システムリスク管理基本方針

システムリスク管理基本方針（概要）

１．目的

当社は、システムリスク（当社以外が管理・運用するシステムを含むコンピュータシステムのダウン又は誤作動等のシステムの不備等に伴いお客様及び当社が損失を被るリスク、更にコンピュータが不正に使用されることによりお客様や当社が損失を被るリスク）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るため、本システムリスク管理基本方針を定めます。

２．システム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、規程等を整備します。また、システムリスクの管理体制は適宜見直し、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。

３．システムリスクの特定・分析・評価・対応方針の決定

当社は、定期的に当社の情報システム、情報資産、及び関連業務に係るシステムリスクを網羅的に調査、特定し、脆弱性及び脅威を分析した上で、当社及びお客様への影響度や対応の必要性等を評価します。

４．サイバーセキュリティ管理

当社は、サイバー攻撃が高度化・巧妙化していることを踏まえ、情報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。

５．システムリスクに係る教育・周知徹底

当社は、当社の役職員が自らの業務において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。

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、目的、特定・分析・評価・対応、並びにそのプロセス及び手順の遵守性、有効性、適切性等、システムリスク全体について定期的に監査を実施します。