システムリスク管理方針

SBI VC トレード株式会社

2021 年 12 月 1 日

1．目的

システムリスク管理方針（以下「本書」という。）は、当社が SBI グループ全体の経営方針に則った戦略目標を踏まえ、システムリスクを管理し、その実効性を維持・向上するため、必要となる基本的な考え方を定めたものであり、当社のシステムリスク管理の考え方の根幹となるものである。

当社は、すべての顧客に安心して取引に参加いただくために、SBI グループの掲げる“顧客中心主義”に基づいて、公正かつ透明のある取引環境をすべての顧客に提供することを第一に取り組んでいる。そのため、システムは当社の業務基盤に位置するものであり、これが安全かつ安定的に稼働することは、金融市場及び当社に対する信頼を確保するための大前提である。以上を踏まえ、当社はシステムリスク管理態勢の充実・強化が極めて重要であることを強く認識し、その態勢構築に努めるものである。

2．定義

本書で用いる主な用語及び定義は次による。

(1)システムリスク

システムリスクとは、コンピュータシステムのダウン又は誤作動等、システムの不備等に伴い顧客や当社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顧客や当社が損失を被るリスクをいう。

(2)システムリスク管理

システムリスク管理とは、上記(1)で定義したシステムリスクを識別、評価し、適切な対応（回避、移転、低減、受容等）を実施することをいう。適切な対応とは、システムに関するリスクの発現を防止するための管理を行うこと、並びにリスクが発現した場合には損失の最小化を図るための管理を行うことをいう。

3．本書の位置付け

本書は、システムリスク管理文書の最上位に位置する。なお、上記２．で規定するシステムリスクの内、情報セキュリティに関するリスク（コンピュータが不正に使用されること等により顧客や当社が損失を被るリスク）の管理に関しては、情報セキュリティポリシーで別途定めるものとする。

4．適用範囲

本書の適用範囲は、当社が顧客向けサービスの提供及び社内向けサービスの提供のために利用するすべてのシステムとする。

5. 適用対象者

本書の適用対象者は、当社の組織内にて、直接又は間接に、当社の指揮監督を受けて、当社の業務に従事しているすべての従業者をいう。従業者には、雇用関係にある者（正社員、契約社員、嘱託社員、パート社員、アルバイト社員等）のみならず、当社との間の雇用関係にない者（取締役、監査役、派遣社員）を含む。

6. システムリスク管理体制

取締役会は、システム障害の未然防止と障害発生時の影響拡大防止を経営上の重大な課題と認識し、当社のシステムリスクを十分認識した上で、全社的なシステムリスク管理の基本方針（本書）を審議し承認する。本書は定期的及び必要の都度、見直しを行うものとする。又、システムリスクに関して問いかけを行うこと、ならびに定期的にシステムリスクに対する施策、その対応や課題について報告を受けるものとする。業務執行取締役は同基本方針に基づき、定期的にシステムリスクに関する情報を経営者及び取締役会に報告する体制を構築する。取締役会はその報告を受け、想定されるリスクの種類と所在を認識したうえで、リスクが顕在化した際の影響を把握し、影響度に応じた意思決定を行うものとする。

また、システムリスク管理の維持・向上を推進するため、システムリスク管理を重視する企業風土を醸成し、もって実効性のあるシステムリスク管理体制を整備するものとする。

システムリスク管理部門はシステム部とし、情報システム管理規程に基づき、システム開発・運用面、及び外部委託先管理においてのシステムリスク管理を行うものとする。

7. システムリスク管理策等の策定方針

システムリスクに関する管理体制及び管理策は、以下の各項目の要件を充足するように構築するものとする。なお、システムリスク管理策の策定にあたっては、当社利用システムに対するリスク分析等に基づいて、対策の有効性・費用対効果・運用の容易性等を考慮する。

(1)システムリスクに対する認識等

当社のシステムリスクを十分認識した上で、全社的なシステムリスク管理の基本方針を策定する。また、システムリスクに関する情報が適切に取締役会及び経営者に報告される体制を構築する。

(2)適切なシステムリスク管理体制の確立

システムリスク管理体制は、当社の業務の実態やシステム障害等を把握・分析し、システム環境等に応じて、その障害の発生件数・規模をできるかぎり低下させて事業内容に必要とされるレベルを維持するべく、実効性のある体制とする。

(3)システム監査

システム部門から独立した内部監査部において定期的なシステム監査を行うこととし、また、外部専門家もしくはグループ内関係企業の監査部門による監査の活用によりこれに代えることができることとする。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するものとする。

内部監査部は、システム監査の結果を適切に取締役会に報告するものとする。

(4)安全対策の整備

安全対策を適正に管理するための管理者を設置するものとし、当該管理者はシステム外部委託先と連携し、システム、データ、ネットワークの管理体制を各々統括する。

システム開発・運用にかかる安全対策の手順詳細は運用細則に定めるものとする。

(5)外部委託管理

外部委託の基本方針を明確にし、システムに係る外部委託について、外部委託管理規程及び外部委託に関する運営細則に基づき、リスク管理の観点から選定・管理及び評価を適切に行う。

当社は、重要な顧客向けサービスに関わるシステムの運用を外部に委託しており、当社の業務に対する外部委託先の比重が高いため、重要な外部委託先とはサービスレベル合意書等を締結し、定期的な運用報告を受けることにより、外部委託先から受けるサービスの継続的な評価と品質のチェックを維持するものとする。

また、外部委託業務に関する顧客への責任は当社に帰することを十分に認識し、問題が発覚した際は、外部委託先と連携して速やかに是正するものとする。

(6)コンティンジェンシープラン

システム関連や大規模地震等の広域災害を含むコンティンジェンシープランを策定し、緊急時体制を構築する。当該体制については、全従業者に対し周知を行い、当社の業務の実態やシステム環境等に応じて常時見直し、また、必要に応じ、訓練等を行うことでその実効性を検証するものとする。

(7)障害発生時の対応

システム障害発生時の指揮命令系統を明確にし、障害発生時には、顧客に無用の混乱を生じさせないよう適切な措置を講じると共に、システム外部委託先と連携し、速やかに顧客へ報告するための体制を整備する。障害の復旧対応にあたっては、システム外部委託先との協力体制のもと、影響の最小化及び復旧の早期化に努めるものとする。

また、発生したシステム障害の影響範囲が、当社が予め定めた基準に該当する場合は、速やかに担当当局にシステム障害の内容を報告する。

また、発生したシステム障害の内容を記録し、顧客に対し重要な影響を与えた障害については、根本原因を調査し再発防止策を講じ、施策の完了まで実行管理を行うものとする。

システムリスク管理部門は、システム障害発生時に適切かつ速やかな対応が行えるよう、当社システムに精通した要員を育成し、かつ、必要な際の連絡手段を確保するものとする。

(8)システムリスクの評価

システムリスク管理部門の責任者は、システム運営上の損失の潜在的規模や発生可能性を分析し、例えば、システム障害発生時の予想損失額やシステム変更及び新規構築時におけるリスクを定量化するなど、システムリスクを適切に評価するものとする。システムリスクの評価は定期的及び必要の都度行うこととし、評価手順の詳細はシステムリスク評価基準に定めるものとする。

8. 教育・周知

すべての従業者に対して、本書及び本書に基づき定められた規程・基準等を遵守するよう教育・周知を行う。また、必要に応じ、システムリスク管理部門が主導となり、全従業者に対しシステムリスクの重要性に

つき周知を図るものとする。

9. 遵守義務

すべての従業者は、システムリスク管理の重要性を認識した上で、本書及び本書に基づき定められた規程・運用細則等を遵守しなければならない。

10. 監査

システムリスク管理策の有効性及び妥当性の確認は、システム部門における自主点検、内部監査部における内部監査及び外部監査等により行う。