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て、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

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、「サイバーセキュリティ経営宣言」の下、経営主導の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、専任部署であるサイバーセキュリティ統括部が中心となって、外部環境や経営戦略等を踏まえながら、基本方針を策定しています。

グループ経営会議でも定期的に議論しているほか、取締役会やリスク委員会、監査委員会等の内部委員会においても議論を行うことで監督を実施しています。

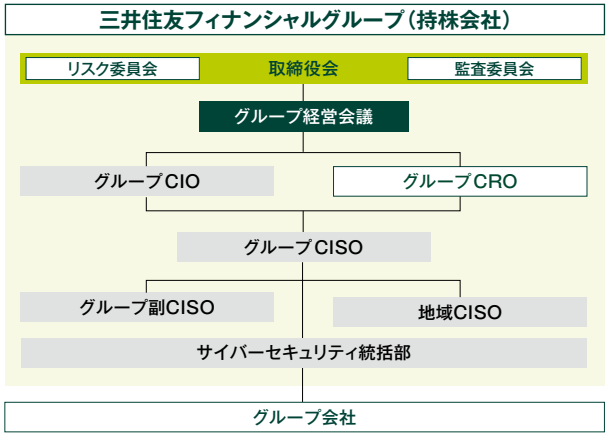
実効性のあるサイバーセキュリティ対策を推進する役割の明確化のため、当社では、グループCIO・CROの下に、グループCISOを設置しています。グループCISOは、サイバーセキュリティ統括責任者として専門的な見地から、グループおよびグローバルでの体制整備や各所の施策推進における監督・指導を担っています。さらに、グループCISOの下には、地域CISOおよびグループ副CISOを設置しており、グループCISOのリーダーシップの下、850名以上[*1]の専門スタッフによるサイバーセキュリティ管理体制を確立しています。

*1 2026年3月末時点

サイバーインシデント発生に備えた体制

万が一のサイバーインシデント発生に備え、CSIRT[*2]を設置しています。CSIRTは、攻撃者の手口や脆弱性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[*3]、日本の金融ISAC等の外部機関とも連携しています。また、セキュリティ監視および分析を行う専門組織であるSOC[*4]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。さらに、欧米やアジア地域に設置した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。

SMBCグループのサイバーセキュリティ管理体制



*2 Computer Security Incident Response Team
*3 Financial Services - Information Sharing and Analysis Center
*4 Security Operation Center

サイバーセキュリティの詳細は、当社Webサイトをご参照ください。
https://www.smfg.co.jp/company/organization/cybersecurity.html

新たな脅威に備えて

高性能AIを脅威と捉え、急激な状況変化に即応するための専門チームを立ち上げました。綿密な情報収集や実態把握のうえで課題を見極め、必要な対策を迅速に実施していきます。

2025年度の取組

グループ共通の管理基準を整備し、全社的なガバナンス強化を推進しました。脅威の動向に応じ、外部からの攻撃への防御に加え、内部に脅威が存在する前提の防御も強化し、新技術の利活用とセキュリティの両立に取り組みました。