションに適しており、企業にとって利用者数が増加することに伴う追加的コストは限定的であると言えます。もちろん、一定程度の固定費は発生数しますが、前述のように証券サービスプロセス全域にわたるセキュリティをプラットフォーム型で担う構造を採用することにより、コストの低減が可能となると考えます。ユーザー利便性の点においてはデジタルデバイスの中核である携帯電話で一連のセキュリティプロセスが完了することは利便性のコアとなり、マイナンバーカード等を持参する、都度利用する煩雑さから解放されるスキームも「ベストプラクティス」においては求められる要素とすべきであると考えます。 セキュリティとコスト・利便性の両立を実現することは広くかつ迅速に仕組みを社会実装するための重要な要件であり、「ベストプラクティス」ではその視点を盛り込むべきであると考えます。 また、社会実装という点において、今後はより一層、顧客がセキュリティの高い証券会社の口座開設を望む場合が多くなることも想定されるため、ガイドラインの「ベストプラクティス」を実装している企業は、その実装内容について顧客に対し開示することが望ましいと考えます。 該当箇所 ガイドライン IV.1.(1)、(2)【ベストプラクティス】 4. 過渡的対応を避け、一気にセキュリティレベルを上げる方針	

項番	ご意見	考え方
	インターネットショッピングや電子マネー決済と比較すると、証券取引の特殊性は高額取引や富裕層顧客への対応が求められることであると考えます。昨今の証券業界を狙った犯罪は専門的なプロ集団によるものも多く、中程度のセキュリティは攻撃対象となり、結果的に業界の安全性は実現できないと考えられます。このような視点に立てば、スタンダードから「ベストプラクティス」への段階的セキュリティ強化は業界のセキュリティ担保にそぐわないともいえ、可及的速やかに、一気に、「ベストプラクティス」の普及を目指すべきと考えます。一見、ベストプラクティスには高いハードルがあるように思われがちですが、前述のようにセキュリティとコスト・利便性の両立は電子署名を中核としたセキュリティプラットフォームの実装により十分に実現可能な範囲にあると考えます。 該当箇所　ガイドライン全体	
102	この度のガイドライン改正は、近年の証券口座不正利用やフィッシング被害拡大を受け、パスキーや PKI ベースのフィッシング耐性型認証を必須化するなど、顧客保護に資する施策を明示された点を高く評価いたします。 しかしながら、改正案全体を通じて「フィッシング対策」に重点が置かれており、認証突破後のセッション管理や継続的な監視といった観点が明示的には示されていない点に懸念を抱いております。実際には、認証情報が窃取された後に発生する インフォスティーラー攻撃やセッションハイジャックによる被害が国際的に多数報告されています。これらは単なるフィッシング耐性強化だけでは防ぎきれず、より包括的な対策が必要です。 米国では NIST SP 800-63B や FFIEC ガイドラインにおいて、認証後のセッション管理、継続的なリスクベース認証、挙動監視の導入が推奨されています。また欧州の ENISA（欧州ネットワーク・情報セキュリティ庁）も金融分野の最新脅威レポートにおいて、AiTM（Adversary-in-the-Middle）による MFA 回避やセッショントークン悪用のリスクを主要な課題として指摘しています。 日本国内でも、2024 年以降ネット証券等における不正ログインや不正取引が複数報告され、各社が MFA 必須化などの対応を進めています。こうした事案は、フィッシング対策	貴重なご意見ありがとうございます。 ログイン後の挙動分析の強化につきましては、本ガイドライン「Ⅳ．５．モニタリング」においてベストプラクティスとして実施することを求めております。 具体的な方法等については、必要に応じ、引き続き、検討させていただきます。

項番	ご意見	考え方
	だけでなく、ゼロトラスト思想に基づく適宜検査（継続的なセッション監視・再認証・行動分析）が導入されていない場合に被害拡大につながることを示しています。 したがって、本改正にあたっては下記の事項も明示されることを強く希望いたします。 パスキーや PKI ベースのフィッシング耐性型認証を必須化した後のインフォスティーラー攻撃やセッションハイジャックといった攻撃に対するリスクを前提に、ゼロトラスト思想に基づく適宜検査（セッション継続監視、異常検知時のリスクベース再認証、デバイス・トークンのバインディング、チャレンジレスポンス検証等）を促すこと。 上記追加により、本ガイドラインが国際的な水準に沿った包括的なものとなるだけでなく、協会参加各社へのより有効なガイドラインとなり、顧客資産の安全と証券市場への信頼向上に一層寄与することになると考えております。	
103	現在、投資家向けサイトを運用しております。以下の情報をもとに、サイバーセキュリティ対策をどこまで対応すれば良いのかご教示頂けますか。取引ができるわけではないので、あまり費用をかけずに十分なセキュリティ対策をできればと考えております。 -----システム概要------ 【セキュリティ対策】 すでに、ログイン時に二要素認証（OTP,TOTP）を設けており、更新系の機能に関しても都度 OTP の入力を求める仕様で開発を進めています。また、Thales 社のリスクベース認証も導入しております。 【既存機能】 資産情報や顧客属性の閲覧　※参照系のみ 【今後追加機能】 更新系の機能をリリース予定です。例えば、顧客属性の変更、リアルタイム口座振替	本質問につきましては、回答を差し控えさせていただきます。
104	私は証券口座乗っ取りの被害者で、被害者コミュニティの一つを運営しています。 私は指紋認証での被害者で、被害当時に証券会社に設定していた有料メールを５年前に解約しておりましたし、顔認証で ID やパスワードは登録時のまま引き出しにしまってあって入力したことがないという被害者もおります。有職者が生体認証とフィッシング詐欺対策で証券口座乗っ取りは解決だとしているなら認識が異なります。デバイス登録	貴重なご意見ありがとうございます。

項番	ご意見	考え方
	と FIDO を突破された高額被害者が私のコミュニティに３人やってきました。高額被害者でないと中々コミュニティにはやってこないので、実際は泣き寝入りもかなり多いと考えられ、改正案を決定する前に、まず何が起こっているか実態を把握した方が良いと思います。私がこの問題の多発で確信しているのは、証券会社が金融法を厳守せず、いろいろな不道徳を働いたことが一番の原因です。私は、認証がどうあっても破られるものと考えにいたり、この問題は VPN に対策することでしか解決しないと理解しました。 まとめ記事にもあるとおり、証券会社には、IP レピュテーション、不正行為に関与したと知られている IP アドレスのリスト（ブラックリスト）を活用し、該当する IP からのアクセスをブロックするシステムがなく、Google の無料メールで全員が自動で有効化されているセキュリティすらなかったのです。前提として本人確認必須の自分の証券口座に、標準設定で匿名サービスからつなげるようにしていたことが異常です。たとえば私の犯人の不正アクセスにおいて、３つの不正アクセスがありますが、すべてで犯人は東京の踏み台サーバーを使って国内からの接続に見せかけています。 接続を匿名化し犯人の足取りを分からなくする踏み台サーバー、それで証券口座につなげる VPN システムが問題なのです。普通の人は家のＰＣや自分のスマホでしか証券口座を見ません。海外や旅行に行く人だけ、前もって VPN を許可するオプションにしておくだけで、ほぼすべての証券口座乗っ取りは防げていたでしょう。また休眠口座に対して VPN から接続できないようにしておけば私は被害に遭わなかった。これは取引の便利性とはなんら関係がありませんし、やるべきだったのです。 VPN は中国やロシアのように禁止にするか、米国のように事業者を登録制にして、仮に犯罪に利用された場合にすぐ対応できるようにしたり、欧州の FIU.net のように金融犯罪情報を共有し、証券業界全体で IP レピュテーションを構築し、証券口座乗っ取りに加担した踏み台サーバーをブラックリストに突っ込んで被害の多発を防ぐべきだったと思われます。いずれは金融 AI に IP アドレスを監視させて怪しい VPN を弾くという手法で被害０は達成できると思いますので、VPN を議題に上げて深く検討されてください。	

以　上

日本証券業協会
Japan Securities Dealers Association
JSDA

「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」の改正について

2025年10月15日
日本証券業協会

1. ガイドライン改正の経緯等

【2025年1月頃～】

- フィッシング等により、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

【2025年4月～】

- 上記フィッシング等による不正アクセス・なりすまし取引等に対応すべく、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」）の見直しを開始

【2025年7月～8月】

- 7月15日から8月18日にかけて、ガイドライン改正案のパブリックコメントを実施

【2025年10月（予定）】

- パブリックコメントをふまえて、ガイドラインを改正

2. ガイドラインの主な改正ポイント

「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」の技術面における主な改正ポイントは以下の3つ

- **フィッシングに耐性のある多要素認証**（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）**の実装必須化**
- **顧客への通知等の必須化**
  - ✓ ログイン・取引時等における顧客への通知
  - ✓ 認証失敗時のアカウント・ロック
- **フィッシング詐欺被害未然防止のための措置**
  - ✓ 顧客へ送付するメール等の正当性の確保
  - ✓ フィッシングサイトのテイクダウン活動の実施
  - ✓ メール・SMS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

上記のような技術的な改正ポイント以外にも、**内部管理態勢の強化や、モニタリング、不正アクセス等を防止・検知するための設定等の利用状況確認等、不正アクセス発生時の対応及び顧客への周知・注意喚起等を実施**するといった事項についても新規追加及び見直しを実施している。

3. パブリックコメントについて

2025年7月15日から同年8月18日までパブリックコメントを実施
44先(協会員14、その他30)、意見数115件(※)のパブリックコメントが寄せられた。

パブリックコメントで寄せられた主な意見

1. フィッシングに耐性のある多要素認証について
2. 顧客へ送付するメール等の正当性、ウェブサイトの真正性の証明について
   (ウェブサイトの真正性の証明方法について⇒P. 9参照)
3. メールやSMSへのURLやログインリンクの記載の是非等について
4. モニタリングの手法、リスクベース認証等について
5. 社内教育／顧客への被害拡大・二次被害等を防止するための周知・注意喚起等について
   (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の実施、ウェブサイトのURLをブックマーク　など⇒P. 10・11参照)
6. 銀行口座との連携サービスについて
   (連携サービス全体を見た対応に関する表記について⇒P.12参照)

⇒　パブリックコメントのご意見をふまえての修正を行った。

※　1つのコメント内に2つの意見があった場合、意見数は2件としてカウントしている。

【参考】パブリックコメントで寄せられた主な意見（一部抜粋）

1. フィッシングに耐性のある多要素認証について

➢ フィッシングに耐性のある多要素認証の導入について

- 多要素認証としてワンタイムパスワードが広く利用されていますが、最近は精巧な偽サイトやフィッシングが蔓延しております。この状況では人の手で作業を行う方法は安全性が低いと言うほかなく、フィッシング耐性がある多要素認証はもはや必須と考えます。その点において、こちらは是非推進していただきたいです。
- パスキーによる認証について、特に Windows 端末でのパスキーの管理は社会的に広く受け入れられているわけではなく、ユーザー側のリテラシーを求める手法であることへの考慮が必要ではないでしょうか。特に高齢者がパスキーを自身で運用することの難易度は非常に高い、という点にも十分に留意した記述にすべきではないかと思います。
- 利便性を追求し、代替的なものも含めたすべての多要素認証の適用を拒否する顧客も存在する。当該顧客に対しては、多要素認証の適用を行わないことのリスクを説明の上適用しないような措置が可能であることを確認したく、その点を明記頂きたい。その際、何らかの追加の措置が必要であれば、考えられる措置についても確認したい。
- 「代替的な多要素認証」として容認される方式として現時点で想定される方式について具体的に記載していただくとともに、それらに対する評価も併せて記載いただきたい。例えば、代替的な多要素認証として様々な方式の中には、採用しないことが望ましい方式や短期的な採用であるならば許容される方式などはあるのかなど、評価に幅があるのではないかと考えており、ガイドラインにおいて認証方式に対する評価や補足的な説明について記載していただきたい。

【参考】パブリックコメントで寄せられた主な意見（一部抜粋）

➢ パスキーの定義

- パスキーという言葉は技術的に多くの要素を含んでおり、一般的には広義のパスキーと狭義のパスキーという形で分けて説明されることが多いかと思います。今回、フィッシング耐性を有するという文脈から、必然的にドメインの検証が行われる FIDO2 の規格に準じた「狭義のパスキー」を指し示していると考えられますが、明示されていない以上事業者が実装を検討するにあたり混乱や、「広義のパスキー」の拡大解釈といったことが懸念されるかと思います。実装を検討するにあたって、不要な確認や要件の不明確化によって生じるコミュニケーションコスト増を避ける為にも、ガイドラインとして「広義のパスキー」を意図していないのであれば、その旨は明示すべきではないでしょうか。

【参考】パブリックコメントで寄せられた主な意見（一部抜粋）

2. 顧客へ送付するメール等の正当性、ウェブサイトの真正性の証明について

➢ DMARC等送信ドメイン認証技術の導入

- DMARCポリシーは「reject」に設定することが必須となるのでしょうか。また、「quarantine」に設定した場合、法令遵守上の懸念が生じるという意味でしょうか。DMARCの進捗状況は公表する必要がありますでしょうか。

➢ 共通ショートコードの利用

- 共通ショートコードはスミッシング対策として一定の効果が期待できる手段ではあるものの、現時点でこれを【スタンダード】の位置づけとして全証券会社に標準的対応として求めることには疑問を感じる。共通ショートコード（0005で始まる送信元番号）がフィッシング対策に有効であるためには、受信者がその番号を確認し、正規メッセージであると判断する行動様式の定着が前提だが、現時点でその仕組みを理解している一般消費者は非常に限定的であり、短期的な実効性は乏しいのではないか。

➢ ウェブサイトの真正性の証明方法について⇒P.9参照

3. メールやSMSへのURLやログインリンクの記載の是非等について

- メールやSMS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ことがルールとされ、その例外として、法令に基づく義務を履行するための場合など代替手段をとなり得ない場合と記載がされていますが、例外事項の対象に『お客さまが取引先の金融機関からログインリンクが送付されてくることを認識済の状況で送付する場合』を追加いただきたい。

＜具体的なシチュエーション＞

- お客様と有価証券の募集について電話で会話し、目論見書交付のためのログインリンク（目論見書交付ページへのリンク）を送付する旨を伝えたうえで送付
- お客様とサービスの申込、住所や氏名の届出事項の変更といったお客様が必要な手続きについて電話で会話し、その意向を確認したうえで、手続きを行うためのWebページへのログインリンクを送付

【参考】パブリックコメントで寄せられた主な意見（一部抜粋）

4. モニタリングの手法、リスクベース認証等について

➢ ログイン後の振る舞い検知

- 「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」という表記になっていますが、実際は検知した後の対応が必要なこともガイドラインに記載すべきと考えます。例えば、ログイン後の挙動の分析について、リスクの高い振る舞い（高額の銀行口座からの入金、特定株式の高額購入、認証情報の変更等）を検知した場合は操作を受けつつ処理を「保留」とし、別途本人に意図した操作か確認した後に処理を「実行」できる運用をとるなど。

➢ 不正アクセスの評価に応じた追加の本人認証

- 不正アクセスの評価に応じた追加の本人認証については、以下のような対応で十分という理解で良いか。
  - モニタリングの結果、不正アクセスが疑われるケースでは、本人に電話し不正アクセスの有無を確認。電話でのコンタクトができなかった場合はログイン規制等を実施、規制解除にはコールセンターに電話するようにメールで案内
  - コールセンターに電話があった際に、発信電話番号や氏名、住所、生年月日等により本人確認を実施の上、ログイン規制を解除、不正アクセスの有無を確認

【参考】パブリックコメントで寄せられた主な意見（一部抜粋）

5. 社内教育／顧客への被害拡大・二次被害等を防止するための周知・注意喚起等について

- ペネトレーションテストの実施、ウェブサイトのURLをブックマークなど⇒P. 10・11参照
- 顧客からの届け出を速やかに受け付ける体制の整備

- 「顧客からの届出を速やかに受け付ける体制を整備」との記載について、「問い合わせに対して速やかに回答する体制」まで求めるものではないという理解で合っているか、確認したい。

【理由】
「顧客からの届出を受け付ける体制」の整備は課題と認識している。たとえば、24h/365dで顧客からの届出・問い合わせをチャットボット等によりまずは受け付け、システム的に回答・反映可能な事項等はシステム的に処理を行うことを想定している。このような対応で題意を満たすものであるか、為念確認したいもの。

6. 銀行口座との連携サービスについて

- 他の銀行口座との連携サービスとは

「他の銀行口座との連携サービス」とは、以下のいずれを指しているものか確認したい。
① 取引時に自動で銀行口座から証券口座へリアルタイムで資金移動を行うサービス
② 口座振替契約を事前に締結し、都度、顧客の指示に基づいて銀行口座から証券口座へリアルタイムで資金移動を行うサービス
③ 口座振替契約を事前に締結し、月１回などの頻度で銀行口座から証券口座へ定期定額の資金移動を行うサービス（リアルタイムでの任意の預金の移動が行えないもの）

- 連携サービス全体を見た対応に関する表記について⇒P.12参照

4. パブリックコメント等を受けたガイドラインの修正案

Ⅳ.4. フィッシング詐欺等被害未然防止のための措置

修正案	修正前（7月15日公表案）
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】 (1)～(4)　（省略） （削除） (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）。	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】 (1)～(4)　（省略） (5) 利用者がアクセスしているウェブサイトが真正なウェブサイトであることの証明を確認できるような措置を講じる。 (6)　（同左）

【コメント概要】

- かつて利用されていた「EV証明書」の無効性や弊害が指摘されている中で、「真正なウェブサイトを証明する方法」で想定される方法を具体的に例示いただきたい。以前はEV証明書が利用されていたが、現在では、主要ブラウザのアドレスバーでのEV証明書の組織表示は行われていない。

【修正理由】

- 上記の指摘のとおり、利用者が正規の証券会社のウェブサイトとフィッシングサイトを判別するための対策として、従来実施されてきたEV SSL証明書の表示などは、現在においてはウェブサイトの真正性の判断とは異なるアプローチであると想定されることから、当該項目を削除することとしたい。

4. パブリックコメント等を受けたガイドラインの修正案

Ⅳ.7. その他（社内教育）

修正案	修正前（7月15日公表案）
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。	7. その他 （1）社内教育 【スタンダード】 （同左） （新設）

【コメント概要】

- 最近、SOCから経営層までの事故対応演習の依頼を受けることが多い。ペネトレーションテストやレッドチーム演習などで模擬的な攻撃テストを実施した際に合わせてSOC側のブルーチーム演習も行うものから、机上でのシナリオベースの訓練があるが、教育のベストプラクティスとして追加されるのはいかがか。

【修正理由】

- ご指摘のとおり、サイバー攻撃・予測される事故等について対応演習や訓練を行うことは、インターネット取引における不正アクセス・不正取引等の対策にとどまらず、自社システムに対する包括的なセキュリティ対策の一環として有効な手段であると考えられることから、ベストプラクティスに追加することとしたい。

- SOC（Security Operation Center）・・・サイバー攻撃の検知や分析を行い、対策を講じる専門組織のこと
- ペネトレーションテスト・・・ネットワーク、PC・サーバーやシステムの脆弱性を検証するテスト手法の一つ。実際にネットワークに接続しシステムに攻撃を仕掛け侵入を試みる、いわゆる疑似的なサイバー攻撃を行い、各社におけるセキュリティ対策の有効性やリスクを評価する。
- レッドチーム／ブルーチーム演習・・・レッドチームが疑似的なサイバー攻撃を行い、ブルーチームがそれを検知・対応するといった取り組みのことで、各社が導入しているセキュリティ対策や体制が実際にサイバー攻撃を受けた際に有効に機能するかを検証・確認することが目的である。

4. パブリックコメント等を受けたガイドラインの修正案

Ⅳ.7. その他(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)

修正案	修正前(7月15日公表案)
7. その他 (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 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。 【スタンダード】 ①～⑤ (省略) 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。	7. その他 (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 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。 【スタンダード】 ①～⑤ (省略) (新設)

【コメント概要】

- 顧客へ周知・注意喚起するべき事項として、「利用する証券会社のウェブサイトへのアクセスは、事前に正しいウェブサイトのURLをブックマークに登録しておき、ブックマークやアプリからアクセスすること」を、スタンダードとして追加してはいかがか。

【修正理由】

- ご指摘のとおり、証券会社が顧客へ周知・注意喚起するべき事項であると考えられることから、顧客の被害拡大・二次被害等を防止するための周知・注意喚起等に関するスタンダードとすることとしたい。

4. パブリックコメント等を受けたガイドラインの修正案

Ⅳ.7. その他(銀行口座との連携サービス)

修正案	修正前(7月15日公表案)
7. その他 (3) 銀行口座との連携サービス 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。	7. その他 (3) 銀行口座との連携サービス 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**に対しては、証券口座の認証のみで預金引き出しが可能であり、**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。

【コメント概要】

- 「新規に預金口座と連携する顧客に対しては、証券口座の認証のみで預金引き出しが可能」と記載されているが、これは「銀行口座での認証を経て新規の連携の登録完了後は、証券口座の認証のみで預金引き出しが可能」という趣旨で相違ないか。明確化のために修正を検討いただきたい。

【修正理由】

- ご指摘の認識で相違ないと考えられることから、当該箇所の記載について、ご指摘をふまえて修正することとしたい。

4. パブリックコメント等を受けたガイドラインの修正案

➢ その他の修正事項

修正案	修正前（7月15日公表案）
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 （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。 **<u>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</u>**	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 （2）ログイン・取引・出金時 【スタンダード】 （同左） **<u>① 多要素認証</u>**

修正案	修正前（7月15日公表案）
6. 不正アクセス発生時等の対応 （3）関係機関への報告・連携強化 【スタンダード】 （省略） 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**<u>当局指定の様式により</u>**、速やかに報告を行う。	6. 不正アクセス発生時等の対応 （3）関係機関への報告・連携強化 【スタンダード】 （省略） 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、速やかに報告を行う。