サイバーセキュリティ基本方針

株式会社山口フィナンシャルグループ（以下「YMFG」）およびグループ会社（注１）は、経団連が「経団連サイバーセキュリティ経営宣言」の中で、経営の重要課題として掲げる「価値創造とリスクマネジメントの両面から主体的にサイバーセキュリティ対策に努めること」の必要性を認識し、「サイバーセキュリティ基本方針」（以下「本方針」）を策定します。本方針のもと、深刻化・巧妙化するサイバー脅威に対し、経営主導によるサイバーセキュリティ対策の強化を推進してまいります。

（注１）本方針の対象となるグループ会社： 株式会社山口銀行、株式会社もみじ銀行、株式会社北九州銀行をはじめとするグループ子会社

１．経営課題としての認識

経営者自らが最新情勢への理解を深めることを怠らず、サイバーセキュリティを投資と位置づけて積極的な経営に取り組みます。また、経営者自らがサイバーセキュリティに関するリスクと向き合い、これらを経営の重要課題として認識し、経営者としてのリーダーシップを発揮しつつ、自らの責任で対策に取り組みます。

お客さまの大切な資産を守ることと金融システムを安定稼働させるために、サイバーリスクを YMFG における重要なリスクの一つとして位置付け、経営主導のもと継続的にその対策を推進します。

２．経営方針の策定と意思表明

特定・防御だけでなく、検知・対応・復旧も重視した上で、経営方針やインシデントからの早期回復に向けた BCP（事業継続計画）の策定を行います。経営者が率先して社内外のステークホルダーに意思表明を行うとともに、認識するリスクとそれに応じた取り組みを各種報告書に自主的に記載するなど開示に努めます。

具体的には、サイバー攻撃に備えて平時・有事の活動を行う部署を設置し、サイバー攻撃に関する情報収集・分析、手続・マニュアル整備を行うとともに、定期的な演習・訓練の実施、コンティンジェンシープランの見直しを実施します。また、統合報告書等を通じてセキュリティ強化の取組みについて開示します。

3．社内外体制の構築・対策の実施

予算・人員等のリソースを十分に確保するとともに、社内体制を整え、人的・技術的・物理的等の必要な対策を講じ、経営・企画管理・技術者・従業員の各層における人財育成や教育を行います。また、取引先や委託先、海外も含めたサプライチェーン対策に努めます。

具体的には、サイバー攻撃のリスクを分析し、継続的なセキュリティ強化を行います。システム共同化行との連携や、外部専門機関への人財派遣等により、外部と連携しながら人財育成を行います。また、経営層やグループ会社を含めた訓練等により、各層における人財育成に取り組みます。

委託先を含めたサイバーセキュリティ対策状況のモニタリング等を通じて、サプライチェーン対策を実施します。

4．対策を講じた製品・システムやサービスの社会への普及

システムやサービスの開発・設計・製造・提供をはじめとするさまざまな事業活動において、サイバーセキュリティ対策に努めます。

具体的には、新たなシステムやサービスの開発時にセキュリティ対策を実施し、お客さまが安心・安全にご利用いただけるサービスの提供に努めます。また、ホームページ等を通じて、お客さまが金融サービスを安全にご利用いただくための対応を呼びかけます。

5．安心・安全なエコシステムの構築への貢献

関係官庁・組織・団体等との連携のもと、積極的な情報提供による情報共有や国内における対話、人的ネットワーク構築を図ります。また、各種情報を踏まえた対策に関して注意喚起することによって、社会全体のサイバーセキュリティ強化に貢献します。

具体的には、金融庁や警察などの関係省庁等と適時適切な連携を行うとともに、金融ＩＳＡＣやシステム共同化行等と情報交換し、社会全体のサイバーセキュリティ対策の強化に努めます。

（2025 年 8 月 28 日制定）