コメントの概要及びコメントに対する金融庁の考え方

No.	項目	コメントの概要	金融庁の考え方
1	全般	主要行等向けの総合的な監督指針に定められているが、電子決済等代行業者はこの「等」に該当するとの理解で良いか。資金移動業などと同様に、事務ガイドラインの第三分冊（金融会社関連）に定めるべきではないか。	電子決済等代行業は銀行法に定めているため、事務の都合上一括して主要行等向けの総合的な監督指針に整理しています。
2	Ⅸ－２	他の金融業者には監督上の着眼点として定められている「法令等遵守（コンプライアンス）態勢」、「利用者保護措置」、「利用者に関する情報管理態勢」、「苦情等への対処」、「事務リスク管理」、「反社会的勢力との関係遮断」、「不祥事件に対する監督上の対応」、「銀行等が行う為替取引との誤認防止」および「利用者に対する情報の提供」は、電子決済等代行業者に対しても、システムリスク管理とは異なるリスクを生じさせるものであり、監督指針上でも明確に定めた方が良いのではないか。	法令に定める利用者保護のための措置は所与のこととして、ご指摘の点は登録審査の時点で確認しています。 本監督指針は、登録後のモニタリングについて、イノベーションの促進と利用者保護のバランスを取りつつ、主要なリスクである、システムリスク管理に着眼して実施することを定めています。 登録後のモニタリングでは、網羅的に各リスクをモニタリングするのではなく、リスクベースでモニタリングを実施していくこととしています。 このため、電子決済等代行業者の規模・業務の特性、業容の拡大の状況等に応じ必要な点については、イノベーションを阻害しないよう配意しつつ、登録後もモニタリングを実施することになります。

No.	項目	コメントの概要	金融庁の考え方
3	Ⅸ－３	銀行システム、預金者口座にAPIを通じて外部からアクセスする電子決済等代行業者の業務特性を踏まえれば、銀行や資金移動業者には定められている以下のシステムリスクに関する主な着眼点について、銀行や資金移動業者に対する着眼点を出発点とし、それに電子決済等代行業者に対して特に求められる着眼点を追加して定めた方がよいのではないか。 ・代表取締役をはじめ、役職員がシステムリスクの重要性を十分認識し、全社的なリスク管理の基本方針（セキュリティポリシーや外部委託先に関する方針を含む）を策定すること。 ・システムに関する十分な知識・経験を有し業務を適切に遂行できる者を、システムを統括する役員として定めること。 ・代表取締役および取締役が、システム障害等発生時の危機時において、果たすべき責任やとるべき対応について具体的に定めること。また、自ら指揮を執る訓練を行い、その実効性を確保すること。 ・システムリスクが顕在化した場合の経営に重要な影響を与える可能性を十分踏まえたリスク管理態勢の整備。 ・レビュー等を通じて洗い出したリスクに対して十分な対応策を講じること。 ・制限値を超えた場合のシステム面・事務面の対応策の検討。 ・ユーザー部門とシステムリスク管理部門の連携。 ・データのバックアップなど、データがき損した場合に備えた措置。 ・適切な認証方法の例示。 ・不正防止策の例示。 ・サイバーセキュリティに係る人材の育成、拡充に関する計画の策定と実施。 ・重要な外部委託先に対して、内部監査部門又はシステム監査人等による監査。	銀行や資金移動業者とは異なる電子決済等代行業者の規模・業務の特性等に応じて、システムリスク管理に関する着眼点を定めています。銀行や資金移動業者と同様に存在する不正利用等によるセキュリティ上の問題については、同様の着眼点を定めています。

No.	項目	コメントの概要	金融庁の考え方
4	Ⅸ－３－１（１）	「利便性が損なわれるおそれがある」とあるが、サイバーセキュリティ事案（不正送金、情報漏えい等）によって発生する影響は、「利用者への損害・被害」ではないか。	電子決済等代行業のシステム障害等については、電子決済等代行業者のサービスのみが停止し利便性が損われるケース、電子決済等代行業者のサービス停止にとどまらずその影響が波及し社会経済生活等へ影響を及ぼすケースがあることを前提に、実態等を踏まえ、分割して記述していましたが、個別の事例が漏れているのではないかとのご指摘を踏まえ、包括的に記載することとします。
5	Ⅸ－３－１（２）	「字義どおりの対応がなされていなくとも、ただちに改善を求める必要はない」とする根拠は、銀行のシステムを利用すれば、送金指図の伝達や口座情報の取得が可能であることではなく、当該電子決済等代行業者の業務内容（送金指図か、口座明細取得か）、業務特性（送金指図であっても少額に限定されている、全明細を取得しているわけではない等）、規模（極めて限定的な業務規模である等）に応じてリスクベースで判断すべき側面があるという点であり、その趣旨から記述を修正すべきではないか。	利用者の利便性の観点からは、「銀行のシステムを利用すれば、送金指図の伝達や口座情報の取得が可能であること」を踏まえる点があると考えています。 なお、「銀行のシステムを利用すれば、送金指図の伝達や口座情報の取得が可能であること」はNO.4に記載したケースのうち、電子決済等代行業者のシステムのみが停止している場合を念頭に置いていますので、その旨を関連箇所に追記するとともに、重要度に応じて並び替えを行います。
6	Ⅸ－３－１（２）	「重大な問題」の例示について、「誤送金」に加え「多量の顧客情報流出」も加えたほうが良いのではないか。	当該記載はあくまで例示になります。 個人情報の漏洩に関する点については、Ⅸ－3－3(2)に明記しているとおり、適正にモニタリングを実施することになります。
7	Ⅸ－３－１（２）	「当該業務を行うにあたって連携・協働する銀行においてその部分を分担する場合には」との記述は、銀行がそのような取扱いを許容する場合に限るとの認識で良いか。	貴見のとおりです。
8	Ⅸ－３－２（１）	他の事業者（銀行、資金移動業者）向けの着眼点では「システムリスク管理部署」という表現が使用されているが、「システムリスク管理担当部署」は同部署と異なるものを想定しているのか。	ベンチャー企業も多い電子決済等代行業者では、システムリスク管理部署が単独では存在せず、一つの部署や職員が複数の業務を行っているケースがありますので、このような記載としています。

No.	項目	コメントの概要	金融庁の考え方
9	Ⅸ－３－２（４）	外部委託先管理については、FISCが出している安全対策基準（第９版）における統２０から２５・監１に沿った態勢を構築することで、今回の監督指針に対応できるという理解で良いか。 特に、クラウドについては「クラウド拠点の把握」「監査権の明記」等の考慮が必要なのか、共同センターについては緊急事態発生時における「時間性」の問題について考慮が必要なのかといった点を教示いただきたい。 また、個人情報保護委員会がhttps://www.ppc.go.jp/legal/policy/faq/のA3-12にて、特定の場合には、クラウド事業者は「委託」にあたらない旨の見解を提示しているが、これは、本指針における「委託」においても同様に解釈されるのかご教示いただきたい。	電子決済等代行業者の規模・業務の特性等に応じて、求められる水準は変わるため、一概に申し上げることはできませんが、一般論として、ご指摘の安全対策基準（第９版）に基づく対応ができている場合は、相当程度高度な業務を行っている場合を除き、本水準は満たしていると判断して差し支えありません。 また、電子決済等代行業者に対する本指針において、業務委託契約に基づき業務を委託している先と外部クラウドサービス利用規約に基づきクラウドサービスを提供している先は区別して考えています。ただし、電子決済等代行業者のサービスがクラウドサービスを利用して提供される場合には、サービス提供上の重要インフラとして、リスク管理等の視点において、外部委託先と一部共通する部分はあるものと考えています。 例えば、クラウドサービス利用について、外部委託契約に基づく委託先と共通する点として、安全対策基準（第９版）における統２９の１が挙げられます。また、クラウドサービス利用に固有の点として、同基準における統２４が関連します。 ただし、同基準は預金取扱金融機関を主な対象として想定していることから、電子決済等代行業者に求められる水準はその規模・業務の特性等に応じて自ずと変わってくるものと考えています。
10	Ⅸ－３－３（１）①（注）	「社会的に影響の大きいシステム障害等」とは、登録事業者において発生する障害のうち、利用者数、復旧時間、影響を受けるサービス内容（参照か決済指示か等）などの観点で特に社会的影響が大きいと考えられる一部の障害を指すものと考えられますが、この理解でよろしいでしょうか。	電子決済等代行業における「社会的に影響の大きいシステム障害等」とは、例えば、一事業者において発生した障害にとどまらず、決済システムへその影響が波及するなど、影響範囲が広範囲に亘る障害を想定しています。

No.	項目	コメントの概要	金融庁の考え方
11	Ⅸ－３－３（１）①（注）	「他のシステム・機器が速やかに交替することで実質的にはこれらの影響が生じない場合」について、オンプレミスにより冗長化を図る対策に加えて、クラウドサービスにより利用事業者の指示や操作によらずサービスの一環として同等の交替が行われる場合も含まれ得ると考えますが、この理解でよろしいでしょうか。 また、クラウドサービスの緊急リソース増強を実施することにより、業務影響を回避できた場合も“実質的に影響が生じない場合”に該当し得ると考えますが、この理解でよろしいでしょうか。	ご指摘のような対応等を講じた結果、実質的に影響が生じない場合は、貴見のとおりです。
12	Ⅸ－３－３（１）①（注）	「サイバー攻撃の予告」について、ＳＮＳの普及等により蓋然性の低い予告も散見される状況を踏まえると、切迫した状況にない予告も含め全てを報告対象とすることは現実的ではなく、「顧客や業務に影響を及ぼす、又は及ぼす可能性が高いと認められる」ものを報告対象とすることでよいと考えますが、この理解でよろしいでしょうか。	貴見のとおりです。
13	Ⅸ－３－３（２）	（業務改善命令が金融庁から発令されるほどではない）情報漏えい等の事案が発生した場合、その情報は電子決済等代行業者から開示されるべきではないか。	貴重な意見として承ります。
14	その他	イノベーション促進のためには、一般に規制が少ないほうが望ましいと思います。 また、政府の規制のために必要な資源は、限られています。 他方、電子決済等代行業者は、その公的性質から強い規制の下にある銀行と必ず契約を行って業務を行うものです。 したがって、電子決済等代行業の適切性確保に当たっては、銀行を通じた「間接統治」の手法を活用するべきだと思います。	銀行が、電子決済等代行業者との契約の範囲内で電子決済等代行業の適切性を監督することはご指摘のとおりです。他方で、電子決済等代行業者は利用者から委託を受けて業務を行っており、銀行から委託を受けて業務を行う銀行代理業者や銀行の外部委託先とは法的性格が異なるため、銀行として監督を行う範囲・程度は必然的に異なってきます。 金融庁では、イノベーションを促進していく観点から、モニタリングについては利用者保護を図るために必要最低限としつつ、電子決済等代行業者の負担軽減に配慮しながら実施してまいります。

No.	項目	コメントの概要	金融庁の考え方
15	その他	貴庁においては、FinTech事業者がその内部管理体制・顧客保護態勢が不十分なままにシステムの堅牢性を以て電子決済等代行業に登録する、といったことのないように対応を行っていただきたい。 現実に、対顧規約の中で、個人情報の漏洩時における補償を、（基本的なサービスを無料で提供しているにもかかわらず、）既受領分の利用料の範囲内でのみ応じるといった、およそ既存の金融事業者ではありえないような規約に基づきサービスを提供してる事例も見受けられる。 このような事業者が電子決済等代行業者として事業を行っていることについて、「内閣総理大臣」に対する「登録」という枠組みにもとづき、内閣総理大臣および貴庁に監督責任が発生する、ということを肝に銘じて、監督政策の立案・運営にあたっていただきたい。	電子決済等代行業者が提供するサービスは、利用者が、同事業者が定める利用規約に同意の上で利用しているものと承知しております。 上記の私法上の契約とは別に、銀行法では、電子決済等代行業者に対して、その業務に関し利用者に損害が生じた場合における銀行と電子決済等代行業者との賠償責任の分担に関する事項を定めた契約を銀行との間で締結・公表することを義務づけ、利用者保護を図ることとしております。 金融庁としては、利用者保護やシステムの安定性を確保しつつ、イノベーションが促進されるよう、モニタリングを実施してまいります。

以上