サイバーセキュリティ

基本的な考え方

デジタル化が加速し、金融サービスを取り巻く環境が変化する中、サイバー脅威はますます深刻化しています。SMBCグループでは、お客さまへのより安全・安心なサービスの提供と、サイバー脅威に強い社会の実現を目指し、サイバーセキュリティのさらなる強化を推進していきます。

サイバーセキュリティ管理体制

● 管理体制の構築

当社では、サイバーセキュリティリスクを、経営上のトップリスクのひとつとして掲げており、「サイバーセキュリティ経営宣言」の下、経営主導でサイバーセキュリティに対する取組を継続的に推進しています。

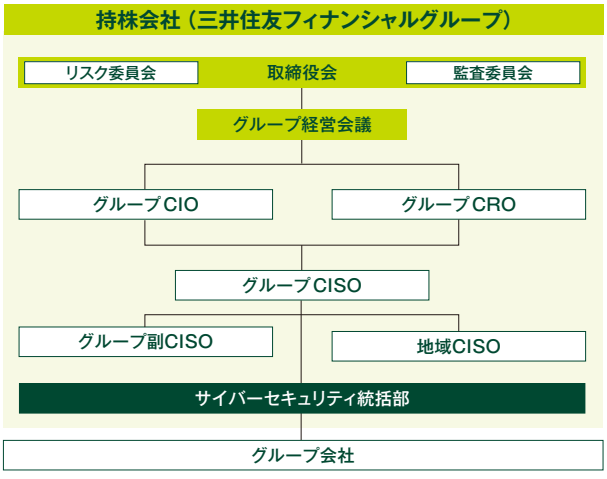
サイバーセキュリティリスクは、全社的なリスク管理の枠組の中で管理しており、サイバーセキュリティの専担部署であるサイバーセキュリティ統括部が中心となり、外部環境や経営戦略等を踏まえ、サイバーセキュリティ管理に関する基本方針を策定しています。

グループ経営会議では、基本方針に基づいて、さらなる体制強化に向けてサイバーセキュリティ管理について定期的に議論しています。加えて、取締役会およびリスク委員会や監査委員会等の内部委員会においても、定期的にサイバーセキュリティ管理について議論しており、取締役による監督を行っています。

実効性を持ったセキュリティ対策の推進を担う役割を明確化するため、当社では、グループCIO・CROの配下に、グループCISO*1という専門的な責任者を設置しています。グループCISOは、サイバーセキュリティ統括責任者として、グループ・グローバルでの体制整備や各所の施策推進の監督・指導を担っています。加えて、グループCISOの配下には、グループ副CISOおよび地域CISOを設置しており、グループCISOのリーダーシップの下、グループ・グローバルベースで600名以上*2のサイバーセキュリティ管理体制を確立しています。

*1 Chief Information Security Officer
*2 2024年3月末時点

SMBCグループのサイバーセキュリティ管理体制



● サイバーセキュリティリスクの特定

当社のサイバーセキュリティに関する体制評価等を通じて、サイバー脅威の特定を行っています。

具体的には、国際的な基準に基づき、定期的に第三者によるセキュリティ対策の成熟度評価を実施しています。

また、脅威インテリジェンスを積極的に活用し、最新のサイバー脅威にも対応しています。攻撃者の動向、脆弱性に関する情報、地政学情報等を収集・評価し、当社のサイバーセキュリティに関する環境に当てはめ、防御や検知等に役立てています。

加えて、脆弱性を悪用した攻撃による被害を抑止するために定期的に脆弱性診断を実施し、さらに、第三者が実際にシステムに侵入してセキュリティ対策状況を評価する、脅威ベースのペネトレーションテストを実施しています。内外環境を踏まえて、当社にかかわるサイバー脅威を特定し、セキュリティ対策のさらなる強化に努めています。

● サイバーセキュリティリスクの防御および検知

不正アクセスや大量アクセス等、さまざまなサイバー攻撃に備えるため、各種セキュリティ対策サービス・システムの運用により、外部からの不審な通信を検知・遮断し、多層的な防御体制を敷いています。

また、ネットワークの監視および分析を行う専門組織であるSOC*3を設置しており、24時間365日の監視体制を確立しています。引き続き、欧米やアジア地域に設置されたSOCとも密に連携することで、グループ・グローバルベースでセキュリティ監視をより一層強化します。

*3 Security Operation Center

● サイバーセキュリティリスクの対応および復旧

当社では、万が一のサイバーインシデント発生に備え、CSIRT*4を設置しています。また、国内のセキュリティ機能および人材を集約したサイバーフュージョンセンター（CFC）を設置することで、管理体制の効率化を図り、迅速なインシデント対応が可能な環境を整備しています。

サイバーインシデント発生に備え、CSIRTは、攻撃者の手口や脆弱性に関する情報等をグループ内外から積極的に収集し、各国当局や米国のFS-ISAC*5、日本の金融ISAC等の外部機関とも必要に応じて共有しています。

また、万が一の攻撃に備えた対応として、外部の専門家による擬似攻撃演習や、金融庁・金融ISAC等が主催するサイバー攻撃対応演習への定期的な参加等を通じ、サイバーレジリエンスのより一層の強化にも取り組んでいます。

*4 Computer Security Incident Response Team
*5 Financial Service Information Sharing and Analysis Center

サイバーセキュリティに関する啓発活動および専門人材

● 啓発活動

当社では、セキュリティ対策に対して意識的に取り組むことができるカルチャーを醸成するため、役割と責任に応じた啓発活動を実施しています。

経営陣に対しては、サイバーセキュリティにおける経営上の留意事項等に関する勉強会を定期的に実施しています。

また役職員に対しては、標的型攻撃メール訓練等を通じてセキュリティ意識を高めるとともに、システム企画者向けの研修等を通じてセキュリティ・バイ・デザインの理念を浸透させています。

● 専門人材

中長期的なサイバーセキュリティ管理体制の維持に向けて、専門人材の育成を重要課題と認識しており、内外のコンテンツの活用や資格取得支援の制度導入、国内外の大学院への派遣、外部業界団体への参画等を通じて、中核を担う人材の育成に注力しています。

また、キャリア採用等の専門人材の確保に努めるとともに、新卒採用ではサイバーセキュリティコースを設置し、継続的な体制の強化を図っています。