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
［令和6年 11 月 28 日開催　資金移動業者］

１．金融行政方針について

○　８月末に、本事務年度の金融行政方針を公表した。今年の大きな柱の１つとして、デジタル技術を用いた金融サービスの変革への対応など、金融メカニズムを通じた持続的な成長を目指し、引き続き、金融面での環境整備を行う方針である。

○　特に、金融サービスのデジタル化の推進を通じて、金融サービスが、利用者保護やシステムの安全性を確保しつつ、特色ある機能を発揮することで、個人や企業の利便性向上に繋がるよう、金融機関やフィンテック事業者の支援を強化していく方針である。

○　資金移動業の実績を見ると、年間送金件数、年間取扱金額とも前年比も大きく伸長しているほか、賃金のデジタル払いをはじめとしてキャッシュレス決済が浸透するための制度整備も進んでいる。更に一段とキャッシュレス決済が浸透するためには、利用者に加えて受取側の事業者等の利便性も重要であると考えており、この点の利便性向上に向けた取組みについても期待している。

○　当局としても、引き続き、環境変化のスピードが速い資金移動業者のニーズを的確に把握し、取り組むべき課題の特定とその解決を図れるよう、深度ある対話を中心にモニタリングを継続してまいりたい。

○　最後に、今年、昨年と、大規模事業者において、システム等の利用困難・処理の滞留・遅延の発生が見られており、この背景には、ソフトウェア障害、運用面での操作ミスや管理ミス等が見受けられる。

○　資金移動業者が提供する決済・送金機能は、利用者からの安定したサービス提供・システム稼働への期待が特に高い領域であると思料。金融サービスの安定的な提供及び利用者保護の観点から、経営陣主導の下で、自社のシステムの開発・更新において円滑な移行ができるプロセスとなっているか、万が一障害が発生した時の対応について今一度確認いただきたい。

２．マネロン・テロ資金供与・拡散金融対策の強化について

○　マネロン等対策については、2024年３月末を期限として、ガイドラインに基づく態勢整備をお願いしてきたところ、皆様のご尽力に改めて感謝申し上げる。

○　経営陣においては、まずは整備した態勢が着実かつ継続的に運用されているか、形式的な運用になっていないか、自らが関与する形で確認いただきたい。また、今後は、整備した基礎的な態勢の実効性を高めていくことが重要であり、マネロンガイドラインでは、各金融機関等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。

○　金融庁では、各金融機関等がこうした有効性検証を行う際に参考となるよう、既に有効性検証に取組んでいる金融機関等との対話を通じて得られた考え方や事例を公表すべく検討・準備しているところ。

○　こうした事例等も参考にしつつ、金融庁の公表物を待つことなく対応を進め、マネロン等リスク管理態勢の高度化に努めていただきたい。

３．「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」の成果物の公表について

○　量子コンピュータが実現されると、現在広く利用されている公開鍵暗号の安全性が損なわれる（危殆化する）ことが指摘されており、耐量子計算機暗号（Post-Quantum Cryptography、PQC）への移行に向けた検討が国内外で始まっている。

○　こうした中、金融庁において、PQC への移行を検討する際の推奨事項、課題及び留意事項について関係者と検討を深めるため、「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」※（以下「本検討会」）を本年 7 月から 10 月にかけて全 3 回開催した。

※　本検討会には、3 メガバンクや預金取扱金融機関に係る業界団体の代表者や暗号に関する有識者等がメンバーとして参加し、オブザーバーとして金融 ISAC、CRYPTREC 事務局、FISC、日銀金融機構局、NISC が参加。

○　耐量子計算機暗号（PQC）への移行対応は、既存の暗号の危殆化によって脅威に晒され得る情報資産を洗い出し、重要性に応じて優先順位を付け、システム投資を行う必要があるなど、長期にわたり多大なリソースを要するため、経営陣のリーダーシップのもと、全社的な対応が必要である。本検討会は、預金取扱金融機関を想定したものだが、経営陣がリスクを正しく認識し、リスク低減策を適切に推進できるようにする観点から、本検討会の議論は預取以外の業態にも参考になるはずである。本検討会の議論を踏まえた成果物（報告書）を 11 月 26 日に公表したので、ぜひ一読いただきたい。

（金融庁ウェブサイト）https://www.fsa.go.jp/singi/pqc/index.html

４．サイバーセキュリティに関するガイドラインについて

○　サイバーリスクは、技術の発展や地政学リスクの高まりなどとともに増加しており、トップリスクの一つとして、金融機関において適切に管理していく必要がある。昨今の脅威動向、これまでのモニタリングの実績、国内外の情勢等を踏まえ、先般、サイバーセキュリティに関する新たなガイドライン案について、パブリックコメントに付したところであり、ご意見をいただき感謝申し上げる。

○　いただいたご意見への当庁の考え方及び同ガイドラインを最終化したものを 2024 年 10 月４日に公表している。

（注）ガイドラインは同日に適用開始。

https://www.fsa.go.jp/news/r6/sonota/20241004/20241004.html

○　金融機関等の規模・特性は様々である。このため、ガイドラインにも記載しているとおり、「基本的な対応事項」及び「対応が望ましい事項」のいずれについても、一律の対応を求めるものではなく、金融機関等が、自らを取り巻く事業環境、経営戦略及びリスクの許容度等を踏まえた上で、サイバーセキュリティリスクを特定、評価し、リスクに見合った低減措置を講ずること（いわゆる「リスクベース・アプローチ」を採ること）が必要であると考えている。

○　また、金融機関におけるサイバーセキュリティ管理態勢上の課題への対応には、時間がかかるものもあると考えている。したがって、重要性・緊急性に応じて、優先順位をつけた上で、順次対応していただければと考えている。

○　当庁としては、金融システム上の重要性・リスクなどを勘案の上、同ガイドラインの運用などを通じて、金融機関におけるサイバーセキュリティ管理態勢の強化を促してまいりたい。

５．金融業界横断的なサイバーセキュリティ演習（Delta Wall Ⅸ）について

○　金融業界全体のインシデント能力向上のため、2024 年も 10 月にサイバーセキュリティ演習（Delta Wall Ⅸ）を実施。

○　参加金融機関におかれては、IT/サイバーセキュリティ担当部署だけではなく、経営層にも積極的に関与いただいたうえ、演習に参加したことで満足せず、演習結果を活かしていただきたい。具体的には、経営者が適切な意思決定を行えたか、組織として顧客対応、業務復旧などのコンティンジェンシープランが有効であったかなどを振り返り、できなかったことを可視化し、改善するにはどうすればよいか、体制、業務プロセス、

予算、人材を含めて考えていただきたい。

６．外部委託先管理の強化について

○　昨今、外部委託先に対するサイバー攻撃により、金融機関の顧客情報が漏えいする事案が発生している。

○　委託先におけるインシデントであっても、金融機関が顧客情報管理の責任から逃れられるわけではない。

○　重要な委託先におけるインシデントの原因の検証及び再発防止策の実効性の確保、これらが確保できない際の代替策の検討を含め、委託先管理の有効性・十分性を確認し、必要に応じて改善していただきたい。

７．ＦＡＴＦ勧告 16（クロスボーダー送金）改訂案の検討進捗について

○　金融活動作業部会（FATF）は、新たな決済手段・技術・プレイヤーの登場等による決済市場構造の変化、及び、決済規格の標準化を念頭に、必要なAML/CFTの遵守及びFATF基準の技術的中立性を確保しつつ、クロスボーダー送金を、より迅速で、より安価で、透明性の高い、包摂的なものとするため、現在、勧告16の改訂作業を進めている。

○　本年２月末～５月初旬にかけて実施された市中協議に際して、業界の皆様から貴重なご意見を頂戴し、感謝申し上げる。

○　本年６月26日～28日に開催されたFATFプレナリーにおいて、本市中協議の結果も踏まえ、勧告改訂の内容の複雑性及び決済システムへの影響に鑑み、最終化の前に官民の関係者との更なる対話が必要であり、もう少し時間をかけて検討していく旨、合意した。

○　金融庁としては、引き続き、皆様方のご意見もよく伺いつつ、最終化に向けた議論に貢献して参る。

８．10 月 G20 及び G7 財務大臣・中央銀行総裁会議の成果物について

○ 10 月 23 日から 24 日にかけて、ワシントン D.C.において G20 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ご紹介したい。

・ まず、国際金融規制改革の適時の実施に強くコミットする旨が再確認された。特に、バーゼル III 枠組みの全ての要素を完全かつ整合的な形で、

かつ可能な限り早期に実施するとの、本年５月の中央銀行総裁及び銀行監督当局長官（GHOS）による合意が、再確認された。

・ ノンバンク金融仲介（NBFI）に関しては、その脆弱性に対処し、強靭性を向上させるための、FSB 等の作業が支持された。NBFI におけるレバレッジによる脆弱性に対処するための勧告への期待が示されるとともに、オープンエンド型ファンドの流動性ミスマッチに係る FSB の政策勧告及びマネー・ マーケット・ファンドの強靭性に係る政策勧告の実施が支持された。

・ クロスボーダー送金に関しては、グローバルな目標を達成するための「ロードマップ」の適時かつ実効的な実施へのコミットメントが再確認された。

・ 暗号資産に関しては、「暗号資産政策実施に関する G20 ロードマップ」に関する最初の状況報告書が歓迎された。また、金融活動作業部会（FATF）基準のグローバルな実施の加速、及び、DeFi、ステーブルコインや P2P 取引などから生じる新たなリスクに関する作業への支持が再確認された。

・ 最後に、サステナブル・ファイナンスに関しては、2021 年に策定された「G20 サステナブル・ファイナンス・ロードマップ」に基づいた、2024 年の「G20 サステブルファイナンス報告書」が支持された。また、採用は任意であるが、金融機関及び企業向けの「信頼性があり、強固で公正な移行計画に関するハイレベル原則」が歓迎された。

○ また、10 月 25 日に 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では、金融関連の主な内容として、上記の論点に加え、

・ サイバーセキュリティに関して、サイバー脅威への対応能力を強化し、将来に備えるための G7 サイバー専門家グループの作業が歓迎された。この点において、2024 年４月に実施したクロスボーダー協調演習が成功裏に完了したことが言及された。

○ 本年 12 月から南アフリカが G20 議長国を、来年 1 月からカナダが G7 議長国を務める予定。引き続き、皆さん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。

９．2024 事務年度における資金移動業者に対するモニタリングについて

（2023 事務年度のモニタリングを通じて把握した主な課題について）

○ まず、各事業者におかれては日々監督行政へのご協力をいただき感謝を申

し上げたい。信頼性の観点からは、アカウントのなりすましや乗っ取り対策に加え、資金移動サービス、電子マネーを利用した不正送金・不正利用対策も重要と考えている。

○　その上で、去る６月に、「国民を詐欺から守るための総合対策」がまとめられ、電子マネーを利用した特殊詐欺被害の増加に伴う犯行利用防止としての、モニタリングの強化、利用停止措置等の対策の検討、資金決済業協会と協力しながら被害防止について、広報・啓発などに取り組むこととされている。

○　日本資金決済業協会においても、電子マネーに係る新たな特殊詐欺被害の事例のウェブサイトへの掲載など、被害防止に向けた取り組みを行っていると承知しており、つい先日（11/26）も貴協会主催のセミナーにおいて、警視庁や事業者の皆様の対策、取組事例等についてお話を伺ったところ。

○　こうした詐欺被害防止対策については、利用者の資産を守り、決済システム全体への信頼性を維持する観点で重要。各事業者においては、引き続き、しっかりとした対策が取られているか、今一度確認いただき、さらなる対策強化に取り組んでいただきたい。

（第一種資金移動業者）

○　第一種資金移動業については、本年、２社に対し認可を行い、足許４社となっている。第一種資金移動業者については、高額の為替取引を扱うという業務の特性上、主にシステムリスク管理、セキュリティ対策、マネロン対策、滞留資金の管理等の観点で、他の種別の資金移動業者と比較して充実した態勢整備を求めている。

○　引き続き、第一種資金移動業の登録・認可に当たっては、取り扱う業務のリスクに見合ったリスク管理態勢が構築されているかどうか、よく確認させていただくこととなる。参入を希望する事業者に置かれては、当庁及び財務局における審査業務への理解と協力をいただきたい。

（資金移動業者の口座への賃金支払いについて）

○　ご案内のとおり、給与のデジタル払いについては、厚生労働省が定める一定の要件を満たす、厚生労働大臣の指定を受けた資金移動業者の口座への賃金支払いを可能とするもので、本年８月、第一号案件の指定がなされたところ。

○　当庁としても、事業者が十分な利用者保護を図りつつ、利用者のニーズに応じたサービスを実現していくことが重要と考えており、引き続き、厚労省

と連携しながら、本制度の運用に向けた取組を進めていく。

○　これまでも各事業者において対応いただいているが、引き続き参入を希望する事業者におかれては、厚労省への相談にあわせて、当庁や財務局にも前広にご相談いただくよう、お願いしたい。

（　以　上　）