多面的なリスクマネジメントの推進

日立のアプローチ

経済のグローバル化、情報通信技術（ICT）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（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。

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。2017年3月には日立化成において、本社対策本部長の指揮のもと、本社および名張事業所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危機管理スキル向上とBCPの改善課題の把握に取り組みました。

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。


日立グループBCP策定のためのガイドライン(部門別)


地震対策シミュレーション訓練

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(BU)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。

2016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200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*1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2016年度は世界各地に拡散するテロの脅威に対し、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。

*1 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

情報セキュリティの徹底

日立では、執行役社長がISMS*1の実施および運用に関する責任および権限をもつ情報セキュリティ統括責任者としてCIO*2を任命しており、2016年度は執行役専務が務めています。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ています。

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。

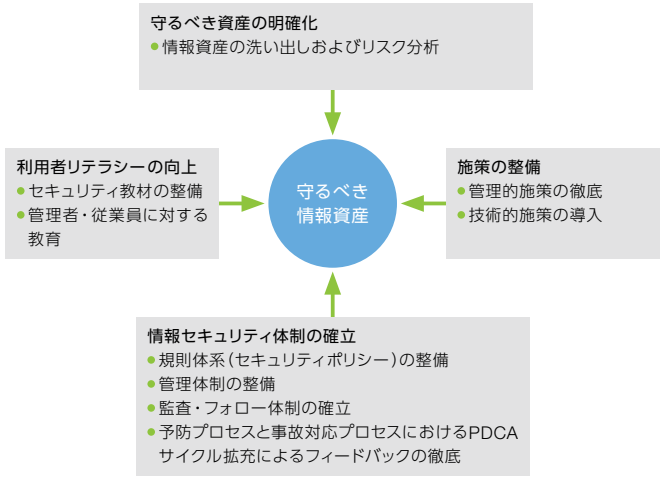
1. **予防体制の整備と事故発生時の迅速な対応**
   守るべき情報資産を明確にし、脆弱性評価とリスク分析に基づいて情報漏えい防止施策を実施しています。事故は「起きるかもしれない」という考え方を一歩進めて、「必ず起きるものだ」という前提に立って、緊急時のマニュアルを作成し、対応しています。
2. **従業員の倫理観とセキュリティ意識の向上**
   担当者向け、管理者向けなど階層別にカリキュラムを用意し、eラーニングによる全員教育などを通じて倫理観とセキュリティ意識の向上を図っています。また、監査を通じて問題点の早期発見と改善にも取り組んでいます。

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2016」に記載しています。

*1 ISMS(Information Security Management System):情報セキュリティマネジメントシステム
*2 CIO(Chief Information Officer):情報セキュリティ統括責任者

情報セキュリティ報告書2016

情報資産保護の基本的な考え方



情報セキュリティ教育の実施

情報セキュリティを維持していくためには、一人ひとりが日々の情報を取り扱う際に必要とされる知識を身につけ、高い意識をもつことが重要です。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%に達しています。そのほかにも、新入社員、新任管理職や情報システム管理者などを対象とした座学教育など、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、最近増加している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。

日立製作所の教育コンテンツは日本国内外のグループ会社に公開しており、日立全体として情報セキュリティ・個人情報保護教育に積極的に取り組んでいます。

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。また万が一、事故が発生した場合は、迅速にお客様に連絡し、監督官庁に届け出るとともに、事故の原因究明と再発防止対策に取り組み、被害を最小限にとどめるよう努めています。

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。昨今多発している標的型メールなどのサイバー攻撃に対しては、官民連携による情報共有の取り組みに加え、IT施策においても防御策を多層化(入口・出口対策)して対策を強化しています。

また、サプライヤーと連携して情報セキュリティを確保するため、機密情報を取り扱う業務を委託する際には、あらかじめ日立が定めた情報セキュリティ要求基準に基づき、調達取引先の情報セキュリティ対策状況を確認・審査しています。さらに、サプライヤーからの情報漏えいを防止するために、サプライヤーに対して、情報機器内の業務情報点検ツールとセキュリティ教材を提供し、個人所有の情報機器に対して業務情報の点検・削除を要請しています。なお、2017年5月、ワーム型ランサムウェアにより一部の社内システムに不具合が生じ、メール送受信などに一時影響が出ましたが、情報漏えいは確認されず、お客様や社外への被害拡大はありませんでした。

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。

ランサムウェアによる被害および復旧状況について

情報セキュリティ管理をグローバルに展開

日本国外のグループ会社については、国際規格であるISO／IEC 27001に則った「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。日本の親会社から日本国外のグループ会社に対してビジネスチャネルによる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することで、セキュリティ対策の徹底を図っています。

情報セキュリティ監査・点検の徹底

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います。日立では、すべてのグループ会社および部門で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監査は、執行役社長から任命された監査責任者が独立した立場で実施。監査員は自らが所属する部署を監査してはならないと定め、監査の公平性・独立性を確保するようにしています。

日本国内のグループ会社(222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、日立全体として監査・点検に取り組んでいます。また、職場での自主点検として、全部門が「個人情報保護・情報セキュリティ運用の確認」を1年に1回実施しています。併せて重要な個人情報を取り扱う業務(654業務*1)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。

*1 2017年3月時点の登録業務数