

サイバーセキュリティ管理に関する基本方針

川口信用金庫（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、今般、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、その対応にあたっては、サイバーセキュリティに関する管理態勢を構築し、サイバーセキュリティ基本法およびその他関係諸法令等を遵守のうえ、業界関連組織（全国信用金庫協会、信金中央金庫、しんきん共同センター、しんきん情報システムセンター等）および関係省庁等と緊密に連携しながら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。

また、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るとともに、サイバーセキュリティに関する専門的な人材の確保・育成に取り組めます。

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、当金庫が提供するシステムサービスに必要なサイバーセキュリティに必要な対策を中期経営計画や単年度の事業計画等に盛り込み実施するとともに、事業環境やリスクの変化に対応するための見直しを実施します。

また、整備した管理態勢の有効性や実効性を確認・検証するため、訓練や演習を実施し、サイバーセキュリティリスクの発生・対応状況等を定期的に経営陣に報告します。

4. 委託先の管理

当金庫は、委託先（サードパーティ含む。）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。

5. 関係者との情報連携

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、サイバーセキュリティに関する情報共有および情報開示に努めます。