システムリスク管理基本方針

株式会社ビットポイントジャパン（以下「当社」といいます。）は、情報システムが事業基盤の重要な要素であること、情報システムに関するリスクを適切に管理することが経営の最重要課題の一つであること、暗号資産交換業者として社会的責任を有することを十分に認識した上で、システムリスクの顕在化を未然に防止するとともに、システムリスクが顕在化した際の損失の極小化を図るべく、お客さま保護の観点から、情報システムの信頼性、安全性、有効性、効率性、遵守性を確保するための管理態勢を維持・充実・向上するうえで必要となる基本的な考え方を定めることを目的に、以下のとおりこのシステムリスク管理方針（以下「本方針」といいます。）を定めます。

第１条（対象・適用範囲）

１．本方針は、当社が業務上使用するハードウェア、ソフトウェア、データベース、ネットワーク及び記憶媒体等で構成される情報システム（以下「情報システム」といいます。）、情報システムに含まれる又は処理される情報（情報システムと情報を併せて、以下「情報資産」といいます。）、並びに情報資産の利用・管理に係る業務（以下「情報資産関連業務」といいます。）を対象とします。

２．本方針は、当社の役員、すべての従業員（社員、契約社員、嘱託社員、パート、アルバイト、常駐する外部委託先からの要員を含みます。）、また、当社が使用する情報システム又は情報資産関連業務に関わる協力会社及び外部委託先（クラウドサービス業者を含みます。）に適用します。

第２条（システムリスク管理態勢の整備）

１．当社の経営陣は、本方針を遵守し、お客さま及び当社の資産が損失を被らないように主導し、システムリスク管理態勢を整備するとともに、新たなシステムリスクに対応するため、継続的改善に努めます。

２．当社は、システムリスク管理を有効に機能させるため、システムリスク管理状況を適確に把握し情報資産に対するリスク管理を推進する責任の所在及び対応部署を明確にし、システム障害やサイバーセキュリティ事案等（以下「システム障害等」といいます。）が発生した場合に備え、迅速な対応と復旧を実現するため、システム障害等発生時における対応指針及び事業継続計画（BCP）等を整備します。

３．システムリスク管理態勢は、業務内容の変更、情報システムの導入・変更・廃棄、その他リスク管理態勢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現することを目指します。

第３条（規程等の整備）

１．当社は、システムリスク管理の要件を明確にするため、システムリスク管理規程のほか、本方針に準拠した規程、マニュアル等を整備します。

２．当社の役職員等は、関連法令及び適用されるガイドラインのほか、前項の社内規則等を遵守し

ます。
3．当社は、役職員等に対して関連法令等のほか、システムリスク管理に関する規程、マニュアルの周知徹底を図るとともに、これに反するような指示、命令を行なわないものとします。

第４条（システムリスクの特定・分析・評価・対応方針の決定）
1．当社は、定期的かつ適宜、当社の情報資産及び情報資産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うえで、当社及びお客さま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、全社的な観点から実施し、その結果を取締役会に報告するものとし、対応方針については、取締役会で検討され、その承認をもって決定するものとします。
3．当社の関連部署は、前項で決定された対応方針に基づき、安全対策を策定するとともに、当該安全対策が速やかに、かつ、適切に実施します。
4．安全対策の実施状況は定期的にモニタリングするとともに、取締役会に対して報告します。

第５条（情報セキュリティ管理）
1．当社は、別途定める情報セキュリティ基本方針及び関連規程と併せて、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。
2．当社は、情報資産の機密性・保全性・可用性を適切に維持するため、情報セキュリティに関する管理態勢を整備し、それに基づく情報セキュリティ管理の適切な運用を行います。また、それらの状況を評価し、必要に応じて適切な予防処置及び是正処置を講じることにより、情報セキュリティの充足を図るものとします。

第６条（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、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、サイバー攻撃対策等を含むサイバーセキュリティ管理態勢を整備します。

第７条（システムリスク管理及び情報セキュリティに係る教育・訓練）
1．当社の役職員が自らの業務において係るシステムリスク管理態勢及び情報セキュリティに関して、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に、システムリスク及び情報セキュリティに関する教育や研修を実施します。
2．当社は、システムリスクが顕在化した際の早期復旧、業務継続を図るべく、定期的な訓練を実施します。

第８条（情報システムの信頼性の向上）

当社は、情報システムの信頼性、安全性、有効性及び機能性を保持するために、情報システムの企画・立案段階から計画性を持ち、一貫した管理方法に基づき、開発、運用及び保守の各フェーズにおいて適確な対策を講じるものとします。

第９条（事業継続管理）

当社は、当社の情報資産の漏洩、紛失、改竄及び不正アクセス並びに情報システムの中断及び信頼性損失等の情報資産に影響を及ぼす可能性のあるシステムリスクとその影響範囲を定期的に把握及び想定し、事業継続性を堅持するために持続的なリスク管理を行います。また、災害、トラブル及び想定外のシステムリスク事象の発生時においても、影響範囲を極小化するためのシステム管理及びシステム運用を目指し、万が一情報システムが中断した場合であっても早急に復旧可能な措置を講じるものとします。

第 10 条（外部委託管理及び外部サービス管理による信頼性の確保）

１．当社は、システム開発、システム運用・保守又は情報資産関連業務を外部に業務委託する場合、選定基準、評価等の手続きを明確にし、外部委託先の適格性を審査したうえで、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。また、外部委託先における安全対策の実施状況が適切であることを確認するために、外部委託先のシステムリスク管理態勢を継続的に検証し、業務委託における信頼性の確保に努めるものとします。

２．外部サービスの利用に関しても、前項に準じて適切な対応を行うものとします。

第 11 条（情報システムのモニタリング）

当社は、情報資産管理の安全性確保及び情報セキュリティ保持の観点から、情報システムに対するモニタリング態勢・環境の構築を行うとともに、定期的に分析及び評価し、必要に応じて是正措置を講じるものとします。

第 12 条（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やシステムリスク管理に関する手法等の情報、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し分析するように努め、それをシステムリスク管理態勢の維持・充実・向上のために活用します。

第 13 条（システムリスクに関するモニタリング・監査）

１．当社は、本方針及びそれに基づく規程やガイドライン、関連法令を遵守し、システムリスク管理態勢を整備・運用しているかにつき、そのリスクの程度に応じた頻度・手法等で監査を実施します。なお、外部の専門家による第三者的な立場からの外部監査の実施も必要に応じて実施します。

２．当社は、システムリスク管理態勢の整備・運用状況の有効性及び妥当性を、自主点検及び日常

的モニタリングにおいても確認するものとします。

3．前二項の監査又は自主点検等モニタリングの結果を踏まえ、必要に応じ適切な是正措置を講じることにより、システムリスク管理の継続的な改善に努めるものとします。

第 14 条（継続的改善）

当社は、システムリスクとその管理状況について定期的なレビューを行い、システムリスク管理態勢の継続的な改善を図るとともに、当該レビューの結果を踏まえ、必要に応じ、本方針の見直しを行い、その実践に努めます。

第 15 条（改廃）

本方針の改廃は、取締役会の決議によります。

2019 年 7 月 29 日制定
2021 年 4 月 22 日改定
2022 年 5 月 10 日改定

株式会社ビットポイントジャパン
代表取締役　　田 代　卓