サイバーセキュリティ

サイバーセキュリティの取組み

当金庫では、高度化・巧妙化しているサイバー攻撃の脅威について、経営上の重要なリスクのひとつと認識し、サイバーセキュリティ対策の強化に努めています。

サイバーセキュリティの基本方針

当金庫は、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基本規程」においてサイバーセキュリティ管理の基本的な方針を定めています。

サイバーセキュリティ体制

組織体制については、IT統括担当理事を「サイバーセキュリティ統括責任者」とし、サイバーリスクに対する役割や責任を明確化しています。サイバーセキュリティ統括責任者のもと、サイバーセキュリティ担当部署(IT統括部)を中心として、さまざまな施策を推進しています。

サイバーインシデントの発生状況や脅威動向、ならびにサイバーセキュリティ対策の整備状況等については、理事会や業務インフラ協議会、オペレーショナル・リスク管理協議会といった経営レベルの会議において定期的に報告され、サイバーセキュリティ対策の方針について議論されています。

IT統括部にはサイバーセキュリティの専門部署として「CSIRT:Computer Security Incident Response Team」を設置しています。当金庫のCSIRTは、外部のセキュリティベンダーが担う「SOC:Security Operation Center」と緊密に連携しており、サイバーインシデントの兆候となるイベントを24時間365日体制で監視し、サイバーインシデント発生時の初動対応を担っています。また、CSIRTは国や法執行機関、ISAC等各種団体とも連携し、サイバー攻撃の手口や新たな脆弱性に関する情報を収集のうえ、対策の強化に取り組んでいます。

さらに、サイバーレジリエンスの確保のため、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し、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を行っています。

サイバーセキュリティの管理プロセス

当金庫では、公益財団法人金融情報システムセンター(FISC)の「安全対策基準」等を用いて、情報システムの「機密性」・「完全性」・「可用性」についてシステムリスクの評価を行い、必要な管理策を実施しています。

組織横断的なサイバーセキュリティの管理プロセスとしては、NISTの「サイバーセキュリティフレームワーク」に従い、「特定」・「防御」・「検知」・「対応」・「復旧」の切り口で「サイバーセキュリティプログラム」を整理し、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て必要な施策を見直しています。

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、内部監査や外部監査のほか、脆弱性診断やペネトレーションテストを通じて有効性を確認しています。

サイバーセキュリティに関する教育

当金庫では、役職員それぞれに求められる知識や意識の向上のため、目的別に教育を行っています。

- 当金庫役職員のセキュリティに関する基礎知識の習得を目的としたeラーニング
- 当金庫役職員のサイバーセキュリティについての意識向上を目的とした、サイバーセキュリティ関連の記事を紹介するニュースレター
- 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
- サイバーインシデント発生時の対応手順確認を目的とした、役員と関係部署の職員参加のインシデント対応訓練
- 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

また、サイバーセキュリティ専門人材育成のため、外部資格奨励制度等も設け、専門スキルの向上に努めています。