狙われる証券口座！今日から始める証券口座防衛術

～3,000 億円の被害を他人事にしないために～

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.“自分ごと”として捉えるセキュリティの重要性

「私の証券口座は、本当に大丈夫なのだろうか…？」。オンライン証券取引が私たちの資産形成において一般的となった現代、NISA 制度の拡充などを背景に、投資を始める人も増え、その利便性を誰もが享受できるようになった。しかし、手軽さの陰で、このような不安を感じたことはないだろうか。

実際に、国内外で報告される個人投資家の証券口座乗っ取り被害は後を絶たない。その深刻な実態は、金融庁が令和 7 年 5 月 8 日に更新した衝撃的なデータ（注 1）によって、より一層鮮明に浮かび上がる。2025 年に入り、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・不正取引被害は急増しており、不正アクセス件数は同年 1 月から 4 月末までのわずか 4 ヶ月間で 6,380 件、関連する不正取引件数は 3,505 件に達し、その結果として生じた不正な売買総額（売却約 1,612 億円、買付約 1,437 億円）は、約 3,049 億円規模にも膨れ上がっている。特に 2025 年 4 月には不正アクセス件数が 4,852 件と突出しており、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。

こうした被害の急拡大は、個人投資家が「自分だけは大丈夫」「面倒だから対策は後回し」という他人事的な意識ことが、いかに危険であり、取り返しのつかない事態を招きかねないかを突きつけている。

なお、前回配信したレポート（「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」（注 2））では、主に証券口座乗っ取り被害の全体像と、その対策における個人・企業・社会それぞれの役割について概観し、広範な視点からの警鐘を鳴らした。本レポートは、その問題提起を踏まえ、特に個人投資家が直面する具体的な脅威と、「今日から」取り組める実践的な防衛策、さらには万が一の際の行動計画に至るまで、より一歩踏み込んで詳説する。

本レポートは、投資初心者からある程度の経験者まで、オンラインで資産を運用する全ての人が、この脅威の本質を深く理解し、具体的な攻撃のメカニズムを学ぶとともに「鉄壁の個人防衛術」を身につけることで、自らの手で大切な資産を守り抜くための一助となることを目指すものである。

2.なぜ“あなたの”口座が標的に？

本節では、攻撃者が証券口座を狙う代表的な手口と、我々自身が、知らず知らずのうちに抱えがちなセキュリティ上の脆弱性について、深く掘り下げて解説する。

1)「デジタル世界の鍵」を狙う常套手段

攻撃の糸口となるのは、依然としてIDやパスワードといった「デジタル世界の鍵」の窃取である。その代表格が、まるでカメレオンのように姿を変え、私たちの日常に溶け込もうとするフィッシング詐欺である。

証券会社や著名な金融機関、時には公的機関を騙る偽の電子メールやSMS（スミッシングと呼ばれる、SMSを悪用して詐欺目的のメッセージを送り、受信者を偽のウェブサイトに誘導して個人情報を盗み取る手口）は、ロゴや文面、ウェブサイトのデザインに至るまで、本物と見分けがつかないほど巧妙に作り込まれ、私たちの警戒心を巧みにすり抜ける。「お客様のアカウントで異常な取引が検知されました。これらは、セキュリティ保護のため、至急ご確認ください」といった緊急性を煽る文言や、「システムの大規模アップデートに伴い、お客様情報の再認証が必要です」といった、もっともらしい理由をつけてメッセージの受信者を偽サイトへと誘い込む。

これらのメッセージに含まれるリンクは、本物のウェブサイトを寸分違わず模倣しており、そこにIDやパスワード、秘密の質問といった情報を入力すると、全ての認証情報が瞬く間に攻撃者の手に渡ってしまう。

また、目に見えない脅威であるマルウェアやスパイウェアによる情報窃取も、依然として深刻な「デジタル感染症」として猛威を振るっている。これらは、不用意に開いたメールの添付ファイルや、何気なく閲覧した改ざんされたウェブサイト、あるいは魅力的に見える無料アプリなどに潜んで、知らぬ間に個人のPCやスマートフォンに侵入する。

一度感染すると、キーボードの入力情報を盗み取る「キーロガー」、画面の情報を盗撮する「スクリーンキャプチャ」、保存された認証情報を外部に自動送信するスパイ機能などによって、個人のデジタルライフは丸裸にされ、攻撃者はその人の資産へのアクセス情報を手に入れてしまうのだ。

2)「第二の鍵」も油断大敵

多要素認証（MFA）という「第二の鍵」を設定していれば絶対安全という神話も、残念ながら過去のものとなりつつある。攻撃者は常にその防御を打ち破ろうと新たな手口を編み出すからである。

近年では、MFAのプッシュ通知を標的の利用者に執拗に送り付け、根負けした利用者の誤操作による承認を狙う「MFA疲労攻撃」という、いわば「デジタルのドアノッ

ク攻撃」や、携帯電話事業者のオンライン手続きの不備を悪用したり、言葉巧みに従業員を騙したりして SIM カードを不正に再発行させ、SMS 認証という「通信経路の脆弱性」を乗っ取る「SIM スワップ詐欺」といった、MFA そのものを突破しようとする攻撃手法も報告されている。

加えて、ソーシャルエンジニアリングと呼ばれる、人間の心理的な隙、たとえば親切心や権威への服従、あるいは恐怖心といった感情を巧みに操り、電話やメッセージを通じて認証コードそのものを聞き出そうとする「言葉巧みな詐欺師」の存在も忘れてはならない。彼らは、人々の良心や不安につけ込み、重要な情報を引き出そうとするのである。

パスワード管理の甘さもまた、攻撃者に「どうぞ入ってください」と、みすみす扉を開けてしまうようなものである。誕生日や名前、ありふれた単語(例:「password123」)といった推測されやすいパスワードの使用や、複数のオンラインサービスで同じパスワードを使い回すという「合鍵の大量生産」は、一度どこかのサービスで情報漏洩が発生した場合に、他のサービスへの不正アクセスを連鎖的に引き起こす「リスト型攻撃」の格好の餌食となる。それは、たった一つの鍵穴から、家中の扉が開けられてしまうようなものである。安全でない場所にパスワードをメモとして書き残す行為は、もはや論外と言わざるをえない。

3)日常生活に潜む危険

また、カフェなどで提供される場合がある、セキュリティ設定が不確かな公衆 Wi-Fi 環境や、不特定多数が利用する共有 PC からの証券取引は、通信内容が第三者に傍受されたり、端末自体が「デジタル病原体」に汚染されていたりするケースがあり、リスクがある。

OS やセキュリティソフトの更新を怠る、「面倒だから」と後回しにする、不審なメールやウェブサイトへの警戒心が希薄であるなど、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」の欠如もまた、攻撃者に絶好の機会を与えてしまう。

これらの個人の脆弱性が重なることで、攻撃者は不正アクセスの糸口を見つけ出し、個人の資産を狙い撃ちにするのである（図表 1）。

図表１　あなたの証券口座の"隙間"はどこか？

資料：筆者作成

3.個人でできる鉄壁のセキュリティ防衛策

これまで述べてきたような、姿を変える忍者や、音もなく忍び寄る刺客のようなサイバー攻撃に対し、我々個人は具体的にどのような「防御の盾」を構え、どのような「鉄壁の砦」を築けば、大切な資産を守り抜くことができるのだろうか。

本節では、個人レベルで「今日から築く」ことができる、多層的かつ効果的なセキュリティ防衛策を、具体的な行動ステップとして詳述する。これらは、決して難しいことばかりではない。むしろ、日々の小さな心がけと行動の積み重ねこそが、デジタル資産を守る巨大な防波堤となる。

1)認証情報の徹底強化

不正アクセスの最初の扉を固く閉ざすには、認証情報の徹底的な強化が不可欠である。

まず、パスワードは、推測されにくい、長く複雑な文字列、すなわち英大文字・小文字・数字・記号をすべて組み合わせ、最低でも 12 文字以上、可能であれば 15 文字以上の「あなただけの難解な呪文」を作成し、利用するオンラインサービスごとに必ず異なる固有のものを設定する「一所懸命の鍵」運用を鉄則とすべきである。

次に、二要素認証（MFA）という「第二、第三の防壁」は、もはや選択ではなく、現代のデジタル社会における「必須装備」と認識し、特にSMS認証よりもセキュリティ強度が高いとされる認証アプリ（TOTP型：Time-based One-Time Passwordの略で、一定時間ごとに新しいパスワードを生成する方式）や、究極の防御策ともいえるハードウェアセキュリティキーの導入を積極的に検討すべきである。ハードウェアセキュリティキーは、USBキーのような物理的なデバイスで、これをPCなどに接続し、キーにタッチするなどの物理的操作を行うことで認証が完了する。オンライン上の攻撃だけでは突破されにくいという特徴がある。

この一手間が、資産を守る「見えざる防壁」となる。

2)利用環境のクリーン化

証券取引に利用するパソコンやスマートフォンといった端末と、インターネット通信環境の安全確保もまた、極めて重要な防衛策である。

OS（オペレーティングシステム）やウェブブラウザ、インストールしている各種ソフトウェアは常に最新の状態に保つよう徹底し、発見された脆弱性の課題に迅速に対処しなければならない。可能であれば自動更新機能を有効にし、常に最新の状態に保つことが望ましい。

信頼できる総合セキュリティソフト（アンチウイルスソフト）を導入・運用し、マルウェアの侵入や不正なウェブサイトへのアクセスをブロックすることも不可欠である。

最も重要なのは、これらのツール任せにせず、利用者自身が「セキュリティ意識」を常にアップデートし続けることである。新しい手口の情報をキャッチし、怪しいメールやウェブサイトに対する警戒心を磨くことが、真に安全な利用環境を築く上で欠かせない。

3)安全なネットワーク利用

カフェや空港などの公衆無線LAN（フリーWi-Fi）は便利だが、その利便性の裏には情報漏洩のリスクが潜んでいることを忘れてはならない。

これらのネットワークで証券取引や個人情報の入力といった機密性の高い通信を行う際は、信頼できるVPN（Virtual Private Network：仮想プライベートネットワーク）サービスを利用し、通信内容を「秘密のトンネル」で暗号化することを強く推奨する。VPNは、データを第三者の目から守るための有効な手段となる。

また、自宅のWi-Fiルーターについても、初期設定のままの安易な管理者パスワード管理ではなく、ファームウェアを常に最新の状態に保つなど、セキュリティ設定を定期的に見直すことが重要である。

4)口座の常時監視と異常の早期発見

とはいえ、どれほど強固な対策を施したとしても、100%安全と言い切ることは難しいのがサイバーセキュリティの現実である。そのため、万が一不正アクセスや不審な取引が発生した場合に、それをいち早く察知し、被害を最小限に食い止めるための「口座の常時監視」と「異常の早期発見」の体制を整えておくことも重要である。

具体的には、証券口座へのログイン履歴や取引履歴を定期的に確認することを習慣化すべきである。確認すべきポイントとしては、身に覚えのない日時や場所からのログイン試行の有無、覚えのない株式の売買注文や出金指示、登録情報の変更履歴などであり、最低でも週に一度、可能であればより頻繁にチェックし、「口座の定期的な確認」を行うことが推奨される。

多くの証券会社は、ログイン通知、出金通知、取引成立通知、登録情報変更通知といった各種アラートを電子メールやSMSで受け取れる「警報システム」を提供している。これらの通知サービスを積極的に活用し、通知があった場合は速やかにその内容を確認する癖をつけることが、異常の早期発見に繋がる。

もし、ログイン履歴や取引履歴、あるいは各種通知の中に少しでも不審な点や身に覚えのない動きを発見した場合は、決して自己判断で放置したり、「気のせいだろう」と見過ごしたりせず、まずは落ち着いて関連情報を再確認した上で、速やかに取引先の証券会社に連絡し、状況を報告するとともに指示を仰ぐことが肝要である。この初動の速さが、被害の拡大を防ぐ「防火シャッター」となる（図表2）。

図表 2　あなたの資産を守る「鉄壁の砦」

資料：筆者作成

4.万が一の事態に備える行動計画

どれほど入念なセキュリティ対策をしても、サイバー攻撃の手口は日々進化しており、100%の安全を保証することは残念ながら不可能である。それは、攻撃者との「終わらない鬼ごっこ」、あるいは「知恵比べ」のようなものである。

したがって、万が一、不正アクセスや不正取引の被害という「想定外の事態」に遭遇してしまった場合に、その被害を最小限に食い止め、冷静沈着に「反撃の狼煙」を上げるための具体的な行動計画を事前に準備し、パニックに陥らずに対応できる心構えをもっておくことが極めて重要となる。

1)緊急時の初動対応

不正アクセスや不正取引の被害が疑われる、あるいは発覚した場合に取るべき行動は、まず一刻も早く取引先の証券会社に電話等で緊急連絡を取り、口座の一時凍結を依頼するとともに、不正アクセスや不正取引の疑いがある旨を明確に報告することである。

同時に、証券口座のログインパスワードはもちろんのこと、同じパスワードを使い回している可能性のある他のオンラインサービス（特にメールアドレスやネットバンキングなど）のパスワードも速やかに変更する。

可能であれば、不正アクセスに利用された疑いのあるパソコンやスマートフォンは、さらなる情報漏洩やマルウェアの活動を防ぐため、一時的にインターネットから切断

し、セキュリティソフトで完全スキャンを実行することが望ましい。

2)証拠の収集と保全

次に、証券会社のウェブサイトや取引ツールにログインし（必ず証券会社の指示に従うこと）、不正なログイン履歴（日時、IPアドレスなど）、身に覚えのない取引履歴（銘柄、数量、日時、約定価格など）、不正な出金履歴（金額、出金先口座など）といった情報を詳細に確認し、可能な限りスクリーンショットやPDFファイルとして記録・保存する。

また、不正アクセスに繋がった可能性のある不審なメールやSMSの本文、送信元アドレス、ヘッダー情報、あるいはウェブサイトの閲覧履歴、マルウェア感染の警告画面なども、重要な「事件解決の糸口」となり得るため、削除せずに保存しておく。

3)関係各所への連絡と相談

そして、最寄りの警察署のサイバー犯罪相談窓口、または各都道府県警察本部のサイバー犯罪対策課に被害を届け出ることが基本となる。被害届の提出には、収集した証拠資料が役立つ。

独立行政法人情報処理推進機構（IPA）や日本サイバー犯罪対策センター（JC3）などの公的機関も、サイバーセキュリティに関する相談窓口を設けており、的確なアドバイスを受けることができる。

クレジットカード情報が盗まれ不正利用された疑いがある場合は、速やかにカード発行会社にも連絡し、カードの利用停止と再発行の手続きを行う必要がある。

被害額が大きい場合や、法的な対応が必要と判断される場合は、一人で抱え込まず、サイバー犯罪に詳しい弁護士などの専門家への相談も検討することが、問題解決への近道となる。

4)今後の脅威と継続的な対策の重要性

今後も、AIによる巧妙なフィッシングメール、ディープフェイクを用いた精巧ななりすまし、IoTデバイスの脆弱性を悪用した侵入など、サイバー攻撃の手口は想像を超える速さで高度化・巧妙化すると予測される。これは、まさにテクノロジーの進化が生み出す「光と影」である（図表3）。

図表 3　進化するサイバー脅威と継続的な対策サイクル

資料：筆者作成

このような進化し続ける脅威に対抗するためには、個人一人ひとりが常に最新のセキュリティ情報をキャッチし、自身の知識や対策を継続的にアップデートし続ける積極的な姿勢が不可欠である。

「自分だけは大丈夫」という根拠のない過信は「最大の敵」であり、常に一定の警戒心を持ち続ける心構えが重要である。

本レポートで紹介した各種対策を地道に実践し、定期的にその有効性を見直すこと、そして何よりも自身の資産を守る最終的な責任は自分自身にあるのだという強い「当事者意識」と「自己防衛の精神」をもつことが、安全なオンライン証券取引を継続していく上での揺るがぬ鍵となる。

テクノロジーの進化は、我々の生活を豊かにし、資産形成の可能性を大きく広げて

くれる。その恩恵を将来にわたって安全に享受するためには、リスクから目を背けるのではなく、それを的確に捉え、防御策を進化させ続けることこそが、我々に課せられた責務である。

【注釈】

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

2) 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～
https://www.dlri.co.jp/report/ld/441951.html