新形態銀行との金融犯罪対策等に係る意見交換会　連絡事項
（６月６日）

１．　口座不正利用要請文のアンケートについて

○　特殊詐欺をはじめとする金融犯罪については、各金融機関において対応を強化いただいているものの、犯罪の手口もより巧妙化・多様化している。

○　こうした状況を踏まえ、2024 年８月、法人口座を含む預貯金口座の不正利用等対策の強化について、要請文を発出した。

○　金融庁では、本要請を受けた各金融機関の対応状況のフォローアップとして、2025 年１月 24 日、各金融機関に対し、要請への対応状況に関するアンケートを発出し、2025 年２月末に回収を行った。

○　アンケート結果については、金融機関向けの詳細な説明会を行ったところ、各金融機関の対応状況の集計・分析について、別途公表する予定である。

○　アンケート項目の中で、未着手と答えた金融機関の割合が多い項目も見受けられた。未着手と回答した項目が著しく多い等、自主的な取組状況が把握できない金融機関については、個別にヒアリングすることも検討している。

○　今回のフォローアップは、今後も継続して行う予定である。金融機関におかれては、経営陣主導のもと、計画的に対策を実施し、不正利用対策の更なる強化・底上げを図っていただきたい。

２．　「国民を詐欺から守るための総合対策 2.0」について

○　2025 年４月、「国民を詐欺から守るための総合対策 2.0」が策定された。新たな項目として、預金取扱金融機関間における不正利用口座に係る情報共有や、架空名義口座を利用した新たな捜査手法や関係法令の改正、インターネットバンキングに係る対策強化が盛り込まれている。

○　2024 年の詐欺被害額が 2023 年の２倍近くに増加しており、その対策が急務となっている。このような状況も踏まえ、今後、利用限度額引上げ時の確認をはじめとするインターネットバンキングに係る対策強化など、対応をお願いする予定である。

○　くわえて、全国銀行協会にて進められている不正利用口座情報を共有する

枠組みの構築についても、官民一体で進めてまいりたい。

３．　オンラインカジノに係る賭博事犯防止等について

○　オンラインカジノについては、海外で合法的に運営されている場合でも、日本国内から接続して賭博を行うことは犯罪であるところ、警察庁の委託調査によると、オンラインカジノで利用されている入金方法として、「クレジットカード」(55.4%)のほか、「電子決済サービス・決済代行業者」(29.8%)や「銀行振込（銀行送金)」(27.4%）も利用されている。また、同調査によると、４割強の人がオンラインカジノの違法性を認識していなかったとされている。

○　こうした状況を踏まえ、2025 年 5 月 14 日、預金取扱金融機関・資金移動業者・前払式支払手段発行者・暗号資産交換業者に対し、以下の内容について要請を発出した。

- 日本国内でオンラインカジノに接続して賭博を行うことは犯罪であることについて利用者へ注意喚起すること
- オンラインカジノにおける賭博等の犯罪行為を含む法令違反行為や公序良俗に反する行為のための決済等のサービス利用を禁止している旨を利用規約等で明らかにすること
- 利用者が国内外のオンラインカジノで決済を行おうとしていることを把握した場合に当該決済を停止すること

○　各金融機関においては、上記要請も踏まえ、オンラインカジノに係る賭博事犯の発生防止に適切に取り組んでいただくようお願いしたい。

４．　マネロン等対策の「有効性検証」に関する対話について

○　マネー・ローンダリング（マネロン）等対策については、各金融機関において 2024 年３月末の期限までに整備した基礎的な態勢の有効性を高めていくことが重要であり、マネー・ローンダリング及びテロ資金供与対策に関するガイドライン（マネロンガイドライン）では、各金融機関が自社のマネロン等対策の有効性を検証し、不断に見直し・改善を行うよう求めている。

○　また、今後の金融活動作業部会（FATF）の第５次審査も見据えると、各金融機関が自らのマネロン等対策の有効性を合理的・客観的に説明できるよう

になることも重要である。

○　金融庁では、「有効性検証」に関する金融機関等の取組を促進するために、「有効性検証」を行うにあたって参考となる考え方や、実際の取組事例集を2025年３月に公表した。

○　今後は順次、「有効性検証」に係る対話を各金融機関と行う予定であり、当局の具体的な対話手法や着眼点も公表文書に明記している。金融機関においては、これらの文書も参考に、経営陣主導のもと、「有効性検証」の取組を進めていただきたい。

５．　顧客口座・アカウントの不正アクセス・不正取引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などから顧客情報（ログインIDやパスワード等）を窃取し、口座に不正にアクセスするものや、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などが想定される。

○　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あまり効果がなく、パスキーなどの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。

○　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、予め対策を進めていただきたい。顧客本位の経営の実現には、顧客資産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。

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

（以　上）