特集2

証券口座への不正アクセス・不正取引による被害の補償について

坂 勇一郎 Saka Yuichiro 弁護士
日本弁護士連合会消費者問題対策委員会委員。東京経済大学現代法学部教授。金融審議会専門委員

証券口座への不正アクセス・不正取引による被害

1．発生状況

第三者による不正アクセスに伴う不正送金、クレジットカードの不正利用はかねてからありましたが、2025年に入って証券会社のインターネット取引サービスにおいて、不正アクセス・不正取引の被害（以下、不正アクセス・不正取引事案）が多発しました。これは、第三者が、フィッシング等により不正に取得したID・パスワードを用いて証券口座にアクセスし、被害口座を勝手に操作して口座内の株式を売却し、その代金で国内外の小型株を高値で買い付けるというものです。当該小型株については相場操縦が疑われており、相場をつり上げ、高値で売り抜けたとみられる第三者に多額の不正な利益が発生し、他方で被害口座側には高値で買った後に下落した小型株の被害が残されます。被害発生は、2025年４月をピークに減少していますが、同年９月時点でも被害は発生し続けています。

2025年１月から９月までの不正アクセス件数は１万5873件、不正取引件数は8970件、不正取引における売却金額は約3670億円、買付金額は約3233億円に上ります*1。

2．証券会社の被害への対応状況

大手証券会社等は、基本的に、不正アクセスによる取引前の口座の状態に原状回復する方針を示し、他方、ネット証券系の一部証券会社は、顧客の損害の２分の１を補償する方針を示しています。いずれも具体的な解決は、個別事案の状況に応じたものとなると考えられますが、対応方針は、現状大きく２つに分かれています。

不正アクセス防止のための取組み

1．不正アクセス・不正取引事案の発生まで

金融事業者におけるセキュリティの確保、不正アクセスの防止は、かねてより重要な課題であり、各金融法制において、金融事業者の体制整備が求められてきました。

証券会社については、日本証券業協会において、2021年３月16日、「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）が策定され（2021年７月20日改正）、必要とされる対応として、ログイン時・取引時の複雑なパスワード、出金時の複雑なパスワードと多要素認証、不正アクセスの検知と評価に応じた適時遮断措置対応等が求められていました。

2．不正アクセス・不正取引事案発生後の動き

不正アクセス・不正取引事案発生を受けて、2025年７月15日、金融庁から「金融商品取引業者等向けの総合的な監督指針」等の一部改定案、日本証券業協会からガイドラインの改正案が公表され、意見募集を経て、それぞれ同年10月15日から適用されました。これらのなかでは、従来必要とされてきた対応に加えて、ログイン時や出金時等における「フィッシングに耐性のある

*1 金融庁「インターネット取引サービスへの不正アクセス・不正取引による被害が急増しています」2025年４月３日（2025年９月８日更新）

多要素認証」の実装及び必須化、不正検知の際の速やかな顧客への通知、フィッシングサイトへの閉鎖依頼の実施等が求められています。

証券口座への不正アクセス・不正取引事案における法律関係

1．法律関係検討の枠組み

不正アクセス・不正取引による被害事案は、第三者が不正に取得したID・パスワードを利用して、顧客の証券口座にアクセスし、顧客になりすまして株式の売買を行うというものです。

第三者が顧客になりすまして行った取引は、顧客が自ら行ったものではないので、この取引が顧客との間で有効に成立するか（売買の効果が顧客に帰属するか）が、まず問題となります。効果が顧客に帰属すれば、顧客は株式の売買の責任を負う必要がありますが、効果が顧客に帰属しなければ、顧客口座は不正アクセスによる取引が行われる前の状態が維持されることになり、顧客には売買による損失は生じません。不正アクセス事案において、原状回復措置により対応する証券会社は、かかる理解を前提にしているものと考えられます。

他方、売買の効果が顧客に帰属するときは、多くの場合、顧客に売買による損失が残されます。この場合には、証券会社の損害賠償責任（債務不履行または不法行為に基づく責任）が問題となります。

さらに、上記とは別に、約款上、何らかの補償制度がないか、その適用がないかも問題となります。

証券口座への不正アクセス・不正取引事案では「補償」という言葉が広く用いられていますが、法的には、①不正アクセスによる売買の効果が顧客に帰属するか、②証券会社が損害賠償責任を負わないか、③約款上の補償制度等の利用はできないか、という３つの枠組みがあることを、まず念頭に置く必要があります。これらのうち③は、約款の補償規定の確認、検討を行うことになります。以下、①②について、法的な考え方を整理します。

2．株式の売買のしくみと効果帰属

株式の売買は、顧客が証券会社に売買を委託し、証券会社が証券取引所において、自己の名で取引を行い、その効果を顧客に帰属させるというかたちで行われます（証券会社は商法551条以下の「問屋（といや）」として業務を行います）。

すなわち、①顧客が証券会社に株式の売買の注文を出し、②証券会社は、証券取引所において、顧客のために、自己の名で株式の売買を行い、③売買の相手方との間で売買の決済を行い、④顧客との間で株式・代金の受渡しを行います。

顧客は、自ら委託した（注文した）がゆえに、株式・代金の受渡しの義務を負い、権利を得るものです。自らの委託によらない売買が行われても、その売買による権利義務は、その顧客には帰属しないのが原則です[*2][*3]。顧客と証券会社の関係では、委任又は代理の規定が準用されますが（商法552条２項）、不正アクセスによる売買については、顧客と証券会社の間には当該売買に関する委託関係は成立していません。

顧客の注文によらない売買の効果が、顧客に帰属しないことについては、証券会社による無断売買の判例も参考になります。最高裁判所平成４年２月28日判決は、証券会社の従業員が、顧客の注文に基づかずに顧客の証券口座を利用して有価証券の売買をした事案について、無断売買の効果は顧客に帰属しない旨を判示しました。不正アクセスによる売買も、無断売買と同様、顧客の注文に基づかずに行われたものです。

3．外観法理の適用は考えられるか

上記が原則的な考え方ですが、顧客への効果帰属の可能性について、検討すべき点が２点あります。

１つは、外観法理の考え方による顧客への効果帰属の可能性です。外観法理は、本人の意思に

*2 この場合も、証券会社が証券取引所で行った売買は、証券会社の取引として有効であり、証券会社は、売買の相手方に対して自ら責任を負う。したがって、不正アクセスの売買によって生じた損失は、証券会社が負担することになる

*3 なお、損失補てんの禁止（金融商品取引法39条）は、自ら取引を行いながら損失の補てんを得る不公正な行為を規制するものである。自ら取引を行ってない顧客がその解決を求める場合は、上記と場面を異にするものであり、損失補てんの禁止は適用されない

基づかずに契約が行われた場合も、①本人の意思に基づくような外観があり、②その外観について当該本人に取引の責任を負わせるに値する事情（帰責事由）があり、他方、③契約の相手方に、本人の意思による契約と信頼した正当な理由がある場合に、契約の相手方を保護するために、本人の契約と認めるべきとの考え方です。

証券不正アクセス事案では、①ID・パスワードにより本人の注文である外観があることから、②かかる外観について本人に取引の責任を負わせるに値する事情があり、③証券会社側に本人の注文と信頼した正当な理由がある場合には、本人への効果帰属が問題となります。

しかし、②については、ID・パスワードがフィッシング被害により流出したような場合であっても、フィッシングの手口が高度化・巧妙化していること等に鑑みれば、フィッシング被害にあったことのみをもって、帰責事由を認めることはできないと考えるべきです[*4]。

また、③について、正当な理由が認められるためには、証券会社において不正アクセス防止のための措置が適切に取られていることが必要です。この点に関して参考となるのが、（外観法理に関する事案ではありませんが）銀行ATMの不正引き出しに関して、金融機関側の過失の検討のあり方について言及された最高裁判所平成15年４月８日判決です。同判決は、「無権限者に払戻しがされたことについて銀行が無過失であるというためには、払戻しの時点において通帳等と暗証番号の確認が機械的に正しく行われたというだけではなく、機械払システムの利用者の過誤を減らし、預金者に暗証番号等の重要性を認識させることを含め、同システムが全体として、可能な限度で、無権限者による払戻しを排除し得るよう組み立てられ、運営されるものであることを要する」としています[*5]。

具体的な事実関係にもよりますが、金融分野において不正アクセスによる被害が大きな問題となっていたこと、攻撃が高度化・巧妙化していることが専門機関により指摘されていたこと、証券会社が金額の大きい顧客資産を扱っていること等に鑑みますと、不正アクセス防止の技術的しくみが必ずしも厳格なものとなっておらず、顧客への注意喚起や警告が十分とはいえず、かえって、顧客の利便性（＝証券会社の契約獲得の利便性）を重視したシステムとなっていたときには、証券会社に前記③の正当な理由を認めることは、一般的には難しいものと考えられます。

4．顧客への効果帰属を定める約款の定め

検討すべきもう１つの点は、証券会社の約款に、ID・パスワードの利用による場合は、当該顧客の意思に基づかないときも、顧客に効果を帰属させるという条項[*6]がある場合です。

このような条項は、銀行取引等でも見られますが、銀行実務では、かかる条項は銀行が必要な注意義務を尽くすことを前提としたものであり、銀行がかかる注意義務を尽くしていない場合には、適用されないこととされています[*7][*8]。この理は、証券会社の約款においても適用されるべきです。さらに、株式の売買が、預金の払戻し（債務の弁済）と異なり、新たな契約を結ぶことであることに鑑みれば[*9]、効果帰属条項の適用には顧客の帰責事由を前提とすべきと考えられます。

また、条項の定め方によっては、その有効性も問題となります。顧客が消費者の場合、外観法理の考え方よりも約款の定めが消費者に不利であり[*10]、かつ、消費者の利益が信義則に反して一

*4 前掲の最高裁判所平成18年２月23日判決、最高裁判所平成15年６月13日判決（いわゆる「外形与因型」）に照らすと、帰責事由が認められるのは、本人の積極的関与があった場合やこれと同視し得るほどあまりにも不注意な行為があった場合に限られるべきである
*5 なお、関連判例として最高裁判所平成５年７月19日判決があるが、金融機関に求められる安全性に関する判示部分については、従前から批判があり、現在ではセキュリティ環境がかなり異なることなどから、証券不正アクセスのような事案には適しないと考えられる
*6 証券会社が損害賠償責任を負わないという条項（「5. 証券会社の賠償責任」参照）や補償しないという条項（「1. 法律関係検討の枠組み」参照）は、これとは異なる
*7 最高裁判所昭和46年６月10日判決、最高裁判所昭和50年６月24日判決等
*8 インターネット・バンキングに関する東京高等裁判所平成29年３月２日判決は、法人利用の事案であることに留意を要する
*9 受領権者としての外観を有する者に対する弁済（民法478条）でなく、外観法理の適用の問題である
*10 消費者契約法10条の「公の秩序に関しない規定」には、一般法理も含まれる（最高裁判所平成23年7月15日判決）

方的に害されるような内容である場合には、消費者契約法10条により無効となり得ます*11。

5. 証券会社の損害賠償責任

不正アクセス・不正取引による売買の効果が顧客本人に帰属する場合（または顧客がこの点を争わない場合）、証券会社の損害賠償責任を検討することも考えられます。

例えば、証券会社の不正アクセス防止システムが、金融庁の監督指針や証券業協会のガイドラインに即した対応を行っていないような場合や、証券会社が把握し得た情報から、不正アクセス防止措置をとるべきであったにもかかわらず、これを怠ったことにより顧客に損害が生じたような場合には、証券会社は債務不履行又は不法行為に基づく損害賠償責任を負うものと考えられます。

証券会社の対応としては、顧客への注意喚起も重要であり、顧客への注意喚起が十分でなく、顧客が適切に不正アクセス防止対応を行うことができなかったような場合も、証券会社の損害賠償責任が問題となり得ます*12。

なお、約款に、証券会社の故意または重過失に起因するものでない限り、証券会社は損害賠償責任を負わないという定めがある場合、当該条項は消費者契約法８条１項３号により無効と考えられます*13。

消費者が留意すべきポイント

消費者には、セキュリティに対する認識を深め、自らの財産を守るための対応を積極的に行うことが望まれます。利便性と安全はトレードオフの関係にあるという面があり、多少の利便性を犠牲にしてでも、より確実なセキュリティ対応を求めるべきです。

証券会社を選択するに際しては、当該証券会社が十分なセキュリティ対応を行っているか、また、万が一のときに適切な補償対応をしてもらえるかについても、十分な検討を行うことが大切です。特に、証券会社において大事な資金、多額の資金を運用する場合には、慎重な選択と利用が必要です。

今後の法制度等のあり方

証券口座の不正アクセス・不正取引事案については、まずは、その原因及び実態について、専門的な調査・解明が行われ、今後のセキュリティ対策の充実の観点からも、社会に対して適切な情報提供が行われることが望まれます。その際、証券会社ごとのセキュリティ体制の脆弱性（ぜいじゃく）やインシデント対応体制のあり方等についても、横断的な検討が行われ、各社の業務の高度化に生かされることが期待されます。

セキュリティ事案・不正アクセス事案においては、加害主体がより高度化しており、国家関連の主体の関与も指摘されています。こうした動きに適切に対応するには、資本力・組織力・技術力を有する事業者に対応を求めるほかなく、かかる対応を促す制度や体制が必要です。セキュリティ対応は、もはや金融サービスの重要な一部、社会的な基盤の一部となっているものであり、国際的な競争力の確保・向上という観点からも重要な課題と考えられます。

事業者の取組みを促す観点からも、セキュリティに関する責任は基本的に事業者が負う制度が望ましいと考えられます*14。セキュリティには専門性があり、市場による競争が働きにくい面があること、公正な取引を確保する観点からも、規制やガイドライン等により、全体の枠組みを整えることが極めて重要です。

*11 内容によっては、（消費者契約に限らず）民法548条の２第１項により、合意しなかったものとみなされることも考えられる
*12 電子マネー提供会社に関する事例だが、顧客への周知義務違反による事業者の損害賠償責任を認めたものとして東京高等裁判所平成29年１月18日判決がある
*13 *12の東京高等裁判所平成29年１月18日判決
*14 例えば、預金者保護法と同様の規律が望まれる

銀行口座への不正アクセス・不正送金

発生状況

警察庁によると*1、2025年上半期におけるインターネット・バンキングに係る不正送金事犯の発生件数は2,593件（うち個人は2,518件）、被害総額は約42億2400万円（うち個人は約19億4900万円）に上っています。フィッシングがその手口の約9割を占め、2019年頃からリアルタイム型フィッシングにより2段階認証を突破される手口が横行しています。

被害救済

銀行口座への不正アクセス・不正送金について、一般社団法人全国銀行協会は、個人顧客に過失がないときには原則として補償することとし、顧客に過失がある場合には個別対応をする旨の申し合わせを行っています*2*3。補償にあたって顧客には、金融機関への速やかな通知と十分な説明、及び捜査当局への被害事実等の事情説明（真摯（しんし）な協力）が求められます。

また、個人顧客のインターネット・バンキングの不正送金について、実務上、補償減額または補償しない扱いとする事例を、以下のとおり公表しています*4。

（1）銀行が複数回にわたり、個別的・具体的に注意喚起していたにも関わらず、注意喚起された手口により騙（だま）されて、ID・パスワード等を入力してしまった場合
（2）警察や銀行等を騙（かた）る者に対し、安易にID・パスワード等を回答してしまった、または安易に乱数表（暗証カード）を渡してしまった場合。その他、正当な理由もなく、ID・パスワード等を他人に教えてしまった場合
（3）お客さまがID・パスワード等を手帳等にメモしていたり、携帯電話等の情報端末等に保存しており、お客さまの不注意により当該手帳や携帯電話等が盗難等に遭う等して当該情報が盗取された場合
（4）以下のような事実があるにも関わらず、取引先の銀行への通報を怠っていた間に犯行が行われた場合
①上記（1）～（3）の事例にあるようなケースに該当すること
②通帳記帳やインターネット・バンキングサービスへのログインなどにより、身に覚えのない預金残高の変動があることを認識していたこと
③お客さまのパソコン等がウイルス感染するなどにより、インターネット・バンキングで不正な払戻しが行われる可能性を認識していたこと

インターネット・バンキングの不正送金事案における補償実績*5は、2021年度から2024年度の4年間で、処理方針を決定した24,889件について、補償を行ったもの（全額補償と一部補償）19,296件(77.5%)、補償を行わなかったもの5,593件(22.5%)と報告されています。補償率は、調査の結果、不正払戻しでないことが判明した件数等を除いた場合、86.0%となります。また、補償を行ったもののほとんどは全額補償です。

（坂　勇一郎）

*1 警察庁サイバー警察局「令和7年上半期におけるサイバー空間をめぐる驚異の情勢等について」（2025年9月）。個人と法人を含む件数・金額
*2 （一社）全国銀行協会「預金等の不正な払戻しへの対応について」（2008年2月19日）
*3 ATMによる預金の不正な払い出しについては、預金者保護法が被害救済の措置を定めているが、不正アクセス・不正送金には、適用されない
*4 （一社）全国銀行協会「インターネット・バンキングにおける預金等の不正な払戻しについて」（別紙2）（2016年6月14日）
*5 金融庁「偽造キャッシュカード等による被害発生等の状況について」（2025年6月10日）。個人と法人を含む件数