システムリスク管理基本方針

1. システムリスク管理の目標

当社は、さまざまな業務において情報システムを使用しており、それら情報システムの停止または誤作動、システムの不備及び障害、コンピュータの不正使用等により、利用者の皆様及び当社自身が被るリスクを、システムリスクとして認識しています。当社は、利用者の皆様に信頼される取引環境を継続的かつ安定的に提供するため、システムリスクの発生の防止及び影響の最小化並びに損失の低減を図り、システムに対して適切な安全対策を講じます。

また、サイバーセキュリティリスクについても重要な経営課題として認識し、適切な管理を実施します。

2. 目標達成のためにとるべき行動

(1) リスク管理体制の整備

当社は、システムリスク管理を推進し、システムリスク事象発生時の迅速な対応と復旧を実現するため、システムリスク管理に関する規程及び関連手続に基づき、システムリスク管理の体制整備を行います。

取締役会は、システムリスクに関する情報共有を行い、対応方針その他必要な事項を審議するとともに、システムリスク管理及びサイバーセキュリティリスク管理に必要な経営資源を適切に配分し、迅速かつ適切な意思決定及び対応を行います。

また、システムリスクの管理体制は、業務内容の変更、システムの導入・廃棄、その他管理体制に影響を及ぼす事象に応じて適宜見直し、その有効性の維持及び向上に努めます。

さらに、取締役会の監督の下、関係部門が連携し、全社的な責任体制の下でシステムリスク管理及びサイバーセキュリティリスク管理を推進します。

(2) リスクの特定、分析、評価及び対応方針の決定

当社は、システムリスク管理に関する規程に基づき、少なくとも年１回、また、システム構成、業務内容その他に重要な変更が生じた場合に、当社の情報システム、クラウドサービス、外部事業者が管理又は運用する情報システム、情報資産及び関連業務に係るシステムリスク及びサイバーセキュリティリスクを網羅的に調査、特定し、分析及び評価を実施します。評価結果に基づき、必要な対応方針を決定し、安全対策を策定・実施します。また、安全対策の実施状況及び有効性を確認するとともに、対策

実施後に残存するリスクを継続的に管理します。
情報システムの企画、開発、導入及び重要な変更に当たっては、セキュリティ・バイ・デザインの考え方を取り入れ、企画段階から適切な安全対策を講じます。また、システム障害及びサイバーセキュリティ事案については、未然防止、迅速な対応及び復旧並びに再発防止に継続的に取り組みます。

(3) サイバーセキュリティ管理

当社は、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攻撃等のいわゆるサイバー攻撃が高度化・巧妙化している状況を認識しています。
当社は、サイバー攻撃等による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対応・復旧を、経営上の重大な課題として認識し、サイバーセキュリティ管理体制を整備します。また、多層防御の考え方に基づく安全対策、脆弱性管理、サイバー攻撃の監視・検知、インシデント対応及び定期的なセキュリティ評価を実施し、サイバーセキュリティ対策の継続的な改善に努めます。

(4) 教育と周知の徹底

当社は、役職員がその役割及び責任に応じてシステムリスク及びサイバーセキュリティリスクを適切に理解し、必要な対応を実施できるよう、教育、研修及び必要な訓練を実施するとともに、関係規程及び手続の周知徹底を図ります。

(5) 情報システムの最新技術及び金融犯罪の動向に係る調査・研究

当社は、常に新たなシステムリスクに対応するために、情報システムの最新技術、サイバーセキュリティ並びに情報システムを利用した金融犯罪及び不正利用の動向等に関する情報を収集・分析し、必要に応じて社内外の関係者と適切に情報共有を行います。

(6) システムリスクに係る監査

当社は、システムリスクの管理方針、管理体制及び運用の有効性並びに関連する規程及び手続の遵守状況について、定期的又は必要に応じて、独立した立場から監査を実施します。また、必要に応じて管理体制及び安全対策の有効性を評価します。監査または評価結果並びにシステム障害及びサイバーセキュリティ事案から得られた知見等を踏まえ、システムリスク管理及びサイバーセキュリティ対策の改善事項については、継続的な改善活動へ反映します。

(7) 法令・規制の遵守

当社は、情報システムに係る法令、規制及びガイドライン等の動向を適切に把握し、必要に応じて規程及び手続きの見直しを実施するとともに、遵守状況を継続的に監視する体制を整備します。

3. システムリスク管理の対象範囲

当社は、システムリスク管理の対象範囲を、当社が業務上使用及び保有するすべてのコンピュータ、データベース及びネットワーク等の情報システム（クラウドサービス及び外部事業者が管理又は運用する情報システムを含む。）、当該情報システムに含まれまたは当該情報システムより出力される情報資産並びにこれらの利用・管理に係る関連業務とします。また、本方針は、当社役員、社員、契約社員、パート、アルバイトを含むすべての従業員、また、当社の業務に従事する業務委託先要員等に適用します。
さらに、当社と契約した協力会社及び外部委託先に対しては本方針を踏まえたシステムリスク管理及びサイバーセキュリティ対策を求めます。

4. 外部委託先におけるシステムリスク管理に関する方針

当社は、システムの開発、運用、保守を外部委託業者に委託する場合、その適格性を十分に審査するとともに、委託先におけるシステムリスクを適切に把握・評価し、必要な安全管理措置を求めます。また、委託期間中は継続的なモニタリングを実施し、委託業務の安全性及び信頼性の確保を図ります。また、クラウドサービスその他のサードパーティについても、その重要性に応じてリスクを評価し、継続的に管理することにより、適切なシステムリスク管理を実施します。

5. システムリスク管理の責任者

当社のシステムリスク管理の責任者は、システム統括管理責任者とします。

株式会社ガイア

2021 年 6 月 18 日制定
2023 年 6 月 27 日改定
2025 年 9 月 26 日改定
2026 年 7 月 29 日改定