業界団体との意見交換会において金融庁が提起した主な論点

[2025 年６月 17 日開催　（日本証券業協会）]

１．インターネット取引における不正アクセス・不正取引事案への対応について

○　証券口座のインターネット取引における不正アクセス・不正取引事案について、先日、金融庁ウェブサイトにおいて 2025 年５月末現在の被害発生状況を公表したところであるが、５月の不正売買の金額は、４月と比べ若干の減少はみられたものの、不正取引が発生した証券会社の数は地域証券会社を含めて 16 社まで拡大するなど、被害の収束には至っていない状況である。

○　現在、各証券会社においては、ログイン時の多要素認証の必須化に順次対応しているものと承知しているが、引き続き、セキュリティ対策は経営陣の責務と認識し、顧客被害の発生防止と被害拡大防止のために万全を尽くしていただきたい。

○　また、不正アクセスにより身に覚えのない取引の被害を受けた顧客に対しては、顧客の不安を解消するべく問合せや相談に真摯に対応し、被害回復に向けた誠実な対応をお願いしたい。

○　補償については、既に原状回復に向けて手続を開始した会社もあると認識しているが、各証券会社とも、今般の事案が自社の顧客、ひいては証券業界全体に与えた不安の大きさを十分認識していただき、安心して投資が行える環境の再構築に向けて、誠意ある対応をお願いしたい。

○　補償をする場合の手続においては、具体的な補償内容の通知や補償の完了までには一定の時間を要する場合もあると認識しているが、顧客が全く連絡を受けないまま不安な状態で過ごすことがないよう、顧客への連絡が滞ることがないようにしていただきたい。

○　現在、各証券会社のコールセンターには、補償など不正取引に関する相談のほか、多要素認証などの認証強化機能に関する問合せも多く寄せられているとの報告を受けており、各証券会社においては、相談体制の強化を図っているものと承知しているが、引き続き、顧客の疑問や不安に迅速に対応できるよう、顧客対応にも万全を尽くしていただきたい。

○　さらに、日本証券業協会の「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」については、現在抜本的な見直しに向けて議論を進めているところと承知しているが、協会と各証券会社が連携し、本事案のほか、昨今のサイバー犯罪の手口の高度化も踏まえ、実効的な内容となるよう、見直しを進めていただきたい。

２．2024 事務年度の証券等モニタリングの結果について

（大手証券会社）

＜顧客本位等＞

○　各証券会社ともに、顧客の最善の利益に資する商品組成・販売・管理等態勢を構築されているが、今後とも、経営陣のリーダーシップの下、適切なモニタリングや品質管理の徹底により、良質な金融商品・サービスを御提供いただきたい。

○　仕組貸出の取扱いに関し、金融庁との対話を通じて把握された課題について、適切に対処いただきたい。

○　また、社員不祥事の再発防止については、行動規範の周知徹底や各種予兆検知等の実施とそれを踏まえた実効性のある取組の継続など、適切な取組をお願いしたい。

＜グループ・グローバルでのガバナンス＞

○　大手証券会社では、グローバルでの事業拡大が進展しており、それに伴うガバナンスやリスク管理態勢の整備に進展が見られた。

○　一方、クロスボーダーでのビジネスが拡大する中で、拠点を跨ぐオペレーションやコンプライアンスの不備に起因する不芳事案も見られた。各証券会社においては、今後も事業拡大が見込まれる中で、コンプライアンスにも留意しつつ、引き続き、グループ・グローバルに一体性をもって、事業戦略に見合った実効性のあるガバナンスやリスク管理態勢の整備に努めていただきたい。

（地域証券会社）

○　今事務年度は、トップヒアリング等を通じ、主に持続可能なビジネスモデル構築の観点から、各証券会社が抱える経営課題や当該課題解決に向けた取

組みなどについて、深度ある対話を実施した。

○　その結果、人口減少・少子高齢化に伴う顧客基盤の維持拡大や人材確保の困難化、安定的な収益確保の観点から資産管理型ビジネスモデルへの転換の必要性、コスト削減の観点からミドル・バックオフィス業務の効率化などを重要課題として挙げる先が多く見られた。

○　このような課題認識の下、各証券会社においては、顧客本位の業務運営の浸透、人材の育成・確保、商品ラインナップの拡充、DX の推進などに取り組んでいる状況が見られたところであり、引き続き、深度ある対話を通じ、各証券会社の取組状況等について注視していきたい。

３．NISA 口座の利用状況調査について

○　2025 年５月８日、NISA 口座の利用状況調査（2025 年３月末時点）を公表した。NISA 口座数は約 2,647 万口座、総買付額は約 59.3 兆円となった。なお、政府目標値は、2027 年末時点の NISA 口座数が 3,400 万口座、総買付額が 56 兆円であり、総買付額の政府目標を約３年前倒しで達成したことになる。

○　このように NISA は、国民の資産形成の重要な手段として定着しつつあるが、実際に、それが、国民の安定的な資産形成にどの程度貢献しているのか、その政策効果について、今後、有識者の意見も踏まえつつ検証し、必要に応じて、利便性の向上等について追加的な改善を検討していくこととなる。

○　また、NISA における、長期、積立、分散の投資手法に関する顧客の理解の促進については、日頃の取引時や相場変動時における金融機関と顧客との間の丁寧なコミュニケーション、あるいは、これを実現するための顧客接点の体制整備が、今後、ますます重要となってくる。こうした点に留意して、顧客の状況把握や必要に応じた改善に引き続き、配慮していただきたい。

４．顧客口座・アカウントの不正アクセス等への対策の強化について

○　昨今の証券口座への不正アクセスについては、その手口として、主に、メールや SMS などによって顧客を誘導し、実在する組織のウェブサイトを装ったフィッシングサイト等から顧客情報（ログイン ID やパスワード等）を窃取するものや、その他、攻撃者が顧客端末をマルウェアに感染させ、リアルタイムで当該端末を監視するとともに操作し、顧客情報を窃取するもの等が想定される。

○　今般の事案は、証券業界に限らず、金融業界の信頼を揺るがしかねないものであり、早急にログイン認証の強化、ウェブサイト及びメールの偽装対策の強化、不審な取引等の検知の強化、取引上限の設定、手口や対策に関する金融機関間の情報共有の強化、顧客への注意喚起の強化などの対策を進める必要がある。

○　ID とパスワードだけの認証が脆弱であることのみならず、メールや SMS メッセージによるワンタイムパスワードだけでは昨今のフィッシングに対しては効果が不十分であるため、パスキー等を用いた強度のある多要素認証を必須化していく必要がある。不正の手口がますます巧妙化している状況を踏まえるとともに、対策を講じてもそれを上回る手法が出現することを前提に、攻撃手法と対策の技術動向を注視していく必要がある。

○　経営陣においては、セキュリティが担保されない場合は、サービスの提供を停止することも視野に、被害が発生してから対策を講ずるのではなく、あらかじめ対策を進めていただきたい。直近でも、外部から不正アクセスを受け、大量の顧客情報が漏えいしたおそれのある事案も発生している。セキュリティの不備により顧客情報を適切に管理できなければ、金融業界への信頼が損なわれる。顧客本位の経営の実現には、顧客資産、顧客情報を守ることが不可欠であり、経営陣自らの問題としてしっかり対応していただきたい。

５．パスワード付きファイルの電子メールによる送付について

○　パスワード付き ZIP ファイル（注）を電子メールに添付して送信する慣行が依然として金融業界に残っている。ZIP ファイルであっても、ZIP 化されていないものであっても、電子メールに添付するファイルにパスワードをかけると、電子メール受信者側でセキュリティスキャンをかけられなくなること等により、電子メール受信者側がセキュリティ上のリスクに晒されてしまい、実際にマルウェアの被害等が発生している。

○　したがって、パスワード付きファイルの送付は基本的には行うべきではなく、電子メールの通信経路自体を暗号化することが基本である。通信経路を暗号化できない場合は、安全性の高いオンラインストレージを活用してファイルの安全性を確保する等、ほかの手段を用いていただきたい。経営陣においては、サイバーセキュリティに関する基本的な対策の一部として徹底していただきたい。

（注）パスワード付きファイルについて

ファイルを相手方に送る際にパスワード付きファイルを作成し（自動的にそうなる場合も含む）、当該ファイルをメールで送付する方法は、受信者側において、メール受信時のウイルスチェックでファイル内のマルウェアを検知できず、メール受信者側がセキュリティ上のリスクに晒されてしまうため、望ましくない。実際に、過去には、このような特性が悪用されてマルウェア（Emotet）が流行した（参考：JPCERT/CC「マルウェア Emotet の感染再拡大に関する注意喚起」https://www.jpcert.or.jp/at/2022/at220006.html）。

また、パスワード付きファイルとパスワードが（別送であっても）同一通信経路で送信される場合は、盗聴リスクがある。

これらを踏まえ、用途に応じた代替選択肢とその代替選択肢に対するセキュリティ対策（メール通信経路暗号化等）の検討が必要である。

○　金融庁は、検査・モニタリング等を通じ、こうした慣行の払拭を促していく予定である。

６．耐量子計算機暗号（PQC）への移行対応について

○　実用的な量子コンピュータ（量子計算機）の実現は社会に恩恵をもたらす一方、攻撃者が量子コンピュータを悪用することで、インターネットバンキング等に用いられている暗号が解読され、金融機関が保有する顧客情報等の情報の機密性が損なわれるリスクがある。こうしたリスクが発現すれば、顧客情報及び財産が危険に晒され、ひいては金融システムに対する信頼が揺らぐおそれがある。

○　そのため、量子コンピュータの実現によってリスクに晒される重要なシステムやサービスは、耐量子計算機暗号（PQC：Post-Quantum Cryptography）を実装したものに移行する必要がある。

○　PQC への移行には、IT ベンダーとの連携を含め、準備段階から多くの時間と人材、投資が必要となる。現在、量子コンピュータが実用化するのは 2035 年が目途とされているが、大規模なシステム更改は、通常、数年に一度程度が予定されており、PQC への移行のタイミングは限られている。PQC への移行に要するリソースを考慮すると、まだ先の問題と捉えて準備への着手を先送りすることは不適切であり、直ちに取り組んでいただきたい。

○　具体的には、

・　金融機関は、検討の開始から移行までの一連の作業に関して、直ちに IT

ベンダーとも相談しながらロードマップを作成する必要がある。現在、金融 ISAC においてロードマップのひな型の検討が進められているが、ひな型の完成を待つ余裕はなく、自社でできることは直ちに着手する必要がある。

・　金融機関においては、PQC への移行対応の優先順位をつけるため、自らの情報資産を網羅的に把握し、それぞれの情報資産にどのような暗号が用いられているかをリスト化したインベントリを整備するとともに、そのリスク評価（量子コンピュータの実現によって危殆化するリスク、量子コンピュータの実現を待たずに HNDL 攻撃（注）に備え、現在から対策を講ずべきリスク等）と重要性・緊急性の評価に取り掛かるべきである。

（注）量子コンピュータの実用化前に、犯罪者において攻撃対象の暗号情報を収集し、実用化後に解読する攻撃（HNDL：Harvest Now Decrypt Later 攻撃と呼ばれる）。

○　金融庁は、金融 ISAC、業界団体と連携するとともに、検査・モニタリング等も活用しながら、各金融機関及び金融業界全体の PQC 移行に向けた対応状況を推進、フォローしていく。

・　（参考）金融庁「預金取扱金融機関の耐量子計算機暗号への対応に関する検討会報告書」（2024 年 11 月公表）https://www.fsa.go.jp/news/r6/singi/20241126.html

７．金融機関の内部監査高度化に関する懇談会の開催

○　金融庁は、金融機関の内部監査の高度化を促すため、2019 年以降、内部監査に関する各種レポートを公表してきた（※）。その後、国際的な動き（グローバル内部監査基準の公表・適用開始）もあり、金融機関の内部監査の在り方について、グローバル内部監査基準との整合性も視野に入れつつ、広く金融業界や有識者の御意見を踏まえて再整理することが適当と判断し、2025 年１月より「金融機関の内部監査高度化に関する懇談会」を開催した。

（※）2019 年６月：「金融機関の内部監査の高度化に向けた現状と課題」
2023 年 10 月：「『金融機関の内部監査の高度化』に向けたプログレポート（中間報告）」
2024 年９月：「金融機関の内部監査の高度化に向けたモニタリングレポート（2024）」

○　本懇談会では、内部監査の水準感や経営陣に求められる姿勢等について、計５回にわたって金融業界団体等と意見交換を行った。これらの御意見を踏まえた報告書を「金融機関の内部監査高度化に関する懇談会報告書（2025）」として公表する予定である（2025 年６月末目途）。今回公表する報告書では、金融業

界の今後の取組の指針となるよう、目指す方向性をより分かりやすく示すことを追求しており、金融機関にとどまらず、広く我が国一般事業会社、さらに海外金融監督当局にも参考となることを期待している。経営陣においては、本報告書も参考に、内部監査の一層の高度化に取り組んでいただきたい。

○　金融庁は今後も、金融機関の内部監査を取り巻く環境変化等を踏まえ、検査・モニタリングにおいて内部監査高度化への取組を促すとともに、モニタリング結果等の有用な情報をレポート等として公表していきたい。

８．リスク性金融商品の販売・組成会社による顧客本位の業務運営に関するモニタリング結果

○　2024 事務年度は、2023 事務年度に課題を指摘した外貨建一時払保険、仕組預金に関する改善状況のフォローアップに加えて、外国株式、ファンドラップ、仕組債、外貨建債券、投資信託といった幅広い金融商品を対象に、販売会社等のプロダクトガバナンス態勢及び販売・管理態勢等についてモニタリングを実施した。

○　当該モニタリング結果については「リスク性金融商品の販売・組成会社による顧客本位の業務運営に関するモニタリング結果」として公表予定である（2025 年６月末目途）。

○　販売会社等との対話や定性・定量アンケート調査の結果を踏まえ、金融商品の販売・管理態勢等に関し、販売会社等において確認された課題や工夫事例のほか、顧客本位に基づく金融商品販売に関する PDCA サイクルの基本的な考え方や重要な要素等について整理している。

○　経営陣においては、当該モニタリング結果等も参考に、顧客本位の業務運営の確保に向けて、リーダーシップを発揮して取り組んでいただきたい。

９．健全な企業文化の醸成及びコンダクト・リスク管理態勢に関する対話結果

○　2024 事務年度は、健全な企業文化の醸成及びコンダクト・リスク管理における取組をテーマに大手金融機関と対話を実施した。

○　当該対話で把握した取組事例については「健全な企業文化の醸成及びコンダクト・リスク管理態勢に関する対話結果レポート」として公表予定である（2025 年６月末目途）。

○　昨今、金融業界で複数の不祥事が発生・発覚する中、経営陣においては、組織体制やルールの強化のみならず、役職員の規範意識への働きかけも不祥事の発生防止に必要であることを再認識し、当該レポートも参考に、健全な企業文化の醸成やコンダクト・リスクの適切な管理に向けてリーダーシップを発揮して取り組んでいただきたい。

10. マネロン等対策に係る対応について

○　「マネロンガイドラインに基づく態勢整備」については、2024 年３月末を期限として態勢整備を要請し、期限までに、ほぼ全ての金融機関から対応が完了した旨の報告があった。

○　他方、一部の証券会社からは、いまだに対応が完了していない旨の報告を受けている。当該証券会社の経営陣においては、率先して態勢整備の完了に取り組んでいただきたい。

○　金融庁は、態勢整備が著しく不十分な証券会社に対しては、他の業態と同様に、必要に応じて行政対応を検討していく。

11. 金融庁 AI 官民フォーラム開催について

○　金融庁は、2025 年３月に「AI ディスカッションペーパー（第 1.0 版）」を公表し、金融機関等による健全な AI の利活用を後押しする方針を明らかにした。リスクベース・アプローチの下でリスクを適切にコントロールしつつ、経営陣の適切な理解と主体的な関与の下で顧客利便性や業務効率化の向上に繋がる取組が進展していくことを期待している。そのような取組を着実に進めていただくため、金融庁は AI に関する取組事例の共有や、規制の適用関係の明確化等を通じて、金融機関が AI を活用したチャレンジに安心して取り組むことができる環境整備に努めていく。

○　その一環として「金融庁 AI 官民フォーラム」を立ち上げ、2025 年６月 18 日に第１回会合を開催する。本フォーラムでは、取組事例の共有や実務上の課題の深掘りなど、金融機関や AI モデル開発者、ベンダー、アカデミア、関係省庁等の官民の様々な関係者をお招きして、多面的な議論を行う予定である。日本証券業協会にも参加いただいているが、今後のプロセスへの積極的な関与をお願いしたい。

・　ウェブサイト：https://www.fsa.go.jp/news/r6/singi/20250603.html

12. ５月 G7 財務大臣・中央銀行総裁会議

○　2025 年５月 20 日から 22 日にかけて、カナダ・バンフにおいて G7 財務大臣・中央銀行総裁会議が開催された。会合後に発出された共同声明における金融関連の主な内容を御紹介したい。

・　まず、金融の安定及び規制上の課題に継続的に焦点を当てることが、金融システムの実効的な機能の確保のために引き続き不可欠であることが再確認された。

・　ノンバンク金融仲介（NBFI）に関しては、実体経済への資金供給において一層重要な役割を果たしていることに鑑み、ノンバンクのデータの入手可能性、利用及び質を評価し、潜在的なリスクを監視・評価するための知見とアプローチを共有する必要性について合意された。

・　AI に関しては、AI の導入が一層進む中で、金融セクターにとっての AI の便益と、金融安定に対する潜在的なリスクをモニターし、評価する必要性が示された。

・　サイバーリスクに関しては、重大なサイバーインシデント発生時の対応能力及び手順の更なる強化に引き続き取り組む旨が示された。

・　最後に、共同声明とともに採択された「金融犯罪に対する行動要請」における金融関連の主な内容は以下のとおり。

- 経済発展と金融包摂の促進に向け、リスクに応じたマネロン等対策の効果的な実施を支援することへのコミットメントが確認された。
- 北朝鮮等による暗号資産窃取が前例のない水準に達しているという深刻な懸念が表明され、サイバーセキュリティやマネロン等対策の観点から、暗号資産に関する新たなリスクについて調査・情報交換を推進し、必要な措置を講ずることが合意された。
- 暗号資産に関する金融活動作業部会（FATF）基準のグローバルな実施の加速や、ステーブルコイン、P2P 取引及び DeFi の悪用等から生じる新たなリスクに関する FATF の作業が引き続き支持された。
- クロスボーダー送金の透明性向上に関する FATF 基準を強化する進行中の作業や、クロスボーダー送金の改善に向けた G20 ロードマップが支持された。

○　今後は、2025 年６月 15 日から 17 日にカナダ・カナナスキスにて G7 首脳会議が開催される予定である。引き続き、各金融機関の意見もよく伺いつつ、国際的な議論に貢献してまいりたい。

13. CDSC による Common Carbon Credit Data Model の検討について

○　CDSC（Climate Data Steering Committee）は、ネットゼロの達成のために不可欠なプライベートセクターの質の高い気候関連データを幅広く入手できる基盤の構築を支援するために、2022 年７月に設立されたものである。

○　G20SFWG では、三つのプライオリティを設定して議論を行っている。本年の議長国である南アフリカ共和国が設定したプライオリティのうち、「カーボンクレジット市場での資金調達ポテンシャルの引き上げ」に関し、御説明したい。

○　南アフリカ共和国は、カーボンクレジットに関するデータの統一基準がなく、市場間でのカーボンクレジットの比較等がしにくい課題に焦点を当て、基準作成の上で参照可能な最低限の主要なデータ属性を整理する「Common Carbon Credit Data Model」をボランタリーなガイダンスと共に作成することとしている。

○　具体的な作業は、冒頭で御紹介した CDSC が進めており、臨時で設置されたワーキング・グループにおいて、データモデルとテクニカルノートを作成し、公表する予定となっている。

○　金融庁は CDSC のメンバーであり、今般設置されたワーキング・グループにも参加し、経済産業省や環境省等と連携しつつ議論を行っている。

○　データモデルは、カーボンクレジット市場におけるデータの標準化と透明性向上のサポートのため、政策立案者や市場参加者が自主的に採用可能なベースラインを提示するものである。概要は資料を御覧いただきたい。

○　2025 年７月から８月にかけてパブリック・コンサルテーションが実施される予定であり、各金融機関にも御覧いただき、必要に応じてコメントを出していただきたい。

14. IOSCO 年次総会の開催について

○　2025 年５月 12 日から 14 日にかけて、証券監督者国際機構（IOSCO）の年

次総会がカタール・ドーハで開催された。代表理事会では、オンライン被害対策、プリヘッジ、フィンテックなどについて議論が行われた。特に、2025年５月 21 日に公表された「オンラインハーム対応とプラットフォーム事業者の役割に関するステートメント」について触れたい。

○　同ステートメントでは、プラットフォーム提供者に対し、①無登録の投資勧誘の排除に向けたデュー・デリジェンスの実施、②投資詐欺的コンテンツや広告の監視及び迅速な削除の実施、③詐欺性が疑われる活動に係るやりとりを含む、当局との積極的なコミュニケーション・チャネルの構築などの対応を検討している。

○　偽広告等への対応については、日本証券業協会及び各証券会社においても、横断的に、偽広告等に関する情報収集や注意喚起を行うとともに、自らになりすました偽広告等を発見した場合には積極的な削除要請を行うよう、2024年９月にお願いしているが、引き続きそうした投資家保護に努めていただきたい。

15. アジア・デーの開催について

○　Japan Weeks 中の 2025 年 10 月 22 日において、アジア開発銀行（ADB）及び日本証券業協会等と共催でアジア地域の資金循環活性化を目指すイベント「アジア・デー」を実施する予定である。

○　当日は、ADB 総裁がキーノートスピーカーとして登壇するほか、アジア当局のハイレベルやアジアの金融資本市場の関係者を広く招く予定である。近日中に金融庁ウェブサイトにて御案内予定なので、是非御関心・御参加いただきたい。

（以　上）