ガバナンス

リスクマネジメント

リスクマネジメント体制

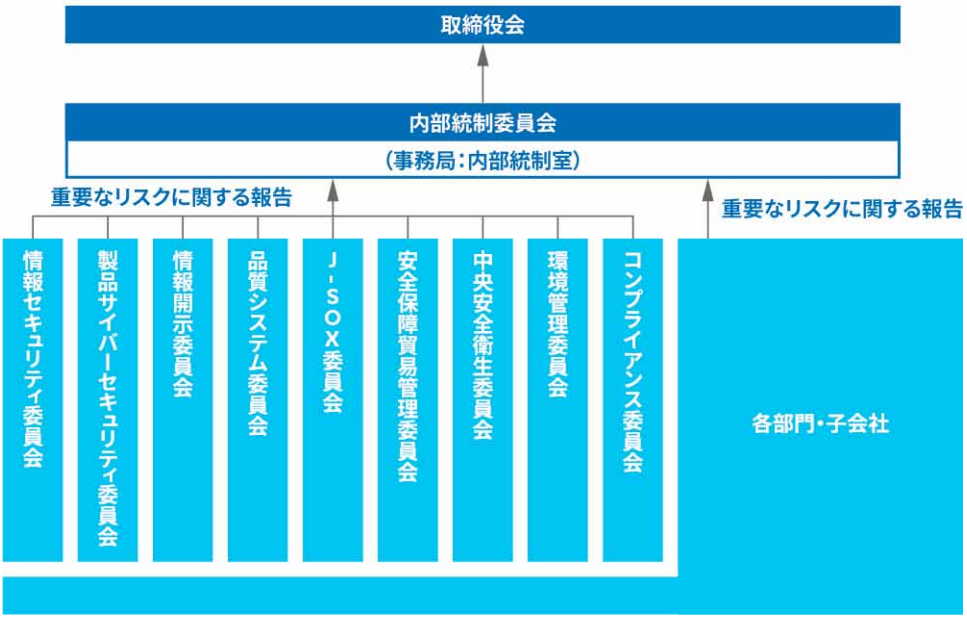
リスクマネジメント体制

委員会を設置してリスクマネジメントを推進

シスメックスでは、グループ全体のリスクマネジメント活動を統括する組織として、内部統制委員会を設置し、戦略リスクも加えたリスク全般に関するマネジメント活動を推進しています。委員長は代表取締役社長が務め、担当執行役員、監査等委員（社外取締役を除く）をメンバーとし、社外取締役がオブザーバーを務めています。

委員会では、公正な取引、腐敗やビジネス倫理を含むコンプライアンス、人材、労働安全衛生、環境、納税を含む会計・財務などの項目についてリスク評価を定期的に実施し、グループとして事業に与える影響が大きなリスクを特定して対策を講じています。また、コンプライアンス委員会などの関連委員会および各部門・関係会社が実施するリスクマネジメントの状況をモニタリングし、定期的に取締役会に報告するとともに、グループ経営に重大な影響を及ぼすリスクが発生した場合についても、取締役会に報告しその対応について審議するなど、継続的に PDCA を回しています。

リスクマネジメント体制



▶コーポレート・ガバナンス
▶シスメックスレポート（リスクマネジメント）

ガバナンス

事業継続に関わるリスクへの対応

事業継続計画（BCP）の整備

大規模災害発生時の対応

シスメックスはグループ全体で、地震や風水害などの大規模災害が発生した際にも重要業務を継続し、迅速な復旧を図るため、生産、調達などの機能ごとに事業継続計画（BCP）を策定して非常時に備えています。

また、安定供給体制をより強固なものにするため、物流センターをより水害リスクが少ない内陸部へ移転しました。そして、免振構造、自家発電、防火シャッターなどの設備も充実させました。

主な BCP の取り組み

- 主要な原材料調達先を分散化（地産地消の考えに基づいた生産場所の選定）
- 半導体など長納期部材の調達に対して中期的な生産計画情報から長納期部品の原材料発注計画をシステムに登録し手配を行う仕組みを構築
- 製商品の保管を機能別（機器、保守パーツ、室温試薬、保冷試薬、危険品試薬など）に分散
- 工場間の相互供給体制の構築、輸送面での代替ルートの確保
- 医療機関への供給を優先する重要製品の選定
- 取引先の自然災害、火災、事故等などの緊急性の高いリスクへの迅速に対応するため、当社と原材料サプライヤー間で危機情報を共有するツール（防災情報クラウドシステム）の導入
- 災害対応に関する規程やマニュアルの整備、模擬訓練の定期的実施
- 従業員の安否確認システムの導入
- 各事業所へのデジタル無線機設置
- 従業員向けの備蓄品、帰宅支援品の設置
- IT 基幹システムの整備（社外データセンターへの配置、緊急時に速やかにバックアップシステムへ移行できるシステム基盤の構築）

▶「試薬の安定供給」という終わりなき使命に挑む

ガバナンス

情報セキュリティの強化

製品セキュリティ、情報・サイバーセキュリティ対策の強化

製品セキュリティの取り組み

シスメックス株式会社は、お客様にご使用いただく製品・サービスに対して「製品セキュリティポリシー」を定め、Product Security Incident Response Team（PSIRT）を設置し、製品の設計・製造、および市販後の脆弱性管理を行っています。また、お客様や研究開発・実験にご協力いただいた方々からお預かりした機微情報（個人・患者・被験者情報含む）や、製品に関する高度な独自技術や知的財産などについては、経営上の重要な情報資産と捉え、情報の外部漏えい防止や、内部不正を未然に防ぐための対策を取っています。

情報・サイバーセキュリティの取り組み

シスメックスではグループ全体で、情報セキュリティポリシーを定め、取締役専務執行役員が務める情報セキュリティ統括責任者の統括・管理の下、DX 戦略推進本部を中心に、グループ全体の情報セキュリティマネジメント体制を構築し、統制管理しています。 Sysmex-Computer Security Incident Response Team（Sysmex-CSIRT）を設置し、マネージド型 SOC（Security Operation Center）からのアラートや外部機関（JPCERT/CC）による脅威情報（脅威インテリジェンス）などを通じ、未然防止や早期対応、さらに情報漏えいやデータ侵害の事前・事後対応などの取り組みの強化を行っています。

外部団体との連携では、厚生労働省・病院・国内医療機器メーカーによる医療サイバーセキュリティ協議会への参加や、一般社団法人 日本シーサート協議会、FIRST（Forum of Incident Response and Security Teams）に加盟するなど、有事や重大インシデントに対する脅威情報の共有を行っています。

社内での具体的な施策としては、情報へのアクセス権限管理の徹底と定期的な棚卸、セキュリティパッチの定期的更新、会社貸与パソコン・モバイル機器の生体認証（顔認証・指紋認証）によるログイン制限、導入アプリケーションの審査など継続的な運用・管理に加え、ランサムウエア対策（エンドポイント技術対策）として、PC・サーバー端末に対するEDR（Endpoint Detection Response）を導入しています。

情報・サイバーセキュリティ教育

シスメックスでは、グループ全従業員に加え、派遣社員、請負業者に対しても、情報セキュリティ教育の e ラーニングを毎年実施しています。2022 年度には、グループ全従業員を対象としたサイバーセキュリティ研修を多言語で実施しました。また、標的型メール訓練（BEC・フィッシング詐欺）に加え、メールの取り扱いに関する講習会など、従業員への情報セキュリティ意識向上の取り組みを実施しています。

当社 Sysmex-CSIRT メンバーに対しては、インシデント対応強化のため、国際的なグローバル資格（ISC2 CISSP, SANS GIAC, CompTIA）の取得を推奨しています。

情報セキュリティに関する認証取得

シスメックス株式会社では、情報セキュリティマネジメントシステム（ISMS）に関する国際規格 ISO 27001 の認証を取得し、遺伝子配列などの個人情報を用いた研究における情報セキュリティ管理を強化しています。また、シスメックス CNA においては、サービス・サポート部門において同認証の取得、シスメックス UK とオックスフォード ジーン テクノロジーでは、ISO 27001 の認証に加え Cyber Essentials※の認証も取得し 6 ヵ月ごとにサーベイランス評価を行っています。

※英国政府が企業のサイバーセキュリティの向上を目的に 2014 年から開始した認証制度

▶情報セキュリティポリシー
▶製品セキュリティポリシー