サイバーセキュリティ管理に関する基本方針

桐生信用金庫（以下「当金庫」という。）は、サイバー攻撃による脅威が高まる状況を踏まえ、サービスを安定的かつ適切に提供するため、サイバーセキュリティへの取組みを重要な経営課題と位置づけ、以下の方針に基づきサイバーセキュリティ管理を継続的に実施します。

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．管理態勢の整備

当金庫は、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。具体的には、サイバー攻撃の検知、特定、防御体制を整備するとともに、インシデント発生時の業務継続計画や緊急対応態勢およびサイバー攻撃に備えた業務継続・復旧体制を整備します。

３．対策の実施

当金庫は、サイバーセキュリティリスクを把握したうえで、必要な対策を中期経営計画や単年度の事業計画等に反映し、実施します。

４．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見直しを継続的に実施します。

５．委託先の管理

当金庫は、委託先（サードパーティを含む。）におけるサイバーセキュリティ対策について、適切な管理に努めます。

６．法令等の遵守

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します。

７．人材育成

当金庫は、役職員のサイバーセキュリティに係る意識向上に必要な教育・訓練等の啓発活動に努め、専門的な人材の確保・育成に取組みます。

８．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。

附則

１．2018年　5月31日　制定
２．2018年　6月　1日　施行
３．2026年　11月　2日　改定