

証券口座の不正利用増加を受けたガイドラインの見直し ～セキュリティ対策強化による個人投資家や証券会社への影響を要注視～

- (1) 本年入り後、フィッシングサイト等通じて窃取された証券口座情報（ログインID、パスワード等）を悪用した不正取引（証券口座乗っ取り）が多発。1～9月累計で、不正取引件数は約9,000件、不正売買額は約6,900億円に拡大（図表1）。
- (2) こうした被害を受けて、本年10月、日本証券業協会は、インターネットでの証券取引における不正アクセスの防止を目的に、それぞれガイドライン（指針）を改正。ログイン、出金、出金先銀行口座変更時に、フィッシングに耐性のある多要素認証（パスキー認証（生体認証等））を必須の対応とする方針（図表2）。
- (3) 証券会社では、大手証券やネット証券を中心に、各社の約款等の定めに関わらず、一定の被害補償を行っているほか、セキュリティ強化のために生体認証等のパスキー認証を導入する動きが拡大（図表3）。
- (4) 個人投資家の株式取引状況をみれば、若年層のみならず、高齢層でもネット取引が主流（図表4）。本件を受けた対応にとどまらず、今後もサイバーリスクが高まることを踏まえれば、継続的なセキュリティ対策が不可欠。取引時の認証手続きが増えることによる投資行動への影響や、システム投資負担増大に伴う証券会社業績への影響等を注視する必要がある。

（図表1）インターネットでの証券取引における
不正取引件数・不正取引額



（資料）金融庁「インターネット取引サービスへの不正アクセス・不正取引の発生状況」をもとに日本総研作成

（図表2）日本証券業協会のガイドラインの
主な改正点

・ログイン時、出金時、出金先銀行口座変更時など、**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（パスキー認証、PKI認証）の実装必須化**
 （注）多要素認証：認証を三要素である「知識情報」、「所持情報」、「生体情報」のうち2つ以上を組み合わせた認証。

・顧客への通知等の必須化

- － ログイン・取引時における顧客への通知
- － 認証失敗時のアカウント・ロック

・フィッシング詐欺等被害未然防止のための措置

- － 顧客に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（閉鎖）活動の実施
- － メール・SMS内にパスワード入力促すページのURLやログインリンクを

（資料）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」をもとに日本総研作成

（図表3）証券口座の不正利用を受けた
証券会社の主な対応

<被害顧客への補償>

約款等の定めに関わらず、一定の被害補償を実施

・保有株等について**被害前への原状回復**

（※）顧客側に明確な過失がない場合、不正に売却された株式等を買い戻し（主に大手証券会社における対応）

・被害額に関する**一部金銭補償**

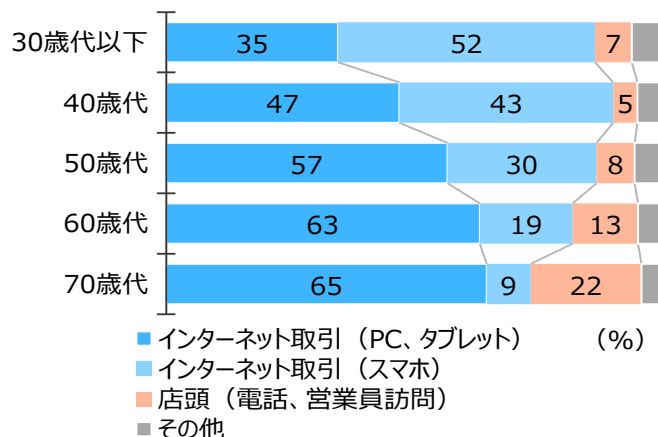
（※）不正取引で購入された株式等から生じる損失（売却損、評価損）の50%を補償（主にネット証券における対応）

<セキュリティ対策の強化>

・パスキー認証（生体認証等）の導入

（資料）各社ホームページ、各種報道等をもとに日本総研作成

（図表4）年代別の株式の主な注文方法



（資料）日本証券業協会「個人投資家の証券投資に関する意識調査」をもとに日本総研作成

【ご照会先】調査部 主任研究員 谷口 栄治 (taniguchi.eiji@jri.co.jp, 080-4377-3420)

本資料は、情報提供を目的に作成されたものであり、何らかの取引を誘引することを目的としたものではありません。本資料は、作成日時時点で弊社が一般に信頼出来るとされる資料に基づいて作成されたものです。情報の正確性・完全性を保証するものではありません。また、情報の内容は、経済情勢等の変化により変更されることがあります。本資料の情報に基づき起因してご閲覧者様及び第三者に損害が発生したとしても執筆者、執筆にあつた取材先及び弊社は一切責任を負わないものとします。