証券口座への不正アクセス事案を踏まえた監督指針改正の要諦

ネット取引サービス提供者に求められる強固な多要素認証の実装・必須化

金融庁
監督局　証券課　課長補佐
眞砂 ルミ

金融庁は2025年10月15日、「金融商品取引業者等向けの総合的な監督指針」（以下、監督指針）の改正案に係るパブリックコメント結果を公表し、監督指針を施行した。今般の改正は、インターネット証券口座における不正アクセス事案を踏まえて、インターネット取引サービスを提供する金融商品取引業者および登録金融機関（以下、金融商品取引業者等）に対する監督上の着眼点等について示したものである。本稿では、監督指針を踏まえて金融商品取引業者等が取るべき対応のポイントについて解説する。

フィッシングサイトや身に覚えのない取引の急増

2025年3月下旬ごろから、証券会社をかたる偽サイト（フィッシングサイト）の検出や、顧客に身に覚えのない不正取引が急増した（図表1）。こうした事態を受け、金融庁は25年4月以降、投資家に向けた注意喚起を継続的に実施し、月次で被害発生状況を公表している（注1）。

また、業界団体である日本証券業協会は25年4月から、インターネット取引におけるログイン時の「多要素認証の設定必須化を決定した証券会社」の公表を開始。各証券会社においても、自社をかたるフィッシングサイトへの注意喚起のほか、ログイン時の多要素認証の必須化等の対策を進めてきた。

ただ、各証券会社が緊急対応として導入・必須化を進めてきた多要素認証は、メールやSMS（以下、ショートメッセージ）でワンタイムパスワードを送付する等の方法で、フィッシング耐性が十分とはいえないものが多く見られた。

リアルタイムフィッシングといった新たな犯罪手口にも対応していくため、金融庁は25年7月15日に監督指針の改正案を公表し、パブリックコメントを実施した。

パブリックコメントの結果、141件のコメント（以下、パブコメ質問）が寄せられた。これに対する「金融庁の考え方」（以下、パブコメ回答）を25年

不正アクセス対策の監督指針改正

10月15日に公表して監督指針の改正案を最終化し、同日施行した。主な改正内容は図表2のとおりである。

以下ではこのうち、内部管理態勢の整備およびセキュリティーの確保の観点から、実務上特にポイントとなり得る点について解説する。

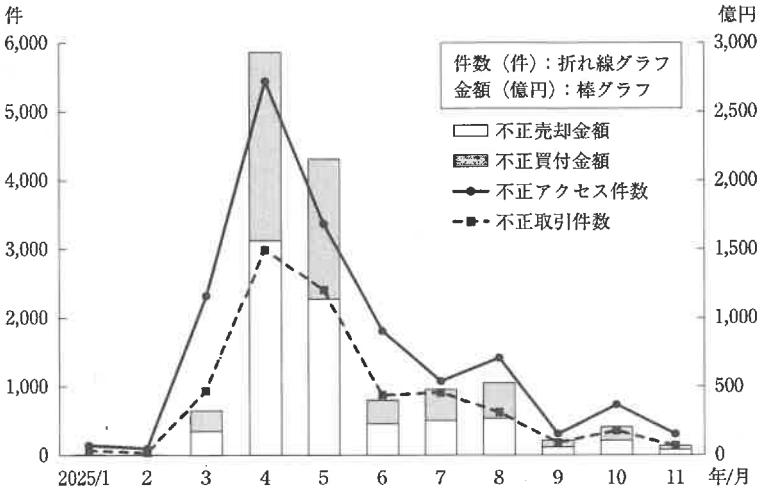
経営陣の責務としてセキュリティー対策を

改正後の監督指針（注2）においては、インターネット取引における不正アクセス・不正取引等の犯罪行為への対策等を最優先の経営課題の一つとして位置付けることを求めている。取締役会等において必要な検討を行い、セキュリティーレベルの向上に努めていく必要がある。これらはインターネット取引に係る犯罪手口が高度化・巧妙化し、被害が拡大していることを踏まえたものである。

改正前の監督指針においても、サイバーセキュリティー事案の未然防止について経営上の重大な課題として認識し、態勢を整備することを求めていた。今回の改正は、日々進化する犯罪手口に即時に対応していくため、不正アクセス等への対策を「最優先の経営課題」として位置付けて取り組んでいくよう、あらためて求めるものである。

インターネット取引サービスを提供する事業者は、顧客や業務の特性、提供するサービスの内容を踏まえながら、その時々のセキュリティー技術水準や犯罪手法等に応じて、不断にセキュリティー対策を見直していくことが重要である（パブコメ回答No.132）。各社の顧客や取扱商品、業務の特性等に応じて自らリスク評価を行った上で、適切な態勢整備を講じる責任がある（パブコメ回答No.133）。

〔図表1〕　インターネット証券口座における不正取引の発生状況



不正取引が発生した証券会社数（社）										
25年1月	2月	3月	4月	5月	6月	7月	8月	9月	10月	11月
2	2	5	10	16	7	6	7	6	8	7

（注）　不正取引件数は、不正アクセス件数のうち不正取引まで行われた件数。
（出所）　金融庁ウェブサイト

〔図表2〕　監督指針改正で求める主な内容

①内部管理態勢の整備として、不正アクセス等への対策を最優先の経営課題として位置付け、セキュリティーレベルの向上に努めること
②セキュリティーの確保として、
- ログイン時等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」の必須化
- メールにログインＩＤやパスワード入力を求めるＵＲＬを記載しないこと、メールの送信ドメイン認証技術の計画的な導入やフィッシングサイトの閉鎖依頼等
- その他、ログイン通知機能の提供、不審な挙動に対する検知やアカウントロック等

③顧客対応として、注意喚起が十分に行われる態勢整備や被害回復に向けて真摯な顧客対応を行うための態勢整備等

（出所）　金融庁

また、インターネット取引サービスの利用時における留意事項等を顧客に説明するための態勢の整備を求めている。顧客の理解に疑義がある場合の対応として、顧客との取引を継続するか否かの判断は各社において適切に行われるべきものである。だが、顧客にインターネット取引サービスを提供する事業者においては、サービスの利用に必要なＩＴリテラシーについて、顧客の意識向上に努めていくことが重要である（パブコメ回答№8、78、136）。

インターネット取引サービスを提供する事業者は、顧客被害を発生させないために、経営陣の責務として、サービスの利用に必要なＩＴリテラシーについて顧客の意識向上に努めていく必要がある。それと併せて、セキュリティー対策に取り組んでいくことが求められる。

フィッシングに耐性のある多要素認証の必須化

認証強化の観点から、監督指針（注3）においては、ログイン、出金、出金先銀行口座の変更など、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（以下、強固な多要素認証）の実装および必須化を求めている。これは、今回の監督指針改正の最も重要なポイントである。強固な多要素認証の例として、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掲げている。

認証の設定では、顧客側の操作が必要不可欠であり、顧客側の物理的な理由で設定できない場合等も想定される。設定に必要な機器（スマートフォン等）を所持していない等のやむを得ない理由がある顧客への対応として、代替的な多要素認証を提供すること、強固な多要素認証を利用できない顧客の割合が低くなるよう多要素認証の方法の見直しを検討・実施することも求めている。併せて、即時に対応できない事業者に対しては、代替的な多要素認証の提供のほか、強固な多要素認証の必須化に向けた具体的なスケジュールを顧客に周知することを求めている。

取引の即時性や利便性が損なわれる懸念から、多要素認証を望まない顧客への対応について複数のパブコメ質問が寄せられた。しかし、顧客の要望による例外を認めることは、顧客がそのリスクを認識していたとしても、不正アクセスの隙を与えることにつながりかねない。そのため、不正ログイン・不正取引防止の観点から、原則として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が適切である（パブコメ回答№44、78）。

これまで、多要素認証を提供していてもその利用は顧客の任意としていた結果、今般のような被害の拡大につながった面は否めない。そのため、業界全体で速やかに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が肝要である。

証券会社以外の業態における対応の必要性についても複数のパブコメ質問が寄せられた。インターネット取引においては、今回のような事案に限らず、不正アクセスにより、真正な顧客ではない第三者等による買い付けや売却といった顧客被害が発生する可能性がある。こうしたことから、証券会社以外の金融商品取引業者等も含めて、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導入を求めるものである（パブコメ回答№28、30）。

監督指針は、証券会社以外の金融商品取引業者および登録金融機関も対象とするものである。これらの業態についても、インターネット取引サービスを提供している場合は、投資家保護の観点も踏まえながら、十分なセキュリティー対策を講じる必要がある。

ログインを促すメールの原則禁止

フィッシング対策の観点から、監督指針（注4）においては、原則としてメールやショートメッセージ内にパスワード入力を促すページのＵＲＬを記載しないことを求めている。さらに、利用者に対して正規のウェブサイトのブックマークや正規のアプリからログインすることを促すこと、送信ドメイン認証技術の

計画的な導入、フィッシングサイトの閉鎖依頼等も求めている。これは、今般の不正アクセス事案において、ログインＩＤやパスワードを窃取するフィッシングサイトに誘導するフィッシングメールが多数確認されていることを踏まえたものである。

ログインＩＤやパスワードの入力を促すページに遷移するリンクについては、メール配信の解除手続きなど、法令に基づきメール本文に記載が義務付けられている場合を除き、メールに記載すべきではない（パブコメ回答№15、19）。

また、法定書面の電磁的提供において、メールを活用する事例が見られる。その際の書面の閲覧方法は、ログインを促すようなリンクをメッセージに記載する方法ではなく、メッセージ内本文にウェブサイト内の掲載場所を記載するなどの方法で案内することが適切である（パブコメ回答№19）。ログインを伴わずに閲覧できる場合であっても、同じページ内にログインボタンが表示されるような状態は適切ではない（パブコメ回答№19、20）。

証券会社の正規のメールやウェブサイトと判別のつかない精巧なフィッシングメールやフィッシングサイトが多数確認されている。慎重な対応を求めるのは、こうした中で顧客に「事業者から送付されたメールでログインＩＤやパスワードの入力を求められたら詐欺かもしれない」と認識できるよう意識付けを狙ったものである。

期限を待つことなく速やかに対応を

監督指針は、パブリックコメントの結果の公表日に即日、適用されている。ただ、対応には一定の時間を要するため、金融庁は、フィッシングに耐性のある多要素認証の必須化について原則26年6月末までに対応するよう各証券会社に求めている(注5)。今般のような不正アクセス事案はどの証券会社でも起こり得るため、対応できる証券会社は期限を待つことなく速やかに対応すべきである。

その他の対策や証券会社以外の業態の対応についても、自らの顧客や業務の特性に応じて、リスクの存在を十分に認識・評価した上で、順次対策を講じていく必要がある。

証券口座への不正アクセス事案はいまだ被害収束には至っていない。また、犯罪手口の進化から、証券会社だけではなく、インターネット取引サービスを提供するどの金融商品取引業者等においても顧客の被害を伴う事案が発生する可能性は否定できない。

各金融商品取引業者等においては、当然のことながら、現行の監督指針で求める対応を取っていればセキュリティー対策として将来にわたって十分ということではない。自らの顧客や業務の特性、提供するサービスの内容を踏まえながら、その時々のセキュリティー技術水準や犯罪手口等に応じて、不断にセキュリティー対策を見直していく必要がある。

金融庁においても、サイバーセキュリティー環境等の変化に応じて、不断に監督指針の見直しを行っていく。

（本稿において、意見に関する記載は筆者の個人的見解であり、所属組織の見解を示すものではない）

（注）1　金融庁ウェブサイト「インターネット取引サービスへの不正アクセス・不正取引による被害が急増しています」https://www.fsa.go.jp/ordinary/chuui/chuui_phishing.html

2　Ⅲ－2－8－2－2(1)「内部管理態勢の整備」

3　Ⅲ－2－8－2－2(2)「セキュリティの確保」

4　前掲注3

5　業界団体との意見交換会において金融庁が提起した主な論点（日本証券業協会、2025年7月15日）

まさご　るみ
03年財務省中国財務局入局、08年から金融庁。主に証券取引等監視委員会で証券検査業務に従事。宮城県石巻市産業部副参事、総合政策局秘書課課長補佐、証券取引等監視委員会事務局証券検査課課長補佐を経て現職。