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
執行役専務兼執行役員（CISO）
米山 学朋

国の重要インフラ事業者である金融機関として最も重要視しているのは、個人情報をはじめとする多彩・多様なお客さまの情報を安全に保つことです。近年のサイバー脅威の技術進展や地政学的緊張等により環境は急速に変化しています。またグループ関係会社や重要な取引先等のサプライチェーンを狙った攻撃も増えています。

サイバーセキュリティの脅威は従来信頼していた境界型防御の内側にも潜在・複雑化しているため、「何も信頼しない」ことを前提に、全てのアクセスを検証するゼロトラストな対策が求められます。

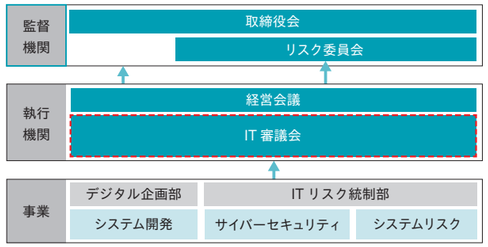
当グループは技術的対策のみでなく、組織的・人的な対応としてCISO、サイバー対策の専門組織CSIRT※1を設置して、サイバー態勢を継続的に強化し、お客さまに安心・信頼して我々のサービスを活用いただけるよう取り組んでいます。

Topics　～複雑化するサイバー攻撃等への対応力の高度化～

当グループは、CSIRTがグループ内外から情報を収集・分析のうえ、各種対策の企画・導入を行い、経営へ報告する管理態勢を構築しています。

DDoS攻撃対策、脆弱性を突く攻撃への対策およびフィッシングサイトの検知・遮断等の多層防御の構築・強化を継続的にプロアクティブ（予防的）に実施し、インシデント発生に備えた対応として外部専門家を活用した疑似攻撃演習や金融ISAC※2・FS-ISAC※3・JC3※4等のセキュリティコミュニティ活動の強化等をリアクティブ（対応的）に実施しています。

2025年4月にIT関連リスク統制機能を担うITリスク統制部を新設し、体制・要員の増強、複雑化するサイバー攻撃等への対応力の高度化を推進しています。



1. 情報セキュリティリスク

基本的な取り組み方針およびリスク管理体制

当グループは、情報資産は最も重要な経営資源の一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一つに設定しています。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。

管理態勢等について、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、社内規程類を整備し、定期的に全社員向け研修を実施する等、日常業務での情報の取り扱いに関する留意事項を周知し、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リスク管理委員会で総合的に審議し、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。これら管理態勢全般は、業務管理部統括役員およびITリスク統制部統括役員が統括しています。

2. サイバーセキュリティ対策

①基本的な取り組み方針および体制

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一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。

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、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の定期的な実施、関連規程類のグループ内共通化など、態勢の高度化・標準化を推進しています。

IT審議会

IT審議会は、議長であるCISOをはじめとした経営管理各部の統括役員、部長、および専門知識を有する外部委員をもって構成され、重要なシステム投資、システム技術に係る事項に関し、多面的な視野から審議を行う経営会議の諮問機関です。リスク管理面においては、システム開発に起因するリスク、サイバーセキュリティおよびシステムリスク等について、本審議会にて審議しています。

サイバーセキュリティ経営宣言
https://www.smtg.jp/-/media/tg/about_us/management/risk/pdf/CSMD.pdf

②サイバーセキュリティ

(1) 監視態勢

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。

(2) 技術的な対策

サイバー攻撃への技術的な対策として、入口対策、出口対策、内部対策の多層防御を構築し、また攻撃者の動向等に関する情報の収集・分析や、当グループの脆弱性管理を高度化するインテリジェンス機能の向上に努めています。

■主な対策
- 悪意のある通信の検知、遮断
- ウイルスやマルウェアの侵入を阻止
- 振る舞い検知による不審な通信の規制
- 脆弱性診断によるインターネット経路の脆弱性の評価・改善
- エンドポイントに侵入したマルウェアの挙動を検知
- ファイアーウォールやプロキシサーバーなどから取得する複数の通信ログを統合的に分析し検知精度を向上
- 暗号化通信を復号化のうえ、分析し検知範囲を拡大

(3) 人材育成

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、社外コミュニティへの参加、社外研修や資格取得支援などを行っています。また、三井住友信託銀行では、全社員を対象とした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を通じて、社員教育にも継続的に取り組んでいます。

③システムリスク

大規模障害や災害による情報システムへの影響極小化、早期復旧ならびに業務継続へ備えるため、グループの連絡・対応体制を明確化し、代替措置・復旧手順などを整備するとともにオペレーションの教育・訓練などを行い、レジリエンス強化に努めています。また、一定規模のシステム開発に起因する遅延・費用増加等に関わるリスクに対しては、大型システム開発案件の進捗管理・品質管理面のモニタリングを行い、IT審議会へ報告・協議する体制となっており、システム開発の適正運営に努めています。

※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
※4 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