セキュリティ

Message

ITリスク統制部統括役員（CISO）メッセージ

三井住友トラストグループ
執行役常務（CISO）
上田 純也

情報セキュリティリスクおよびシステムリスクの管理は、情報（Information）と技術（Technology）による事業価値創造を支える重要な基盤です。近年、AIを悪用したサイバー攻撃やサプライチェーン攻撃、地政学的リスクを背景とする攻撃など、外部脅威は中長期的に高度化・複雑化することが想定されています。加えて、サイバー領域は経済安全保障の観点からも戦略的重要性を一層高めています。こうした環境変化を踏まえ、当グループは、グループ・グローバルー体となってセキュリティ態勢の強化に取り組んでいます。重要インフラ事業者である金融機関として、お客さまの大切な資産を守ることは当グループの重要な責務であるとの認識のもと、安心・安全な金融サービスを利用いただけるよう、努めてまいります。

Topics

高度化・複雑化する脅威への取り組み

当グループでは、IT関連リスクの統制機能として2025年に新設したITリスク統制部を中心に、体制・要員を強化し、高度化・複雑化するサイバー攻撃等への対応力向上を推進しています。

同部に設置されたCSIRT※1がグループ内外の情報を収集・分析し、サイバーセキュリティ対策を企画・推進しています。年4回以上の取締役会等への取り組み状況報告や役員向け勉強会を通じて、環境変化に対応可能なガバナンス態勢を構築しています。

CSIRTは、DDoS攻撃や脆弱性を突く攻撃、フィッシングサイトの検知・遮断等の対策について、多層防御の構築・強化をプロアクティブ（予防的）に実施しています。あわせて、外部専門家を活用した疑似攻撃演習の実施、JC3※2・金融ISAC※3・FS-ISAC※4等のセキュリティコミュニティへの参画、役員・社員への教育・啓発を通じて、リアクティブ（対応的）にインシデント発生時の対応力向上を図っています。

※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 JC3（Japan Cybercrime Control Center）：サイバー脅威に関する情報共有・分析等をする産学官連携の非営利団体
※3 金融ISAC（Information Sharing and Analysis Center）：国内金融機関の情報共有組織
※4 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

01 情報セキュリティリスク

基本方針およびリスク管理体制

当グループは、情報資産を最も重要な経営資源の一つと認識し、個人情報・顧客データの保護に取り組んでいます。また、情報セキュリティリスクの統括役員・管理部署を設置し、情報の適切な管理を行っています。

また、個人情報の保護にかかる取組方針を「個人情報保護宣言」として公表し、遵守することを宣言しています。

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」等に則り、社内規程を整備し、定期的に全社員向け研修を実施するなど、日常業務での情報の取り扱いの留意事項を周知し、プリンシプルベースでの理解浸透を図っています。

管理態勢の整備、計画の策定およびリスクの特定・評価・モニタリング・コントロールなどの一連のプロセス等はCRO Committeeで総合的に協議し、方針や計画は経営会議での審議を経て取締役会が決定、一連のプロセスは権限規程等に基づき業務管理部、ITリスク統制部等が実行しています。

02 システムリスク

❶ 基本方針およびリスク管理体制

当グループは、システム障害が業務継続やサービス提供へ影響を及ぼし得ることを踏まえ、情報システムの安定性・信頼性の確保を経営上の重要事項の一つと位置付けています。障害の発生を完全に排除することが難しいとの前提に立ち、影響の最小化と早期復旧を重視したシステムリスク管理に取り組んでいます。

経営層の関与のもと、グループ横断の連絡・対応体制を整備し、障害発生時の役割分担や意思決定プロセスを明確化しています。平時から関係部門が連携し、継続的な見直しと改善を行っています。

❷ 取り組み等

大規模障害等に備え、重要システムに対するバックアップや代替手段の整備、関係部門が連携した教育・訓練を継続的に実施し、非常時に実効性ある対応が可能となるよう、業務継続性の確保に努めています。

03 サイバーセキュリティ対策

❶ 基本方針およびリスク管理体制

当グループは、サイバー攻撃に関するリスクをトップリスクに位置付け、「サイバーセキュリティ経営宣言」のもと、経営主導で対策を推進しています。

金融庁が定める「金融分野におけるサイバーセキュリティに関するガイドライン」やCyber Risk Institute Profile等を踏まえて、規程や対策基準を定め、また、第三者評価を含むアセスメントを通じてリスク管理態勢の実効性確保に努めるとともに、グループ・グローバル全体で態勢強化を図っています。さらに、脆弱性診断や適時のTLPT※5により、システムの安全性・堅牢性を検証しています。

重要な委託先やクラウド事業者を含むサードパーティリスクを重要な経営課題と捉え、契約締結前後を通じたセキュリティ管理態勢の確認・モニタリングを行い、サプライチェーン全体でのサイバーセキュリティリスク低減に取り組んでいます。

※5 TLPT（Threat-led Penetration Testing）：脅威ベースのペネトレーションテスト

❷ 取り組み等

当グループは、ISO27001認証取得のグループ基盤にて、Security Operation Centerによる24時間365日監視や脅威検知を行っています。これらの情報を集約しているCSIRTを中心とした監視体制を構築しています。また、入口・出口・内部対策による多層防御を構築するとともに、攻撃者動向の収集・分析等インテリジェンス機能の強化を進めています。

CSIRTでは、高度な専門人材育成のため資格取得支援等を行っています。取締役向けの勉強会や訓練、役員・社員向けの情報セキュリティ研修やフィッシングメール訓練、外部機関と連携したサイバー演習等を通じて、インシデント発生時の検知・初動対応・復旧に至る一連の対応力を高め、組織全体のサイバーレジリエンス強化を図っています。

● サイバーセキュリティ管理態勢