# 福井銀行グループ　サイバーセキュリティリスク管理の基本方針

福井銀行グループは、地域社会の一員として、地域の持続的な発展に貢献するため、「地域産業の育成・発展と地域に暮らす人々の豊かな生活の実現」を企業理念に掲げています。企業理念に基づき、持続可能な地域社会を実現していくため、サイバーセキュリティリスク管理が経営上の重要な課題の一つであると認識し、本方針を定め、お客さまの大切な情報と資産を守り、安全で信頼される金融サービスの提供に努めます。

1. **サイバーセキュリティ対策の目的と方向性**

   福井銀行グループは、高度化・巧妙化するサイバー攻撃を重要な経営リスクと認識し、お客さまに安心してサービスをご利用いただくため、強固なサイバーセキュリティ管理態勢の構築と継続的な改善に取り組みます。

2. **関係主体等への対応および法令遵守**

   福井銀行グループは、お客さま、地域社会、株主、規制当局など全てのステークホルダーの期待に応えるべく、サイバーセキュリティに関する適切な対応と、関連法令および規制の遵守に努めます。

3. **経営陣によるコミットメント**

   福井銀行グループは、サイバーセキュリティリスク管理を経営上の重要課題の一つとして位置付け、経営陣の主体的かつ積極的な関与のもと、強固な管理態勢を構築します。また、必要な経営資源を適切に配分し、福井銀行グループ全体のサイバーセキュリティ対策の継続的な強化に取り組みます。

4. **組織体制および管理態勢の整備**

   福井銀行グループは、サイバー攻撃への迅速かつ効果的な対応を目的として、専門的知識を有する関連部署の横断的な組織「CSIRT」（Computer Security Incident Response Team）を設置します。

   この体制を中心に、情報共有機関等との連携による脅威情報の収集・分析、サイバー攻撃の常時監視、インシデント対応プロセスの整備など、包括的な防御戦略を展開します。これらの取り組みを通じて、福井銀行グループは常に進化するサイバー脅威に対して強固かつ柔軟な防御態勢を維持し、継続的な改善を推進します。

5. **人財育成と組織風土の醸成**

   福井銀行グループは、サイバーセキュリティに関する人財の育成を継続的に行うとともに、全役職員のセキュリティ意識向上を図るため、定期的な教育と訓練を実施し、サイバーセキュリティを重視する組織風土の醸成に取り組みます。

6. **監査**

   福井銀行グループは、サイバーセキュリティリスク管理態勢の有効性および適切性を評価するため、定期的な内部監査を実施します。また、必要に応じて外部専門機関に

よる監査も活用し、客観的かつ専門的な視点からの検証を行います。これらの監査結果を基に、継続的な改善を図り、最適な態勢の維持に努めます。

**7. 情報開示と透明性の確保**

福井銀行グループは、サイバーセキュリティリスク管理に関する取り組みについて、適切な情報開示を行い、透明性の確保に努めます。これにより、福井銀行グループのサイバーセキュリティリスク管理態勢に対するステークホルダーの理解と信頼の向上を図ります。ただし、セキュリティリスクに配慮し、開示する情報の範囲と内容については慎重に判断します。

以上