（2025 年 9 月 25 日 制定）

サイバーセキュリティ経営宣言

当行は、サイバーセキュリティ対策を経営の重要課題として認識して、このたび、「サイバーセキュリティ経営宣言」（以下「本宣言」）を策定しました。

本宣言のもと、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より一層推進してまいります。

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、DX を進める上で必須となるサイバーセキュリティを投資と位置付けて積極的な経営に取り組みます。また、経営者自らが現実を直視してデジタル化に伴うリスクと向き合い、サプライチェーン全体を俯瞰したサイバーセキュリティの強化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。

お客さまに安心して金融サービスをご利用いただくとともに、金融インフラの安定稼働と持続的発展に貢献するため、サイバー攻撃を経営上のトップリスクの 1 つと位置付け、経営主導のもと継続的にサイバーセキュリティ態勢強化に取り組みます。

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記載するなど開示に努めます。

サイバーセキュリティに関するリスクに対応するため、リスクの特定、防御、検知、対応、復旧を担当する「CSIRT（Computer Security Incident Response Team）」を設置し、規定の整備、定期的な演習・訓練を通じてインシデント対応の実効性を強化するとともに、コンティンジェンシープランの整備を行います。また、ホームページや統合報告書などを通じてサイバーセキュリティ態勢強化の取り組みの開示に努めます。

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材育成や教育を行います。また、サイバーセキュリティ対策のガイドライン・フレームワークの活用や、政府によるサイバーセキュリティ対策支援活動との連携を通じて取引先や、海外も含めたサプライチェーン対策に努めます。

サイバーセキュリティに精通した人材の育成・確保については、中長期的に取り組むべき重要課題と認識し、外部のセキュリティトレーニングなどを通じて積極的に取り組みます。 経営層も参加する訓練や、業界横断での演習への参加を通じて、社内体制や対策の実効性を向上させます。全役職員のサイバーセキュリティに関するリテラシー向上策として、定期的な研修・訓練の実施や、グループウェア等を活用した情報発信などを行います。

４．対策を講じた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・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。

インターネットバンキング等のサービスを安心・安全にご利用いただくために、最新のセキュリティ対策ソリューションの導入や取引モニタリングなど、さまざまなセキュリティ対策を実施します。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けるよう啓発活動にも努めます。

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、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、外部委託先等全体、ひいては社会全体のサイバーセキュリティに寄与します。

金融庁、国家サイバー統括室、情報処理推進機構、警察などの関係機関と適時適切な連携を行うとともに、金融 ISAC や JPCERT などを通じて情報交換を行い、社会全体のサイバーセキュリティ強化に努めます。

（※）エコシステム：組織や機関、技術、プロセスの相互連携ネットワーク

以上