

リスクマネジメント

基本的な考え方

気候変動、自然災害の多発及び激甚化、地政学リスクの高まり、デジタル化の進展、価値観の多様化など、企業を取り巻く環境は日々変化しています。このような情勢のもと、持続的な企業価値向上を実現するためには、将来発現し得るリスクを幅広くかつ正確に把握し、適切に対応することが必要です。明電グループでは、グループ全体のあらゆる重要な事業リスクを把握し、経営層の議論を経て全社統合的にそれらのリスクをコントロールする仕組み

(ERM = Enterprise Risk Management)を構築しています。

また、平常時のリスクマネジメントに加えて、事故や災害の発生による事業継続の危機に対応するための管理(BCM = Business Continuity Management)を組織一体的に実施・運営することで、常に変化するあらゆる平時・有事のリスクに対応できる体制を構築しています。

リスクマネジメントの体制と委員会の運営

明電グループでは、スリーラインモデルによるリスクマネジメント体制を構築しています。「リスクマネジメント委員会」は、社長を委員長とし、役付執行役員で構成されます。同委員会では、内部統制推進部が年1回集計・抽出した明電グループの重要な事業リスクについて審議を行い、全社重要リスクを選定します。審議の結果、要対応と判断されたリスク

については優先的に対策を進め、その内容を常務会及び取締役会に報告することで適切に監督される仕組みとなっています。これにより、第1ラインから経営層まで一貫したリスクマネジメント体制を構築し、グループ全体を統括するERMを運用しています。

リスクマネジメント体制の詳細はWebサイトをご覧ください。
<https://meidensha.disclosure.site/ja/themes/103>

事業活動に伴う

主なリスク

明電グループは、上記のような体制のもと、リスクマネジメント委員会での議論を経て、グループ全体の重要な事業リスクを定めています。その結果として経営に影響を及ぼす可能性のあるリスク事象は右記の通りであると考えています。

リスク名称			リスク評価			
			影響度	発生可能性	リスクが顕在化する速度	リスク発生による影響期間
外部環境リスク	1-1	市場環境変化への認識・対応不足	大	高	中	中
	1-2	自然災害の発生	大	中	速い	短い
	1-3	サイバー攻撃	大	中	速い	短い
	1-4	地政学リスク	中	高	速い	中
戦略リスク	2-1	人財の不足	大	高	速い	長い
	2-2	経営方針、事業戦略に対するリスク	大	中	中	短い
オペレーショナルリスク	3-1	設備起因の生産停止リスク	大	高	中	中
	3-2	品質の低下	大	高	中	中
	3-3	労務管理・労働環境の悪化	大	中	速い	長い
	3-4	労働災害のリスク	大	中	速い	短い
	3-5	内部情報の流出、不正利用	大	中	速い	短い
	3-6	調達リスク	大	中	中	中
コンプライアンスリスク	4-1	建設業法違反	大	中	中	中
	4-2	独禁法違反・贈収賄	大	低	速い	長い
	4-3	環境規制違反	大	低	速い	中
	4-4	品質偽装・検査不正	大	低	中	長い

※リスク評価は明電グループにおける多種のリスク事象を独自に評価したものです

情報セキュリティ管理の強化

明電グループは、取り扱う情報に関するセキュリティの確保を重要な経営課題と認識し、情報資産を災害・事故・犯罪・過失などの脅威から保護します。また、情報管理を維持・向上させることで、情報の

情報セキュリティ管理体制

近年のサイバー攻撃の巧妙化を踏まえ、日々変化する脅威へ総合的に対応するため、全社的なセキュリティ体制を構築し、運用しています。製品・サービスの情報セキュリティを担うPSIRT^{※1}、社内の情報セキュリティを担うCSIRT^{※2}の配下に、工場を統括するFSIRT^{※3}、サプライチェーンのリスク低減を目指すPrSIRT^{※4}を設置し、平時とインシデント発生時の対応はこれらの専門組織を中心にを行っています。各部門には情報セキュリティを担当するSIRTマネージャーを配置し、組織内でのルール普及、教育、実施状況の点検・改善を継続的にを行っています。また、各組織との連携を促進する統括窓口(MEIDEN-SIRT)を設置し、情報セキュリティリスクや事故発生時の迅速な対応を行っています。こうした取組みは、「情報セキュリティ基本方針」に基づき、情報セキュリティ委員会を中心に推進しており、全社リスクマネジメント委員会とも連携し、不測の事態には全社BCP対策の一環として対応する体制を整えています。併せて、サイバーセキュリティインシデントによるシステム停止などを想定し

情報セキュリティ対策

サプライチェーン全体での情報セキュリティ強化に向けた活動を継続して実施しています。

●インシデント発生状況の分析と原因別対策実施

「予測／防御／検知／対応／復旧」の枠組みでセキュリティ対策を実施しています。技術的対策と人的要因対策を両面から分析し、多層防御とゼロトラストを導入する他、社外向け対策強化とインシデント対応体制も整備しました。

●情報セキュリティ教育・訓練

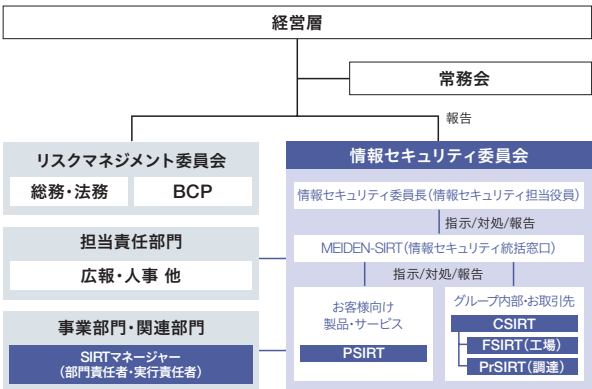
全役員・従業員を対象に情報セキュリティ教育を

漏洩・改ざん・盗難・紛失などの事件・事故防止に努めています。お客様へ提供する製品・サービスについても情報セキュリティ管理を徹底し、安全性を保っています。

たBCP強化を進め、2025年度は全社ワークショップを通じて対応・復旧上の課題を抽出しました。

当社は、サイバー攻撃や内部情報の流出・不正利用を全社重要リスクの一つとして位置付け、全社的なリスクマネジメントの枠組みの中で管理しています。情報セキュリティ委員会における審議内容や対応状況は、定期的に社長・経営層へ報告するとともに、全社重要リスクに関する議論を通じて経営レベルで監督しています。

※1 PSIRT : Product Security Incident Response Team
※2 CSIRT : Computer Security Incident Response Team
※3 FSIRT : Factory Security Incident Response Team
※4 PrSIRT : Procurement Security Incident Response Team



実施しています。ハード、ソフト、人的対策を組み合わせた総合的な情報セキュリティ対策を継続しています。

●サプライチェーンの情報セキュリティ強化

お取引先の情報セキュリティ強化活動を実施しています。SECURITY ACTION制度活用による啓発、集合教育・説明会実施、現場診断訪問、サプライヤポータルでの情報共有の4つの施策により、お取引先の情報セキュリティ対策を総合的に支援しています。