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
［2024 年 12 月 12 日開催　前払式支払手段発行者］

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。

○　前払式支払手段の発行額および発行者の推移を見ると、年間発行金額は伸長傾向にあるが、更に一段と前払式支払手段発行者が提供する決済サービスが浸透するためには、利用者利便に加えて受取側である加盟店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前払式支払手段発行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。

○　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。

○　前払式支払手段発行者が提供する決済サービスは、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する。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．高額電子移転可能型前払式支払手段発行者に対するマネロン等対策に係るモニタリング方針等について

○　前払式支払手段発行者のうち、高額電子移転可能型前払式支払手段発行者に該当する事業者はマネロンガイドラインの対象となる。従来、マネロ

ンガイドラインの対象となる事業者には、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。

○　高額電子移転可能型前払式支払手段発行者については、業務実施計画の届出に係る経過措置期間が 2025 年５月で終了することも踏まえて、経営陣主導のもと、ガイドラインに基づく態勢整備を計画的に実施いただきたい。

○　また、他業態同様に、高額電子移転可能型前払式支払手段発行者に対しても、金融庁所管の特定事業者として、業法に基づき、取引実態及びマネロン等リスク管理態勢に係る定量・定性情報を毎年ご提出いただき、個別金融機関に対するリスクの特定・評価を行っていく予定である。

○　高額電子移転可能型前払式支払手段については、特に高額のチャージや多額の譲渡が可能であることに着目したモニタリングを実施していくことを考えている。

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 2024 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、金融情報システムセンター（FISC）、日銀金融機構局、内閣サイバーセキュリティセンター（NISC）が参加。

○　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。

○　いただいたご意見への金融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。

○　金融庁としては、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）を実施した。

○　参加金融機関においては、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上、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．フィッシング対策について

○　2023 年におけるフィッシングによるものとみられるインターネットバンキングにおける預金の不正送金の被害件数及び被害総額は、それぞれ 5,578 件、約 87.3 億円であり、過去と比べて急増している。足元、2024 年上半期においては、被害件数 1,728 件、被害総額約 24.4 億円となり、被害は高止まりしている。また、フィッシング攻撃による被害は、預金取扱金融機関に限ったものではなく、それ以外の金融機関の顧客に対しても、発生している。

○　金融庁は、警察庁とも連携し、一般利用者向けに注意喚起を行っているほか、金融機関に対して、累次にわたりフィッシング対策強化の要請を行ってきた。政府としても、2024 年６月の「国民を詐欺から守るための総合対策」（※1）において、フィッシング対策の強化の方策として、「送信ドメイン認証技術（DMARC（※2））への対応促進」を始め、「フィッシングサイトの閉鎖促進」や「パスキー（※3）の普及促進」を掲げている。

※1　国民を詐欺から守るための総合対策（令和６年６月 18 日、犯罪対策閣僚会議）
https://www.kantei.go.jp/jp/singi/hanzai/kettei/240618/honbun.pdf

※2　DMARC(Domain-based Message Authentication, Reporting, and Conformance):SPF・DKIM の認証結果を利用し総合的に送信ドメイン認証を行う技術。受

信したメールが正規の送信元から送られてきたかを検証できる技術の一つ。ドメイン管理者は、認証に失敗したメールの取扱いを送信側でポリシー（DMARC ポリシー）として宣言できる。これにより、なりすまされているメールは受け取らない、といった強いポリシーを受信側に伝えることができるようになる。

※3　パスキー:パスワードが不要な認証技術。フィッシングサイト等の正規サイト以外のウェブサイトにおいては、認証が機能しないといった観点から認証技術の漏洩リスクを低減できる効果があるとされている。

○　こうした足元の状況や「総合対策」を踏まえ、2024 年 12 月中に金融庁は警察庁と連携し、業界団体を通じ、各金融機関に向け、フィッシング対策の強化を求める要請文を発出予定である(2024 年 12 月 24 日発出済み)。

○　各金融機関においては、これまでもフィッシング対策の強化を推進してきたものと承知しているが、フィッシングの手口がますます巧妙化している状況も踏まえ、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る。対応が不十分と認められる場合には、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。

８．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。

○　2024 年６月 26 日～28 日に開催された FATF プレナリーにおいて、2024 年２月末～５月初旬にかけて実施した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、前払式支払手段発行者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まいる。

９．10 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、金融安定理事会（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、FATF 基準のグローバルな実施の加速、及び、Decentralized Finance （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である。引き続き、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る。

10. 2024 事務年度における前払式支払手段発行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）

○ 各前払式支払手段発行者が提供するサービスについては、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、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、日本資金決済業協会と協力しながら被害防止についての広報・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組を行っていると承知しており、先般（2024 年 11 月 26 日）も協会主催の詐欺被害防止に向けたセミナーにおいて、警視庁や事業者の対策、取組事例等について説明があり、事業者間でモニタリングの強化等に資する観点からの情報共有が図られた。

○ 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である。各前払式支払手段発行者においては、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、更なる対策強化に取り組んでいただきたい。

（高額電子移転可能型前払式支払手段に係る対応について）

○ 2023 年６月に施行された改正資金決済法により、高額電子移転可能型前払式支払手段（以下「高額プリカ」という）を発行する場合にはあらかじめ業務実施計画を届出する必要がある。

○ 業務実施計画については、特に特定事業者として犯罪による収益の移転防止に関する法律の諸規定に係る態勢整備について確認する必要があるが、高額プリカを発行する計画のある前払式支払手段発行者においては、業務実施計画の内容について、従前より所管の財務局へご相談いただいている。

○ 業務実施計画の届出義務に係る経過措置の期限（2025 年５月）まで半年を切る中、該当する前払式支払手段発行者においては、計画的に態勢整備等の対応を進めるよう改めてお願いする。

（監督現場からの留意事項について）

○　「前払式支払手段の発行に関する報告書」について、依然として法令で定める期限までに提出いただけない事業者がいるほか、報告書の記載誤りが多く見られる。また、当局検査において過去の報告書について計数の算出誤りを指摘された事例のほか、報告書の作成作業中に供託不足が判明したものの、法令の期限までに供託が間に合わず法令違反行為等届出の提出に至るケースも見られる。内部管理部門を中心として定期的に帳簿の管理状況を確認するなど、引き続き適正な業務運営に努めていただきたい。

○　払戻し手続関係について、掲示物と電子公告で、日にちや曜日、時間が異なっている、ドラフトと実際に公告したものが違うなどの基本的な誤りが多く見られるところ、複数人によるチェックなど徹底していただきたい。また、事務ガイドラインにも定められているが、払戻しに係る申出期間について、法令で定める 60 日間は、最低限の申出期間であり、利用者が払戻しを受ける機会を確保する観点から、十分な申出期間、具体的には 90 日程度の申出期間の確保をお願いしているので引き続き協力をお願いする。

（　以　上　）