

# システムリスク管理方針

株式会社CryptoGarage

株式会社Crypto Garage（以下「当社」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又は誤動作等のシステムの不備に伴い当社の利用者及び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、当社の利用者及び当社が損失を被るリスクをシステムリスクと認識しています。当社ではシステムリスクの発生防止及び最小化、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、当社の責任として、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。

## （対象・適用範囲）

第1条 本方針は、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（以下「情報システム」という。）、情報システムに含まれる、安全管理の対象となる情報及び当該情報を管理又は保管する仕組み（電子機器及び紙の資料を含むがこれに限られない。）（以下「情報資産」という。）、並びに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、当社の役員及び当社と契約した外部委託先に適用します。

## （システムリスク管理態勢の整備）

第2条 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で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規程』及び関連規程・手続（以下、これらを併せて「規程類」という）に基づき、システムリスク管理の態勢整備を行います。

2 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、その他態勢に影響を与え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 当社は、規程類に基づき、定期的かつ適宜に、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、当社及び利用者への影響度や対応の必要性等を評価します。

## （情報セキュリティ管理）

第4条 当社は、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 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、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、サイバー攻撃対策を実施します。

## （外部委託先管理）

第6条 当社は、システムの開発・運用・保守その他システムに係る業務を外部企業に委託する場合、規程類に則り、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われるよう、外部委託先におけるシステムリスク管理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。

## （緊急事態への対応）

第7条 当社は、規程類に則り、コンティンジェンシープランを策定し、システム障害等緊急事態発生時において速やかかつ適切な措置を行うものとします。また、コンティンジェンシープランに基づく訓練を定期的実施します。

(システムリスクに係る教育・周知徹底)

第8条 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。

(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9条 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10条 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かつ適宜監査を実施します。

(法令・規制の遵守)

第11条 当社は、情報システムに関連する法令・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等、文書類への変更適応及び遵守状況を監視する体制を整備します。

以上