情報の安全管理に関する規則

（2018 年 7 月 30 日　制　定）
（2018 年 10 月 23 日 一部改正）

第 1 章　総則

（目的）

第 1 条　本規則は、会員が行う仮想通貨関連取引に係る業務における情報の安全管理のための基本的な事項を定めることを目的とする。

（情報の安全管理措置）

第 2 条　会員は、情報の漏えい、滅失、毀損又は盗難の防止その他の情報の安全管理のために必要な措置を講じなければならない。

2　会員は、自らの業務の内容及び方法に応じ、協会が別に定める「システムリスク管理に関する規則」に従い、情報の安全管理のためにシステムリスク管理を行わなければならない。

（緊急時対応等）

第 3 条　会員は、協会が別に定める「緊急時対応に関する規則」に従い、情報の安全を脅かす緊急事態が生じた場合の対応等を定めなければならない。

（基本姿勢）

第 4 条　会員は、情報の安全管理に関する方針を示し、計画的に運用しなければならない。

2　会員は、情報の安全管理に要する資源（人的資源を含む。）を適切に配分しなければならない。

3　会員は、情報の安全管理の実施状況を把握し、その有効性について評価しなければならない。

4　会員は、情報の安全管理上、不適合な状況が生じた場合には、速やかにこれを是正し、情報の安全管理態勢を継続的に改善していかなければならない。

第 2 章　基本方針

（情報セキュリティ方針等）

第 5 条　会員は、以下の内容を含む情報資産の安全管理に関する基本方針（以下、「情報セキュリティ基本方針」という。）を定め、その概要を公衆縦覧に供しなければならない。なお、本規則において、「情報資産」とは、安全管理の対象となる情報及び当該情報を管理又は保管する仕組み（電子機器及び紙の資料を含むがこれに限られない。）をいう。

(1)情報セキュリティの目標
(2)目標達成のためにとるべき行動
(3)情報セキュリティが必要な理由
(4)対象範囲とセキュリティの程度
(5)外部委託先における情報資産の安全管理に関する方針

(6)情報セキュリティの責任者

2　会員は、前項により策定する方針に基づく具体的な実施事項及び体制、役割、責任者を明らかにし、これらを業務活動に組み入れ、機能させるために必要となる社内規定を整備しなければならない。

3　会員は、前項の規定を実践するための手順その他具体的な行動を明らかとする情報セキュリティ対策手順書を策定しなければならない。

4　会員は、情報セキュリティ対策の遵守、運用状況を記録し、保管しなければならない。

第3章　体制の整備

（組織体制）

第6条　会員は、情報の安全管理の目的及び実施体制等の枠組みを示さなければならない。

2　会員の経営陣は、業務の仕組みに情報の安全管理のために必要な措置を組み入れ、業務態勢を整備しなければならない。

3　会員の経営陣は、役職員等（情報の安全管理の対象とする業務の一部を外部に委託する場合にあっては、当該外部委託先を含む。以下、この条において同じ。）を指揮し、情報の安全管理に対する役職員の取り組みを支援しなければならない。

4　会員の経営陣は、役職員等に情報の安全管理の重要性を伝達し、かつ、成果達成の意識を高めるために必要な措置の実施に努めなければならない。

（情報セキュリティ委員会の設置）

第7条　会員は、情報の機密性、完全性、可用性を維持するために、次の各号の役割を担う情報セキュリティ委員会を設置しなければならない。

(1)リスク管理の環境整備

(2)情報の安全管理に関する文書の決定

(3)情報の安全管理に関する施策の策定及び改訂

(4)発生したセキュリティ問題の検討

(5)情報の安全管理の運用評価に基づく改善

2　会員は、前項の委員会を管掌する役員を任命しなければならない。

3　会員は、第1項の委員会が有効に機能するために必要な人員その他の経営資源を配備しなければならない。

（情報セキュリティ最高責任者）

第8条　前条第2項により任命された役員は、情報セキュリティ最高責任者として、情報セキュリティ委員会を運営するほか、次の各号の役割を担うものとする。

(1) 情報管理責任者の監督

(2) 取締役会への情報セキュリティに係るリスク管理状況の報告

(3) 重大インシデント発生時の対応指揮（当局等への外部連絡を含む。）

2　情報セキュリティ最高責任者は、協会が別に定める「システムリスク管理に関する規則」第 6 条に規定するシステム統括管理責任者を兼務することができる。

（情報管理責任者の設置）
第 9 条　　会員は、部署又は業務単位ごとに情報管理責任者を設置しなければならない。
2　　情報管理責任者は、部署等に存在する情報資産を把握し、その利用及び保管方法その他日常業務における情報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情報資産の安全管理を指導しなければならない。
3　　情報管理責任者は、管理対象とする情報資産の漏えいその他情報の安全管理上の問題が発生した場合には、直ちに情報セキュリティ最高責任者に報告しなければならない。
4　　情報管理責任者は、協会が別に定める「システムリスク管理に関する規則」第 7 条に規定するシステム管理責任者を兼務することができる。
（モニタリング）
第 10 条　会員は、情報資産が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さなければならない。
（社員教育）
第 11 条　会員は、全役職員にセキュリティ教育を行わなければならない。

第 4 章　リスク管理
（リスク管理プロセス）
第 12 条　会員は、情報の安全管理に影響を及ぼす組織内外の状況を把握し、リスクアセスメントを行わなければならない。
2　　会員は、前項の結果を踏まえ、情報の安全管理に係るリスクを低減しなければならない。
3　　会員は、第 2 項の結果及び前項による低減後のリスクを用いて情報の安全管理の仕組みに期待された成果との差異を特定し、当該仕組みの適切性、妥当性、有効性を検証しなければならない。
4　　会員は、前項の検証結果を利用し、情報の安全管理の改善を継続して行わなければならない。
（リスク基準）
第 13 条　会員は、リスク管理を行うため、次の各号を含むリスク基準を定めなければならない。
(1)リスク受容基準（組織として保有することを許容するリスク水準）
(2)情報セキュリティアセスメントを実施するための基準
（リスク特定）
第 14 条　　会員は､情報の安全管理に係るリスクとその所有者を特定しなければならない。
2　　会員は、第 1 項の特定のために情報資産の目録を作成し、以下の各号の事項を明らかとしなければならない。
(1)資産の重要度又は資産価値
(2)各情報資産の管理責任者
(3)各情報資産における脅威

(4)各情報資産の脅威に対する安全管理上の脆弱性

（リスク分析）

第 15 条　会員は、リスクの発生する可能性及び発生時の結果を分析し、リスクレベルを決定しなければならない。

2　会員は、次の各号のいずれか又は組み合わせてリスク分析を行わなければならない。

(1)ベースラインアプローチ（既存の標準や基準をベースラインとして策定し、チェックする方法）

(2)非形式的アプローチ（熟練者の知識や経験に頼ったアプローチ）

(3)詳細リスク分析（情報資産ごとに資産価値、脅威、セキュリティ要件を識別して評価する手法）

3　リスク分析は、他者における不正、不祥事件も参考として行わなければならない。

（リスク評価）

第 16 条　会員は、前条の結果と第 13 条のリスク基準を比較し、リスク対応のための優先順位を決定しなければならない。

（リスク対応）

第 17 条　会員は、リスクを有する情報資産について、次の各号のいずれかの方法又は組み合わせることにより、第 13 条第 1 号により定めるリスク受容基準を満たすための対応方針を決定しなければならない。

(1)リスク低減

(2)リスク回避（リスクに関係する業務及び情報資産の廃止・廃棄）

(3)リスク共有(情報資産あるいは安全管理対策の外部委託又は保険によるリスクファイナンスなど契約等)

（管理策の決定）

第 18 条　会員は、前条の対処方針を具体化し、情報の安全管理策を決定しなければならない。

2　会員は、前項の管理策と管理策を採用した理由を記載した文書を作成し、保管しなければならない。

（情報の安全管理計画書の作成）

第 19 条　会員は、前条の管理策の実行計画を情報の安全管理計画書として取りまとめなければならない。

2　前項の計画書の作成は情報セキュリティ委員会の管掌とし、当該計画は取締役会決議により決定しなければならない。

（残留リスクの承認）

第 20 条　会員は、情報の安全管理リスク計画書に記載する各情報資産に対するリスク所有者に対し、当該計画と受容リスクについて十分に説明を行い、了解を得なければならない。

第 5 章　利用者の重要情報等

（洗い出し）

第 21 条　会員は、会員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、管理しなければならない。

2　前項の洗い出しについては、次の各号を含め、業務、システム、外部委託先を対象範囲として行わなければならない。

(1)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

(2)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

(3)使用を終え収納された文書

（利用者の重要情報に係る管理ルール）

第 22 条　会員は、利用者の重要情報に関し、それぞれの重要度及びリスクに応じ、次の各号の情報管理ルールの策定し、管理しなければならない。

(1)情報の暗号化、ハッシュ化及びマスキングのルール

(2)情報を利用する際の利用ルール

(3)記録媒体等の取扱いルール 等

（重要情報の取扱い）

第 23 条　会員は、利用者の重要情報について、次の各号の不正アクセス、不正情報取得、情報漏えい等を牽制、防止する仕組みの導入に努めなければならない。

(1)職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

(2)アクセス記録の保存、検証

(3)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

(4)システムテスト等を実施する際のテスト環境と本番環境の分離 等

（機密情報の取扱い）

第 24 条　会員は、利用者の重要情報のうち、利用者に損失が発生する可能性のある情報（機密情報）のうち、次の各号に掲げる情報について、暗号化、ハッシュ化及びマスキング等の管理ルールを定めなければならない。

(1)暗号鍵等

(2)暗証番号

(3)パスワード

(4)クレジットカード情報

(5)その他利用者に損失が発生する可能性のある情報

2　会員は、前項に関し、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なければならない。

3　会員は、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なければならない。

（個人情報）

第 25 条　会員は、利用者に関する情報管理の適切性を確保する必要性及び重要性を認識し、適切性を確保するための組織体制の確立、社内規程の策定等、内部管理態勢の整備を図らなければならない。

2　会員は、利用者の個人情報の取扱いについて、法令、保護法ガイドライン、金融分野ガイドライン、実務指針の規定に従って、取扱基準を定めなければならない。

3　会員は、利用者に関する情報へのアクセス管理の徹底、情報の持ち出しの防止に係る対策、外部からの不正アクセスの防御等情報管理システムの堅牢化を図らなければならない。

（取引時確認等により取得する個人情報の取扱い）

第 26 条　会員は、マネー・ローンダリング及びテロ資金供与対策に係る業務により取得した個人情報データの取扱いについては、「マネー・ローンダリング及びテロ資金供与対策に関する規則」に従い、保管及び廃棄を適切に行わなければならない。

第 6 章　仮想通貨管理

（仮想通貨の保管）

第 27 条　会員は、次の各号に従い、仮想通貨を安全に保管しなければならない。ただし、利用者が預託する仮想通貨の保管については、本条のほか、「利用者財産の管理に関する規則」第 5 章に従い、適切に管理しなければならない。

(1)ハッキングによる仮想通貨の盗難を防止するため、単位時間あたりに外部送金する予想数量を著しく上回る数量をオンライン環境に保管しないようにすること。

(2)複数のウォレットを設置し、盗難リスクを分散すること。

(3)保管する仮想通貨に関する最新のセキュリティ情報を入手し、保管上の対策向上に努めること。

2　会員は、次の各号の基準を設け、取り扱う仮想通貨の入出金状況をモニタリングしなければならない。

(1)1 回の指示による入出金額

(2)同一利用者からの一定期間内に指示された入出金総額

(3)全利用者による単位時間当たり入出金累計額

3　会員は、モニタリングにより基準値に達した場合には、即時に責任者に伝達され、売買停止その他必必要な措置を速やかに実施する態勢を整備しなければならない。

（暗号鍵の管理）

第 28 条　会員は、仮想通貨を保管するウォレットにより使用する暗号鍵及び乱数生成器の管理に関し、次の各号を定め、適切に管理しなければならない。

(1) 使用する暗号鍵及びシード（乱数生成に用いる設定値）の生成者に関する事項

(2) 暗号鍵及びシードの生成手法の事前検証に関する事項

(3) 暗号鍵及び乱数生成器の仕様に関する事項

(4) 乱数の保管量に関する事項

2　会員は、仮想通貨を保管するウォレットの使用方法に関し、次の各号を定め、適切に管理しなければならない。

(1) 仮想通貨の移動時に使用するアドレスに関する事項

(2) 仮想通貨の移動に必要とする秘密鍵の数の設定に関する事項

(3) リカバリーのために使用する秘密鍵の管理に関する事項

(4) アドレスを生成するウォレットの仕様に関する事項
(5) ウォレットの機能の検証に関する事項
(6) 暗号鍵の場所的分散管理に関する事項
(7) 暗号鍵の組織的分散管理に関する事項

3　会員は暗号鍵の保管に関し、次の各号を定め、適切に管理しなければならない。
(1) 暗号鍵及びシードの暗号化に関する事項
(2) バックアップ用暗号鍵及びシードの保管場所に関する事項
(3) バックアップ用暗号鍵及びシードの保管状況に関する事項
(4) バックアップ用暗号鍵及びシードのアクセス権に関する事項
(5) バックアップ用暗号鍵及びシードのアクセス検知に関する事項
(6) バックアップ用暗号鍵及びシードの暗号化に関する事項

(暗号鍵の利用)

第 29 条　会員は、暗号鍵の利用に関し、次の各号を定め、適切に管理しなければならない。
(1) 暗号鍵及びシード使用者の認証に関する事項
(2) 暗号鍵及びシードの使用環境に関する事項
(3) 暗号鍵及びシード使用者の適正性確認に関する事項
(4) 署名前の送金確認に関する事項
(5) マルチシグネチャーに使用する暗号鍵の保管場所の分離に関する事項
(6) 暗号化方式及び暗号強度に関する事項

(漏えい時の対応)

第 30 条　会員は、保有する仮想通貨の漏えいに備え、当該事態の発生時における対応手順を文書にて定めなければならない。

2　会員は、仮想通貨の管理に係るシステム等の変更が行われるときには、当該変更にあわせて前項の文書を改訂し、変更後のシステムに適した対応手順を定めなければならない。

3　会員は、暗号鍵の保管者に対し、漏えい時対応に係る訓練を実施し、当該事態が発生した場合には、速やかに手順を実行する準備が整っていることを確認しなければならない。

4　会員は、サイバー攻撃等により仮想通貨が漏えいした際の利用者に対する損害賠償に係る方針を定めなければならない。

(暗号鍵の保有者権限付与等)

第 31 条　会員は、暗号鍵及びシードの保有者への適切な権限の付与及び権限の完全な解除、変更（以下、「権限の付与等」という。）を確実に行わなければならない。

2　会員は、前項の規定を実践するため、保有者が権限を有するシステム領域を特定し、付与等を行うための手順を定めなければならない。

3　会員は、仮想通貨の管理に関連するすべての情報システムの役割と権限の付与等を記録するチェックリストを作成し、暗号鍵等の保有者権限を管理しなければならない。

4　会員は、暗号鍵等の保有者への権限の付与等について、あらかじめ定める承認

手続きを経由して適切に行わなければならない。

5　会員は、暗号鍵等の保有者への権限の付与等を承認した者及び付与等に係る作業を行った者、作業結果の確認結果を記録し、保管しなければならない。

6　会員は、内部監査をもって、暗号鍵等の保有者への権限の付与等の業務が適切に行われていることを検証しなければならない。

（セキュリティ監査）

第 32 条　会員は、仮想通貨の管理に係るシステムに対して、システムへの外部からの侵入に対する脆弱性や特権 ID の管理状況など、セキュリティに関する重要事項について、定期的に点検しなければならない。

2　会員は、前項の点検により把握した脆弱性への対処方針を策定し、計画的に対処に努めなければならない。

（データの破棄方針）

第 33 条　会員は、仮想通貨の管理に係る業務において使用されるすべての情報記録媒体に対し、当該媒体に蓄積するデータを削除するための要件及び削除手順、廃棄の検証手順を定めなければならない。

2　会員は、前項の手順に従い行ったデータの廃棄状況について検証し、その結果を記録保存しなければならない。

（残高確認）

第 34 条　会員は、少なくとも 1 日に 1 回、保管すべき仮想通貨の数量の記録とブロックチェーン上に記録された保有数量と照合し、差異が生じていないことを確認しなければならない。

2　会員は、前項の照合の結果、差異を発見した場合には、速やかにその原因を特定し、仮想通貨資産保全のために必要な措置を施すとともに、プログラムの欠陥その他システム上の不具合に起因する場合には、プログラム等の改修を図らなければならない。

3　会員は、自己が保有する仮想通貨の数量について、第三者による監査を実施しなければならない。

附則

この規則は、2018 年 10 月 24 日から施行する。

情報の安全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）
（2018 年 10 月 23 日 一部改正）

第 5 条第 1 項関係

情報セキュリティ基本方針の概要を公衆縦覧に供する方法としては、例えば、会員のウェブサイトに掲載する方法が考えられます。公表することにより、情報の安全管理に支障が生じるような内容は、情報セキュリティ基本方針の概要に含めるべきではありません。

第 7 条第 2 項関係

情報セキュリティ委員会を管掌する役員（情報セキュリティ最高責任者）については、会員における情報の安全管理の最高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。また、情報セキュリティリスクは、システムリスクの１つとして位置付けられるものであるため、会員の規模や業容に応じて、システムリスク管理に関する規則第５条に定めるシステムの統括責任者が情報セキュリティ最高責任者を兼ねることも合理的であると考えられます。

第 9 条関係

企業規模にもよりますが、日常の業務管理においても情報の安全管理は必要となることから、部署単位又は業務単位での責任者を設けて、かつ、横断的な監督を図る趣旨です。例えば、一人のみ配置されている部署であれば、当該者を情報管理責任者として指名することになります。

第 22 条関係

利用者の重要情報とは、業務上収集、蓄積、利用される顧客に関するすべての個人情報（氏名、生年月日、取引内容等）及び法人情報（代表者、決算内容、取引内容等）のうち、漏えい等の問題が起きた場合に顧客に影響を与えるおそれのある情報をいいます。

第 25 条第 2 項関係

利用者の個人情報の取扱基準においては、利用者の個人情報の具体的な取扱いを行う際の具体的なルールや手続を定めることが必要となります。これらの内容が適切に定められている限り、名称が「取扱基準」でなくても支障はありません。

第 6 章関係

本章の仮想通貨管理に関する規定については、当面の措置とし、国内外における仮想通貨の安全管理に関する議論を踏まえて、適時に見直しを行うものとします。

第 30 条関係

利用者に対する損害賠償に係る方針には、会員の責めに帰すべき事由により利用者から預託を受けた仮想通貨が漏えいした場合には損害賠償を行う旨及び損害賠償の方法並びに賠償時期に関する方針を含める必要があります。

第 32 条関係

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や脆弱性診断、いわゆるペネトレーションテスト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）

附則

このガイドラインは、2018 年 10 月 24 日から施行します。