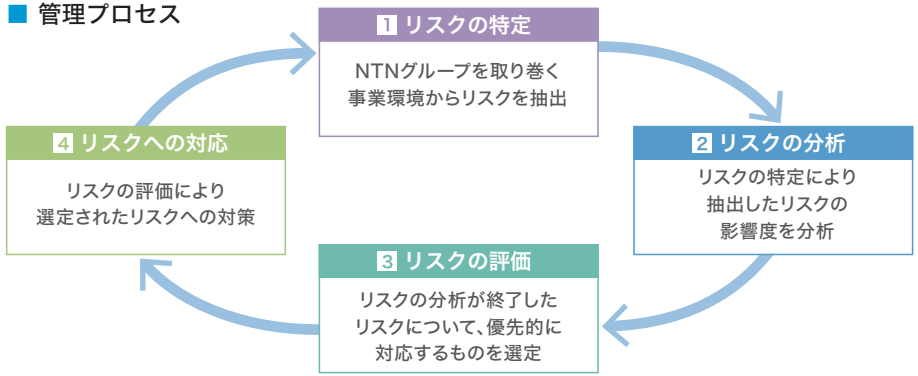
リスクマネジメント

リスク管理に関する基本的な考え方

当社グループの事業遂行を阻害する恐れのあるリスクの未然防止と発生時の対応に関する基本的な考え方を定めた「リスク管理に関する基本方針」ならびにリスク管理の組織・役割などを定めた「リスク管理規程」を制定し、グループ全体のリスク管理やBCP/BCM（事業継続計画/事業継続管理）推進に取り組んでいます。

リスクの未然防止と危機発生時の被害極小化を図ることを目的として、ESG推進部を担当する執行役（リスク管理の統括責任者）を委員長とする「リスク管理委員会」を設置し、当社グループの経営に大きな影響を与えるリスクの「特定」、「分析」、「評価」、「対応」を定期的に確認しています。リスク分類については、網羅性の観点から以下20のリスクに分類した上で、具体的なリスク内容ごとに管理責任者と推進部門を決定し、リスク低減に取り組んでいます。リスク管理委員会の審議内容については、年間2回取締役会に報告しています。

■ 管理プロセス



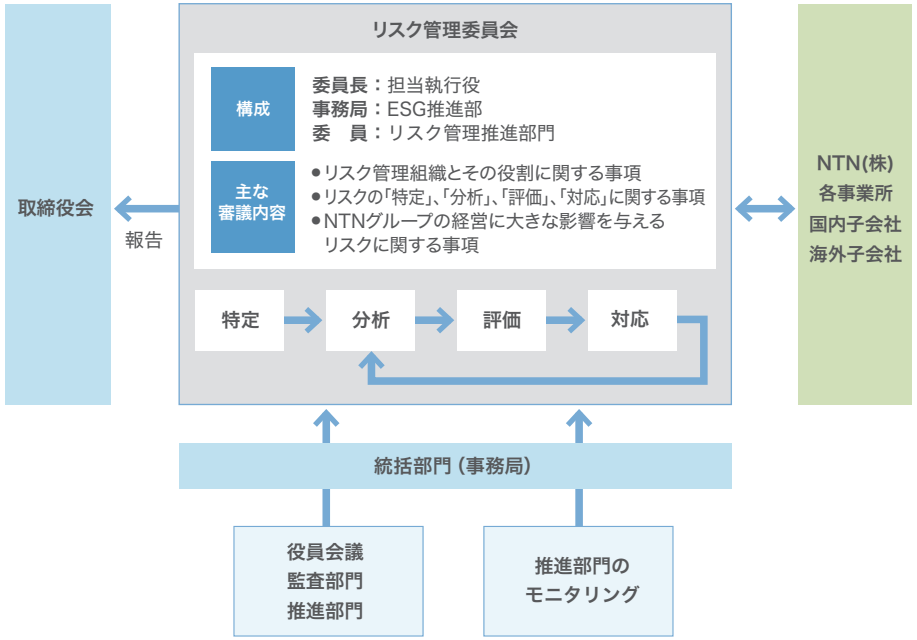
■ 対象となるリスク

1 自然災害	8 技術・研究開発	15 安全衛生
2 地政学リスク	9 調達	16 環境
3 政治経済環境変化	10 物流	17 情報システム
4 市場環境変化	11 生産・在庫	18 財務・経理
5 労働環境変化	12 品質	19 法務・コンプライアンス
6 カーボンニュートラル	13 営業・販売	20 その他
7 法令・規制の変化等	14 人事・労務	

体制図

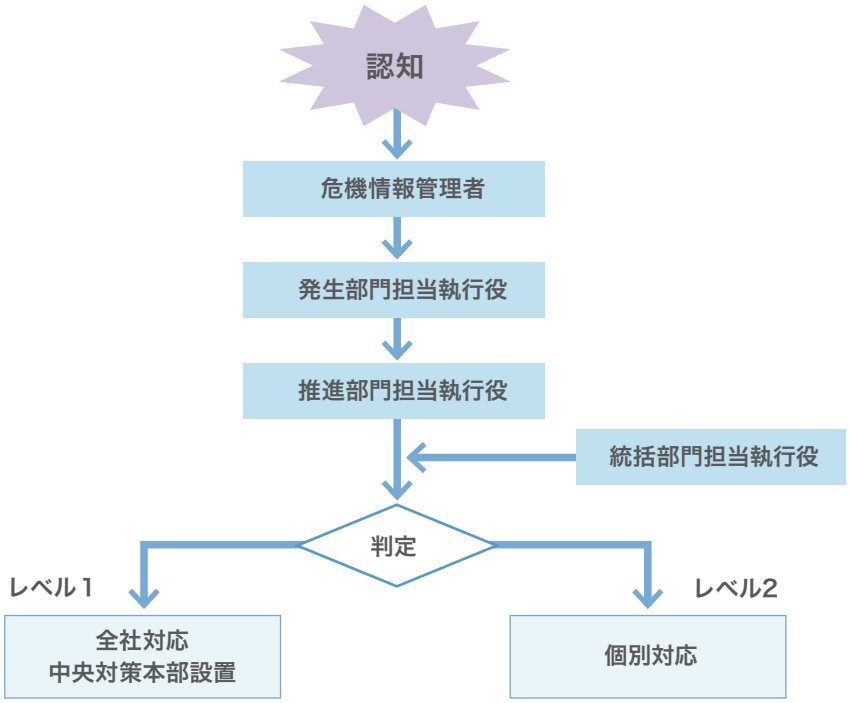
リスク管理体制は、リスク管理に関する担当執行役を統括責任者とし、統括部門、推進部門、実施部門（実務部門）で構成しており、統括部門は、リスク管理委員会の事務局として、NTNグループ全体のリスクの特定、分析、評価、対応の総括に取り組んでいます。推進部門は、担当する業務における各リスクに対する責任部門として、リスクアセスメントの実施、統括部門への報告、担当するリスクに関する規程・その他諸施策等の立案、管理体制の整備、担当するリスクについてのリスク管理に関する教育・啓発、子会社に対する指導および助言を担っています。

■ 体制図



危機管理体制

生命に関わる緊急事態、経営に影響を与える事件・事故に関わる緊急事態が発生した場合、発生部門の危機情報管理者は自部門の担当執行役へ報告します。報告を受けた当該担当執行役は、当該リスク推進部門の担当執行役、およびリスク管理統括部門の担当執行役と協議の上、緊急事態の危機対策レベルを判定します。危機対策レベルは、経営に対する影響度に応じて次の2つのレベルに区分しています。レベル1は、経営に対する影響度が極めて大きいと判断される場合を指し、判定会議にてレベル1と判断された場合は、本社に中央対策本部を設置し全社対応を行います。レベル2は、経営に対する影響度がレベル1には至らないと判断される場合を指し、緊急事態発生部門にて必要に応じて担当推進部門の協力を得て個別対応します。



BCP/BCMの推進

当社では、国内における大規模地震を想定したBCP/BCM活動に取り組み、グループ会社を含めた災害発生時の体制強化を図っています。国内すべての生産拠点で、早期に復旧するためのBCPが立案されており、令和6年能登半島地震での被災経験を踏まえて、BCP訓練に取り組み、有事の際も早急に復旧する体制の整備を進めています。加えて、地震発生から復旧までの対応を資料として取り纏め、BCM活動で活用しています。

情報セキュリティの強化

CSIRT体制の強化

サイバー攻撃や情報漏洩に対するリスクが高まる中、昨今の情報セキュリティの重要性に鑑み、「経営の基本方針」のもとに設定するNTNグループの基本方針として、「環境基本方針」、「人権基本方針」、「安全衛生基本方針」、「調達基本方針」等とともに「情報セキュリティ基本方針」を定めています。

サイバー攻撃は日々複雑化、巧妙化しており、他社でも同様の被害や情報漏洩などが数多く発生しており、情報セキュリティ事故発生時の対応においては、情報セキュリティ・リスクに対し検知から報告、対処に至るまでを迅速に行う必要があります。情報セキュリティ・リスクに対応する部門横断の緊急体制（NTN-CSIRT：NTN Computer Security Incident Response Team）を整備し、サイバー攻撃を早期に検知するため24時間365日サイバー攻撃を監視するセキュリティ専門組織（SOC：Security Operation Center）の運用とあわせ運用を開始しております。

また、人的安全管理措置の取り組みとして、情報セキュリティ事故の発生を想定したインシデント対応訓練や不正メールの対応訓練、情報セキュリティ関連規程類や、情報セキュリティの脅威への対応の理解を深めるためのeラーニングを定期的に実施しています。

［情報セキュリティ緊急対応体制（NTN-CSIRT）の整備の目的］

（1）情報セキュリティ・リスクの検知と発生時の連絡、報告、対応および復旧の迅速化
（2）情報セキュリティ事故発生のリスク低減と未然防止
（3）情報セキュリティの底上げのためのガバナンス強化

WEBサイトの関連情報　NTN基本方針