リスクマネジメント

リスクをチャンスに変える挑戦とリスクをコントロールする取り組みで持続的な企業価値向上に貢献します

■ 当社を取り巻くリスクについて

国際情勢や地政学リスク、サイバー攻撃といった外部環境の変化や、人権尊重や環境規制などの外部要請が高まる中、当社を取り巻く環境は大きく変化しつつあります。その中で自動車業界においては、保護主義の台頭に伴う関税の発動や、電動化の進展が鈍化している状況です。このようにリスク範囲が広く、予測が困難な変化が続く事業環境の中で、持続的な企業価値向上を実現するには、変化を先取りし、グローバルにリスクマネジメントを推進することが重要です。

また、ここ数年、自動車業界は相次ぐ認証不正により品質の信頼を揺るがしています。加えて、サプライチェーンでの不適切な取引によるコンプライアンス問題も発生しています。ステークホルダーや社会から信頼され、「選ばれる企業」であり続けるために、リスク管理の重要性が一層高まっています。

■ 2030事業計画の実現に向けたリスクマネジメント活動

基本的な取り組み

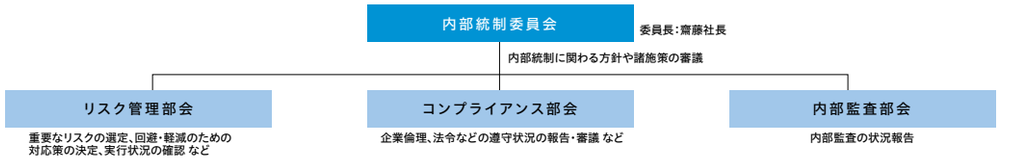
当社では、情報収集の充実とその分析をするために、PEST※1や3C※2などの手法を活用しています。この分析を通じて、リスクを機会と捉えて事業成長につなげる「事業戦略リスク」と、発生時の損失を最小限に抑えるための「経営基盤リスク」に分類し、CROがグループ全体をリードしながら、各々のリスク低減活動に取り組んでいます。

具体的には、社長を委員長とする「内部統制委員会」を年2回開催し、その中で構成される「リスク管理部会」にて、各々の重点リスクの議論やリスク低減活動のフォローをしています。重点リスクの選定は、毎年、外部環境と内部環境の分析により、経営への影響度合いと発生の可能性をベースに、リスク評価を行っています。

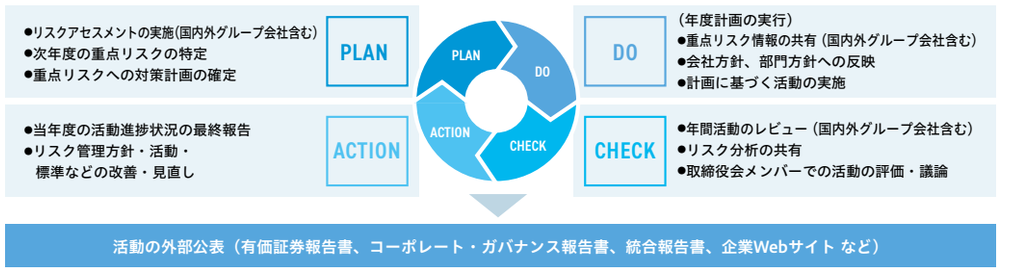
事業戦略リスクは、2030事業計画の実現に向けて、重点施策を中心にリスクに対する施策の実行計画をバックキャストとフォアキャストの視点で整理し、戦略の見直しとともに、年度方針へ反映しながら、さらなる事業成長に向けて取り組んでいます。一方、経営基盤リスクについては、持続的な経営に影響を及ぼす要素を機能ごとに抽出し、リスク低減を推進しています。

※1　外部環境を政治、経済、社会、技術の4つの要因に分類し、自社に与える影響を読み解く分析手法
※2　顧客、競合、自社の観点から市場環境を読み解く分析手法

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



2024年度の振り返り

事業戦略リスクは、2030事業計画の確度を高めるために、世界経済や主要国の関税動向、BEV普及のスローダウン、中資系カーメーカーの躍進など事業環境の変化に鑑み、各戦略へ織り込みました。また、経営基盤リスクは、自動車業界での品質認証問題を踏まえ、体制基盤強化や職場風土改革に継続して取り組みました。具体的には、各職場での困りごと抽出を継続するとともに、2025年6月には、独立した法規認証管理体制組織を室から部へ格上げしました。加えて独禁法や下請法遵守に向けた仕入先様とのコミュニケーションの充実も図ってきました。

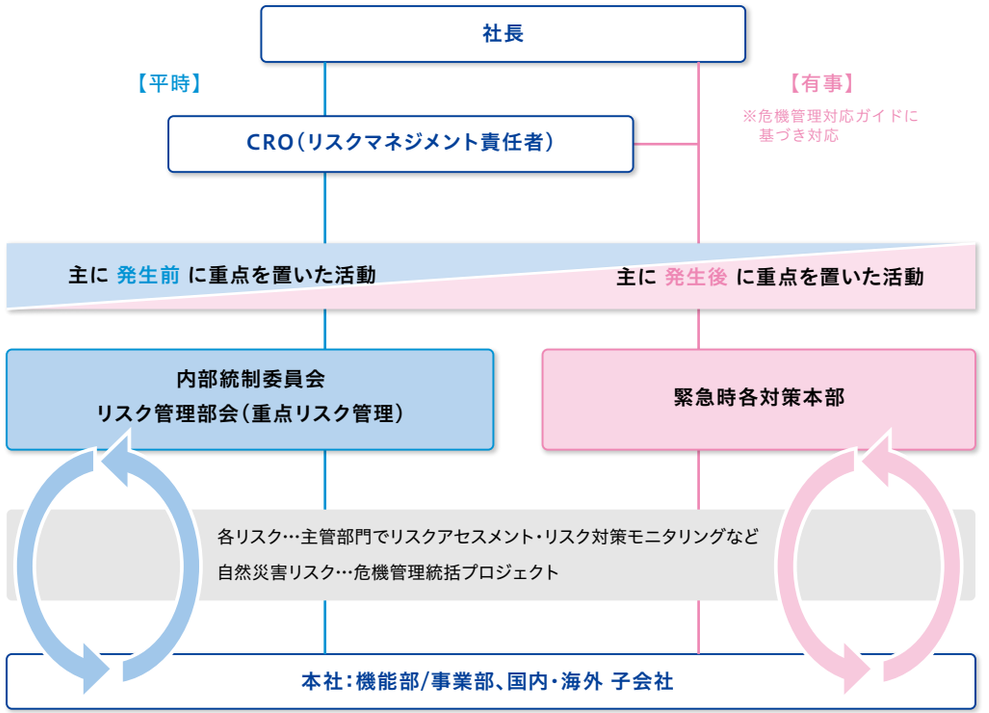
リスクマネジメント

また、重点リスクの中でグローバルで影響の大きいリスクは、国内外グループ会社に展開し、年間を通じてリスク低減活動のためのPDCAサイクルを回しています。特に、品質認証や取引適正化など、世の中から注視されている領域では、コンプライアンス活動を通じて取り組んでいます。また、経済安全保障に関しては、ワーキンググループで継続的に、国内外の動向を勘案した施策を推進しています。

2024年度の重点取組に掲げていたリスク低減活動及びリスク発生後の活動の連携とマネジメント強化に向けて、リスク管理に関する社内機能と役割を再整理しました。また、役員向けに専門家を招聘してクライシスマネジメントの研修を実施しました。

なお、リスク顕在化時の対応に関して基本的事項を取りまとめた「危機管理対応ガイド」を制定しており、万一の場合に適切かつ迅速な行動をとるための対応事項を明記しています。

全社リスク管理体系



今後の取り組み

2025年度の事業戦略リスクは、カーボンニュートラルやサーキュラーエコノミーへの対応や、BEVの普及動向に鑑みたバリューチェーンの構築（BEV動向の変動に対応するサプライチェーン、生産体制の構築含む）など全4項目の重点リスクを選定しました。これらを踏まえ、戦略的な投資や製品開発など具体的に事業活動へ落とし込み、推進しています。

一方、経営基盤リスクでは、米中貿易摩擦や関税含めた米国政策への対応、重要鉱物の輸出規制など各国規制への対応不足によるサプライチェーン分断などをリスク要因として選定しました。これらを含む全8項目を重点リスクとして選定し、具体的なリスク低減策に取り組んでいます。選定した重点リスクは、国内外の関係会社にも展開し、個社のリスクアセスメントや本社との協働による自主点検活動を行い、グループ全体でPDCAを回しています。また、経済安全保障は、2023年度に新設したワーキンググループ活動にて、各国の法規動向を捉えた対応策を講じるとともに、変化する環境や要請を踏まえ、原材料や部品の安定調達に向けて、サプライチェーンの強靭化に取り組んでいます。

また、経済安全保障を含む重点リスクや、政情不安による突発的なリスクへの取り組みについて取締役会などでの議論を通じて、変化に即した継続的な改善を行っています。

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（財務影響など） × 発生の可能性（頻度）	大	●カーボンニュートラル、サーキュラーエコノミー対応（カーボンプライシング対応、ゴム・樹脂材料対応含む） ●大規模災害（異常気象、他） ●米中貿易摩擦（地政学リスクなど） ●関税含めた米国政策 ●各国規制への対応不足によるサプライチェーン分断 ●重大労働災害による人的被害・操業停止 ●重要品質問題によるリコール発生 ●サイバー攻撃・詐欺メール
	中	●BEV化対応（BEV市場への新製品市場投入、燃料系部品減少対応など含む） ●火災・爆発事故による企業活動の停止

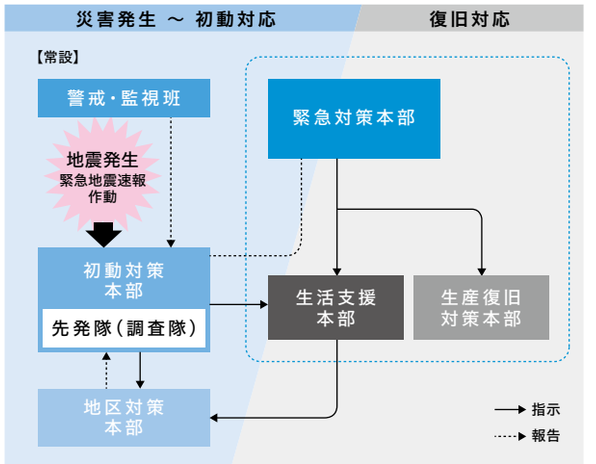
リスクマネジメント

リスクへの対応事例

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240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。

大規模災害時のイメージ



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。

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　●スターリンクの初動・生産復旧対策本部への配備 ●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、見える化 ●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・災害時までさまざま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）

サイバーセキュリティ対策の活動

当社では、企業活動における情報の重要性とリスクの高まりを踏まえ、機密情報管理の徹底とサイバーセキュリティの強化をリスクマネジメントの重要課題と位置づけて、その対策活動を行っています。2025年1月には、セキュリティ推進チームの専門組織を設置し、対策の活動を加速しています。

機密情報を適正に管理するため「機密管理規程」に基づき、全社横断での年次点検を実施し、各部門におけるルールの遵守状況を確認しています。国内外のグループ会社に対しても自主点検や現地監査を行い、管理体制の浸透を図っています。

具体的には、本社・関係会社・仕入先を含めたサプライチェーン全体で包括的な取り組みを推進しています。特に、製造・出荷への影響度合いに応じて、リスクの高い拠点・仕入先から優先的に安全性の検証をしています。今後の重点施策として、有事の際に関係者が機動的に動けるよう、環境（ツール類）の整備と実際の事故を想定した対応訓練を計画しています。また、グローバルセキュリティ啓発活動やグローバルでの会議体を通して、グループ全体の底上げを図っていきます。なお、これらの取り組み状況は、全社会議体にて定期的に報告・議論されており、環境変化などを鑑みながら対策の改善を進めています。

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仕入先は影響度に応じて対応）
過失による漏洩防止	ハード	●パソコンデータの暗号化 ● USB デバイス接続制限
	ソフト	●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・侵害防止	ハード	●コンピュータウイルス対策ソフトの導入 ●ファイアウォールによる社外との通信制御 ●不正通信の常時監視 ●社外公開システムの改ざん検知・防止対策 ●ネットワークへの不正接続防止
	ソフト	●機密保持の誓約 ●ファイルサーバへのアクセス制限 ●物品持出申請の強化
啓発活動（モラル対策）		●従業員へのセキュリティ教育 ●標的型メールへの対応訓練 ●チェックシートを用いた全社機密管理点検／現地監査