主要行等向けの総合的な監督指針　新旧対照表

現　　行	改　正　後
Ⅷ　銀行代理業	Ⅷ　銀行代理業
（新設）	Ⅸ　電子決済等代行業 Ⅸ－１　意義 　フィンテックの動きが世界的規模で加速する中で、利用者保護を確保しつつ、金融機関とフィンテック企業との連携・協働によるオープン・イノベーションを進めていくための制度的枠組みとして、銀行法等の一部を改正する法律（平成 29 年法律第 49 号。以下Ⅸ－２－２（１）において「改正法」という。）により電子決済等代行業者の登録制度が導入され、平成 30 年 6 月 1 日より施行された。 　電子決済等代行業者には、利用者のニーズを起点としたサービス展開の一つの核となることが期待されるとともに、利用者保護やシステムの安定性を確保しつつ機動的に金融サービスのイノベーションを実現することが期待される。 Ⅸ－２　基本的な考え方 Ⅸ－２－１　電子決済等代行業者の監督に関する基本的な考え方 　電子決済等代行業の登録制度については、他の金融関連の諸制度とは異なり、人的構成要件は求めておらず、財産的基礎も純資産額が負値でないことのみを求めているなど、新規参入のハードルは非常に低く設定されており、個人や中小・零細企業が申請してくることも想定して制度設計がなされている。その趣旨は、IT 企業等を含む多様な参加者による金融サービスのイノベーションを促進する観点にあり、規制は利用者保護を図る観点から必要最小限のものとなっている。

主要行等向けの総合的な監督指針　新旧対照表

現　　行	改　正　後
	他方で、電子決済等代行業は、利用者と銀行との中間に位置し、決済指図の伝達や口座情報の取得・顧客への提供を行うことから、利用者保護を図るため、システムの安定性が求められる。 このため、電子決済等代行業者の監督においても、利用者保護を図る観点から、主要なリスクにフォーカスし、業容拡大に伴う体制の充実に向けた取組についてモニタリングを行っていくものとする。 電子決済等代行業は基本としてITを活用した業務であり、その主要なリスクは、システムリスクとなる。電子決済等代行業者の監督に当たっては、システムリスク管理態勢を中心にモニタリングを実施し、電子決済等代行業者が、システムの安定性や利用者保護を確保しつつ、技術の進展をリードし、利用者利便の向上に資するサービスを提供することを促していくものとする。 Ⅸ－２－２　監督に係る事務処理の基本的考え方 （１）監督手法 改正法の附帯決議では、フィンテックが急速に進展する中で、IT 企業等を含む多様な参加者による金融サービスのイノベーション促進を支援する観点から、報告徴求・検査等が関係事業者等の活動やイノベーションを阻害しないこと等に留意することが求められている。こうしたことや、小規模な事業者も多く、利用者の金銭を預からない業務特性も踏まえ、事業者の負担軽減の観点から、主要なリスクであるシステムリスクについて、原則オフサイト・モニタリングによりモニタリングを実施するものとする。

主要行等向けの総合的な監督指針　新旧対照表

現　　行	改　正　後
	（２）監督部局間の連携 　登録電子決済等代行業者が、信用金庫法に基づき届出を行い信用金庫電子決済等代行業等を営む場合において、登録電子決済等代行業者の監督部局は、システムリスク管理態勢など電子決済等代行業者の業務運営に問題を認めた場合には、問題の状況等を関係する信用金庫電子決済等代行業者の監督部局等に、遅滞なく情報提供するなど、密接な連携を図ることで、電子決済等代行業者の事務負担の軽減を図るものとする。 　情報提供に当たっては、その方法を問わず、遅滞なく行うよう努めるものとする。 （３）管轄財務局長権限の一部の管轄財務事務所長等への内部委任 　電子決済等代行業者の主たる営業所又は事務所の所在地が財務事務所又は出張所の管轄区域内にある場合においては、管轄財務局長に委任した権限は、財務局長の判断により当該財務事務所長又は出張所長に内部委任することができるものとする。 　なお、法令等に基づく申請書、届出書等は、管轄財務局長あて提出させるものとする。 （４）金融庁との調整 　財務局長は、電子決済等代行業者の監督事務に係る財務局長への委任事項等の処理に当たり、以下に掲げる事項（その他の事項についても必要に応じ金融庁と調整することを妨げない。）については、あらかじめ金融庁と調整するものとする。なお、調整の際は、財務局にお

主要行等向けの総合的な監督指針　新旧対照表

現　　行	改　正　後
	ける検討の内容及び処理意見を付するものとする。 ①　法第 52 条の 61 の 16 の規定による業務改善命令 ②　法第 52 条の 61 の 17 第１項の規定による登録の取消し又は業務の停止命令 （５）行政報告 財務局長は、各四半期末現在における電子決済等代行業者の状況について、翌月 20 日までに金融庁へ報告することとする。 また、財務局長は、電子決済等代行業者の監督に関し、以下の①から⑤までに掲げる場合は、その内容を遅滞なく金融庁に報告するものとする。加えて、以下の⑥に掲げる場合は、その内容を遅滞なく金融庁に報告するとともに、他の財務局あて関係資料を送付するものとする。その際は、当該取消しの日前30日以内の役員の氏名に関する資料もあわせて報告・送付するものとする。 ①　法第 52 条の 61 の４第１項による登録を行った場合 ②　法第 52 条の 61 の７第１項による廃業等の届出を受理した場合 ③　法第 52 条の 61 の 14 により報告及び資料の提出を求めた場合 ④　法第 52 条の 61 の 16 による業務改善命令を行った場合 ⑤　法第 52 条の 61 の 17 第１項の規定による業務停止命令を行った場合 ⑥　法第 52 条の 61 の 17 第１項の規定による登録の取消しを行った場合

主要行等向けの総合的な監督指針　新旧対照表

現　　行	改　正　後
	（６）電子決済等代行業者が提出する申請書、届出書等における記載上の留意点 　電子決済等代行業者が提出する申請書、届出書等において、役員等の氏名を記載する際には、婚姻により氏を改めた者においては、婚姻前の氏名を括弧書きで併せて記載できることに留意する。 Ⅸ－３　システムリスク Ⅸ－３－１　意義 （１）　システムリスクとは、コンピュータシステムのプログラムミスや脆弱性等によるダウン又は誤作動等に伴い、利用者及び電子決済等代行業者並びに銀行が損失を被るリスクやコンピュータが不正に使用されることにより利用者及び電子決済等代行業者並びに銀行が損失を被るリスクをいうが、電子決済等代行業者には新商品・サービスの提供の拡大等に伴い、システム上の諸課題に的確に対応することが求められている。仮に電子決済等代行業者において、システム障害やサイバーセキュリティ事案（以下「システム障害等」という。）が発生した場合は、利用者の社会経済生活、企業等の経済活動において利便性が損われるのみならず、利用者保護上重大な影響を及ぼす問題が発生するおそれがある。このため、決済システムの補助的機能を担う電子決済等代行業者にとってシステムリスク管理態勢の充実強化は重要である。 （２）　ただし、以下の着眼点に記述されている字義どおりの対応が電子決済等代行業者においてなされていない場合にあっても、当該電子

現　　行	改　正　後
	決済等代行業者の規模・業務の特性等や、電子決済等代行業者のシステムのみが停止した場合においては、利用者は、当該電子決済等代行業者のシステムを経由せずとも、直接的に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、誤送金などの重大な問題が発生しておらず、利用者保護の観点から特段の問題が認められないのであれば、直ちに改善を求める必要はない。 　また、電子決済等代行業者の能力に照らして、当該電子決済等代行業者単独では、その行う電子決済等代行業に必要な水準を満たすことができない部分があったとしても、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、必要な水準を満たすものと判断する（ただし、この場合、電子決済等代行業者が新たに別の銀行と連携・協働する場合には、新たに連携・協働する銀行が、その部分を分担できているかに留意するものとする。）。 （注）サイバーセキュリティ事案とは、情報通信ネットワークや情報システム等の悪用により、サイバー空間を経由して行われる不正侵入、情報の窃取、改ざんや破壊、情報システムの作動停止や誤作動、不正プログラムの実行やDDoS攻撃等の、いわゆる「サイバー攻撃」により、サイバーセキュリティが脅かされる事案をいう。 Ⅸ－３－２　主な着眼点 （１）　システムリスク管理

主要行等向けの総合的な監督指針　新旧対照表

現　　行	改　正　後
	①　システムリスク管理担当部署は、サービスの多様化による大量取引の発生や、ネットワークの拡充によるシステム障害等の影響の複雑化・広範化などを踏まえ、定期的に又は適時にリスクを認識・評価しているか。 　また、定期的なレビューに加え、新規サービス（利用者への影響の大きい変更や、システムの変更を伴わないものの大規模な販売促進活動を行う場合を含む。）の提供とともに、レビューを実施しているか。 ②　システム障害等の発生時の被害拡大防止策及び迅速な復旧対応について、経営上の重大な課題と認識し、態勢を整備しているか。 　特に、サイバーセキュリティ事案の未然防止について、重大な課題と認識し、態勢を整備しているか。 ③　経営に重大な影響を及ぼすシステム障害等が発生した場合に、速やかに経営上責任を負う立場の者に対して報告することとなっているか。 　また、必要に応じて、対策本部を立ち上げ、速やかに問題の解決を図る態勢を構築できるよう検討を行っているか。 ④　現行システムの仕組み及び開発技術の継承を含め、事業継続のために必要な技術的対応に関する計画を策定し、実施しているか。 ⑤　提供する新サービス、銀行の API 仕様変更及び認証方式の変更等について、利用者側の動作環境を踏まえたテストシナリオを設定し、検証しているか。 ⑥　システムリスク管理態勢の整備・見直しに当たっては、その内容について第三者による評価や金融情報システムセンターが示す基準

現　　行	改　正　後
	（API 接続チェックリスト解説書等）など、客観的な水準が判定できるものを根拠として整備しているか。また、システムリスク管理態勢は、システム障害等の把握・分析、リスク管理の実施結果や技術進展等に応じて、不断に見直しを実施しているか。 （２）　情報セキュリティ管理 ①　情報資産を適切に管理するために方針の策定、組織体制の整備、社内規程の策定、内部管理態勢の整備を図り、定期的に見直しを行っているか。また、他社における不正事案等も参考に、情報セキュリティ管理態勢の PDCA サイクルによる継続的な改善を図っているか。 ②　情報の機密性、完全性、可用性を維持するために、情報資産の安全管理に関する業務遂行の責任者を定め、その役割・責任を明確にした上で、管理しているか。また、同責任者は、システム、データ、ネットワーク管理上のセキュリティに関することについて統括しているか。 ③　コンピュータシステムの不正使用防止対策、不正アクセス防止対策、コンピュータウィルス等の不正プログラムの侵入防止対策等を実施しているか。 ④　電子決済等代行業者が責任を負うべき利用者の重要情報を網羅的に洗い出し、把握、管理しているか。利用者の重要情報の洗い出しに当たっては、必要に応じ、業務、システム、外部委託先及び電子決済等代行業再委託者を対象範囲とすることも検討しているか。 ⑤　洗い出した利用者の重要情報について、重要度判定やリスク評価を実施しているか。

現　　行	改　正　後
	また、それぞれの重要度やリスクに応じ、以下のような情報管理ルールを策定しているか。 ・情報の暗号化、マスキングのルール ・情報を利用する際の利用ルール ・記録媒体等の取扱いルール　等 ⑥　洗い出した利用者の重要情報について、以下のような不正アクセス、不正情報取得、情報漏えい等を牽制、防止する仕組みを導入しているか。 ・社員の権限に応じて必要な範囲に限定されたアクセス権限の付与 ・アクセス記録の保存、検証 ・開発担当者と運用担当者の分離、管理者と担当者の分離等の相互牽制体制　等 ⑦　機密情報について、暗号化やマスキング等の管理ルールを定めているか。また、暗号化プログラム、暗号鍵、暗号化プログラムの設計書等の管理に関するルールを定めているか。また、情報の重要度に応じて管理ルールを設定しているか。 なお、「機密情報」とは、パスワード、トークン等、漏えいにより利用者に損失が発生する可能性のある情報をいう。 ⑧　機密情報の保有・廃棄、アクセス制限、外部持ち出し等について、業務上の必要性を十分に検討し、より厳格な取扱いをしているか。 ⑨　情報資産について、管理ルール等に基づいて適切に管理されていることを定期的にモニタリングし、管理態勢を継続的に見直しているか。 ⑩　セキュリティ意識の向上を図るため、全社員に対するセキュリティ

現　　行	改　正　後
	教育（外部委託先におけるセキュリティ教育の実施状況の確認等を含む）を行っているか。 ⑪　第三者機関のクラウドサービスを利用する場合には、選定に際して、その特性を踏まえた上で、セキュリティの安全性について適切な評価を実施しているか。 ⑫　電子決済等代行業者のサービスへのアクセスにおいて、利用者保護のため適切な認証機能を備えているか。 （３）サイバーセキュリティ管理 ①　サイバーセキュリティについて、経営上責任を負う立場の者は、サイバー攻撃が高度化・巧妙化していることを踏まえ、サイバーセキュリティの重要性を認識し必要な態勢を整備しているか。 ②　サイバーセキュリティについて、組織体制の整備、社内規程の策定のほか、以下のようなサイバーセキュリティ管理態勢の整備を図っているか。 ・サイバー攻撃に対する監視体制 ・サイバー攻撃を受けた際の報告及び広報体制 ・組織内 CSIRT（Computer Security Incident Response Team）等の緊急時対応及び早期警戒のための体制 ・情報共有機関等を通じた情報収集・共有体制　等 ③　サイバー攻撃に備え、入口対策、内部対策、出口対策といった多段階のサイバーセキュリティ対策を組み合わせた多層防御を講じているか。 ・入口対策（例えば、ファイアウォールの設置、抗ウィルスソフト

現　　行	改　正　後
	の導入、不正侵入検知システム・不正侵入防止システムの導入等） ・内部対策（例えば、特権 ID・パスワードの適切な管理、不要な ID の削除、特定コマンドの実行監視　等） ・出口対策（例えば、通信ログ・イベントログ等の取得と分析、不適切な通信の検知・遮断　等） ④　サイバー攻撃を受けた場合に被害の拡大を防止するために、以下のような措置を講じているか。 ・攻撃元の IP アドレスの特定と遮断 ・DDoS 攻撃に対して自動的にアクセスを分散させる機能 ・システムの全部又は一部の一時的停止　等 ⑤　システムの脆弱性について、OS の最新化やセキュリティパッチの適用など必要な対策を適時に講じているか。 ⑥　サイバーセキュリティについて、ネットワークへの侵入検査や脆弱性診断等を活用するなど、セキュリティ水準の定期的な評価を実施し、セキュリティ対策の向上を図っているか。 ⑦　サイバー攻撃を想定したコンティンジェンシープラン（緊急時対応計画）を策定し、訓練や見直しを実施し、高度化を図っているか。 （４）外部委託管理 ①　外部委託先の選定に当たり、選定基準に基づき評価、検討のうえ、選定しているか。 ②　外部委託契約において、外部委託先との役割分担・責任、監査権限、再委託手続き、提供されるサービス水準等を定めているか。ま

現　　行	改　正　後
	た、外部委託先の全社員が遵守すべきルールやセキュリティ要件を外部委託先へ提示し、契約書等に明記しているか。 ③　システムに係る外部委託業務（二段階以上の委託を含む）について、リスク管理が適切に行われているか。 特に外部委託先が複数の場合、管理業務が複雑化することから、より高度なリスク管理が求められることを十分認識した体制となっているか。 システム関連事務を外部委託する場合についても、システムに係る外部委託に準じて、適切なリスク管理を行っているか。 ④　外部委託業務（二段階以上の委託を含む）について、委託元として委託業務が適切に行われていることを定期的にモニタリングしているか。 （５）被害拡大防止措置 ①　システム障害等が発生した場合に、利用者に対し無用の混乱を生じさせないよう、利用者の被害拡大防止策を含め適切な措置を検討しているか。特に、電子決済等代行業者のシステムのみが停止した場合においては、利用者は、当該電子決済等代行業者のシステムを経由せずとも、直接的に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から、適切にそうした案内・利用者からの相談・照会対応ができているか。 なお、クラウドサービスに障害が発生した場合に備え、対応策の検討又は利用者への適時適切な注意喚起が重要であることを念頭にクラウド事業者との障害発生時の連絡体制等の構築に努めているか。

現　　行	改　正　後
	②　また、システム障害等の発生に備え、最悪のシナリオを想定した上で、必要な対応を行う態勢を検討しているか。 　特に、業務への影響が大きい重要なシステムについては、バックアップシステム等を事前に準備し、災害、システム障害等が発生した場合に、速やかに業務を継続できる態勢を整備しているか。 ③　システム障害等の発生原因の究明、復旧までの影響調査、改善措置、再発防止策等を的確に検討しているか。 ④　システム障害等の影響を極小化するために、例えば、部分的障害の影響が波及する経路や迂回不能な単一障害点の把握など、影響波及の観点からリスク評価を行い、クラウドサービスの仕組みを適切に利用してリスク低減を図るなど、利用者の被害を最小化するためのサービス・システム的な仕組みの整備について検討しているか。 Ⅸ－３－３　登録後の監督手法・対応 （１）電子決済等代行業に係る障害発生時 ①　システム障害等の発生を認識次第、直ちに、その事実を当局宛てに報告を求めるものとする。 　また、復旧時、原因解明時には改めてその旨報告を求めることとする。 　ただし、復旧原因の解明がされていない場合でも、１か月以内に現状についての報告を求めるものとする。 　特に、社会的に影響の大きいシステム障害等の場合や障害の原因解明に時間を要している場合等には、直ちに、障害の事実関係等についての一般広報及びホームページ等における利用者対応等も含めたコン

現　　行	改　正　後
	ティンジェンシープランの発動状況をモニタリングするとともに、迅速な原因解明と復旧を要請するものとする。 （注）報告すべきシステム障害等 その原因の如何を問わず、電子決済等代行業者等（外部委託先や利用しているクラウドサービス提供事業者を含む。）が現に使用しているシステム・機器（ハードウェア、ソフトウェア共）に発生した障害であって、その機能に遅延、停止等が生じているもの又はそのおそれがあるもの。 ただし、一部のシステム・機器にこれらの影響が生じても、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を除く。 なお、障害が発生していない場合であっても、サイバー攻撃の予告がなされ、又はサイバー攻撃が検知される等により、利用者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時は、報告を求めるものとする（電子決済等代行業者の業務特性に応じて対応するものとする。）。 ② 必要に応じて法第 52 条の 61 の 14 第 1 項に基づき追加の報告を求め、重大な問題があると認められる場合には、法第 52 条の 61 の 16 に基づき業務改善命令を発出するものとする。 （２）不正送金、誤送金、情報漏えい等 特権 ID の悪用による不正送金やシステムのプログラムミスによる誤送金等の利用者や経営に重大な影響がある問題を認識後、30 日以内にその事実を当局宛てに報告を求め、重大な問題があると認められる場

現　　行	改　正　後
	合には、法第 52 条の 61 の 16 に基づき業務改善命令を発出するものとする（個人である利用者に関する情報の漏えいに関するものについては、銀行法に基づく対応の他、個人情報の保護に関する法律における事業所管大臣への権限委任の状況に従い、必要な措置を執る場合があることに留意するものとする。）。 （３）外部委託先への対応 システムに係る外部委託業務について、外部委託先における適切な業務運営が懸念される場合など、必要があると認められる場合には、以下のとおり取り扱うものとする。 ①　電子決済等代行業者の管理態勢に問題が認められる場合 上記（２）の当局宛報告等により、電子決済等代行業者の業務の外部委託先に係る管理態勢に問題があると認められる場合には、必要に応じ、法第 52 条の 61 の 14 第１項に基づき報告を求め、重大な問題があると認められる場合には、法第 52 条の 61 の 16 に基づき業務改善命令を発出する等の対応を行うものとする。 ②　外部委託先の業務運営態勢等に問題が認められる場合 委託者である電子決済等代行業者を通じて、事実関係等の把握等に努めることを基本とする。この場合においても、当該電子決済等代行業者に対しては、必要に応じ、法第 52 条の 61 の 14 第１項に基づき報告を求め、重大な問題があると認められる場合には、法第 52 条の 61 の 16 に基づき業務改善命令を発出する等の対応を行うものとする。ただし、事案の緊急性や重大性等が高い場合、電子決済等代行業者に対して確認するだけでは十分な実態把握等が期待できな

現　　行	改　正　後
	い場合などには、外部委託先に対して、直接、ヒアリングを行うなど事実関係の把握等に努めることとするが、特に必要があると認められる場合（例えば、当該外部委託先に対して多数の他の電子決済等代行業者が同種の外部委託を行っている場合など）には、当該外部委託先に対して、事実関係や発生原因分析及び改善・対応策等必要な事項について、法第52条の61の14第２項に基づく報告を求めることとする。 （注）　外部委託先に対してヒアリングを実施するに際しては、必要に応じ、委託者である電子決済等代行業者の同席を求めるものとする。 Ⅸ－４　監督指針の準用 信用金庫法に基づき登録を受けた信用金庫電子決済等代行業者、協同組合による金融事業に関する法律に基づき登録を受けた信用協同組合電子決済等代行業者及び労働金庫法に基づき登録を受けた労働金庫電子決済等代行業者については、Ⅸ－１からⅨ－３までの規定を準用する。