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）

1 情報セキュリティリスク

1. 情報セキュリティリスク管理態勢

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、情報の不正使用等、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、お客さまや株主の皆さまの個人情報などの保護に万全を期するための取組方針を「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。

管理態勢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」等に則り、社内規程類を整備するとともに、三井住友信託銀行では、年2回定期的に全社員向け研修を実施する等を通じて、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。

■ 情報セキュリティリスク管理に関連する規程類

規程	個人情報保護宣言に関する規程、リスク管理規程
規則	リスク管理規則、オペレーショナル・リスク管理規則、情報セキュリティリスク管理規則、システムリスク管理規則
要領	情報セキュリティリスク管理要領、システムリスク管理要領、個人情報取扱要領、個人データ管理事務取扱要領、CSIRT運営要領、社内OA管理取扱要領、顧客情報の社外持出に係る事務取扱要領、等

2. 組織体系等

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、三井住友トラスト・ホールディングス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・コントロールといった一連のプロセス等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等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。これら管理態勢全般について、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態勢としています。

組織体制	取締役会、経営会議、リスク管理委員会（三井住友トラスト・ホールディングス） オペレーショナル・リスク管理委員会（三井住友信託銀行）
統括役員	業務管理部統括役員およびIT統括部統括役員
管理部署	業務管理部およびIT統括部

2 サイバーセキュリティ対策

1. サイバーセキュリティ管理態勢

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。

・CISO（Chief Information Security Officer）を設置して、CISOのリーダーシップのもとサイバーセキュリティ対策の強化等を推進していきます。
・サイバーセキュリティ対策の専門組織としてSuMiTRUST-CSIRT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態勢を構築しています。

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。

・米国のサイバー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態勢の高度化・標準化を推進しています。

2. 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※1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。

※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

3. 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、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、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・遮断等の各種対策によりリスク低減を図っています。

さらにお客さまに安心してインターネットバンキングサービスをご利用いただくため、フィッシング対策として振込上限金額の設定や脅威動向の情報収集を強化するとともに、技術的な対策として不正取引のモニタリングの強化に取り組んでいます。

また攻撃者の動向等に関する情報の収集・分析や、当社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。

■ 技術的な主な対策

入口対策 出口対策	・悪意のある通信の検知、遮断（含むDDoS攻撃対策） ・ウイルスやマルウェア（不審なアプリ）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
内部対策	・エンドポイント（社内OA端末やサーバー）に侵入したマルウェアの挙動を検知
統合監視	・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（HTTPS等）を複合化の上分析し検知範囲を拡大

また、サイバーセキュリティヒートマップを用いたリスク状況の自己分析、FFIEC-CAT※2など国際的なサイバーセキュリティアセスメントツールを用いた第三者評価を定期的に実施するほか、金融ISAC※3や内閣サイバーセキュリティセンターが主催するサイバー演習への参加や当社独自に経営層やグループ関係会社向けの演習を実施することで、サイバーレジリエンス強化に向けPDCAサイクルによる対策高度化を進めています。さらに、サイバー保険による万が一への備えも行っています。

※2 FFIEC-CAT：FFIEC（米連邦金融機関検査協議会）が金融機関向けに公表したリスク評価ツール（Cyber Assessment Tool）
※3 金融ISAC：Information Sharing and Analysis Center：国内金融機関の情報共有組織

4. サイバー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、FS-ISAC※4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。

加えてCSIRTとアプリケーションやインフラの開発部署がタスクフォースと呼ばれる組織を組成することで、サイバーセキュリティ対策に関する各課題の協議・調整による実効性向上、専門性相互補完と人材プール化に取り組んでいます。

※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

5. システムリスク管理態勢

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。

6. IT審議会

IT審議会は、議長であるIT統括部統括役員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おり、諮問機関として社外の専門家である外部委員の知見を積極的に活用し、議論の充実化、管理高度化に取り組んでいます。