システム等のリスク管理及び事業継続体制の整備に関する規則

（総論）

第１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、利用者及び協会員並びに金融機関等（金融サービスの提供に関する法律第11条第２項第１号イないしヨに定める者、同条３項第１号ないし第３号に定める者、同条第４項第１号イ、ロに定める者、及び貸金業者をいう。以下同様とする。）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協会員並びに金融機関等が損失を被るリスク（以下「システムリスク」という。）、事務リスク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、本規則に規定するリスク管理態勢を構築するものとする。但し、当該協会員の規模・業務の特性等により利用者保護の観点から特段の問題が認められない場合にはこの限りでない。また、協会員は、協会員に要求されるリスク管理態勢を金融機関等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への経営陣の関与）

第２条　協会員の経営陣（代表者、取締役会のほか代表者等で構成される経営に関する事項を決定する組織等をいう。以下同じ。）は、自社におけるシステムリスク管理の重要性を認識し、システムリスク管理態勢の構築のために必要な措置を講ずるものとする。例えば、以下の措置を講ずることが考えられる。

（１）システムリスクを十分認識し、全社的なシステムリスク管理の基本方針を策定すること。
（２）システム障害等の未然防止、発生時の被害拡大防止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、態勢を整備すること。
（３）システムリスクの重要性を十分に認識した上で、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、システムを統括管理する役員として定めること。
（４）システム障害等発生の危機時において、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、必要に応じて自らが指揮を執る訓練を行う等して、その実効性を確保すること。

（システムリスク等のリスク管理）

第３条　協会員は、協会員の構築したシステム障害、誤作動又はコンピュータの不正使用等が発生することによる利用者の損害発生防止に努めるものとする。例えば、以下の措置を講じるものとする。

（１）セキュリティポリシー（組織の情報資産を適切に保護するための基本方針）及び外部委託先に関する方針を含むシステムリスク管理の基本方針を策定すること。
（２）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が示す評価や基準など、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こと。また、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。
（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態勢を整備すること。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。
（４）定期的又は適時（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。）の提供時を含むが、これに限られない）にリスクを特定・分析・評価の上、当該リスクに対して十分な対応策を講ずること。
（５）提供する新サービス、金融機関等の連携に関する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。
（６）金融機関等との連携における想定外のインシデントを回避するために、必要な対策を講じること。

２　協会員において、事務リスクの所在を認識した上で事務リスク軽減のため措置（例えば、内部管理部門、内部監査部門による適切な牽制、適切な事務規程の整備と適時の見直し等）を講じなければならない。

（情報セキュリティ管理）

第４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ものとする。例えば、以下の措置を講ずることが考えられる。

（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）金融サービス仲介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。例えば、以下のようなデータを洗い出しの対象範囲とすることも検討すること。
・ 通常の業務では使用しないシステム領域に格納されたデータ
・ 障害解析のためにシステムから出力された障害解析用データ
（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）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を保有する場合には、暗号化やマスキング等の管理ルールを定めていること。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。
（８）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。
（９）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。
(10) 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。
(11) 金融サービス仲介業者のサービスへのアクセスにおいて、利用者保護のためリスクに見合った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を利用する場合には、必要な漏洩対策を実施すること。
(12) 情報資産のうち、利用者に係る情報の取扱い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」を遵守する
(13) 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５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しなければならない。

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ることの当否を真摯に検討するものとする。

（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６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の措置としては、例えば、以下のような措置を講ずることが考えられる。

（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じなければならない。

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らなければならない。

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、高度化を図らなければならない。

（システム企画・開発・運用管理）

第７条　協会員は、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人材の確保及び技術的対応に関する計画を策定し、実施するものとする。

２　協会員は提供する新サービス、金融機関等の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、検証するものとする。

（システム監査）

第８条　協会員は、システム関係に精通した要員による内部監査、システム部門から独立した内部監査部門又はシステム監査人等による外部監査を活用することによって、定期的なシステム監査を行わなければならない。

２　前項に規定する監査の対象はシステムリスクに関する業務全体をカバーし、経営陣にも適切に報告がなされるものでなければならない。

（外部委託管理）

第９条　協会員は、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、選定しなければならない。
２　協会員は、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なければならない。
３　協会員は、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、契約書等に明記しなければならない。
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わなければならない。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を整備する。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わなければならない。
５　協会員は、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なければならない。

（コンティンジェンシープラン）

第10条　協会員は、災害による緊急事態を想定するだけではなく、金融サービス仲介業者の内部又は外部に起因するシステム障害等を想定したコンティンジェンシープランを策定しなければならない。
２　協会員は、前項に規定するコンティンジェンシープランにつき、他の金融機関等や金融サービス仲介業者におけるシステム障害等の事例を踏まえるなど、想定シナリオの見直しを適宜行わなければならない。

（障害発生への対応準備）

第11条　協会員は、クラウドサービスを利用する場合には、同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なければならない。
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、必要な対応を行う態勢を構築し、外部委託先を含めた報告態勢、指揮・命令系統を明確にしなければならない。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しなければならない。

（再発防止）

第12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、再発防止策等及び当局への報告を的確に行わなければならない。
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しなければならない。

（危機管理態勢の整備）

第13条　協会員は、下記危機例も参考に自社の業務の実態や自社を取り巻くリスク環境等に応じた、初期対応の重要性等の説明、危機発生時における明確化された責任体制が明確化され、危機発生時の組織内及び関係者（当協会及び国内外の関係当局を含む。）への報告・連絡体制、最低限必要な重要な業務の特定、重要なデータ等のバックアップ体制、顧客への連絡体制の整備等を内容に含む危機管理マニュアルを整備し、常時見直しを行わなければならない。
・ 自然災害（地震、風水害、異常気象、伝染病等）

・ テロ・戦争（国外において遭遇する場合を含む。）
・ 事故（大規模停電、コンピュータ事故等）
・ 風評（口コミ、インターネット、電子メール、憶測記事等）
・ 対企業犯罪（脅迫、反社会的勢力の介入、データ盗難、役職員の誘拐等）
・ 業務上のトラブル（苦情・相談対応、データ入力ミス等）
・ 人事上のトラブル（役職員の事故･犯罪､内紛､セクシャルハラスメント等）
・ 労務上のトラブル（内部告発、過労死、職業病、人材流出等）

2　協会員は、危機管理マニュアルに基づく危機時における対応について、自社のホームページへの掲載等により、利用者への開示に努めなければならない。

3　協会員は、第１項の危機管理マニュアルを協会員の役職員に周知しなければならない。

4　協会員は、危機発生時の体制整備として、危機のレベル・類型に応じて組織全体を統括する対策本部の下、部門別・営業店別に対応内容を想定し整備するよう努めるものとする。

5　協会員は、定期的な点検・訓練を行うなど危機の未然防止に向けた取組みを実施するとともに、可能な限りその回避・予防（不可避なものは対応策を準備）に努めなければならない。