証券口座が危ない！急増する“乗っ取り”の手口と守りの極意

～フィッシング・マルウェア・相場操縦…最新手口から資産を守るアナリスト提言～

ライフデザイン研究部 主席研究員/テクノロジーリサーチャー 柏村 祐

1.あなたの証券口座が狙われている

想像してみてほしい。ある日突然、長年コツコツと築き上げてきたあなたの貴重な資産が、見知らぬ第三者の手によって弄ばれ、価値のないものに変えられてしまう光景を。これは決して SF の世界の話ではない。現在、オンライン証券取引の普及という利便性向上の裏側で、「証券口座乗っ取り」という深刻なサイバー犯罪が静かに、しかし確実に広がりを見せているのである。

本人の知らぬ間に保有株は売却され、換金性の低い、あるいは意図的に価格操作された銘柄へと姿を変える。被害者は金銭的な損失のみならず、大切な資産を蹂躙されたという精神的な苦痛、そして自身の情報管理に対する不安という重荷を背負わされる。

事実、金融庁が令和 7 年 4 月 18 日に更新した情報によると、証券会社のインターネット取引サービスにおける不正アクセス・不正取引被害は、2025 年に入り急増している。同年 2 月から 4 月 16 日までのわずか 3 ヶ月弱で、不正アクセス件数は 3,312 件、関連する不正取引件数は 1,454 件にのぼり、不正な売買総額（売却約 506 億円、買付約 448 億円）は約 954 億円規模に達している。これは、我々が直面する脅威がいかに現実的かつ差し迫ったものであるかを物語っている（注 1）。この問題は、単なる個人の不注意として片付けられるべきではない。アナリストとして、これをデジタル金融インフラそのものを揺るがしかねない重大な脅威と捉え、そのメカニズムを解明し、有効な対策を講じる必要性を強く訴える。

本レポートは、その実態と深層に迫り、我々が取るべき道筋を明確に示すことを目的とする。

2.なぜ“あなた”が狙われるのか？

なぜ、堅牢であるはずの証券口座が、いとも簡単に第三者の手に落ちてしまうのか。その背景には、複数の要因が巧妙に絡み合った、現代特有の脆弱性が存在する。攻撃

の糸口となるのは、多くの場合、IDやパスワードという「デジタル世界の鍵」の窃取である。その手口は、証券会社を騙る偽メールやSMSで利用者を欺き、本物と見分けがつかない偽サイト（フィッシングサイト）へと誘い込み、認証情報を入力させる古典的だが依然として強力なフィッシング詐欺である。特に、NISAの拡がりなど、国民的な関心事に乗じた手口は巧妙さを増している。あるいは、個人のPCやスマートフォンが、知らぬ間にマルウェアやスパイウェアという「デジタルスパイ」に感染し、キーボード入力情報や保存されたパスワードが筒抜けになっているケースも後を絶たない。これらは、不用意に開いたメールの添付ファイルや、何気なく閲覧したウェブサイトから侵入する。

さらに深刻なのは、「パスワードの使い回し」という悪しき習慣である。どこか一つのサービスから漏洩したパスワードが、まるで合鍵のように他のサービスへの不正アクセスを可能にしてしまう（リスト型攻撃）。単純なパスワードの設定は、いわば玄関のドアに鍵をかけずに外出するようなものである。加えて、二要素認証（2FA）や多要素認証（MFA）という「第二の鍵」を設定していない、あるいは突破されやすいSMS認証に頼っている状態は、防御体制の決定的な欠陥といわざるを得ない。証券会社側のシステムにおけるわずかな隙間や、外部システム連携（API）のセキュリティ不備が狙われる可能性も常に存在する。

そして、これらの技術的な問題に加え、利用者自身のセキュリティ意識、すなわち「デジタル護身術」の欠如も、攻撃者に絶好の機会を与えている。たとえば、不審なメールへの警戒心の薄さ、安全でないWi-Fi環境での無防備な取引、OSやセキュリティソフト更新の怠慢などがあてはまる。

これら一つ一つが、堅牢なはずの壁に穴を開ける要因となる。攻撃者は、単に資金を盗むだけではない。最近では、乗っ取った口座で既存資産を売却し、その資金で事前に仕込んだ流動性の低い銘柄（特に外国株などがターゲットになりやすい）を大量に買い付けることで株価を不正に吊り上げ、自らが別口座で保有する同銘柄を高値で売り抜けるという、悪質な相場操縦に利用するケースが報告されている。被害者の口座には売るに売れないジャンク銘柄だけが残り、直接的な資金流出を伴わないため、発見が遅れるという二重の罠が仕掛けられているのである（図表1）。

図表 1　証券口座乗っ取りの脆弱性構造

資料：筆者作成

3.アナリストが示す鉄壁の防御網

この巧妙かつ複合的な脅威に対し、我々はどう立ち向かうべきか。答えは、個人、証券会社、そして社会全体がそれぞれの持ち場で責任を果たし、多層的かつ重層的な防御壁を築き上げることにある。それは、単一の対策では決して達成できない、総力戦である。

1）個人での対策

まず、個人投資家、すなわち“あなた”自身が取るべき行動は、「デジタル資産の門番」としての意識改革から始まる。認証情報の管理は、もはや自己責任の範疇を超えた、資産防衛の最重要課題である。パスワードは決して使い回さず、複雑で強固なものを設定し、定期的に見直す。可能であればパスワード管理ツールの導入を検討すべきである。何よりも、二要素認証（多要素認証）は必須といえる。SMS認証だけでなく、認証アプリや物理トークンなど、より突破されにくい方式を選択することが、不正アクセスに対する決定的な防波堤となる。次に、フィッシング詐欺やマルウェアに対する「デジタル免疫力」を高めなければならない。メールやSMSのリンクは決して鵜呑みにせず、送信元を疑う眼をもつことが求められる。OSやセキュリティソフトを常に最新の状態に保つことは、いわばデジタル世界の予防接種のようなものである。安全なネットワーク環境を自ら維持・構築する意識が重要である。最後に、「異常の早期発見と迅速な初動」が被害を最小限に食い止める鍵となる。取引通知を必ず

確認し、定期的なログイン履歴・取引履歴・資産状況のチェックを怠らないことが重要である。僅かでも不審な点を発見した場合は、一刻も早く証券会社に連絡し、指示を仰ぐ。この初動の速さが、資産を守る最後の砦となり得るのである。

2）証券会社としての対策

証券会社は、顧客から資産を預かる者として、「デジタル要塞」としての役割を全うする責務がある。システムセキュリティの強化と不正検知能力の継続的な向上が不可欠である。アクセスパターン分析やAIを活用した不正取引検知システムの高度化は待ったなしの課題であり、脆弱性診断と迅速な修正対応は当然の義務である。また、より強固な認証オプション（生体認証、リスクベース認証等）の導入を積極的に推進し、顧客にその重要性を啓発していく必要がある。そして、利用者に対する継続的な情報提供を行いつつ、万が一の際のサポート体制を万全にしておくことは、信頼の維持において生命線となる。最新の脅威情報と対策を分かりやすく伝え、不正被害発生時には迅速かつ親身な対応を行うとともに、被害者救済に関する明確な方針を示すことも、顧客の不安を和らげる上で不可欠である。

3）社会・制度レベルでの対策

社会・制度レベルでは、業界全体で「セーフティネット」を構築する必要がある。日本証券業協会等の業界団体は、セキュリティ基準の底上げ（たとえば、強固な二要素認証の義務化検討）を主導し、金融庁はそれを後押しする役割を担う。また、国境を超えるサイバー犯罪に対抗するための捜査能力強化と国際的な連携は、警察庁をはじめとする関係機関の重要なミッションである。さらに、金融リテラシー教育の中に、実践的なサイバーセキュリティの知識を組み込むことは、将来世代を守るための長期的な投資となる（図表 2）。

図表 2　個人・企業・社会が担うべき役割と多層的な防御戦略

資料：筆者作成

4.脅威を直視し、進化する防御を

オンライン証券口座の乗っ取りと不正操作は、デジタル金融の利便性の影に潜む、現代社会の深刻なリスクである。フィッシング、マルウェア、パスワード管理の脆弱性、そして相場操縦という悪意など、その根は深く、手口は巧妙化の一途を辿っている。この見えざる脅威から我々の資産を守り抜くためには、付け焼き刃の対策では及

ばない。個人投資家一人ひとりの防衛意識の向上、証券会社の揺るぎないセキュリティ体制の構築、そして社会全体での監視と協力体制による三位一体の多層防御戦略こそが、唯一の有効な処方箋である。

個人は自らの資産を守る「第一責任者」として、パスワード管理、二要素認証、不審メールへの警戒、取引履歴の確認という基本動作を徹底しなければならない。証券会社は顧客の信頼に応えるべく、技術的・制度的な防御壁を絶えず強化し、万全のサポート体制を敷く必要がある。そして社会は、業界基準の向上、法執行体制の強化、国際協力、金融教育を通じて、安全な取引環境の土台を築き上げていかなければならない。

テクノロジーの進化は、我々の生活を豊かにする一方で、常に新たなリスクを生み出す。この現実から目を背けることなく、最新の脅威を的確に捉え、防御策を進化させ続けることこそが、デジタル金融時代の恩恵を将来にわたって安全に享受するための、我々に課せられた責務である。対策の先送りが招くのは、取り返しのつかない損失だけである。

【注釈】

1) 金融庁HPより
https://www.fsa.go.jp/ordinary/chuui/chuui_phishing.html