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 11 日開催　日本暗号資産等取引業協会]

１．国内外の情勢の動向を踏まえた対応について

○　暗号資産業界と金融庁幹部が意思疎通を図ることが重要との認識から、日本暗号資産等取引業協会理事会メンバー及び事務局の方々と継続的に意見交換会を開催している。今事務年度は昨年 11 月に引き続き二度目の開催である今回は、事務年度末の総括として率直に意見交換したい。

○　暗号資産業界においては、日頃から、内部管理態勢・システムリスク管理態勢の強化やマネロン対策・金融犯罪対策の高度化等に取り組んでいるものと承知している。しかしながら、昨年５月には大規模な暗号資産不正流出事案が発生したほか、詐欺やオンラインカジノに関する送金に暗号資産が使用されているという実態がある。暗号資産業界が安定的かつ継続的に発展するためには、これらの問題に業界全体で適切に対処することで、国民の信頼を広く得ることが必要不可欠である。

○　昨年５月に発生した暗号資産不正流出事案は、北朝鮮を背景とするサイバー攻撃グループ「TraderTraitor」（トレイダートレイター）」による窃取であったことが警察庁から公表された。これを受けて、金融庁は警察庁や内閣サイバーセキュリティセンター（NISC）と連名で、暗号資産業界に対して適切なセキュリティ対策を講ずるよう注意喚起するとともに、日本暗号資産等取引業協会を通じて会員に改めて自主点検を行うよう要請した。

○　日本暗号資産等取引業協会においては、当該自主点検の結果も踏まえて、同様の事案の再発防止に向け、自主規制規則の改正等の取組を検討しているものと承知している。今回の事案を教訓として、会員に対する指導も含めて、業界全体の底上げを図っていただきたい。

○　また金融庁は、５月１４日付で、「国民を詐欺から守るための総合対策 2.0」を踏まえた詐欺被害防止に向けた取引モニタリングの強化等とともに、利用者が国内外のオンラインカジノに関連した取引を行おうとしていることを把握した場合に当該取引を停止することを、日本暗号資産等取引業協会を通じて会員に要請した。

○　日本暗号資産等取引業協会においては、不正流出事案対応と同様、暗号資産が詐欺やオンラインカジノ等の犯罪に使用されることを防止するため、会員に対する指導も含めて、業界全体の底上げを図っていただきたい。

○　本年３月には、いわゆる「ステーブルコイン」の仲介業者である電子決済手段等取引業者を初めて登録した。これまでもお伝えしているとおり、電子決済手段等取引業者の適切な業務運営を確保するためには日本暗号資産等取引業協会の役割は極めて重要である。日本暗号資産等取引業協会においては、自主規制機関としての業務を着実に遂行していただきたい。

○　また、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。

○　本懇談会では、金融業界における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回にわたって意見交換を行った。日本暗号資産等取引業協会にも御参加いただき、暗号資産等取引業者の実状等について御説明いただいた。懇談会での議論を踏まえ、金融庁は、2025 年６月末を目途に報告書を公表する予定としている。日本暗号資産等取引業協会においては、本報告書を参考に、業界全体の内部監査の底上げを図っていただきたい。

○　また金融庁は、引き続き Web3.0 の健全な発展に向けて、利用者保護に配慮しつつ、健全なイノベーションの推進に貢献していく所存である。暗号資産業界においては、国民の利便性向上につながるサービスの提供に向けて、リスク管理や利用者保護のための措置を適正に行った上で、新たな取組にもチャレンジしていただきたい。

○　今事務年度においては、昨今の暗号資産に係る取引の実態等を踏まえた暗号資産に関連する制度のあり方等について検証し、その検証の結果について本年４月にディスカッション・ペーパーを公表して広く意見募集を行った。金融庁では、その結果を踏まえて規制・監督等の見直し等を実施していくことから、日本暗号資産等取引業協会においても自主規制規則等の見直しが必要になると予想される。今後の見直しに向け、日本暗号資産等取引業協会と金融庁幹部は一層連携を強化して取り組んでいく必要がある。日本暗号資産

等取引業協会においても課題に感じていることなどがあれば、忌憚なく金融庁に御相談いただきたい。

２．暗号資産交換業等を取り巻く当面の課題等について

（１）暗号資産交換業等を取り巻く当面の課題等について

○　昨年５月に発生した暗号資産不正流出事案について、昨年 12 月、金融庁は警察庁や内閣サイバーセキュリティセンター（NISC）と連名で、適切なセキュリティ対策を講じていただくことを目的とした注意喚起を公表するとともに、日本暗号資産等取引業協会を通じて、会員各社に対して改めて自主点検を行うことを要請した。

○　日本暗号資産等取引業協会からの御報告によれば、自主点検の結果、会員各社ではおおむね適切に対応していることが確認できたものの、一部の事業者より、自主規制規則や安全管理標準に対して対応できていない項目があるとの回答があったとのことであり、日本暗号資産等取引業協会においては、当該結果も踏まえて、自主規制規則の改正等の取組を検討しているものと承知している。

○　自主規制規則の改正等については、準備ができた部分から複数回に分けて段階的に取り組んでいくとの御説明をいただいており、今回の事案を教訓として、暗号資産の流出リスクへの対応を万全の態勢とするべく、日本暗号資産等取引業協会から会員各社に対する指導も含めて、適切かつ確実な対応をお願いしたい。

○　また、暗号資産交換業者においても、証券会社の事案と同様に、不正アクセスされた口座内で不正取引された事案が発生している。（直近では同様の事案が拡大しているような状況は見られていないものの、）不正アクセスを防止して利用者の財産を守るために、各会員のウェブサイトへのログイン時における多要素認証の必須化等のセキュリティ対策強化に向けて取り組んでいただきたい。

○　くわえて、各暗号資産交換業者においては、多要素認証のみならず、利用者のログイン活動等のリアルタイムモニタリングを行い、ログインが連続して失敗した場合のロック、不審な IP アドレスからのログイン試行の利用者への通知等も併せて考えるなど、攻撃手法の変化に併せてこうした対策を常

時見直していただきたい。

○　さらに、フィッシングを防ぐには、各暗号資産交換業者において、自ら電子メールにリンク先を貼付しないよう徹底するほか、利用者に対して電子メールに貼付されたリンク先には絶対にアクセスしないよう広報活動を強化する必要がある。あわせて、強固なパスワードを使用することやパスワードの使い回しをやめることを伝達すること等により、セキュリティ強化について利用者への広報活動を強化していただきたい。

○　本年４月に政府が策定した「国民を詐欺から守るための総合対策 2.0」においては、暗号資産関連の新たな項目として、暗号資産交換業者による送金のモニタリングの強化や、預金取扱金融機関と暗号資産交換業者における情報連携・被害拡大防止に係る取組の推進が盛り込まれている。

○　これを踏まえ、５月１４日付で日本暗号資産等取引業協会を通じて各会員に対して要請文を発出し、詐欺被害防止に向けて、

・　暗号資産を利用した詐欺事案を速やかに発見するためのモニタリングや当該事案発見時の迅速な取引停止を行うこと、

・　暗号資産を送金した後も、当該送金に係る取引の流れを適切にモニタリングすること

などの取引モニタリングの強化等の態勢整備に関する充実・強化の取組の実施を要請している。

○　また、当該要請文においては、オンラインカジノに係る賭博事犯防止についても、

・　オンラインカジノは違法であることの利用者向け注意喚起

・　オンラインカジノ等を含む法令違反・公序良俗に反する利用禁止の規約等への明示

・　オンラインカジノ利用の取引を把握した場合の取引停止

を要請している。

○　詐欺やオンラインカジノ等の犯罪において暗号資産が送金手段に使用されることの防止に向け、各会員における要請内容への対応状況の確認等につ

いて、日本暗号資産等取引業協会と連携して取り組んで参りたいので、御協力をお願いしたい。

○　昨今、暗号資産交換業者におけるシステム更改や IEO において利用者に影響を及ぼすシステム障害が多発している。障害発生のリスクを低減させるために、各会員においては、まずは経営陣がしっかりとリスクを認識した上で適切に御対応いただくとともに、金融庁においてもシステム更改計画がビジネス優先でリスクの高いものとなっていないか等を確認する必要があるため、システム更改計画のなるべく早い段階から、前広に金融庁に御相談いただきたい。

（２）金融庁 AI 官民フォーラム開催について

○　本年３月に「AI ディスカッションペーパー（第 1.0 版）」を公表し、金融庁は、金融機関等による健全な AI の利活用を後押ししていく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、経営陣の皆様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が、そのような取組を着実に進めていただくために、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、金融機関等の皆様が 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たい。

○　そこで、「金融庁 AI 官民フォーラム」を立ち上げ、６月 18 日（水）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。

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

（３）Japan Fintech Week 2025 開催報告について

○　金融庁は、フィンテックの更なる発展に向けたビジネス機会を創出するため、３月３日～７日をコアウィークとして「Japan Fintech Week 2025」を開催した。

○　地方公共団体や業界団体、大使館等と連携し、80 を超えるフィンテック関連イベントが集中的に開催されたことで、地方や海外からを含め多くの方が Japan Fintech Week に参加し、多面的な議論とネットワーキングが行われ

た。

○　FIN/SUM をはじめとして、多くのイベントへの御参加等の御支援をいただき、２回目の開催となった「Japan Fintech Week」も充実したものとすることができた。

○　来年も、２月 24 日（火）～３月６日（金）に「Japan Fintech Week 2026」を開催予定である。

○　各暗号資産交換業者のビジネス機会の更なる拡大や課題解決に資するようなイベントに育てていければと思っており、引き続き連携を強化していきたい。

３．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関する要請等について

（１）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関する要請について

○　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、そのほか、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、パスキーなど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。

○　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。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。

（２）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。

・　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、業界団体等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

（３）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で、ほかに手段がない場合は、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。

（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。

○　こうした問題は、金融機関の規模の大小を問わず依然として見受けられるが、グローバルに見てこうした慣行が続けられていることは異例であり、我が国の金融業界のセキュリティ水準に疑義を生じさせているといった声が

金融庁に寄せられている。

○　金融庁としては、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。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する必要がある。

４．マネロン等対策の「有効性検証」の考え方・対話の進め方に関する文書の公表等について

（１）マネロン等対策の「有効性検証」の考え方・対話の進め方に関する文書の公表について

○　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」を行うに当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っていく予定であり、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。経営陣においては、これらの文書も参考に、「有効性検証」の取組を進めていただきたい。

（２）「疑わしい取引の参考事例」の改訂について

○　金融庁が策定・公表している「疑わしい取引の参考事例」は、所管の特定事業者が疑わしい取引の届出義務を履行するにあたり、犯罪等に関連する可能性のある取引として特に注意を払うべき事例を例示したものである。

○　金融機関等におけるリスク動向や、昨今の金融犯罪の傾向等を踏まえ、非対面取引における具体的な観点の追記を中心に参考事例の改訂を行う。参考

事例の見直しに当たり、警察庁策定の「疑わしい取引の届出における入力要領」も改訂され、併せて 2025 年７月頃に公表予定である。

○　経営陣においては、改訂された事例を参考とし、疑わしい取引の届出業務を着実に実施するともに、足元で特殊詐欺等の被害が拡大している状況も踏まえ、犯罪等に関連する疑いのある取引に気づくことのできる、あるいはシステム等で検知できる態勢を構築し、金融犯罪等の抑止に繋げていただきたい。

（３）「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。暗号資産関連の新たな項目として、暗号資産交換業者による送金のモニタリングの強化や、預金取扱金融機関と暗号資産交換業者における情報連携・被害拡大防止に係る取組の推進が盛り込まれている。

○　2024 年の詐欺被害額は 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、官民一体で対応を進めてまいりたい。

（４）犯罪収益移転防止法施行規則の改正案の公表について（非対面の本人確認方法の見直し）

○　近年、非対面での本人確認において、偽変造された本人確認書類が悪用されている実態があり、治安上の大きな課題となっている。

○　このような情勢を背景に、2024 年６月 21 日に閣議決定された「デジタル社会の実現に向けた重点計画」等において、「非対面の本人確認手法は、マイナンバーカードの公的個人認証に原則として一本化し、運転免許証等を送信する方法や、顔写真のない本人確認書類等は廃止する」との記載が盛り込まれた。

○　これを受け、非対面での本人確認方法のうち、本人確認書類の偽変造によるなりすまし等のリスクの高い方法を廃止するため、警察庁において、犯罪収益移転防止法施行規則の改正案に係るパブリックコメントを実施した（2025 年２月 28 日～同年３月 29 日）。

○　口座開設時の確認等の実務に影響する改正であり、システム対応が必要となる金融機関もあると思われるところ、内容について御確認いただきたい。なお、対面での本人確認方法についても、今後警察庁において対策が検討さ

れていく予定である。

５．金融行政モニター制度について

○　金融行政モニター制度は、金融機関及びその職員などからの金融行政に対する率直な御意見等を中立的な第三者である外部専門家に直接お届けし、金融行政に反映させる仕組みとして運用しており、本年で 10 年目を迎える。

○　昨年（１月～12 月）は 42 件の御意見を受け付けており、

・　保険募集人に対する規制の強化

・　事業ファクタリングに関する規制法令の制定

などに関する御意見について、金融庁の対応の公表を行った。

○　金融庁としては、受け付けた御意見について、金融行政の改善に繋げる観点から前向きに対応していきたいので、本金融行政モニター制度を日本暗号資産等取引業協会傘下金融機関及びその職員に周知いただき、金融制度や金融庁に対する率直な御意見をお寄せいただきたい。

（以　上）