暗号資産関連デリバティブ取引業に係るシステムリスク管理に関する規則（案）

第１章 総則

（目的）

第１条　本規則は、会員が暗号資産関連デリバティブ取引に使用する情報システムに係るリスク管理における基本的な事項を定めることを目的とする。

（定義）

第２条　本規定においてシステムリスクとは、次の各号をいう。なお、各号ともに、会員以外が管理・運用するシステムも含むものとする。

(1)コンピュータシステムのダウン又は誤作動等のシステムの不備等に伴い顧客及び会員が損失を被るリスク。

(2)コンピュータが不正に使用されることにより顧客や会員が損失を被るリスク。

（システムリスク管理）

第３条　会員は、顧客や会員が自ら損失を被ることを防止するため、適切にシステムリスクの管理を行わなければならない。

２　前項の管理にあたっては、会員が直接管理するコンピュータシステムのほか、会員が暗号資産関連デリバティブ取引に係る業務を執り行うに当たり利用する外部事業者において管理・運用されるコンピュータシステムにおけるリスク管理を含むものとする。

３　会員は、システムリスクの管理においては、会員自らの経営規模及び特性等を勘案し、実効性のある体制をもって行わなければならない。

（経営姿勢）

第４条　会員の取締役会等は、システムリスクが顕在化した場合に経営に重大な影響を与える可能性があることを十分踏まえ、経営上の重大な課題と認識し、リスク管理体制を整備しなければならない。

２　会員は、中長期計画(経営戦略・ビジネス戦略)との整合性を踏まえたうえで、役職員にそのシステムリスク管理の重要性について十分に認識させ、顧客保護の観点から全社的なシステムリスク管理の基本方針を定め、リスク特性に応じて、 経営資源配分等も踏まえた安全対策の達成目標、安全対策へ投下する経営資源を決定しなければならない。

３　会員は、システムリスクとその管理状況について、定期的なレビューを行い、管理体制の改善を図るとともに、レビューの結果を踏まえて全社的なシステムリスク管理の基本方針の見直しを行い、その実践に努めなければならない。

４　会員は、前二項に定めるシステムリスク管理の基本方針の概要を公衆縦覧に供しなければならない。

５　会員は、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。）の未然防止と発生時の迅速な復旧対応及び再発防止のための体制を整備しなければならない。

6　　会員は、経営戦略の一環としてシステム戦略方針を明確にした上で、中長期の開発計画を策定し、当該開発計画につき取締役会の承認を受けなければならない。

第 2 章 体制の整備

（組織体制）

第 5 条　会員は、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役員を、システムの統括管理責任者とし、体制の整備及び改善に努めなければならない。

2　　会員の代表取締役及びシステムの統括管理責任者は、別に定めるコンティンジェンシープランの一部として、システム障害等発生の危機時において、果たすべき責任及び執るべき対応について具体的に定め、自らが指揮を執る訓練を行い、その実効性を確保しなければならない。

（システム統括管理責任者）

第 6 条　前条第 1 項に規定するシステム統括管理責任者は、システムリスク管理を指揮するほか、システム管理の最高責任者として、次の各号の役割を担うものとする。

(1)　システム管理責任者の監督

(2)　取締役会へのシステム管理状況の報告

(3)　システムトラブル発生時の対応指揮（当局等への外部連絡を含む。）

(4)　その他システム管理に係る重要な事項

（システム管理責任者の設置）

第 7 条　会員は、部署又は業務単位ごとにシステム管理責任者を設置しなければならない。

2　　システム管理責任者は、部署等に存在するシステム機器及び情報の流路を把握し、その利用及び保管方法その他日常業務におけるシステムの安全管理に必要とする事項を取りまとめ、管理状況を記録し、管轄する業務に関わる役職員のシステム安全管理を指導しなければならない。

3　　システム管理責任者は、管理対象とするシステムにおける情報漏えいその他システムの安全管理上の問題が発生した場合には、直ちにシステム統括管理責任者に報告しなければならない。

（システムリスク管理体制）

第 8 条　会員は、「暗号資産関連デリバティブ取引業に係る情報の安全管理に関する規則」第 4 章の規定に従い、システムリスク管理体制の水準を客観的に評価し、体制の整備、改善に努めなければならない。

2　　会員は、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、不断に見直しを行い、システムリスク管理体制の整備、改善に努めなければならない。

3　会員は、新サービスの導入時又はサービス内容の変更時において、ユーザー部門とシステムリスク管理部門との連携体制を整えなければならない。

4　会員は、システムに関する他社における不正・不祥事件も参考とし、システムリスク管理体制の継続的な改善を図らなければならない。

5　会員は、システムリスク管理部門によるシステム部門のモニタリングやシステム部門内の開発担当者と運用担当者の分離など、相互牽制が行われる管理体制を整備しなければならない。

第 3 章 サイバーセキュリティ管理

（サイバーセキュリティ管理）

第 9 条　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　会員は、サイバーセキュリティについて、実効性のある組織体制の整備、社内規程を策定しなければならない。

3　会員は、次の各号の事項を含め、サイバーセキュリティ管理体制の整備に努めなければならない。

(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

(5)　情報共有体制

(6)　サイバーセキュリティに係る人材の育成、拡充するための計画の策定、実施

（サイバー攻撃対策）

第 10 条　会員は、サイバー攻撃に備え、入口対策、内部対策、出口対策など、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の構築に努めなければならない。

2　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、例えば次の各号の措置の構築に努めなければならない。

(1)　攻撃元の IP アドレスの特定と遮断

(2)　DDoS 攻撃に対して自動的にアクセスを分散させる機能

(3)　システムの全部又は一部の一時的停止

3　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　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らなければならない。

5　会員は、インターネット等の通信手段を利用した非対面の取引を行う場合には、取引のリスクに見合った適切な認証方式を導入しなければならない。

6　会員は、インターネット等の通信手段を利用した非対面の取引を行う場合、例えば次の各号に掲げる措置を含め、自らの業務に応じた不正防止策を講じなければならない。

(1)　不正な IP アドレスからの通信の遮断。

(2)　顧客に対してウィルス等の検知･駆除が行えるセキュリティ対策ソフトの導入、最新化を促す措置

(3)　不正なログインや異常な取引等を検知し、速やかに顧客に連絡する体制の整備。

第 4 章 システム管理

第 1 節 企画・開発・運用

（システム企画・開発）

第 11 条　会員は、現行システムに内在するリスクを継続的に洗い出し、その維持・改善のための投資を計画的に行わなければならない。

2　会員は、システムの企画・開発に当たっては、経営戦略の一環としてシステム戦略方針の明確化及び取締役会の承認を受けた中長期の開発計画の策定に努めなければならない。

3　会員は、システム開発案件の企画・開発・移行に関し、業務の適正な実施に資する内部牽制の仕組みを設け、承認するルールを明確にしなければならない。

4　会員は、システム開発プロジェクトごとに責任者を定め、開発計画に基づいた進捗管理に努めなければならない。

5　会員は、システム開発に当たっては、テスト計画を作成し、ユーザー部門も参加するなど、適切かつ十分にテストを行わなければならない。

6　会員は、システム企画及び開発、運用管理その他システムの運用管理に係る業務の実施状況を文書にて記録し、業務に用いた資料とともに保管しなければならない。

（運用管理）

第 12 条　会員は、コンピュータシステムが正常に稼働し、適切に運用管理されていることをモニタリングし、管理体制を継続的に見直さなければならない。

2　会員は、利用するシステムに関し、現状の全体構成を把握し、システム企画、開発及び運用管理を行わなければならない。

3　会員は、システム構成の管理（構成管理）の目的及び方針、構成管理の適用範囲を定め、システム企画、開発及び運用に係る計画を立案しなければならない。

4　会員は、構成管理における現状については、次の各号を参考に整理し、構成の把握に努めるものとする。

(1)　物理資源（ハードウェア、ネットワーク、サーバー、ＰＣなど）

(2) 論理資源（ライセンス、ソフトウェア、接続構成、ドキュメント（仕様書、 設計書、契約書、運用マニュアル等）など）

5　会員は、クラウドサービス、第三者への委託業務についても構成管理の対象とするものとする。

6　会員は、構成管理が有効に機能しているかを評価、確認しなければならない。

（メンテナンス）

第 13 条　会員は、システムを安定して運用するため定期的又は適時にメンテナンスを行わなければならない。

2　会員は、定期メンテナンスにより業務を停止する予定を顧客に公表しなければならない。

（システム要員）

第 14 条　会員は、現行システムの仕組みに精通し、システム企画・開発・運用管理について専門性を持った人材の確保に努めなければならない。

2　会員は、現行システムの仕組み及び開発技術の継承並びに専門性を持った人材の育成のための具体的な計画を策定し、その実施に努めなければならない。

第 2 節 品質管理

（品質管理）

第 15 条　会員は、使用するシステムに関し、その品質を管理しなければならない。

2　会員は、顧客への提供機能の安定性及び顧客財産の安全性の向上を品質管理の最重要課題とし、品質改善に取り組まなければならない。

（品質管理計画）

第 16 条　会員は、使用するシステムの品質管理計画を定め、品質の向上に努めなければならない。

（開発管理）

第 17 条　会員は、システム開発に際し、品質を疎かにすることなく、開発の進行及び導入を管理しなければならない。

（設計）

第 18 条　会員は、システム開発に際し、セキュアコーディング（悪意のある攻撃者やマルウェア等による攻撃への耐性に係るプログラム）のルールなど開発基準を設け、システム設計段階から品質確保に努めなければならない。

（品質評価）

第 19 条　会員は、導入するシステムに関し、品質に係るテスト計画を示し、当該計画に従い品質評価を実施しなければならない。

2　会員は、品質評価の結果が所定の水準に達しなかった場合には、その導入を延期するなど、必要な措置を施さなければならない。

（導入時検査）

第 20 条　会員は、システムの新規導入又は更新に先立ち十分な実用テストを実施し、品質基準を満たしていることを確認し、実用の適否を判定しなければならない。

2　　会員は、品質基準を満たしていないシステム又は稼働状況が不安定なシステムを妄りに実用してはならない。

3　　会員は、導入時検査の結果を記録し、保管しなければならない。

（稼働状況の監視）

第 21 条　会員は、システムの稼働状況を常に監視しなければならない。

2　　会員は、システムの稼働状況を分析し、異常がないことを確認しなければならない。

（変更時の品質管理）

第 22 条　会員は、システムの変更に際しても、第 17 条から前条に規定する事項を遵守し、変更後の品質を確認しなければならない。

（システム統合リスク）

第 23 条　会員の役職員は、暗号資産関連デリバティブ取引業に関するシステム統合を行う場合、システム統合により生じるリスクについて十分認識し、そのリスクの管理体制を整備しなければならない。

2　　会員は、システム統合を行う場合、テスト体制を整備しなければならない。また、システム統合に係るテスト計画は、システム統合に伴う開発内容に適合したものとしなければならない。

3　　会員は、システム統合に係る業務を外部委託する場合であっても、会員自らが主体的に関与する体制を構築しなければならない。

4　　会員は、システム統合に係る重要事項の判断に際して、システム監査人による監査等の第三者機関による評価を活用するよう努めなければならない。

5　　会員は、システム統合に関する不測の事態に対応するため、コンティンジェンシープラン等を整備しなければならない。

第 3 節 システム監査

（システム監査）

第 24 条　会員は、システム部門から独立した内部監査部門又は外部監査によって、システム関係に精通した要員により定期的なシステム監査を行わなければならない。

2　　会員は、システム監査の対象を、システムリスクに関する業務全体をカバーするものとしなければならない。

3　　会員は、システム監査の結果を、適切に取締役会に報告しなければならない。

第 5 章 外部委託管理

（外部委託管理）

第 25 条　会員は、システム子会社を含めシステムに関する外部委託先の選定に当たり、選定基準に基づき評価、検討し、選定しなければならない。

2　　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・責任の分担、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　　会員は、システムに係る外部委託先の役職員が遵守すべきルール及びセキュリティ要件を外部委託先に提示し、契約書等に明記しなければならない。

4　　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。

（外部委託先のモニタリング）

第 26 条　会員は、システムに係る外部委託した業務について、委託元として委託業務が適切に行われていることについて、再委託された場合には最終受託者に至るまで、 定期的にモニタリングしなければならない。

2　　会員は、システムに係るリスク管理が、外部委託先任せにならないように、委託元として要員を配置するなどの措置を講じなければならない。

3　　会員は、システムに係る外部委託先における顧客データの運用状況を、委託元が監視、追跡できる体制を構築しなければならない。

4　　会員は、システムに係る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の実施又は委託先の内部統制に関する報告書の入手に努めなければならない。

（クラウドサービス利用に関する留意事項）

第 27 条　会員は、使用するシステムに関し、クラウドサービスを利用する場合には、特に次の各号に掲げる事項に留意し、システムの安定性及び情報資産の安全管理に努めなければならない。

(1)　コンピュータセンターの設置場所
(2)　契約上の義務及び保証事項
(3)　データのセキュリティ
(4)　セキュリティ実施状況の確認
(5)　暗号鍵情報の管理
(6)　暗号鍵情報以外の重要情報の管理
(7)　稼働状態の安定性
(8)　単位時間当たり情報処理能力
(9)　緊急事態への対応能力