サイバーセキュリティ取組方針

２０２１年　2月　1日

伊達信用金庫

伊達信用金庫は、高度化・巧妙化しているサイバー攻撃に対応するため、サイバーセキュリティへの取組みを重要な経営課題として認識し、サイバーセキュリティに関する関係諸法令などを踏まえ、「サイバーセキュリティ取組方針」を制定する。

１．セキュリティ対策の推進

⑴ 管理体制の構築

・　経営者自らがリーダーシップを発揮し、サイバーセキュティリスクを経営の重要課題として認識し、全役職員が一丸となって取組み、継続的な体制整備に努め、サイバーセキュリティ対策の強化を推進する。

・　サイバーセキュリティ対策を行うため、事務管理部門担当役員をサイバーセキュリティ統括責任者とする。

・　サイバーセキュリティ対策を投資の一つと位置付け、積極的にサイバーセキュリティ対策に取り組む。

　また、役職員に対しサイバーセキュリティ教育や人材育成に努める。

⑵ 対象情報システム

「セキュリティポリシー」に定める情報システムのうち、リスク評価の結果から、サイバー攻撃により情報流出や機能停止に陥る可能性のある情報システムを対象とする。対象システムは随時見直す。

⑶ サイバーセキュリティリスクの特定と対策

・　サイバーセキュリティリスクを把握し、適切なリスク認識により必要な対策を講じる。

・　サイバーセキュリティ対策を実施するための体制を構築する。

・　サイバーセキュリティ対策を継続的に実施するため、課題の抽出と改善策の実施によるＰＤＣＡサイクルを構築する。

(4) インシデント発生に備えた体制構築

・　インシデント発生時に影響範囲の特定、被害拡大防止、再発防止策の検討を速やかに実施するための対応体制を整備する。

　また、インシデント発生時の対応訓練として、実践的な演習を実施する。

・　インシデントからの早期回復に向けた実効性のある事業継続計画（ＢＣＰ）を策定する。

２．委託先、提携先等のセキュリティ対策の推進

・　委託先等のサイバーセキュリティ対策状況について、定期的に確認する。

３．情報共有

・　サイバー攻撃に関する情報共有活動へ参加し、積極的な情報提供および情報入手を行う。また、入手した情報を有効活用するための環境整備を行う。

以　上