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、サイバー脅威のリスクはますます深刻化しています。SMBCグループではサイバー脅威に強い社会の実現と、お客さまへのより安全・安心なサービスの提供を目指し、セキュリティ対策の強化をより一層推進していきます。

サイバーセキュリティ管理体制

ガバナンス体制

サイバー脅威を経営上重要なリスクのひとつとして定義し、「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。

また実効性を持ったセキュリティ対策の推進を担う役割・責任を明確化するため、グループCIO・CROの配下に「CISO*1」という専門的な責任者を配置し、システムセキュリティ統括部長がその責任を担っています。CISOは、経営会議等における議論を通じて経営と一体でサイバーセキュリティ戦略を推進しています。CISOのリーダーシップの下で、高まるサイバー脅威に応じた対応体制を、グループ・グローバルベースで構築しています。

*1 Chief Information Security Officer

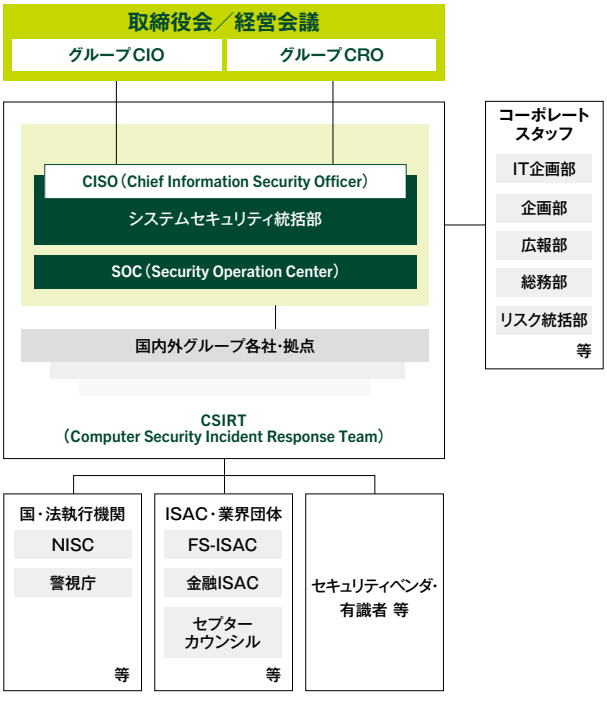
インシデントレスポンス体制

SMBCグループでは、CSIRT*2・SOC*3を設置し、インシデント発生に備え、レスポンス体制を整備しています。

CSIRTはサイバーセキュリティを専担とするシステムセキュリティ統括部が中心となって構成する組織で、サイバーインシデント発生に備え、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*4、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。

SOCは日本総合研究所を中心に組織し、24時間365日の監視体制を整備しており、欧米・アジア地域に設置しているSOCとも連携しながら、グループ・グローバルベースでセキュリティ監視のより一層の強化に努めています。

SMBCグループのサイバーセキュリティ経営体制



また、サイバーフュージョンセンター（CFC）に国内のセキュリティ機能を集約し、CSIRTとSOCの常時緊密な連携を実現しています。

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

サイバーセキュリティに関する主な取組

サイバーセキュリティ対策

不正アクセス・大量アクセス等、さまざまなサイバー攻撃に備えるため、外部からの不審な通信の検知・遮断を実施しているほか、各種セキュリティ対策サービス・システムの運用や監視等、多層的な防御体制を敷いています。

また攻撃者の最新の手口や動向等に関する情報の収集・分析を実施するインテリジェンス機能の成熟度のさらなる向上に努めています。

さらに万一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。

セキュリティ啓発および専門人材育成

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、メール訓練や勉強会等を通じて、継続的に啓発活動を実施しています。

また専門人材については、キャリア採用を積極的に進めるとともに、新卒採用ではサイバーセキュリティコースを新設しました。加えて、外部業界団体へのさらなる参画、国内外の大学院への派遣、専門資格の取得・維持等の支援を通じて、中核を担う人材の育成にも注力していきます。