HITACHI

情報セキュリティ報告書 2025




日立グループ

INDEX

〈本報告書の概要〉

●報告範囲・期間：2024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：2025年12月発行

CD&SOメッセージ

執行役常務
Chief Digital and Security Officer (CD & SO)
マイケル・グッドマン

より安全な未来の構築に向けて「ハーモナイズドソサエティ」の実現をめざしてサイバーセキュリティの取り組みを強化

日立は、世界中の政府、企業、地域社会から信頼されるパートナーであり、私たちの技術は交通、エネルギー、ヘルスケア、金融など人々の生活に不可欠なシステムに深く組み込まれています。日立は社会の基盤となる重要なインフラを常に支え、守っていく重大な責任を有しており、私たちの事業活動において、「安全性」と「レジリエンス」を最優先に考えていかなくてはなりません。

2025年4月、日立は新経営計画「Inspire 2027」を発表しました。「Inspire2027」では、環境・幸福・経済成長が調和する「ハーモナイズドソサエティ」の実現に貢献することを目標としています。より良い未来を築く上で「イノベーション」と「コネクティビティ」の重要性が高まっていることを意識し、デジタルを私たちの全事業のコアに据えていることが、この経営計画における大切なポイントです。

現在のデジタル化が進む中、サイバーセキュリティは、私たちがこれからめざす社会の実現において、その中核となるテーマです。もはや単なる技術的な挑戦ではなく、「安全」と「レジリエンス」を支える重要な柱となっています。一方、サイバーセキュリティに対する脅威の状況は絶えず変化しており、組織や個人への影響は複雑さと規模の両面で拡大しています。自社のシステムだけでなく、パートナー企業やお客さまのシステムのセキュリティを守ることは、単なる事業上の必要性を越えて、企業が果たすべき根本的な社会的責任となっています。

日立はサイバーセキュリティを企業にとっての最重要リスクとして、重要な経営課題と位置づけています。現在および将来にわたって、日立の企業活動、提供するソリューション、そしてお客さまやそのエンドユーザーを守っていくことに、強い決意をもって取り組んでいます。そのために、私は、Chief Digital & Security Officer（CD&SO）として、日立のサイバーセキュリティ能力の向上のための取り組みを推進していきます。先端テクノロジーとグローバルな専門知識を統合し、日立が製品・サービスを提供する地域、産業界に対して、新たなリスクにも対応できる強固で適応力をもった、迅速な対応が可能な防御体制を構築していきます。

日立のサイバーセキュリティの全体戦略は、長年培ってきた安全とイノベーションの文化を基盤としています。より挑戦的なビジョンをもって、強固なガバナンスを強化するとともに、組織のすべてのレベルにおいて高度なサイバーセキュリティ対策の統合を加速させていきます。これらの取り組みは、これまで築いてきた基盤から転換するのではなく、むしろ継続的な進化を意味するものです。これにより、新たに発生するリスクや変化し続ける事象に先んじて対応できるようにしていきます。

今後、より強い意志を持って、グローバルで社会を支える重要なシステムの「レジリエンス」を強化するための、技術、人財の確保、関連企業とのパートナーシップの強化に注力し続けていきます。ステークホルダーの皆様と共に、より強くつながり、より安全で調和の取れた社会を築いていくことをめざしていきます。

日立は、すべての人々にとってより安全で豊かな未来を築くために、ステークホルダーの皆様の信頼を大切にし、揺るぎない決意をもって、サイバーセキュリティに取り組んでいきます。

情報セキュリティの考え方

デジタル化の急速な進展により、新たな価値が生み出される中、グローバルでの複雑な政治・経済情勢などにより、事業環境も日々変化しています。一方で、日々高度化・巧妙化するサイバー攻撃による情報漏えいやシステム停止など、事業そのものの継続に支障をきたすリスクが拡大しています。このリスクを最小化するため、情報セキュリティ※に関わ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。

※ 本報告書で使用する「情報セキュリティ」の用語については、特段の記載がない限り個人情報保護を含んでいます。

経営戦略としての情報セキュリティ

日立は、日々変化する事業環境を把握・分析し、社会的課題や日立の競争優位性、経営資源などを踏まえ、日立として備えるべき「リスク」への対応と、さらなる成長「機会」の両面からリスクマネジメントを実施し、リスクをコントロールしながら収益機会の創生を図っています。

日々、高度化・巧妙化するサイバー攻撃は、従来の社内IT※1システムだけでなく、OT※2分野である生産・製造環境、開発環境、お客さまに提供した製品・サービスやサプライチェーンを狙った攻撃にまで拡大してきています。

その結果、世界のどの地域でも攻撃を受ける可能性が高まっており、情報漏えいやシステム停止など、その攻撃が事業継続に与える影響は計り知れません。

加えて、各国・地域でセキュリティやデータ保護に関する法規制強化が進められており、サイバー攻撃によって、万が一、情報が漏えいした場合は企業コンプライアンスの観点からもリスクが高まっています。

2025年に策定した日立の新経営計画「Inspire 2027」において、情報セキュリティに関する目標として、セキュリティを取り巻く世の中の動向やグローバルでの法令動向を踏まえ、「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」と設定しています。その目標に向けて、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もとにした「サイバーセキュリティスコア」をモニタリングし、日立製作所 グループ・コーポレートの情報セキュリティリスク統括部門（以下、情報セキュリティ統括部門）が的確なセキュリティ施策を実行しているかどうかを自己評価し、その結果にもとづいた対策を実行していきます。

※1 Information Technology
※2 Operational Technology

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	サイバーセキュリティを経営課題として位置づけたセキュリティ対策を継続的かつ着実に実行する。しかし、絶対の安全はない。故に、有事の際には、短い時間で回復できる抵抗力をつける。（事業継続性の担保）
協創	高度化/増加するサイバー攻撃へ対処するために、社内のコミュニケーションを拡充し、さらには、社会全体でのセキュリティエコシステムを構築し仲間を増やす。
自分ゴト化	社員一人一人がセキュリティを正しく理解・共感し、自分ゴトとしてとらえて行動することができる意識づくりを醸成する。

セキュリティレジリエンスの向上 → しなやかなセキュリティ耐性を身に付ける

■ 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、調達部門などと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。

このエコス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）

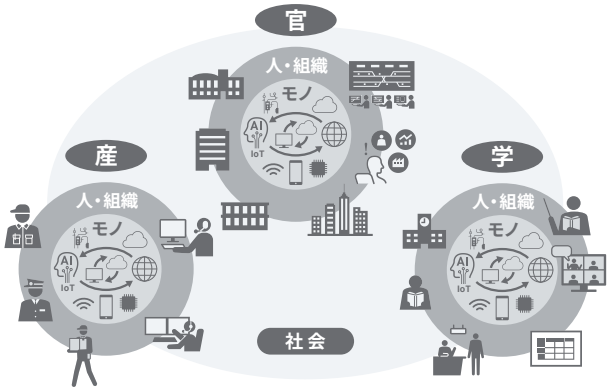
※1 Digital Transformation　※2 Internet of Things

■ 自分ゴト化：新たなセキュリティ啓発に向けた取り組み

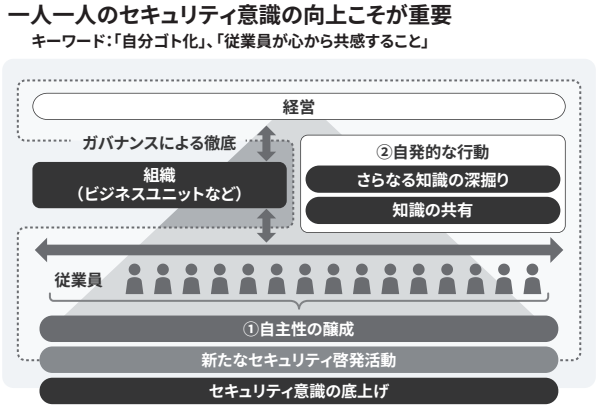
ここ数年で定着したテレワーク中心の働き方においては、「セキュリティ意識のぜい弱性」が狙われることが想定されます。オフィス以外で仕事をすることにより、近くに相談できる相手がいないなど、誰しもがリスクと隣り合わせになってきているのが現状です。

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スタートさせています。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



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

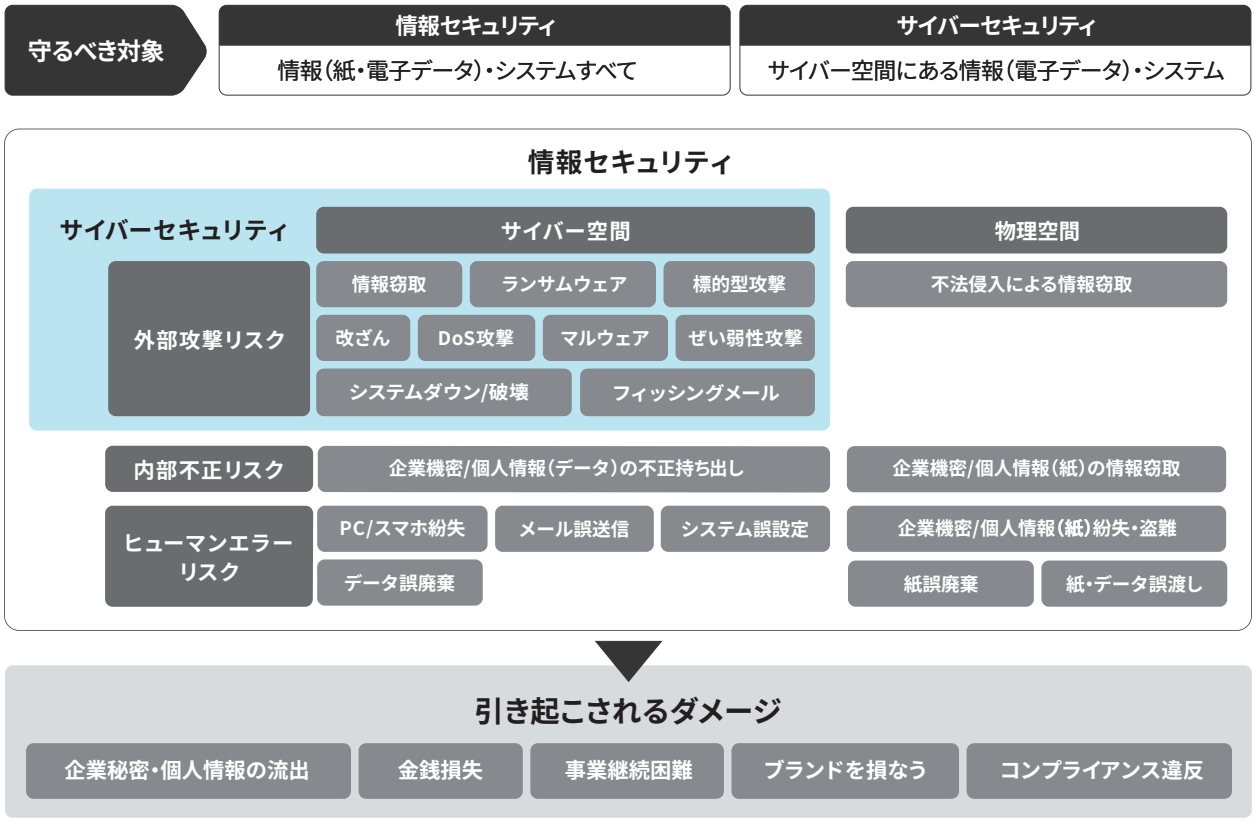
日立が「情報セキュリティ」の維持のために守るべき対象は、図表1-④に示すとおり、いわゆる情報資産である「情報」と「システム」のCIA、機密性（Confidentiality）、完全性（Integrity）、可用性（Availability）と考えています。

■ 情報セキュリティの対象範囲

「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。

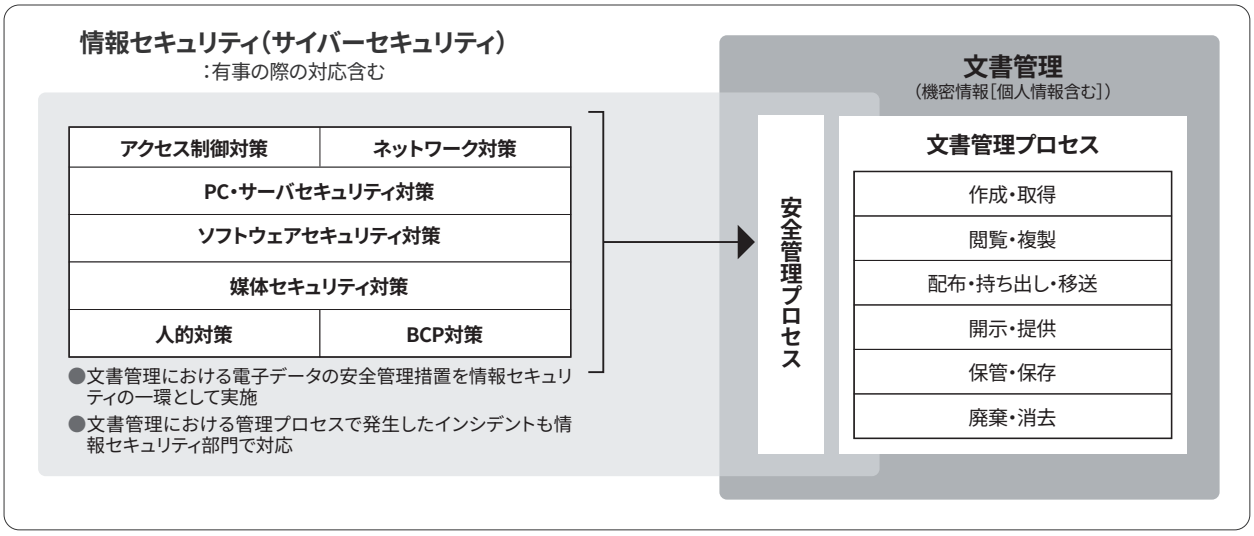
日立では、外部からの攻撃、内部不正、ヒューマンエラーなどリスクの発生要因と情報の流出、経済損失、事業継続が困難になる、ブランドを損なう、コンプライアンス違反などのリスク事象からリスクが具現化した場合に引き起こされるダメージを想定し、リスク管理の視点で情報セキュリティの戦略・施策を立案しています。

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。

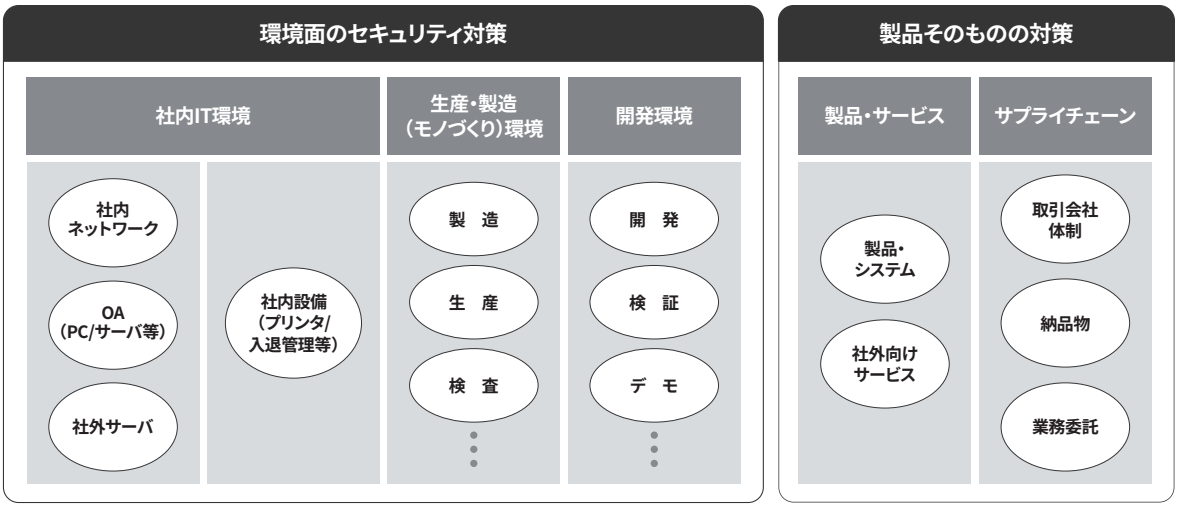
図表1-⑤　現状の情報セキュリティ部門の管理範囲



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

日立は、世の中のセキュリティインシデントの状況やセキュリティおよびデータ保護の法規制動向を踏まえ、価値創造とリスクマネジメントの両面から情報セキュリティ戦略を立案し、施策を展開しています。

■ 情報セキュリティを取り巻く環境

近年のセキュリティインシデントの特徴としては、攻撃手法の多様化やアタックサーフェス※が拡大し続けていることがあげられます。攻撃者がインターネットに露出した機器におけるぜい弱性や、それら機器に対する管理不備があれば、そこを攻撃して情報窃取やランサムウェア感染を行い、身代金を要求する手口は、いまだに変わっておらず、引き続き、対策不備や管理不備を放置すると、必ず被害発生につながるということを認識する必要があると考えています。

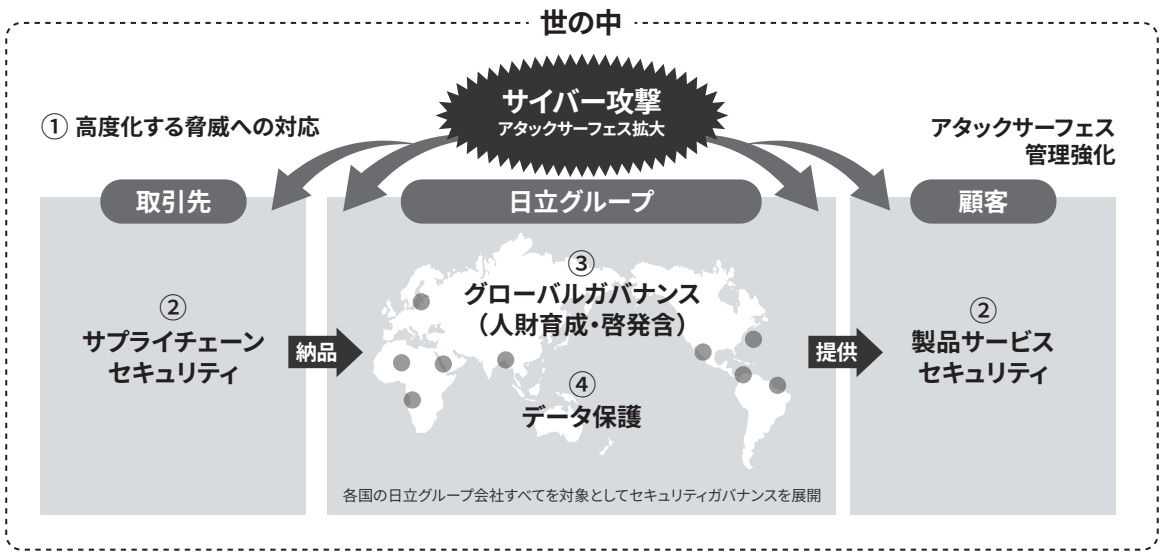
また、セキュリティの法規制動向としては、23年度から継続しているEU圏でのビジネスを展開する際の製品サービスへの規制の動きに加え、日本でもセキュリティに関する規制強化の動きが活性化してきています。特に日本では、24年度に入り経済安全保障推進法、能動的サイバー防御、セキュリティクリアランスに関して急速な動きがあり、25年度には新たな法案審議や各種法律の施行が始まるため、今後各種法令に関わる実施事項に関して注視が必要と考えています。

※インターネットなど外部から攻撃を受ける可能性のある情報資産

■ 重点テーマと活動状況

情報セキュリティを取り巻く環境を踏まえ、日立ではセキュリティ戦略として、図表1-⑦に示す4つのポイント①高度化する脅威への対応、②製品サービス・サプライチェーンセキュリティ、③グローバルガバナンス、④データ保護への対応を推進してきました。

図表1-⑦　重点テーマ



1.高度化する脅威への対応

グローバルでの迅速な対応を実現するために、サイバー攻撃の検知および対策能力の強化を進めるとともに、インテリジェンス情報のグローバルでの活用を進めてきました。また、万が一の攻撃の際に対象を迅速に特定するために情報資産管理の強化に取り組んできました。さらに、アタックサーフェス管理※を強化するとともに、攻撃の対象となることが増えてきているクラウドサービスやインターネットに露出している機器など高リスク環境について再チェックを進めてきました。

※インターネットなど外部から攻撃を受ける可能性のある情報資産を把握、監視、分析、修復を継続的に行うこと。

2.製品サービス・サプライチェーンセキュリティ

手順やルールの確実な実行などセキュリティ対策を維持するために、3つのディフェンスライン※のコンセプトに基づいて仕組み構築を進めてきました。また、製品・サービスセキュリティに関しては、各ビジネスユニット（以下、BU）・グループ会社に設置された PSIRT（Product Security Incident Response Team）のメンバーと情報共有やそれぞれの課題解決のための連絡会を定期的に開催し、各PSIRTの機能強化を進めてきました。サプライチェーンにおいては、セキュリティ意識の向上をめざし、説明会など調達パートナーとのコミュニケーション強化を進めてきました。

※3つのディフェンスラインの詳細は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。

3.グローバルガバナンス強化

日本以外の米州、欧州、アジア、インド、中国の五つの各国・地域に本社直轄の情報セキュリティ担当部門として設置したリージョンブランチを中心に、各国・地域のグループ会社を対象とした情報共有会議、セミナーを開催し、セキュリティマネジメント機能とインシデントレスポンス機能強化を進めてきました。また、2027年12月からEU域内で完全適用されるCRA(サイバーレジリエンス法)など、各BU・グループ会社で対応が必要となるサイバーセキュリティ法制度への支援を進めてきました。

4.データ保護強化

データ保護においても、現状のデータ保護部隊の強化を行い、グローバルで情報セキュリティ統括部門をヘッドとした一体運営を進めてきました。また、データ保護プロセスを規定したプレイブックを作成し、これらの周知徹底や訓練など対応プロセスの整備を進めてきました。さらに、中国デジタル三法に加え、インド、ベトナムの個人データ保護法に関しても、各種対応を進めてきました。

今後の重点取り組み

日立は、世の中動向、日立の施策の実効状況を踏まえ、グループ全体の情報セキュリティリスク低減のために、さらなる情報セキュリティリスク管理の実効性向上およびサイバー攻撃対策の着実な実効を目標として、次の対応を推進していきます。

1.情報セキュリティリスク管理の実効性向上

グローバルでの情報セキュリティマネジメントおよびデータ保護マネジメントの継続的かつ着実な実効が重要と考え、情報セキュリティ統括部門が、日立グループ全体のガバナンス状況および各BU・グループ会社の施策実効状況の把握と管理制度の向上に取り組んでいきます。

2.高度化・巧妙化するサイバー攻撃への対応

サイバー攻撃は確実に増加し、攻撃の質も高度化・巧妙化し、無差別攻撃とピンポイント攻撃の混在により攻撃目的の判断がより困難になっています。どのような攻撃にも対処できるよう、既存施策の研さんと新たな課題への対応、より高度化した監視やインシデントレスポンスの迅速化を推進していきます。

3.グローバル法規制強化への着実な対応

高度化する脅威への対応として、各国・地域で法規制強化が加速している中、これらに対応をするために、情報セキュリティ統括部門が日立グループに対する情報収集・発信および具体的な対応を実行するための体制整備を推進していきます。

情報セキュリティマネジメント

日立は、日本を代表するグローバル企業として、お客さまからお預かりした情報やその情報を保管するシステムなど、さまざまな情報資産を保護するために、情報セキュリティマネジメントシステムを構築し、情報セキュリティマネジメントの強化に取り組んでいます。

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、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。

(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全社における情報セキュリティ推進体制を確立し、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。

日立製作所の執行役社長(以下、執行役社長)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と、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。

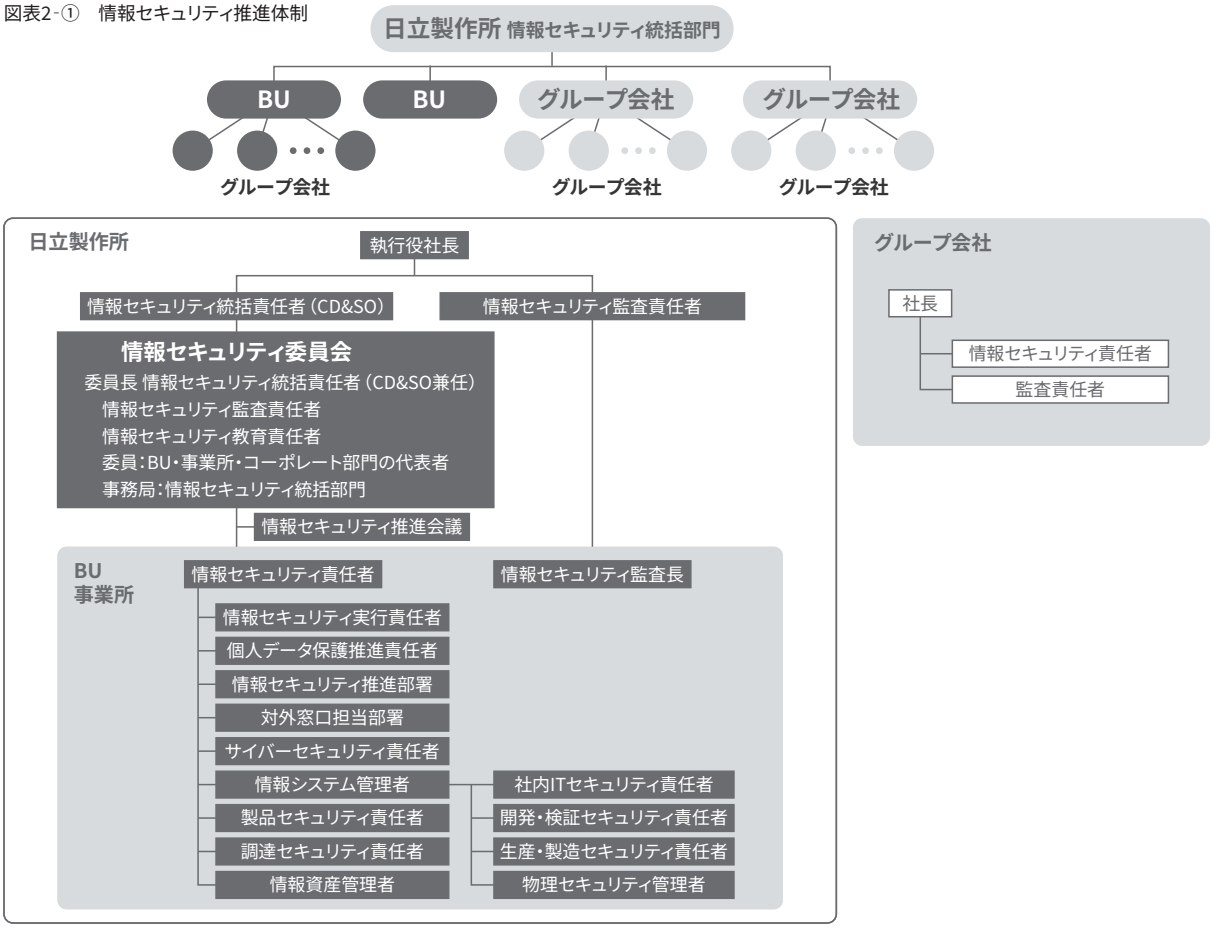
情報セキュリティ統括責任者は、情報セキュリティ委員会を組織し、情報セキュリティに関する方針、個人情報保護方針、教育計画、各種施策を決定します。

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。

BU・事業所では、原則BU長・事業所長が情報セキュリティ責任者を務めます。情報セキュリティ責任者は、推進をサポートする情報セキュリティ実行責任者、個人データ保護推進責任者を任命し、情報セキュリティおよび個人情報保護を管理、統括します。加えて、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環境における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。また情報セキュリティ推進部署を設置し、各組織の個人情報保護、情報セキュリティ、機密情報管理、入退管理、外注管理に対応するとともに、従業員に対して教育を行います。さらに、各部署には情報資産管理者を置き、個人情報を含む情報資産の取り扱いに対して責任をもつ体制を整えています。

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

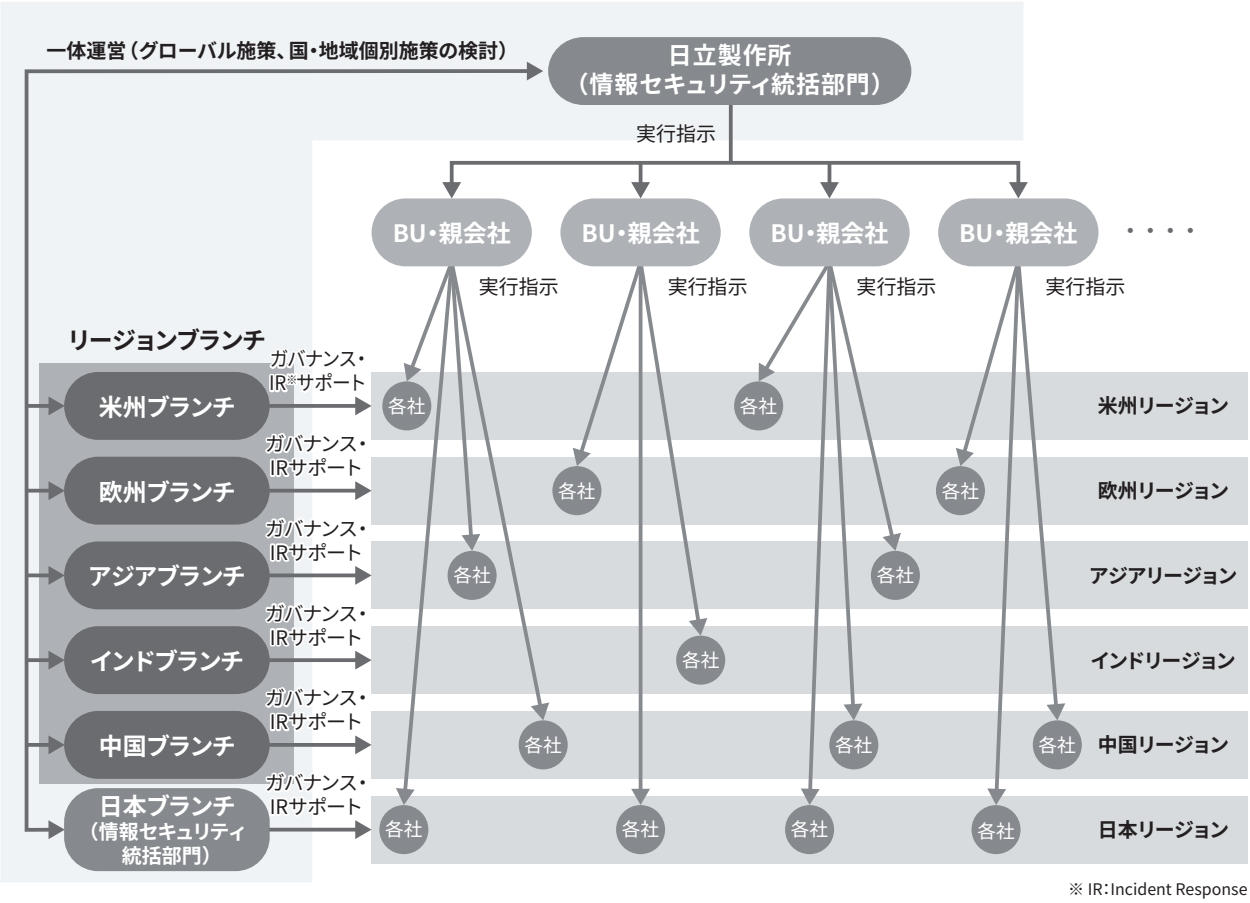
グローバルビジネスの拡大に伴い、日立では、セキュリティ施策の確実な遂行に向け、各国・地域に情報セキュリティ担当部門（リージョンブランチ）を設置し、グローバルガバナンス強化に取り組んでいます。

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。

Security One 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、中国の各国・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・国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一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、マネジメントモニタリング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、各社に個人データ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

日立では日立グループ情報セキュリティポリシーに基づき各種セキュリティ関連規則を定めています。(図表2-③参照) 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。米国政府基準SP800に対応した「情報セキュリティ対策基準」により、グローバルで通用するサイバーセキュリティ対策を推進しています。

個人情報保護に関しては、日立グループ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、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※を参照し定めています。また、「個人情報保護方針」「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)相当の規則としています。

機密情報管理に関しては、機密情報の保全に関する取り扱いを「機密情報管理規則」に定めています。

※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規定など、物理的なセキュリティの確保について定めています。

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、監査計画にのっとった監査、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、情報セキュリティ・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。昨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。そのほかにも、日立製作所は、毎年情報セキュリティ教育計画を策定し、新入社員、新任管理職といった階層別教育や個人情報保護担当者などを対象とした専門教育など、対象別、目的別に多様な教育プログラムを用意して実施しています。（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。

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

情報セキュリティの施策が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を実施しています。

日立製作所および国内すべてのグループ会社では、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。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、監査の公平性・独立性を確保するため、相互監査を行っています。

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
- 個人情報保護およびJIS Q 15001と個人情報管理体制の合致状況
- 個人情報保護マネジメントシステムとJIS Q 15001の合致状況

国内の全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。

情報セキュリティマネジメント

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、セキュリティ人財育成、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わ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の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。

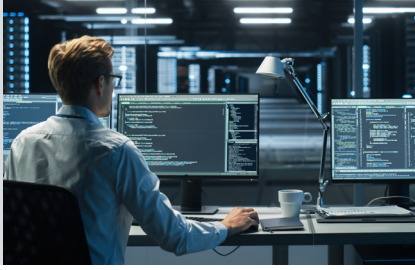
M&A時のセキュリティリスク評価は、契約締結の前後2フェーズに分けて行います。(図表2-⑥参照)

①契約締結(Day0)前:「情報セキュリティリスク評価」

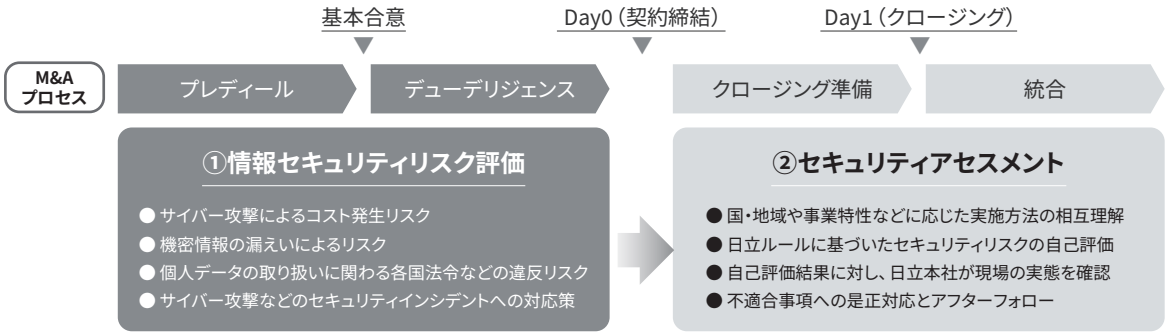
情報セキュリティの組織・体制、規則などの整備状況、事業の特性や国・地域における法制度対応、サイバーセキュリティ事故の有無および事後対応の状況など、公開情報や事前に提供された情報に基づき、買収する会社の情報セキュリティリスクを分析します。

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。

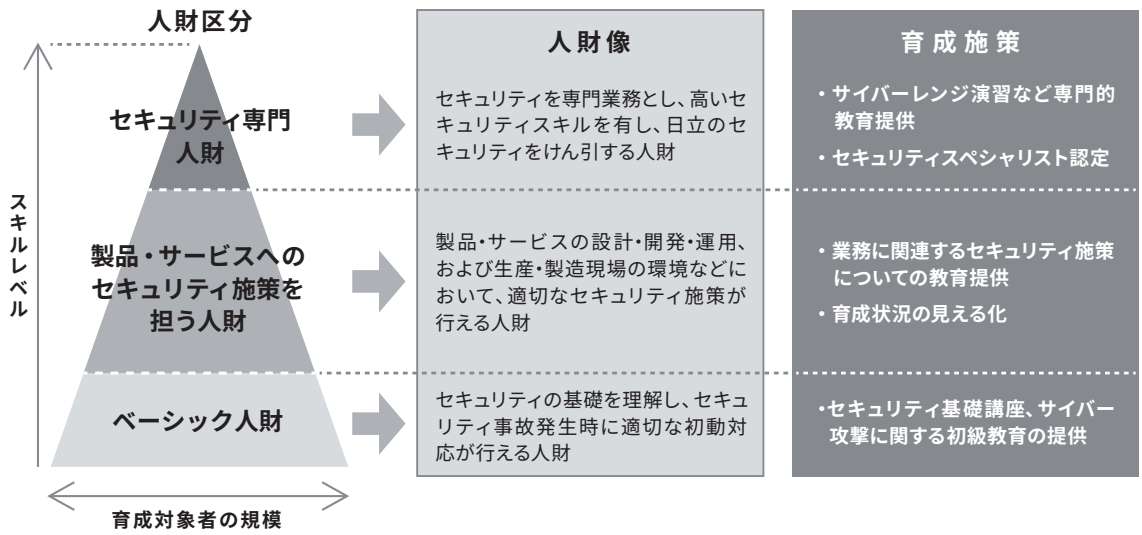
■ セキュリティ人財育成の考え方

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、社内規定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・運用しなければならないため、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。

■ 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CSIRT（Cyber 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。

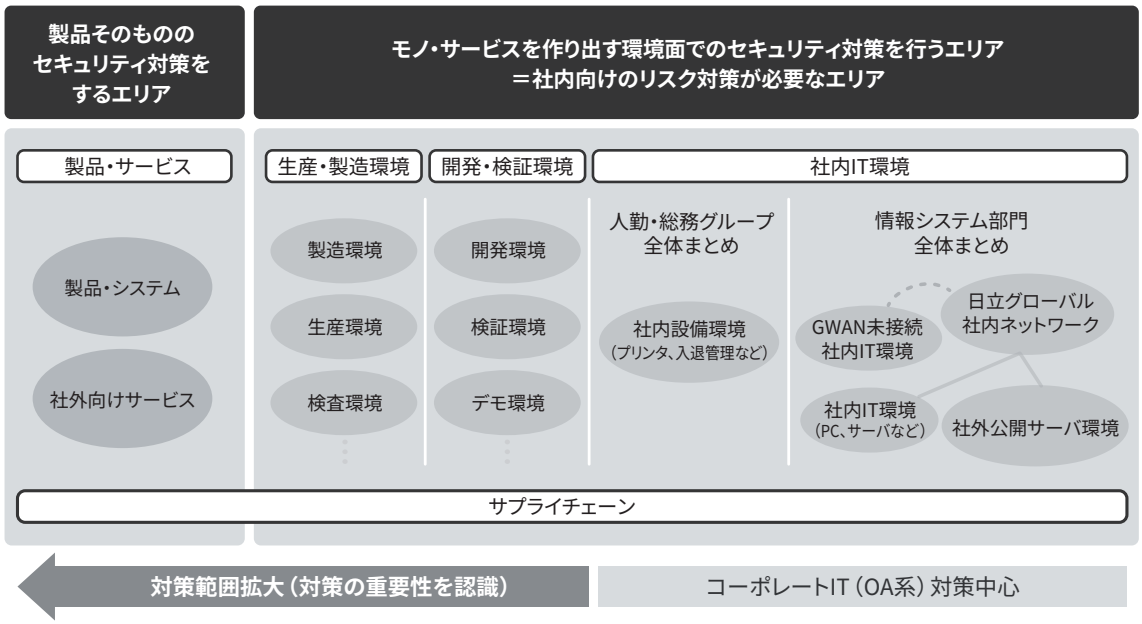
サイバーセキュリティ強化施策の考え方

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IT環境以外の生産・製造環境、開発・検証環境に対する攻撃への対応に加え、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（three lines of defense）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。

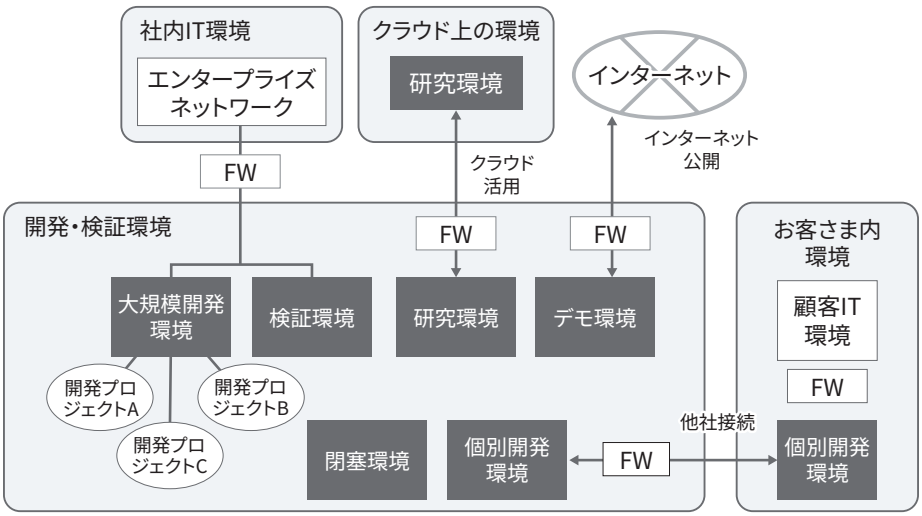
開発・検証環境におけるセキュリティ強化

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2-⑪参照)

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	環境面	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	プロセス面	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

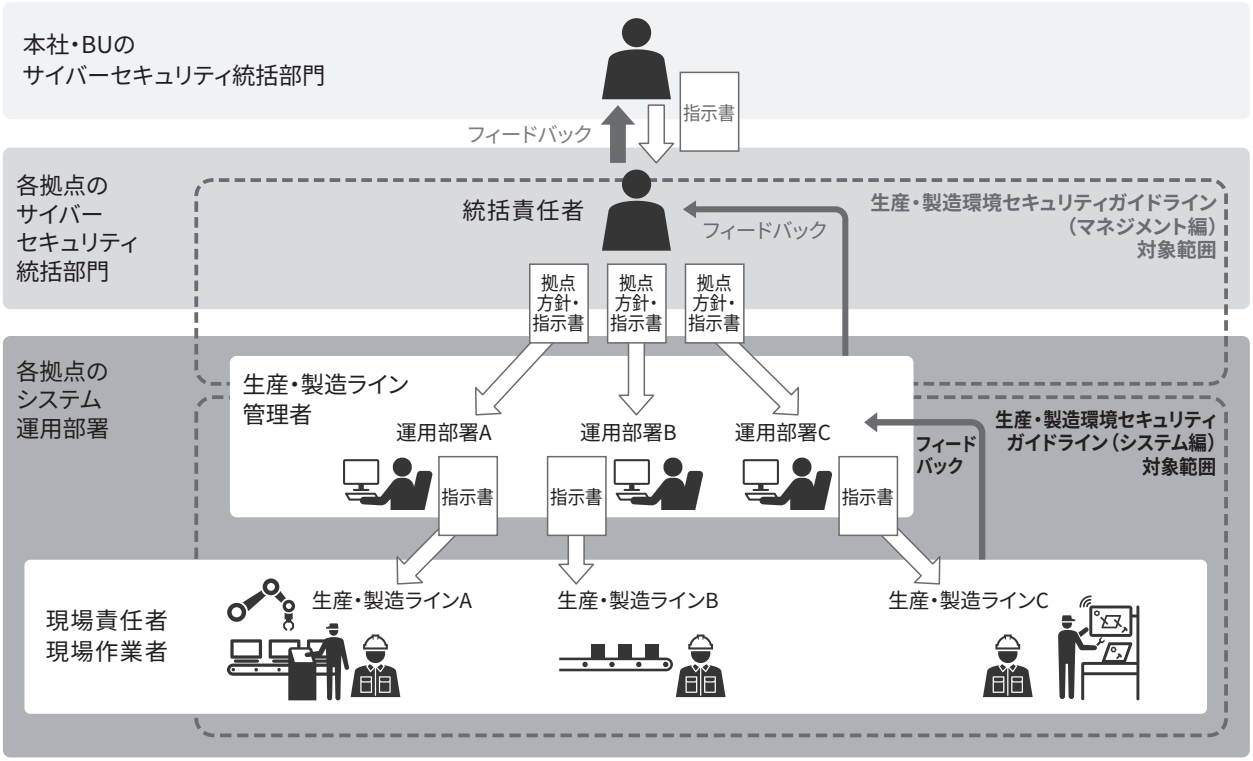


生産・製造環境におけるセキュリティ強化

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・管理上ルールの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
		現場作業者

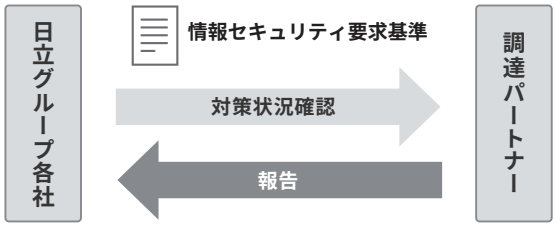
サイバーセキュリティの取り組み

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

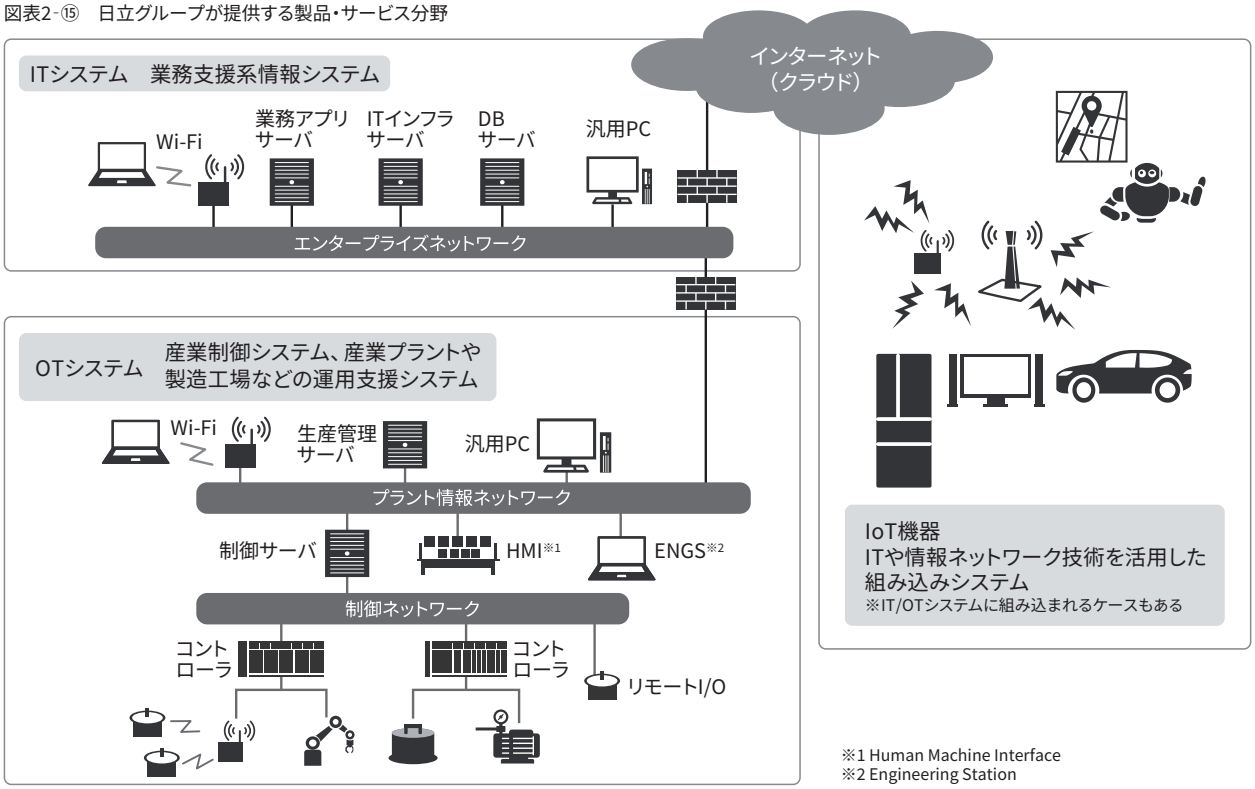


製品・サービスにおけるセキュリティ強化

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定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処を行っています。

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

規定等の文書	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レスポンスの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・インシデントレスポンス強化

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。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・インシデントレスポンスの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）を導入し、端末の動作監視を強化することで端末への攻撃の早期検出と対処の迅速化を行っています。

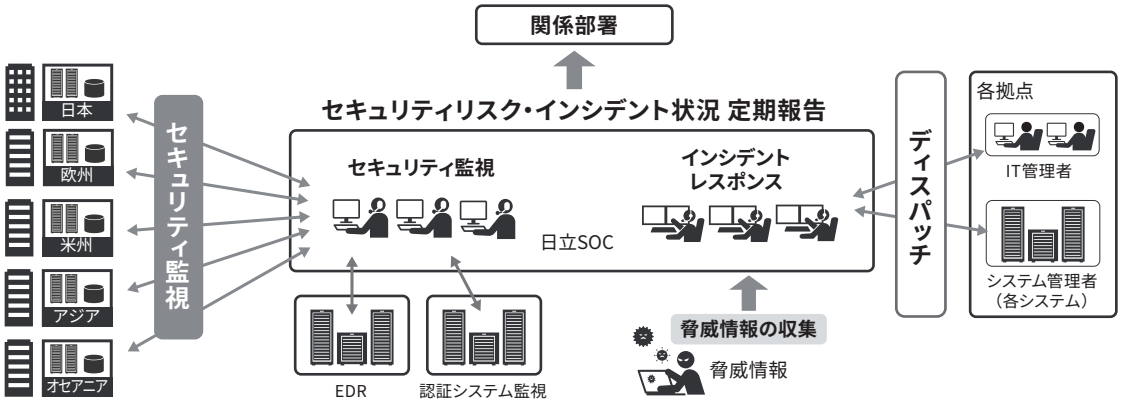
さらに、認証システムの監視を強化することで、第三者によるアカウント不正利用や認証システムへの攻撃の早期検知と対処の迅速化も行っています。これらの施策により複雑化・巧妙化するサイバー攻撃、在宅勤務などの働き方の変化により生じる新たな脅威にも対応しています。

■ インシデントレスポンス

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、事態の収束を行っています。また、基幹拠点のログ監視とEDR、認証システム監視による調査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までの時間短縮が可能となり、より効率的なインシデントレスポンスを実現しています。さらに、新たな技術を活用したインシデントレスポンスの自動化を推進することで対応の迅速化、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　グローバルでのセキュリティ監視・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。

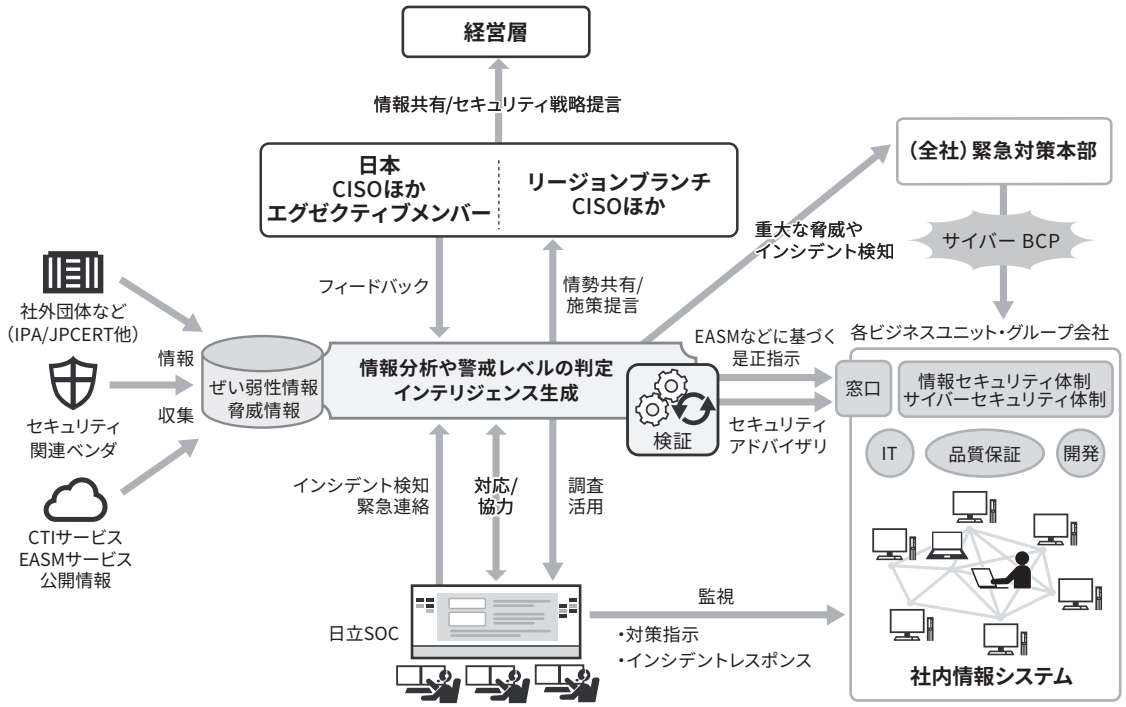
これらのぜい弱性に迅速に対応するために、アタックサーフェスマネージメント(EASM)ツールを用いて外部公開機器の最新状態を管理しています。リスクが顕在化した、または恐れのある機器については、該当部署へ「サイバー警報」を発報し、早急な確認と是正を依頼することで、外部からの攻撃リスクを低減し、対応の迅速化を図っています。

■ 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2-⑲参照)

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



CSIRT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CSIRT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。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、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。

インシデントレスポンスチームとは

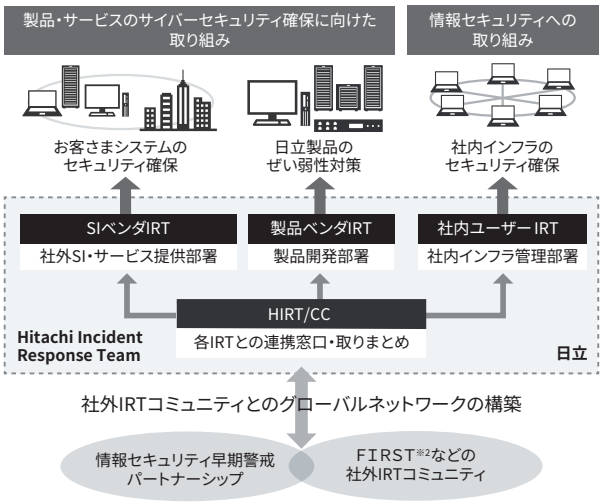
インシデントレスポンスチームは、組織間ならびに国際間の連携によって問題解決にあたるために、「技術的な視点で推し量り、伝達できること」「技術的な調整活動ができること」「技術面での対外的な協力ができること」という基本的な能力を持ち、インシデントの予防（レディネス：事前対処）と解決（レスポンス：事後対処）を通じて、「インシデントオペレーション」を先導する組織です。

HIRTの活動モデル

HIRTの役割は、「ぜい弱性対策：サイバーセキュリティに脅威となるぜい弱性を除去するための活動」と「インシデント対応：発生しているサイバー攻撃を回避ならびに解決するための活動」を通じて、「組織単体活動：自身の企業情報システムを対象とする『情報セキュリティへの取り組み』」と「組織連携活動：お客さまの情報システムや制御システムを対象とする『製品・サービスのサイバーセキュリティ確保に向けた取り組み』」の視点から、日立のサイバーセキュリティ対策活動を支援していくことにあります。さらには、「次の脅威をキャッチアップする」過程の中で早期に対策の展開を図ることによって、安全・安心なインターネット社会の実現に寄与することにあります。

HIRTは、ぜい弱性対策とインシデント対応とを推進するために、下記のように、四つのIRT（Incident Response Team）という活動モデルを採用しています。四つのIRTとは、(1) 情報システムや制御システム関連製品を開発する側面（製品ベンダIRT）(2) その製品を用いてシステムの構築やサービスを提供する側面（SI［System Integration］ベンダIRT）(3) インターネットユーザーとして自身の企業情報システムを運用管理する側面（社内ユーザーIRT）の三つとともに、(4) これらのIRT間の調整業務を行うHIRT/CCを設け、各IRTの役割を明確にしつつ、IRT間の連携を図る効率的かつ効果的なセキュリティ対策活動を推進するモデルです。（図表2-⑳参照）

図表2-⑳　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



分　類	役　割
HIRT/CC※1	該当部署：SIRTコーディネーションセンタ FIRST※2、JPCERT/CC※3、CERT/CC※4などの社外IRT組織との連携、SIベンダ・製品ベンダ・社内ユーザー IRT間の連携を通してぜい弱性対策とインシデント対応活動を推進する。
SIベンダIRT	該当部署：SI・サービス提供部署 公開されたぜい弱性について、社内システムと同様にお客さまシステムのセキュリティを確保するなど、お客さまシステムを対象とするぜい弱性対策とインシデント対応活動を支援する。
製品ベンダIRT	該当部署：製品開発部署 公開されたぜい弱性について影響の有無を迅速に調査し、該当する問題について、修正プログラムを提供するなど、日立製品のぜい弱性対策を支援する。
社内ユーザーIRT	該当部署：社内インフラ提供部署 日立サイトが侵害活動の基点とならないようぜい弱性対策とインシデント対応活動の推進を支援する。

※1 HIRT/CC：HIRT Coordination Center　※2 FIRST：Forum of Incident Response and Security Teams
※3 JPCERT/CC：Japan Computer Emergency Response Team/Coordination Center　※4 CERT/CC：CERT Coordination Center

サイバーセキュリティの取り組み

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、各事業部・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※1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。

※1 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

(2) 研究活動基盤の整備

「次の脅威のキャッチアップ」と早期に対策展開を図るための技術として「動的活動観測」に取り組んでいます。動的活動観測は、標的型攻撃などのサイバー攻撃を調査するために構築した組織内ネットワークの疑似環境下で、侵入後の攻撃者の行動を記録し分析する観測手法です。(図表2-㉑参照)

(3) 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、エキスパート人財への技術継承を推進しています。また、実践的な社内セキュリティ啓発の一環として、標的型攻撃やランサムウェアなどのサイバー攻撃に対する疑似体験演習の開発にも取り組んでいます。

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。

(4) 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※2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。

※2 HIRT-FIS:Financial Industry Information Systems

■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

日本シーサート協議会活動を活用して、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、JPCERTコーディネーションセンターと独立行政法人情報処理推進機構(IPA)が共同運営するJVN※3を用いた情報利活用基盤の整備を支援しています。

※3 JVN:Japan Vulnerability Notes(ぜい弱性対策情報ポータルサイト)

(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※4活動を推進しています。

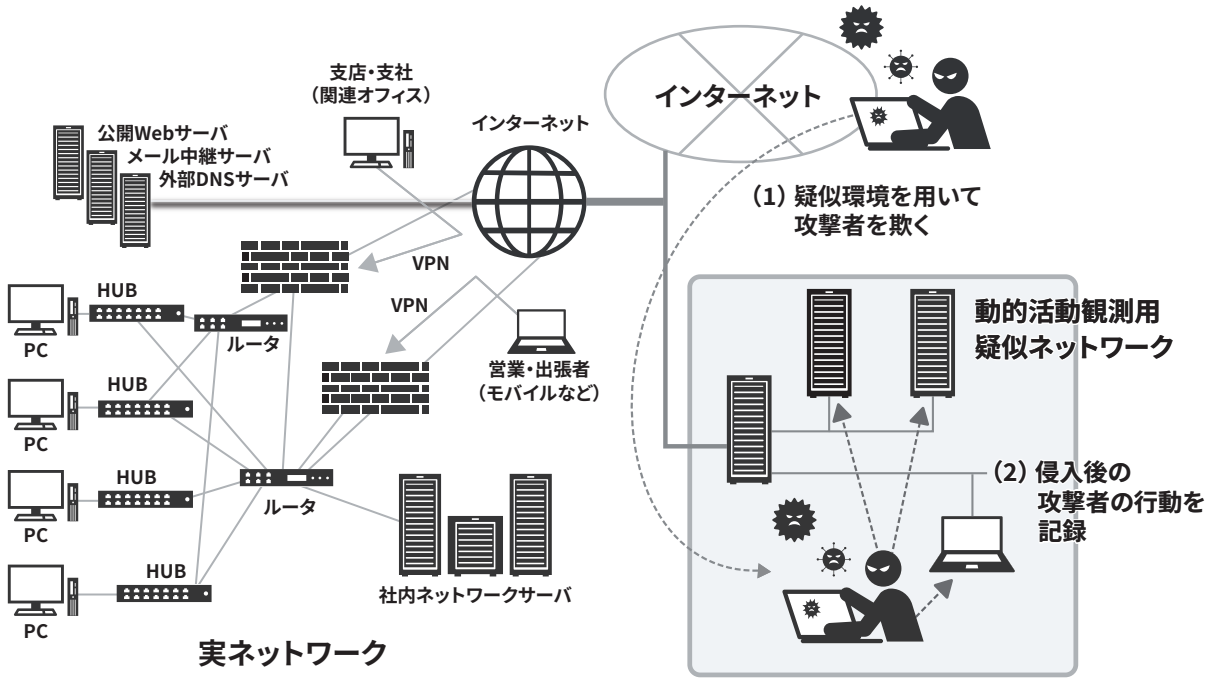
※4 Vulnerability Reporting and Data eXchange

(3) 人財育成の場の整備

マルウェアとサイバー攻撃対策研究人材育成ワークショップなど学術系研究活動への参画を通じて、産学連携による人財育成の場の醸成、専門知識を備えた研究者や実務者の育成を推進しています。

■ Hitachi Incident Response Team
https://www.hitachi.co.jp/hirt/
https://www.hitachi.com/hirt

図表2-㉑　攻撃者の行動を記録する動的活動観測システム



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ことを掲げ、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2-㉒参照)

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定を策定しています。また、社内規定が法令、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。このような規定の整備とともに、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2-㉓参照)

図表2-㉒　個人情報保護ガバナンスのビジョン

VISION

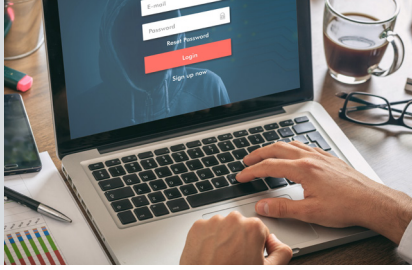
グローバル社会の一員として個人情報保護に取り組む

1　安心・信頼を提供する

- 法令などに適合した個人情報保護・機密情報管理プログラム(プロセス規定)の遵守により、事業に取り組み、安心・信頼を提供してまいります。

2　個人の権利を大切にする

- グローバル全体の動向である個人の権利尊重に対して、日立として誠実に向き合います。
- 「個人情報保護」は基本的人権の尊重であり、日立での経営の重要イシューとして取り扱います。



■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を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、日立製作所では下記、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。

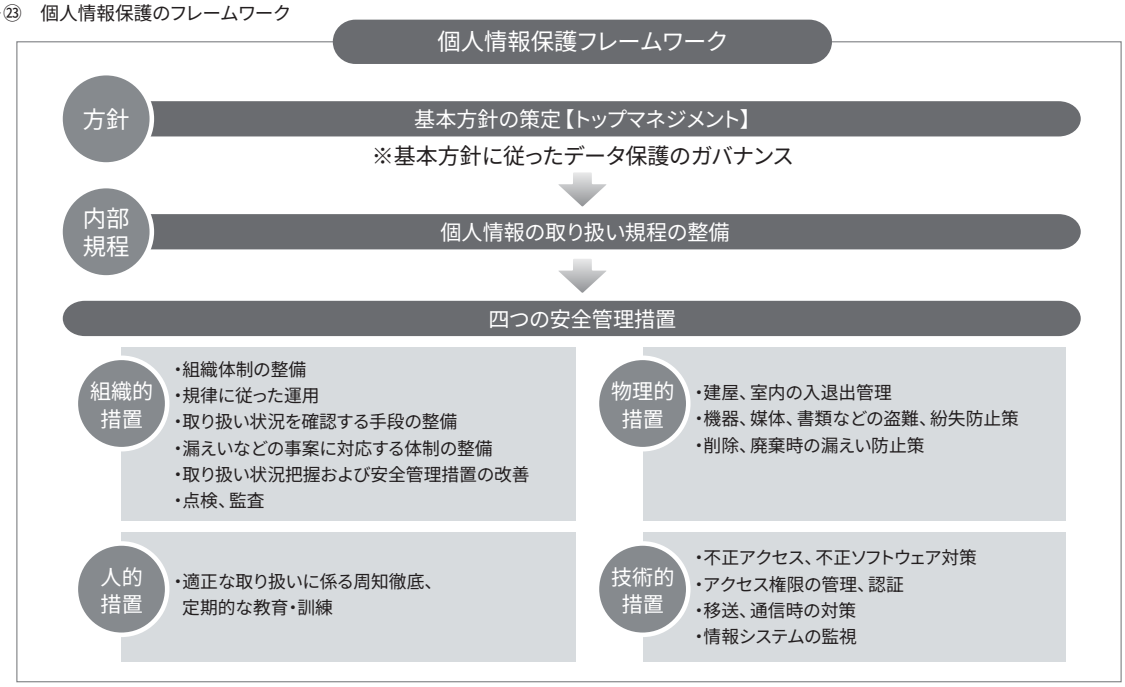
(4) 法令・規範の遵守

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2-㉓　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者の役割・責任や個人情報の取り扱いに関する規定などを定め、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定を定め、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。

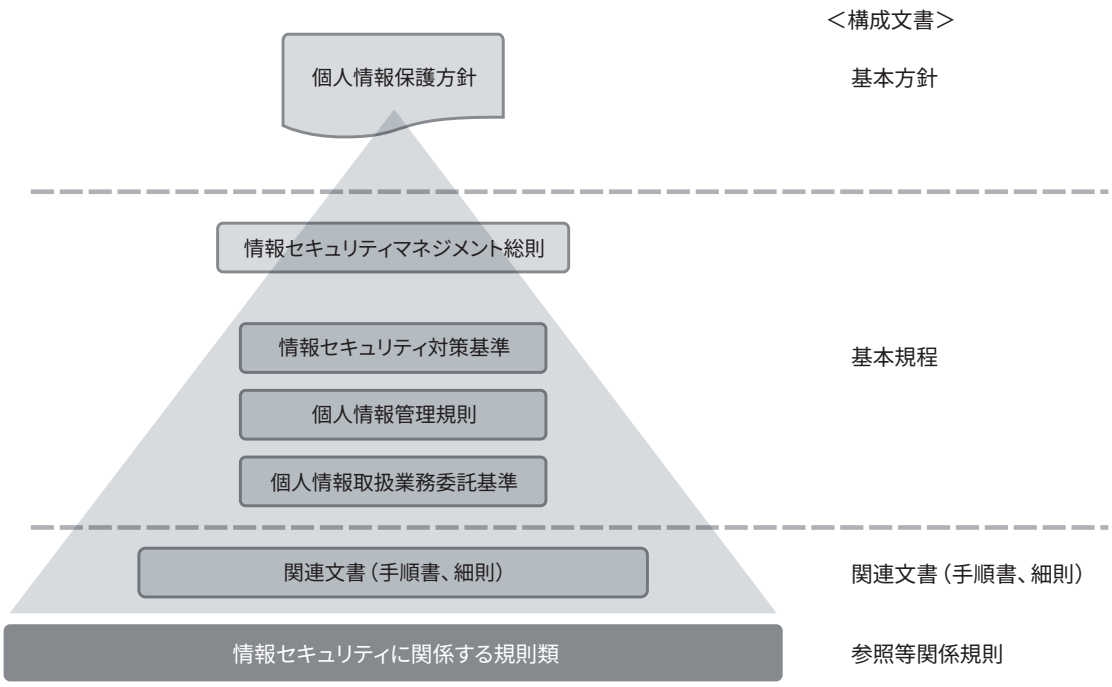
技術的安全管理措置では、情報システムに対する不正アクセス、不正ソフトウェア対策の実施などを行っています。また、取り扱う個人情報の重要度に応じてアクセス権限の管理、認証、移送、通信時の対策、情報システムの監視などを行っています。

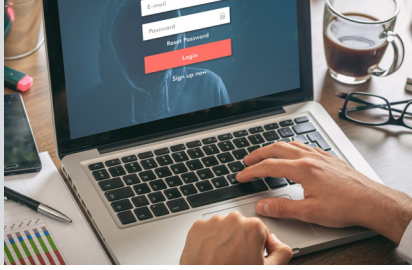
個人情報保護マネジメントシステム

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に実施し、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2-㉕参照）

個人情報の管理と適切な取り扱い

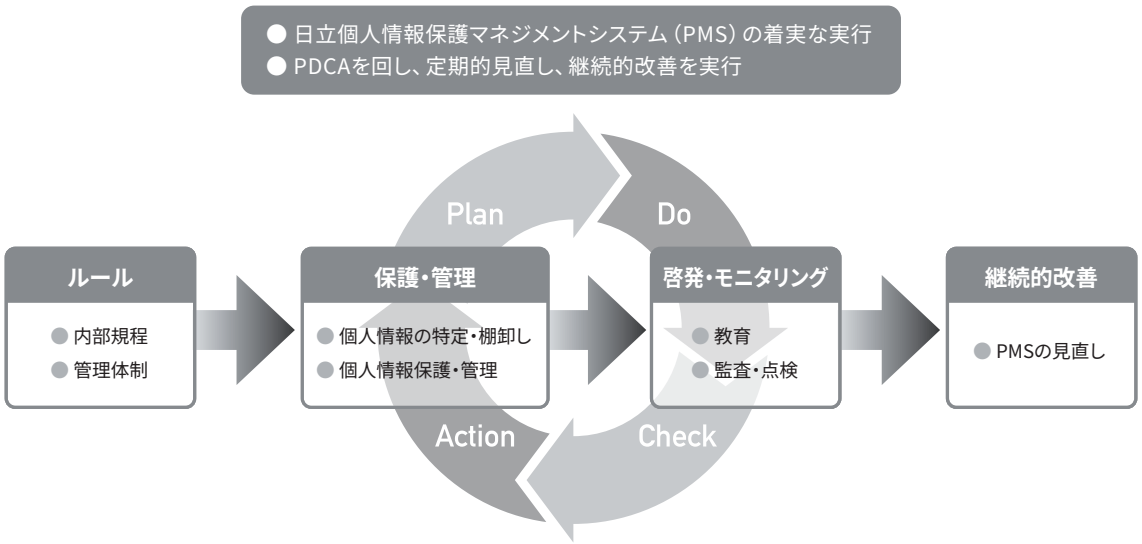
日立では、個人情報保護法より一段高いレベルの管理を行うためにJIS規格「個人情報保護マネジメントシステム－要求事項」（JIS Q 15001）相当の社内規定を制定し、規則にのっとり、厳格な管理と適切な取り扱いに努めています。職場ごとに個人情報管理の責任者（情報資産管理者）を置き、業務で取り扱う「すべての個人情報」を特定し、当該個人情報の重要性およびリスクに応じて管理し、適切な措置を講じています。

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定にのっとり、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2-㉕　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布しています。

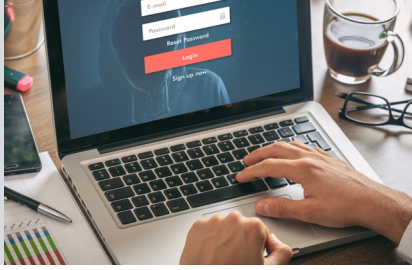
■委託先の管理強化

日立では、早くから個人情報の委託先管理を強化し、個人情報の取り扱いを委託する際の社内規定を定め、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、2025 年7月末時点、37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

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（2025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
日和サービス株式会社
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 日立リアルエステートパートナーズ
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

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

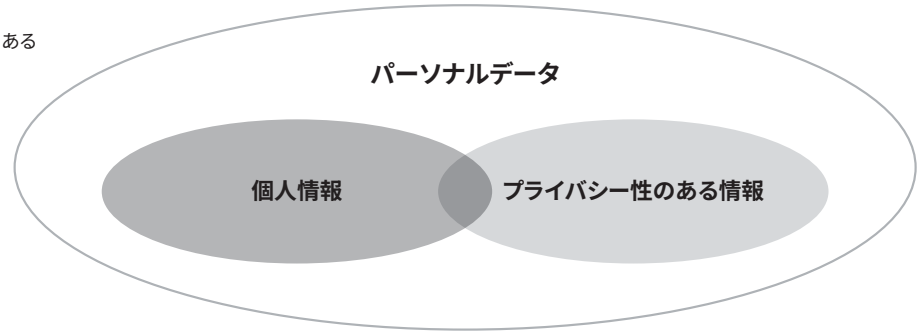
日立製作所は、パーソナルデータの安全・安心な利活用による価値創出をめざし、デジタルシステム&サービスセクターにおいてデータ利活用におけるプライバシー保護に取り組んでいます。

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。このようなサイバー攻撃の脅威に対抗するためには、社内の部門間を越えた、また、社外の組織と連携したセキュリティエコシステムの構築が重要となります。そのために、各種社内活動を通じたセキュリティ部門以外の部門間が相互に協力していける体制づくりを進めています。加えて、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

IoTに代表される機器やシステムなどのモノが「つながる」環境になっている現在、今まで考える機会が少なかった部門でもセキュリティを考える必要がでてきています。

そのために、ITシステムやツール、規則やガイドラインなど統制による対策徹底に加えて、立場、組織の垣根を越えたコミュニティづくりを目的としたセミナーやワークショップなどを開催しています。この機会を通じ、自身の役割を再認識すると同時に、周囲との連携を深めることで、セキュリティ強化につながることをめざしています。

米州、欧州、アジア、インド、中国の各国・地域では、ワークショップを開催し、統制として推進している内容の理解をさらに深める活動をしています。また、日本においては、セミナーやワークショップを定期的に開催し、情報セキュリティの専門的な知識を学ぶ機会を提供しています。講師については、多様な分野の方を招き、知識だけでなく、セキュリティ意識向上のための気づきを提供できるように努めています。

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生かし、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活動

日立では、日立グループにおけるCSIRT活動に加え、HIRTを窓口（PoC: Point of Contact）として社外CSIRT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。2024年10月現在で、111カ国、753チームが加盟しています。

■ 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大脅威執筆者会ほか
- 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） PA・FA計測制御委員会、セキュリティ調査研究WG
- 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

日立グループのIT会社である日立システムズでは、安全で信頼性のあるデジタル基盤を提供することで、サイバー領域を含む社会全体の安全・安心の実現をめざしています。日立システムズのセキュリティリスクマネジメント部門では、顧客先のセキュリティインシデント対応支援などを通じて技術的な実践を積み、その技術を人財育成や研究開発にフィードバック、さらに社外に対して技術・知見を発信して社会に還元するというサイクルを回すことで、社会の持続的なセキュリティレベルの成長を支えています。重要な要素の一つである社外との連携として、警察組織やNPOをはじめとする産官学関係機関との連携、学術機関との共同研究開発、人財交流、社外カンファレンスへの講演など、社外団体との連携を積極的に進めています。

■ 県警テクニカルアドバイザーとしての活動

各県警察では、警察のサイバー犯罪およびサイバー攻撃対処能力の向上を図るため、民間事業者等の技術者をアドバイザーとして委嘱するアドバイザー制度を設けています。日立システムズでは、2019年に島根県警察察本部の「島根県警察サイバー犯罪対策テクニカルアドバイザー」に、2022年に広島県警察本部の「広島県警察サイバー犯罪対策テクニカルアドバイザー」、近畿管区警察局の「近畿管区警察局サイバーセキュリティテクニカルアドバイザー」に、自社の社員が就任しています。

アドバイザーに就任している社員は、セキュリティのエキスパートとして、サイバー犯罪の捜査および対策に関する助言や研修、セキュリティ技術に関する最新の動向や知見などの提供を行い、捜査員の育成を支援しています。また、県が産官学合同で開催するセミナーなどに登壇し、地域の事業者や住民の方へ、一人一人ができるセキュリティ対策についてわかりやすく伝えるなど、警察におけるサイバー犯罪対処能力の向上に貢献しています。

テクニカルアドバイザー委嘱式の様子

■ NPO日本セキュリティネットワーク協会との活動

日立システムズは、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。その活動の一環として、日立システムズの社員が作成実行委員会の委員長を務め、会員各社と連携し、主催のイベント「みんなの『サイバーセキュリティコミック』」を推進しました。「みんなの『サイバーセキュリティコミック』」は、セキュリティ知識の普及とネットリテラシーの向上、ネットを守るハッカーへの興味とイメージアップ、セキュリティ人材育成を促進することを目的とした活動です。2020年度から2023年度に『みんなの「サイバーセキュリティコミック」』を作成しTwitterで配信しました。なお、この活動は、総務省や経済産業省などが後援するデジタル政策フォーラム主催の「サイバーセキュリティアワード2023」において、Web・コンテンツ部門で優秀賞を受賞しました。2024年度には、より多くの方々に閲覧いただけるよう英語版コミックも作成、公開しました。

サイバーセキュリティコミック（英語版）

＊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。そのために、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」

テレワークなど多様な働き方が定着する一方で、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対策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。「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図る活動に取り組んでいます。「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、自分ゴト化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。

新た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KYT(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の米国およびそのほか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

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。

GREEN AEGIS

トピックス

イベントを通じてGREEN AEGISのコミュニティ活動を活性化

GREEN AEGIS では、コミュニティ内での情報発信、情報の提供など、その活動に積極的に参加した従業員や協力した従業員を対象に、年度ごとに、GREEN AEGIS Awardとして表彰しています。また、各年度の受賞者を対象に、GA Summitというイベントを開催し、メンバー間のコミュニケーションの活性化、ネットワークの強化を進めています。

2024年度は、2025年3月に、日立グループ16部門から約40名が参加し、GA Summit 2024を開催しました。ワークショップ、GREEN AEGIS Award 2024表彰式、懇親会といったプログラム構成で実施しました。

表彰式では、情報セキュリティ統括責任者から受賞者一人一人に、表彰状と記念盾を授与しました。また、小グループに分かれたワークショップや懇親会を通じて、各部門の好事例から業務のヒントを得ることや、課題や担当者の思いを共有することができ、横連携の場となりました。このメンバーを核にして、さらなるコミュニティの拡大、活性化を推進していきます。

GA Summit 2024の当日の様子

コラム
COLUMN

攻撃の高度化や生成AI前提システムに対応していくためのセキュリティ対策

ランサムウェアの攻撃や組織からの情報漏えいによる被害は、情報処理推進機構（IPA）の情報セキュリティ10大脅威2025の上位に選ばれるなど、依然として大きなセキュリティ課題となっています。こうした脅威に対抗するためには、攻撃動向を把握して対策を常に最新化していく必要があります。日立ではマルウェアの攻撃手口の分析や、大規模言語モデルを活用した情報漏えい対策技術の研究開発を行っています。

TOPIC 1　マルウェア動的解析画面から取得可能な情報のセキュリティ対策への応用可能性

近年、サイバー攻撃の件数が増えていることに伴い、攻撃に使われる「マルウェア」も種類や数がどんどん増えています。このような状況の中で、マルウェアの動きを詳しく調べて、適切な対策を考えることがますます大切になっています。

マルウェアを調べる方法にはいくつか種類があります。たとえば、ファイル名やマルウェアの種類など、表面的な情報を調べる「表層解析」。マルウェアを実際に動かしてみて、そのときの動作を記録する「動的解析」。また、マルウェアの中身のコードやアセンブリと呼ばれる言語を調べる「静的解析」などがあります。この中でも「動的解析」は、実際の挙動がわかるため、多くの専門家が使っています。

動的解析のひとつの手法として、解析中の画面をスクリーンショットで記録する方法があります。この画面には、マルウェアが起動したアプリや表示されたメッセージなど、たくさんの情報が映し出されています。これらを利用することで、たとえばランサムウェアの検出や、Androidマルウェアの発見精度を高める研究などに役立てられています。

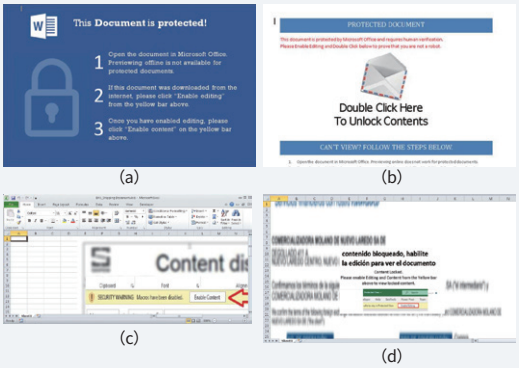
さらに、こうした画面には、攻撃者がユーザーをだますためにどんな工夫をしているかも映っているため、攻撃手法の理解やユーザー教育にも使える可能性があります。画面に含まれる情報は、単に技術的なデータだけでなく、視覚的にどのようにユーザーを誘導しようとしているかといった、人間の行動に関わるヒントも含んでいます。

しかし、今までのところ、こうした解析画面から得られる情報を体系的に調べた研究はあまりありませんでした。そこで本研究では、実際に多くの解析画面を集めて、そこから得られる情報を整理し、どんな使い方ができるのかをまとめました。

具体的には、93種類のマルウェアファミリーについて211件の解析レポートを調査し、合計3,590枚の画面を分析しました。さらに、ログから得られる情報と比較して、画面でしかわからない情報を明らかにしました。また、マルウェアがユーザーをだましたり（図表4-①参照）脅す工夫（図表4-②参照）や、解析者が苦労している様子なども確認できたため、教育やツールの改善にも役立つ提案を行いました。

このように、解析画面の情報を上手に活用することで、より深いマルウェア理解や、サイバー攻撃への備えを強化することが期待されます。今後のセキュリティ対策の発展にとっても、重要な手がかりとなると考えられます。

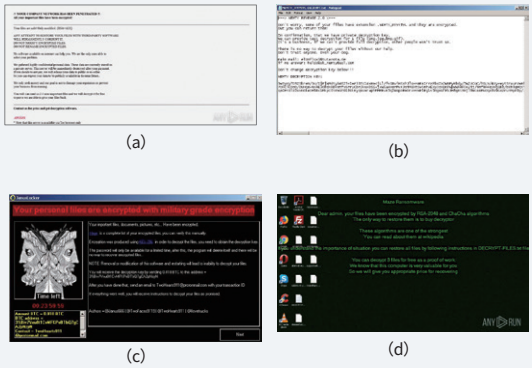
図表4-①　ユーザーのクリックを誘導するマルウェアの画面例



(a)　(b)　(c)　(d)

著名なソフトウェアのアイコンなどを
模擬することでユーザーにクリックを促す。

図表4-②　ランサムウェアの脅迫文の画面例



(a)　(b)　(c)　(d)

「時間内に支払いを終えないとデータが復旧しない」
などの脅しでユーザーに身代金支払いを促す。

TOPIC 2

大規模言語モデルを活用した企業秘密情報の識別自動化

組織が競争上の優位性を保つためには、企業の事業活動に有用で、かつ秘密にされている情報、すなわち、企業秘密情報を適切に管理していくことが求められます。このためデータセキュリティ対策を推し進めることが求められますが、その実態は教育だよりとなっており、規則に則った機密分類の運用が進んでいないため、情報資産の管理漏れのリスクが生じます。

情報漏えい防止を支援する技術として、テキスト中の機微データ検出技術が開発されてきました。顧客名や製品名など短い語句を検出する技術は固有表現抽出として研究され、プライバシー情報の検出にも応用されています。一方で、企業秘密情報の識別は文意の理解が必要なため、有力な自動技術の構築が難しい状況でした。

このため、現状では企業秘密情報は人手での管理がしやすいファイル単位で管理されています。厳密な管理には意味的単位（センテンス単位）での管理が求められますが、工数が膨大なため実施されていません（図表4-③参照）。このため、ファイル内の機密・非機密情報の区別が曖昧で、非機密情報の知見の共有が妨げられる要因となっています。

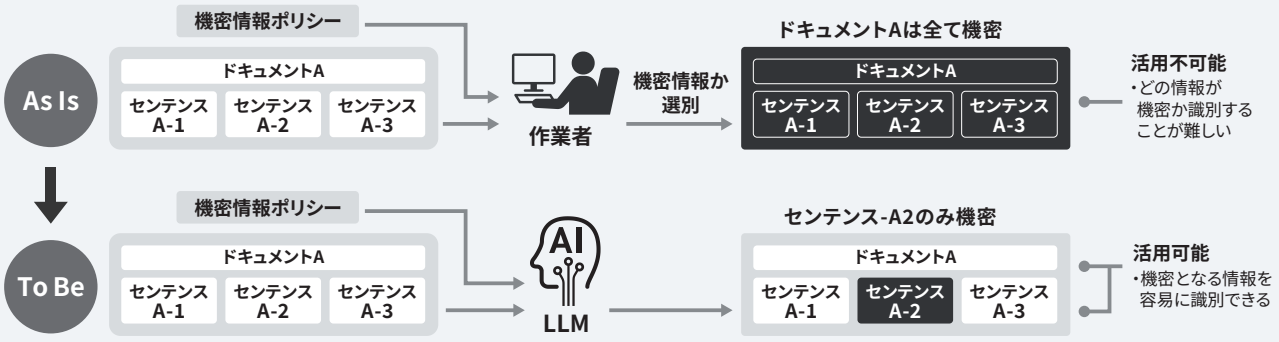
近年、大規模言語モデル（Large Language Model。以降では、LLMと省略する）は日進月歩で発展しており、文意理解力も向上しています。これを活用すれば企業秘密情報の自動識別が可能との仮説のもと、識別自動化を検討しました。具体的には、企業秘密情報を意味的単位で識別する作業をLLMで自動化するために、企業秘密情報名、ドキュメント全体、センテンスを与え、センテンス中に該当の企業秘密情報を含むか判断させました（図表4-④参照）。その結果、企業秘密情報を有するセンテンスを高精度で検出でき、その実現可能性が示されました。

この識別自動化技術により、意味的単位での情報管理にかかる工数が大幅に低減でき、企業秘密の保護と非企業秘密の利活用を両立できます。これにより、企業秘密のファイル中の非機密部分の活用によるRAG※の検索性能向上も期待されます。

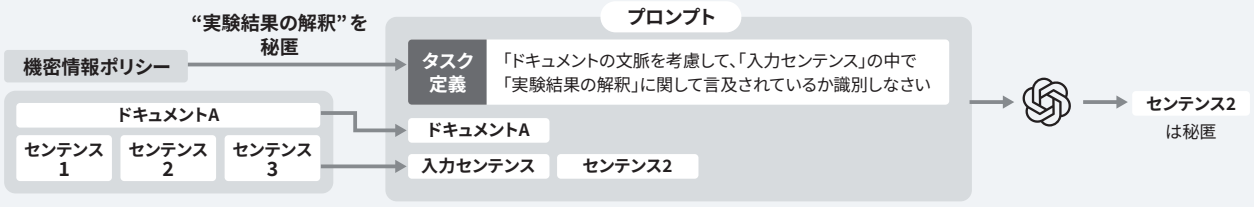
さらに、当技術は、情報管理規則（ルール）に則ったデータ管理/運用の徹底を支援することができます。当技術による識別結果を管理者が参照することで、データ管理・運用コストの低減やセキュリティリテラシの向上につなげることが期待されます。

※RAG:Retrieval Augmented Generation.

図表4-③　企業秘密情報の管理形態の現状（As Is）と理想像（To Be）



図表4-④　LLMによる企業機密情報識別の概要図



第三者評価・認証

日立では、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。

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（2025年7月末時点）。なお、以下の組織名はISMS-ACによるISMS認証取得組織一覧の表記などを参考に記載しています。

- 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 AIビジネスユニット 水・環境事業統括本部 バリューチェーンTSS事業開発本部 TSSグリーンデジタルソリューション部、環境事業部 情報システムエンジニアリング部、インダストリアルデジタル・水環境業務統括本部 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 日立アドバンストシステムズ（本社）
- 株式会社 日立製作所（インダストリアル AIビジネスユニット インダストリアルデジタル事業統括本部 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・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）
- 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（システムサービス事業部）
- 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 日立ICTビジネスサービス（ソリューションビジネスサポート第一部 メディアサービスグループ）
- 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・社会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 保守事業推進本部 プラットフォームサポート部）
- 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 デジタル・ライフサイエンスサービス本部 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（システム開発事業グループ 企業システム事業部 企業第二システム本部 企業第三システム部）
- 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（東京オフィス 開発センター）
- 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）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（2025年8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

※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保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（2025年8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 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。

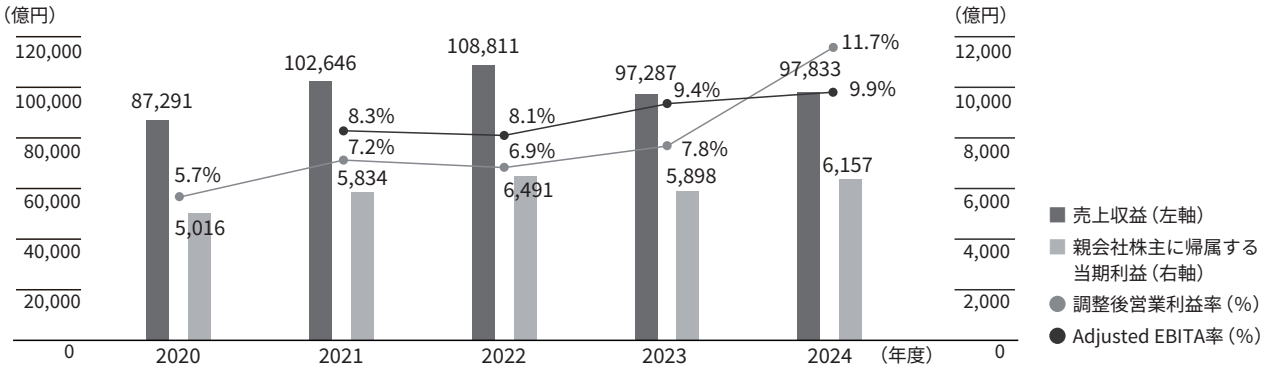
日立グループの概要

会社概要 （2025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**	464,384百万円
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**	28万2,743人（国内11万2,749人、 海外16万9,994人）

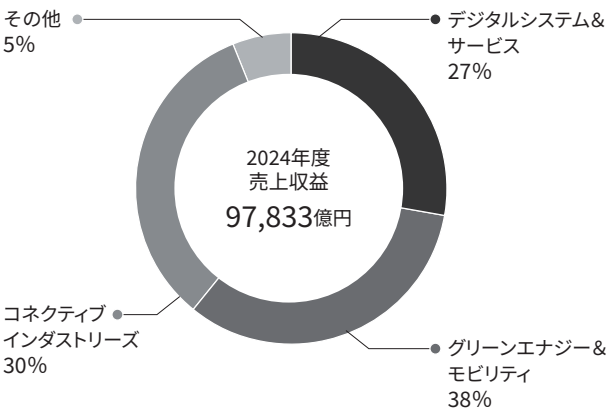
業績ハイライト （2025年3月期連結IFRS）当社の連結財務諸表は、国際財務報告基準（IFRS）に基づいて作成しています。

売上収益	9兆7,833億円（前期比1%増）	**調整後営業利益率**	9.9%（前期比2.1ポイント増）
当期利益（親会社株主帰属）	6,157億円（前期比4%増）	**Adjusted EBITA率**	11.7%（前期比2.3ポイント増）
Adjusted EBITA※1	11,418億円（前期比4%増）		

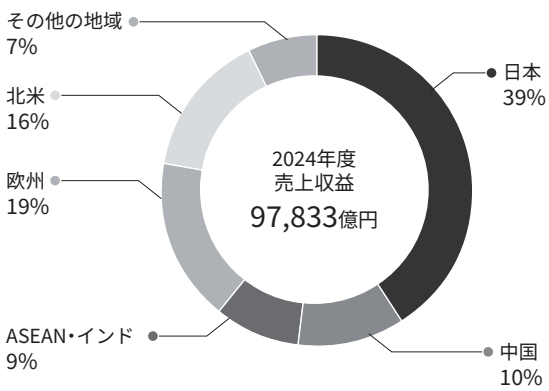


※1 Adjusted EBITA（Adjusted Earnings before interest, taxes and amortization）：調整後営業利益に、企業結合により認識した無形資産等の償却費を足し戻した上で、持分法による投資損益を加算して算出

■ 日立グループの事業構成※2



■ 地域別売上収益/構成比※2



※2 各部門の売上収益の売上収益合計に占める割合です。各部門の売上収益には、部門間内部売上収益を含んでいます。

株式会社 日立製作所

情報セキュリティリスク統括本部

〒100-8280 東京都千代田区丸の内一丁目6番6号

TEL.03-3258-1111

Printed in Japan (H) (2025.12)