情報システムのリスク管理に関する規程

（目的）

第１条　この規程は、当社が業務を遂行するに当たって、情報システムのリスク管理に関する事項を定め、適切かつ効果的に情報システムを利用することを目的とする。

（定義）

第２条　この規程において「情報システム」とは、ハードウェア、ソフトウェア、コンピュータ単体、及び社内ＬＡＮ（構内通信網）によって構成されたコンピュータ集合体（サーバ及びクライアント）のことをいう。

２．この規程において「情報システム資産」とは、情報システム、情報システムに係るコンピュータ・周辺機器類、記録媒体・紙、及び情報システムに係る情報（顧客情報、技術情報等）の一切のことをいう。

３．この規程において「情報システムのリスク」とは、情報システムのダウン又は誤作動等、情報システムの不備等に伴い当社が損失を被るリスク、さらに情報システムが不正に使用されることにより当社が損失を被るリスクのことをいう。

４．この規程において「情報システムのリスク管理」とは、前項に係るシステム障害やサイバーセキュリティ事案の未然防止、及び発生時の迅速な復旧について対策を講じることをいう。

（情報システムの重要性）

第３条　当社は、情報システムの重要性について、次の各号に留意するものとする。

（１）金融商品取引業者等における情報システムは、それ自体が経営戦略と一体となっていること。

（２）情報システムのリスクは、事業活動に伴って生ずるビジネスリスクのコアリスクとなっていること。

（３）情報システムのリスクは、経営環境に伴って変化するものであり、また、他のビジネスリスクへと連鎖する性質をもつこと。

（管理責任者）

第４条　当社の情報システムにおける情報システム管理責任者は、管理部長又は管理部長が適当と判断する管理部内のシステム担当者とする。

（情報システム管理責任者）

第５条　情報システム管理責任者は、情報システムのリスク管理について、迅速かつ効果的な対応を行うために、その管理責任と手続きを確立するものとする。

２　情報システム管理責任者は、情報システムのリスク管理に関する情報の収集と分析を継続的に行い、情報システムのリスクの発生を未然に防ぐとともに、実際に情報システムのリスクが発生した場合には、情報システムのリスクを局所化し、損害を最小限に抑制するものとする。

（教育・訓練）

第６条　情報システム管理責任者は、役職員に対し、情報システムに対する意識の向上、及び情報システム資産の適切な管理に関する教育・訓練を行うものとする。

（外部委託）

第７条　当社は、情報システムの適切かつ効果的な利用のために必要と判断するときは、情報システムの構築・運用の全部又は一部を外部業者に委託するものとする。

２　前項においては、情報システムのリスクを認識し、外部委託先と締結する契約書に適切なリスク管理に関する規定を設けるものとする。

３　外部委託先に対する管理責任は、委託者である当社が負わなければならないことに留意し、外部委託する場合であっても、情報システムのリスク管理のレベルは、内部管理の基準と同等の水準を維持するものとする。

（利用管理）

第８条　役職員は、作為・不作為を問わず、情報システムのリスクが発生するおそれのある行為を慎むものとする。

２．役職員は、前項に関して次の各号を遵守するものとする。

（１）インターネットについては、業務に関する必要な情報を検索・収集する場合であっても、安全性が確認できないサイトの閲覧及びダウンロードを行わない。

（２）電子メールについては、業務に関する必要な情報の伝達にのみ使用し、その他の目的において使用しない。

（３）情報システムにリスクが発生するおそれのある状況（差出人不明の電子メールの受信、コンピュータ・ウィルスに起因すると思われる不具合等）を感知した場合においては、直ちに情報システム管理責任者に報告し、その指示に従う。

（パスワード管理）

第９条　管理部は、業務において必要とする役職員に限り、情報システムに接続するための

パスワード、及びモバイル機器等から情報システムに接続するためのアクセス番号等を開示するものとする。

２．前項によりパスワード及びアクセス番号等を開示された役職員は、それらを第三者に開示・提供しないものとする。

３．管理部は、情報システムに接続するためのパスワード及びアクセス番号等を定期的に変更し、外部からの不正侵入等の防止に努めるものとする。

４．管理部は、役職員が退職した場合においては、情報システムに接続するために当該役職員が使用していたパスワード及びアクセス番号等を直ちに変更し、外部からの不正侵入等の防止に努めるものとする。

（不正接続等の禁止）

第１０条　情報システムへの接続を制限されている役職員は、他人のパスワードを使用する等、不正な方法で情報システムに接続しないものとする。

２．前項について管理部は、役職員に対して周知・徹底を行うものとする。

３．役職員は、前２項に違反する行為を発見した場合においては、直ちに情報システム管理責任者へ通報するものとする。

（モニタリング）

第１１条　情報システム管理責任者は、当社の内部環境（リスク・プロファイル等）や外部環境の状況に照らし、当社の情報システムのリスクの状況についてモニタリングを行うものとする。

２．前項における「モニタリング」とは、当社の情報システムが正常な状態に保たれるように適切な頻度で監視することをいう。

３．情報システム管理責任者は、当社の情報システムのリスクの状況に関して、役職員が適切に評価及び判断できる情報を、定期的に又は必要に応じて随時報告するものとする。

４.情報システム管理責任者は、モニタリングによって必要と判断した場合においては、本規程の改定を取締役会に諮るものとする。

５．当社は、モニタリングによってリスク管理を情報システムに実装すると判断した場合においては、可能な限り国際標準に準拠した技術を採用するものとする。

（稼働環境の確保）

第１２条　情報システム管理責任者は、情報システム資産の設置及び管理に当たっては、適切と判断する場所（以下、「セキュリティエリア」という。）を役職員に対して指示するものとする。

２．当社は、セキュリティエリアについて、地震、落雷、暴風雨及び洪水等の自然災害への

対策を講じるものとする。

３．当社は、セキュリティエリア及びその関連施設について、防火への対策を講じるものとする。

４．当社は、セキュリティエリアについて、停電等の電源異常への対策を講じるものとする。

５．当社は、セキュリティエリアについて、空調管理への対策を講じるものとする。

（保守管理）

第１３条　管理部は、情報システムの利用について、適切な保守を行うことにより、有効性・完全性を確保するものとする。

２．管理部は、情報システムを正常に稼働させるため、情報システムの能力及び容量に関わる評価を行うものとする。

３．管理部は、情報システム資産が記録されている媒体・紙の機密性及び完全性を確保するものとする。

（バックアップ）

第１４条　情報システム管理責任者は、情報システムのバックアップについての対策を講じるものとする。

２．情報システム管理責任者は、情報システムのバックアップについての対策を定期的に検証するものとする。

（資産の廃棄）

第１５条　管理部は、不要となった情報システム資産を廃棄する場合においては、格納・記録されている情報等を完全に削除するものとする。

２．前項について管理部は、削除に関する記録を作成するものとする。

（規程の改廃）

第１６条　この規程の改廃は、取締役会の決議により行うものとする。

附則

この規程は平成 30 年 7 月 13 日より施行する。

以上