「SBI 新生銀行グループ サイバーセキュリティ経営宣言」

SBI 新生銀行および SBI 新生銀行グループ各社※1は、日本経済団体連合会による「経団連サイバーセキュリティ経営宣言」の趣旨に賛同し、「SBI 新生銀行グループサイバーセキュリティ経営宣言」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、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リスクと向き合い、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・安全な金融サービスをご利用いただき、社会的な責任を遂行するため、サイバー攻撃を経営上の重要なリスクの一つとして位置づけ、経営会議・取締役会等での議論・検証のもと、サイバー攻撃対策を推進します。

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等開示に努めます。

サイバーセキュリティ態勢の構築は、経営の重要課題との認識のもと、グループのセキュリティ戦略を策定し、外部環境や脅威の変化に対応して常に防御態勢の強化に努めます。

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ます。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。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。

サイバーセキュリティの専担組織として「SBI 新生銀行グループ CSIRT※2」をグループ本社内に設置し、必要な予算、人員等を確保して組織的な対応力を強化します。サイバーセキュリティ関連規程の整備、最新の攻撃手口や脆弱性情報の収集、ネットワーク・サーバー・PC へのサイバー攻撃対策の実装と定期的な点検、不正送金のモニタリング、従業員へのセキュリティ訓練、教育を実施します。

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・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。

お客さまに安心・安全な金融サービスをご利用いただき、社会的な責任を遂行するため、システム開発におけるセキュリティチェックを強化します。インターネットを介した取引の運用については、認証方法や不正取引検知等のセキュリティの高度化等に努めます。また、増加するフィッシングへの対策として、フィッシングサイト閉鎖サービスを導入しています。

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、各自の積極的な情報提供による情報共有や国内外における対話、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、内閣サイバーセキュリティセンター、情報処理推進機構、各種捜査機関等の官庁に適時適切な報告を行うと共に、金融 ISAC※3、 FS-ISAC※4、 JPCERT※5 等のセキュリティに関する情報機関との積極的な連携を通して、社会全体のより安心・安全なサイバー環境の実現に貢献します。

※1 本宣言の対象となるグループ会社：アプラス、新生フィナンシャル、昭和リース
※2 Computer Security Incident Response Team
※3 一般社団法人金融 ISAC
※4 Financial Services Information Sharing and Analysis Center の略。1999 年に米国で設立され、5,000 を超える会員組織が情報共有を行う。
※5 一般社団法人 JPCERT コーディネーションセンターの略。コンピュータセキュリティの情報を収集し、インシデント対応の支援、コンピュータセキュリティ関連情報の発信などを行う。

以 上