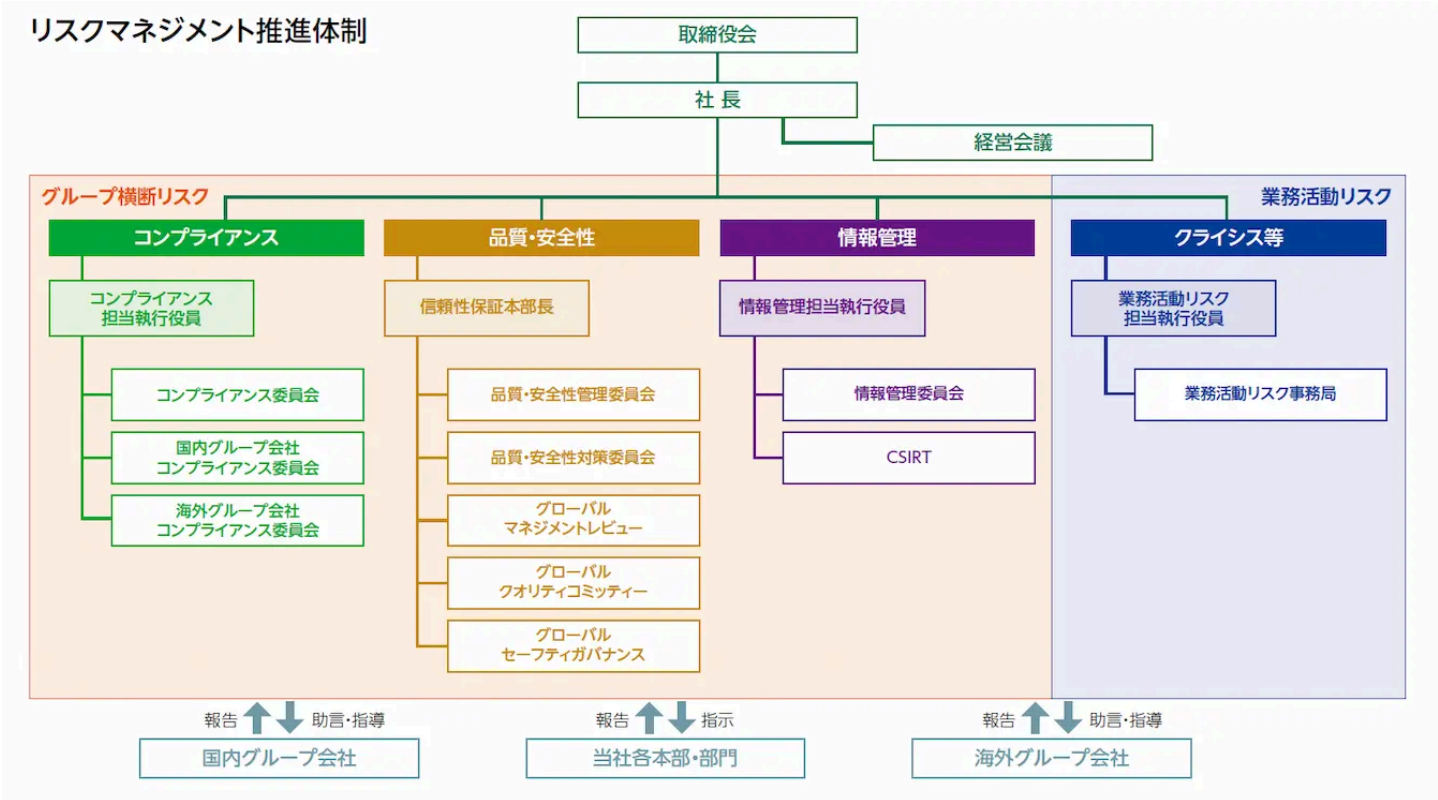
Sumitomo Pharma
Innovation today, healthier tomorrows

Risk Management

リスクマネジメント | 2023年度 アーカイブ

リスクマネジメント

当社グループとしてのリスクマネジメントに関する基本的な考え方を定めた「SMP Group Risk Management Policy」を制定し、当社が当社グループのリスクマネジメントを適切に推進する体制を構築しています。この推進体制では、リスクごとの特性に応じて、グループ横断的に取り組むリスク（グループ横断リスク）とグループ各社が自らの責任において取り組むリスク（業務活動リスク）に分類しています。それぞれのリスクについて、当社がグループ各社から報告を受けることによって、グループ全体のリスクマネジメントを当社が把握し、必要に応じて、助言・指導等の対応を行っています。
当社では、事業活動に影響を及ぼすリスクに対応するため「リスクマネジメント規則」を制定し、社長がリスクマネジメントを統括することを明確にするとともに、特性に応じて分類されたリスクごとにリスクマネジメントを推進する体制を整備しています。各推進体制の運用状況については、定期的に取締役会に報告しています。具体的な取組の一つとして、年度ごとにグループ全体のリスクアセスメントを実施し、その結果を踏まえた対策の策定・実施・評価を行い、全社各部門がそれぞれの課題解決に向け計画的に取り組んでいます。



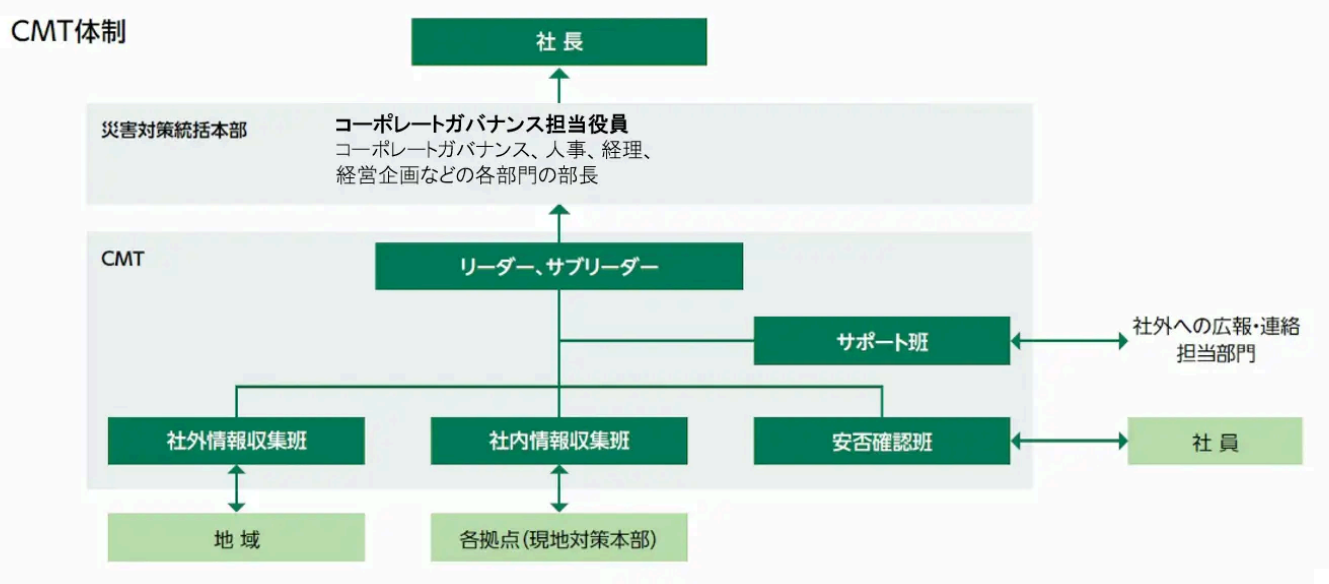
事業継続計画（BCP：Business Continuity Plan）と事業継続マネジメント（BCM：Business Continuity Management）

当社の社会的使命である医薬品の安定供給という観点から、大規模災害やパンデミックはもとより、多様な災害や想定外の事態に対応した事業継続計画（オールハザード型BCP）を策定しています。さらに、当社のリスク管理の強化および実効性向上を図るため、BCPの見直し、事前対策の実施、教育・訓練の実施等の継続的なマネジメントサイクルを確立し、平常時からのマネジメント活動を推進する持続的な事業継続マネジメント（BCM）を進めています。

初動対応計画

災害発生後速やかに情報収集を開始し、被害状況を取りまとめ、災害対策統括本部の設置可否の進言や本部設置後の情報収集を行うCMT（Crisis Management Team）※を設置しています。CMTでは、迅速かつ的確な初動対応力の向上を目的に、定期的な訓練等を実施しています。現在は、CMTと事業所（現地災害対策本部）や災害対策統括本部との連携訓練を実施し、災害発生時の危機管理対応力の向上を図っています。

※CMT（Crisis Management Team）は、災害発生後速やかに参集して情報収集を開始、被害状況を取りまとめて災害対策統括本部の設置可否の進言を行う。災害対策統括本部設置後も引き続き情報収集、取りまとめ等を実施する。



情報管理

当社は、企業活動において大切な資産である情報を活用し、確実に保護することが重要であると考えています。記録と情報管理に関するグローバルポリシーおよび情報管理、ITセキュリティ等に関する各種規則を定め、適切なリスク管理を行っています。

機密情報および内部情報の管理

当社は、社内規則に基づき、重要度に応じて適切に保有情報を管理しています。また、情報管理担当執行役員、情報管理委員会等の管理体制を整備しています。さらに、インサイダー取引の未然防止を図るため、社内規則において内部情報の適切な管理を含む、役職員が遵守すべき基本的事項を定めています。また、役職員への教育研修も定期的に実施し、意識の向上を図っています。

個人情報の管理

当社は、個人情報保護方針を定め、社内規則に基づき、事業活動を通じて取得した医療関係者、製品使用者、取引先、株主、役職員等の個人情報を、国内外の個人情報保護法制に従い適切に取り扱い、保護しています。また、個人情報管理担当執行役員、個人情報相談窓口等の管理体制を整備し、役職員に対し定期的に教育研修を実施するなど、個人情報保護の推進に取り組んでいます。

情報セキュリティ

社会環境の変化や情報技術の進歩に合わせた技術的な対策に加え、社内規則、手順類の見直しと遵守状況のモニタリングを続けるとともに、役職員に対する情報セキュリティ教育を定期的に実施し、意識の向上を図っています。
また、グループ会社や取引先におけるセキュリティリスクへの対応にも取り組んでいます。さらに、サプライチェーンを通じた情報セキュリティリスクへの対策として、セキュリティレイティングサービスを利用して取引先のITセキュリティ評価を実施しています。
加えて、サイバー攻撃による不正侵入の未然防止策の検討を行うとともに、侵入を検知した場合に迅速に対応するための体制（CSIRT: Computer Security Incident Response Team）を設置するとともに、情報セキュリティ事故に対する予防活動を継続的に実施しています。また、CSIRTでは定期的にサイバー攻撃の発生を想定した対応訓練を実施しています。