システムリスク管理に関する規則

（2018 年 7 月 30 日　制　定）

第 1 章　総則

（目的）

第 1 条　本規則は、会員が仮想通貨の売買等及びその他重要な仮想通貨関連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利用者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利用者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、利用者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、会員が仮想通貨関連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、実効性のある態勢をもって行わなければならない。

（経営姿勢）

第 4 条　会員は、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、リスク管理態勢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、利用者保護の観点から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、管理態勢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 2 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態勢を整備しなければならない。

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、態勢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態勢）

第８条　　会員は、「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態勢の水準を客観的に評価し、態勢の整備、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態勢の整備、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態勢を整えなければならない。

４　　会員は、システムに関して他社における不正・不祥事件も参考とし、システムリスク管理態勢の継続的な改善を図らなければならない。

５　　会員は、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態勢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態勢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)利用者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、速やかに利用者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、管理態勢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利用者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、利用者への提供機能の安定性及び利用者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。

第3節　システム監査

（システム監査）

第23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24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25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利用者データの運用状況を、委託元が監視、追跡できる態勢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26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

附則

この規則は、2018 年 10 月 24 日から施行する。

システムリスク管理に関する規則に関するガイドライン

（2018 年 7 月 30 日　制　定）

第 1 条関係

本規則において「会員」とは第一種会員を指します。

第 3 条関係

システムが安全かつ安定的に稼働することは、資金決済システム及び仮想通貨交換業者に対する信頼性を確保するための大前提となります。システムリスク管理とは、システムを取り巻く種々のリスクを適切にコントロールすることを言います。

第 4 条関係

システムリスクを適切に管理するためには、システムリスク管理の基本方針の策定、及びシステムリスク管理態勢の整備等を行い、PDCA サイクルによる継続的な改善活動を行うことが重要です。

この PDCA サイクルにおいて、会員の経営陣が、新たな脅威の出現や他社の被害事例等を考慮して、適切なリスク管理プロセスを確立し、自社の経営目標や経営資源を踏まえて基本方針に基づく具体的な対応方針を決定することになります。

第 5 条第 1 項関係

システムの統括管理責任者は、会員におけるシステムリスク管理の責任者としての権限と責任を有する限り、必ずしも会社法上の役員に限定するものではありません。その場合、システムの統括管理責任者は、本条第 2 項の代表取締役及びシステムリスク管理を担当する取締役と連携し、態勢の整備及び改善に努める必要があります。

第 6 条第 1 項第 2 号関係

仮想通貨交換業においては、システムの管理状態が経営管理上の最重要課題と考えられますので、取締役会にその状況を報告すべきものと考えます。

第 7 条関係

コンピュータシステムを取扱う部署又は業務単位ごとに、システム管理責任者を設置する必要があります。当該部署等におけるシステムリスク管理の必要性によりますが、必ずしもシステムに関する専門家を設置する必要はなく、当該部署等においてシステムのリテラシーが高い人材を指名することで対応することも可能とします。

第 3 章関係

本規則における「サイバーセキュリティ」の意義については、サイバーセキュリティ基本法第 2 条の定義に則り、「電子的方式、磁気的方式その他人の知覚によっては認

識することができない方式（以下この条において「電磁的方式」という。）により記録され、又は発信され、伝送され、若しくは受信される情報の漏えい、滅失又は毀損の防止その他の当該情報の安全管理のために必要な措置並びに情報システム及び情報通信ネットワークの安全性及び信頼性の確保のために必要な措置（情報通信ネットワーク又は電磁的方式で作られた記録に係る記録媒体（以下「電磁的記録媒体」という。）を通じた電子計算機に対する不正な活動による被害の防止のために必要な措置を含む。）が講じられ、その状態が適切に維持管理されていること」をいいます。

第 9 条第 3 項第 6 号関係

仮想通貨交換業者に対するサイバー攻撃は、日夜、巧妙化・高度化しており、その対策としてサイバーセキュリティ業務を担う人材の育成、採用・拡充が求められています。

サイバーセキュリティ業務においては、他の IT 業務とは異なる、サイバー攻撃特有のスキルを要する面もあるため、人材育成計画においてはスキルマップに関する考慮が必要です。人材育成計画は、他の職種も含む会社全体の人材活用戦略、あるいはシステム戦略の中で明確化するなど、経営層のレベルで関与・把握することが重要です。

第 10 条関係第 1 項関係

「サイバー攻撃」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、サイバーセキュリティを脅かそうとする攻撃を指します。

サイバー攻撃のステップが「偵察」から始まり、「C&C サーバー」を介して最終的に攻撃者の目的達成（情報搾取（特に特権 ID）・破壊）といったように攻撃のステップが鎖のようにつながっていると捉え、その鎖のどこかで断ち切ることで攻撃目的を阻止する、サイバーキルチェーンという考え方があります。多層防御は、システムに不正侵入された場合でも、各ステップに施した対策により、情報資産の外部への流出リスクを軽減する上で有効です。

一方、多層防御は検知に負う機能が多いため、アンチウィルス製品のパターンマッチングや振る舞い検知機能、機械学習、適切なセキュリティアラート設定の困難さ、などの限界も指摘されています。このような多層防御の弱点を補う商品として、DMZ（DeMilitarized Zone）ネットワーク上のサーバーでデータ処理を行い無害化した後、クライアントに転送するソフトや、マルウェアが動き出した後に検知するのではなく、動き出す前に未然に防御する人工知能型のソフトも近年提供されています。

第 10 条関係第 3 項関係

サイバー攻撃による不正プログラム対策としては、まずインシデント情報の収集が欠かせませんが、システムへの影響度を見極め、社内規則やセキュリティポリシー等に従い、重要度の高いものから可及的速やかに OS の最新化やセキュリティパッチの適用を行うことが重要です。実務的には、外部ネットワークと接続していない社内ネットワ

ーク上のコンピューター環境等のように、リスクが相対的に小さいと判断できる場合は、重要度に従って計画を立て、パッチの適用を実施することも考えられます。

第 10 条関係第 4 項関係

仮想通貨交換業における業務の性質上、ネットワークへの侵入検査（いわゆるペネトレーションテスト）等の脆弱性診断による外部評価を定期的に実施し、改善策を講じる活動が特に望まれます。また、例えば以下のようなフレームワークやベストプラクティスを参考に、各会員の業務上の特性を踏まえて、内部評価を定期的に行うことも重要と考えられます。

・米国 NIST（国立標準技術研究所）のサイバーセキュリティフレームワーク
・米国 CIS（インターネットセキュリティセンター）の CIS-Controls（Version-7）

第 10 条関係第 5 項関係

認証方式としては、例えば以下のような方式があり、これらを組み合わせて利用することも有効です。

・可変式パスワードや電子証明書などの、固定式の ID・パスワードのみに頼らない認証方式
・取引に利用しているパソコンのブラウザとは別の携帯電話等の機器を用いるなど、複数経路による取引認証
・ログインパスワードとは別の取引用パスワードの採用
・乱数表
・トランザクション認証
・リスクベース認証
・チャレンジレスポンス認証　等

第 10 条関係第 6 項関係

各号に掲げる措置のほかにも、例えば以下のような対策が考えられます。また、これらを組み合わせて利用することも有効です。

・前回ログイン（ログオフ）日時の画面への表示
・アクセス情報の管理（異常値の検出）
・取引機能制限（取引金額の上限、送金先口座・アドレスの事前登録）
・一定期間使用されていない ID の利用停止

第 14 条第 1 項関係

本項における専門性を持った人材は、必ずしも内部の従業員のみに限らず、業務委託先における担当者であっても支障がない場合もありうると考えられます。ただし、システム企画・開発・運用管理を業務委託先に任せきりにしてはなりません。

第 15 条関係

品質管理の流れとしては、例えば、管理項目を特定し、それぞれの指標を設定し、

モニタリングを行うことが考えられます。

管理項目としては、例えば、性能管理面（CPU、ディスク、ネットワーク、サーバ等)、バグ管理面（テスト計画、障害管理等)、セキュリティ面等が考えられます。

第 18 条関係

ネットワーク構成やシステムの設計段階において、セキュリティを十分考慮することが重要です。さらに、安全性の高くなるようなコーディングルール（SQL インジェクション攻撃の余地の排除等）を作成し、教育やレビュー等でルール順守を徹底することや、安全なコーディングかどうかを自動的にチェックする市販ソフトを活用することも有効と考えられます。

第 23 条第 1 項関係

外部監査人によるシステム監査を導入する方が監査の実効性があると考えられる場合には、内部監査に代え外部監査を利用して差し支えありません。システム監査により指摘された事項に関しては、対応完了までフォローを行う必要があります。

第 25 条第 3 項関係

外部委託先との関係で利用者データの運用状況の監視、追跡が困難な場合であっても、可能な限りこれに準じた措置をとることが必要となります。

第 25 条第 4 項関係

外部委託先のリスク管理については、一次委託先に留まらず、最終次まで遡って適切に行われるよう努める必要があります。

クラウドサービスが重要な外部委託先に該当する場合、クラウド拠点に対して実質的な統制を行うにあたって必要となる権利（監査権等）を確保するために、クラウド事業者と交わす契約書等にその権利を明記することが望ましい対応といえます。もっとも、リスク評価の結果や契約交渉力など種々の制約から会員による立入監査が困難である場合などには、例えば、ISO／IEC27001、ISO/ IEC27017、SOC2／SOC3 などの第三者認証及びその報告書をもって代替することも有効です。

第 26 条第 1 号関係

クラウドサービスを提供するコンピュータセンターの場所は、所在国の法制度、自然災害などの影響を受ける可能性もあるため、サービス契約時に確認しておくことが望ましいものと考えられます。所在場所の指定が可能な場合には、リスクを検討の上で指定することにより、リスクを管理することが可能です。

第 26 条第 3 号関係

クラウドサービス上に保存するデータのセキュリティについては特に以下の観点からの検討が必要となります。

①データにアクセスできるのはだれか、操作履歴、監査等の態勢

②データが外部に流出する可能性
・クラウド上の利用者システムへの直接攻撃
・ホスト OS（ハイパーバイザー）に対する攻撃
・海外当局からのデータ提供要請への対応
・内部不正対策
③データ移行・廃棄
・契約終了時やストレージ交換時のデータ廃棄方法
・データ移行時対応（ベンダーロックイン問題）

附則

このガイドラインは、2018 年 10 月 24 日から施行します。