

HITACHI

情報セキュリティ報告書 2026



日立グループ

INDEX

CD&SOメッセージ	1
情報セキュリティの考え方	2
情報セキュリティマネジメント	8
情報セキュリティマネジメントシステム	8
情報セキュリティ強化の取り組み	14
サイバーセキュリティの取り組み	17
サイバーセキュリティマネジメント	17
サイバーセキュリティ対策	22
SIRT活動	25
データ保護の取り組み	28
個人情報保護の取り組み	28
プライバシー保護の取り組み	34
情報セキュリティに関する社内外活動	35
情報セキュリティ啓発活動	38
コラム OTシステムと機器を守るAI活用セキュリティ検証技術	40
第三者評価・認証	42
日立グループの概要	45

〈本報告書の概要〉

- 報告範囲・期間:2025年度までの日立グループにおける情報セキュリティの取り組み
- 報告書の発行時期:2026年9月発行

CD&SOメッセージ

株式会社 日立製作所
執行役常務
Chief Digital & Security Officer (CD&SO)
藤森 聡子



デジタル活用のスピードと信頼性を両立し、 お客さまと社会に安心・安全を提供

サイバーセキュリティやIT、AIを取り巻く環境は日々刻々と変化しています。特にサイバー攻撃は、AIを悪用したものなど、より急速に高度化・巧妙化しています。このような状況下においても、日立は社会イノベーション事業を通じて、社会やお客さまに安心・安全な価値を提供する使命を担っています。

この使命を果たすため、日立のIT部門とセキュリティ部門は連携を一層強化し、サイバー攻撃に対する防御施策の推進、堅牢なデジタル基盤の提供、グループ全体のIT・セキュリティガバナンスの高度化に取り組んでいます。また、AIの徹底活用を前提とした業務・プロセスの見直しやデジタル基盤およびサイバーレジリエンスの強化により、迅速かつ柔軟な意思決定を支援し、日立の経営計画「Inspire 2027」の実現に貢献してまいります。

情報セキュリティの分野では、日立は攻撃者の視点を取り入れたリスク分析を起点に、優先度の高い対策を迅

速かつ継続的に実行していきます。グループ全体で変化に即応できる体制を整え、ガバナンスを強化するとともに、AIを活用した防御技術の高度化にも取り組みます。さらに、自らが先行してサイバーセキュリティ施策を実践する「Customer Zero」の考えのもと、社内で価値を実証し、その知見や成果を日立グループ内で共有するとともに、お客さまにも提供することで、実践に裏付けられたセキュリティ強化を広く展開していきます。

日立は、ITとセキュリティが一体となった戦略の立案・統制を進め、日立グループにおけるデジタル活用の加速と情報セキュリティリスクの最小化を図ります。変化に柔軟に対応できる体制と、確かな安全性を備えたデジタル環境を整えることで、デジタル活用のスピードと信頼性を両立し、今後の事業成長を支える基盤をさらに強化していきます。

情報セキュリティの考え方

日立は、日々変化する事業環境を把握・分析し、社会的課題や競争優位性、経営資源を踏まえたリスクマネジメントを実施しています。これにより、備えるべきリスクへの対応と成長機会の創出を両立し、リスクをコントロールしながら収益機会の拡大を図っています。

その中でも情報セキュリティを取り巻く環境は、大きく変化しています。世界的にサイバー攻撃が拡大しており、その影響は自社にとどまらず、バリューチェーン全体や社会問題へと広がる事案が増加しています。

加えて、AIの悪用により攻撃は量的・質的な高度化が進んでおり、企業におけるリスクは増大しています。このリスクを最小化するため、情報セキュリティにかかるリスクマネジメントは、企業の重要な経営課題の一つとなっています。こうした背景から、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やデータ保護などの各種情報セキュリティ対策に取り組んでいます。

経営戦略としての情報セキュリティ

日立では、2025年に策定した日立の経営計画「Inspire 2027」において、「日立グループの情報セキュリティを維持、向上させること」を目標に設定し、情報セキュリティに取り組んでいます。この目標の達成に向けて、日立製作所のデジタル&セキュリティ統括本部（以下、情報セキュリティ統括部門）が、毎年、経済産業省のサイバーセキュリティ経営ガイドラインなどを参照し作成した「サイ

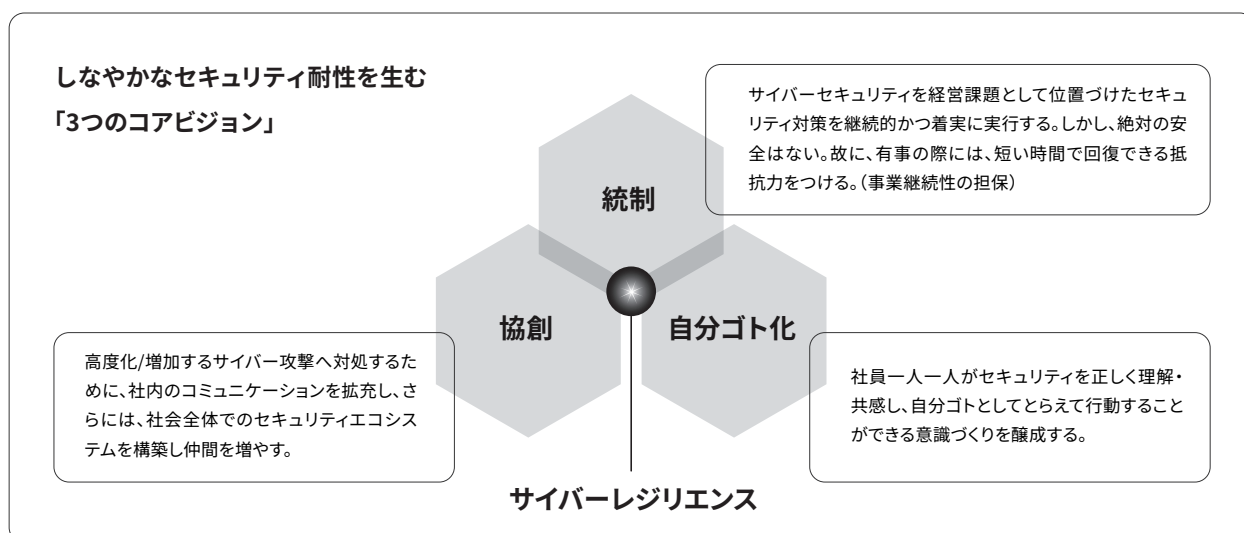
バーセキュリティスコア」をもとにセキュリティ施策を自己評価し、その結果にもとづいた対策を実行しています。

また、経営視点でリスク対策を検討し、その有効性を定期的にモニタリングし、必要に応じて、追加の対応を行うなど、継続的に改善に取り組んでいます。

情報セキュリティビジョン

日立は、「統制」「協創」「自分ゴト化」の三つのアプローチで、サイバーレジリエンス向上に向けたさまざまな取り組みを推進しています。（図表1-①参照）

図表1-① 日立の情報セキュリティビジョン





■ 統制:ゼロトラストセキュリティに向けた取り組み

日立では2017年に起きたランサムウェアWannaCryによる被害を教訓に、社内ITだけでなくOTエリアへ対策範囲を拡大するとともに、製品・サービス、サプライチェーンにおけるセキュリティやサイバーBCP※の強化を中心に、運用面、技術面、組織面での対策強化を継続的に、かつ、着実に実行しています。

加えて、業務システムのクラウド化、テレワークによる働き方の変化を踏まえた最適なセキュリティをめざし、クラウドベースITアーキテクチャーを基準としたゼロトラストセキュリティ対策に着手しています。実装にあたっては、ゼロトラストセキュリティを実現する上で、「認証」「エンドポイント」「サイバー統合監視」を重要な要素と考え、攻撃の検知能力の強化を推進しています。

※Business Continuity Plan

■ 協創:セキュリティエコシステム構築に向けた取り組み

セキュリティにおける有事の対応では、IT部門に加えて広報、人事・勤労、法務などのあらゆる部門と連携が必要です。また、セキュリティ対策の対象範囲が拡大している中、モノづくり部門や品質保証部門、調達部門などもしっかりとした連携をしないと、対応はうまく機能しません。日立では、このようなセキュリティエコシステムが重要と考え、その構築を推進しています。

このエコシステム構築の要素となるのが、「モノ」「人・組織」「社会」が「つながる」という考え方です。

DX※¹においては、IoT※²に代表される機器やシステムなどの「モノ」が「つながる」環境が必要となります。今までつながっていなかった「モノ」が「つながる」中でセキュ

リティを確保するために、異なる組織が相互に協力して対策を推進できる「人・組織」が「つながる」体制づくりに取り組んでいます。また、つながりは日立の中だけではなく、サイバーセキュリティ対策に取り組んでいる企業、官公庁、教育機関との脅威情報や対策実行時の課題共有など、枠組みを超えたコミュニティの形成が必要不可欠になっています。各企業や組織が、これらのコミュニティから得られたノウハウを自分たちのセキュリティ対策にフィードバックし、さらに広げるといった、「社会」が「つながる」活動も、積極的に推進しています。(図表1-②参照)

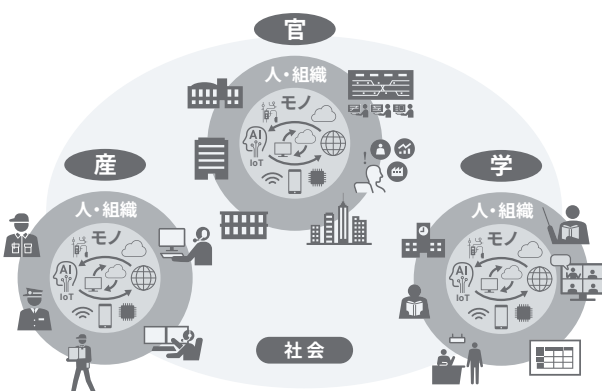
※1 Digital Transformation ※2 Internet of Things

■ 自分ゴト化:新たなセキュリティ啓発に向けた取り組み

ここ数年で定着したテレワーク中心の働き方においては、「セキュリティ意識のぜい弱性」が狙われることが想定されます。オフィス以外で仕事をするにより、近くに相談できる相手がいないなど、誰しもがリスクと隣り合わせになってきているのが現状です。

そのために、これからは一人一人のセキュリティ意識の向上こそが最後の砦(とりで)であると考え、既存のガバナンス徹底に加え、従業員の自主性の醸成と、自発的な行動により、セキュリティ意識の底上げをする活動を行っています。これにより、セキュリティを義務感ではなく、自ら興味を持ってもらい、従業員が心から共感し、自分ゴト化して取り組んでいくことをめざしています。(図表1-③参照)

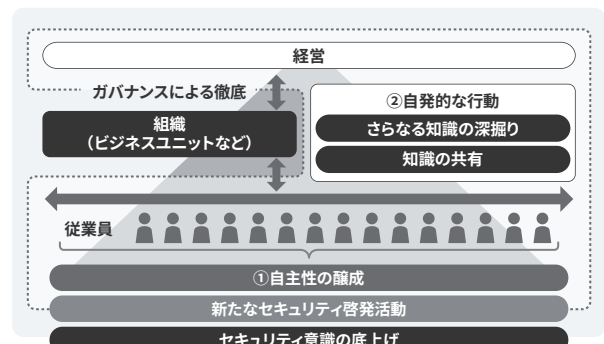
図表1-② セキュリティエコシステムのイメージ



図表1-③ これからのセキュリティ啓発のめざす姿

一人一人のセキュリティ意識の向上こそが重要

キーワード:「自分ゴト化」、「従業員が心から共感すること」



情報セキュリティの考え方

情報セキュリティの対象範囲

日立が情報セキュリティの維持のために守るべき対象は、図表1-④に示すとおり、いわゆる情報資産である「情報」と「システム」のCIA、機密性(Confidentiality)、完全性(Integrity)、可用性(Availability)と考えています。

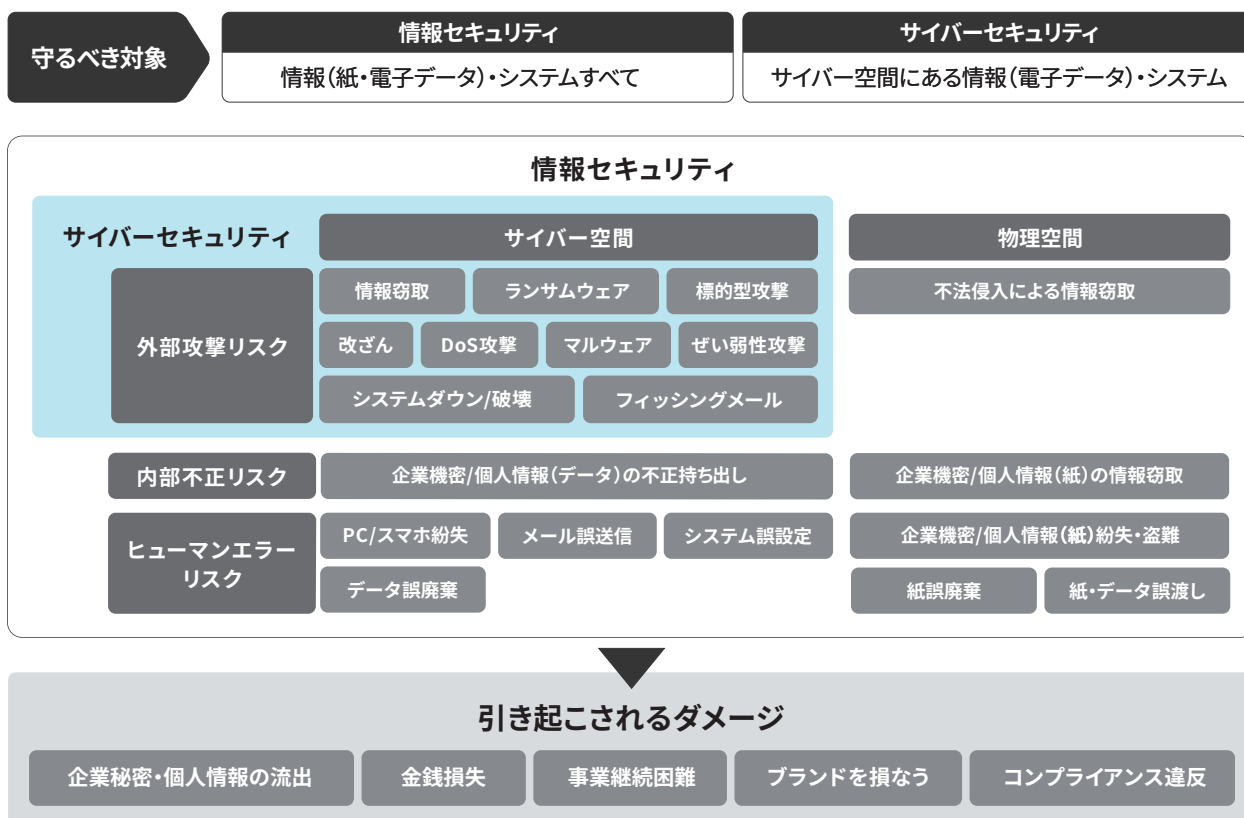
■ 情報セキュリティとして守るべき対象範囲

「情報」についてはサイバー空間のデータだけでなく物理空間に存在する紙や物理媒体も情報セキュリティとして守るべき対象としています。

日立では、外部からの攻撃、内部不正、ヒューマンエラー

などリスクの発生要因と情報の流出、経済損失、事業継続が困難になる、ブランドを損なう、コンプライアンス違反などのリスク事象からリスクが具現化した場合に引き起こされるダメージを想定し、リスク管理の視点で情報セキュリティの戦略・施策を立案しています。

図表1-④ 情報セキュリティとして守るべき対象範囲

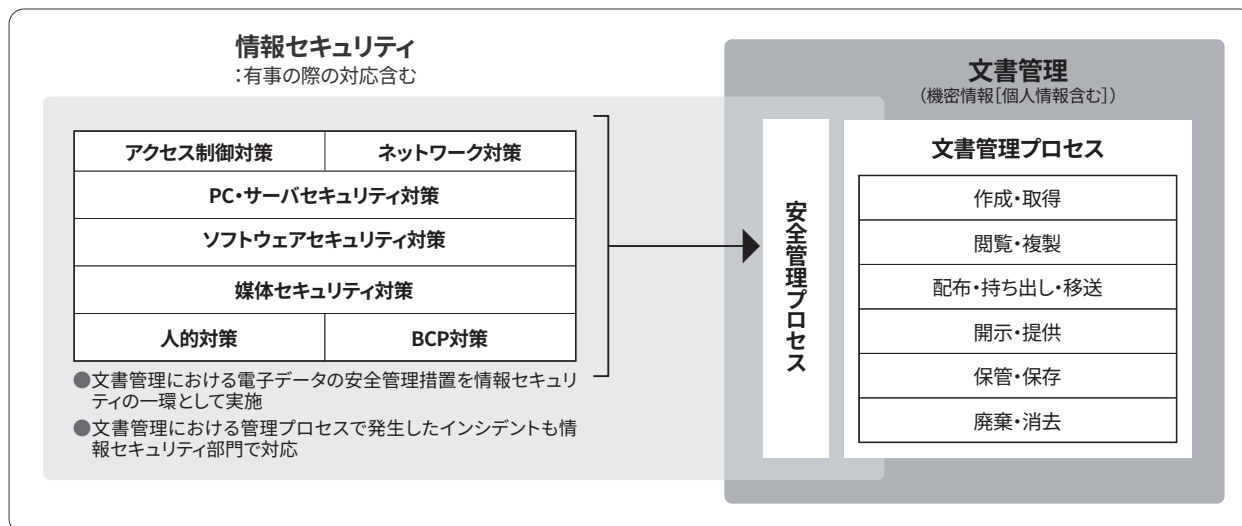




なお、情報セキュリティの戦略・施策の立案においては、サイバーセキュリティ視点での各種対策のほか、機密情報管理の視点において安全管理措置だけでなく、図表1-⑤

に示すとおり、情報の作成・取得から廃棄・消去に至るいわゆる文書管理プロセスについても情報セキュリティ維持対策の対象と捉えています。

図表1-⑤ 現状の情報セキュリティ部門の管理範囲

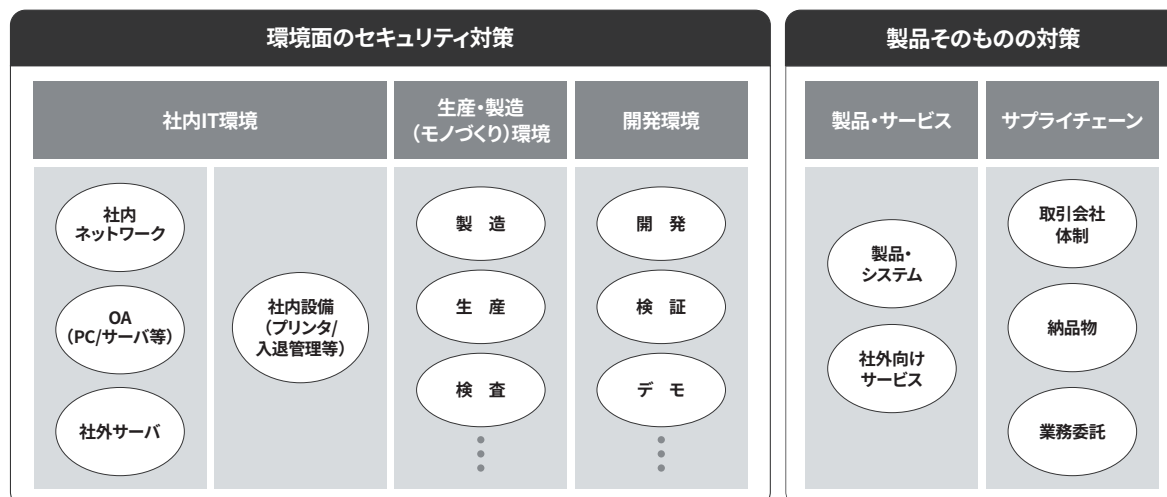


ガバナンス対象範囲

情報セキュリティ維持のために必要なガバナンス対象範囲については、2017年のランサムウェアWannaCryによる被害を契機に2018年より対象範囲を再定義し、図表1-⑥に示すとおり、社内IT環境だけでなく、生産・製

造環境、開発環境など社内環境すべてと、製品・サービスおよびサプライチェーンを情報セキュリティのガバナンスの対象としています。

図表1-⑥ ガバナンス対象範囲



情報セキュリティの考え方

情報セキュリティ戦略と重点テーマ

日立では、情報セキュリティ統括部門が、図表1-⑦に示すとおり、大きく3つの構成要素に基づきセキュリティ戦略を立案しています。

一つ目は、統制・管理になります。いわゆる統制機能としてルール策定、周知を行い、あわせてルール順守状況のモニタリング・監査を計画します。また、ルールを守るための管理およびサポートを目的として、ガイドラインやプロセスの策定、必要となる教育・訓練を計画します。

二つ目は情報セキュリティという専門分野にかかわる動向把握、技術動向把握および技術対策になります。攻撃動向や技術動向、法令動向を収集し事業部門に対し周知するとともに、対応する施策の立案に反映します。また、サイバー技術の専門家として日立グループの監視およびインシデント対応に必要な施策を立案します。

三つ目は、意識・リテラシーの向上になります。日立グループ全従業員のセキュリティに関する意識およびリテラシー向上のための啓発活動を実施する観点で、ボトムアップ、トップダウン両方の視点から施策を立案しています。

■ 情報セキュリティを取り巻く環境

2025年度のセキュリティインシデントの動向としては、AI悪用の顕在化とランサムウェア被害が長期化していることが挙げられます。AI悪用の顕在化については、言語の壁がなくなったことによりフィッシングの巧妙化と攻撃スピードの急激な高速化が進んでいると認識しています。人手での対応には限界があり、AI活用や兆候が検知された時点で端末を即隔離するなど、従来のインシデント対応の考え方そのものの見直しが必要になってくると考えています。

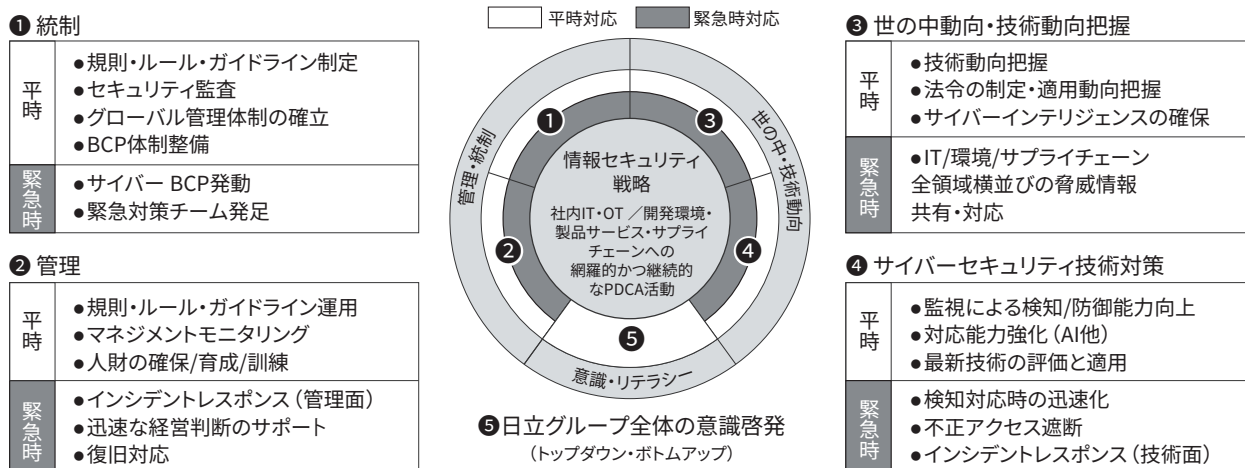
ランサムウェア被害については、国内大手企業での事案をはじめ、事業影響が長期化する傾向にあります。被害発生後の安全性確保に要する時間を考慮した事業継続の考え方がこれまで以上に重要になると考えています。また、

大きな流れとしては、金銭目的で事業を徹底的に破壊し、身代金を得る攻撃が主流となっています。加えて、AI悪用により、攻撃の準備から実行までが自動化され、攻撃は常時・高速・高密度化しています。その結果、従来の防御策では追いつかない巧妙な攻撃が現実の脅威となっていることを改めて認識する必要があると考えています。

政策動向としては、グローバルでCRA*などのセキュリティ法制強化が進む中、特に日本ではセキュリティ規制の強化が急速に進展しており、経済安全保障推進法、サイバー対処能力強化法、セキュリティクリアランス、サプライチェーン強化に向けたセキュリティ対策評価制度などへの対応が重要となってきています。

重要インフラ案件を多く担う日立グループとしては、動

図表1-⑦ セキュリティガバナンスの構成





向を注視し、的確な対応を進める必要があると認識しています。また、データ保護分野では、AIプライバシーやデータ利活用に関する法制がグローバルで進展しており、引き続き計画的な準備と対応が求められています。

※CRA：2027年12月からEU域内で完全適用されるサイバーレジリエンス法

■ 重点テーマと活動状況

2025年度は世の中でのセキュリティインシデント動向、政策動向を踏まえ、①情報セキュリティリスク管理の実効性向上、②高度化・巧妙化するサイバー攻撃への対応、③グローバル法規制強化への着実な対応の3つを重点テーマとし各種施策を推進してきました。

1. 情報セキュリティリスク管理の実効性向上

情報セキュリティリスク管理の実効性向上の取り組みとしては、昨年度より継続している3DL※モニタリングの結果をもとに社内IT、開発・検証、生産・製造、製品・サービスの環境別にビジネスユニット（BU）およびグループ会社の実行状況の可視化を行い、改善点を明確化した上で是正に取り組んできました。

また、サプライチェーンを狙ったサイバー攻撃が増加していることを受け、主要調達パートナーを中心に、事故防止策の徹底と改善促進を推進してきました。データ保護においては、国内外のグループ会社を対象に毎年実施しているモニタリングに、対策が必要なグループ会社の指定や改善点を明確化するなどの改善機能を実装し、実行状況の把握と改善に取り組んできました。

※3DL：3つのディフェンスライン。詳細はP17の「サイバーセキュリティ強化施策の考え方」を参照ください。

2. 高度化・巧妙化するサイバー攻撃への対応

高度化・巧妙化するサイバー攻撃への対応としては、クラウド環境利用時のセキュリティ強化、データセキュリティ強化、内部不正監視を中心に対策を進めてきました。

クラウド環境利用時のセキュリティ強化については、日立グループで利用しているクラウドサービスの相互認証リスクに対応できるようガイドライン整備を行い、監視を開始しました。データセキュリティ強化としては、ユーザーが理解しやすい機密情報区分の再設計、規則との整合性などの整備を行い、2026年度からの運用を推進していきます。内部不正監視についても検討、機能検証を行い、実運用に向けた課題を整理し、2026年度からは実装の検討を進めていきます。

3. グローバル法規制強化への着実な対応

CRAについては、2026年9月に適用が開始される脆弱性およびインシデント報告への対応に向けて、準備を進めています。またEU Data Actについては、契約書・通知文の雛形および実務ガイドの整備を完了し、2026年9月からの適用開始に向けて、各事業部門において設計面での対応を推進しています。

また、2025年5月に施行された重要経済安保情報保護活用法への対応として、適合事業者認定取得に向けた各種ひな型を整備し、申請する場合の準備を着実に進めています。

今後の重点取り組み

AI悪用によるサイバー攻撃の高速化・高度化、AIエージェントなどの導入による攻撃対象となるアカウント数の拡大、グローバルでのデータ保護法令の強化などを踏まえ、中長期での抜本的かつ継続的な対策が不可欠と考えています。

今後は、自らが先行してAI活用を実践する「Customer Zero」の考えのもと、「攻撃者視点の優先度付けによる、俊敏かつ継続的なサイバーレジリエンス向上」を戦略として、次の項目を重点的に推進していきます。

- ・ 攻撃者視点で優先度を定め対策を強化
- ・ AI活用を中核とした技術対策と俊敏で持続可能な管理対策の推進
- ・ AIを活用した最前線の対策適用と事業環境の強化

情報セキュリティマネジメント

情報セキュリティマネジメントシステム

日立では、情報セキュリティの方針および個人情報保護に関する方針を定め、日本国内およびグローバルでの推進体制を構築し、各種規則の整備、従業員に対する教育および各種施策が適切に実施されているかを把握するためのモニタリング、監査に取り組んでいます。

情報セキュリティの方針

日立では、企業の経営方針を織り込んだセキュリティの方針を定め、情報セキュリティを確保しています。

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

日立グループは、情報セキュリティの取り組みを、経営ならびに事業における重要課題の一つと認識し、法令およびその他の規範に準拠・適合した情報セキュリティ管理規則を策定する。さらに、当社役員を中心とした情報セキュリティ管理体制を確立し、これを着実に実施する。加えて組織的、人的、物理的および技術的な情報セキュリティを維持し、継続的に改善していく。

(2) 情報資産の保護と継続的管理

日立グループは、扱う情報資産の機密性、完全性および可用性に対する脅威から情報資産を適切に保護するため、安全な管理策を講じる。また、事業継続のために、適切な管理措置を講じる。

(3) 法令・規範の遵守

日立グループは、情報セキュリティに関する法令およびその他の規範を遵守する。また、情報セキュリティ管

理規則を、これらの法令およびその他の規範に適合させる。また、これらに違反した場合には、しかるべき処分を行う。

(4) 教育・訓練

日立グループは、役員および従業員へ情報セキュリティの意識向上を図るとともに、情報セキュリティに関する教育・訓練を行う。

(5) 事故発生予防と発生時の対応

日立グループは、情報セキュリティ事故の防止に努めるとともに、万一、事故が発生した場合には、再発防止策を含む適切な対策を速やかに講じる。

(6) 企業集団における業務の適正化確保

日立グループは、前第1項から第5項に従い、日立グループにおける業務の適正を確保するための体制の構築に努める。

個人情報保護方針

日立では、個人情報保護方針を定め、個人情報保護に努めています。個人情報保護方針の詳細については、P29

「個人情報保護の取り組み」を参照ください。

情報セキュリティ・個人情報保護推進体制

■ 情報セキュリティ推進体制

日立では、情報セキュリティ統括部門がグループ全体のガバナンスを行います。日立製作所の各BU・事業所およびグループ会社に対して各統制ラインより実行の指示を行うことでガバナンスを実現しています。また、BU・グループ会社はそれぞれが管掌するグループ会社(子会社)に対しても同様の統制を行うことで日立グループ全体のガバナンス

を実現しています。これは日本国内だけではなく海外に対しても同様となります。

日立では、日立製作所の執行役社長兼CEO(以下、執行役社長兼CEO)が、日立グループ全体の情報セキュリティに関する方針の決定や施策の実施などについて責任と権限を有する情報セキュリティ統括責任者および個人情報保護・情報セキュリティ監査について責任と権限を有する



情報セキュリティ監査責任者を任命します。

Chief Digital & Security Officer(CD&SO)は、情報セキュリティ統括責任者として、情報セキュリティ委員会を組織し、情報セキュリティに関する方針、個人情報保護方針、教育計画、各種施策を決定します。

情報セキュリティ委員会の決定事項は、全BU・事業所実務者が出席する情報セキュリティ推進会議を通じて、各組織に徹底されます。

情報セキュリティ委員会で審議、決定された規則および各種施策については、経営会議および取締役会メンバーである監査委員に対して定期的に報告を行っています。

BU・事業所では、原則としてBU長・事業所長が情報セキュリティ責任者を兼任しています。情報セキュリティ責任者は、情報セキュリティ推進部門を設置し、情報セキュリティ実行責任者を任命します。情報セキュリティ実行責任者は、自部門や管掌するグループ会社に対し、情報セキュリ

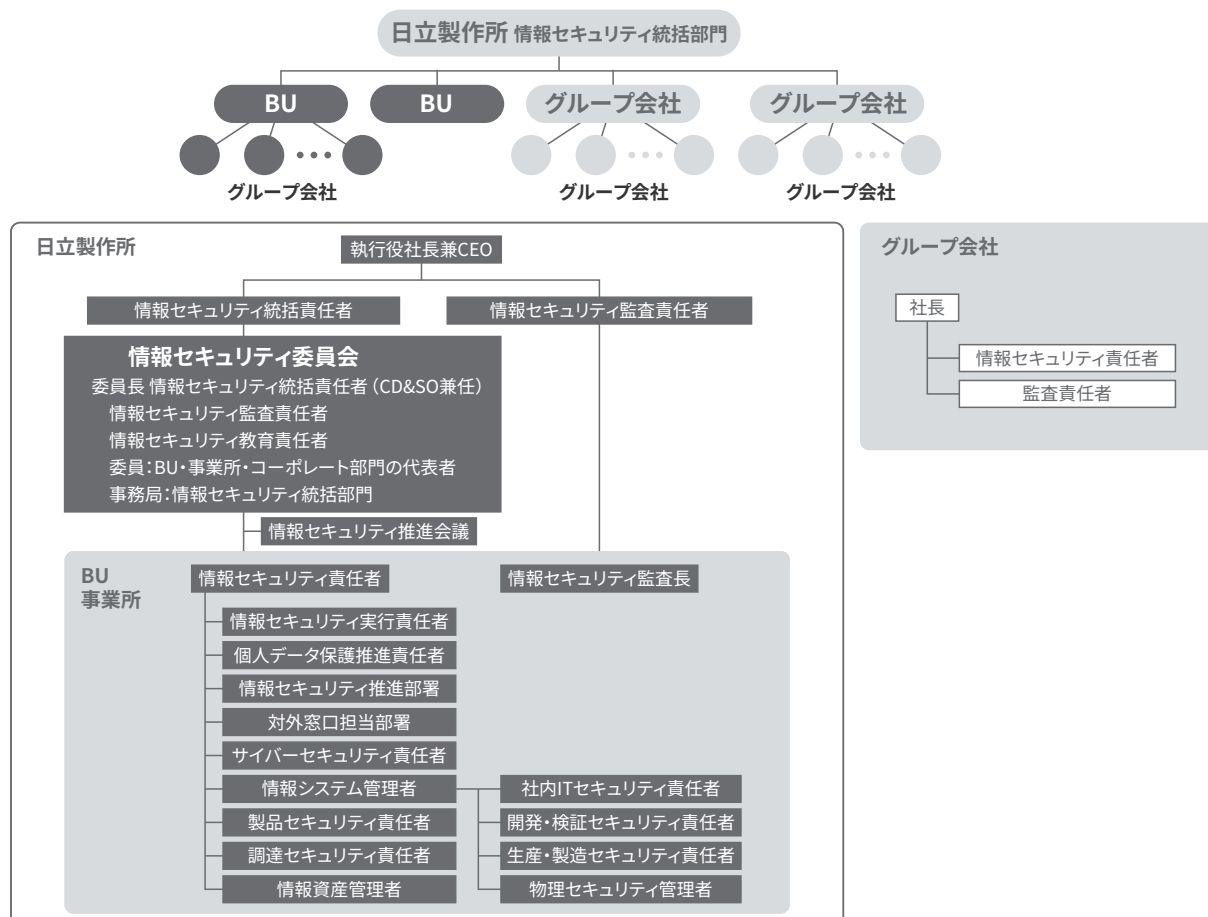
ティに関する各種施策の徹底や従業員への教育などを推進します。また、サイバー攻撃の対象範囲が拡大していることから、情報システム管理者のもとに、社内IT環境、開発・検証環境、生産・製造環境、オフィスの入退室などの物理セキュリティなどの環境別に各責任者を設置しています。さらに、お客さまに提供する製品・サービス、取引先などのサプライチェーンのセキュリティを強化するため、製品セキュリティ責任者、調達セキュリティ責任者も設置しています。

個人情報保護については、個人データ保護推進責任者を選任し、個人データ保護推進責任者が個人情報保護に関する各種施策の徹底や従業員への教育などを推進しています。

グループ会社において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。

(図表2-①参照)

図表2-① 情報セキュリティ推進体制



情報セキュリティマネジメント

■ 情報セキュリティ・グローバル推進体制

グローバルビジネスの拡大に伴い、日立では、セキュリティ施策の確実な遂行に向け、各地域に情報セキュリティ担当部門（リージョンブランチ）を設置し、グローバルガバナンス強化に取り組んでいます。

情報セキュリティのガバナンスラインは、情報セキュリティ統括部門より方針・施策を各BU・グループ会社へ共有・指示を行い、各BU・グループ会社はそれぞれ管掌する海外グループ会社に対し、その実行を指示します。

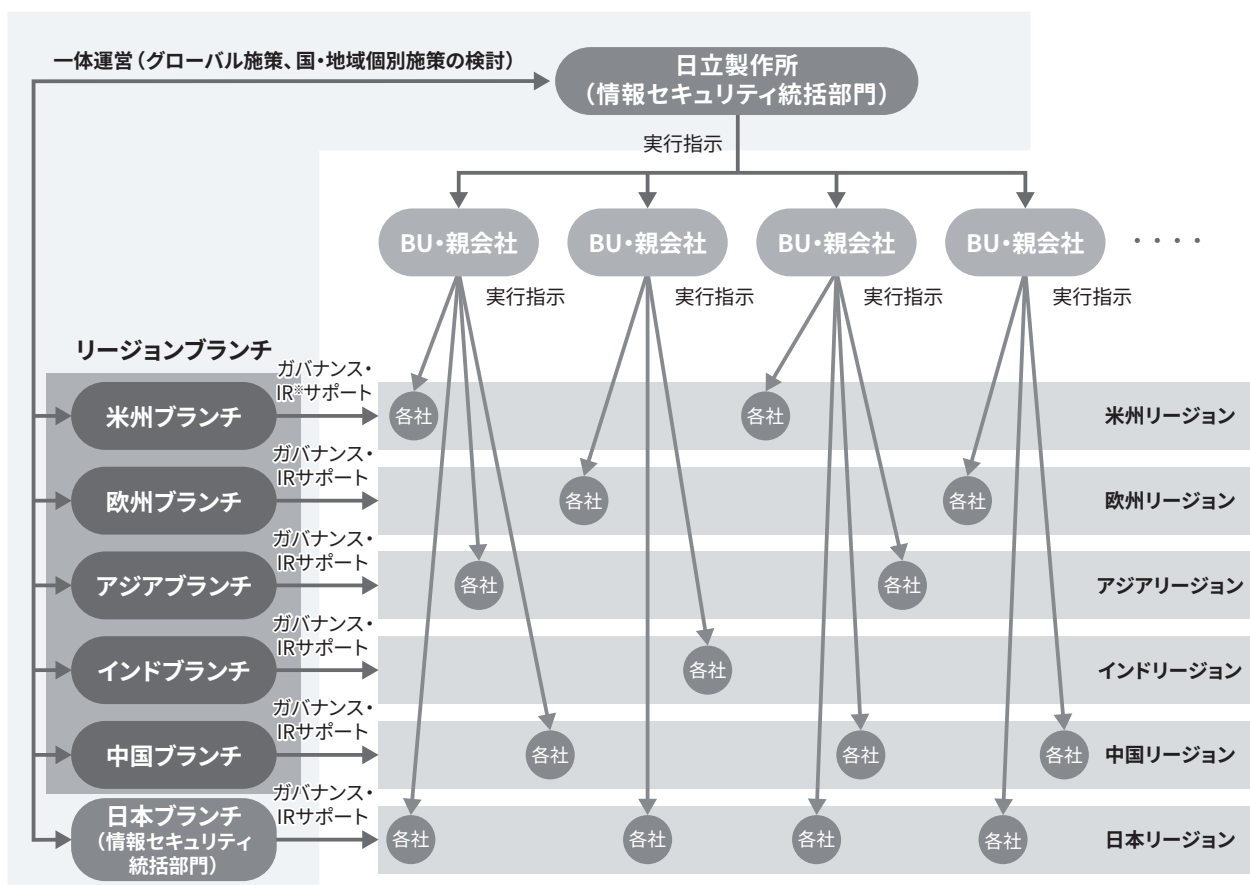
One Security Teamによる迅速な対応、変化する地域法規制への準拠を目的に、米州、欧州、アジア、インド、中国の各地域にリージョンブランチを設置し、グローバルで

ガバナンス浸透を向上させる活動に取り組んでいます。

ガバナンスラインであるBU・親会社から各グループ会社への縦軸に加え、ブランチより各地域現地法人へ横軸でサポートすることで、グローバル全体でのセキュリティ施策の推進強化を図っています。なお、日本においては、情報セキュリティ統括部門が、日本ブランチとして、同様の役割を果たしています。

各地域のリージョンブランチにおいては、Head of Cybersecurityを任命し、有事の際にグローバル丸となった対応をするため、平時よりコミュニケーション強化、インシデントマネジメント強化、モニタリングマネジメント強化対応を行っています。（図表2-②）

図表2-② リージョンブランチによるガバナンス強化体制



※ IR: Incident Response



■ データ保護推進体制

データ保護においては、各地域のグループ会社で適切な個人情報保護法令遵守対応を進めるため、各社に個人情報保護推進責任者を設置しています。なおかつ、米州、欧州、アジア、インド、中国の地域統括会社に現地グループ会社を支援する個人データ保護アドバイザを設置し、各国・地域での法令対応を推進しています。

執行役社長兼CEOをトップとする情報セキュリティ推

進体制を通じ、個人情報保護に関する施策の徹底を図り、適切に個人情報の管理を行っています。日立製作所のBU・事業所では、情報セキュリティ責任者のもと、各部署に情報資産管理者を置き、個人情報保護の取り扱いに関する責任体制を整えています。国内のグループ会社においても同様の組織を設け、日立グループとして、個人情報保護管理の徹底を図っています。

情報セキュリティ・個人情報保護規則体系

日立では、図表2-③に示すとおり、各種セキュリティ関連規則を定めています。また、グループ会社も同等の規則を定め、情報セキュリティを推進しています。

■ 基本規則

「情報セキュリティマネジメント総則」は、情報セキュリティマネジメントシステムの策定、実施、維持、継続的な改善に関する基本的な遵守事項を定めています。

「日立グループ情報セキュリティポリシー」は、前述の情報セキュリティの方針を定めた規則になります。

「情報セキュリティ対策基準」は、米国政府基準NIST※SP800に対応したグローバルで通用するサイバーセキュリティ対策を定めた規則になります。

「日立グループ プライバシー プリンシプル」は、各国・地域の個人情報保護法制の基本原則として取り入れられているOECDプライバシーガイドライン※を基に、日立グルー

プ共通のデータ保護に関する行動規範を定めています。

「個人情報保護方針」および「個人情報管理規則」は、個人情報保護法より一段高いレベルの管理を行うためにJIS規格(JIS Q 15001)相当の基準を規則として定めています。

「機密情報管理規則」は、機密情報の保全に関する取り扱いを定めています。

※NIST:米国国立標準技術研究所

※OECDプライバシーガイドライン:経済協力開発機構(OECD)が1980年に採択した個人データの国際流通に関する一連の原則を定めた指針

■ 個別規則

「Webサイト作成および情報開示に関する規則」は、Webサイトにおいて、情報の開示および利用を正しく行うために遵守すべき事項を定めています。

「入退および立入制限区域管理規則」は、建物への入退管理に関する事項など、物理的なセキュリティの確保についての規程を定めています。

図表2-③ 情報セキュリティ・個人情報保護関連規則

分 類	規則名
基本規則	情報セキュリティマネジメント総則
	日立グループ情報セキュリティポリシー
	情報セキュリティ対策基準
	日立グループ プライバシー プリンシプル
	個人情報保護方針
	個人情報管理規則
	機密情報管理規則
個別規則	Webサイト作成および情報開示に関する規則
	入退および立入制限区域管理規則
	個人情報取扱業務委託規準

情報セキュリティマネジメント

情報セキュリティ・個人情報保護マネジメントサイクル

日立では、個人情報マネジメントを含む情報セキュリティマネジメント全体をPDCA(Plan-Do-Check-Action)として実施するフレームワークを構築し、[Plan]ルール・施策を定め、[Do]施策を実施し、[Check]評価・モニタリングを行い、[Action]継続的改善を通じて、情報セキュリティマネジメントサイクルを実現しています。

個人情報保護マネジメントサイクルの詳細については、P31を参照してください。

[Plan]では、情報セキュリティ方針、情報セキュリティ施策の策定、情報セキュリティ教育計画、個人情報保護・情報セキュリティ監査計画を立案します。

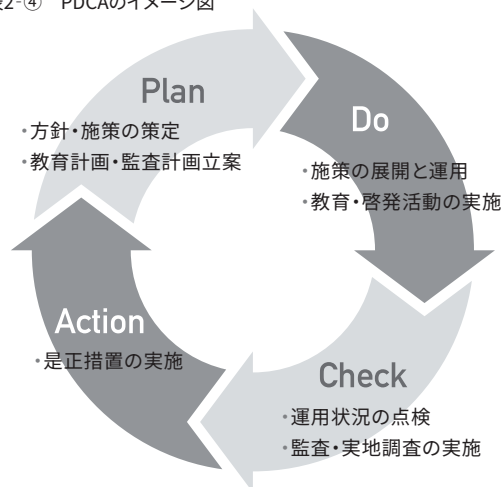
[Do]では、セキュリティ施策の社内への展開と運用を行います。情報セキュリティ教育や啓発活動を通じ、セキュリティ施策の周知徹底と従業員一人一人の意識の向上を図ります。

[Check]では、セキュリティの運用状況の定期的な点検、

監査計画にのっとりた監査、セキュリティ専門家による実地調査などを実施します。

[Action]では監査や実地調査の結果などに基づいて是正措置を講じます。(図表2-④参照)

図表2-④ PDCAのイメージ図



情報セキュリティ・個人情報保護に関する教育

■ 情報セキュリティ・個人情報保護に関する教育

情報セキュリティを守り、個人情報や機密情報を保護するためには、従業員一人一人がその重要性を理解し、日々の業務の中で意識して行動することが必要です。

日立では、すべての役員、従業員、派遣社員などを対象に、毎年eラーニングによる情報セキュリティおよび個人情報保護教育を実施しています。

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eラーニングの受講を必須としており、昨年度の受講率は、100%(休職者など受講不可能な者を除く)に達しています。そのほかにも、日立製作所では、毎年情報セキュリティ教育計画を策定し、新入社員、新任管理職や情報セキュリティ実行責任者などを対象とした座学教育、対象別・目的別に多様な教育プログラムを用意し、情報セキュリティおよび個人情報保護教育に取り組んでいます。(図表2-⑤参照)

日立製作所の教育コンテンツは国内外のグループ会社にも公開しており、日立グループ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。

■ 標的型攻撃メール訓練教育

標的型攻撃メールによるサイバー攻撃は日々行われており、従業員が攻撃を受けた場合、適切に対応できるよう一人一人の訓練が欠かせません。

日立では、グループ会社も含めて全従業員を対象とした標的型攻撃メール訓練教育をグローバルで実施しています。実際に標的型攻撃メールを装った模擬メールを各人に送付して、不審メールとはどういうものか、受信した際にどのように対応すべきかなどについて、実体験を通して対応力の強化を図っています。また、訓練終了時に、不審メールの見分け方などについて従業員に解説・周知することで、訓練の効果を高めています。



図表2-⑤ 情報セキュリティに関する教育の実施対象者とその内容

分 類	対 象 者	内 容
全従業員教育	・全従業員 ・派遣社員 ・出向受入者	個人情報保護および機密情報管理の必要性、情報セキュリティ最新情報
階層別教育	新任課長相当職	個人情報保護、機密情報管理、情報セキュリティについて管理職として必要な知識および日立製作所の個人情報保護の取り組み
	新任主任相当職	個人情報保護、機密情報管理、情報セキュリティについて主任相当職として必要な知識および日立製作所の個人情報保護の取り組み
	新入社員	個人情報保護、機密情報管理、情報セキュリティに関する基本的な知識
専門教育	個人情報保護担当者	個人情報保護担当者として必要となる、社内規則体系や管理体系、実運用手順などの専門的な知識および事例を踏まえた実践演習
	情報資産管理者	各部署で個人情報を含む情報資産の管理責任者として行動するために必要な知識

マネジメントの評価とモニタリング

日立では、情報セキュリティおよび個人情報保護マネジメントシステムを情報セキュリティマネジメント総則に定めたPDCAサイクルにより推進しています。マネジメントシステムが各BU、事業所、グループ会社などで適切に実施されているか確認するために定期的に監査、アセスメント、モニタリングなどを実施しています。

情報セキュリティを含む事業全般については、日立製作所の監査部門がBU・事業所・グループ会社に対し、定期的に監査を行っています。

情報セキュリティについては、情報セキュリティ部門・BU・事業所などのセキュリティ専門家で構成される専門チームが定期的にアセスメントを行っています。なお、情報セキュリティ統括部門では、日立製作所および国内グループ会社を対象に社外に公開しているサーバーなどの外見ぜい弱性調査を四半期に1回実施しています。

個人情報保護については、国内および海外のグループ会社に対し、情報セキュリティ統括部門が「日立グループ プライバシープリンシプル」に従った社内規則の整備、運用が日立グループ各社で実行されているか年に1回、モニタリングを実施し、各社の対応状況を確認しています。

日立製作所および国内すべてのグループ会社では、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。日立製作所における内部監査は、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門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。また、その結果を情報セキュリティ統括部門が確認しています。

個人情報保護および情報セキュリティ監査では、次のような事項を確認しています。

- ・情報セキュリティ規則と情報資産の管理および情報セキュリティ対策の合致状況
- ・個人情報保護規則と個人情報保護管理体制の整備運用との合致状況

また、日立製作所の全部門においては、個人情報保護運用の自主点検を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部門では1カ月に1回、業務ごとの運用を確認するなど、運用状況を定期的に確認しています。

情報セキュリティ強化の取り組み

日立は、情報セキュリティマネジメント強化の取り組みとして、平時、有事における情報資産管理、M&Aの際のセキュリティ確保、セキュリティ人材育成、海外グループ会社に対するガバナンス強化活動などに取り組んでいます。

情報資産管理の考え方と取り組み

さまざまな脅威から狙われている情報資産が漏えい、または、使用不能にならないよう、適切な保護・管理を行っています。

■ 平時の対応

日立では、情報資産を保護・管理していくためには、どのシステムにどのような情報が存在しているかを認識することが不可欠であると考え、機密情報管理実施手順書などの各種情報セキュリティ関連規則に従い、情報資産の管理を実施しています。

各BU・事業所の情報システム管理者が、情報システムの一覧を取りまとめます。アタックサーフェス管理との連携により、インターネット公開の情報システムについては抜け漏れのないよう管理を行っています。情報システムの一覧では、当該情報システムの管理者情報のほか、インターネット接続、クラウド利活用といった情報も管理し、運用管理に活用しています。また、各情報資産管理者が、各情

報システムに格納される情報資産を定期的に管理することで、お客さま情報、個人情報などの有無を含め、どのような情報が格納されているかを把握できるようにしています。

■ 有事の対応

情報システムを管理・運用している中では、不正アクセスなどにより情報システムが侵害されてしまうことがあります。そのような場合には、情報資産の特定を迅速に行い、事故の侵害・影響範囲を速やかに確認することが重要になります。日立では、日頃からの情報資産管理を徹底することで、情報資産の特定に有用に活用し、迅速な事故対応につなげています。

M&Aの際のセキュリティ確保の取り組み

日立では、日立が積極的に推進しているM&Aでのセキュリティリスクを最小化するために、日立グループに新たに加入する企業の情報セキュリティガバナンスの強化に取り組んでいます。

M&Aにおいて異なる企業文化を持つ企業が統合された結果、新たな価値を生み出していく一方で、情報セキュリティにおいては、ポリシーやシステム統合において生じるリスクを最小化することが必要です。買収会社に対して、M&Aの早い段階から日立ルールを理解および遵守を働きかけ、日立のポリシーに基づいて統制管理することが重要となります。

M&A時のセキュリティリスク評価は、契約締結の前後2フェーズに分けて行います。(図表2-⑥参照)

① 契約締結 (Day0) 前: 「情報セキュリティリスク評価」

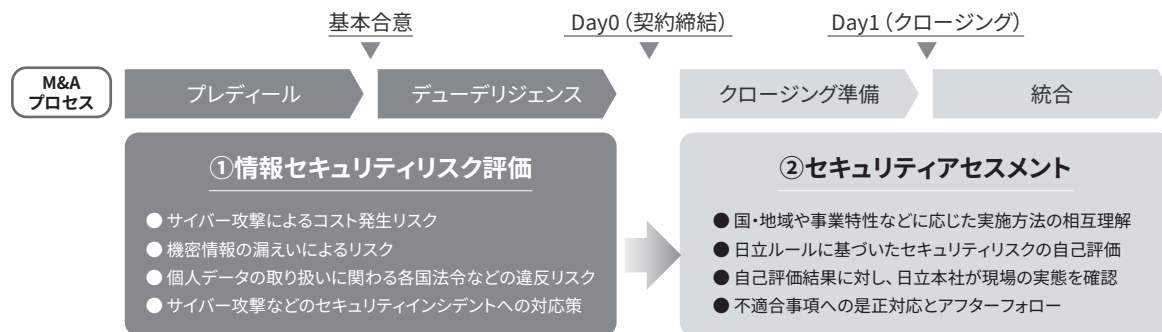
情報セキュリティの組織・体制、規則などの整備状況、事業の特性や国・地域における法制度対応、サイバーセキュリティ事故の有無および事後対応の状況など、公開情報や事前に提供された情報に基づき、買収する会社の情報セキュリティリスクを分析します。

② 契約締結 (Day0) 後: 「セキュリティアセスメント」

買収会社が事業展開している国・地域の状況や事業特性を考慮して、アセスメントする拠点を選定し、次に日立ルールでのリスク評価項目により自己評価を行ってもらいます。その結果に対して、情報セキュリティ統括部門が対象拠点を直接訪問して現場状況を確認します。最後に、不適合がある場合には是正計画を作成の上、是正完了までアフターフォローを行います。



図表2-⑥ 情報セキュリティリスク評価とセキュリティアセスメント



セキュリティ人財育成の考え方と取り組み

日立では、近年のサイバー攻撃の激化に伴い、社内のセキュリティを強化し、また、お客さまに提供する製品・サービスにおけるセキュリティ対応を適切に行うために、グループ全体でセキュリティ人財の育成を推進しています。

■ セキュリティ人財育成の考え方

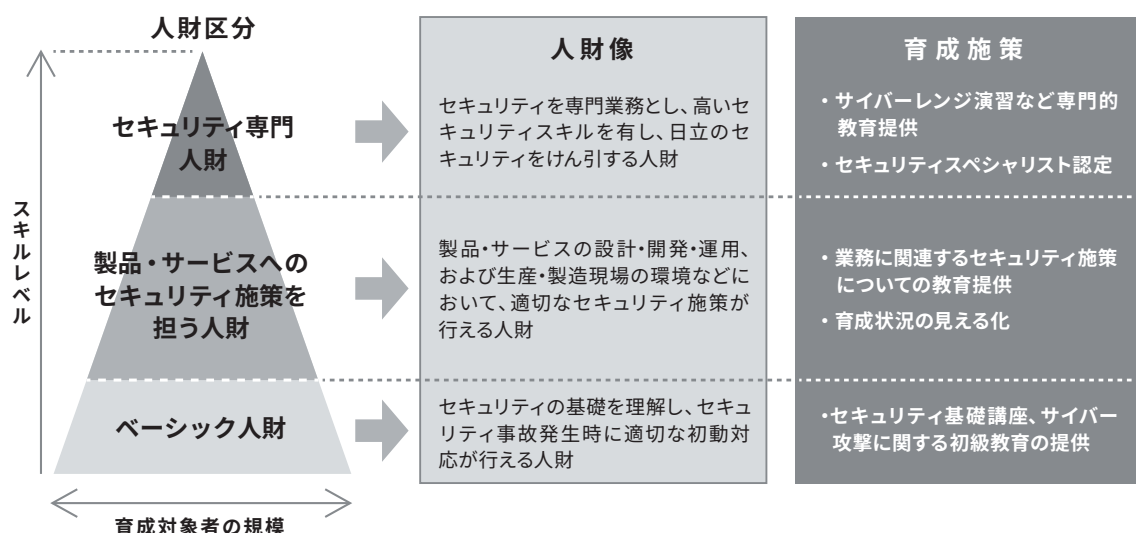
日立では、セキュリティ人財育成を図表2-⑦に示すようにセキュリティ専門人財、製品・サービスへのセキュリティ施策を担う人財、ベーシック人財の3種類に分類しています。これらの人財区分に合わせた育成プログラムを開発し、それぞれの目的に応じた人財育成を効果的に推進しています。

■ セキュリティ専門人財

セキュリティ専門人財向けには、サイバーレンジ演習などのハイレベルの教育提供、セキュリティ専門人財間の

情報共有・連携を支援するコミュニティサイトの運営などを行っています。また、セキュリティ専門人財を認定する仕組みとして、一般社団法人情報処理学会「認定情報技術制度」の企業認定に準拠した日立ITプロフェッショナル認定制度(Hitachi Certified IT Professional)を創設し、運営しています。この制度の下、情報セキュリティスペシャリスト(HISSP:Hitachi Certified Information Security Specialist)として、必要なセキュリティスキルとキャリア(業務実績など)を備えたセキュリティ専門人財を発掘・育成・評価し、認定しています。

図表2-⑦ 三つのセキュリティ人財区分と育成施策



情報セキュリティマネジメント



■ 製品・サービスへのセキュリティ施策を担う人財

製品・サービスへのセキュリティ施策を担う人財とは、製品・サービスの提供という業務を推進する中で、必要なセキュリティ施策を推進する人財です。まず必要となるのは製品・サービスの設計・開発・運用保守、それら業務の環境整備などにおいて、セキュリティ施策を適切に行う人財の育成です。また、生産・製造の現場にフォーカスしたセキュリティ人財の育成も重要です。これらの人財に対しては、社内規程などで示されたセキュリティ施策の理解を促進するための教育を提供しています。製品・サービスの設計・開発と生産・製造現場はそれぞれ安全を確保しつつお互いに悪い影響を及ぼさぬよう環境を構築・運用しなければなりません。このため、IT/OTに関わるセキュリティ対策を実施するためのさまざまなスキルアップに取り組んでいます。加えて、製品・サービスに対するセキュリ

ティ体制強化の取り組みに対応し、PSIRT※要員やセキュリティリスクアセッサ、セキュリティシステムアーキテクトなどの育成も実施しています。

※PSIRT(Product Security Incident Readiness/Response Team)

■ ベーシック人財

ベーシック人財の育成は、全社におけるセキュリティ意識を底上げし、セキュリティ対応を強化することを目的に、職場の担当者など多くの人財を対象とするものです。セキュリティの基礎知識に加え、サイバー攻撃といったセキュリティ事故発生時の適切な初動対応の習得を目的に育成を行います。ベーシック人財向けの教育としては、「サイバー攻撃対応基礎知識習得eラーニング」教育と「サイバー攻撃対応コミュニケーション訓練」教育があります。また、さらなる導入教育が必要な人財向けに、セキュリティ基礎知識に関するeラーニング教育なども提供しています。

グローバルでのガバナンス強化活動

リージョンブランチでは、当該地域の日立グループ会社のセキュリティ管理者や担当者を対象にセキュリティカンファレンスやワークショップを開催し、日立全体戦略や取り組みへの理解度向上、具体的セキュリティ施策への実行支援を行っています。これらの活動を通して、地域コミュニティの確立、さらに、地域を超えた横断的なコミュニケーション活性化を図っています。また、セキュリティニュースレターを広範囲に展開することで、セキュリティへの認識や意識の醸成をめざしています。

インシデントマネジメント強化において、インテリジェンスおよびインシデント情報を定期的に共有し、有事へのレジリエンス強化を図るとともに、有事の際は関係部署と連携しリスクを最小化できる対応支援を促進しています。

リージョンブランチでは、これらの活動を通して、グローバルにおける基本施策の着実な実行を促進しています。

(図表2-⑧参照)

図表2-⑧ リージョンブランチの主な活動内容

リージョンブランチの主な活動内容
セキュリティカンファレンス開催による、日立全体戦略・取り組み理解度向上支援
個別テーマワークショップによる、具体的セキュリティ施策実行支援
各地域セキュリティコミュニティ確立と地域を超えた横断的なコミュニケーションの活性化
セキュリティニュースレターなどによるセキュリティ啓発意識の醸成
「自分ゴト化」を意識したセキュリティ啓発活動の促進
最新動向把握のための社外カンファレンスなどへの参画
インテリジェンス・インシデント情報共有による有事へのレジリエンス強化
有事における関係部署と連携したインシデント対応支援の促進

サイバーセキュリティの取り組み



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、環境別のサイバーセキュリティマネジメント、サイバー攻撃や各種インシデントに対応するためのサイバーセキュリティ対策および対策活動を支援するSIRT (Security Incident Readiness /Response Team)活動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

日立では、これまでのOAで利用する社内IT環境の対策が中心であった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。

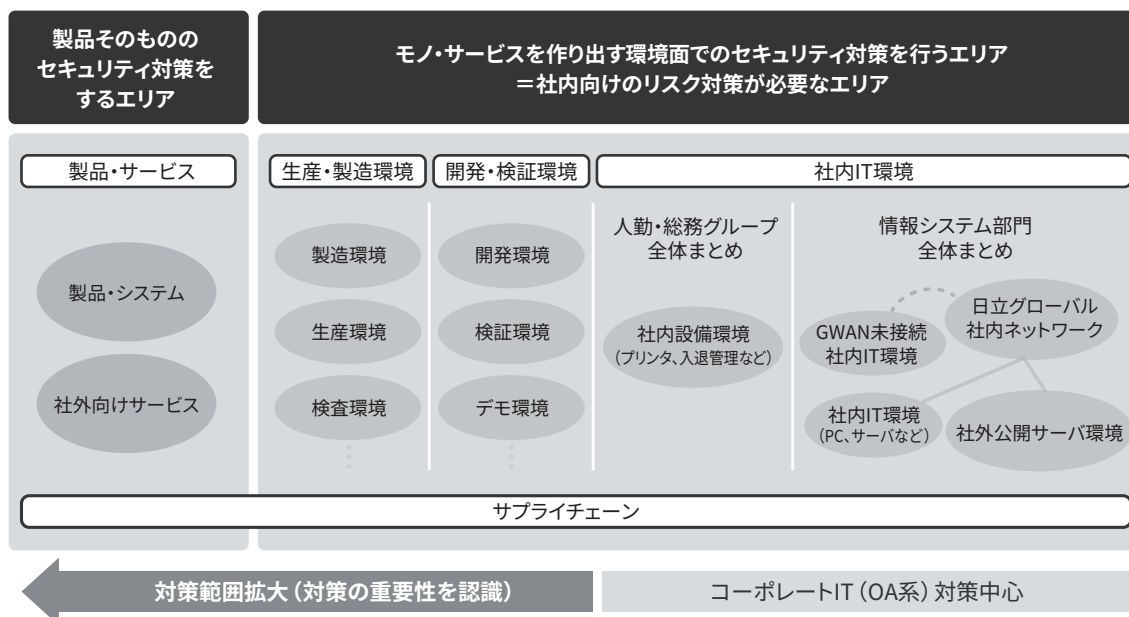
サイバーセキュリティ強化施策の考え方

ITが、生産・製造、開発・検証などの事業の現場に浸透していく中、従来の社内IT環境以外の生産・製造環境、開発・検証環境に加え、製品・サービスやサプライチェーンに対するサイバーセキュリティ対策も求められるようになってきました。(図表2-⑨参照)

このため、社内IT、生産・製造、開発・検証の環境系のサイバーセキュリティ対策と、製品・サービスやサプライチェーンにおけるプロセス系のサイバーセキュリティ対策強化に取り組んでいます。各領域のサイバーセキュリティ対策の強化について、さまざまな取り組みを進めています。(図表2-⑩参照)

また、2023年より、3つのディフェンスライン(3DL)のコンセプトに基づき、生産・製造環境、開発・検証環境、製品・サービスを対象に、セキュリティ対策を維持していくための仕組みの構築を進めています。まず、第1のディフェンスラインとして、各BU・グループ会社によるガイドライン・マネジメント指針に適合しているかどうかの自己点検を実施し、第2のディフェンスラインとして、情報セキュリティ統括部門がこの自己点検結果をモニタリング、第3のディフェンスラインとして、監査部門がモニタリング実施状況を確認します。

図表2-⑨ サイバーセキュリティ対策範囲の拡大



サイバーセキュリティの取り組み

社内IT環境におけるセキュリティ強化

社内IT環境のセキュリティ強化としては、社内のオフィス業務で使われるネットワーク、IT機器、情報システムをセキュリティリスクから守るために、ぜい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、各機器のぜい弱性対策状況の監視とユーザー/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・検証環境におけるセキュリティ強化

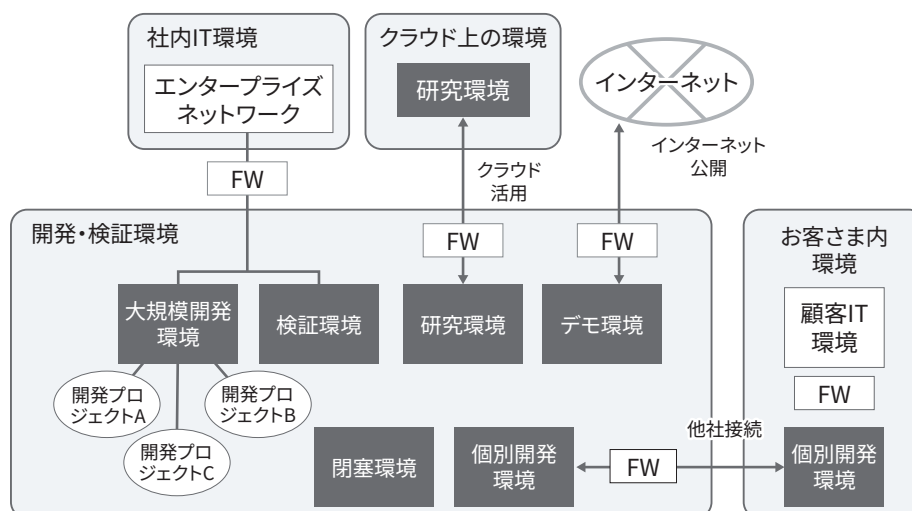
開発・検証環境は、開発、検証、研究、デモなどの目的に応じたさまざまな環境があります。また、お客さま環境やインターネットとの接続、クラウド環境の活用などがあります。環境によりセキュリティの要件が異なりますが、それぞれの環境が安全に構築され、接続されるよう、ガイド

ラインを整備し、日立グループでのガイドライン対応を進めています。また、クラウド活用やテレワーク利用などにより開発形態が変化していくため、実態に沿うよう定期的にガイドラインの見直しを行い、セキュリティの維持改善を図っています。(図表2-⑩参照)

図表2-⑩ 各領域のサイバーセキュリティ対策強化の取り組み概要

領域	対象部門	取り組み概要
社内IT	IT	・社内IT環境の接続・分離要求事項の策定と展開
開発・検証	設計・開発	・社内IT環境と安全な接続環境の構築ガイドラインの策定と展開
生産・製造	生産・製造	・制御システムをサイバー攻撃から守るための汎用的な標準規格であるIEC62443をベースとした生産・製造環境の構築ガイドラインの策定と展開
製品・サービス	設計・開発 品質保証	・製品・サービスのセキュリティ品質マネジメント指針の策定 ・製品の設計、開発・保守の各プロセスの要求事項策定と展開
サプライチェーン	調達	・取引先パートナーへのサイバーセキュリティ対策の要求事項の策定と評価プロセスに基づいた評価

図表2-⑪ 開発・検証環境のセキュリティネットワーク



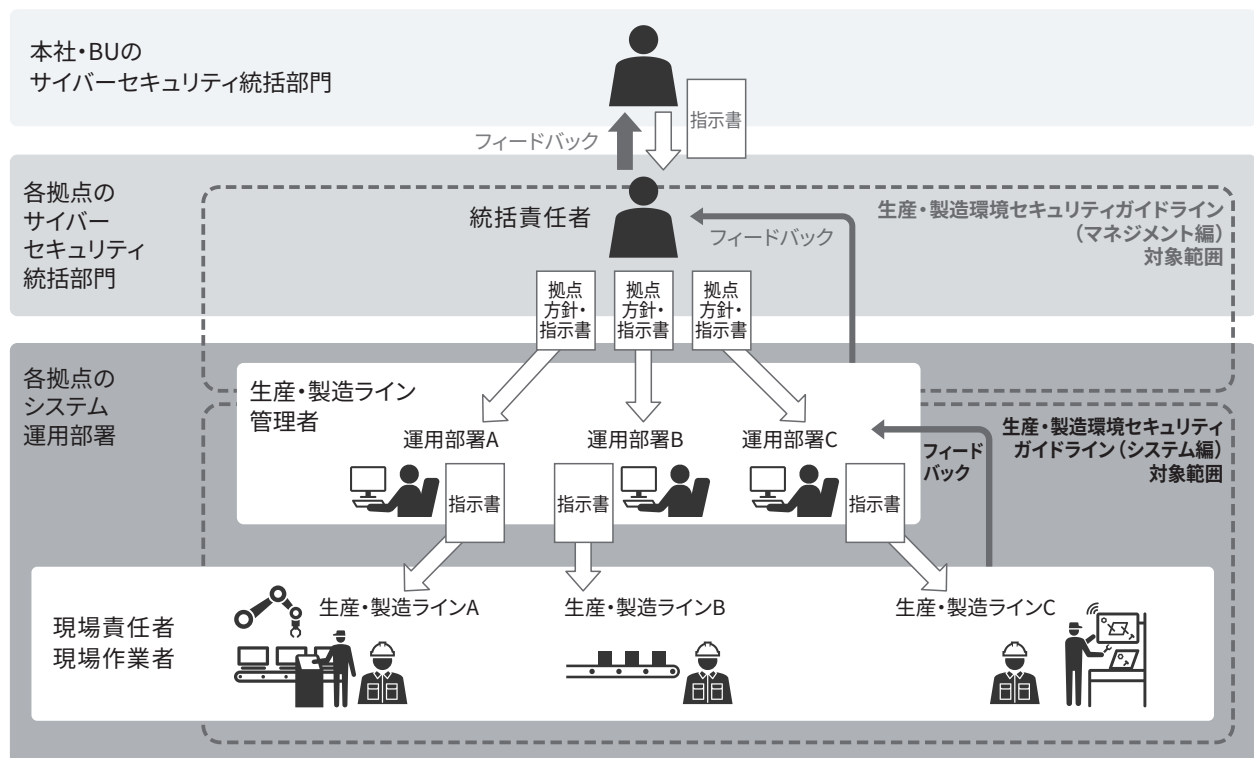
生産・製造環境におけるセキュリティ強化

生産・製造環境は、他環境(社内IT、開発など)と相互に影響を与えない、受けないようにするため、相互の安全な接続環境の構築および運用管理について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。(図表2-⑫参照) また、実際の生産・製造現場においては、現場作業員の日々の作業において、遵守すべき項目をポスターやルール集などの啓発コンテンツの展開を行い、現場のセキュリティ意識を高めています。(図表2-⑬参照)

図表2-⑬ 生産・製造現場向けのポスター・ルール集



図表2-⑫ 生産・製造環境におけるガイドラインの内容と活用イメージ



ガイドライン構成	内 容	対象者
マネジメント編	マネジメント面(組織・人的管理面としての取り組み)として、組織体制の整備および、拠点全体・部署個別のセキュリティ運用・管理上のルール策定と見直しについて記載。	サイバーセキュリティ統括責任者
システム編	「IEC62443-3-3」に基づき、現状把握と対策検討としてシステム構成およびその対策方法は、日立グループの代表的なモデルを用いて記載し、各部門・各部署でカスタマイズして利用する。	生産・製造ライン管理者 現場責任者 現場作業員

サイバーセキュリティの取り組み

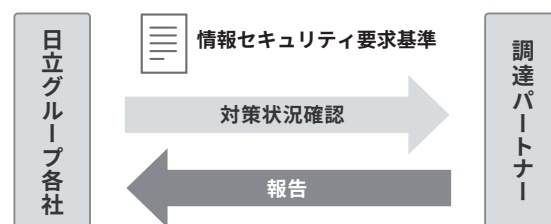
サプライチェーンにおけるセキュリティ強化

セキュリティ上、日立の情報資産に注意を払っていただくため調達パートナーに業務を委託する際には、サプライチェーン向けのセキュリティ対策項目を付加した「情報セキュリティガイドライン」を提供しています。日立の要求事項を具体的に示すことで、調達パートナーに対しても、日立と同水準のセキュリティ対策の実施を求めています。また、調達パートナーの情報セキュリティに関する対策状況を定期的に確認、審査しています。(図表2-⑭)

さらに、調達パートナーに情報セキュリティ対策を推進いただくために、調達パートナーの経営層に対して、サイバー

攻撃事例を通し、サプライチェーンセキュリティ施策の重要性・セキュリティ対策依頼などの説明を実施しています。

図表2-⑭ サプライチェーンにおけるセキュリティ強化体制

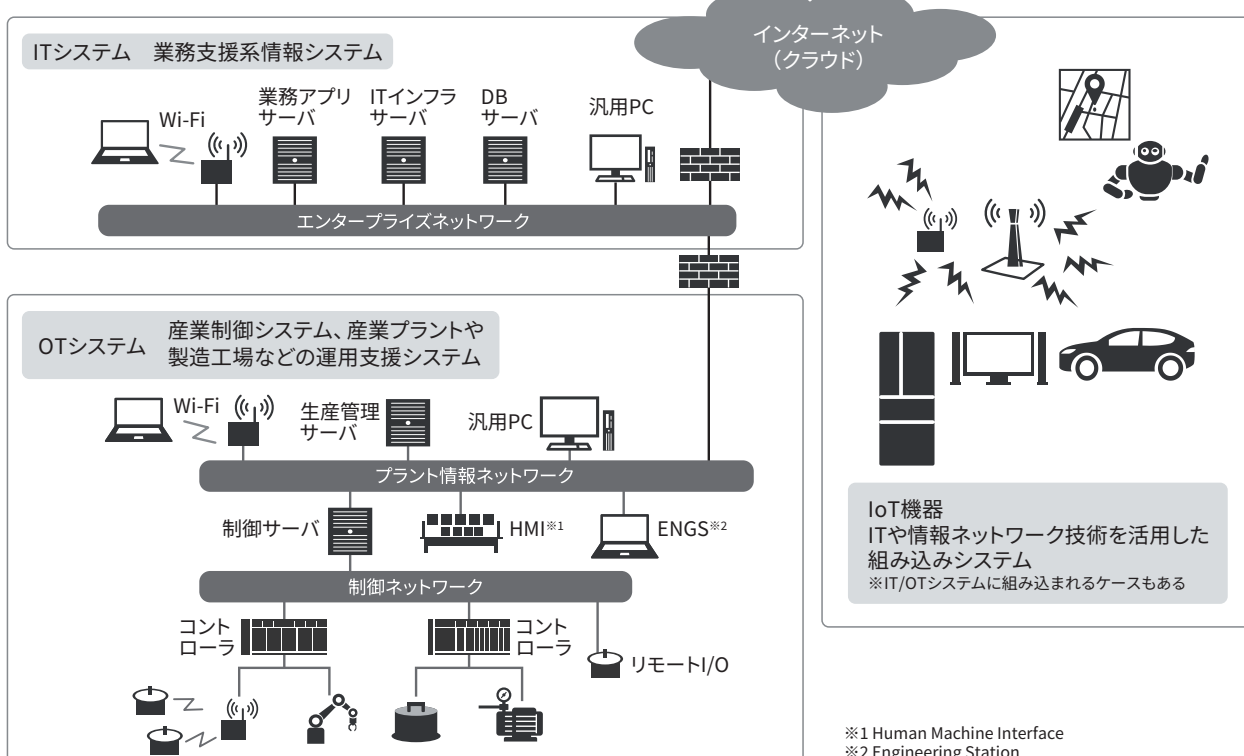


製品・サービスにおけるセキュリティ強化

デジタルソリューション事業の推進において、デジタル化やネットワーク化といった技術の高度化やシステムのオープン化によって新たな顧客価値を提供する一方で、サイバーセキュリティリスクとその対応の重要性も増しています。

日立グループが提供するITシステム・OTシステム・IoT機器といった幅広い分野の製品・サービスでは、サイバー攻撃からお客さまの資産や社会インフラを守るための取り組みを継続的に進めています。(図表2-⑮参照)

図表2-⑮ 日立グループが提供する製品・サービス分野



※1 Human Machine Interface
※2 Engineering Station



■ 製品・サービスにおけるセキュリティマネジメント指針

日立グループの多種・多様な製品・サービスに対して、セキュリティマネジメントに関する考え方の統一を図るために、「製品・サービスに関するセキュリティマネジメント指針」と関連文書を品質保証規程として作成しています。(図表2-⑯参照)

各部門は、セキュリティマネジメントに関する部門規則類に指針の内容を反映することにより、製品・サービスの開発・製造・保守・運用などのライフサイクルにわたるセキュアプロセスの実装を推進しています。(図表2-⑰参照)

■ ガイド類の展開とサポート活動

各部門がセキュリティマネジメントに関する部門規則類を整備する際の参考資料として、「セキュアプロセス実装ガイド」をはじめとする各種ガイド類を展開しています。これらのガイド類において、セキュリティ対策が先行している部門の取り組みを実践事例として紹介し、設計・製造・運用・保守、セキュリティインシデントの各プロセスでの実装手順などについて、日立グループ全体でノウハウの蓄積と共有を図っています。

これらのガイド類をイントラネットで共有するとともに、各部門でのセキュア開発プロセスの構築をサポートする活動を行っています。

■ 製品・サービスのセキュリティマネジメント体制とPSIRT

前述の「製品・サービスに関するセキュリティマネジメント指針」に基づき、安心・安全な製品・サービスを提供し続けるため、各BU・グループ会社にて製品セキュリティ責任者を配置し、その統制の下で、セキュリティマネジメント体制を構築しています。そのセキュリティマネジメント体制において、ぜい弱性やインシデントが発生した場合の有事対応を行うために、製品・サービスに関するセキュリティ技術対応を担う組織を、情報セキュリティ統括部門とBU・グループ会社にてPSIRTとして整備し、おのおのが連携して、製品・サービスにおけるぜい弱性やインシデントレスポンスへの適切な対応を行っています。

日立グループのPSIRTは、PSIRTで必要な活動についてガイドラインを整備し、それに従って活動しています。また、情報セキュリティ統括部門からBU・グループ会社への施策展開と技術的な情報共有、各部門からの活動事例の共有を目的としたPSIRT連絡会を定期的に開催しています。

さらに、PSIRT関係者を対象にしたインシデント対応訓練の実施など、BU・グループ会社の自律的なPSIRT活動に向けた取り組みを推進しています。

図表2-⑯ 製品・サービスに関するセキュリティマネジメント指針

規程等の文書	概要
製品・サービスに関するセキュリティマネジメント指針	日立グループ内における製品およびサービス（以下、製品）のセキュリティマネジメントに関する考え方の統一を図ることを目的とした指針。
製品の開発・保守の各プロセスへの要求事項	製品の開発・保守プロセスへの要求事項。製品の特性に応じて要求事項を具体的なタスクに展開し、必要に応じてチェックリストなどを整備する。
製品セキュリティ点検チェックリスト	自部門の製品開発・保守プロセスが指針および要求事項に準拠しているかを確認するための点検チェックリスト。

図表2-⑰ セキュリティ確保のための開発・保守プロセスの全体像

1.設計・製造プロセス	2.運用・保守プロセス	3.セキュリティインシデント対応プロセス
1-1. リスク分析・要件定義/基本設計	2-1. 変更管理	3-1. 社内で検知した場合
1-2. 構成管理	2-2. ぜい弱性情報の収集	3-2. 社外で検知した場合
1-3. 設計/製造	2-3. 予防保守	3-3. 定期訓練
1-4. 調達（OSS含む）	2-4. 定期ぜい弱性点検	
1-5. テスト/評価	2-5. ぜい弱性および 対策情報の顧客への告知	
1-6. 検査		

サイバーセキュリティの取り組み

サイバーセキュリティ対策

サイバー攻撃や各種インシデントに対応するために、日立では、社内で運営する日立セキュリティオペレーションセンター(SOC:Security Operation Center)にて、セキュリティ監視およびインシデント発生時の対応強化を図っています。また、脅威情報の収集・分析と、警戒情報の配信を行いプロアクティブな対策を推進しています。

セキュリティ監視・インシデント発生時の対応強化

標的型攻撃やランサムウェア、システムのぜい弱性を突いた攻撃など、複雑かつ巧妙なサイバー攻撃により、個々の企業や組織にとどまらず、サプライチェーン全体のセキュリティリスクが増大しています。また、AIの悪用により、サイバー攻撃はより高度化・大規模化しています。このようなサイバー攻撃に対峙(たいじ)するためには、その脅威をいち早く発見し、被害拡大を防止することが重要です。日立では、マルウェア感染や不正アクセスなどの脅威を早期に検知し、インシデント発生時の初動から対策までを迅速に対応し、サイバー攻撃に対する被害を最小限に抑えるための24時間365日体制の日立セキュリティオペレーションセンター(日立SOC)を設置し、セキュリティ監視・インシデント発生時の対応強化を行っています。また、欧州、米州地区との連携によるグローバルでの対応力強化を行っています。

■ サイバーセキュリティ監視

日立では、グローバルの基幹拠点すべてにおいて対象とするシステムおよびネットワークの監視ポイントを定め、ログの連携・分析・監視を行っています。また、EDR(Endpoint Detection and Response)による端末監視および認証システムの監視を強化することで、端末への攻撃や認証システムへ

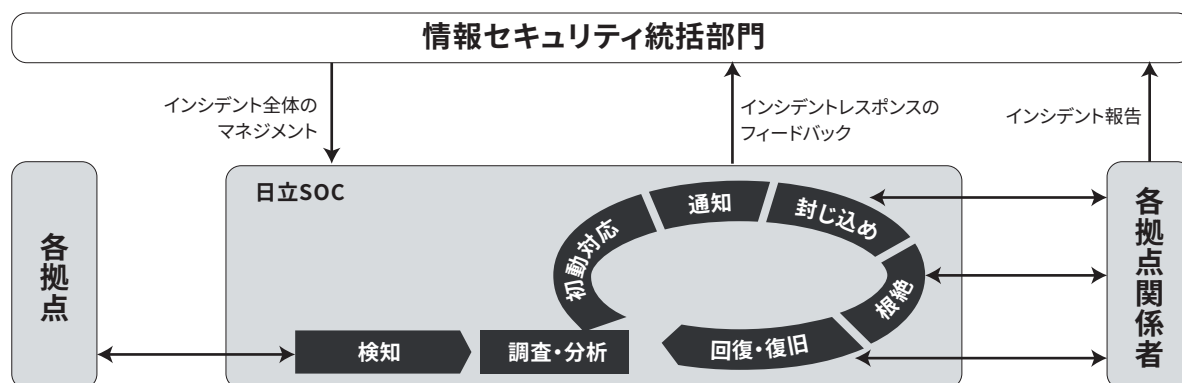
の攻撃の早期検知と迅速な対処を実現しています。これらの強化施策により、従来の境界型からゼロトラストの考え方に基づくセキュリティ監視への転換を推進しています。

■ インシデント発生時の対応

日立では、インシデント発生時に備えた対応手順、連絡体制を整備しており、インシデント発生時には、迅速に原因究明や影響範囲の特定を行い、封じ込め・根絶・復旧に至る一連の対応を実施しています。日立SOCでは、基幹拠点のログ監視とEDR、認証システム監視による調査に脅威情報を組み合わせることで、より迅速にインシデントの詳細を把握することを可能としています。これにより、対応優先度や対応要否の判断(トリアージ)の時間短縮を実現しています。さらに、SOAR(Security Orchestration, Automation and Response)やAIを活用し、トリアージ・調査・封じ込めといったインシデント対応プロセスの自動化を推進し、対応の迅速化と精度向上にも取り組んでいます。

また、インシデントレスポンスから得られたノウハウをセキュリティ監視や社内の各種セキュリティ施策にフィードバックすることで、同様のインシデントを発生させない取り組みも実施しています。(図表2-18参照)

図表2-18 セキュリティ監視・インシデントレスポンス





脅威情報の収集・分析と警戒情報の配信

日立製作所では、社内利用の情報システムおよびお客さまに提供する製品・サービスのセキュリティを確保するための活動として、脅威情報の収集・分析、警戒情報の配信を行っています。また、これらの活動によって得られた知見を情報セキュリティ統括責任者とも共有し、経営層を交えた日立グループのセキュリティ戦略策定に向けた議論を進めています。

■ 脅威情報の収集・分析・検証

情報の収集においては、一般に公開されているぜい弱性・脅威情報に加え、各種CTI(Cyber Threat Intelligence)サービスを活用した国内外の脅威情報を収集しています。

収集した情報は、情報元が公開する指標(深刻度、CVSS値など)や悪用状況、攻撃成功の可能性、社内システムでの利用状況などを基に脅威を分類整理しています。一部の脅威では、模擬環境で実際に検証することで影響や対策・被害調査に寄与する情報を整理し、対策に活用しています。

また、急速に変わりつつあるセキュリティに係る各国・地域の法制度などについても情報収集・整理を行い、日立グループにおけるリスク対応の促進を図っています。

■ 警戒情報の配信・対策徹底

収集した情報は、各BU・グループ会社から選出されたサイバーセキュリティ責任者に対して、即時～週次でのメール配信、社内Webへの掲載などを通じて周知を行っています。日立グループ全体に影響を与える大きな脅威に対しては、サイバーBCPの発令を検討するとともに、対策を徹底させるための実行力を持った「サイバー警報」を発報することで対策指示を行っています。

また、これらの情報を日立SOCや情報システム部門とも連携した脅威ハンティング、インシデント対応、監視強化へ活用しています。

■ 戦略的インテリジェンスへの昇華

脅威情報の収集・分析、警戒情報の発信活動から得られた知見を基に、日立グループの現状や改善点を分析しています。この結果を情報セキュリティ統括部門や情報セキュリティ統括責任者、リージョンブランチと共有し、日立グ

ループのセキュリティ戦略策定に役立てています。これにより、日立グループにおけるセキュリティ対応実行サイクルの加速を図っています。

■ 外部からの攻撃への対処

インターネットに公開されたシステムは常に外部からの攻撃の危険にさらされています。毎日のように多数のぜい弱性情報が報告されており、攻撃者は不正アクセスを通じて機密情報を窃取したり、ランサムウェアなどのマルウェアを感染させたりしています。また、情報が公開された時点で既に悪用されているゼロデイぜい弱性(Nデイぜい弱性)を利用した攻撃も増加しています。

これらのぜい弱性に迅速に対応するために、アタックサーフェスマネージメント(ASM)ツールを用いて外部公開機器の最新状態を管理しています。リスクが顕在化した、または恐れのある機器については、該当部署へ「サイバー警報」を発報し、早急な確認と是正を依頼することで、外部からの攻撃リスクを低減し、対応の迅速化を図っています。

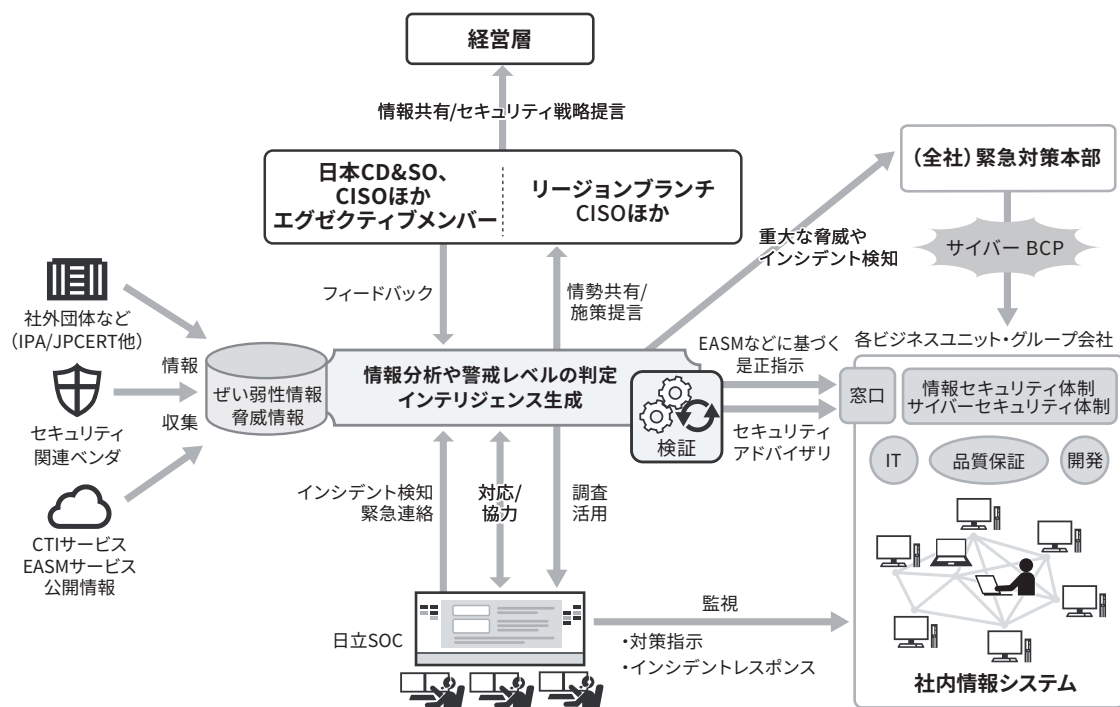
さらに、ASMで得られた知見を横断的に活用し、日立グループに関連する機密情報やアカウント認証情報の漏えい兆候を監視しています。兆候が認められた場合には、関係部門と連携し対応を行うことで被害の未然防止および早期対応を図っています。

■ 緊急時の際の対応

社内の多数の拠点において重大な業務影響がある場合や、全社レベルで業務継続が不可能な場合には、全社対策本部を設置し、サイバーBCP発令なども視野に入れたセキュリティ対策指示を行います。(図表2-⑨参照)

サイバーセキュリティの取り組み

図表2-19 脅威情報における平時の活用と緊急時の対策展開



統制

サイバーセキュリティの取り組み



SIRT活動

日立では、日立のサイバーセキュリティ対策活動を支援する組織として、日立インシデントレスポンスチーム（HIRT：Hitachi Incident Response Team）を設置しています。日立の社内インフラのみならず、日立が提供する製品・サービスをも対象に、セキュリティインシデントの発生を予防し、万一発生した場合は迅速に対処することにより、CSIRT※並びにPSIRTの両面から、お客さまや社会の安全・安心なネットワーク環境の実現に寄与します。

※ CSIRT (Cyber Security Incident Readiness/Response Team)

HIRTとは(コンセプトと定義)

HIRTは、単一の組織ではなく、日立グループ全体のサイバーセキュリティ対策活動を推進する「機能の集合体」です。組織間ならびに国際的な連携を通じて問題解決にあたり、日立グループおよびお客さま、社会の安全・安心なネットワーク環境の実現に寄与します。HIRTは次の3つのアプローチを通じて「インシデントオペレーション」を推進します。

- **Readiness(レディネス:発生の予防)**: 平時からのぜい弱性情報の収集・管理、開発・検証環境の堅牢化など、インシデントの発生を未然に防ぐための事前対策を行います。
- **Response(レスポンス:技術的対応)**: インシデント発生時には、迅速な調査・分析および技術的な調整を行い、サイバー攻撃による被害の回避・解決を支援します。
- **Resilience(レジリエンス:適応力、耐性の強化)**: 脅威情報の分析に基づく継続的な改善を行い、攻撃を受けた場合でも業務を復旧・継続できる能力を高め、「耐性」を強化します。

HIRT活動の推進体制

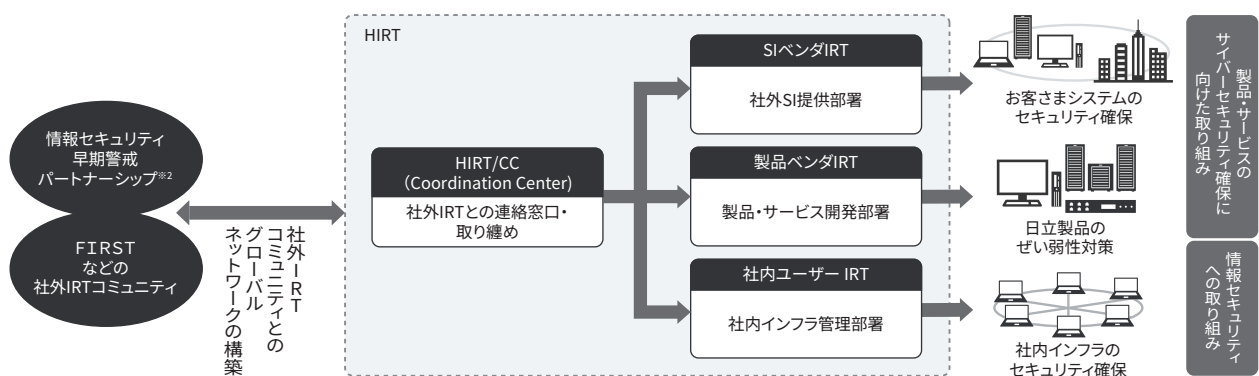
■ 四つのIRT(Incident Readiness/Response Team)モデル

HIRTでは、ぜい弱性対策やインシデント対応を推進するため、HIRT/CCT※1をハブ（各IRTとの連絡窓口・取りまとめ）

とし、各社内IRTが連携するモデルを採用することで、製品・サービスおよび社内インフラのセキュリティを確保に努めています。（図表2-②⑩参照）

※1 HIRT/CC: HIRT Coordination Center

図表2-②⑩ ぜい弱性対策とインシデント対応活動を支える四つのIRT



※2ソフトウェア製品およびWebサイトに関するぜい弱性関連情報の円滑な流通、および対策の普及を図るための、公的ルールに基づく官民連携体制

名 称	役割と担当領域
1. HIRT/CC	【全体統括・連携窓口】 FIRST※3やJPCERT/CC※4等の社外IRT組織との連絡窓口(PoC: Point of Contact)および、社内各IRT間の調整・取りまとめを行い、日立全体のぜい弱性対策とインシデント対応活動を推進します。
2. SIベンダIRT	【お客さまシステムの保護】 SI提供部署が担当。公開されたぜい弱性情報に基づき、お客さまシステムのセキュリティ確保に向けた対策とインシデント対応を支援します。
3. 製品ベンダIRT	【製品セキュリティ】 製品・サービス開発部署が担当。日立製品の影響調査、修正情報の提供(CVE採番・管理含む)など、ぜい弱性対策を支援します。
4. 社内ユーザーIRT	【社内インフラの保護】 社内インフラ管理部署が担当。日立の社内IT環境が侵害活動の拠点とならないよう、社内インフラのぜい弱性対策とインシデント対応を推進します。

※3 FIRST: Forum of Incident Response and Security Teams

※4 JPCERT/CC: 一般社団法人JPCERTコーディネーションセンター (Japan Computer Emergency Response Team/Coordination Center)

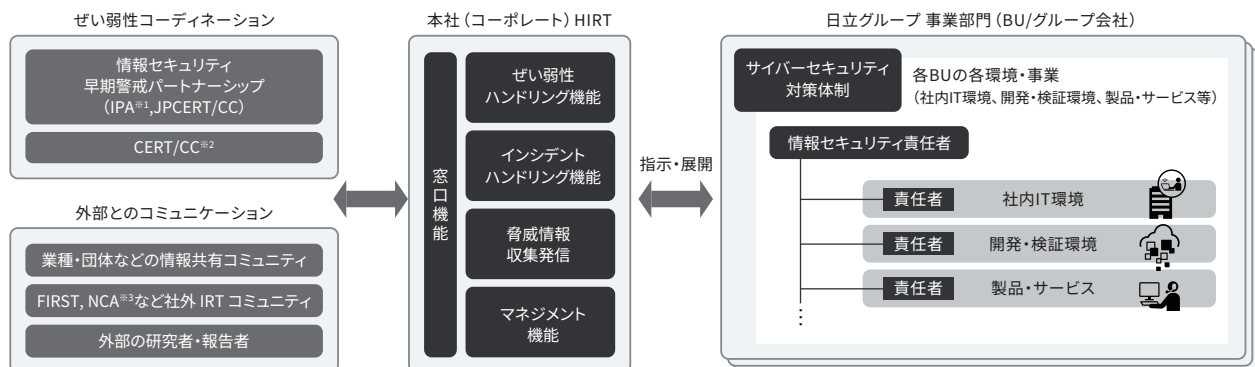
サイバーセキュリティの取り組み

■ 自律分散型のガバナンス体制

ガバナンス体制としては、日立グループ全体で推進する階層的なIRT構造をとっています。ここでは、本社(情報セキュリティ統括部門)が全てを管理するのではなく、各BU・グループ会社の責任者が、自律的にサイバーセキュリティ対策体制を構築・運用する自律分散型の体制を採用しています。(図表2-②)

- ・ **本社(コーポレート)体制**: 外部のCSIRT組織等とのコーディネーション(連絡窓口機能)を担うとともに、マネジメント機能としてぜい弱性・インシデントハンドリング、脅威情報の収集展開などの施策を推進します。
- ・ **各BU・各社サイバーセキュリティ対策体制**: 各BUやグループ会社に任命されたサイバーセキュリティ責任者がコーポレート部門の窓口となり、自律的に各環境(社内IT環境、開発・検証環境、製品・サービス等)における平時・有事のセキュリティ対策の計画、整備・運用および継続的な施策実行を主導します。

図表2-② HIRT活動のガバナンス体制



※1 IPA:独立行政法人 情報処理推進機構 (Innovation Platform Agency, Japan)

※2 CERT/CC: CERT Coordination Center

※3 NCA:一般社団法人日本シーサート協議会 (Nippon CSIRT Association)



HIRTが推進する活動

HIRTの活動には、組織内IRT活動として、制度面を先導する情報セキュリティ統括部門と品質保証部門との協力による制度・技術両面でのサイバーセキュリティ対策の推進、各BU・グループ会社へのぜい弱性対策ならびにインシデント対応の支援があります。また、日立の対外的なIRT窓口として、組織間のIRT連携によるサイバーセキュリティ対策を推進しています。

■組織内IRT活動

組織内IRT活動では、セキュリティ情報の収集や分析を通じて得られたノウハウを注意喚起やアドバイザリとして発行するとともに、各種ガイドラインや支援ツールの形で製品・サービス開発プロセスにフィードバックします。

(1) セキュリティ情報の収集・調査分析・展開

情報セキュリティ早期警戒パートナーシップの推進などを通じて、ぜい弱性対策ならびにインシデント対応に関する情報やノウハウを組織内に展開しています。

(2) 製品・サービスのセキュリティ技術の向上

組織的なIRT活動能力の向上に向け、情報システムならびに制御システム関連製品に対するセキュリティ対策の具体化、エキスパート人材への技術継承を推進しています。

■組織間IRT活動

組織間IRT活動では、複数のIRTが協調して、新たな脅威に立ち向かうための組織間連携、互いのIRT活動の改善に寄与できる協力関係の構築を推進しています。

(1) IRT活動の国内連携の強化

一般社団法人日本シーサート協議会(NCA)との活動を活用して、情報収集において知り得たぜい弱性やインシデント情報を他加盟組織のPoC(Point of Contact)に通知するなど、連携網の整備に努めています。また、一般社団法人JPCERTコーディネーションセンター(JPCERT/CC)と独立

2022年6月、HIRTはぜい弱性をユニークに識別するCVE IDを日立製品のぜい弱性に割り当て、CVEレコードを作成し公開することのできるCVE Numbering Authority(CNA)に登録しました。HIRTはCNAとして、弊社製品にぜい弱性が報告された際にはCVE IDを割り当て、適宜ぜい弱性情報を公表することで、お客さまに安心して弊社製品をご利用いただけるよう努めています。

(3) 分野別IRT活動の実践

分野ごとの背景や動向を踏まえた対応を具体化していくため、金融分野におけるHIRT-FIS^{※1}を設置するなど、分野に特化したIRT組織を設置しています。

※1 HIRT-FIS: Financial Industry Information Systems HIRT

行政法人情報処理推進機構(IPA)が共同運営するぜい弱性対策情報ポータルサイトJapan Vulnerability Notes(JVN)を用いた情報利活用基盤の整備を支援しています。

(2) IRT活動の海外連携の強化

FIRSTを通じた活動を活用した海外IRT組織ならびに海外製品ベンダIRTとの連携体制の整備、ぜい弱性対策情報の交換形式を整備するVRDX^{※2}活動を推進しています。

※2 Vulnerability Reporting and Data eXchange

■Hitachi Incident Response Team

<https://www.hitachi.co.jp/hirt/>

<https://www.hitachi.com/hirt>

データ保護の取り組み

個人情報保護の取り組み

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、安全・安心な社会インフラシステムを提供する日立は、お客さまからお預かりした個人情報や、事業運営に関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。

個人情報保護ガバナンスのビジョン

日立の個人情報保護のビジョンとして、①安心・信頼を提供する、②個人の権利を大切にするを掲げ、個人情報

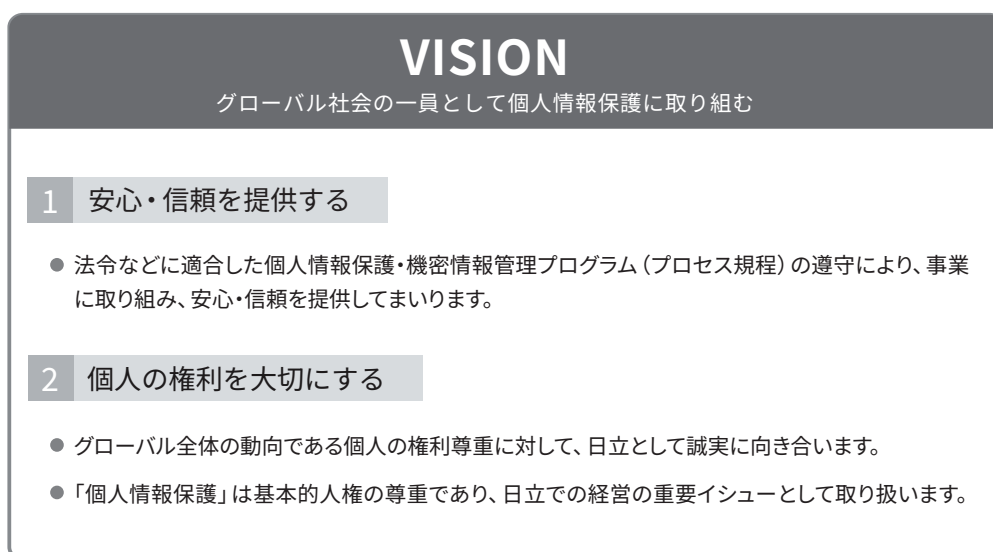
保護を経営の重要イシューとして位置づけ、着実に推進しています。(図表2-②参照)

個人情報保護のフレームワーク

日立では、個人情報の適正な取り扱いの確保について組織として取り組むために、トップマネジメントが個人情報保護方針を策定、この基本方針に従った個人情報管理規則やガイドラインなどの社内規程を策定しています。また、社内規程が法令、プライバシーマーク準拠規格である

JIS Q 15001に適合しているかを確認、評価する仕組みを整備しています。このような規程の整備とともに、実際に個人情報を取り扱うにあたり、四つの側面(組織的、人的、物理的、技術的)から具体的な安全管理措置を講じています。(図表2-③参照)

図表2-② 個人情報保護ガバナンスのビジョン





■個人情報保護方針

日立は、トータルソリューションを提供できるグローバルサプライヤーとして、社内の技術情報や、お客さまからお預かりする情報ははじめさまざまな情報を取り扱っています。このことから、日立ではこれら情報価値を尊重す

るために、情報管理体制の確立とその徹底に努めてきました。この考え方に立ち、日立製作所では以下の個人情報保護方針を制定し、ホームページに掲載するなど広くステークホルダーに公表しています。

(<https://www.hitachi.co.jp/utility/privacy/>)

個人情報保護方針

(1) 個人情報管理規則の策定および個人情報保護マネジメントシステムの継続的改善

当社は、役員および従業員に個人情報保護の重要性を認識させ、個人情報を適切に利用し、保護するための個人情報管理規則を策定し、個人情報保護マネジメントシステムを着実に実施します。さらに、維持し、継続的に改善します。

(2) 個人情報の収集・利用・提供および目的外利用の禁止

当社は、事業活動において、個人情報をお預かりしていることを考慮し、それぞれの業務実態に応じた個人情報保護のための管理体制を確立するとともに、個人情報の収集、利用、提供において所定の規則に従い適切に取り扱います。

また、目的外利用は行わない、およびそのための措置を講じます。

(3) 安全対策の実施ならびに是正

当社は、個人情報の正確性および安全性を確保するため、情報セキュリティに関する諸規則にのっとり、個人情報へのアクセス管理、個人情報の持ち出し手段の制限、外部からの不正アクセスの防止などの対策を実施し、個人情報の漏えい、滅失またはき損の防止に努めます。また、安全対策上の問題が確認された場合など、その原因を特定し、是正措置を講じます。

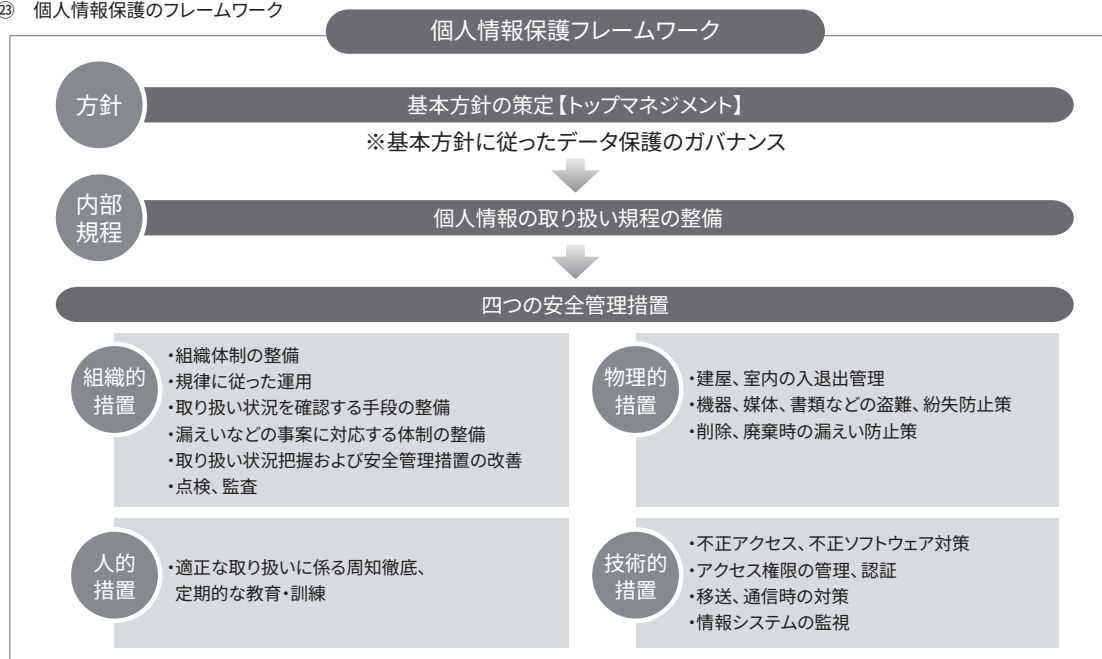
(4) 法令・規範の遵守

当社は、個人情報の取り扱いに関する法令、国が定める指針その他の規範を遵守します。また、当社の個人情報管理規則を、これらの法令および指針その他の規範に適合させます。

(5) 個人情報に関する本人の権利尊重

当社は、個人情報に関して本人から情報の開示、訂正もしくは削除、または利用もしくは提供の拒否を求められたとき、および苦情、相談の申し出を受けたときは、個人情報に関する本人の権利を尊重し、誠意を持って対応します。

図表2-③ 個人情報保護のフレームワーク



データ保護の取り組み

■個人情報規則体系

日立が取得、お預かりした個人情報は、個人情報保護規則群に従って、適切に管理しています。(図表2-②④参照)

■安全管理措置

組織的安全管理措置では、個人情報保護責任者を設置し、個人情報保護体制を整備しています。

個人情報の安全管理に関する従業員の役割・責任や個人情報の取り扱いに関する規程などを定め、それに従った運用を実施しています。また、漏えい事故発生時の対応体制の整備や点検監査に係る規程を定め、運用を実施しています。

人的安全管理措置では、個人情報保護の教育計画に基

づき、階層別教育、専門教育、全従業員eラーニングなど、個人情報の適正な取り扱いに係る各種教育、訓練を実施しています。

物理的安全管理措置では、各所建屋や室内の入退管理や機器・書類などの物理的な保護、盗難などに対する対策、また、機器・書類などの廃棄時の漏えい防止策といった安全対策を行っています。

技術的安全管理措置では、情報システムに対する不正アクセス、不正ソフトウェア対策の実施などを行っています。また、取り扱う個人情報の重要度に応じてアクセス権限の管理、認証、移送、通信時の対策、情報システムの監視などを行っています。

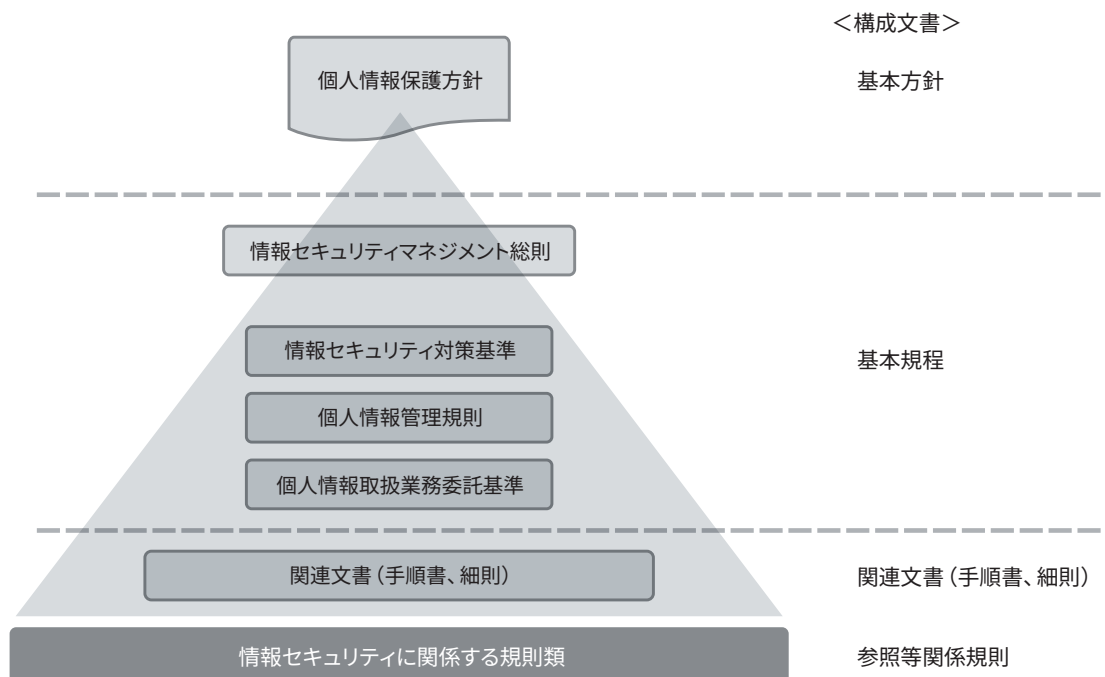
個人情報保護マネジメントシステム

日立の個人情報保護マネジメントシステムはJIS Q 15001に準拠して定められています。個人情報保護に関する方針は個人情報保護方針として定めています。個人情報保護のマネジメントの規則は、52条で規定される情報

セキュリティマネジメント総則で定めています。

個人情報の取り扱いに関しては、73条で規定される個人情報管理規則および12条で規定される個人情報取扱業務委託基準、ならびに関連文書に規定されています。

図表2-②④ 個人情報保護規則体系





■個人情報保護マネジメントサイクル

日立の個人情報保護マネジメントは、定期的にPDCA (Plan-Do-Check-Action) サイクルで実施するフレームワークで、計画を確実に実施し継続して改善していく仕組みを構築しています。

[Plan]では、個人情報保護方針、個人情報保護施策の策定、個人情報保護教育計画、個人情報保護監査計画を立案し、代表者である執行役社長兼CEOが承認します。

[Do]では、個人情報保護施策の社内への展開と運用を行います。個人情報保護教育を実施し、個人情報保護施策や管理方法の周知徹底を図ります。また、個人情報保護に関する推進会議を開催し、各所への情報提供と施策

の実施状況をフィードバックします。

[Check]では、全部署に対し、セルフチェックによる運用確認を定期的の実施し、加えて、監査計画にのっとり他部署の状況を確認する監査を実施します。全社監査計画書、報告書は、監査責任者が策定し執行役社長兼CEOが承認します。指摘事項がある場合は、是正が完了するまで確認します。

[Action]では、個人情報の取り扱いに関する法令などの改正状況、社会情勢の変化、社内外から寄せられた意見、事業領域の変化といった経営環境の変化、社内運用状況の結果などに基づいてマネジメントシステムの見直しを行っています。(図表2-⑤参照)

個人情報の管理と適切な取り扱い

日立では、個人情報保護法より一段高いレベルの管理を行うためにJIS規格「個人情報保護マネジメントシステム—要求事項」(JIS Q 15001) 相当の社内規程を制定し、規則にのっとり、厳格な管理と適切な取り扱いに努めています。職場ごとに個人情報管理の責任者(情報資産管理者)を置き、業務で取り扱う「すべての個人情報」を特定し、当該個人情報の重要性およびリスクに応じて管理し、適切な措置を講じています。

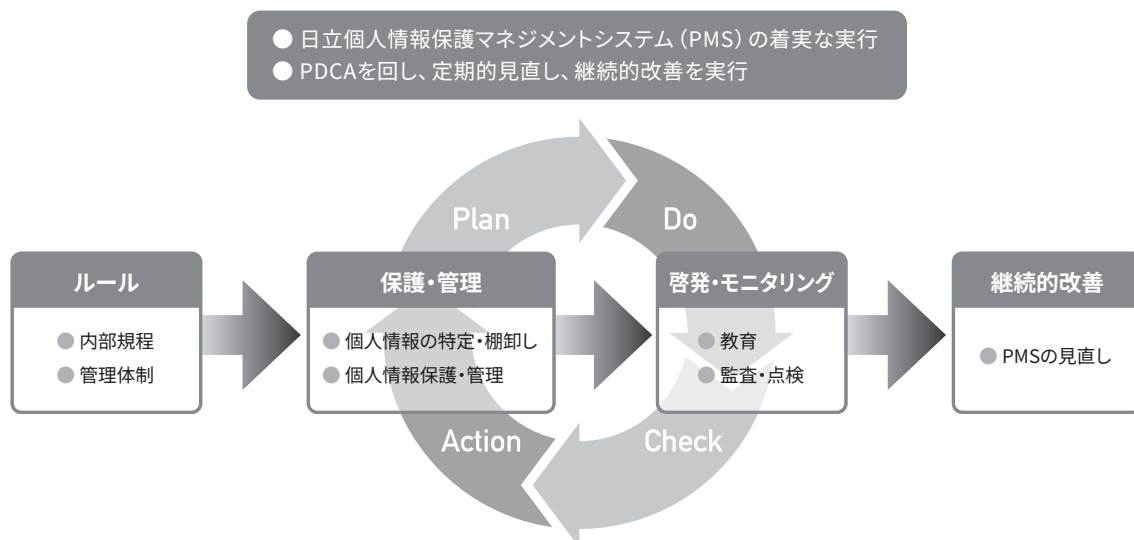
個人情報の取り扱い業務ごとにリスクの認識、分析を実施し、取り扱いに関するルールを定めて運用する「個人情報取扱業務」は、全社一括管理を行っており、定期的に見

直しを実施しています。

また、個人情報取扱者には、当該業務の取り扱いルールの周知徹底を行い、確認した記録を残してから業務を開始しています。運用時は、1カ月に1回職場での自主点検を行い、安全管理措置や運用状況を定期的に確認しています。

日立では、マイナンバー制度に対応した社内規程にのっとり、厳格な管理と適切な取り扱いに努めています。マイナンバーの管理体制を確立して、マイナンバー取り扱い業務のリスクを評価し、適切な措置を講じています。

図表2-⑤ PDCA (Plan-Do-Check-Action) サイクルで実施する個人情報保護マネジメントのフレームワーク



データ保護の取り組み

■個人情報保護に関する監査と点検

日立製作所および国内すべてのグループ会社で1年に1回個人情報保護ならびに情報セキュリティの監査を実施しています。「個人情報保護・情報セキュリティ監査」では、個人情報保護、管理の遵守事項を確認し、法令への適合性を監査します。

また、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により、対応状況をモニタリングし、日立全体として点検に取り組んでいます。また、職場での自主点検として、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、併せて重要な個人情報を取り扱う業務を有する部門については「個人情報保護運用の確認」を1カ月に1回実施するなどし、安全管理措置や運用の状況を定期的に確認しています。

■個人情報保護に関する教育と従業員の理解促進

個人情報の確実な保護のため日立ではすべての役員、

従業員、派遣社員などを対象にeラーニングによる教育を毎年実施しています。また、日立製作所では、個人情報保護方針および情報セキュリティの基本事項を従業員に周知するために、個人情報保護カードを作成し、従業員一人一人に配付しています。

■委託先の管理強化

日立では、個人情報の委託先管理強化にいち早く取り組み、個人情報の取り扱いを委託する際の社内規程を定め、委託先の審査や監督を実施しています。業務を委託する際には、日立と同等以上の個人情報保護の水準にある委託先を選定するために、委託先審査を行っています。さらに、管理体制の確立、再委託原則禁止など厳格な個人情報管理条項を盛り込んだ契約を締結した上で、委託しています。また、定期的に委託先の審査を実施し委託先に責任の自覚を促すなどを行い、委託先の管理・監督を推進しています。

グローバルでの個人情報保護の取り組み

日立では個人情報保護に関する共通の行動規範である「日立グループ プライバシープリンシプル」を定め、各社に個人データ保護推進責任者を設置しています。加えて各社への法令動向の情報共有や各地域の個人データ保護アドバイザーによる支援を通じ、グループ各社に対し、個人情報保護の取り組みの徹底を図っています。また、日立

グループ内の個人情報保護に関するリスク状況を把握し、対処するため、各社の対応状況を継続してモニタリングし、適切な措置を講じています。

今後も引き続き、日立グループ全体の個人情報保護コンプライアンスの徹底に取り組みます。



日立グループのプライバシーマーク※への取り組み

日立では、グループ一体となり、個人情報保護に取り組んでいます。1998年にグループ会社が初取得して以来、2026年7月末時点、38事業者が「プライバシーマーク」を取得し、法令より管理レベルの高い個人情報の保護と取り扱いを行っています。日立製作所は、2025年3月に10回目の付与適格決定を受け、2027年3月の次回更新に向け継続的に取り組んでいます。また、プライバシーマーク取得会社を主体として、「日立グループPマーク連絡会」を組織し、定期的に情報交換会、勉強会、外部有識者を招いての講演会などを実施するほか、グループ全体として、個人情報保護に関する情報共有および研さんを重ねています。

※プライバシーマークとは：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られた事業者に付与される、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）

日立製作所のプライバシーマーク（2026年9月時点）



一般財団法人日本情報経済社会推進協会 プライバシーマーク制度のWebサイトへ (<https://privacymark.jp/>)

■日立グループ プライバシーマーク付与事業者

日立グループのプライバシーマーク付与事業者は、以下のとおりです（2026年7月末時点）。

株式会社 日立製作所
株式会社 日立製作所 病院統括本部
日立健康保険組合
沖縄日立ネットワークシステムズ株式会社
株式会社 九州日立システムズ
日和服务株式会社
株式会社 日立ICTビジネスサービス
株式会社 日立アカデミー
株式会社 日立医薬情報ソリューションズ
日立グローバルライフソリューションズ株式会社
株式会社 日立ケーイーシステムズ
日立交通テクノロジー株式会社
株式会社 日立コンサルティング
株式会社 日立産業制御ソリューションズ
株式会社 日立システムズ
株式会社 日立システムズエンジニアリングサービス
株式会社 日立システムズパワーサービス
株式会社 日立システムズフィールドサービス
株式会社 日立社会情報サービス

株式会社 日立情報通信エンジニアリング
株式会社 日立総合計画研究所
株式会社 日立ソリューションズ
株式会社 日立ソリューションズ・クリエイト
株式会社 日立ソリューションズ西日本
株式会社 日立ソリューションズ東日本
日立チャンネルソリューションズ株式会社
株式会社 日立ドキュメントソリューションズ
株式会社 日立ハイシステム21
株式会社 日立パワーソリューションズ
株式会社 日立ビルシステム
株式会社 日立フーズ&ロジスティクスシステムズ
株式会社 日立プロパティアンドサービス
株式会社 日立保険サービス
株式会社 日立マネジメントパートナー
株式会社 日立リアルエースパートナーズ
株式会社 北海道日立システムズ
日立ヴァンタラ株式会社
株式会社 日立ハイテク

データ保護の取り組み



プライバシー保護の取り組み

AIやIoTなどのデジタル技術の進展に伴い、多種多様なデータの利活用による社会イノベーションの実現が期待される一方で生活者のプライバシー保護への関心が高い状況にあります。日立は、安全・安心を確保した価値創出に向けてプライバシー保護に取り組んでいます。

日立のプライバシー保護の考え方

昨今、個人情報に該当するかどうかを問わず、パーソナルデータの利活用による価値創出が期待されています。それに伴い、個人のプライバシーへの配慮が求められています。加えて、DX時代においては、収集されるパーソナルデータがますます増え、プライバシーに関わるリスクも変化しています。図表2-26に示すとおり、パーソナルデータには、個人情報と一部重複して、「位置情報」や「購買履歴」などのプライバシー性のある情報が含まれます。パー

ソナルデータを利活用した価値創出のためには、個人情報を保護するとともに、プライバシーを保護していく必要があります。

日立は、これまで多数の業務でプライバシー保護に対応したノウハウをお客さまとのビジネスにおいても活用し、プライバシーに配慮したよりよいサービスや技術をお客さまに提供していくことで安全・安心な社会イノベーションの実現に貢献していきます。

日立のプライバシー保護の取り組み

日立製作所は、パーソナルデータの安全・安心な利活用による価値創出をめざし、デジタルシステム&サービスセクターにおいてデータ利活用におけるプライバシー保護に取り組んでいます。

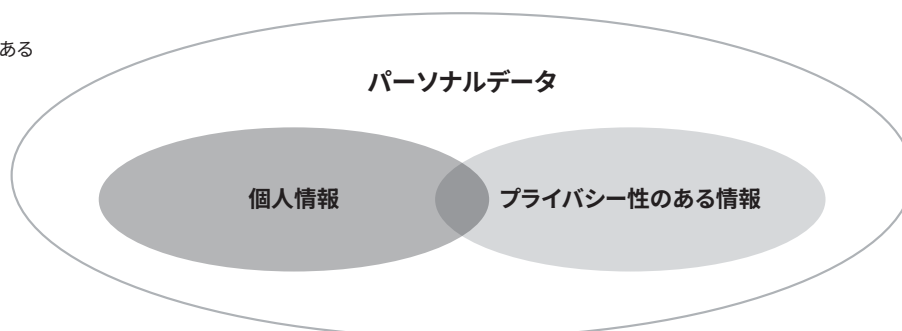
さらに、プライバシー保護対策に対する社会的要請から、プライバシー保護と個人データ活用を両立することで、より適切で高品質なサービスや製品を提供し、消費者をはじめとするステークホルダーとの信頼を醸成することをめざし、日立製作所では、日立プライバシー保護(PIA)制度(以下「PIA制度」)を導入し、個人データを取り扱う業務においてプライバシー影響評価を実施しています。

PIA制度を推進するにあたって、従業員向けのガイドラインおよびチェックシートを整備し、プライバシー影響評価を

行うにあたっての具体的なプロセスやチェックシートにおける留意事項を解説することで、個々の従業員がプライバシー保護対策を実践できるようにしています。チェックシート作成の際に、従業員による判断が難しい場合には、個別相談による支援を行っています。併せて定期的な教育を実施することによって、プライバシー保護の意識向上を図っています。

また、デジタル事業をけん引するデジタルシステム&サービスセクターにおいては、その事業特性から、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、より積極的に、プライバシー保護に関する取り組みを進めています。

図表2-26
パーソナルデータ・プライバシー性のある
情報・個人情報の関係



情報セキュリティに関する社内外活動



昨今のサイバー攻撃の高度化・巧妙化によりサプライチェーンも含め、その影響範囲は拡大しています。日立では、このようなサイバー攻撃の脅威に対抗するために社内のセキュリティ部門とそれ以外の部門が相互に協力していける体制づくりを進めています。また、産・官・学が「協創」できるよう社外への活動などに積極的に参画しています。

情報セキュリティに関する社内活動

サイバー攻撃の対象が企業活動の広範囲にわたることから、平時より社内の多様な部門との連携が不可欠になっています。そのために、製品セキュリティ、サプライチェーンセキュリティ、機密情報管理、セキュリティ技術情報、Webセキュリティなどテーマ別に品質保証、調達、知的財産管理、研究開発、Web管理を管掌する各部門との分科会を設置しています。この活動を通じ、確実なセキュリティ対策ができるよう、タイムリーに相互に情報

交換する体制を構築しています。また、万が一、インシデントが発生した場合は、各ステークホルダーに対する対応も必要であり、営業部門、広報部門、法務部門、調達部門、人事部門などと協力して推進していかなければなりません。有事の際に迅速な対応ができるよう、関係する各部門に窓口を設置し、セキュリティ施策についての情報を提供しています。

情報セキュリティに関する社外活動

サイバーセキュリティ推進に取り組んでいる政府機関、大学や研究機関、他の企業との枠組みを越えたコミュニティでのコミュニケーションを通じ、脅威情報や対策実行時の課題やノウハウを共有・共感することにより、自社にとってより有効な対策につなげることができるだけでなく、

社会全体のセキュリティ強化に寄与することができます。

その観点に立ち、日立では、従業員それぞれの持つ経験や知識を活かし、グローバルに国際標準化活動、CSIRT活動など、情報セキュリティに関する各種社外活動に参画しています。

■ 国際標準化活動

次のセキュリティに関する国際標準化活動に参画しています。

■ ISO/IEC JTC1/SC27

国際標準化機構(ISO)と国際電気標準会議(IEC)による国際標準化のための合同技術委員会ISO/IEC JTC1のサブコミッティであるSC27では、情報セキュリティマネジメントシステム(WG1)、暗号とセキュリティメカニズム(WG2)、セキュリティ評価技術(WG3)、セキュリティコントロールとサービス(WG4)、アイデンティティ管理とプライバシー技術(WG5)などに関する規格化が検討されています。

■ ISO TC292

ISOのテクニカルコミッティ(TC)292では、一般的なセキュリティマネジメント、事業継続マネジメント、レジリエ

ンスおよびエマージェンシーマネジメント、不正防止対策および管理、セキュリティサービス、ホームランドセキュリティ、サプライチェーンの信頼性確保など、さまざまなセキュリティに関する規格化が検討されています。

■ ISO TC262

ISOのTC262はリスクマネジメントをテーマとしており、すべてのリスクを対象とし、用語、原則および指針、リスクアセスメント技法などの規格化が検討されています。

■ ITU-T SG17

国際電気通信連合(ITU)の電気通信標準化部門(ITU-T)のスタディグループ(SG)の一つであるSG17では、サイバーセキュリティ、通信事業者向けセキュリティ管理、

情報セキュリティに関する社内外活動

テレバイオメトリクス、通信・アプリケーションサービスに対するセキュリティ機能、スパム対策、ID管理などの規格化が検討されています。

■ IEC TC65/WG10およびWG20、ISA-99 WG

IECのTC65では、産業用オートメーション、計測、制御の標準化が進められています。その中のWG10では、国際計

測制御学会 (ISA) のISA-99 WGと共同で制御システムに求められる技術的、運用的、および管理的セキュリティ対策の規格化を進めております。また、IEC TC65/WG20では、制御システムにおけるセキュリティと機能安全を両立する開発プロセスに関する規格化を進めています。

■ CSIRT/PSIRT活動

日立では、日立グループにおけるCSIRT/PSIRT活動に加え、HIRTを窓口 (PoC: Point of Contact) として社外CSIRT/PSIRT活動に参画しています。また、社外CSIRT組織などとの連携として、ぜい弱性などに関する情報の共有・交換を推進しています。

■ FIRST

FIRST (Forum of Incident Response and Security Teams) は、大学、研究機関、企業、政府機関などが加盟する信頼関係で結ばれたインシデント対応チームの国際コミュニティです。2026年6月現在で、118カ国、862チームが加盟しています。

■ 一般社団法人日本シーサート協議会 (NCA)

日本で活動するCSIRT組織間の情報共有・連携を通して、CSIRT活動上の課題解決を図るために設立された団

体です。CSIRT設立の促進・支援、インシデント発生した場合のCSIRT間の連携体制づくりなど、国内のCSIRTコミュニティが、いざというときに協力できるよう、組織自身が自主的に「インシデント対応基礎能力」の向上を図れる場を提供しています。日立は、協議会発足メンバーであり、2015年から2020年にかけて運営委員長の立場で一般社団法人化を進め、2021年からは幹事会員として、2022年から副理事長を務め、国内のCSIRT活動の普及を推進しています。

■ そのほかの活動

グローバルでの社外活動として、サイバー空間の安全を保つためにIT・テクノロジー業界に呼びかけられた共同宣言「Cybersecurity Tech Accord」へ賛同し、グローバルな協力体制のもと、サイバー攻撃からユーザー企業を守ることをめざしています。また、情報セキュリティの標準化、サイバーセキュリティ／デジタルリスク対策のベストプラクティスなどに関する先進的な調査研究を行うISF (Information Security Forum) に加盟し、情報セキュリティにおける先端分野の情報交換・共有を行っています。

国内では、次に示すセキュリティに関する研究・検討、普及・啓発などを推進する各種社外活動へ参画しています。また、全国で開催される各種セミナー、学会などにおける講演も行っています。

- ・独立行政法人情報処理推進機構 (IPA) 10大脅威執筆会ほか
- ・一般財団法人日本情報経済社会推進協会 (JIPDEC) ISMS専門部会 ほか
- ・一般財団法人日本サイバー犯罪対策センター (JC3)
- ・特定非営利活動法人日本セキュリティ監査協会 (JASA)
- ・NPO日本ネットワークセキュリティ協会 (JNSA)

- ・日本セキュリティオペレーション事業者協議会 (ISOG-J)
- ・デジタルトラスト協議会 (JDTF)
- ・一般社団法人日本電気計測器工業会 (JEMIMA) 産業計測機器・システム委員会
- ・技術研究組合制御システムセキュリティセンター (CSSC)
- ・一般社団法人電子情報技術産業協会 (JEITA) 情報セキュリ



- ティ調査専門委員会、個人データ保護専門委員会 ほか
- ・フィッシング対策協議会
- ・独立行政法人製品評価技術基盤機構(NITE)評価機関認定技術委員会
- ・ロボット革命・産業IoTイニシアティブ協議会
- ・一般社団法人サイバーリスク情報センター 産業横断サイバーセキュリティ検討会、セキュリティ品質検討委員会ほか
- ・日本セキュリティ・マネジメント学会(JSSM)

- ・計測自動制御学会(SICE)産業応用部門 産業ネットワーク・システム部会
- ・一般社団法人日本自動認識システム協会(JAISA)
- ・一般社団法人ICT-ISAC
- ・一般社団法人Japan Automotive ISAC
- ・一般社団法人交通ISAC
- ・電力ISAC

トピックス

■ NPO日本ネットワークセキュリティ協会との活動 ーゲームによる情報セキュリティ教育への寄与

日立製作所では、サイバーセキュリティの普及啓発に寄与する特定非営利活動法人日本ネットワークセキュリティ協会(以下、JNSA)に、会員企業として参画しています。その一環として、JNSA教育部会ゲーム教育ワーキンググループに参加し、活動を行っています。本ワーキンググループでは、ゲームを活用した情報セキュリティの普及啓発や、実践的なセキュリティ教育に関する調査・研究、企画等を実施しています。

2025年度は、このワーキンググループの活動として、会員各社のメンバーとともに新教材「CoRepo」を企画・制作しました。「CoRepo」は、インシデントが発生した組織の一員となり、情報漏えい事案に

おける対応と報告を通して、その重要性を学習できるボードゲームです。「報告・共有・公表」というテーマは重要である一方、状況によって適切な判断が変化するため、“ケースバイケース”となりがちです。本教材は、様々な状況下における対応を通じて最善の説明ができるかを疑似体験することで、実務に即した判断と、それを適切に伝える説明力の向上に寄与することを目指しています。

今後は、学校(大学・大学院、高専、専門学校、高等学校等)や、NPO・社団法人、コミュニティの勉強会等での活用を推進していきます。



「CoRepo」で使用するカード

*出典：特定非営利活動法人 日本ネットワークセキュリティ協会 ホームページより

情報セキュリティ啓発活動

日立では、一人一人のセキュリティ意識の向上こそがセキュリティの最後の砦(とりで)であると考えています。そのため、既存のガバナンス徹底に加え、従業員の自主性の醸成と、自発的な行動により、セキュリティ意識の底上げをするセキュリティ啓発活動を進めています。

情報セキュリティの「自分ゴト化」

経営幹部や身近な部門になりすました不審メールや電話、不安に付け込むサポート詐欺など、従業員を狙ったサイバー攻撃の脅威はますます高まっており、社員一人一人の十分なセキュリティ意識がこれまで以上に不可欠となっています。今まで攻撃者の主なターゲットは組織のITのぜい弱性でしたが、オフィス以外での働き方においては、「セキュリティ意識のぜい弱性」が狙われることが想定されます。

本来、セキュリティ対策は、「IT」「プロセス」と「人」の3要

素でバランスを取る必要があります。

「セキュリティ意識のぜい弱性」を狙ってくる攻撃に対して、セキュリティリスクを低減するために、従業員への啓発・教育を拡充し、よりバランスの取れたセキュリティ対策を進めています。啓発活動では、「自分ゴト化」と「従業員が心から共感すること」をキーワードに、従業員が受け身ではなく、自らセキュリティに興味を持ち、自分ゴトとして取り組むことをめざしています。

自主性の醸成に向けた活動:Harry's Security

「意識の改革」として、従業員にセキュリティを身近に感じてもらうための社内コミュニケーション「Harry's Security」を推進しています。(図表3-①参照)

この活動は、難しい、面倒というネガティブな印象を持たれがちなセキュリティに対して、まずは興味を持ってもらうこと、そして、身の回りのセキュリティを意識してもらうことをめざしています。

独自に開発したキャラクター「Harry」を活用し、イントラネットやMicrosoft Teams※を活用した社内チャットなどを通じて、従業員一人一人に寄り添った視点で、楽しく、親しみやすい情報発信をしています。イントラネットでは、気軽に情報セキュリティに触れていただけるよう、「Harry」が登場するアニメーションや危険予知トレーニングなどのコンテンツを通じて、情報セキュリティに関する情報を提供しています。

※ Microsoft Teamsは、米国Microsoft Corporationの米国およびその他の国における商標または登録商標です。

図表3-① Harry's Securityの活動

意識の改革

Harry's Security

- 1) 共感 (認知/理解) を得る取り組み
⇒セキュリティに興味を持ってもらう。
- 2) 自分ゴト化をする取り組み
⇒身の回りのセキュリティを意識してもらう。





自発的な行動に向けた活動：GREEN AEGIS

「行動の改革」として、従業員がそれぞれのセキュリティ対策のために自発的に行動することをサポートする社内コミュニティ活動「GREEN AEGIS」を推進しています。(図表3-②参照)

この活動は、セキュリティに興味を持った従業員が、自ら知識を習得・深掘り、共有してもらうことをめざしています。

「セキュリティと楽しく関わりながら、オープンに共有・調和し、広げていくコミュニティ」と位置づけ、イントラネットや専用のMicrosoft Teamsを活用し、実施している取り組みを紹介したり、従業員自らが企画した動画を配信したり、従業員同士が自由に意見交換したり、それぞれが自分に合ったやり方で、自発的にセキュリティに関わっていけるような場を提供しています。

また、毎年、GREEN AEGISにおいて積極的に活動したメンバーを対象に、セミナーやワークショップを開催し、メン

バー間のネットワークの強化を図ることで、コミュニティ活動の拡大に努めています。

図表3-② GREEN AEGISの活動

行動の改革

GREEN AEGIS

セキュリティを自分ゴトとしてとらえ、
従業員一人一人が自発的に行動して
もらう取り組み
⇒知識の習得・深掘り・
共有をしてもらう。



トピックス

■ 攻撃者視点でリスクを考えるための施策を展開

会社幹部や身近な部門の名前を騙るなど、より巧妙にメールや電話などで情報を詐取する攻撃が増加しています。そのような状況下で、攻撃者の視点にたつてどのようなリスクが存在するか考えることは、攻撃を未然に防ぐ意味で重要です。そこで、2025年度は、攻撃者がどのように考えているかを、意識してもらうための施策を展開しました。

「Harry's Security」の活動として、攻撃者のキャラクターである「ワルモノくん」を主人公にして、3話構成のコンテンツを作成して、イントラネットで公開しました(図表3-③)。それぞれ、コンテンツを見た従業員が、攻撃者の立場に立って、職種によってだましやすい方法は何か、フィッシングメールで人をだますためにどういう点を工夫するとだ

ましやすくなるのか、オフィスや電車の中で攻撃できそうなところはどこか、を考えてもらう内容になっています。情報セキュリティe-ラーニングにも取り込んで、広く活用してもらえるように展開しています。

日立グループ従業員向けのセミナーでは、「ワルモノ目線でセキュリティを考える～視点を変えて行動しよう～」をテーマに、外部の有識者の方に講演をいただきました。また、2026年2月1日からの日本政府が定めるサイバーセキュリティ月間にあわせて、攻撃者視点で考えることを伝えるポスター(図表3-④)やPCでのポップアップ表示を日立グループ内に展開しました。

図表3-③ 攻撃者視点で考えるためのイントラコンテンツ



図表3-④ サイバーセキュリティ月間に展開した日立グループ向けポスター



日立は、重要インフラを支えるOTシステムとOT機器のセキュリティ強化に向け、AIを活用したペネトレーションテスト自動化技術と、機密情報を開示せず低帯域環境でも効率的に検査できる出荷前セキュリティ検査技術を開発しています。デジタルツイン環境や通信量削減技術を用いることで、実システムへの影響を抑えつつ、検査の効率化・標準化を進め、社会インフラのレジリエンス向上に貢献します。

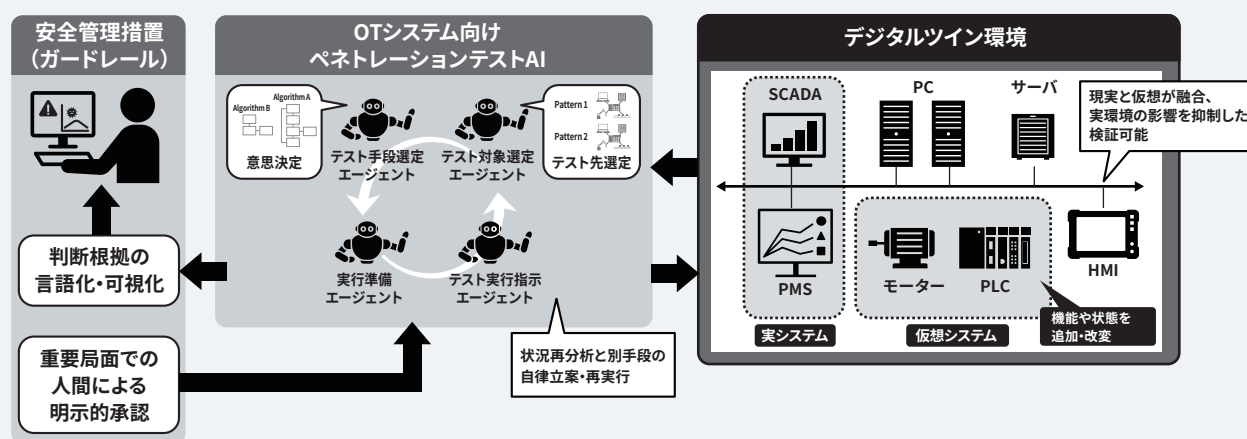
TOPIC

社会の基盤となる電力や交通、製造業などのOT(制御・運用技術)システムの安定稼働を保つためには、システムおよびそれを構成する機器をサイバー攻撃から守るセキュリティ対策を、高品質かつ継続的に推し進めることが求められます。近年、OTを狙ったサイバー攻撃が巧妙化・多様化するとともに、Frontier AIの悪用による攻撃の自動化・高速化も懸念される中、運用中のOTシステム全体の弱点を検証する取り組みと、製品出荷前のOT機器のぜい弱性を発見・修正する取り組みの双方が重要になっています。日立は、OTシステムとOTデバイスの両面からセキュリティ検証技術の高度化に取り組み、重要インフラの強靱性(レジリエンス)向上をめざしています。

OTシステムを狙ったサイバー攻撃が巧妙化・多様化する中、システムの弱点(ぜい弱性)を実際の攻撃者の視点から徹底的に検証する「ペネトレーションテスト(侵入テスト)」の重要性が増しています。しかし、OTシステムは多様なプロトコルや構造を有し規模も大きいいため、ペネトレーションテストの実施は、ITとOT双方の高度な専門知

識を持つ一部の専門家に依存しており、世界的な人財不足が課題となっています。さらに、24時間稼働し続けるインフラシステムを停止させてテストを行うことは困難であるため、実業務への影響を懸念し、網羅的な検証が十分に進まないというリスクが生じていました。これに対し日立では、大規模言語モデルなどのAI技術の活用により検証を自動化することで、専門家の作業負担や属人性を低減できるとの仮説のもと、「OTシステム向けペネトレーションテストAI」(図表4-①)の研究開発を進めています。本技術では、複数の装置やネットワークから構成されるOTシステムに対して、装置やネットワークなどといったシステム構成要素単位のテスト対象の選定、情報収集や管理者レベルの権限取得といったテスト手段の選定、そして実際のテスト実行準備、テスト実行指示といった各フェーズを、専門の「エージェント」たちが分担します。これにより、単なる定型作業の自動化にとどまらず、一つのテストパターンが行き詰まった際にも状況を再分析し、別の手段を自律的に立案・再実行するなど、まるで熟練の専門家チームのように協調的で柔軟なテストの実現をめざしま

図表4-① OTシステム向けペネトレーションテストAI技術概要



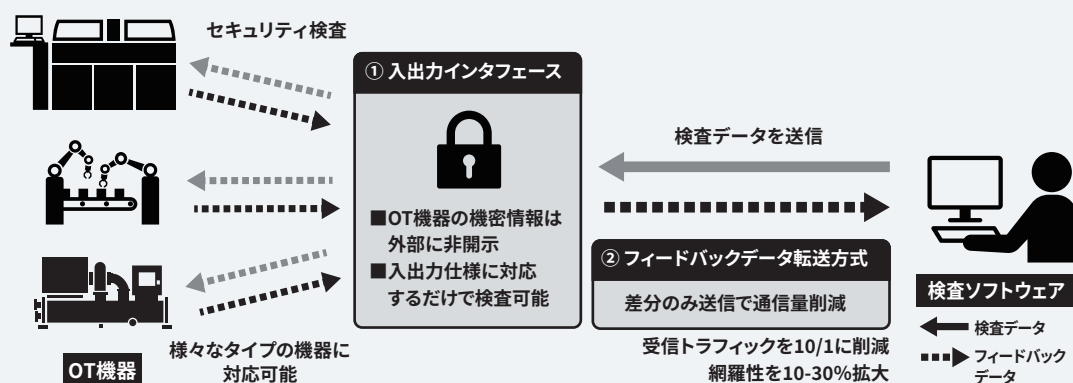
す。また、本技術の特筆すべき強みのひとつは、現実のシステムを構成するソフトウェアやハードウェアといった実システムと、それらをベースに機能や状態を仮想的に追加・改変した仮想システムが融合する「デジタルツイン環境」へテストを行う点です。これにより、稼働中の実システムへの影響を可能な限り抑制しつつ、現実のシステムに極めて近い検証が可能になります。同時に、AIによる不適切な判断やテストを防ぐための安全管理措置（ガードレール）として、AIがそのテスト手法を選んだ判断根拠を人間が理解できるように言語化・可視化するほか、装置の操作やデータの外部転送など、システムに重大な影響を及ぼす可能性のある局面では必ず「人間の明示的な承認」を要求する仕組みを開発しています。

一方、OTシステムを構成する工場や電力設備などのOT機器についても、製品出荷前にぜい弱性を発見して修正することは、運用開始後の被害を抑えるうえで重要です。OT機器の安全性確認では、疑似的な攻撃を繰り返して弱点を見つける検査（ファジング）が有効です。しかし、検査には専門的な設備やノウハウが必要なため、外部機関に委託する場合があります。その際、ソースコードなどの機密情報を開示しにくいことが課題でした。加えて、通信帯域に制限がある環境では、検査の進み具合を示すカバレッジビットマップの送受信が通信のボトルネックとなり、検査回数を増やしにくい状況でした。そこで日立は、機密情報を開示せずに通信帯域に制限がある環境でもOT機器の

出荷前セキュリティ検査を効率化する技術（図表4-②）を開発しました。本技術では、製品ごとに異なる検査ツールと機器の接続方法を検査用ソフトウェアの工夫で共通化し、検査に必要な情報だけをやり取りする入出力インタフェースを定義します。これにより、外部の検査機関にソースコードなどの機密情報を開示せずに、ファジングなどの検査を実施できます。さらに、検査の進み具合を示すカバレッジビットマップについては、変化した部分だけを送信し、変化がない場合は過去の類似データのIDのみを送ることで通信量を抑えます。通信速度が10Mbps～100Mbpsの通信帯域に制限がある環境で、OTで用いられるWebサーバを想定して評価した結果、従来方式と比べて、検査ツール側の受信トラフィックを10分の1に削減し、検査の精度を維持したまま網羅性を10～30%拡大できることを確認しました。これにより、時間当たりの検査回数を増やすことが可能となり、出荷前セキュリティ検査の標準化・省力化を進めることができます。日立は、こうしたOTシステム向け、OT機器向けのセキュリティ検証技術を通じて、お客様の大切な資産と社会インフラのレジリエンスを継続的に高め、安全・安心な社会の実現に貢献していきます。

なお、本成果の一部はNEDO(国立研究開発法人新エネルギー・産業技術総合開発機構)の委託事業「経済安全保障重要技術育成プログラム／先進的サイバー防御機能・分析能力強化」(JPNP24003)によるものです。

図表4-② OT機器向けファジング技術概要



第三者評価・認証

ISMS認証取得状況

日立製作所および国内グループ会社が、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認証を取得した組織は以下のとおりです (2026年7月末時点)。

また、海外においても認証取得を進めており、例えば、日立エナジーでは、ISO/IEC 27001に基づくグローバルなマルチサイト認証制度を活用し、組織全体でISMS認証を取得しています。

- 株式会社 日立製作所 (金融第二システム事業部 公共系金融システム部門)
- 株式会社 日立製作所 (AI&ソフトウェアサービスビジネスユニット・マネージド&プラットフォームサービス事業部・デジタル事業開発統括本部 Business Development Data & Design・アプリケーションサービス事業部 テクノロジートランスフォーメーション本部 デリバリー・トランスフォーメーション本部)
- 株式会社 日立製作所 (社会システム事業部 戦略企画本部、エネルギーシステム第一本部、エネルギーシステム第二本部、エネルギーソリューション本部及びモビリティソリューション&イノベーション本部)
- 株式会社 日立製作所 (社会ビジネスユニット 公共システム事業部)
- 株式会社 日立製作所 (インダストリアルOTソリューション事業統括本部 環境事業部 TSSグリーンデジタルソリューション部 スマートユーティリティ本部 情報システムエンジニアリング部 水事業部 社会システム本部 サービス部 SIDXグループ、コネクティブインダストリーズセクター デジタルITイノベーション本部 セキュアITイノベーションセンタ 情報保全グループ)
- 株式会社 日立製作所 社会ビジネスユニット ディフェンスシステム事業部 (横浜事業所)、営業統括本部 デジタルシステム&サービス営業統括本部 ディフェンス営業本部および株式会社 日立アドバンスシステムズ (本社)
- 株式会社 日立製作所 (デジタルシステム&サービスセクター デジタルサービスビジネスユニット エンタープライズソリューション事業部 ライフインダストリー・プラットフォームソリューション本部 プラットフォームソリューション部)
- 株式会社 日立製作所 (デジタルサービスビジネスユニット 金融第一システム事業部 金融システム第五本部 サービス事業推進センタ)
- 日立チャネルソリューションズ株式会社
- 株式会社 日立社会情報サービス
- 日本スペースイメージング株式会社
- 株式会社 日立情報通信エンジニアリング (マネージドサービス部)
- 株式会社 九州日立システムズ
- 株式会社 日立システムズ (公共・社会事業グループ)
- 株式会社 日立システムズ (公共プラットフォーム事業部)
- 株式会社 日立システムズ (コンタクトセンタ&BPOサービス事業部)
- 株式会社 日立システムズ (サービス・ソリューション事業統括本部 フロントライン協創推進本部 フィールドサービスプラットフォーム推進部)
- 株式会社 日立システムズ (産業・流通事業グループ 産業・流通情報サービス第一事業部 ライフサイエンス&SAPインフラサービス本部 福祉・健康支援サービス部)
- 株式会社 日立システムズ (マネージドサービス事業部、セキュリティサービス事業部)
- 株式会社 日立システムズ (アライアンス・サービス事業部 テクニカルサービス第一本部、テクニカルサービス第二本部)
- 株式会社 日立システムズ パワーサービス (ICTサービス事業部 プラットフォームサービス本部)
- 株式会社 日立システムズ エンジニアリングサービス (マネージドサービス事業グループ)
- 株式会社 日立システムズ エンジニアリングサービス (公共・社会システム事業部、企業システム事業部 企業第二システム本部 第三システム部)
- 株式会社 北海道日立システムズ
- 株式会社 日立ソリューションズ・クリエイト
- 株式会社 日立ソリューションズ西日本 (クラウド基盤運用サポート部)
- 株式会社 日立ソリューションズ東日本 (社会基盤ソリューション第三本部)
- 株式会社 日立ソリューションズ東日本 (サービスデリバリ第一グループ)
- 株式会社 日立ソリューションズ (サブスクリプションプラットフォームサービスの運用保守)
- 株式会社 日立ソリューションズ (セキュリティ診断業務)
- 株式会社 日立ソリューションズ (資産配布管理ソリューション部)
- 株式会社 日立医薬情報ソリューションズ
- 株式会社 日立ケーイーシステムズ
- 株式会社 日立ハイテク (ソリューションセンター)
- 株式会社 日立ハイテク (粒子線治療製品本部 運用サービス部 オペレーション&サービスグループ)
- 株式会社 日立マネジメントパートナー (経営企画本部、人事ソリューション事業部)

IT セキュリティ評価・認証の取得状況

独立行政法人情報処理推進機構 (IPA) が運用するISO/IEC15408に基づく「ITセキュリティ評価および認証制度」によって認証された主な製品は、次のとおりです (2026年7月末時点で“認証製品アーカイブリスト”への掲載を含みます)。(図表5-①参照)

図表5-① 「ITセキュリティ評価および認証制度」によって認証された主な製品一覧

製 品	TOE種別 ^{※1}	認証番号	評価保証レベル ^{※2}
HiRDB/Parallel Server Version 8 08-04	データベース管理システム	C0225	EAL4+ALC_FLR.1
HiRDB/Single Server Version 8 08-04	データベース管理システム	C0216	EAL4+ALC_FLR.1
HiRDB Server Version 9 (Linux版) 09-01	データベース管理システム	C0351	EAL2+ALC_FLR.2
Smart Folder PKI MULTOS application 03-06	スマートカード用アプリケーションソフトウェア	C0014	EAL4
Hitachi Device Manager Software, Hitachi Tiered Storage Manager Software 8.0.1-02	Access Control Device and Systems	C0536	EAL2+ALC_FLR.1
Hitachi Virtual Storage Platform G1000, Hitachi Virtual Storage Platform VX7 Control Program 80-01-25-00/00 (R8-01A-06_Z)	ストレージ装置制御ソフトウェア	C0514	EAL2+ALC_FLR.1
Hitachi Unified Storage VM Control Program 73-03-09-00/00 (H7-03-10_Z)	ストレージ装置制御ソフトウェア	C0513	EAL2+ALC_FLR.1
Hitachi Unified Storage 110用マイクロプログラム 0917/A	ストレージ装置制御ソフトウェア	C0421	EAL2
Hitachi Unified Storage 130用マイクロプログラム 0917/A	ストレージ装置制御ソフトウェア	C0420	EAL2
Finger Vein Authentication Device UBReader2 Hardware: D, Software: 03-00	生体認証装置	C0332	EAL2
証明書検証サーバ 03-00	PKI	C0135	EAL2
CBTエンジン 01-00	CBT試験システム 主要アプリケーション	C0288	EAL1+ASE_OBJ.2、 ASE_REQ.2、ASE_SPD.1
汚染拡大防止システム SHIELD/ExLink-IA 1.0	セキュリティ管理ソフトウェア	C0090	EAL1
Hitachi Virtual Storage Platform One Block 23/24/26/28 with Drive Box HA-DKC-04A-03X	リモート管理付き ディスクストレージ装置	C0870	PP適合(collaborative Protection Profile for Network Devices Version 3.0e(認証識別: CCEVS-VR-PP-0099))

※1 TOE (Target Of Evaluation)

評価の対象となるソフトウェアやハードウェアなどの製品のことをTOEと言います。関連する管理者および使用者の手引書 (利用者マニュアル、ガイダンス、インストール手順書など) を含むことがあります。

※2 EAL (Evaluation Assurance Level)

ISO/IEC 15408では、規定した評価項目 (保証要件) に対する保証の度合いを、EAL1から7まで7段階のレベルで規定しており、段階が上がるごとに評価の内容が厳しくなります。

・EAL1は、セキュリティ機能の妥当性とテスト、セキュリティを維持するためのガイダンスが客観的に評価されます。

・EAL2は、一般的な攻撃能力を想定したぜい弱性分析、製造から運用開始まで、製品の完全性の観点から評価が追加されます。通常の開発ライフサイクルにセキュリティ的な視点を加味しています。

・EAL3は、EAL2で得られる保証に加えて、テストの網羅性や開発時の製品の改ざんを防止するための開発環境の評価が実施されます。

・EAL4は、一般的な商用製品として最高位とされており、開発環境での開発資産の健全性やソースコード、要員の信頼性など開発ライフサイクル全般にわたって評価されます。

・ALC_FLR.1は、製品にセキュリティの欠陥が発見された場合、必要なパッチを提供する基本的な手続きを客観的に評価します。規格では規定のEALに含まれない保証要件を追加することができ、その場合、EAL2+ALC_FLR.1のように表記します。

・ALC_FLR.2は、利用者からのぜい弱性情報の報告受け付けと利用者への通知手続きが求められます。

第三者評価・認証

暗号モジュール試験・認証の取得状況

IPAが運用するISO/IEC19790に基づく「暗号モジュール試験および認証制度（JCMVP）」または米国NISTとカナダCSEが運用するFIPS140-2、FIPS140-3に基づく「Cryptographic Module Validation Program」

（CMVP）によって認証された主な製品は、次のとおりです（2026年7月末時点でCMVPによる“historical list”への掲載を含みます）。

（図表5-②参照）

図表5-② 「Cryptographic Module Validation Program」（CMVP）によって認証された主な製品一覧

製 品	認証番号	レベル
Hitachi Storage Hardware Encryption Module	5389	Level 2
Hitachi Embedded Storage Manager Kernel Crypto API Cryptographic Module	5086	Level 1
Hitachi Storage Hybrid Firmware Encryption Module	5013	Level 1
Hitachi Vantara Cryptographic Library	4239	Level 1
Hitachi Virtual Storage Platform (VSP) Encryption Board for NVMe	4194	Level 1
Hitachi Virtual Storage Platform (VSP) Encryption Module	4183	Level 2
Hitachi Virtual Storage Platform (VSP) Encryption Board for NVMe	4076	Level 1
Hitachi Virtual Storage Platform (VSP) Encryption Module for NVMe	3803	Level 2
Hitachi Flash Module Drive HDE	3314	Level 2
Hitachi Virtual Storage Platform (VSP) Encryption Board	3279	Level 1
Hitachi Virtual Storage Platform (VSP) Encryption Module	3278	Level 2
Hitachi Virtual Storage Platform (VSP) Encryption Adapter	2727	Level 2
Hitachi Virtual Storage Platform (VSP) Encryption Board	2694	Level 1
Hitachi Virtual Storage Platform (VSP) Encryption Module	2462	Level 2
Hitachi Virtual Storage Platform (VSP) Encryption Engine	2386	Level 1
Hitachi Unified Storage Encryption Module	2232	Level 1
HIBUN Cryptographic Module for User-Mode 1.0 Rev.2	JCMVP #J0015、CMVP#1696	Level 1
HIBUN Cryptographic Module for Kernel-Mode 1.0 Rev.2	JCMVP #J0016、CMVP#1697	Level 1
HIBUN Cryptographic Module for Pre-boot 1.0 Rev.2	JCMVP #J0017、CMVP#1698	Level 1
Keymate/Crypto JCMVP ライブラリ (Solaris ^{※1} 版 および Windows ^{※2} 版)	JCMVP #J0007	Level 1
Keymate/Crypto JCMVPライブラリ	JCMVP #J0005	Level 1

※1 Solarisは、Oracle Corporationおよびその子会社、関連会社の米国およびその他の国における登録商標または商標です。

※2 Windowsは、米国Microsoft Corporationの米国およびその他の国における商標あるいは登録商標です。

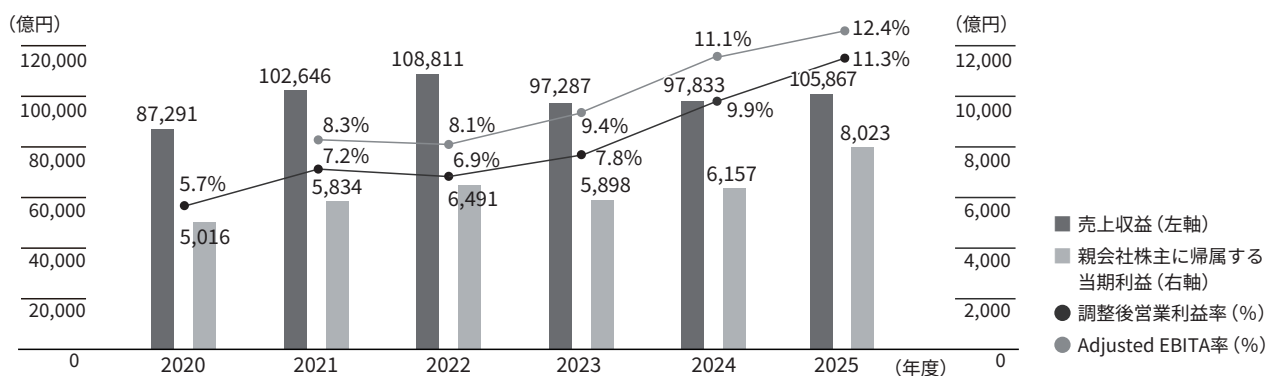
日立グループの概要

会社概要 (2026年3月31日時点)

商号	株式会社 日立製作所	代表者	代表執行役 執行役社長兼 CEO 徳永 俊昭
設立年月日	大正9年(1920年)2月1日 (創業明治43年<1910年>)	資本金	466,666百万円
本店の所在地	東京都千代田区丸の内一丁目6番6号	従業員数	287,901人(国内115,544人 海外172,357人)

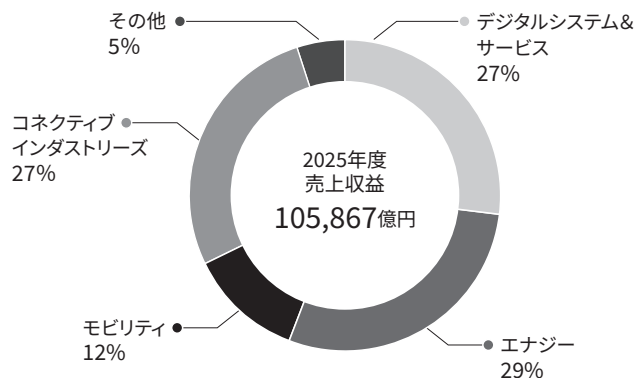
業績ハイライト (2026年3月期連結IFRS) 当社の連結財務諸表は、国際財務報告基準(IFRS)に基づいて作成しています。

売上収益	105,867億円(前期比8%増)	調整後営業利益率	11.3%(前期比1.4ポイント増)
当期利益(親会社株主帰属)	8,023億円(前期比30.3%増)	Adjusted EBITA率	12.4%(前期比1.3ポイント増)
Adjusted EBITA ^{※1}	13,114億円(前期比21.0%増)		

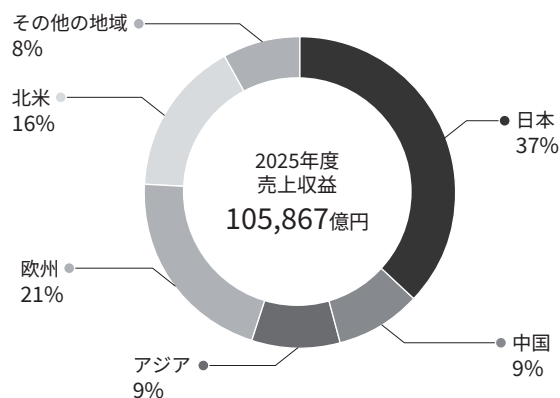


※1 Adjusted EBITA (Adjusted Earnings before interest, taxes and amortization): 調整後営業利益に、企業結合により認識した無形資産等の償却費を足し戻した上で、持分法による投資損益を加算して算出

日立グループの事業構成^{※2}



地域別売上収益/構成比^{※2}



※2 各セグメントの売上収益の売上収益合計に占める割合です。各セグメントの売上収益には、セグメント間の内部売上収益を含んでいます。

株式会社 日立製作所
デジタル&セキュリティ統括本部

〒100-8280 東京都千代田区丸の内一丁目6番6号
TEL.03-3258-1111