リスクマネジメント

CRO MESSAGE

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。

CRO 執行役員　大谷 勝文

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、人権保護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、必要とさ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ると強く感じています。

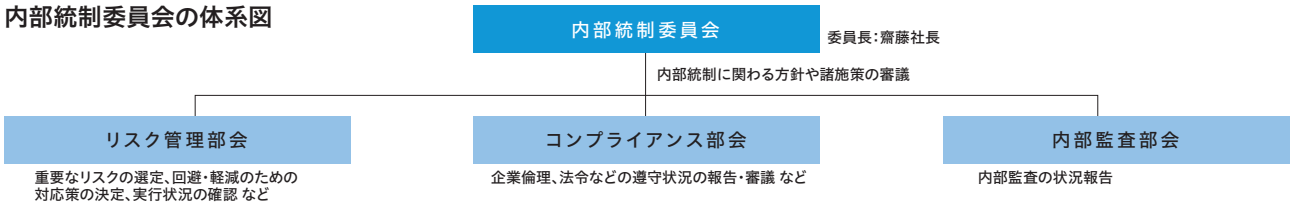
2030事業計画の実現に向けたリスクマネジメント活動

《 基本的な取り組み 》

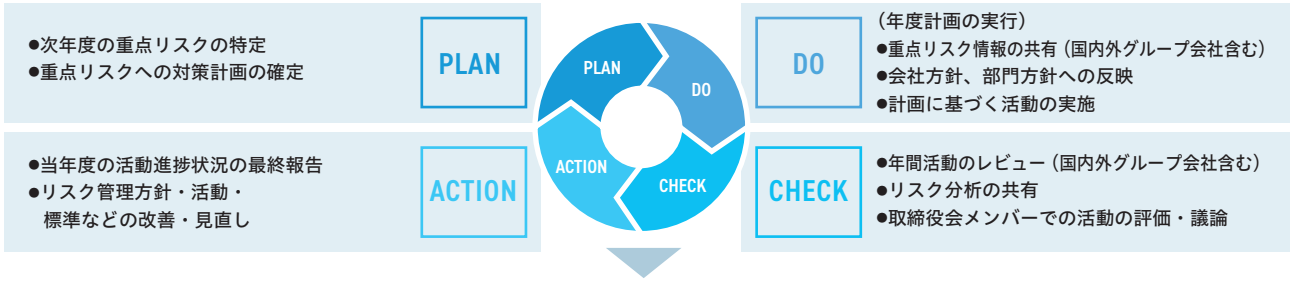
当社では、情報収集の充実とその分析をするために、PEST※1や3C※2などの手法を活用しています。この分析を通じて、リスクを機会と捉えて事業成長につなげる「事業戦略リスク」と、発生時の損失を最小限に抑えるための「経営基盤リスク」に分類し、CROがグループ全体をリードしながら、各々のリスク低減活動に取り組んでいます。

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。

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 など）

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毎に抽出し、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

《 2023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、国際政情不安、経済低迷、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をふまえ、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ふまえ、体制基盤強化や職場風土改革に取り組みました。具体的には、独立した法規認証管理体制組織の新設や、各職場での困り事の抽出。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まいりました。

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を新設し、国内外の動向を勘案した施策を実施しています。

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。

《 今後の取り組み 》

2024年度の事業戦略リスクは、BEV普及の鈍化に伴う各カーメーカーの戦略変更や全方位戦略への対応などに加え、重点施策である成長市場のインド事業戦略に関わるリスク、そして、従来より取り組んでいる、アセアンを中心とした中資系カーメーカーのグローバル展開への対応を追加し、全11項目の重点リスクを選定しました。これらをふまえ、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、各国の保護主義的な通商政策懸念や中東、ロシアなどの地域紛争の長期化などの地政学リスクに加え、少子高齢化による労働力の減少や採用難による人材不足、中資系新興BEVメーカーの経営問題などを新たなリスク要因として追加しました。これらを含む全14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ふまえ、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。

《 持続的成長に向けて 》

地政学リスクや各国の経済政策による外部環境の急速な変化、さらには各国の規制やルールの複雑化といった外部要請に加え、グループ各社について丁寧な分析と評価を行うことが不可欠です。これらのリスク分析をふまえ、スピード感を持って適切なリスク低減策を実行することや、リスクが具現化した場合の危機対応が重要となります。今後もステークホルダーのみなさまから信頼される企業であり続けるために、リスクマネジメント体制を継続的に強化し、先回りしたリスク対応を通じて、誠実な事業運営に努めてまいります。

重点リスク事例

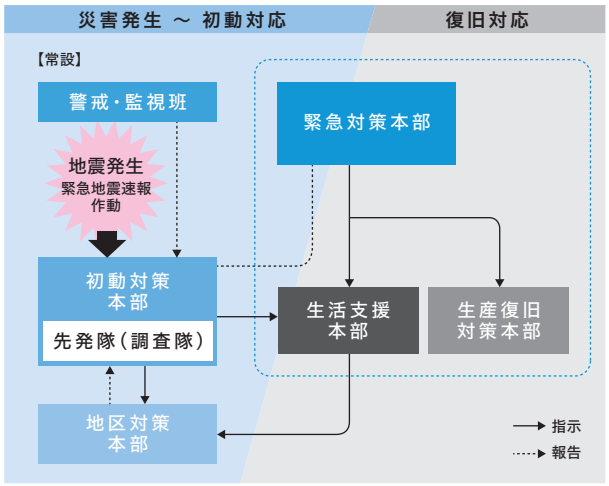
区分		主な重点リスク
リスク規模 経営への影響（財務影響など） × 発生の可能性（頻度）	大	●カーボンニュートラル対応（カーボンプライシング対応、ゴム・樹脂材料対応含む） ●サーキュラーエコノミー対応（グリーンテクノロジー対応含む） ●大規模災害（異常気象、他）　●原材料調達・エネルギー高騰、など　●成長分野・市場への対応 ●重要品質問題によるリコール発生　●サイバー攻撃・詐欺メール　●中資系カーメーカーのグローバル躍進 ●重大労働災害による人的被害・操業停止
	中	●BEV化対応（BEV市場への新製品市場投入、燃料系部品減少対応など含む） ●人員不足（労務費高騰含む）　●サプライチェーン分断（地政学、市況動向、感染症・災害などによる影響など） ●機密情報の漏洩　●貿易摩擦（経済安全保障関連含む）　●ハラスメントの発生 ●交通事故（死亡・悪質）　●火災・爆発事故による企業活動の停止
	小	●特許網構築不足

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210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

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」などをもと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