# サイバーセキュリティ

## 基本的な考え方

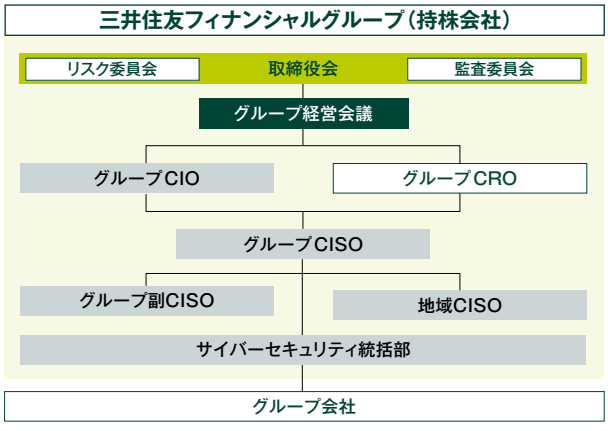
**デジタル化が加速し、金融サービスを取り巻く環境が変化する中、サイバー脅威はますます深刻化しています。SMBCグループではお客さまへのより安全・安心なサービスの提供と、サイバー脅威に強い社会の実現を目指して、サイバーセキュリティのさらなる強化を推進していきます。**

### 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、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、基本方針に基づき、サイバーセキュリティ管理のさらなる強化に向けて定期的に議論しています。また、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、定期的にサイバーセキュリティ管理について議論を行い、取締役会による監督を実施しています。

#### SMBCグループのサイバーセキュリティ管理体制




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*1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、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700名以上*2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 Chief Information Security Officer
*2 2025年3月末時点

### サイバーインシデント発生に備えた体制

当社では、万が一のサイバーインシデント発生に備え、CSIRT*3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*4、日本の金融ISAC等の外部機関とも連携しています。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*5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。

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