セキュリティ

情報セキュリティリスクとサイバーセキュリティ対策

当グループは、情報資産は最も重要な経営資源の1つという認識のもと、個人情報・顧客データ保護をマテリアリティテーマの1つに設定するほか、情報セキュリティリスクを「情報の漏えい、情報が正確でないこと、情報システムが利用できないこと、情報の不正使用など、情報資産が適切に維持・管理されないことにより、当グループが損失を被るリスク」と定め、オペレーショナル・リスク内のリスクサブカテゴリーの1つに位置付けて、統括役員および管理部署を設置し、顧客情報の適切な管理やサイバーセキュリティ対策を行っています。

また、お客さまや株主の個人情報などの保護に万全を期するための取り組み方針を「個人情報保護宣言」として定め、公表し、これを遵守することを宣言しています。

管理体制や情報の取り扱い等について、個人情報保護法、関連法令および金融庁が定める「金融分野における個人情報保護に関するガイドライン」などに則り、社内規程類を整備するとともに、年2回定期的に全社員向け研修を実施するなど、日常業務における各種情報の取り扱いに関する留意事項の周知に加え、情報セキュリティに関するプリンシプルベースでの理解浸透を図っています。

(1) 組織体制など

情報セキュリティリスクに関する事項は、オペレーショナル・リスク内のリスクサブカテゴリーとして、当社ではリスク管理委員会において、三井住友信託銀行ではオペレーショナル・リスク管理委員会において、管理体制の整備、計画の策定およびリスクの特定・評価・モニタリング・コントロールといった一連のプロセスなどを総合的に審議しています。また、方針や計画については経営会議での審議を経て取締役会が決定しています。

一連のプロセスについては権限規程などに基づき情報セキュリティリスクの管理部署である業務管理部およびIT統括部をはじめとする各部署等において実行しています。これら管理体制全般について、業務管理部統括役員およびIT統括部統括役員が情報セキュリティリスク管理全般の統括役員として統括する体制としています。

(2) サイバーセキュリティ管理体制

当グループは、サイバー攻撃対応をマテリアリティテーマの1つに設定するほかトップリスクに選定しており、「サイバーセキュリティ経営宣言」を策定の上、経営主導によるサイバーセキュリティ対策の企画・推進を行っています。

- サイバーセキュリティ対策の専門組織としてSuMiTRUST-CSIRT[※1]を設置し、グループ内外から脅威情報や脆弱性情報を収集・分析、セキュリティ対策を企画・導入し、経営へ報告する管理体制を構築しています。またセキュリティ対策の検討会やIT審議会を通じて、外部知見も活用の上、高度化を進めています。
- 米国のセキュリティ基準に基づく社内規程類を制定し、サイバー攻撃に対する平時、有事の対応プロセスを整備しています。
- 関係会社を含む当グループにおいて、サイバーセキュリティリスクアセスメントやシステム脆弱性診断を定期的に実施するほか、サイバーセキュリティ関連規程類の共通化を進め、グループ全体のサイバーセキュリティ体制の高度化・標準化を推進しています。

(3) 監視体制

当グループはインターネット通信のグループ共通基盤を構築しており、共通基盤ネットワークにおいてSOC（Security Operation Center）による24時間365日監視や各種データの相関分析による脅威検知を行っています。これらはSuMiTRUST-CSIRTに情報集約しており、CSIRTを中心とした監視体制を構築しています。

(4) サイバーセキュリティ対策高度化

サイバー攻撃への技術的な対策として、境界型防御策（入口対策、出口対策、内部対策の多層防御）を構築しており、DDoS攻撃対策やフィッシングサイトの検知・遮断等の各種対策によりリスク低減を図っています。

(5) セキュリティ人材の育成

サイバーセキュリティの高度な専門知識を有する人材を育成するため、CSIRTでは社内検討会における社外専門家との協業、金融ISAC[※2]、FS-ISAC[※3]等の社外コミュニティへの参加、社外研修や資格取得支援、大学院への社員派遣などを行っています。

※1 CSIRT（Computer Security Incident Response Team）：
攻撃予兆情報の収集・分析・対応策を進める社内組織
※2 金融ISAC（Information Sharing and Analysis Center）：
国内金融機関の情報共有組織
※3 FS-ISAC（Financial Services Information Sharing and Analysis Center）：
米国を中心とする金融機関の情報共有組織