2025 年 9 月 1 日　全 10 頁

今後の証券業界において求められる不正アクセス等防止策とは

金融庁と日本証券業協会がインターネット取引の新指針案を公表

金融調査部　研究員　谷 京

［要約］

■ 2025 年前半、日本の証券業界はインターネット取引サービスでの不正アクセス・不正取引の被害に揺れた。犯罪組織が多数の証券口座を乗っ取り、株式を不正売買したとみられる。2025 年 7 月 15 日、金融庁と日本証券業協会は証券口座の乗っ取り事件を受け、インターネット取引における認証方法や不正防止策を強化すべく、それぞれ「『金融商品取引業者等向けの総合的な監督指針』等の一部改正（案）」（以下、監督指針改正案）および「『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（案）」（以下、ガイドライン改正案）を公表した。

■ 米国では日本よりも先に、証券口座の乗っ取りによる株式やオプションの不正取引が発生していた。これを受け、金融業規制機構（FINRA）や証券取引委員会（SEC）は多要素認証の導入を強く推奨し、フィッシング攻撃や内部脅威への対策を促してきた。また、SEC 規則でも個人情報保護やインシデント対応計画の策定、情報漏洩時の顧客通知義務などが定められた。米国証券業界では、多要素認証をはじめとする不正アクセス等防止策が事実上の業界標準になっていると考えられる。

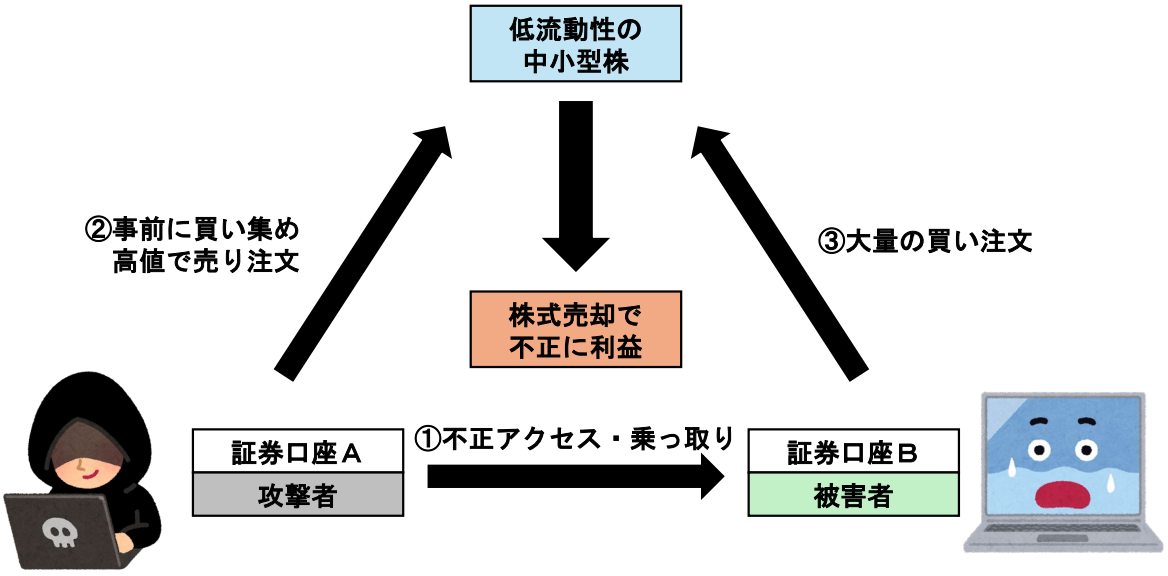
■ 監督指針改正案では、インターネット取引に特有のリスクを踏まえ、内部管理態勢・セキュリティ確保・顧客対応の 3 点を主な着眼点として、多要素認証の実装および必須化や不正アクセス検知・通知システムの導入などが求められている。また、ガイドライン改正案も重要な操作時の多要素認証を「対応が必要とされる事項」に引き上げるとともに、不正アクセス発生時の関係機関への報告・連携強化を義務付けた。

■ 監督指針改正案およびガイドライン改正案は、特にフィッシング詐欺対策に重点を置いている。今後の証券業界では、単に複数の認証要素を組み合わせるだけでなく、公開鍵暗号方式を用いた多要素認証などを採用し、フィッシング詐欺対策に取り組むことが求められる。なお、生体認証はフィッシング耐性のある多要素認証の構成要素であるものの、すべての生体認証がフィッシング耐性のあるものと認められるわけではない点には注意が必要であろう。

1. 証券口座の乗っ取り事件を受けた金融庁と日本証券業協会の対応

2025 年前半、インターネット取引サービスでの不正アクセス・不正取引（第三者による取引）の被害が、証券業界を大きく揺るがした。2025 年 1 月から 7 月末までに、証券会社を狙った不正取引は 8,111 件、不正取引金額は約 6,205 億円に達した[1]。攻撃者が多数の証券口座を乗っ取り、不正に株式を売買することで利益を得たとみられる（図表 1）。証券口座の乗っ取り被害が確認された証券会社は、ネット・対面の大手から中堅まで、2025 年 6 月時点の累計で 17 社に上った[2]。堅調な株式市場や少額投資非課税制度（NISA）の改正も相まって、ようやく日本でも動き出した「貯蓄から投資へ」に水を差す事件といえよう。

図表 1　証券口座の乗っ取りによる不正取引のイメージ



（出所）大和総研作成（イラストは「かわいいフリー素材集 いらすとや」）

証券口座の乗っ取り事件を受け、金融庁は 2025 年 7 月 15 日、インターネット取引における認証方法や不正防止策を強化するための「『金融商品取引業者等向けの総合的な監督指針』等の一部改正（案）」（以下、監督指針改正案）を公表した[3]。また、日本証券業協会も同日、「『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』の改正について（案）」（以下、ガイドライン改正案）を公表した[4]。すでに多くの証券会社が不正アクセス等への対策として、インターネット取引のログイン時における多要素認証の設定必須化を決定している。その中で、監督指針改正案とガイドライン改正案は、一般的なワンタイムパスワードの入力を求める方式よりも高度な多要素認証の実装を求める内容となった。

ところで、他人の証券口座を乗っ取ったハッカーが不正に株式を売買するという事件は、規模

[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」令和 7 年 8 月 7 日更新。
[2] 「証券口座乗っ取り対策、生体認証を必須に 金融庁・日証協が新指針」日本経済新聞、2025 年 7 月 15 日。
[3] 金融庁「『金融商品取引業者等向けの総合的な監督指針』等の一部改正（案）の公表について」令和 7 年 7 月 15 日。
[4] 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（案）」2025 年 7 月 15 日。

の大小という違いこそあるものの、実は米国でも 2000 年代半ば以降に散発していた。そして、金融分野における多要素認証の重要性を強調する報告書や通知が当局や自主規制機関により作成され、すでに米国証券業界では多要素認証が事実上不可欠のセキュリティ対策として定着しているとみられる。

そこで、本稿では先行事例として、米国における証券口座の乗っ取り事件と関連規制を紹介する。その上で、監督指針改正案とガイドライン改正案の内容を概観し、今後の証券業界において求められる不正アクセス等防止策を論じたい。

2. 米国における証券口座の乗っ取り事件と関連規制

米国では、早くも 2006 年には大手ネット証券を狙った大規模ハッキング被害が発生した。攻撃者は、他人のキーボード入力情報を盗み取ることで証券口座に不正アクセスし、当該口座が保有する株式を無断で売却した。そして、その資金を使って、自らが仕込んだ銘柄の株式を大量購入させ、株価を人為的に吊り上げるという手口で利益を得た[5]。また、2017 年末には、少なくとも 31 の米国個人投資家口座をハッキングして不正に株式を売買し、100 万ドル以上の利益を得た事件が発生した。こちらも同様に、攻撃者は乗っ取った証券口座で低流動性の小型株を購入して株価と出来高を吊り上げ、自らが保有する同銘柄の株式を高値で売り抜けたという[6]。

2020 年以降も、パンデミック下で個人投資家のオンライン取引が急増したことに乗じ、証券口座の乗っ取り事件が発生した。特に、著名な投資アプリでは数千件規模のアカウント侵害が起こった。この時期の乗っ取り事件では、先述したような株式の不正売買だけでなく、不正なオプション取引による相場操縦も行われた。すなわち、攻撃者はほぼ無価値で市場の関心が低い「アウト・オブ・ザ・マネー」のオプションを仕込んだ上で、乗っ取った証券口座に高値でオプションを購入させることで利益を得たとみられる[7]。レバレッジ効果のあるオプションの不正取引では、短期間に多額の被害が生じ得るため、株式の不正取引より悪質な手法といえる。

米国では、証券口座の乗っ取りとは異なる手法の事件も起こっている。2013 年から 2014 年にかけて、大手金融機関のネットワークサーバーへの不正アクセスにより、大量の顧客情報（社会保障番号やメールアドレス、その他の機密データ）が流出した。顧客情報を入手した攻撃者は、無価値な小型株の価格を吊り上げるためのスパムメールを一斉に送信することで株価操作を図ったとされる[8]。

このような証券口座の乗っ取りや不正アクセスを受けて、米国証券業の自主規制機関である金融業規制機構（FINRA）は多要素認証の導入を推進してきた。まず、2018 年 12 月のサイバー

[5] Ellen Nakashima, “Hackers target online stock accounts” in NBC NEWS, 2006/10/24.
[6] “SEC Charges 18 Defendants in International Scheme to Manipulate Stocks Using Hacked US Brokerage Accounts” in U.S. Securities and Exchange Commission, 2022/8/15.
[7] “FINRA Reminds Firms to Be Aware of Fraudulent Options Trading in Connection With Potential Account Takeovers and New Account Fraud” in FINRA, 2020/9/17; “FINRA Shares Practices Firms Use to Protect Customers From Online Account Takeover Attempts” in FINRA, 2021/5/12.
[8] “Scottrade Breach Hits 4.6 Million Customers” in Krebs on Security, 2015/10/2.

セキュリティ実務報告では、フィッシング攻撃や内部脅威（組織内の人物や関係者によって引き起こされるセキュリティリスク）の対策として、多要素認証に言及した。2020 年 10 月の情報通知でも、ユーザーが本人であるかどうかを確認・認証するための「要素」を五つに分けて整理した上で（図表 2）、単一要素認証が悪意のある攻撃者に対して脆弱である一方、多要素認証は「二つ以上の異なる種類の要素や秘密情報を使用することで、パスワードなど一つの認証情報が漏洩した場合でも、アカウントが侵害される可能性を大幅に低減できる」としている [9]。

図表 2　認証における「要素」

①　知っていること	ユーザーが記憶している秘密の情報に基づく認証 例）パスワード、PIN コード
②　持っているもの	ユーザーが所持している物理的またはデジタルなトークンに基づく認証 例）専用端末・スマホアプリ・SMS 等で送信されるワンタイムパスワード
③　本人であること	ユーザーの身体的特徴に基づく認証 例）指紋認証、顔認証、虹彩スキャン、声紋認証
④　いる場所	ユーザーの地理的な位置情報に基づく認証 例）IP アドレスによる位置判定、国外からのアクセス検出
⑤　行動	ユーザーの操作や動作に基づく認証 例）画面上のジェスチャー・タッチ操作、登録デバイスでの確認通知

（出所）“Cybersecurity Background: Authentication Methods” in FINRA, 2020/10/15 より大和総研作成

また、2021 年 5 月の規制通知では、証券口座の乗っ取り対策に関する業界ヒアリング結果を共有した。同通知は「新たな法的・規制上の義務や既存の義務の新たな解釈を示すものではない」としながらも、多要素認証の導入を含むベストプラクティスを列挙し（次ページ図表 3）、各社が自社のリスクプロファイルや業態、業務規模に応じてこれらの対策を採用するよう促している。特に多要素認証については、メールアカウント自体の乗っ取りが多発していることから、メールアドレスを認証要素として用いることの危険性について注意喚起しつつ、SMS でのパスコード送信や電話による確認、認証アプリ、生体認証など多様な手段を組み合わせて本人認証を強化することが奨励されている [10]。

米国証券取引委員会（SEC）も、証券会社や投資顧問向けにサイバーセキュリティ上の期待事項を示してきた。たとえば、2020 年 9 月のコンプライアンス検査局（OCIE）リスクアラートは、証券口座への一連の不正アクセス事案（クレデンシャル・スタッフィング）を受けて発出され、多要素認証の重要性を強調している。具体的には、「適切に実装された多要素認証は、パスワード関連の攻撃に対する最も有効な防御策の一つとなり、証券口座乗っ取りのリスクを大幅に低減できる」とする一方、SMS でのパスコード送信による認証は携帯電話会社のセキュリティ対策に依存するため万全ではないとも述べ、他人の電話番号を不正に奪取する手口（SIM スワップ）への警戒を促している [11]。

---

[9] “Cybersecurity Background: Authentication Methods” in FINRA, 2020/10/15.
[10] “FINRA Shares Practices Firms Use to Protect Customers From Online Account Takeover Attempts” in FINRA, 2021/5/12.
[11] “Cybersecurity: Safeguarding Client Accounts against Credential Compromise” in SEC, 2020/9/15.

図表 3　FINRA ラウンドテーブルで共有されたベストプラクティス

オンライン口座開設時の本人確認	提出書類の検証	社会保障番号・住所・運転免許証などの情報を確認、顔写真の一致確認
	追加情報の要求	追加書類や質問で本人確認
	外部ベンダー活用	疑わしい情報の検証支援やデータベース照合を委託
ログイン時の認証	多要素認証	パスワード＋SMS や認証アプリで安全性向上
	適応型認証	ログインリスクや取引リスクを評価し、必要に応じて追加認証を要求
	補完的認証要素	SMS・電話・位置情報・生体認証など
バックエンド監視・制御	異常検知	ログイン失敗の急増・大口取引・メールアドレス変更後の送金依頼などを監視
	広域監視	多数口座でのログイン試行・失敗の急増を検知
	資金移動制御	電話確認等で不正送金を防止
	ダークウェブ監視	企業名・口座番号・役員名・パスワードなどの流出情報を検知
乗っ取り発生時の対応手順	専任チーム設置	顧客口座乗っ取りの調査を専門に行うチームを設置
	顧客対応強化	頻繁な状況報告、アカウント・ロックや取引停止時間を最小化
	連絡手段の提供	音声・チャットによる即時対応窓口
	全口座の調査	問題のある口座が見つかった場合、他の口座も確認
	セキュリティ対策の再通知	多要素認証などの推奨事項を顧客に再通知
自動脅威検知	WAF[12]や社内ツールの活用	大量ログイン試行をブロックし、クレデンシャル・スタッフィング（漏洩した ID とパスワードの組み合わせを使った他サービスへのログイン攻撃）を阻止
	IP 隔離	不審な IP アドレスを隔離
	地理的制御	不審な地域からの接続を拒否
アカウント復旧	パスワードリセット時の二段階認証	SMS コードによる認証
	コールセンター対応	ダークウェブや SNS に出回りにくい情報を使った本人確認
投資者教育	セキュリティ啓発	教材提供、通知機能、高齢者向け教育

（出所）“FINRA Shares Practices Firms Use to Protect Customers From Online Account Takeover Attempts”

[12] Web アプリケーションの脆弱性を突くサイバー攻撃から情報を保護するセキュリティシステムのこと。

in FINRA, 2021/5/12 より大和総研作成

さらに、証券口座の乗っ取りに関連する SEC 規則として、Regulation S-ID（2013 年制定）と Regulation S-P（2024 年改正）が挙げられる。前者は、証券会社や投資顧問など SEC 登録業者に対し、顧客の個人情報を悪用した詐欺等を防ぐための体制整備を義務付けた個人情報盗難防止規則（Red Flags Rule）である。具体的には、住所・連絡先の変更や異常な口座利用といった警戒すべき不正の兆候（Red Flags）を検出し、個人情報の盗難を防止・軽減するための書面化された「本人確認プログラム」を策定するよう求めている[13]。

後者は、SEC がグラム・リーチ・ブライリー法（1999 年制定、金融機関に対して顧客の個人情報の保護を義務付ける法律）に基づき、SEC 登録業者に対して顧客の個人情報を保護するためのプライバシーおよびセキュリティ対策を求めるものである。顧客情報保護ルールを現代化し、2000 年制定当時から激変したサイバー環境に対応すべく、24 年ぶりの大幅な改正が行われた。この改正により、証券会社や投資顧問はデータ漏洩発生時の顧客保護と報告体制を大幅に強化することとなった。具体的には、顧客情報への不正アクセスを検出・対応・回復するためのインシデント対応計画の策定が義務化され、データ漏洩発生時には影響を受けた顧客に対する 30 日以内の書面通知も義務付けられた[14]。

これらの規則は、多要素認証をはじめとする特定技術の実装を明示的に義務付けてはいない。とはいえ、顧客情報を保護するための技術的対策を求める文脈において、多要素認証の導入は事実上の標準的な義務履行方法として捉えられているように思われる。実際、FINRA は 2024 年 10 月、内部脅威対策として業務用メールアカウントに多要素認証を導入していなかったために顧客情報の流出を招いた証券会社 2 社に対し、罰金を科している[15]。

3. 監督指針改正案とガイドライン改正案の内容

2025 年 7 月 15 日、金融庁と日本証券業協会は証券口座の乗っ取り事件を受け、それぞれ監督指針改正案とガイドライン改正案を公表した。

監督指針改正案における最大の変更点は、インターネット取引に関する定め（Ⅲ-2-8-2）の新設である。ここでは、非対面で行われるインターネット取引は「異常な取引態様を確認できないことなどの特有のリスクを抱えている」ため、「金融商品取引業者においては、利用者利便を確保しつつ、利用者保護の徹底を図る観点から、インターネット取引に係るセキュリティ対策を十分に講じるとともに、顧客に対する情報提供、啓発及び知識の普及を図ることが重要である」ことを前提に、①内部管理態勢の整備、②セキュリティの確保、③顧客対応の 3 点が「主な着眼

[13] “Identity Theft Red Flags Rules” in SEC, 2013/5/17.
[14] “SEC Adopts Rule Amendments to Regulation S-P to Enhance Protection of Customer Information” in SEC, 2024/5/16.
[15] “Finra Fines, Censures Osaic and Securities America Over Cybersecurity Lapses” in AdvisorHub, 2024/3/15.

点」として掲げられている[16]。

特にセキュリティの確保に関しては、重要な操作時（ログイン、出金、出金先銀行口座の変更など）におけるフィッシング耐性のある多要素認証の実装および必須化や不正アクセス検知・通知システムの導入、認証に連続して失敗した場合のアカウント・ロックの自動発動機能の実装および必須化といった具体策が盛り込まれた。また、フィッシング詐欺を未然に防止するために講じるべき措置として、証券会社から顧客宛てに送るメールや SMS 内にパスワード入力を促すページの URL やログイン画面へのリンクを記載しないことや、フィッシングサイトの閉鎖依頼を実施することなども明文化された[17]。

さらに、「監督手法・対応」の項目では、金融商品取引業者がインターネット取引における不正アクセス・不正取引を認識した場合には、「速やかに『犯罪発生報告書』にて当局宛てに報告することを求める」とともに、「犯罪防止策や被害発生後の対応について、必要な検討がなされず、被害が多発するなどの事態が生じた場合など、投資者保護の観点から問題があると認められる場合には、法第 51 条に基づき業務改善命令を発出する等の対応を行う」と明記された[18]。

ガイドライン改正案でも、インターネット取引の各段階で不正アクセス防止策を強化し、顧客資産の安全を確保するための抜本的な見直しが行われた。具体的には、これまでは「対応することが望ましいとされる事項」（ベストプラクティス）との位置付けであった重要な操作時におけるフィッシング耐性のある多要素認証の実装および必須化を「対応が必要とされる事項」（スタンダード）に引き上げた。また、重要な操作時だけでなく取引時においても多要素認証を提供することや、顧客の要望に応じて取引可能な商品や取引金額の上限を制限できるようにすることが、ベストプラクティスに追加された[19]。

多要素認証以外では、不正アクセス発生時の関係機関への報告・連携強化もベストプラクティスからスタンダードに引き上げられた。すなわち、①金融当局への報告、②捜査当局との連携、③その他市場関係者（取引所、日本証券業協会等）との連携・報告、④銀行との連携という 4 点について、不正アクセス発生時を想定した社内態勢の整備が義務化された。とりわけ銀行との連携に関しては、「銀行口座との連携サービスを提供している場合には、攻撃者が証券口座への不正アクセスにより、銀行預金を証券口座に移し株式を購入する被害も想定されることから、連携する金融機関との対応について整理する」ことがスタンダードに位置付けられ、銀行口座から証券口座への出金に係る認証強度の確認や、顧客被害発生時の連携元・連携先の間の被害拡大防止に向けた協力体制の確立、連携元・連携先における責任・役割分担の明確化が求められている[20]。

---

16 「(金融商品取引業者等向けの総合的な監督指針（新旧対照表））（案）」金融庁、2025 年 7 月 15 日、3-9 ページ。
17 同資料、4-8 ページ。
18 同資料、9-10 ページ。
19 「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（案）」日本証券業協会、2025 年 7 月 15 日、3-4 ページ。
20 同資料、8-10 ページ。

4. 今後の証券業界において求められる不正アクセス等防止策

今回の監督指針改正案およびガイドライン改正案により、今後の証券業界において求められるであろう主な不正アクセス等防止策を整理すると、図表 4 のとおりである。

図表 4　今後の証券業界において求められる主な不正アクセス等防止策

項目	従来の監督指針・ガイドライン	2025 年改正案
ログイン時の認証	✓ 複雑なパスワード（推測可能なパスワードの抑止）	✓ フィッシング耐性のある多要素認証の実装・必須化
出金・銀行口座変更	✓ 複雑なパスワード ✓ 多要素認証（顧客選択制）	✓ フィッシング耐性のある多要素認証の実装・必須化
不正アクセスの検知・遮断	✓ 顧客のログイン時の挙動の分析による不正アクセスの検知（振る舞い検知） ✓ 不正アクセスの評価に応じ、追加の本人認証や適時遮断対応	✓ 左記に加えて、不正なログインや異常な取引を検知し、速やかに顧客に連絡する体制の整備 ✓ これらの検知・通知機能の顧客の利用状況確認と普及の促進
フィッシング詐欺対策	✓ 特に規定なし	✓ メールや SMS からログイン誘導リンクを排除 ✓ ウェブサイトやメッセージが正規であることの証明 ✓ フィッシングサイトの閉鎖依頼 ✓ 送信ドメイン認証技術の導入
不正アクセス発生時の対応	✓ 迅速かつ真摯な顧客対応 ✓ 関係機関との連携強化に向けた対応を整理（努力義務）	✓ 顧客対応の具体化（アカウント・ロックや取引及び出金の制限等） ✓ 一時凍結後の再開手続きでも本人確認を実施 ✓ 金融当局への報告、捜査当局との連携、その他市場関係者との連携・報告、銀行との連携を義務化

（出所）各種資料より大和総研作成

総じて、証券口座の乗っ取りに関連する規制で先行してきた米国と比較しても、高い水準のサイバーセキュリティ対策が求められる内容となった。特にフィッシング詐欺対策に重点を置き、具体的な技術的措置を列挙していることは、監督指針改正案およびガイドライン改正案の大きな特徴といえる。

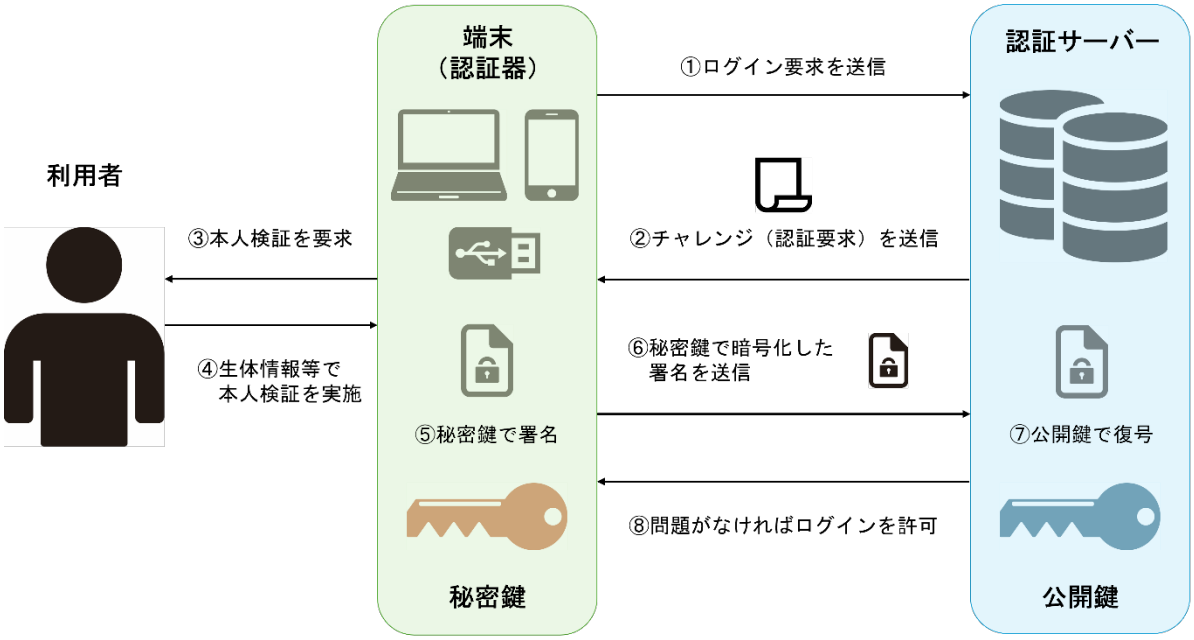
また、重要な操作時の認証については、単なる多要素認証ではなく「フィッシング耐性のある多要素認証」の実装および必須化が要求されている。これは、利用者が偽サイトに ID やパスワードを入力する様子をリアルタイムで監視し、正規のサイトから追加で求められるワンタイムパスワードまで盗み取るリアルタイム型フィッシングのような、従来の多要素認証を突破する攻撃手法の登場を念頭に置いた記述と推測される。今後の証券業界では、知識情報（前掲図表 2－①）・所持情報（前掲図表 2－②）・生体情報（前掲図表 2－③）という認証の要素を複数組み合わせるだけでなく、公開鍵暗号方式を用いた次のような多要素認証などを採用し、フィッシング詐欺対策に取り組むことが必要となる（次ページ図表 5）。

図表 5　フィッシング耐性のある多要素認証の例

PKI ベース認証	認証局（Certificate Authority）が発行する電子証明書を用いて、ユーザーや端末の身元を確認する認証
FIDO 認証	サーバーに保存された公開鍵と利用者端末に保存された秘密鍵を使用する認証。端末の秘密鍵は、利用者が端末上で生体情報等を用いてロック解除することで利用可能となる。パスワードに依存しない安全な認証を実現
パスキー認証	端末ごとに秘密鍵を保存する FIDO 認証を応用し、秘密鍵とそのメタデータに相当する「FIDO 認証資格情報」をクラウド経由で同期することで、複数の端末での利用を可能にした（利用者の利便性を向上させた）認証

（出所）大和総研作成

図表 6　FIDO 認証の仕組み



（出所）大和総研作成

なお、一部の報道等はフィッシング耐性のある多要素認証を「生体認証」と読み替えている。確かに、生体認証はフィッシング耐性のある多要素認証の代表的な構成要素である。しかし、すべての生体認証がフィッシング耐性のあるものと認められるわけではない。なぜならば、フィッシング耐性を有するには「接続先が正しいかどうか」（偽サイトでないこと）を判定する機能が必要であり、生体認証は「本人確認」には有効であるものの、接続先が正しいかどうかは保証しないからである。たとえば、利用者と正規サイトの間に偽サイト（中継サーバー）を設置し、正規サイトから発行される認証済のセッション Cookie を窃取する攻撃手法（AiTM）は、生体認証だけでは防げない。逆に、所持情報による認証であっても、メールや SMS（ワンタイムパスワード）ではなく、スマートカードや専用 USB デバイスなどの物理的なセキュリティ装置を用いるものであれば、上記の FIDO 認証等と組み合わせることでフィッシング耐性を有すると考えられる。

いずれにせよ、インターネット取引サービスを提供する証券会社は、多要素認証を突破する攻撃手法も踏まえた上で、高度な多要素認証を実装することが必要となろう。