サイバーセキュリティ管理基本方針

第1条　（経営課題としての認識）

当社は、公共的使命を有する銀行として、サイバーセキュリティの強化を経営の重要課題として認識し、サイバーセキュリティ管理体制を整備する。

サイバー攻撃の高度化・巧妙化を踏まえ、サイバーセキュリティリスクを当社の重要なリスクの一つとして位置付け、情報資産の保護やサービス・システムの安定的な運用を確保するため、経営主導によるサイバーセキュリティ対策を推進する。

第2条　（基本原則）

（１）情報資産の保護・システム等の安定運用

情報資産の適切な保護およびサービスやシステムの安定運用のため、最新の技術動向や脅威の進化に対応したサイバーセキュリティ対策を講じる。

（２）リスク管理の徹底

サイバーセキュリティリスクに対する予防措置の強化および早期発見・対応を通じてリスクの最小化を図る。

（３）教育・訓練

役職員のサイバーセキュリティ意識の向上に向けて、研修や啓発活動を継続的に実施する。有事の情報連携、意思決定、対外広報、技術対応を迅速に行えるよう、定期的に演習・訓練を行い、サイバーセキュリティ対策の実効性を確保する。

（４）法令等の遵守

サイバーセキュリティに関連する法令、規則およびガイドラインを遵守し、社会的責任を果たすことでステークホルダーの信頼を確保する。

（５）継続的な改善

本方針に基づく体制整備・実践状況等を定期的に検証し、サイバーセキュリティ管理体制の改善に努める。

第3条　（管理体制）

当社は、サイバーセキュリティを統括する責任者を定め、組織横断的な連携によりサイバーセキュリティリスク管理を徹底するとともに、外部専門機関との連携を通じて実効性向上を図る。

第4条　（サイバーインシデントへの対応）

当社は、サイバーインシデントの早期発見および迅速な対応を可能とする仕組みを構築するとともに、インシデント発生時の影響を最小限に抑えるため、手順・マニュアルの整備や適切な教育・訓練によりインシデント対応力を強化する。

社内人材の育成および外部専門機関との連携により、セキュリティ人材を確保する。

以　上