

事業等のリスクとその対応

三菱重工業グループの経営者が財政状態、経営成績およびキャッシュ・フローの状況に重要な影響を与える可能性があるとして認識している主要なリスクには、以下のようなものがあります。これらの主要なリスクは、10年以内に顕在化する可能性があり、特に「新型コロナウイルス感染症の感染拡大」および「SpaceJetの開発遅延」は、既に顕在化し、当社グループへの影響が大きいリスクです。また、これら

の主要なリスクの中には、より中長期的な観点で、当社グループを取り巻く事業環境や社会構造のさらなる変化をもたらす可能性があるものも含まれており、当社グループは、先んじて対策を取っていかねばならないと認識しています。なお、記載事項のうち将来に関する事項は、2019年度末において判断したものです。

主要リスク	主要リスクの内容	対策
新型コロナウイルス感染症の感染拡大	● 案件の進捗遅延による売上計上時期の遅れ ● 渡航制限やサプライチェーンの停滞 ● 契約交渉や受注プロセスの遅延 ● 生産やサービス事業への影響の発生 ● 操業度の低下や停止、生産調整の実施 ● サプライチェーンの停滞	人員対策を含めた固定費の圧縮、従業員の一時帰休、工場稼働率の見直しや生産調整、外部流出費用の削減、投資計画の見直し、余剰リソースの有効活用、各国の助成制度の活用等の対策を進めています。
SpaceJetの開発遅延	● 売上計上時期の遅れ ● 顧客からの契約解除 ● 顧客やパートナー企業その他の関係者からの損害賠償の請求の発生	今後の市場動向を注視しながら関係者との情報共有・関係維持に努めつつ、引き続き開発スケジュールの精査を行うとともに、予算についても適正な規模で推進するなどの対策を進めています。
各種の災害	● 生産設備の毀損・滅失 ● サプライチェーンの停滞・混乱 ● 生産に必要な材料・部品等の不足やサービスの提供停止 ● 生産拠点の操業低下・稼働停止 ● 代替となる生産設備や取引先の喪失 ● 損害保険等で補填されない損害の発生 ● テロや感染症の世界的流行等による製品・サービスの需要縮減	災害対策支援ツールの活用、連絡体制・事業継続計画（BCP）の策定・整備、工場の点検や各種訓練の定期的な実施に加え、各国の情勢や安全に関する情報収集等の対策を進めています。

主要リスク	主要リスクの内容	対策
事業環境の変化	●環境意識の高まりによって、製品・サービスの需要が減少し、事業規模の縮小や投下資本の回収が困難となる事態の発生 ●化石燃料由来の電力需要の低下や競合他社との競争激化が発生した場合による、建設工事やアフターサービスなどの受注減少 ●M&Aやアライアンスが目論見どおり実現できない場合の減損損失等の計上	性能・信頼性・価格面の競争力を向上させるべく、研究開発や設備投資を通じた製品競争力の維持・強化を図っています。また、社外の知見も取り入れて市場の動きを先取りした新たな機能やソリューションの提案に注力しています。さらに、2020年4月に成長推進室を設置し、既存の事業部門では対処しにくい新しい領域の事業開拓や既存事業の組み合わせを通じた事業開発等の対策を進めています。
製品関連の問題	●損害賠償請求等の発生 ●賠償額等の負担が、保険で補填されない事態の発生	適切な品質の管理および安全性の確保に取り組むとともに、事業リスクグローバルポリシーや各種規則の制定・運用、事業リスクマネジメント体制の整備・強化、個別案件の事前審議や受注後のモニタリング、事業部長クラスへの教育の実施、製品安全に関する講座の継続的な開催等の対策を進めています。 ▶ 詳細はP74の「事業リスクマネジメント」をご覧ください。
知的財産関連の紛争	●損害賠償責任の発生 ●特定の技術を利用できなくなる事態の発生 ●技術導入を受けられず事業遂行に支障をきたす事態の発生	製品の基本計画・設計・製造の各段階で他者が保有する知的財産を十分に調査することによる知的財産関連の紛争の未然防止、教育・人材育成を通じた知的財産部門の専門性向上等の対策を進めています。
法令等の違反や情報漏洩	●行政処分等の措置を受ける事態の発生 ●損害賠償責任の発生 ●事業遂行が困難となる事態の発生 ●競争力の大幅な低下、社会的評価および信用の失墜	コンプライアンス・情報管理・ブランド戦略等の各種社内教育の充実と継続的な実施、グローバルポリシーや各種規則の制定・運用を行っています。また、サイバー攻撃によるリスクを最小化するため、CTO※直轄のサイバーセキュリティ推進体制を構築し、当社グループのサイバーセキュリティ統制（基準整備・対策実装・自己点検・内部監査）やインシデント対応等の対策を進めています。 ※ CTO: Chief Technology Officer ▶ コンプライアンス強化に関する詳細はP76の「コンプライアンス」をご覧ください。 ▶ 情報管理に関する詳細はP77の「サイバーセキュリティの取り組み」をご覧ください。