サイバーセキュリティ管理に関する基本方針

令和７年10月
三島信用金庫

三島信用金庫（以下「当金庫」という。）は、サイバー攻撃の脅威が増大する現状を踏まえ、お客さまへの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り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、必要な経営資源を適切に配分し、サイバーセキュリティ管理態勢の整備および対策の実施に努めます。

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、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。）の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意識向上のための教育・訓練を行い、専門

的な人材の確保・育成に努めます。

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、業界関連組織と緊密に連携し、ステークホルダーに対する適切な情報開示に努めます。

９．法規制等および関係主体の要求事項への対応

当金庫は、関連する法令、規制、監督指針およびお客さま、取引先、関係省庁等の関係主体からの要求事項に適切に対応します。

以　上