サイバーセキュリティ基本方針と取組みについて

2026 年 8 月 3 日
鹿児島興業信用組合

鹿児島興業信用組合（以下「当組合」といいます。）は、地域金融を支える協同組織金融機関として、お客さまからお預かりした情報資産及び金融サービスをサイバー攻撃等の脅威から保護し、安全かつ安定的な金融サービスを提供することが重要な社会的責任であると認識しております。

近年、インターネットやＡＩの普及により各種サービスのデジタル化が進み、サイバー攻撃の手口も高度化・巧妙化しており、金融機関におけるサイバーセキュリティ対策の重要性はますます高まっています。

当組合は、サイバーセキュリティの強化を経営の重要課題の一つとして位置付け、以下の方針に基づき、継続的な安全対策の強化に取り組んでまいります。

１．経営管理態勢の整備

当組合は、サイバーセキュリティリスクに対し、経営陣が主体的に関与するとともに、関係部署が連携した管理態勢を整備し、継続的なリスク管理に取り組みます。

また、サイバーセキュリティに関する内部規程・対応手順等を整備し、適切な運用に努めます。

２．サイバーセキュリティ対策の実施

当組合は、不正アクセス、マルウェア感染、情報漏えい等のリスクに対応するため、以下を含む技術的・組織的安全管理措置を講じます。

- 不正アクセス防止対策
- マルウェア対策
- システム及び機器の脆弱性管理
- ＩＤ・パスワード等の適切な管理
- アクセス権限管理
- 情報資産の適切な管理
- ネットワーク及びシステムの監視
- インターネットバンキング等の安全対策

また、システム環境やサイバー攻撃の動向等を踏まえ、必要な対策の見直し及び改善に努めます。

３．委託先等の管理

当組合は、外部委託先、クラウドサービス提供事業者等について、必要に応じて安全管理状況を確認し、適切なリスク管理に努めます。

４．サイバーインシデントへの対応

当組合は、サイバーインシデント発生時に備え、対応手順及び連絡体制を整備し、被害拡大防止及び迅速な復旧に努めます。

また、必要に応じて関係機関等と連携し、適切な対応を実施します。

５．役職員への教育・訓練

当組合は、役職員に対する教育・訓練を実施し、サイバーセキュリティに関する知識及び意識の向上に努めます。

６．関係機関との連携

当組合は、関係省庁、業界団体、外部専門機関等と連携し、サイバーセキュリティに関する情報収集及び対策強化に努めます。

７．継続的改善

当組合は、サイバー攻撃の高度化・巧妙化等の環境変化に対応するため、サイバーセキュリティ対策について継続的な見直し及び改善に取り組みます。

以　上