サイバーセキュリティ基本方針

倉吉信用金庫は、サイバーセキュリティリスクが金融機関にとって重要な経営課題であると認識し、サイバーセキュリティ基本法（平成 26 年 11 月 12 日 法律第 104 号）、金融庁が定めるサイバーセキュリティ関連ガイドライン、および関連する法令を遵守します。また、顧客情報および情報資産を保護し、高度化・巧妙化するサイバー攻撃から安全を確保するため、継続的なセキュリティ対策の強化に努めます。

１．経営層は、サイバーセキュリティに関する責任を認識し、自らリーダーシップを発揮して、組織体制の構築および運営を行います。リスクベースアプローチに基づき、適切なリソースを確保し、サイバー攻撃から顧客情報および重要な業務を守るための対策を講じます。

２．サイバーセキュリティリスクを継続的に評価し、その結果に基づき優先順位をつけた対策を実施します。重要なインフラおよび顧客情報を含む情報資産の保護を最優先とし、必要な技術的および組織的対策を講じます。

３．サイバー攻撃等のインシデントが発生した場合に、迅速かつ適切に対応するための体制を整備します。業務継続基本計画（BCP）を策定・維持し、定期的に訓練を実施して対応能力の向上に努めます。

４．業務委託先やビジネスパートナーに対してサイバーセキュリティ対策の徹底を求め、委託先のリスク管理体制を継続的に評価します。外部委託先との契約にはセキュリティ条項を明確にし、リスクに応じた監視または監査を行います。

５．平時およびインシデント発生時には、関係機関および監督機関との適切なコミュニケーションを図り、法令に基づく報告や情報共有を行います。また、お客さまや関係者に対して透明性を持って必要な情報を提供します。

６．サイバーセキュリティに関する役職員の意識向上と専門的なスキルの習得を目的とした継続的な教育を行います。さらに、お客さまに対してセキュリティリスクへの理解を促し、適切な対策を取るための情報提供に努めます。

以上