リスクマネジメント

基本方針

富士電機は、「富士電機リスク管理規程」に基づきリスクを体系的、組織的に管理しています。富士電機の経営に影響を及ぼす可能性のあるさまざまなリスクに関して、遺漏なく適切に管理・対処することでリスクの顕在化(危機的事態の発生)を未然に防止し、リスクによる影響の最小化を図っています。

リスク管理体制

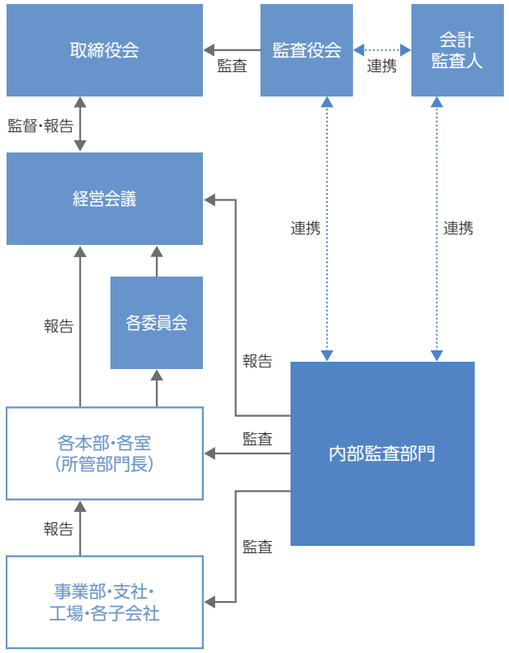
当社の各部門および関係会社は、事業責任の一環としてその事業活動に伴うリスクの管理に責任を負い、適切なリスク管理体制を整備してリスク対策を実施していますが、気候変動、広域大規模災害、地政学リスクや経済安全保障対応など、取り巻く環境が複雑化する中、全社横断的な共通リスク管理についてリスクマネジメントを強化していきます。

事業計画や大規模投資などに関わる重要なリスクについては経営会議などで適宜報告し、共有を図っています。また、リスク管理を確実に実施するためにマニュアル類を整備し、リスクの種類に応じた教育を実施するとともに、社内報などでリスク管理の取り組みを周知しています。

内部監査部門は、当社の各部門および関係会社が富士電機リスク管理規程に基づいてリスクを抽出・評価し、対策方針を定めて適切に管理体制を構築し的確に運用しているかを定期的に監査しています。2025年度は46拠点の内部監査を実施しました。

2026年度は、全社のリスク管理を統括する経営企画本部にリスクマネジメント室を新設し、内部統制システムとして、経営に重大な影響を与える可能性のある全社BCP※、セキュリティ、経済安全保障などのリスクを体系的に把握・評価し、関係先との連携による情報収集、体制の整備、対策の展開に取り組みます。

※Business Continuity Plan



主要なリスク一覧は当社HPをご参照ください。
https://www.fujielectric.co.jp/csr/governance/risk_management/risk/index.html

緊急事態発生時の対応

大規模災害や事故などの緊急事態が発生した場合、事態の拡大防止と早期収束が図れるよう、平常時の準備、緊急事態発生時の緊急連絡、緊急対策本部の設置について定めた対応要領を策定しています。

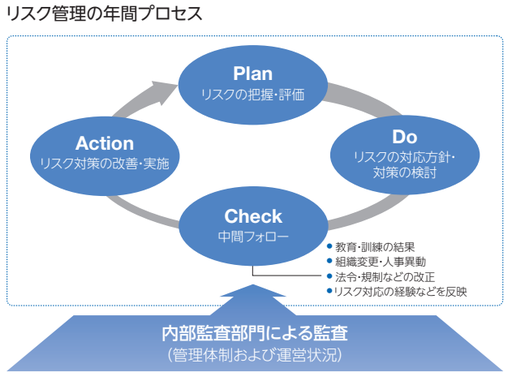
リスク管理プロセス

当社の各部門および関係会社は、年次の予算策定時に事業活動に伴うリスクの把握・評価を行っています。

各リスクへの対策は、経営への影響および発生頻度を踏まえて、各リスクに関する対応(回避、低減、移転、保有など)の方針や対策を検討し、各部門などで実行責任者などを定め実施しています。

第2四半期終了後に中間フォローを行い、リスク対策の年度評価・次年度対策を行っています。

リスク管理の年間プロセス



自然災害・事故への対応(BCPの取り組み)

大規模災害や事故などの不測の事態においても重要な事業を必要な時間内に再開・継続するため、「富士電機事業継続マネジメント(BCM)規程」に基づき、全社で事業継続計画(BCP)の策定と継続的な改善に取り組んでいます。

BCPは本社や工場、お客様の対応窓口となる支社で策定するとともに、ITシステムの早期復旧や被害最小化に向けた対応、調達分野における自然災害リスクへの対応やマルチソース化の対応など、事業継続に欠かせない機能に対して網羅的に策定しています。また策定したBCPに基づいた教育訓練を実施するとともに、BCPおよびその管理体制の有効性を半期に1回「全社BCM推進会議」で定期的に評価しています。工場や支社で策定したBCPにおいては、想定する災害・被害規模が最新のリスクに応じているか、目標とする被害の復旧時間と事業継続に向けた戦略の妥当性について危機管理事務局が確認、評価、検証し、BCPの改善および事業継続力の強化に取り組んでいます。

さらに緊急時対応および事業継続対応の確実な実行に向け、事業責任者クラスを対象とした「事業継続セミナー」、各拠点の「災害対策本部訓練」に継続的に取り組むとともに、大規模地震発生などにより本社の災害対策本部が機能できない場合を想定した訓練を年4回実施しています。

このような事業継続の積極的な取り組みが評価され、「国土強靱化貢献団体認証(レジリエンス認証)」を更新取得しています。

セキュリティ対策の強化

サイバー攻撃の脅威に対応するため、サイバーセキュリティと、情報管理・運営体制などのガバナンスの継続的な強化に取り組んでいます。

情報セキュリティの維持・強化の取り組み

保有する経営、営業または技術上の情報、個人情報などの資産価値を機密情報として適切に管理するために、情報セキュリティに関する方針および規程類をNIST(米国国立標準技術研究所)サイバーセキュリティフレームワークをベースに再整備し展開しています。

また富士電機および国内外グループ各社に管理体制を構築し、全従業員への定期的な教育、事業所や執務室の入退場者管理、インターネットやパソコン端末のセキュリティ対策などを実施するとともに、各職場の取り組み状況を毎年点検しています。

さらに、多様化・高度化するサイバーセキュリティ脅威への対応として、セキュリティ対応体制(CSIRT/SOC)の強化、新たなサイバー攻撃の兆候や情報の監視の強化、情報システムの防御・攻撃監視機能の強化を図っています。

各拠点においても、お取引先様の要求事項や関連する業界団体のガイドライン・市場動向などを踏まえて情報セキュリティの対策向上に努めており、情報セキュリティ管理の公的認証が求められる事業ではISMS認証を富士電機㈱2部門と子会社2社が取得しています。また、個人情報保護に関しては、プライバシーマークを富士電機㈱と子会社2社が取得しています。

製品セキュリティと工場セキュリティの強化

製品セキュリティは、EUサイバーレジリエンス法(CRA)など法規制への対応と強化が求められています。駆動制御機器、制御機器、監視制御システムなどの製品・システムは、デジタル化によりネットワークへの接続される機会が急増しています。製品のライフサイクル全体(設計、開発、出荷、運用など)を通じてセキュアな状態を保つ技術(組込セキュリティ)とサポートの重要性が高まっています。

当社製品・サービスの品質向上と安定供給を実現するため、2023年度より制御システムセキュリティ国際標準規格「IEC※1 62443-4-1」の認証取得を進めています。2026年4月には、これまでに認証を取得した5拠点(東京工場、鈴鹿工場、神戸工場、発紘電機㈱、富士電機機器制御㈱)に加え、新たに筑波工場でも認証を取得しました。さらに東京工場においては「セキュアな製品を作るためのプロセス」の継続的な運用が認められ、認証更新を取得しました。

2026年度、新たにセキュリティ委員会を設置し、従来の情報セキュリティインシデント対応(CSIRT※2)機能に加え、新たに製品セキュリティインシデント対応(PSIRT※3)機能および工場セキュリティインシデント対応(FSIRT※4)機能を持つ組織を立ち上げます。これら各組織が連携して、多様なサイバー脅威に適切に対処し、リスクを最小化する等、組織横断的に活動を進めます。これらの取り組みにより、お客様へお届けする製品・サービスの品質向上と安定供給の実現に向けた取り組みを推進しています。

※1 IEC : International Electrotechnical Commission (国際電気標準会議)
※2 CSIRT : Computer Security Incident Response Team
※3 PSIRT : Product Security Incident Response Team
※4 FSIRT : Factory Security Incident Response Team

プロジェクト案件管理の強化の取り組み

利益重視の経営による更なる企業価値向上の実現に向け、プロジェクト案件管理の強化による損失発生リスクの低減に取り組んでいます。

損失発生リスクの早期把握と予知保全のため、これまでに発生した大口損失発生事例をもとにその発生原因を分析して社内関連部門と共有するとともに、再発防止策の実行および運用状況のモニタリングを実施しています。

特に海外拠点向けの教育充実化の取り組みを継続し、更なるプロジェクト案件管理の強化および一層の損失発生リスクの低減につなげていきます。