サイバーセキュリティ経営宣言

商工中金グループは、中小企業専門の金融機関として中小企業組合や中小企業者の未来を支えるため、金融サービスを安全かつ安定的に提供するが社会的責務であると認識しており、主体的にサイバーセキュリティ対策を推進し、安心・安全なサイバー空間の構築に貢献します。

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 を進めるうえで必須となる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。

サイバー攻撃等に関するリスクを商工中金グループの最重要のリスクの１つとして定義のうえ、経営会議・取締役会で定期的に議論・検証し、生成 AI を始めとする DX およびデジタル化とセキュリティ対策の両立を意識して、適切なリソースを配分し、経営主導で継続的にリスク対策を推進します。

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、組織を横断したサイバーセキュリティの対応チームとして CSIRT（Computer Security Incident Response Team）を設置し、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、被害発生の抑止対策を行うとともに、不正アクセスや大量アクセス等に対して多層的な防御対策により不審通信の検知・遮断を行います。加えて、サイバー攻撃に関する分析・検知を行う専門組織である SOC を設置し、24 時間 365 日の監視を行います。

CSIRT では、サイバー攻撃によるインシデントの発生に備え、定期的に経営層も参加した対応訓練を実施しています。

また、統合報告書・ディスクロージャー誌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材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、情報セキュリティの専門組織を設置し一元的に主管させるとともに、主管する役員を明確化し、経営主導による管理体制とします。加えて、専門人材を確保するため、積極的なキャリア採用を進めるとともに、IT 子会社との人財ローテーションや資格奨励制度等による人財育成に努めます。

また、サイバー攻撃による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、取締役会等において定期的に報告のうえ、サイバーセキュリティ対策の方針について議論のうえ必要な予算・人員等のリソースを確保します。

また、FISC 等の国内外のガイドラインやフレームワークを参考にすると共に、政府・関係当局との連携を通じて、クラウドサービス等の委託先や海外も含めたサイバーセキュリティ対策状況のモニタリング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。

例えば、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、ワンタイムパスワード及びスマートフォンアプリを配布するなど、お客さまにおいてご利用可能なセキュリティ対策を充実させるとともに、不正な取引のモニタリングを実施します。新たなシステムやサービスの開発時には安全なセキュリティ対策を実施し、お客さまが使いやすく安心して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、パスワード悪用やウイルス感染への注意等、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、政府機関や監督当局、警察等の関係官庁等に適時適切な報告を行うと共に、金融 ISAC、JPCERT/CC 等のセキュリティに関する情報機関には、積極的に情報提供を行い、社会全体のセキュリティ対策の向上に努めます。