サイバーセキュリティ基本方針

東京三協信用金庫（以下、当金庫という）は、地域社会の金融インフラとしての責務を果たすため、サイバー攻撃による業務中断、情報漏えい、信頼毀損等のリスクへの対応を重要な経営課題と位置付け、サイバーセキュリティの確保に継続的かつ組織的に取り組みます。

１．経営陣の責務

経営陣は、自らがリーダーシップを発揮し、サイバーセキュリティリスクを把握するとともに、必要となる経営資源を配分し、サイバーセキュリティに関する管理態勢の整備および対策の実施等に努めます。

２．法令等の遵守と管理態勢の整備

当金庫は、サイバーセキュリティに関する法令等および契約上の義務を遵守することはもとより、サイバーセキュリティリスクへの対応に関する役割と責任範囲を明確にし、サイバーセキュリティ管理態勢を構築します。

３．施策の実施

当金庫は、外部および、内部双方のサイバー脅威に対し、被害の可能性と影響度に応じた技術的・組織的対策を適切に講じるため、サイバーセキュリティリスクの動向を踏まえたうえで、必要な施策を実施します。

４．教育の実施

当金庫は、全役職員がサイバーセキュリティの重要性を理解し、適切に行動できるよう、役割に応じた教育と実践的な訓練を継続します。

５．委託先への要請と確認

当金庫は、この基本方針を当金庫が業務を委託する外部組織にも周知し、委託先のサイバーセキュリティ対策に関して、適切な確認を実施します。

６．情報連携

当金庫は、平時およびインシデント発生時において、関係省庁、委託先、業界関連組織等と緊密に連携のうえ、ステークホルダーに対する適切な情報開示に努めます。

７．継続的な改善

当金庫は、事業環境やリスクの変化に対応するため、サイバーセキュリティ管理態勢の継続的改善に努めます。

令和７年９月１日制定