

リスクマネジメント

多面的なリスクマネジメントの推進

経済のグローバル化、情報・通信技術の進化・普及といった事業環境の変化は、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「万が一のとき」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。特に近年は、各国・地域の社会インフラ構築に深くかかわる企業として、世界経済フォーラムなどでの国際的なリスクに関する議論を踏まえて、続発するテロや激甚化する異常気象、世界規模での気候変動、サイバー攻撃の大規模化・巧妙化などを新たなリスク要因として考慮しています。さらに、製品・サービスの安定供給の徹底と事業活動に深刻な影響を及ぼすネットワークの脅威への対応強化を重視し、事業継続計画(Business Continuity Plan:BCP)の充実と情報セキュリティの継続的強化にも取り組んでいます。引き続き、リスクマネジメントの対応強化をグループ全体で推進し、事業リスクが社会に及ぼす影響の最小化を徹底しています。

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担当役員(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。

事業等のリスク

日立は、幅広い事業分野にわたり、世界各地において事業活動を行っています。また、事業を遂行するために高度で専門的な技術を利用しています。そのため、日立の事業活動は、多岐にわたる要因の影響を受けます。その要因の主なものは、次のとおりです。なお、これらは、本報告書発行日現在において合理的であると判断する一定の前提に基づいています。

- 経済の動向
- 為替相場の変動
- 資金調達環境
- 株式等の価格の下落
- 原材料・部品の調達
- 長期契約に係る見積り、コストの変動および契約の解除
- 取引先の信用リスク
- 需要と供給のバランス
- 急速な技術革新
- 人材確保
- 競争の激化
- 社会イノベーション事業強化に係る戦略
- 企業買収、合併事業および戦略的提携
- 事業再構築
- 持分法適用会社の業績の悪化
- 海外における事業活動
- コスト構造改革への取り組み
- 知的財産
- 訴訟その他の法的手続き
- 製品の品質と責任
- 大規模災害等
- 情報システムへの依存
- 機密情報の管理
- 退職給付に係る負債
- 株式の追加発行に伴う希薄化

詳細な事業等のリスクは、第149期有価証券報告書をご参照ください。
<http://www.hitachi.co.jp/IR/library/stock/index.html>

安定的な製品・サービスの提供

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、2次、3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。

また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1998年度から毎年実施しています。2018年3月には日立製作所本社において、本社対策本部長の指揮のもと、首都近郊での大規模地震を想定した初動訓練を行い、本社各部門の役割の理解促進と連携強化に取り組みました。

なお、2017年12月に、大規模地震により本社機能が一時的に停止した際の関西地区での代替本部立ち上げを前提とした行動基準を策定するなど、首都直下地震を想定した対策にも取り組んでいます。

主要海外拠点では、2013年度に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。

調達BCPの策定

日立の事業は社会インフラに深くかかわっているため、事業の共同運営者であるサプライヤーが大規模地震などの自然災害の発生によって被災した場合、日立やサプライヤーの事業活動だけではなく、社会に大きなインパクトを与える可能性があります。日本国内のビジネスユニットと主要グループ会社の調達部門では、災害発生時のインパクトを最小限にとどめるため、調達業務のBCPとして、①徹底した標準化と汎用部品の使いこなしによる調達保全リスクの極小化、②マルチサプライヤー化の推進、③製造拠点の複数分散化、④戦略在庫の予算化、⑤代替品の検討などを策定・整備しました。また策定した調達BCPが機能するかどうかを確認するため、デスクトップエクササイズ(震災被害を想定し、グループ単位でなすべき行動を議論する机上演習)も実施して、さらなる改善を進めました。

2017年度には、国内外の製造ラインを有する主要な事業所のすべて(約208サイト)が前年度までに確立した調達BCPをメンテナンスする形で強化を図り、グローバルに展開する日立グループの事業継続に貢献しています。

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。また2017年度は世界各地に拡散するテロの脅威や現地で流行している感染症に対し、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推進

情報セキュリティ方針

IoTの進展により、さまざまなモノがつながることで、新たな価値が生まれています。その一方で、日々巧妙化するサイバー攻撃の対象も従来のITからIoT・OTの分野にまで広がっています。情報漏えいや操業停止など、事業そのものの継続に支障をきたすリスクを最小化するため、情報セキュリティにかかわるリスク管理は、企業の最重要の課題の一つとなっています。

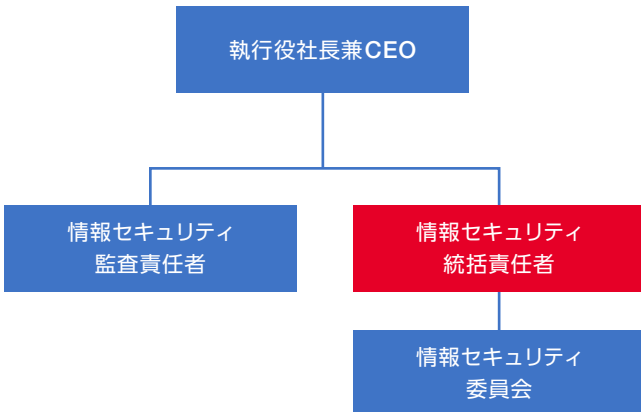
こうした背景のもと、社会イノベーション事業を展開する日立は、情報セキュリティガバナンスを最も重要な経営課題の一つと位置づけています。2018年3月に日本経済団体連合会が発表した「経団連サイバーセキュリティ経営宣言」においても、価値創造とリスクマネジメントの両面からサイバーセキュリティ対策に努めることが経営の重要課題であると述べられており、日立は同じ理念で情報セキュリティのガバナンスに取り組んでいます。

情報セキュリティ推進体制

日立製作所では、情報セキュリティおよび個人情報保護の実施・運用に関する責任・権限をもつ情報セキュリティ統括責任者を執行役社長兼CEOが任命します。

従来は、CIO*1が情報セキュリティ統括責任者の役割も担い、情報セキュリティ対策、管理を行ってきました。2017年10月より、日立全体の情報セキュリティガバナンスをさらに強化し、一括して推進するため、新たにCISO*2を任命しました。CISOは、情報セキュリティ統括責任者として、日立のすべての製品や社内設備を対象に情報セキュリティを推進する役割を担い、2017年度は執行役副社長が務めました。

情報セキュリティ推進体制図



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」が決定します。決定事項は各事業所およびグループ会社に伝達され、各組織の情報セキュリティ責任者が職場に徹底しています。

*1 CIO:Chief Information Officer

*2 CISO:Chief Information Security Officer

情報セキュリティマネジメント

情報セキュリティ管理

日立は、国際規格であるISO/IEC 27001に基づく「グローバル情報セキュリティ管理規程」を定め、情報セキュリティ管理の強化に努めています。グローバルには日本の親会社から日本国外のグループ会社に対して展開を行うとともに、米州、欧州、東南アジア、中国、インドなどの地域統括会社によるサポートとセキュリティシェアドサービスの利用を積極的に推進しています。

セキュリティ監視

日立ではサイバー攻撃の早期検知と迅速な対応のために、SOC*1による24時間365日のセキュリティ監視と、IRT*2によるセキュリティ関連情報の収集・展開とインシデント対応を行っています。

*1 SOC:Security Operation Center

*2 IRT:Incident Response Team

2017年9月以前 CIOが就任
2017年10月以降 CISOが就任

機密情報漏えいの防止

日立製作所では情報漏えいを防止するために「機密情報漏えい防止3原則」を定め、機密情報の取り扱いに細心の注意を払い、事故防止に努めています。

機密情報漏えい防止3原則

- 原則1 機密情報については、原則、社外へ持ち出してはならない。
- 原則2 業務の必要性により、機密情報を社外へ持ち出す場合は、必ず情報資産管理者の承認を得なければならない。
- 原則3 業務の必要性により、機密情報を社外へ持ち出す場合は、必要かつ適切な情報漏えい対策を施さなければならない。

情報漏えい防止の具体的施策として、暗号化ソフト、セキュアなパソコン、電子ドキュメントのアクセス制御・失効処理ソフト、認証基盤の構築によるID管理とアクセス制御、メールやWebサイトのフィルタリングシステムなどをIT共通施策として実施しています。サイバー攻撃に対しては、防御策を多層化(入口・出口対策)して対策を強化しています。

また、サプライヤーに対しては、日立が定めた情報セキュリティ要求基準に基づき、調達取引先の状況を確認・審査しています。

個人情報保護

日立製作所は、「個人情報保護方針」に基づいて構築した、日立製作所個人情報保護マネジメントシステムを運用しています。また、日立製作所ほか日本国内44事業者*がプライバシーマークを取得しています。

なお、2017年度、顧客プライバシーの侵害および顧客データの紛失に関して、個人情報の取り扱いに関する苦情・申し立てなどはありませんでした。

また、2018年5月に欧州で施行されたGDPR(欧州一般データ保護規則)など、個人情報の保護に関する法制化が各国で進んでおり、日立はその動向を注視しながら適切な取り組みを進めています。

* 2018年5月末現在

情報セキュリティ監査

日立の情報セキュリティは、日立製作所が定めた情報セキュリティマネジメントシステムのPDCAサイクルにより推進しており、すべてのグループ会社および部門に対し、1年に1回情報セキュリティおよび個人情報保護の監査を実施しています。

日立製作所における情報セキュリティ監査は、執行役社長兼CEOから任命された情報セキュリティ監査責任者が独立した立場で実施しています。221社の日本国内のグループ会社については、日立製作所と同等の監査を実施し、その結果を日立製作所が確認しています。日本国外のグループ会社についてはグローバル共通のセルフチェックを実施しています。

個人情報保護については、1年に1回、全部門が職場での自主点検として、「個人情報保護・情報セキュリティ運用の確認」を実施しています。併せて重要な個人情報を取り扱う業務(693業務*)については「個人情報保護運用の確認」を1カ月に1回実施し、安全管理措置や運用の状況を定期的に確認しています。

* 2018年3月時点の登録業務数

情報セキュリティ教育の実施

日立では、すべての役員、従業員、派遣社員などを対象に、情報セキュリティおよび個人情報保護について、eラーニングによる教育を毎年実施しています。日立製作所では約4万人が受講し、受講率はほぼ100%に達しており、そのほかにも対象別、目的別に多様な教育プログラムを用意し、情報セキュリティ教育を実施しています。また、標的型攻撃メールなどのサイバー攻撃への教育として、実際に攻撃メールを装った模擬メールを従業員に送付し、受信体験を通してセキュリティ感度を高める「標的型攻撃メール模擬訓練」を2012年より実施しています。

サイバーセキュリティは経営課題へ

2017年5月にランサムウェア*1である「WannaCry」に感染し、一部のシステムで障害などが発生しました。日立は、この事案からの学びを踏まえ、経営課題としてサイバーセキュリティ対策のさらなる強化に取り組んでいます。

ランサムウェア感染に対する初動対応

始まりは2017年5月12日の22時ごろ、データセンター内のシステムの動作が不安定となる事象でした。この時点ではウイルス感染であることは分かっておらず、システムの障害を疑って原因調査を進めていました。1時間後、ランサムウェアへの感染が確認されたため、その情報が速やかに社内のIncident Response Team (IRT)に報告され、攻撃および被害状況の把握を開始しました。

翌13日深夜1時過ぎ、IRTは把握した情報から今回の事案がランサムウェア「WannaCry」への感染によるものであると判断、経営幹部に報告し、被害拡大防止の初動対応に着手しました。同日の5時過ぎに日立グループ全社への緊急対策指示を展開、9時に本社に緊急対策本部を設置して、被害状況の把握と、復旧に向けた対策および感染ルートの分析を開始しました。

事案を通して学んだこと

ランサムウェア感染事案への対策を通して学んだことが4点あります。

1点目は、ネットワーク内で一気に拡散するサイバー攻撃の脅威です。社内のネットワークに接続される機器は、パソコンやサーバーなどOA機器だけでなく、現場の開発・生産用設備などのOT機器にまで広がっています。今回の事案では、セキュリティパッチ*2が自動適用されていないOA機器や、そもそも適用が慣習化されていないOT機器など、セキュリティが弱い箇所からウイルスに感染し、ネットワーク内で一気に拡散して被害の拡大につながりました。

2点目は、サーバーなどOA機器のセキュリティ対策徹底の重要性です。業務システムが稼働している場合、業務の調整ができずシステムを止められないといった理由から、タイムリーなセキュリティパッチの適用ができていなかった機器が感染の被害を受けました。

3点目は、OT機器のセキュリティ対策の困難さです。これらの機器にはそもそもセキュリティパッチの適用が想定されていないものも多く、また導入後にシステムをアップデートする必要性を意識していない、という実状がありました。

4点目は、サイバー攻撃を想定したBCP(事業継続計画)強化の必要性です。「絶対の安全はない。有事の際には影響を限定し、いかに早く元に戻すか」という考えのもと、ランサムウェアなどのサイバー攻撃についても、災害などと同様に日ごろから最悪のシナリオを想定して手順書の整備やトレーニングを行い、現場力を向上しておくことが必要です。

このような課題への対応には、技術的な側面に加えて、事業の継続性を観点とする経営視点での総合的なリスク分析と対策の判断が必要となります。

昨今のサイバー攻撃の高度化に加えて、ヒューマンエラー、内部不正、環境変化など情報セキュリティを取り巻く脅威は年々増加し、事案の発生による経営インパクトは大きくなっています。日立は、今後も重要な経営課題の一つとして、組織・運用・システムのバランスを考慮したサイバーセキュリティ対策の強化と耐性の向上に取り組んでいきます。

*1:感染したコンピューターに特定の制限をかけて、その制限の解除と引き換えに金銭などを要求するコンピューターウイルスの一種

*2:コンピューターのプログラムに不具合や脆弱性が発見された際に、それらの問題を修正するために提供されるプログラム

気候関連のリスクと機会への取り組み

日立は、気候変動に関する「リスク」と「機会」を重要な経営課題と認識しています。「リスク」と「機会」を検討するためのガバナンスとしては、気候変動にかかわるグローバルな法規制や政策動向を踏まえ、気候変動のリスクを最小化し、機会を生かす事業戦略を立案するために、執行役社長兼CEOを議長、経営層をメンバーとする「サステナビリティ戦略会議」を設置しています。

2017年には、G20財務大臣・中央銀行総裁会議の要請を受けて、金融安定理事会(FSB)により設置された気候関連財務情報開示タスクフォース(TCFD)により、企業のリスクと機会についての情報開示を求める提言が公開されました。日立は、2018年6月にTCFDへの賛同を表明し、TCFDの要請に基づいた情報開示を進めています。日立では、環境関連のリスクと機会の認識について、グローバルでの新たな要請であるTCFDの分類に合わせて、気候関連のリスクを①低炭素経済への移行に関連したリスク、②気候変動の物理的影響に関連したリスクに分類し、検討を進めています。機会については、日立の提供する製品・サービスの省エネルギー化により低炭素社会の構築に貢献していくことが大きな機会であると位置づけ、今後もその拡大に向けた議論を進めていきます。

低炭素経済への移行リスク

政策および法規制

炭素税や燃料・エネルギー消費への課税、排出権取引などについては、各国・地域の制度・規制の遵守に加え、今後も新設や強化が進む可能性があり、経営コストに直結するリスクと想定しています。

日立はこれらのリスクに対して、生産の効率化や省エネルギー化を進めることにより、コスト負担の軽減や最小化を図っており、2017年度は約54億円の省エネルギー投資を行いました。また、製品のエネルギー効率の基準や規制は、基準値を満たしていない場合、市場での販売機会を失うリスクになるため、既存の規制や基準の遵守を徹底するとともに、常に法規制動向の把握に努め、政策立案の機会などにも参画しています。

技術

日立のバリューチェーン全体の中で多くを占める、販売した製品・サービスの使用に伴うCO₂排出量を削減していくには、製品・サービスのさらなる省エネルギー化を実現する技術が必須です。

そのため、日立では、製品・サービスの設計・開発段階において「環境配慮設計アセスメント」を適用することで、ライフサイクルの各段階におけるさまざまな環境側面を評価し、環境に与える負荷の低減を図っています。さらに、長年取り組んできた幅広い社会インフラの技術をOT(制御・運用技術)やITと組み合わせることで、最適なソリューションを提供し、事業機会の創出につなげています。

市場・評判

気候変動問題への企業の取り組み姿勢に対するステークホルダーからの評価や、気候変動対策を重要視するなどの市場の価値観の変化は、お客様の製品・サービス選択の意思決定に影響し、事業継続のリスクになる可能性があります。日立はバリューチェーンにおけるCO₂排出量を2010年度比で2030年度に50%、2050年度に80%削減する環境長期目標を掲げ、省エネルギー投資による高効率設備・機器への更新、デジタルライゼーションによる生産の効率化を進めています。

気候変動の物理的影響に関連したリスク

急性・慢性

気候変動による物理的リスクには、台風や洪水などの激化による急性リスク、海面上昇や長期的な熱波の原因になり得る気候パターンによる慢性リスクがあります。グローバルに事業拠点を置いている日立にとって、台風の大型化や降水量の増加など、気候変動の影響と考えられる気象現象による災害は事業継続のリスクになると考えています。

これらのリスクに対しては、工場新設時に洪水被害を念頭に置いて立地条件や設備の配置などを考慮するほか、災害発生時の対策を取り決めた「日立グループBCP策定のためのガイドライン」を活用し、リスクの軽減に努めています。

気候関連の機会

資源の利用効率

日立は、廃棄物の発生抑制や再生利用などにより資源の効率的な利用を推進しています。また、天然資源の効率的で持続可能な利用を図るため、省資源設計や生産プロセスでの改善などにより、天然資源投入量の最小化に向けた取り組みも推進しています。

エネルギー源

日立は、工場やオフィスにおいて、再生可能エネルギーを積極的に活用しています。工場では、生産ラインのエネルギー使用状況を把握・管理し、蓄電池を活用することで、発電量の変動が大きい太陽光発電設備から供給される電力を有効に利用しています。また、再エネクレジットの導入を推進するとともに、インターナルカーボンプライシングや、自家消費型太陽光発電の導入拡大を進めています。オフィスにおいても、照明や空調設備の高効率化を進めるとともに、エネルギーの見える化やBEMS*による建屋全体のエネルギー使用量の最適化を行っています。事業においては、風力発電などによる再生可能エネルギーなどを積極的に提供することで、事業機会の創出につなげています。

* BEMS: Building and Energy Management System (ビル・エネルギー管理システム)のことで、ビルの室内環境とエネルギー性能の最適化を図るためのシステム

製品およびサービス・市場

気候変動の緩和および適応への貢献が期待できる革新的な省エネルギー技術を有する製品・サービスの提供を拡大することは、市場価値や収益増大の機会を創出することにつながると考えています。エネルギーを使う製品を多く扱う日立にとって、気候変動問題の解決への貢献は、製品・サービスの効率向上による低炭素化が重要になります。そのため日立は、高効率プロダクトや低炭素エネルギーの開発・普及、環境負荷の削減に寄与する革新的なデバイス・材料の開発を推進しています。2017年度は、研究開発全体で3,329億円の投資を行っています。

また、気候変動問題への企業の取り組み姿勢は、ステークホルダーからの評価や、お客様の製品・サービス選択の意思決定に影響するため、製品のエネルギー効率の基準や規制を満たすだけでなく、基準値を上回る省エネルギー性能の製品・サービスのさらなる開発・提供により、お客様に選ばれる機会を増やすことをめざしていきます。

レジリエンス

日立の主要な工場においては、停電発生時などでも再生可能エネルギーや蓄電池の活用によって重要な機能を維持できるように対策を講じています。

事業においては、各国・地域において増加する自然災害対策のため、防災ソリューションを提供することで貢献しています。日立は、長年培ってきた高度なITを活用して、生活情報や天候などの自然情報や、社会インフラシステムの稼働情報などを分析・評価する、気候変動への適応に資するさらなるソリューションの提供を推進していきます。