情報セキュリティ基本方針

1. 情報セキュリティの目標

当社は、インターネットを活用する暗号資産の特性を踏まえ、利用者の皆様に信頼される取引環境を継続的かつ安定的に提供するため、企業活動のあらゆる面において情報資産の適切な利用・管理を行い、情報セキュリティの確保に力を尽くします。

2. 目標達成のためにとるべき行動

(1) 人的資源のセキュリティ

情報資産に対する最も大きな脅威の一つは役職員によるもので、人的エラー、知識不足、情報資産の処理や保存の場面で配慮すき基本的なステップを（故意または過失により）実施しなかった場合に発生します。当社は、新入社員に対して教育研修を実施するとともに、既存の社員が当方針を遵守すべく支援を行います。

(2) 物理的セキュリティ

当社施設内では適切なセキュリティ管理策を適用し、窃盗や不正アクセスに起因するリスクを低減する必要があります。当社施設への入退管理や、警備員による巡回監視等を行い、建物内外の不審者や不審物に注意することができるよう、防犯責任者は、各拠点・業務組織に応じた防犯組織を整備・統括します。また、特に重要な情報資産を設置したエリアについては常時施錠し、事前に許可された者以外の入室を制限する等の対策を講じます。

(3) アクセス管理

当社は、情報、システムおよびネットワークリソースへのアクセス制御を実施し、故意または過失により情報資産が毀損するリスクを軽減します。アクセス権限は、役職員が業務で必要とする最低限の権限およびアクセス先に限って付与します。

(4) システムの開発・運用

当社は、サービスやシステムの開発段階からセキュリティ対策を組み込むことにより、システムがリスクに晒される事態を最小限に抑えます。これはシステムの安定化やコスト削減にも資すると考えています。また、当社は、サービスやシステムの開発中に生み出された知的財産、独自仕様に関する情報を適切に保持し、管理します。

(5) 法令規制の遵守

当社が提供する業務の運営や保有する情報の取扱いは、複数の規制当局による監督の影響を強く受けるものです。当社が法令、規制または契約上の義務を順守しない場合、罰則を科せられ、また当社に対する信頼性が低下する等により、事業の継続性に重大な影響が及ぶおそれがあります。このため、方針、規程の策定やその運用に当たっては、関連する法令、規制の要求事項に十分配慮します。

3.　情報セキュリティが必要な理由

(1) すべての情報資産は以下の 3 つの特性を持ちます。

① 機密性 (許可されていない者に対して、情報を使用不可または非公開にする特性)

② 完全性（情報の正確さおよび完全さを保護する特性）

③ 可用性 (許可された者が要求したときに、情報へのアクセスおよび使用が可能である特性)

(2) 情報資産は、これに対するさまざまな脅威（故障、災害、誤処理、不正使用、破壊、改ざん、漏えい等) により毀損されるリスクがあり、このリスクを低減するためには、適切な情報セキュリティ管理が必要なのです。

4.　対象範囲とセキュリティの程度

(1) 当社は、情報資産を以下のように適切に分類し、それに応じたセキュリティ対策を実施します。

① 公開情報（公開しても会社に影響を及ぼすことのない情報）

② 社外秘の情報（自社外への公開が禁止される情報）

③ 機密情報（当該情報に含まれる内容と直接関係する業務に従事する担当者以外への開示が禁止される情報）

(2) 機密情報には、個人情報保護法に定める個人情報が含まれます。また、個人情報には、利用者に係る情報と当社従業員に係る情報の双方が含まれます。利用者に係る情報の取扱いにあたっては、利用者保護措置に関する規程を遵守します。

5.　外部委託先における情報資産の安全管理に関する方針

当社は、外部委託先に対しても、情報セキュリティに関連する方針および規程に準拠した契約内容を定め、その遵守を要請します。

6.　情報セキュリティの責任者

当社の情報セキュリティ最高責任者は、システム統括管理責任者であるシステム担当取締役が兼務するものとします。

以上

2022 年 8 月 2 日