サイバーセキュリティ基本方針と取組みについて

2026 年 4 月 23 日
ゆきぐに信用組合

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・巧妙化しています。特に社会インフラとしての役割を担う金融機関においては、サイバーインシデントの発生を起因として金融システム全体に影響を及ぼす事態も想定されます。こうした状況を踏まえ、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とし、組織全体でサイバーリスクへの対応力を高めるため「サイバーセキュリティ基本方針」を策定致しましたので、下記のとおりお知らせいたします。

記

- サイバーセキュリティへの基本的な考え方
  - 金融機関は、サイバーセキュリティ基本法に基づき、重要社会基盤事業者として国や他の関連主体と連携し、サイバーセキュリティの確保に努める必要があります。当組合は経営陣が主体的にサイバーセキュリティに関与し、日々変化する脅威に対して能動的に対応体制を見直します。また形式的な法令遵守にとどまらず、実質的かつ効果的なリスク管理を行い、組織全体でセキュリティ体制を構築・運営致します。

- サイバーセキュリティガバナンス

1. 経営層の役割
   - サイバーインシデントは金融機関やシステムの信頼に大きな影響を与える重大なリスクであり、これに対応するためには経営陣のリーダーシップと各部門、外部機関との緊密な連携が不可欠です。経営陣は、サイバーセキュリティが経営上の極めて重要な課題であると認識し、情報を収集し知見を深めるほか、自らリーダーシップを発揮し、サイバーセキュリティ対策を推進します。
   - また経営陣はサイバーセキュリティの重要性を踏まえた上で、サイバーセキュリティ対策システムの導入、システム構築に必要な予算の配分、サイバーセキュリティ担当部署への外部人材を含む専門性を有する人材の配置など、適切な資源配分を行います。

2. サイバーセキュリティ対策

◆ 高度化・巧妙化しているサイバー攻撃に適切に対処するため、サイバーセキュリティリスク関連規程類を定め、システムへの不正侵入防止やウイルス検知等の多層的な対策を実施するとともに、その有効性を確保するための見直しを継続的に行います。またサイバーセキュリティリスク管理体制を整備し、リスクの特定、評価、対応計画の策定、管理・コントロール等の各業務部門による自律的な統制活動および、サイバーセキュリティリスクの未然防止やサイバーインシデントへの適切な対応等を行います。

3. サイバーセキュリティ管理態勢

◆ サイバー攻撃から、お客さまの大切なご資産を守り、預金、融資、為替といった金融サービス・業務を維持するため、サイバーセキュリティリスク対応を行う部署やその責任範囲を明確にすることに加え、サイバーセキュリティ統括責任者を設置し当組合におけるサイバーセキュリティ管理態勢を構築します。具体的には、サイバー攻撃の検知、特定、防御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時対応態勢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。サイバー攻撃に備えた業務継続では、当組合内での演習・訓練を行うとともに、必要に応じて外部の共同演習などに参加し、インシデント発生時の対応の実効性向上に取り組みます。

以上