情報セキュリティ

基本的な考え方

デジタル化の進展により、新たな価値が生み出される一方で、日々巧妙化するサイバー攻撃による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が大きくなっています。この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マネジメントは、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のグローバルリーダーをめざす日立は、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を重要な経営課題の一つと位置づけ、情報セキュリティに取り組んでいます。

テーマ	概要
情報セキュリティ	日立は、情報セキュリティ方針に基づき、情報セキュリティ統括責任者であるChief Information Security Officer（CISO）のもと、“One Hitachi”として一体感と迅速性を重視し、最適なセキュリティ構築を進めています。具体的には、情報漏えいの防止に向けた取り組み、社内情報セキュリティ教育の推進、情報セキュリティの内部監査などに取り組んでいます。
サイバーセキュリティ	サイバー攻撃手法の多様化に伴うリスクに対応するため、セキュリティリスクのマネジメント範囲を拡大し、製品・サービスを作り出すための開発・検証環境や生産・製造環境、サプライチェーンや製品・サービスの開発プロセスにおいて事業のリスク低減に取り組んでいます。
データプロテクション	「安心・信頼を提供する」、「個人の権利を大切にする」という個人情報保護に関するビジョンを定め、グローバル社会の一員として個人情報保護に取り組んでいます。

Governance

コーポレートガバナンス
企業倫理・コンプライアンス
リスクマネジメント
情報セキュリティ
エグゼクティブサマリー
情報セキュリティ
ガバナンスデータ

情報セキュリティ

情報セキュリティの考え方

考え方

デジタル化の進展により、新たな価値が生み出される一方で、日々巧妙化するサイバー攻撃による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が大きくなっています。この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マネジメントは、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のグローバルリーダーをめざす日立は、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を重要な経営課題の一つと位置づけ、情報セキュリティに取り組んでいます。日立は数多くの会社が集まり構成されていることから、“One Hitachi”のもと、グループ一体となって事業を推進しています。この事業方針と呼応して、情報セキュリティに関しても、“One Hitachi”として取り組み、共通の施策に基づいて、一体感と迅速性を重視し、最適なセキュリティ構築を加速させていきます。

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

情報セキュリティの方針

方針 GRI 2-23

日立は、お客さまからお預かりした情報やそれを保管するシステム、また、社会インフラのサービスを行う情報システムなどさまざまな守るべき情報資産を保護するために、情報セキュリティに関する方針を定め、その方針に基づき各種規則、推進体制を確立し、情報セキュリティマネジメントに取り組んでいます。

情報セキュリティの方針

1. 情報セキュリティ管理規則の策定および継続的改善
2. 情報資産の保護と継続的管理
3. 法令・規範の遵守
4. 教育・訓練
5. 事故発生予防と発生時の対応
6. 企業集団における業務の適正化確保

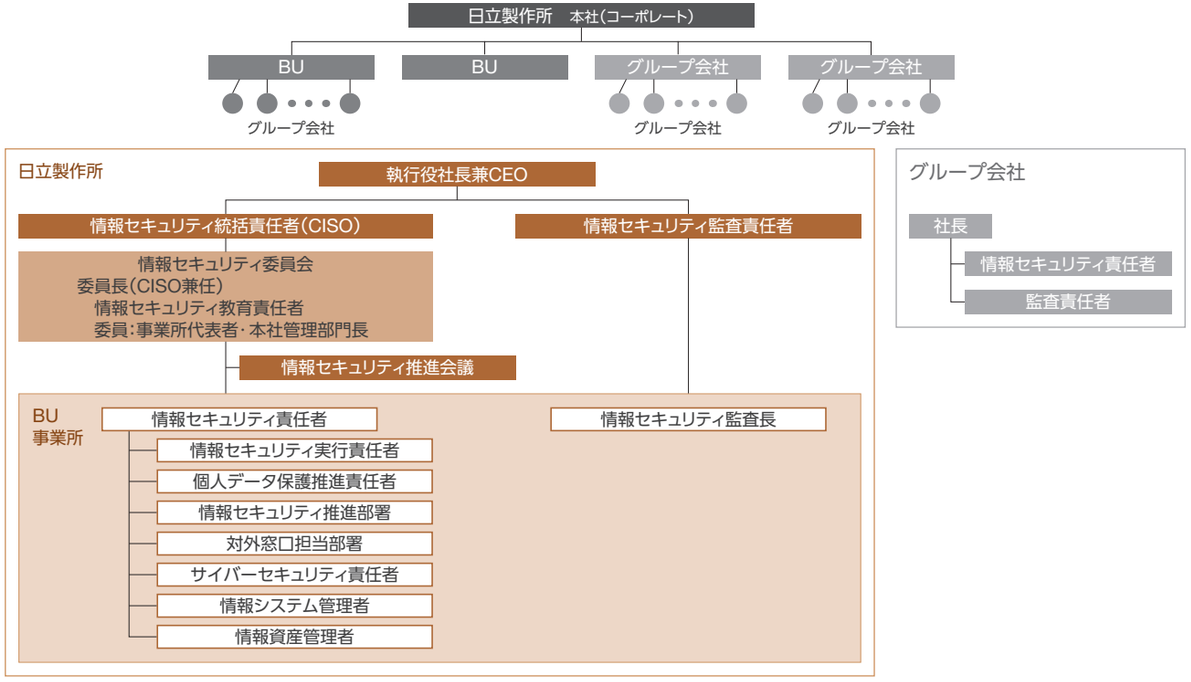
情報セキュリティ推進体制

体制 GRI 2-13／2-24／3-3

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であるChief Information Security Officer（CISO）は、日立のすべての製品・サービス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っています。

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、CISOを委員長とする「情報セキュリティ委員会」

情報セキュリティ推進体制図



が決定し、「情報セキュリティ推進委員会」などを通じて、各事業所およびグループ会社に伝達されます。ビジネスユニット(BU)・事業所は、情報セキュリティ推進部署を設置し、原則BU長・事業所長を情報セキュリティ責任者として、各職場における情報セキュリティの徹底や従業員への教育などを行います。グループ会社でも同様の組織を設け、互いに連携して横断的な情報セキュリティを推進しています。

情報セキュリティマネジメント

活動・実績

日立は国際規格であるISO／IEC 27001を元に、情報セキュリティマネジメントを構築してきました。また、昨今のサイバー攻撃の激化を鑑み、米国政府基準SP800-171に対応した「情報セキュリティ対策基準」により、情報セキュリティの強化に努めています。本基準を含めた、「情報セキュリティ・個人情報保護関連規則」を日立製作所および各グループ会社の本社からグローバルに展開するとともに、米州、欧州、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ードサービスの利用を推進しています。

情報漏えいの防止

日立は、情報漏えい防止のために、デバイス暗号化、セキュリティPC、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。標的型攻撃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に加え、多層防御などさまざまなIT対策を強化しています。

また、調達パートナー側からの情報漏えいを防止するために、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、調達パートナー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、調達パートナーに対して、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。

情報セキュリティ教育の実施

日立は、すべての役員および従業員を対象に、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。2022年度の日立製作所における受講率は100%(休職者など受講不可能な者を除く)に達しています。その他にも、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、標的型攻撃メールなどのサイバー攻撃に対する教育として、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」を実施しています。

日立製作所の教育コンテンツはグループ内に共有し、日立全体で情報セキュリティ・個人情報保護教育に積極的に取り組んでいます。

情報セキュリティマネジメントの評価とモニタリング

日立の情報セキュリティとデータ保護の活動は、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、情報セキュリティとデータ保護に関するマネジメントや対策が各部門で適切に実施されているかを評価・モニタリングするために、定期的な監査や点検を実施しています。

日立製作所および国内グループ会社の全部門では、年に1回、個人情報保護および情報セキュリティの内部監査を実施しています。日立製作所での内部監査は、執行役社長兼CEOから任命された監査責任者が独立した立場で実施しています。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・独立性を確保しています。国内のグループ会社は、日立製作所と同等の内部監査を実施し、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の実施を義務付け、日立グループ全体として点検に取り組んでいます。また、日立製作所全部門が「個人情報保護・情報セキュリティ運用の確認」の自主点検を1年に1回実施しているほか、重要個人情報を取り扱う業務(739業務*1)部門では「個人情報保護運用の確認」を1カ月に1回実施するなど、運用状況を定期的に確認しています。

また日立は、日立グループ全体の情報セキュリティ対策の状況について、社内のセキュリティ専門チームによる現場のアセスメントを定期的に行い、セルフチェックとの乖離を確認することで、セキュリティリスクの低減活動に取り組んでいます。さらに、日立製作所および国内のグループ会社では、社外に公開しているサーバーなどの外見脆弱性調査を外部機関により四半期に1回実施しています。

*1 2023年3月時点の登録業務数

Note: 日立では、調達先(いわゆるサプライヤー、ベンダー、プロバイダー等)を「対等な立場で一緒にビジネスをつくり上げるパートナー」に位置づけており、「調達パートナー」と表現しています。

サイバーセキュリティの取り組み

活動・実績

サイバー攻撃手法の多様化に伴い、インシデントの発生源や影響が拡大する中、こうしたリスクに対応するため、日立は、これまでのOAで利用する社内IT環境対策が中心であったセキュリティリスクマネジメントの範囲を拡大し、製品・サービスを作り出すための開発・検証環境や生産・製造環境、サプライチェーンや製品・サービスの開発プロセスに対しても対象を広げ、事業のリスク低減に取り組んでいます。

サイバーセキュリティマネジメント

日立は、社内IT環境に関する脆弱性対策やネットワークセキュリティなどの基準を定め、BU／グループ会社に対して、対策状況の定期的な確認と是正を求めています。また、全社共通の施策として、各機器の脆弱性対策状況の監視とユーザ／管理者へのフォローアップを行う取り組みを開始し、適用拡大を図っています。

開発・検証環境、生産・製造環境においては、各環境のセキュリティ遵守のための環境構築や運用に関する基準やガイドラインを整備し、日立グループ内でガイドラインに基づいた対応を進めています。また、調達パートナーに対しては、日立が定めた情報セキュリティ要求基準を共有し、連携してセキュリティを強化しています。

製品・サービスについては、製品・サービスのセキュリティを対策・維持するためのマネジメント指針を策定し、日立グループ内でこの指針に基づいた対応を進めています。

サイバーセキュリティ監視

日立は、グローバル規模のサイバー攻撃の早期検知と迅速な対応のために、セキュリティオペレーションセンター（SOC）による24時間365日のセキュリティ監視、インシデントレスポンスチーム（IRT）による脅威情報の収集・展開とインシデント対応を行っています。

サイバー攻撃の手法は年々巧妙化し、検知システムを掻い潜られ、発覚まで長期化して被害が拡大する傾向にあります。その中で、日立は、EDR*1の導入による機器の動作監視や、認証保護のための監視を実装し、サイバー監視強化を図っています。今後も最新のテクノロジーを取り入れたサイバー監視環境の改善・強化を進めていきます。

*1 EDR(Endpoint Detection and Response)：コンピュータなどのエンドポイントデバイスにおける不審な動作や攻撃を監視し、迅速な対応を行うためのシステム

データプロテクションの取り組み

活動・実績

GRI 418-1

デジタルテクノロジーの進展に伴いグローバルでのデータの利活用が急速に進む中、個人情報の保護や国境を越えたやり取りへの関心も高まっています。そのような環境の中、日立はお客さまからお預かりした個人情報や、事業運営にかかわる個人情報を確実に管理するため、個人情報保護の取り組みを重視しています。「安心・信頼を提供する」、「個人の権利を大切にする」という個人情報保護に関するビジョンを定め、グローバル社会の一員として個人情報保護に取り組んでいます。

個人情報保護の取り組み

日立製作所は「個人情報保護方針」を定め、役員および従業員に周知するとともに一般に広く公表しています。また、当該方針に基づいて構築した、日立の個人情報保護マネジメントシステムにより、個人情報の適切な管理、全従業員を対象とする教育および定期監査などを実施し、個人情報の保護に努めています。事前の同意を得ずに、個人情報を第三者に提供することはなく、事前の同意をいただいた場合には、データを提供する第三者に対して、日立製作所の個人情報保護方針の遵守を求めています。

グループ会社においても各社の「個人情報保護方針」に基づき、各国・地域の法令および社会的な要請に合わせた個人情報の保護に取り組んでいます。

日立製作所 個人情報保護方針
https://www.hitachi.co.jp/utility/privacy/index.html

Note: 日立では、調達先(いわゆるサプライヤー、ベンダー、プロバイダー等)を「対等な立場で一緒にビジネスをつくり上げるパートナー」に位置づけており、「調達パートナー」と表現しています。

プライバシーマークの取得

日立製作所は、個人情報保護に関する第三者認証であるプライバシーマーク*1を取得しています。また、グループ全体で個人情報の保護に取り組んでおり、日本国内では2023年7月末時点で、37事業者がプライバシーマークを取得しています。

*1 プライバシーマーク：外部審査機関が適切に個人情報の安全管理・保護措置を講じていると認めた事業者に付与する第三者認証（付与機関：一般財団法人日本情報経済社会推進協会）。

プライバシー保護の取り組み

日立製作所は、プライバシー保護対策に対する社会的要請から、プライバシー保護と個人データ活用を両立することで、より適切で高品質なサービスや製品を提供し、消費者をはじめとするステークホルダーとの信頼を醸成することをめざしています。

これまで、2014年からデジタル事業を牽引するデジタルシステム&サービスセクターにおいて、個人データの取り扱いを統括する「パーソナルデータ責任者」と、プライバシー保護に関する知見を集約してリスク評価や対応策検討を支援する「プライバシー保護諮問委員会」を設置し、プライバシー保護に関する取り組みを進めてきました。

さらに、2023年から日立プライバシー保護（PIA）制度を導入することで、全社をあげた取り組みを開始しました。

これらの取り組みを通じて、従業員は個人データを取り扱う業務においてプライバシー影響評価を実施することでプライバシーにかかわる問題の発生を防ぐための対策を講じています。

グローバルな個人情報保護関連法制度への対応

プライバシーリスクの高まりを受け、世界各国・地域で関連法制度の制定・改定の動きが活発になっています。日立は、グローバル全体で法制度の遵守を徹底し、関連法制度や社会動向をモニタリングして、適切な措置を講じています。

日本国内では、改正個人情報保護法における漏えいなどの報告、本人への通知の義務化に対応し、万が一、個人の権利・利益を害するおそれがある漏えいが発生した場合には、速やかに個人情報保護委員会へ報告し、本人に通知します。なお、2022年度の日立製作所の個人情報の漏えいなどの事案は1件でした。本事案については、影響範囲を特定し、適切な対応を実施しました。

また、欧州一般データ保護規則（GDPR）をはじめとする、海外の関連法制度に配慮したグループ共通のプライバシー保護に関する行動規範を制定し、2022年4月より施行しています。さらに、グループ全社で個人データ保護推進責任者を選任するとともに、地域統括会社に地域グループ会社支援機能を構築し、グローバルで個人情報保護の徹底を図っています。

第三者評価・認証

活動・実績

日立は、情報セキュリティマネジメントに関する第三者評価・認証の取得を推進しています。日立は、一般社団法人情報マネジメントシステム認定センター（ISMS-AC）から、情報セキュリティマネジメントシステム国際規格（ISO／IEC 27001）に基づくISMS認証を日立製作所の8部門、グループ会社23社の28部門*1で取得しています。

*1 2023年6月末時点