システムリスク管理基本方針

東光商事株式会社（以下、「会社」という）は、さまざまな業務においてコンピュータシステムを使用しており、それらコンピュータシステムのダウンまたは誤動作、システムの不備、コンピュータの不正使用等により、会社のお客様又は他の業者及び会社が損失を被るリスクをシステムリスクと認識します。会社ではシステムリスクの発生の防止及び最小化、並びにリスク発生による損失の低減を図り、事業の継続性を確保するうえで、システムに対して適切な安全対策を講じ、金融機関の責任として、また経営リスクの一つとして認識し、本方針を策定しこれを遵守します。

令和1年12月1日制定
東 光 商 事 株 式 会 社
代表取締役 片岡 龍郎
【情報システム管理責任者 山本 剛史】

（対象・適用範囲）

第１条　本基本方針は、会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（以下、「情報システム」という）、情報システムに含まれる又は出力される情報（以下、「情報資産」という）、また情報システム及び情報資産の利用・管理に係る業務（以下、「関連業務」という）を対象とし、役員、すべての従業員（社員、契約社員、パート、アルバイト、常駐する外部委託先からの要員を含む）、また会社と契約した協力会社及び外部委託先に適用します。

（システムリスク管理体制の整備）

第２条　会社は、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での迅速な対応と復旧を実現するため、別途定めたシステムリスク管理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。

２．会社は、各部門の管理責任者により構成される「情報セキュリティ委員会」において、システムリスクに対する情報の共有化、対応等を検討し、システムリスクに対して迅速かつ適切な意思決定及び対応の実施を目指します。

３．情報セキュリティ委員会は、情報システム管理責任者をシステムリスク管理統括責任者として、全社横断的なシステムリスク管理体制の構築を推進します。

４．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、その他体制に影響を与えうる事象に応じて適宜見直し、常に有効なシステムリスク管理を実施することを目指します。

（システムリスクの特定・分析・評価・対応方針の決定）

第３条　会社は、システムリスク管理規程及び関連手続に基づき、定期的かつ適宜、会社の情報システム、情報資産、また関連業務に係るシステムリスクを網羅的に調査、特定し、脆弱性及び脅威を分析した上で、お客様又は他の業者及び会社への影響度や対応の必要性等を評価します。

２．システムリスクの特定・分析・評価については、システム部門担当者及び情報資産管理責任者又は情報資産管理者が中心となり、関連各部門と連携し全社的な観点から実施し、その結果を情報セキュリティ委員会に報告するものとし、対応方針については情報セキュリティ委員会内で検討され、その承認をもって決定します。

３．システム部門担当者及び情報資産管理責任者又は情報資産管理者は当該対応方針に基づき、関連各部門と協力し安全対策を策定し、関連各部門が安全対策を速やかに実施できるよう支援します。

４．対応の実施状況については情報セキュリティ委員会で定期的に報告され、全社的なリスク・マネジメントの一環として推進します。

（情報セキュリティ管理）

第４条　会社は、別途定めた情報セキュリティ基本方針及び情報セキュリティ管理規程と併せて、情報資産の機密性・完全性・可用性を適切に維持するため情報セキュリティの観点からもシステムリスク管理活動を推進します。

（サイバーセキュリティ管理）

第５条　会社は、サイバー攻撃が高度化・巧妙化していることを踏まえ、サイバーセキュリティ事案の未然防止と発生時の迅速な復旧対応について、経営上の重大な課題と認識し、サイバーセキュリティ管理体制を整備します。

サイバーセキュリティ事案とは、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攻撃等の、いわゆる「サイバー攻撃」により、サイバーセキュリティが脅かされる事案をいいます。

（外部委託先管理による信頼性の確保）

第６条　会社は、システムの開発・運用・保守を外部業者に委託する場合、個人情報保護基本規程及び個人情報保護細則に則り、外注（委託）先選定要領にて選定基準を明確にし、適格性を審査した上、安全かつ正確な委託業務の運用が行なわれるよう、外部委託先におけるシステムリスクの状況把握と評価を行い、適切な安全対策を要請し、委託業務の信頼性の確保を図ります。

（システムリスクに係る教育・周知徹底）

第７条　会社の役職員が自らの業務において係るシステムリスクの内容を認知し、適切な

対応を実施できるよう、システムリスクに関する啓蒙活動や教育を実施します。

（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）

第８条　会社は、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に関する情報、システムに係る金融犯罪の動向等に関する情報を収集するように努め、社内外の関係者に対する情報共有を推進します。

（システムリスクに係る監査）

第９条　会社は、システムリスクの管理方針、目的、特定・分析・評価・対応、またそのプロセス及び手順の遵守性、有効性、適切性等について定期的かつ適宜監査を実施します。

２．情報システムに係る監査は監査室によって内部監査の一環として実施する他、専門家による第三者的な立場からの外部監査の実施も検討します。

３．監査において検出された事項は、情報セキュリティ委員会及び取締役会で報告され、内部監査規程に則り、改善が完了するまで報告対象とします。

（法令・規制の遵守）

第１０条　会社は、情報システムに係る法令・規制に関する情報収集に努め、変更等が行われた場合の各規程、文書類への変更適応、遵守状況を監視する体制を整備します。

２．システム部門担当者が情報システムに係る法令・規制の変更に対応します。

（見直し・改廃）

第１１条　本管理基本方針及びシステムリスクに係る規程の改廃については、情報セキュリティ委員会で協議し、社長の決裁を得たうえで施行します。

２．本管理基本方針及びシステムリスクに係る規程の見直しについては、システム部門担当者において定期的かつ適宜実施し、その内容についても情報セキュリティ委員会で協議し、変更時には社長の決裁を得ることとします。