サイバーセキュリティ管理基本方針

大阪厚生信用金庫（以下「当金庫」という。）は、サイバーセキュリティリスクを経営上の重要課題として認識し、以下の基本方針に基づきサイバーセキュリティ管理を徹底します。

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体制を構築します。具体的には、サイバー攻撃の特定、防御および検知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体制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人材の確保・育成に取り組みます。

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、年度毎の行動計画等に反映し実施するとともに、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への対応力の向上に努めるとともに、把握した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、委託先のリスク管理態勢を継続的に評価する体制を整えます。

5. 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及び契約上の義務を遵守します。

6. 情報連携

当金庫は、平時及びインシデント発生時において、関係省庁、業界関連組織、委託先等と緊密に連携の上、サイバーセキュリティに関する情報共有及び情報開示に努めます。

2026 年 4 月
大阪厚生信用金庫