日本証券業協会
Japan Securities Dealers Association

「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

© Japan Securities Dealers Association.All Rights Reserved.

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

© Japan Securities Dealers Association.All Rights Reserved.

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。

© Japan Securities Dealers Association.All Rights Reserved.

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。

© Japan Securities Dealers Association.All Rights Reserved.

JSDA

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。

© Japan Securities Dealers Association.All Rights Reserved.

【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）

JSDA

➢ 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。

© Japan Securities Dealers Association.All Rights Reserved.

【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）

JSDA

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

© Japan Securities Dealers Association.All Rights Reserved.

JSDA

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

© Japan Securities Dealers Association.All Rights Reserved.

【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）

JSDA

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

© Japan Securities Dealers Association.All Rights Reserved.

JSDA

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。

© Japan Securities Dealers Association.All Rights Reserved.

JSDA

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。

© Japan Securities Dealers Association.All Rights Reserved.

JSDA

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。

© Japan Securities Dealers Association.All Rights Reserved.

JSDA

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。

© Japan Securities Dealers Association.All Rights Reserved.

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

JSDA

➢ 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。

© Japan Securities Dealers Association.All Rights Reserved.