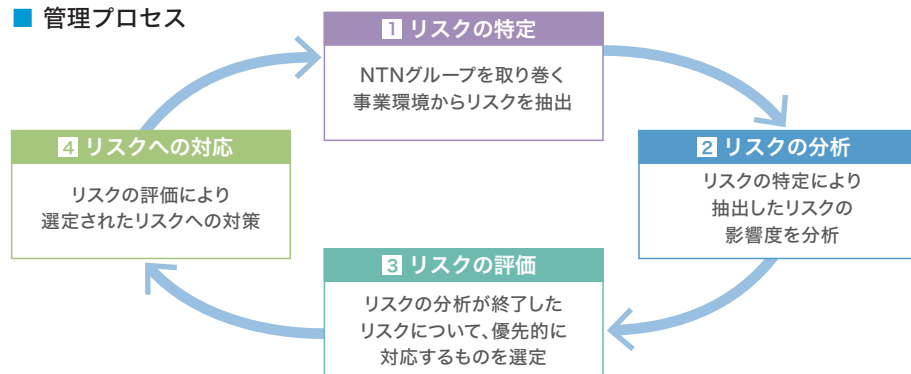


リスクマネジメント

■ リスク管理に関する基本的な考え方

当社グループは、事業の持続的成長と中期的な企業価値の向上を実現するため、事業遂行を阻害するリスクの未然防止および発生時の的確な対応を重要な経営基盤と位置づけています。この考え方のもと、「リスク管理に関する基本方針」および「リスク管理規程」を制定し、グループ全体でリスク管理およびBCP/BCM(事業継続計画/事業継続管理)を推進しています。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を委員長とする「リスク管理委員会」を設置し、経営に重要な影響を及ぼすリスクについて「特定」、「分析」、「評価」、「対応」を定期的に確認しています。リスクは20項目に体系的に分類し、管理責任者と推進部門を明確化することで実効性ある管理を行っています。これらの審議内容は年2回取締役会へ報告し、経営による監督を確保しています。

■ 管理プロセス



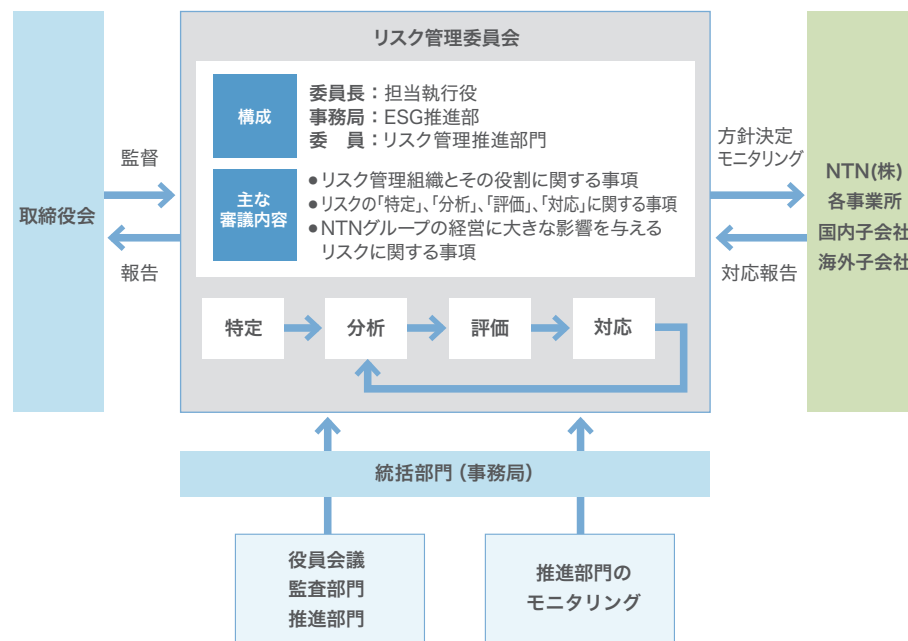
■ 対象となるリスク

- | | | |
|--------------|-----------|----------------|
| 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 情報セキュリティ |
| 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 | |

■ リスク管理体制

当社グループのリスク管理体制は、リスク管理を担当する執行役を統括責任者とし、統括部門・推進部門・実施部門で構成しています。統括部門はリスク管理委員会の事務局として、グループ全体のリスクの「特定」、「分析」、「評価」、「対応」を一元的に統括しています。推進部門は担当業務に関わるリスクの責任部門として、リスクアセスメントの実施、統括部門への報告、関連規程や諸施策の立案、管理体制の整備、担当するリスク管理に関する教育・啓発や子会社への指導・助言を実行しています。

■ 体制図

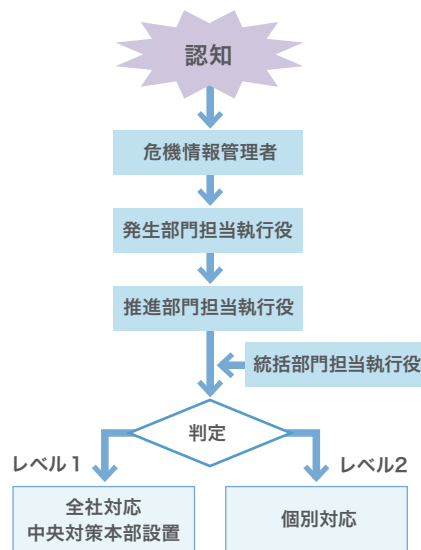


リスクマネジメント

■ 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速やかに担当執行役へ報告します。報告を受けた担当執行役は、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し、経営への影響度を踏まえて危機対策レベルを判定します。経営に対する影響度が極めて大きい場合はレベル1とし、本社に中央対策本部を設置して経営主導による全社対応を実施します。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はレベル2として、発生部門を中心に担当推進部門と連携し、迅速かつ機動的な対応を行います。

■ 緊急事態における意思決定プロセス



中央対策本部設置訓練

当社は、大地震の発生など重大な経営リスク発生時においても被災後のレジリエンスを早期に発揮し、迅速かつ的確な初動対応を行う体制の確立を重要な経営課題と位置づけています。その一環として、社長および全執行役、関係部門長が参加する中央対策本部設置訓練を実施しました。本訓練では、震度7の地震発生を想定し、上記の緊急事態における意思決定プロセスに基づく危機対策レベルの判定により中央対策本部の設置を行いました。従業員の安全確保を最優先に、安否確認や被災状況把握など実践的な対応を行うとともに、経営トップを含む意思決定層自らが危機対応を体感することで、非常時における判断の迅速性と事業継続に関するガバナンス体制の実効性を検証しました。訓練で抽出された課題は規程や手順の見直しに反映し、継続的な改善を図っていきます。これにより、重大災害時における企業価値の毀損リスク低減と事業継続力の強化につなげています。



訓練の様子

■ BCP/BCMの推進

当社は、国内の大規模地震を想定したBCP/BCM活動を通じ、グループ全体の事業継続力の向上に取り組んでいます。国内すべての生産拠点で早期復旧を可能とするBCPを整備し、令和6年能登半島地震での被災経験を踏まえた訓練を継続的に実施しています。さらに、発災から復旧までの対応プロセスを体系的に整理し、BCM活動に活用することで、有事対応力の向上と中期的な事業の安定性確保を図っています。

■ 情報セキュリティの強化

CSIRT体制の強化 セキュリティ対策のグローバル展開

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、「情報セキュリティ基本方針」を定めています。

当社は、ICT戦略部担当執行役が情報セキュリティ全体の責任者として、戦略・運用・インシデント対応を統括し、担当執行役から取締役会へ直接報告しています。また、情報セキュリティ監督機能については、執行役を統括責任者とするリスク管理委員会から取締役会へ報告する体制を確立しており、取締役会はサイバーリスク、重大インシデントなどの定期報告を監督しています。

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、グループ全体で統一されたセキュリティガバナンスの確立を目指し、地域別CSIRTの構築と展開を進めています。また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）を運用しています。

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実施しています。

[WEBサイトの関連情報](#)

[NTN基本方針](#)

