2025年４月１日

各　位

旭川信用金庫

サイバーセキュリティ基本方針

当金庫は、サイバーセキュリティリスクへの対応を経営上の重要課題の一つとして位置づけ、サイバーセキュリティ基本法（平成26年11月12日法律第104号)、サイバーセキュリティ経営ガイドライン（平成27年12月28日経済産業省策定)、その他サイバーセキュリティに関する関係諸法令等を遵守するとともに、必要な態勢整備に努めます。

１．目的

顧客情報を含む重要な情報資産を保護し、安心で信頼できる金融サービスを提供します。

サイバー攻撃への耐性を高め、業務の継続性を確保します。

２．関係主体への対応および法規制等

平時および緊急時において、関係官庁・関係団体等と緊密に連携のうえ、サイバーセキュリティ対策にかかる情報共有および情報開示に努めます。

関連法規制を遵守し、監督当局の指針に準拠します。

３．経営陣のコミットメント

経営陣はサイバーセキュリティリスクを認識のうえ、自らリーダーシップを発揮し、サイバーセキュリティ対策を推進します。

サイバーセキュリティ確保に向けた組織風土を醸成するとともに必要な経営資源を適切に配分し、継続的な改善に取り組みます。

４．維持すべきサービスと水準

重要な業務を選定したうえで、業務中断後のお客さまへの影響を一定の範囲内に収めるため、最低限維持すべき水準を設定し、サービスを継続的に提供できるよう努めます。

５．リスク管理体制の整備

サイバーセキュリティリスクへの対応を迅速に行うため、CSIRT（Computer Security Incident Response Team）を設置します。

情報収集・分析、監視、インシデント対応等の態勢を構築し、インシデントからの早期回復に向けてBCP（事業継続計画）を策定します。

６．緊急対応体制・復旧計画

インシデント発生時のマニュアルを策定し、訓練を通じて緊急対応・復旧対応の実効性を確保します。

７．委託先の管理

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。また、委託先との契約にあた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化するとともに、履行状況等の継続的な確認を実施します。

８．監査と継続的改善

定期的な監査を実施し、管理態勢の有効性を検証するともに、監査結果や環境変化を踏まえて継続的に改善を図ります。

以　上