リスクマネジメント

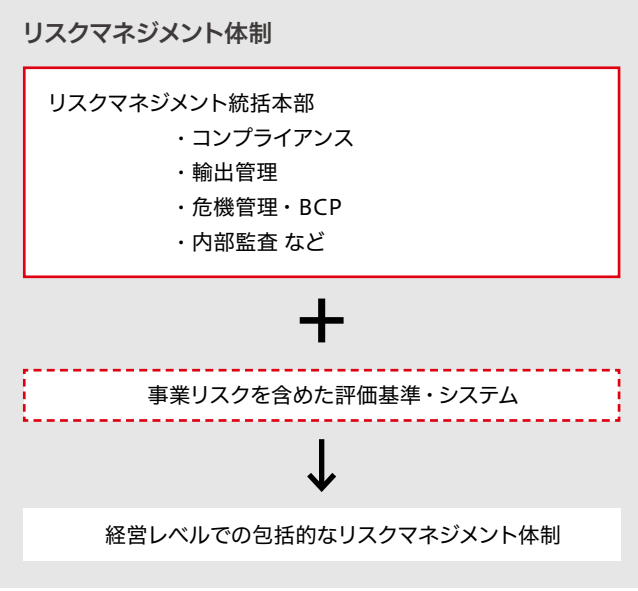
経済のグローバル化、情報通信技術（ICT）の進化・普及などの事業環境の変化は、日立の事業機会を広げるとともに、日立が対処すべき事業リスクの多面化にもつながっています。

日立は、変化を続ける経済・社会情勢を的確に捉えた上でリスク分析を実施し、問題を未然に回避する施策を講じ、同時に「万一のとき」にも迅速に対応し得る多面的な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体制の強化

日立では、昨今の複雑化するグローバルリスクに対応するため、グループ全体でリスクマネジメント体制の強化に取り組んでいます。

グループ全体のリスクマネジメントを統括する管掌役員（日立グループリスクマネジメント責任者）のもと、各事業体に経営層レベルのリスクマネジメントの責任者を設置し、コンプライアンス、輸出管理、危機管理を中心に対応し、相互に連携を図る体制をとっています。今後は、企業を取り巻くさまざまなリスクを客観的に評価する基準・システムを確立するとともに、包括的なリスクマネジメント体制を構築していきます。



日本国内外主要拠点でのBCP*策定

社会インフラに深くかかわる日立では、リスクの発生によって事業が中断し、社会に甚大な影響を及ぼすことのないよう、BCPの充実に取り組んでいます。2006年12月に「日立グループBCP策定のためのガイドライン（導入編）」を作成。2010年度にはガイドラインを英語と中国語に翻訳して日本国内外のグループ各社に提供し、大規模災害などのリスクに備えてきました。

2011年3月に発生した東日本大震災では、BCPに基づいて初期対応や意思決定を迅速に行うことができました。一方で、二次、三次のサプライヤーの把握、生産情報のクラウド化・多重化、代替輸送手段・燃料の確保などの課題が浮かび上がりました。

大震災から得たこれらの教訓を踏まえ、2011年10月に「日立グループBCP策定のためのガイドライン（部門別のBCP策定編）」を作成・配布し、BCPのさらなる充実を図りました。日本国内では2011年度末までにそれぞれの事業に応じてBCPの策定・見直しを完了し、現在、日立製作所49事業所、グループ会社96社が大規模地震および新型インフルエンザに備えたBCPを策定しています。

さらに1998年度から日本国内の主要拠点では、大規模地震を想定した地震対策シミュレーション訓練を毎年実施しています。2015年11月には日立オートモティブシステムズにおいて、リスク対策担当役員の指揮のもと、本社および3事業所（佐和、厚木、福島）を連動させ各部署の責任者・担当者がBCPに基づいて緊急時の行動計画を確認しました。

2013年度には、主要海外拠点においてもリスク対策担当責任者を配置し、約300社がBCPの策定に取り組みました。これにより大規模災害や新型インフルエンザ、政変・騒乱・テロなどの事業リスクへの対応力は強化されています。今後も、BCPの策定を拡大していきます。

* BCP（Business Continuity Plan）：事業継続計画。有事に際して基幹業務を早期に復旧し、継続して遂行するための計画。

危険地域への従業員派遣時の安全対策強化

2013年1月に発生したアルジェリア人質事件*を受けて、2013年2月、紛争やテロなどのリスクが高い地域に従業員を派遣する場合は、事前に社内外の専門家による現地調査を実施して、派遣する従業員の安全に万全を期すことを社長方針として再徹底しました。また、現地派遣後も半年に一度、現地調査を実施し、安全対策の有効性を確認しています。2014年度は、中東・アフリカの数カ国で現地調査を実施し、また2015年1月の日本人人質事件などのテロ情勢を踏まえ、迅速に従業員へ注意喚起情報を提供するなど、グローバルに活動を展開する従業員の安全確保に努めています。

さらに日立製作所は外務省主催の海外安全官民協力会議への参加や、2014年以降、テロ誘拐対策官民合同実地訓練に参加するなど、官民の連携を深めつつ、日本企業の海外安全対策に寄与する活動を行っています。

* アルジェリア人質事件：2013年1月にアルジェリアの天然ガス精製プラントが武装テロ集団に襲撃され、日本人10人を含む30人以上が犠牲となった事件。

情報セキュリティの徹底

日立では、情報セキュリティ統括責任者を委員長とする「情報セキュリティ委員会」が、情報セキュリティと個人情報保護に関する取り組み方針、各種施策を決定しています。決定事項は「情報セキュリティ推進会議」などを通じて各事業所およびグループ会社に伝達し、情報セキュリティ責任者が職場に徹底します。

日立では、情報セキュリティと個人情報保護の取り組みにおいて、特に次の2点を重視しています。

1. 予防体制の整備と事故発生時の迅速な対応

守るべき情報資産を明確にし、脆弱性評価とリスク分析に基づいて情報漏えい防施策を実施しています。事故は「起きるかもしれない」という考え方を一歩進めて、「必ず起きるものだ」という前提に立って、緊急時のマニュアルを作成し、対応しています。

2. 従業員の倫理観とセキュリティ意識の向上

担当者向け、管理者向けなど階層別にカリキュラムを用意し、eラーニングによる全員教育などを通じて倫理観とセキュリティ意識の向上を図っています。また、監査を通じて問題点の早期発見と改善にも取り組んでいます。

情報セキュリティの担当役員からのメッセージ、第三者評価・認証などのより詳細な内容は「情報セキュリティ報告書」をご覧ください。

情報セキュリティ報告書
http://www.hitachi.co.jp/csr/download/pdf/securityreport.pdf

情報資産保護の基本的な考え方