電子決済等代行業に関する自主規制規則

（令和2年12月10日制定）

第１章　総則

（目的）

第１条　この規則は、電子決済等代行業の業務の適正を確保し、並びにその健全な発展及び利用者の利益の保護に資することを目的とする。

（定義）

第２条　この規則において使用する用語の定義は、銀行法で定める例によるほか、次の各号に掲げる用語の定義は、当該各号に定めるところによる。

(1)法 銀行法をいう。

(2)政令 銀行法施行令をいう。

(3)内閣府令 銀行法施行規則をいう。

(4)監督指針　金融庁が定める主要行等向けの総合的な監督指針をいう。

(5)電子決済等代行業再委託者　内閣府令第34条の64の9第3項に規定される電子決済等代行業再委託者をいう。

(6)協会員 一般社団法人電子決済等代行事業者協会の正会員である電子決済等代行業者をいう。

(7)経営陣 協会員における代表者、取締役及び執行役等の経営者をいう。

(8)ログイン情報　平成29年5月26日成立の改正銀行法附則第11条第2項の識別符号等であって、次号に規定する取引用パスワード等に該当しないものをいう。

(9)取引用パスワード等　ログイン情報のうち、口座に係る資金を移動させる為替取引を行うことの当該銀行に対する指図に利用する第二暗証、取引パスワード等であって、別途自主規制委員会が指定するものも含む。

第２章　経営管理及び内部管理態勢の構築

（経営管理）

第３条　協会員は、電子決済等代行業の適切な運営のために必要な会議体（会社法上の機関も含む。）を配置した上で、電子決済等代行業の業務内容や状況等を経営陣が適切かつ適時に把握し対応するための体制を整備するものとする。

2 協会員は、前項の会議体の設置に際しては、その権限や運営方法等を明確にするための規程を策定するものとする。

（内部管理）

第４条　協会員は、業務運営全般に関し、法令、自主規制及び社内規則等に則った電子決済等代行業の適切な業務を遂行するための適切なモニタリング・検証を行い、経営陣に対し重要な項目について適切に報告を行い、経営陣が重大な問題等を認識した場合には、一定期間内に改善を行うよう、その規模や特性に応じて、適当と認められる内部管理体制を構築するものとする。

2 協会員は、諸法令等の違反、不正行為その他適正な電子決済等代行業の業務運営に重大な影響があると認められる問題を役職員が確認した場合に、速やかに協会員の内部管理部門（以下、単に「内部管理部門」という。）に報告が行われ、その報告内容を内部管理部門において調査することができる態勢を整備するものとする。

3 協会員は、前項に規定する問題が諸法令等に照らして重要な問題と認められる場合は、速やかに監督当局に届け出る態勢を整備するものとする。

4 内部管理部門は、刑罰法令に抵触しているおそれのある事実が発覚した場合においては、警察等関係機関等への通報を直ちに行うものとする。
5 協会員は、第2項の規定に基づき確認された問題について、発生原因の分析を行い、責任の明確化や再発防止策の策定が行われる態勢を整備するものとする。
6 協会員は、内部通報又は報告を行った役職員が不利益を受けることがないよう、当該役職員を保護するための態勢を整備するものとする。
7 協会員は、内部監査として、以下の各号に定める事項を実施するための態勢を整備し、業務執行状況や内部管理・内部統制の適切性、有効性、合理性等の検証・評価を行わなければならない。
(1) 内部監査部門又は外部監査人に対して、監査目的を明確に指示し、監査結果を業務改善に活用するための態勢を整備していること
(2) 被監査部門は、前号の監査における指摘事項を一定期間内に改善すること
8 個人又は事業規模等により内部監査の実施が困難な協会員は、内部監査に代わる措置として、自己点検を実施することができるものとし、この場合には第7項は適用しない。
9 協会員は、電子決済等代行業の適切な運営を確保するために必要な社内規則、マニュアル等を策定し、整備するものとする。

第３章　コンプライアンス態勢

（コンプライアンス基本方針等の整備）

第５条　協会員は、コンプライアンス確保、利用者の利益の保護の観点から、適正な業務運営を確保するために、内部管理態勢の確立及び整備を行うものとする。
2 協会員は、前項の内部管理態勢整備のために、基本方針を策定のうえ、基本方針に基づく社内規則、マニュアル等を策定するものとする。
3 協会員は、前項の基本方針、社内規則、マニュアル等を作成するに際し、以下の事項を定め、適切な機関決定等を行うものとする。
(1)第７条第１項に定める組織的コンプライアンス態勢の構築
(2)遵守すべき内容及び適正な業務運営に関する具体的内容
(3)社内規則等の違反があった場合の違反者に対する懲戒処分を定めた社内規則その他の実効性確保の措置
(4)コンプライアンスに係るモニタリング及び検査に関する事項
(5)コンプライアンス確保の態勢の見直しに関する事項
4 協会員は、法、政令、内閣府令、監督指針、本規則、社内規則、マニュアル等を遵守し健全かつ適切な業務運営を実施するものとする。

（障害者への差別解消）

第６条　協会員は、前条第１項の整備にあたり、「障害を理由とする差別の解消の推進に関する法律」及び「金融庁所管事業分野における障害を理由とする差別の解消の推進に関する対応指針」に則った適切な対応を行うものとする。

（コンプライアンスに関する組織的対応）

第７条　協会員は、コンプライアンス確保に係る態勢の整備を行うために、コンプライアンスに係る組織及び権限、並びに内部管理について責任を負うべき役員等の者を明確に定めるものとする。
2 協会員は、役職員の法令等遵守意識の醸成のため、コンプライアンス研修など、役職員に対する周知徹底を行うものとする。
3 協会員は、電子決済等代行業に関し、新サービス・商品を開始する際には、法令等への抵触の有無等を判断するものとし、そのための事前確認態勢を整備するものとする。

4 協会員は前項の事前確認態勢を整備するに際し、法令等遵守に限らないコンプライアンス確保のための態勢を整備するよう努めるものとする。

第４章　反社会的勢力による被害の防止

（反社会勢力による被害の防止）

第８条　協会員は反社会的勢力（暴力団、暴力団員、暴力団員でなくなった時から ５ 年を経過しない者、暴力団準構成員、暴力団関係企業、総会屋等、社会運動等標ぼうゴロまたは特殊知能暴力集団等、その他これらに準ずる者を含む。）との関係を遮断するためには、経営陣自らが率先して断固たる態度で反社会的勢力との関係を遮断し、反社会的勢力の排除を進めるものとする。

2 協会員は、反社会的勢力との関係遮断のための社内態勢として、社内規則、マニュアル等を策定し、以下に掲げる項目のうち全部又は一部を含めるものとする。

(1)反社会的勢力による被害防止に係る基本方針
(2)協会員が締結する契約における反社会的勢力排除条項の導入
(3)反社会的勢力対応部署による一元的な管理態勢の構築(外部専門機関との連携も含む)
(4)取引に関する適切な事前審査及び事後検証の実施
(5)反社会勢力との取引解消に向けた対応方法
(6)反社会勢力からの不当要求に対処するための社内態勢の整備
(7)株主情報の適切な管理態勢

3 協会員は、前項に定める社内規則、マニュアル等を遵守し、断固たる態度で反社会的勢力との関係を遮断し、反社会的勢力の排除を進めるものとする。

第５章　利用者保護措置

（利用者保護措置を行う態勢）

第９条　協会員は、利用者保護措置の実効性の観点から、利用者保護措置に関する責任の所在を明確に定めるものとする。

2 協会員は、法第５２条の６１の８第１項各号に基づいて、以下に定める事項についての利用者に対する説明の実施を行う態勢を整備するものとする。

(1)協会員の商号、名称又は氏名及び住所
(2)協会員の権限に関する事項
(3)協会員の損害賠償に関する事項
(4)電子決済等代行業に関する利用者からの苦情又は相談に応ずる営業所又は事務所の連絡先
(5)登録番号
(6)利用者が支払うべき手数料、報酬若しくは費用の金額若しくはその上限額又はこれらの計算方法
(7)法第２条第１７項第１号に掲げる行為（内閣府令第１条の３の３に掲げる行為を除く。）を行う場合において、同号に規定する指図に係る為替取引の額の上限を設定している場合には、その額
(8)利用者との間で継続的に電子決済等代行業を行う場合には、契約期間及びその中途での解約時の取扱い（手数料、報酬又は費用の計算方法を含む。）
(9)利用者から当該利用者に係るログイン情報及び取引用パスワード等を取得して電子決済等代行業を行う場合には、その旨
(10)その他協会員の行う電子決済等代行業に関し参考となると認められる事項

3 協会員は、法第５２条の６１の８第２項に基づいて、以下に定める利用者保護措置を行う態勢を整備するものとする。

(1)協会員と銀行が営む業務との誤認を防止するための情報の利用者への提供
(2)電子決済等代行業に関して取得した利用者に関する情報の適正な取扱い及び安全管理を確保するための以下の措置

ア その業務の内容及び方法に応じ、電子決済等代行業に係る電子情報処理組織の管理を十分に行うための措置

イ 個人である利用者に関する情報の安全管理、従業者の監督及び当該情報の取扱いを委託する場合にはその委託先の監督について、当該情報の漏えい、滅失又は毀損の防止を図るために必要かつ適切な措置

ウ その取り扱う個人である電子決済等代行業の利用者に関する人種、信条、門地、本籍地、保健医療又は犯罪経歴についての情報その他の特別の非公開情報（その業務上知り得た公表されていない情報をいい、ログイン情報及び取引用パスワード等を含むものとする。）を取り扱うときは、適切な業務の運営の確保その他必要と認められる目的以外の目的のために利用しないことを確保するための措置

(3)電子決済等代行業の業務を第三者に委託する場合には、業務の内容に応じ、当該業務の的確な遂行を確保するための措置

(4)法第２条第１７項第１号に掲げる行為（内閣府令第１条の３の３に掲げる行為を除く。）を行ったときは、遅滞なく、利用者に対し、当該行為に基づき銀行が行った利用者が当該銀行に開設している口座に係る資金を移動させる為替取引の結果の通知

(5)第16条に定める電子決済等代行業再委託者の管理に関する措置

4 協会員は、前項に定める利用者保護措置に関する実効性を、定期又は必要に応じ検証するために必要な社内態勢を整備するものとする。

5 協会員は、接続先の金融機関との間での法第５２条の６１の１０第２項各号及び内閣府令第３４条の６４の１６に規定する以下の事項を含む契約の締結及び当該契約内容の公表を着実に行うことを含む、法令等遵守に関する態勢を構築するものとする。

(1)電子決済等代行業の業務に関し、利用者に損害が生じた場合における当該損害についての銀行と協会員との賠償責任の分担に関する事項

(2)協会員が電子決済等代行業の業務に関して取得した利用者に関する情報の適正な取扱いに関する事項

(3)協会員が電子決済等代行業者の業務に関して取得した利用者に関する情報の安全管理のために行う措置に関する事項

(4)協会員が電子決済等代行業者の業務に関して取得した利用者に関する情報について、協会員が上記(2)、(3)の措置を行わない場合に、銀行が行うことができる措置に関する事項

(5)協会員が電子決済等代行業再委託者の委託を受けて電子決済等代行業を行う場合において電子決済等代行業再委託者の業務（協会員に委託した業務に関するものに限る。）に関する以下の措置に関する事項

ア 当該電子決済等代行業再委託者が取得した利用者に関する情報の適正な取扱い及び安全管理のために協会員が行う措置

イ 協会員が当該措置を行わないときに銀行が行うことができる措置

6 協会員は、利用者保護の観点から、銀行との協議を行った上で、銀行と協会員とが分担して必要な利用者保護のための態勢の整備を行うものとする。

7 協会員は、法第５２条の６１の９に定める誠実義務を履行するために、第１２条に定める苦情処理対応を含め、その業務に応じた利用者に対して誠実に業務を行うために必要な社内態勢の整備を行うものとする。

8 協会員は、更新系APIを利用して業務を行う場合は、オープンAPIのあり方に関する検討会「銀行法に基づく API 利用契約の条文例」第10条第1項但書を踏まえ、銀行との契約において、一般社団法人全国銀行協会が公表しているインターネットバンキングにおける預金等の不正な払戻しに関する申し合わせにおける補償の考え方に基づき補償を行うことに関して銀行と合意した場合には、当該合意内容を誠実に履行するものとする。

（利用者への補償）

第１０条　協会員は、協会員の行う電子決済等代行業に関して利用者に生じた損害を補償する必要がある場合に、協会員の利用規約及び銀行との契約内容に従い、補償を適切に行う態勢を整備するものとする。

2 協会員は、自らの利用規約が消費者契約法等の消費者保護に関する法令に違反しないよう、必要な規約の整備を行うものとする。
3 協会員は、利用者保護の観点から、利用者に補償を行う場合の利用者向けの補償窓口を設置し、適切な運営を実施するための態勢を整備するものとする。

（重大問題の公表）
第１１条　協会員は、業務方法の変更や重要な問題の発生等において、利用者の利益の保護のために必要がある場合には、速やかに、対象となる情報を公表するものとする。

第６章　苦情等への対処

（利用者からの苦情等に対する対応）
第１２条　協会員は、電子決済等代行業の利用者から苦情等の申出がなされた場合に対応するため、以下の各号に定める内容を含む苦情処理態勢を構築する。
(1)苦情等に対し迅速かつ適切に処理又は対応ができるよう、苦情等に係る担当部署及び責任者並びに処理手続を制定すること。
(2)利用者からの苦情を受け付ける窓口を設け、その連絡先を利用者に対し公表していること。
(3)苦情等の内容に関する一定の基準を設け、当該基準を充たすものについては内部監査部門や経営陣に報告する等、事案に応じ必要な関係者間で情報共有が図られること。
(4)苦情等に係る担当部署により、苦情等申出を行った利用者に対し、対応状況についての説明等、苦情処理の進捗状況に応じた適切なフォローアップが一貫してなされること。
(5)苦情等の内容は、正確かつ適切に記録された上で、各協会員が定める適切な期間が経過するまでの間保存されるとともに、蓄積と分析を行うことによって、勧誘態勢や事務処理態勢の改善、再発防止策の策定に十分活用されること。
(6)委託業務に関する苦情等について、利用者から委託元である電子決済等代行業者に対し直接苦情を申し立てる窓口を設け、その連絡先を利用者に対し公表していること。
2 協会員は、自己の電子決済等代行業の利用者から、協会に対して苦情解決の申出がなされ、協会から苦情の内容の通知を受けた場合、協会の定めるところに従い、以下の各号に定める対応を行う。
(1)協会より苦情の処理を求められた場合に、申出人と速やかに連絡をとり誠意をもってこれに対応し、当該苦情の早期解決に努めること。
(2協会より口頭若しくは文書による説明又は資料の提供を求められた場合には、速やかに説明又は提供すること。
(3)苦情に対する処理結果について、協会へ報告すること。

（利用者の利益を保護するために必要な協会への情報報告）
第１３条　協会員は、以下の情報を取得した時は、これを速やかに協会に報告するものとする。
(1)法第５２条の６１の２の登録を受けないで電子決済等代行業を営んでいる者を知ったときは、当該者の氏名、住所及び電話番号（法人にあっては、商号又は名称、住所、電話番号及び代表者の氏名）その他の当該者に関する情報並びに当該者が行う電子決済等代行業に係る業務に関する情報
(2)電子決済等代行業該当行為を行う前に、接続先銀行との間で、法第５２条の６１の１０第１項に規定する契約を締結せずに電子決済等代行業を営んでいる電子決済等代行業者を知ったときは、その者に関する前号に掲げる情報
(3)その他利用者の利益を保護するために協会が必要と認める情報

（苦情等処理に関する社内周知）

第１４条　協会員は、社内規則等に規定された苦情処理態勢に基づいて実際の苦情処理がなされるよう、研修の実施、役職員に対するマニュアルの配布その他の社内周知のための方策を実施するものとする。

第７章　基本的なリスク管理態勢

（基本的なリスク管理態勢）

第１５条　協会員は、電子決済等代行業にかかるリスク（本条におけるリスクとは、協会員の役職員が正確な事務を怠る、あるいは事故・不正等を起こすことにより、協会員が損失を被るリスクをいう。事務リスク及び第１７条に定めるシステムリスクを含む。）管理のため、以下の各号に定める内容を含むリスク管理態勢を構築する。

(1)リスクの発生に対し迅速かつ適切に処理又は対応ができるよう、リスク対応に係る責任部署及び責任者を制定すること。

(2)関係者間での情報共有を含むリスク対応に係るフローを規定するとともに、発生したリスクの内容について蓄積と分析を行うことによって再発防止策の策定に十分活用されること。

2 協会員は、電子決済等代行業にかかるリスクを定期的にかつ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・広範化など重要な変更がある場合には適時に、(1)洗い出し、(2)リスクを認識・評価し、(3)当該リスクに対応して事務手順の見直し等を行い、また、(4)当該リスクを役職員に対し周知徹底するための態勢を構築するものとする。

3 協会員は、事務リスク及びシステムリスクに対処できるよう、前２項の対策を行うものとするが、システムリスクにおいては第８章に定める対策も実施するものとする。

（電子決済等代行業再委託者の管理）

第１６条　協会員は、電子決済等代行業再委託者の委託を受けて電子決済等代行業を営む場合においては、以下の措置を講ずるものとする。

(1)協会員において、当該電子決済等代行業再委託者をして、当該電子決済等代行業再委託者が取得した利用者に関する情報の適正な取扱い及び安全管理のために必要と認める措置を実施させることを契約等において担保すること。

(2)当該電子決済等代行業再委託者が前号の措置を講じなかった場合につき、協会員が当該電子決済等代行業再委託者に対するサービスを停止することができることその他の適切と認める対応策を、当該電子決済等代行業再委託者との間の契約において規定すること。

第８章　システムリスク管理

（総論）

第１７条　協会員は、協会員の構築したコンピュータシステムについて、プログラム上の瑕疵や脆弱性等によるシステム障害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（以下「システムリスク」という。）その他の各種のリスクが存在することを認識し、適切にリスク管理を行うため、本章に規定するリスク管理態勢を構築するものとする。但し、電子決済等代行業務を行うにあたって連携・協働する銀行においてリスク管理を担当する場合には、この限りでない。また、協会員は、本章において、協会員に要求されるリスク管理態勢を当該銀行と共同で構築することを妨げられないものとする。

（システムリスク管理）

第１８条　協会員は、協会員の構築したシステムに障害が発生することによる利用者の損害発生防止のため、以下の措置を講じるものとする。

(1)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。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うこと。
(2)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、実施すること。
(3)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、検証すること。
(4)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（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すること。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すること。
(5)APIの想定外の利用を回避するために、API利用頻度の設定、不正アクセス検知等の必要な対策を講じること。

(情報セキュリティ管理)
第１９条　協会員は、利用者から取得した情報資産を適切に管理するため、以下の措置を講じるものとする。
(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、社内規則の策定、内部管理態勢の整備を図り、定期的に見直しを行うこと。また、協会からの情報提供等を通じて把握する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ること。
(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、管理すること。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すること。
(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すること。
(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、管理すること。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すること。
(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すること。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こと。
・ 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
・ サービスの解約時及び記録媒体等の廃棄時のルール
(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こと。
・ 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
・ アクセス権限の登録、登録変更、削除の正式な手順等の制定及び管理
・ 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
・ 物理的な執務室への入室管理、外部持ち出し制限等
(7)トークン等、ログイン情報及び取引用パスワード等の漏えいにより利用者に損失が発生する可能性のある機密情報について、暗号化やマスキング等の管理ルールを定めていること。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、当該ルールにおいては、ログイン情報及び取引用パスワード等の取得及び利用は、業務上必要かつ他に実施可能な代替手段がない場合に限定していること。また、情報の重要度に応じて管理ルールを設定していること。なお、スクレイピング（電子決済等代行業に関する

ものに限る。以下、第９章において同じ。）を実施する場合には、第９章に定める措置を実施していること。
(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こと。
(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こと。
(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）を行っていること。
(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こと。
(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こと。認証認可に関する機密情報については、必要な漏洩対策を実施すること。
(13)情報資産のうち、個人である利用者の機微（センシティブ）情報については、金融庁が定める、「金融分野における個人情報保護に関するガイドライン」第５条第１項各号に列挙する場合を除き、利用しないこと。
(14)利用者に係る情報について、第三者にアクセス権を与え、または提供する場合には、当該利用者から同意を取得し、また、当該第三者の認証を適切に行うこと。
(15)偽アプリケーション、フィッシングサイトへの対応を実施し、必要に応じて利用者への注意喚起を行うこと。

（サイバーセキュリティ管理）
第２０条　協会員は、サイバーセキュリティの重要性を認識し必要な体制を整備するものとする。
2 協会員は、サイバーセキュリティについて、組織体制の整備、社内規則の策定のほか、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らねばならない。
(1)サイバー攻撃に対する監視体制
(2)サイバー攻撃を受けた際の報告及び広報体制
(3)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
(4)情報共有機関等を通じた情報収集・共有体制

（サイバー攻撃対策）
第２１条　協会員は、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ずるものとする。
2 協会員は、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ずるものとする。
(1)攻撃元のIPアドレスの特定と遮断
(2)DDos攻撃（アクセス集中等によるサービス妨害攻撃）に対して自動的にワークロードを分散させる機能
(3)システムの全部又は一部の一時的停止
3 協会員は、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ずるものとする。
4 協会員は、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、セキュリティの実装状況の定期的な評価を実施し、セキュリティ対策の向上を図るものとする。
5 協会員は、サイバー攻撃を想定したコンティンジェンシープランを策定し、訓練や見直しを実施し、高度化を図るものとする。

（外部委託管理）

第２２条　協会員は、システムに係る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、選定するものとする。
2 協会員は、システムに係る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るものとする。
3 協会員は、システムに係る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、契約書等に明記するものとする。
4 協会員は、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、リスク管理を適切に行うものとする。また、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うものとする。
5 協会員は、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、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するものとする。
6 協会員は、クラウドサービス事業者について、当該サービスの内容及びリスク特性に応じて、前五項に規定する措置に準じる措置を講ずるものとする。また、クラウド事業者の統制対象クラウド拠点が統制可能となる地域に所在していることを確保するものとする。
7 協会員は、システム以外の業務を外部委託する際にも、本条各項に定める措置を行うものとする。

（システム障害等の発生時の対応）
第２３条　協会員は、システム障害等が発生した場合には、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講ずるものとする。特に、協会員のシステムのみが停止した場合においては、利用者は、当該協会員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示の伝達や口座情報の取得が可能であることから、適切にかかる案内、利用者からの相談・照会対応を行うものとする。

（障害発生への対応準備）
第２４条　協会員は、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の連絡体制等の構築に努めるものとする。
2 協会員は、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、コンティンジェンシープランの策定等、必要な対応を行う態勢を構築するものとする。特に、業務への影響が大きい重要なシステムや利用者情報については、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するものとする。

（再発防止）
第２５条　協会員は、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講じるものとする。
2 協会員は、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を整備するものとする。

（不正アクセスへの対応）
第２６条　協会員は、不正アクセス発生時の態勢を整備し、被害拡大を最小限に止める対策を実施するものとする。
2 協会員は、アクセスログの一定期間の確保、アクセス検知のための監視体制等、原因調査・対策検討のための追跡調査方法を講じておくものとする。

（クレジットカード番号）

第２７条　協会員は、PCIDSS（Payment Card Industry Data Security Standard）の認証を受け、これに準拠した対応を行う場合を除き、クレジットカード番号の全部を保有しないものとする。

（取引用パスワード等に関する情報セキュリティ管理）

第２８条　協会員は、取引用パスワード等を保有する場合には次章による特則を遵守し、かつ、協会員の取引用パスワード等を利用するサービスへのアクセスに強い認証強度（Strong Authentification）を設定するほか、取引用パスワード等の漏洩のリスクは最も高いものと認識して必要な対策を実施するものとする。

第９章　スクレイピングを行う場合における特則

（ログイン情報に関する情報セキュリティ管理）

第２９条　協会員は、電子決済等代行業に関し、利用者からログイン情報を取得した場合には、取得したログイン情報を適切に管理するため、以下の措置を講じるものとする。

(1)ログイン情報は、機密情報の中でも最重要情報として取り扱い、以下の情報管理ルールを策定すること。

・ログイン情報の暗号化、マスキング等の安全管理措置を定めたルール

・ログイン情報の暗号化プログラム、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

・ログイン情報を利用する際の利用ルール（利用を必要最小限とすることを含む）

・ログイン情報の記録媒体等に関する取扱いルール

・利用者とのサービスに関する契約関係が終了した場合のログイン情報の廃棄ルール

(2)ログイン情報の保有については最小限度に止め、業務上不要となったログイン情報は速やかに廃棄するほか、アクセス制限、外部持ち出し等について、業務上の必要性及び不可欠性を十分に検討し、特別の厳格な取扱いを実施すること。

（スクレイピング接続による情報の不正取得、不正利用の防止）

第３０条　協会員は、スクレイピング接続により、銀行から利用者に関する情報を取得し、利用する場合には、その取得又は利用する情報の種類及び範囲を、銀行との契約等において合意したサービスの利用目的の範囲に限定するものとする。

（スクレイピング接続に関する利用者説明）

第３１条　協会員は、スクレイピング接続を実施するにあたっては、以下に定める利用者説明を行う態勢を整備し、適切な説明を行うものとする。

(1)協会員のスクレイピング接続に関する方針

(2)ログイン情報及び取引用パスワード等の管理に関する事項（適切な管理のために実施している方策の要旨を含む）

(3)スクレイピング接続により取得する情報の種類及び範囲

(4)スクレイピング接続により取得した情報の利用目的

(5)サービスに関する契約関係が終了した場合のログイン情報及び取引用パスワード等の廃棄に関する方針（業務上不要となったログイン情報及び取引用パスワード等は速やかに廃棄すること及びスクレイピング契約からAPI利用契約に移行した場合の、スクレイピングに係るログイン情報及び取引用パスワード等の破棄に関する方針を含む）

（API接続への早期移行）

第３２条　協会員は、スクレイピング接続が、API接続を開始するまでの暫定的な措置であることに鑑み、銀行と協議の上、API接続への移行期限を定めること。また、銀行において将来的

に一切APIの提供を行わない場合を除き、当該移行期限に関わらず、可能な限り早急にAPI接続に移行できるよう取り組むこととする。

第１０章　個人情報保護

（個人情報の保護）

第３３条　協会員は、個人情報の適切な取扱のために、個人情報保護法その他の法令、政府令その他の規則等、並びに、金融庁の定める金融分野における個人情報保護に関するガイドライン及び金融分野における個人情報保護に関するガイドラインの安全管理措置等についての実務指針その他の適用があるガイドライン、指針等を遵守するものとする。

2　前項のガイドライン等の遵守に当たっては、オープンAPIのあり方に関する検討会「オープンAPI のあり方に関する検討会報告書」のうち、API接続先に求められる対応として重要な情報の表示、同意取得についての規定に特に配意して、適切な対応を行うよう努めるものとする。

（データ移転に関する対応）

第３４条　協会員は、その業務の性質や方法に応じて、次の各号に留意しつつ、利用者から適切な同意の取得を図るものとする。

(1)スマートフォン等の非対面による方法で第三者提供の同意を取得する場合、例えば、同意文言や文字の大きさ、画面仕様その他同意の取得方法を工夫することなどにより、第三者提供先、当該提供先に提供される情報の内容及び当該提供先における利用目的について、明確に認識したうえで同意できるような仕様としていること。

(2)過去に第三者提供の同意を取得した場合でも、第三者提供先や提供する情報の内容が異なる場合、又はあらかじめ特定された第三者提供先における利用目的の達成に必要な範囲を超えた提供となる場合には、改めて個人である利用者の同意を取得すること。

(3)第三者提供先が複数に及ぶ場合や、第三者提供先により情報の利用目的が異なる場合には、個人データの提供先が複数に及ぶことや各提供先における利用目的が認識できるように、同意の取得方法、 同意の取得時機等を適切に検討していること。

(4)第三者提供先や第三者提供先における利用目的、提供される情報の内容について、過剰な範囲について第三者提供の同意を得る、又は同意を強制する等しないこと。

2 協会員は、利用者の電子決済等代行業により得られた情報を第三者に提供する場合には、自社の審査基準を設定し、当該第三者から必要な情報の提供を受ける等して、利用者の情報が安全に利用されるよう対応するものとする。

3 協会員は、協会員に課される法令又は契約上の義務に違反しない限り、自らが観測した又は利用者から提供を受けた利用者情報に係るデータポータビリティの確保に努める。

第１１章　協会への報告

（協会への報告対象事項）

第３５条　協会員は、金融庁による、銀行法52条の61の14第1項に基づく報告徴求命令又は金融分野における個人情報保護に関するガイドラインに基づき以下のいずれかの報告書を金融庁に提出した場合は、事前に又は事後の場合は遅滞なく、協会に対しても当該報告書の内容（当該報告書の写し又は当協会が当該報告書に関して別途指定する内容）を報告するものとする。

(1) 不祥事件等報告
(2) 障害発生等報告書
(3) 電子決済サービスを通じた不正取引発生報告等
(4) 個人情報漏えい等報告書（電子決済等代行業の利用者に影響する漏えいに関するものに限る。）

附　則
この規則は、理事会の決議の日（令和2年12月10日）から施行する。

令和4年12月22日　一部改正
令和5年9月28日　一部改正