# 情報セキュリティ基本方針

東京ハッシュ株式会社（以下、「当社」といいます。）は、情報資産（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ません。）をいいます。以下同様。）の機密性・完全性・可用性を適切に維持するためには情報セキュリティの確保が必要不可欠であることを十分に認識し、また、利用者をはじめ社会からの信頼を常に得ることを情報セキュリティの目標として、これらの情報資産の適切な保護・管理を通じた情報セキュリティの確保を経営上の最重要課題に位置づけています。当社は、以下の項目を通じて、情報セキュリティマネジメントシステムを確立し、情報セキュリティを確保できるよう、継続的に取り組んでまいります。本情報セキュリティ基本方針（以下、「本基本方針」といいます。）の対象となる情報資産は、当社が保有するすべての情報資産とします。

１．目的

本基本方針は、当社が行う暗号資産関連取引に係る業務における情報の安全管理のための基本的な事項を定めることを目的としています。

２．情報セキュリティ体制の構築

情報資産の保護および適切な管理を行うために、経営陣を中心とした管理体制のもと情報セキュリティ最高責任者を設置し、情報セキュリティマネジメントシステムを構築し、情報セキュリティの維持、向上に取り組みます。

３．情報資産の適切な管理

情報の漏えい、滅失、毀損又は盗難の防止その他の情報の安全管理のために必要な措置を講じます。

４．基本姿勢

① 当社は、情報セキュリティに関する社内規程等を整備し、情報資産の保護及び適切な管理を行うためのルールを社内に周知徹底します。
② 当社は、情報の安全管理に要する資源（人的資源を含む。）を適切に配分します。
③ 当社は、情報の安全管理の実施状況を把握し、その有効性について評価します。
④ 当社は、情報の安全管理上、不適合な状況が生じた場合には、速やかにこれを是正し、情報の安全管理態勢を継続的に改善していきます。
⑤ 当社は、情報セキュリティ対策の遵守、運用状況を記録し、保管します。

５．委員会の設置

情報セキュリティ管理については定例開催のコンプライアンス委員会において検討事項を協議し、検討結果を取締役会に報告します。

６．リスク評価の実施

情報資産を定期的に調査・把握し、リスク評価を行い、リスク評価結果に基づいて情報資産の管理方法の見直しを行います。

７．社員教育・訓練の実施

当社の全役職員および関係者の情報セキュリティに関するリテラシーの向上を図るとともに、情報資産の適切な管理を実行するために、情報セキュリティ教育・訓練を徹底します。

８．監査体制の整備・充実

情報セキュリティに関する法令、規制等および本基本方針、その他社内規程、ルール等への準拠性に対する内部監査を実施できる体制を整備します。

９．外部委託先の管理監督

当社の業務を外部委託する場合には、外部委託先としての適格性を十分に審査し、当社と同等以上のセキュリティレベルを維持するよう要請していきます。また、これらのセキュリティレベルが適切に維持されていることを確認し続けていくために、外部委託先との契約の強化を図り、定期的に外部委託先の見直しを行います。

２０２４年１０月３１日

東京ハッシュ株式会社