リスクマネジメント

基本的な考え方

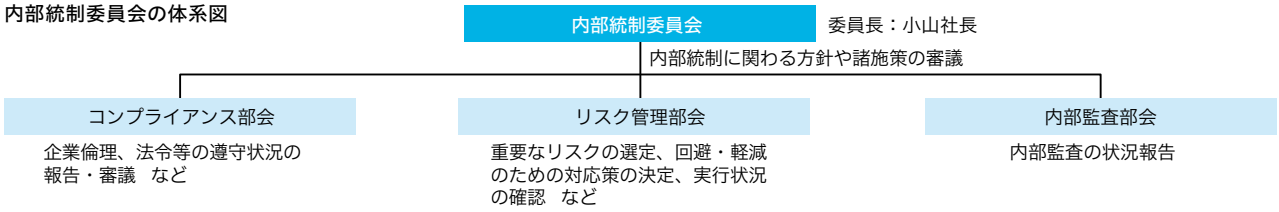
経営に重大な影響を及ぼす危機を未然に防止するとともに、万一発生した場合の被害の極小化を図ることを目的とし、取締役会、内部統制委員会ならびに各種の全社会議体で各機能におけるリスクの把握および対応について意思決定を行っています。

社長を委員長とする内部統制委員会においては、重点リスクの選定、対応策の決定、対応策の実行状況の確認などを行い、より実効性のある対策を行っています。

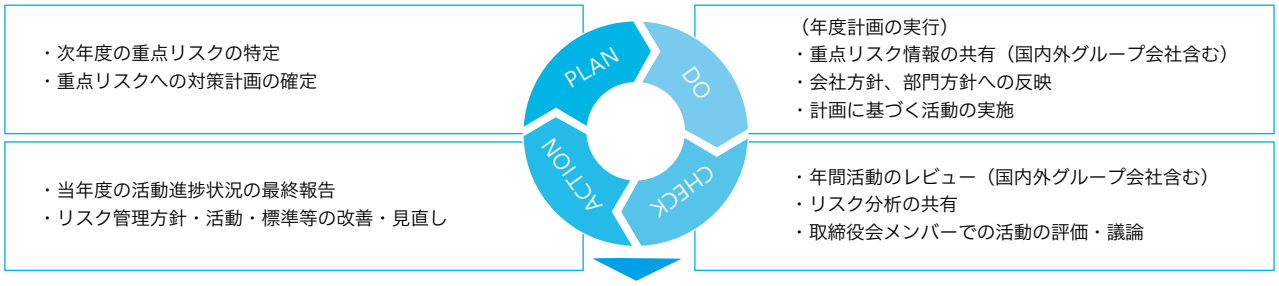
加えて、取締役会では、重点リスクや政情不安などによる突発的な事業リスクへの取り組みについて定期的な議論を行っており、継続的な改善を実施しています。

また、リスクに対する基本的事項を取りまとめた「危機管理対応ガイド」を制定し、想定されるリスクに対する未然防止、および万一の場合に適切・迅速な行動をとるための対応事項を明記しています。なお、新型コロナウイルスについては、取締役会にてBCP報告の一部として議論しており、感染拡大状況に鑑みた(1)在宅勤務の推進、出張や来訪者の規制、社内イベントの中止等による感染防止の実施、(2)感染者が発生した場合の対策の実施、(3)サプライヤーも含めた課題把握による生産体制の維持、(4)収益改善策の実施等により、新型コロナウイルスの影響の極小化を図っています。

内部統制委員会の体系図



リスクマネジメントの主たる活動



活動の外部公表（有価証券報告書、コーポレート・ガバナンス報告書、統合報告書、企業Webサイト 等）

重点リスクへの対応

事業環境に基づく経営基盤リスクおよび事業戦略リスクを「経営への影響(財務影響等)」と「発生の可能性(頻度)」の観点でリスク評価をし、重点リスクを選定しています。

重点リスクは重要な取り組み事項として会社方針等へ反映し、リスク低減・未然防止を図っています。

重点リスク事例

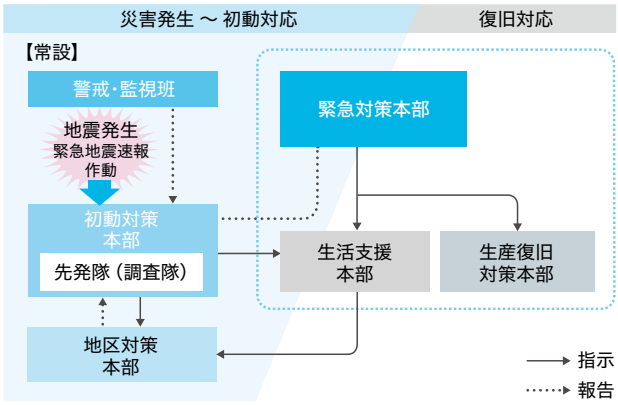
区分		主な重点リスク		
リスク規模 経営への影響(財務影響等) × 発生の可能性(頻度)	大	•大規模災害(地震・風水害、他) •TCFDに基づくリスク・機会と対応 •DX対応 •重要品質問題によるリコール発生	•新型コロナウイルス(感染防止・生産体制維持) •カーボンニュートラル対応 •ロシア・ウクライナ情勢影響 •重大労働災害による人的被害・操業停止	•サイバー攻撃・詐欺メール
	中	•機密情報の漏洩	•交通事故(重大加害)	•ハラスメントの発生
	小	•独占禁止法違反	•パートナー企業の事業運営	•火災・爆発事故による企業活動の停止

大規模災害を想定した「危機管理統括プロジェクト」

当社では、南海トラフ巨大地震や気候変動による自然災害などの大規模災害を想定して、「人命第一」「地域支援」「早期復旧」を基本とする危機管理体制を整えています。具体的には「危機管理統括プロジェクト」を中心にハード・ソフト面の対策に加えて、災害時の対応者のスキルが不可欠と考え、役員をはじめとする対策本部メンバーの「レジリエント訓練」(災害模擬演習)を2013年度から全社で延べ160回以上実施。また、生産復旧体制の整備として、被災した建屋・設備・工程の復旧と代替生産の手順の具体化を進めています。

被災後も製品開発を継続できるよう、設計図面データなどの復旧訓練も行っています。さらに社内だけでなくグループ会社・サプライヤーの危機管理強化の研鑽会を定期的に実施。「地震対策実施状況チェック表」による評価、グラフ化による弱点の明確化、当社や他社の対応事例の紹介や事業継続計画書(BCP)の作成協力などを行っています。

災害対応イメージ



これまでの取り組み

区 分	実 施 事 項
ハード	•建物、設備の耐震対策 •災害時の全社の対策本部基地となる防災センターの設置 •MCA無線※1、衛星電話の全拠点への配備 •危機管理サーバー(免震構造)、非常用発電機の設置 •DR※2、DC※3の運用
ソフト	•敷地建物安全判定の導入 •地震速報システム、安否情報システムの運用訓練 •サプライチェーン情報の整備 •事業継続計画書(BCP)の作成
スキル	•レジリエント訓練(災害模擬演習)の継続的な実施

※1 日常の業務から緊急・災害時まで様々な用途で使用される無線
※2 被害を受けたシステムを復旧・修復する体制(Disaster Recovery)
※3 コンピューターやデータ通信などの装置の設置・運用に特化した施設の総称(Data Center)

グローバルリスク対応の強化

国内にとどまらず、次々に発生するグローバルリスク(部品・原材料の逼迫、新型コロナウイルス関連の稼働停止、ウクライナ情勢等)に対し、国内外で早期状況把握(BCP週報毎週発行)およびグローバルで必要なアクションを取っています。また、国内外各拠点が自発的に対策が打てるよう順次標準化を進め、各社の事業環境が捉えている重点リスクへの対応力を強化しています。

サイバーセキュリティ対策の基本方針

機密情報の管理強化のため「機密管理規程」に基づき全部門のルール遵守状況を年1回点検するとともに、現地監査も実施。国内外グループ会社に加えて、主要サプライヤーも対象に自主点検を行っています。

全部門に機密保持責任者を置き「情報システムセキュリティ運用標準」や「機密情報管理のてびき」などを基に機密管理の啓発活動を行っています。また、国内外グループ会社および主要サプライヤーにおいては、当社への影響度合いと各社のサイバーリスク対策の点検結果に基づいた具体的な対策を層別・実行しており、全社会議体の中で定期的に報告・議論を行うことで、グローバル一体でのサイバーセキュリティ対策を推進しています。

サイバーセキュリティ対策の主な取り組み

区分		実施事項(国内外グループ会社およびサプライヤーは影響度に応じて対応)
過失による漏洩防止	ハード	•複合機、図面専用印刷機のIDカード認証による印刷制限
	ソフト	•全パソコンのデータ暗号化 •電子メール社外送信時のセキュリティ措置(上司アドレスCCの義務化、添付ファイルの暗号化)
悪意による漏洩防止	ハード	•監視カメラの増強 •外部記憶媒体への書き出し制限 •PC盗難防止用ワイヤーロックの設置
	ソフト	•機密保持の誓約 •システム利用の記録、アクセス記録取得の監視 •物品持出申請の強化 •不正侵入防止対策の強化(インターネット) •ファイルサーバーへのアクセス制限 •外部からの持込端末の不正接続防止
啓発活動(モラル対策)		•新入社員教育 •各部門への現地点検実施 •チェックシートを用いた全社機密管理自主点検 •標的型メールへの対応訓練