サイバーセキュリティの取組み

サイバーセキュリティの基本方針

当金庫は、サイバーセキュリティリスクを、事業の継続性および社会的信用に重大な影響を及ぼし得る経営上の重要なリスクの一つと認識しています。サイバーインシデントにより当金庫のお客さまに被害が及ぶリスクや、当金庫の業務ひいては金融システム全体の任務遂行に支障を及ぼすリスク等を最小化することを目的として、サイバーセキュリティ水準の維持・向上を図っています。

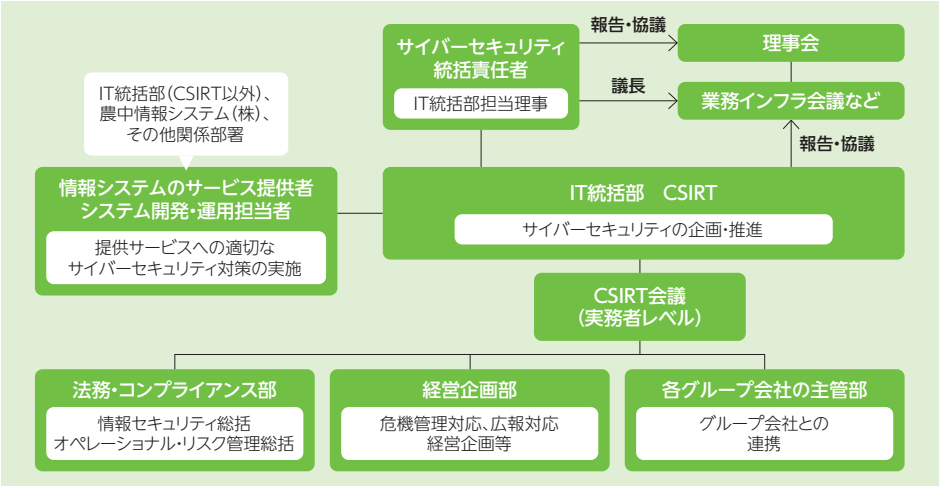
サイバーセキュリティ管理体制

当金庫では、サイバーセキュリティに関する最終的な責任を理事会が有しており、サイバーセキュリティ統括責任者を中心とした体制のもと、IT統括部がサイバーセキュリティに関する基本方針の策定および施策の推進を行っています。また、IT統括部には、サイバーセキュリティインシデントへの対応を目的として、「CSIRT: Computer Security Incident Response Team」を設置し、平時からの備えおよびインシデント発生時の迅速な対応に努めています。

サイバーインシデントの発生状況や脅威動向、サイバーセキュリティ対策の整備状況等については、理事会および理事会のもとに設置された業務インフラ会議等において、定期的に報告・共有※されており、これらの情報を踏まえ、サイバーセキュリティ対策の方針や対応の方向性について議論・意思決定を行っています。

※ 理事会には年2回、業務インフラ会議には年4回以上報告しています。

サイバーセキュリティ体制図



サイバーセキュリティインシデントへの対応

当金庫では、インシデントの兆候を24時間365日体制で監視し、インシデントの検知・分析、被害の封じ込めおよび復旧対応を担うとともに、平時においては脅威動向の把握や脆弱性管理を行い、未然防止に取り組んでいます。インシデント発生時には、影響度等に応じて関係者へエスカレーションし、経営判断のもとで全社的な対応を行う体制としています。また、必要に応じて外部の専門機関等とも連携し、被害の拡大防止および早期復旧を図っています。さらに、サイバーインシデント発生時の対応手順やコンティンジェンシープランを整備するとともに、定期的なインシデント対応演習を通じて、各部門の役割や手順の確認・実効性の向上を図っています。

サイバーセキュリティの管理プロセス

当金庫では、サイバーセキュリティ対策を継続的に実効性のあるものとするため、脅威の把握、リスク評価、対策の実施、運用状況の監視および見直しからなる管理プロセスを構築しています。この管理プロセスのもと、「サイバーセキュリティプログラム」を策定し、攻撃者の手口の変化等の外部脅威や内部の脆弱性を踏まえた必要な施策の検討・実践に取り組んでいます。

2025年度には、当金庫のサイバーセキュリティ対策状況に関する現状認識や外部評価等を踏まえ、本プログラムにおいて2026～2028年度を期間とするサイバーセキュリティにかかる取組計画を策定しました。脅威動向やシステム環境の変化等を踏まえ、サイバーセキュリティリスクの状況や対策の有効性を定期的に評価するとともに、その結果を踏まえた対策の改善・高度化を行っています。

また、こうしたサイバーセキュリティ管理の取組みについては、脆弱性診断やペネトレーションテストの実施のほか、年1回の内部監査および外部監査を通じて、その有効性を検証しています。

サイバーセキュリティに関する教育

当金庫では、全役職員のサイバーセキュリティに対する意識およびリテラシーの向上を目的として、eラーニングや不審メール訓練をはじめとしたサイバーセキュリティに関する教育を継続的に実施しています。教育にあたっては、役割や職責に応じた内容とすることで、各職員が担う業務に即したサイバーセキュリティ対応力の向上を図っています。

- セキュリティに関する基礎知識の習得を目的とした全職員対象のeラーニング
- サイバーセキュリティへの意識向上を目的とした全役職員向けのニュースレター配信
- 全役職員を対象とした、標的型攻撃メールへの耐性や意識の向上を目的とした不審メール訓練
- 役員のサイバーセキュリティに関する知見の向上を目的とした有識者講演会
- CSIRTのフォレンジック技能向上を目的とした、外部有識者による技能トレーニング