

情報セキュリティ報告書 2023
Information Security Report 2023



INDEX

■ CISOメッセージ	1
■ 日立の情報セキュリティの考え方.....	4
■ 情報セキュリティマネジメント.....	6
情報セキュリティマネジメントシステム.....	6
セキュリティ人材育成の取り組み.....	12
グローバル情報セキュリティ強化の取り組み.....	14
M&Aにおける情報セキュリティ強化の取り組み.....	16
■ サイバーセキュリティの取り組み.....	18
サイバーセキュリティマネジメント.....	18
サイバーセキュリティ対策.....	24
日立グループにおけるCSIRT活動.....	26
■ データプロテクションの取り組み.....	30
個人情報保護の取り組み.....	30
プライバシー保護の取り組み.....	36
■ 情報セキュリティに関する社内外活動.....	38
■ 情報セキュリティ啓発活動.....	40
■ コラム 社会のレジリエンスを高める協調型サイバー防衛技術の研究開発.....	42
■ 第三者評価・認証.....	44
■ 日立グループの概要.....	47

〈本報告書の概要〉

- 報告範囲・期間: 2022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: 2023年10月発行
-

CISOメッセージ

グローバル視点にたって 個別最適から全体最適へ。 “One Security Team”として 一丸で推進する。

企業を狙ったランサムウェアによるサイバー攻撃は、毎年、高度化、巧妙化し、情報漏えいやシステム停止といったインシデントが頻発しています。もはやセキュリティリスクに関しては、国・地域や会社間といった隔たりさえなくなっており、セキュリティインシデントが、いつでもどこから起きても不思議ではない状況下に、今、わたしたちは置かれていると認識しています。

2024中期経営計画において、事業運営のグローバル化やデータを活用するLumada事業の拡大を進めていくうえで、セキュリティ対策はますます重要になってきています。日立グループの事業に関わるすべての企業、そして日立グループの全従業員が一つになり、“One Security Team”として情報セキュリティに取り組んでまいります。

株式会社日立製作所
執行役常務 CTrO兼CISO

村山 昌史

1985年入社。Smart Transformation Project強化本部プロジェクト・マネジメント推進室長といった経験を生かし、2016年からCPO兼バリューチェーン・インテグレーション統括本部長として調達関係の戦略策定や、構造改革をけん引。2019年執行役常務、2020年CISO就任。



高度化するサイバー攻撃の脅威

ここ数年、サイバー攻撃の件数は急増しており、また、多要素認証を突破して不正ログインしてくる攻撃も増加しています。この状況はハッカーの手口がますます巧妙化していることを表すと同時に、起こるべくして起こっていることだと認識しています。

ビジネスがデジタルデータを扱い、システムがオンプレミスからクラウドベースに移行し、多くのデータがオープンな環境で取り扱われる現在、サイバー攻撃の脅威は避けて通ることはできません。加えて、大量の個人情報が入ったデータを不注意な扱いで情報漏えいを引き起こすなど、人的ミスによるインシデントもあとを絶ちません。決してひと事ではないこの状況をよく認識し、日立グループとして、リスクマネジメントにおける重要課題と位置付けて、まず、わたしたち自身ですべきことをしっかり取り組んでいくことが必要となります。



グローバルに進むデータ保護強化

今、欧州のGDPRや中国のデジタル三法をはじめ、国や地域単位でデータ保護規制の強化が進んでいます。これらの動きが日立グループの事業に与える影響は決して小さくありません。グローバルビジネスを展開するうえで、それぞれの国と地域の法規制を考慮し

てしっかりと順守していく必要があります。特に、データ越境移転規制の強化に対しては、事業を行ううえで情報を適切にどのように運用していくかなど、専門家の知識を組み込みながらよく認識し、対応していかなければなりません。そのためには、現地の人財の活用、その人財のもつ情報や知見、ノウハウの活用が鍵を握ります。すべてを本社のメンバーで行うのではなく、各リージョンの人財を生かしていく体制が不可欠だと考えています。

情報セキュリティは重要な経営課題のひとつ

日立グループは、2024中期経営計画で「データとテクノロジーでサステナブルな社会を実現して人々の幸せを支える」ことを掲げています。その根幹をなすIT・OT・プロダクトによる社会イノベーション事業には、データの活用が欠かせません。安全に事業を推進し、お客さまにサービス提供できるように、IT部門と連携して、情報セキュリティが担保され、しっかりとその支えとなるような環境づくりを進めていきます。

お客さまのデータに光を当て、輝かせることで新たな知見を引き出し、お客さまの経営課題の解決を提供するLumada事業では、データ保護やプライバシー保護は重要な課題です。個人情報を含む機密情報の漏えいやプライバシーに関わるリスクを最小化する取り組みを進めています。そのためには、法律やルールに抵触するのはどのようなケースなのかを精査し、絶対に避けなければなりません。情報のすべてを持たないと事業ができないわけではありませんから、その切り分けをしっかりと情報セキュリティと事業推進の最適なバランスを保っていきたいと思います。

迅速かつ効率的なセキュリティ体制を構築

日立グループは、事業ポートフォリオ改革を進め、事業構造が大きくグローバル化しました。今後は、この事業構造を基盤に、サステナブルな経営を推進していきます。経営のフェーズは変わっても、情報セキュリティの取り組みが大きく変わることはありません。ただし、リスクマネジメントはスピード感が問われますので、グローバルでどのように実現していくかについて取り

組んでいくことは必要です。

リスクマネジメントにおいて、情報共有するスピードをより速くし、攻撃の検知から対策までのサイクルをより効率よく回すことが求められます。グローバルでは24時間365日、さまざまなことが起きています。その対応を逐一日本で行っていると後手になりかねませんから、時差のないオペレーションが不可欠です。さらに、事業部門起点の「縦」の情報共有だけでは、子会社、孫会社が海外にある場合、伝達が遅くなったり違うニュアンスで伝わったりしかねません。“バケツリレー”で水がこぼれてしまうように、伝言ゲームになってしまい、情報の正しい内容が十分に伝わらないケースもでてきます。「縦」に加え、地域拠点による「横」連携を一層強化することで、情報共有の迅速化・正確化をめざしていきます。

ゼロトラストセキュリティの実現へ

頻発するサイバー攻撃に対して、その脅威は避けて通れないものと認識して、まず、私たち自身ですべきことにしっかりと取り組んでいきます。自社の情報セキュリティの環境を構築していくうえでは、有事の際に被害を甚大化させない、を基本として対策を進めていきます。その際は、対策が効果的であり、かつ、平常時の事業に支障をきたすような厳格すぎるものにならないように、適切なバランスが大切と考えています。

消防の活動とよく似ていて、防火のためにガチガチなルールや仕組みをとれば、リスクは減るかもしれませんが、日常生活でやりにくいことが増えてしまいます。そうではなくて、必要最低限、火災の際に被害が甚大にならないように、いろいろな防火の対策をうつわけです。情報セキュリティも同様に、何かあったときの被害が拡大しないように、事業と両立をするかたちで対策を講じていきます。

さらに、こういった自社内のセキュリティの取り組みに加え、お客さまに提供している製品・サービスや、取引先企業のセキュリティの強化についても注力していきます。取引先から日立グループへ製品・サービスが納品され、それらをもとに、お客さまに製品・サービスを提供していくというサプライチェーン全体で、さらなる安全を期すためのゼロトラストセキュリティの実現をめざしていきます。

社員の意識向上と産官学連携の推進

故意あるいは過失によってインシデントが引き起こされる人的リスクについては、社員への対策を徹底するとともに、社員が真に守りやすいルールになっているかを見直していく必要があります。人は目に見えないものに対する危機管理意識をなかなか持ちにくいものです。不注意によるデータ漏えい防止などについて、わかりやすい動画による啓発や、定期的なセキュリティ訓練の実施を通して、社員のさらなる意識向上につなげたいと考えています。加えて、日々のセキュリティにまつわる困りごとや気づきを情報セキュリティ部門と気軽に相談できるオープンな関係を築いておくことも大切です。

また、巧妙化かつ組織化が進むサイバー攻撃への対策として、産官学連携による取り組みも進めていきます。行政が求めていることにしっかりと対策をし、行政を仲介として企業同士で緊密な関係を築き、研究機関と協創し、その知見を導入しながら、セキュリティ体制の強化を図っていきます。

”One Security Team”として 持続的に推進

情報セキュリティに関するさまざまなリスクを想定し、しかるべき対策を講じても、新たなリスクが生まれてきます。対策に終わりはありません。したがって、情報セキュリティにおいては、あきらめない取り組みが大事だと考えます。

グローバルのさまざまな国・地域にある数多くの会社から構成される日立グループは、“One Hitachi”として、組織全体でリスクを管理していくエンタープライズマネジメントを実践していかなくてはなりません。これまで個別で持っていた情報を、全体で最適化するかたちで組み入れていく必要があります。これまで培ってきたセキュリティ対策をさらに進め、全体最適の視点で、グローバルに運用していくためには、「One Security Team」であることの意識が欠かせません。国内外のグループ各社や各部門、さらにはビジネスパートナーが一丸となって、同じセキュリティポリシーの下で、よりスピーディーかつ効果的なセキュリティの取り組みを推進していきます。

日立の情報セキュリティの考え方

デジタル化の進展により、新たな価値が生まれる一方で、日々巧妙化するサイバー攻撃による情報漏えいや操業停止など、事業そのものの継続に支障をきたすリスクが大きくなっています。このリスクを最小化するため、情報セキュリティに関わるリスクマネジメントは、企業の最重要の課題の一つとなっています。こうした背景のもと、社会イノベーション事業のグローバルリーダーをめざす日立は、価値創造とリスクマネジメントの両面からサイバーセキュリティ対策に努めることを重要な経営課題の一つと位置づけ、情報セキュリティに取り組んでいます。

リスクマネジメントとしての情報セキュリティの推進

急速なデジタル化の進展や、グローバルでの複雑な政治・経済情勢の変化などにより、事業環境は日々変化しています。日立では、このような事業環境を把握・分析し、社会的課題や当社の競争優位性、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。

昨今のサイバー攻撃では、その高度化、巧妙化により、その攻撃範囲は拡大し、従来の社内ITシステムだけでなく、OTの分野である、生産・製造環境、開発環境も対象となってきています。また、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も起きています。その結果、グローバルのどこでも攻撃を受ける可能性が高まっており、情報漏えいや工場の操業停止など、その攻撃が事業継続に大きな影響を与えるインシデントも多く発生しています。加えて、中国デジタル三法をはじめとし、各国・地域でのデータ保護法令の強化が進んでおり、サイバー攻撃の結果、万が一、情報が漏えいした場合、企業のコンプライアンスとして法令遵守の観点からもリスクが高くなっています。このような背景から、日立では情報セキュリティを大きなリスクの一つとして認識し、経営課題として、その対策に積極的に取り組んでいます。

日立の情報セキュリティビジョン

デジタル社会において、膨大かつ多様なデータが価値を生み出す一方で、安全・安心への脅威も飛躍的に高まっています。またテレワークの推進など大きく働き方が変わり、今後のセキュリティのあり方も大きな変革が必要となってきています。そして、今まで以上に標的型攻撃は高度化、多様化し、さらに、ランサムウェアにおけ

る脅迫手法を情報窃取に応用するなど、今まで存在する攻撃手法が複合的に使われてきています。このような状況下、ネクストノーマルな社会に向けて、現在日立では、「統制」「協創」「自分ゴト化」の3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	社員一人ひとり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
みにつける

■ **統制:ゼロトラストセキュリティに向けた取り組み**

2011年よりサイバー攻撃対策を本格開始した日立グループでは2017年のWannaCry感染を教訓に、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、昨今の業務システムのクラウド化の活性化やテレワークの定着など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。

■ **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際の対応では、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においては、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。

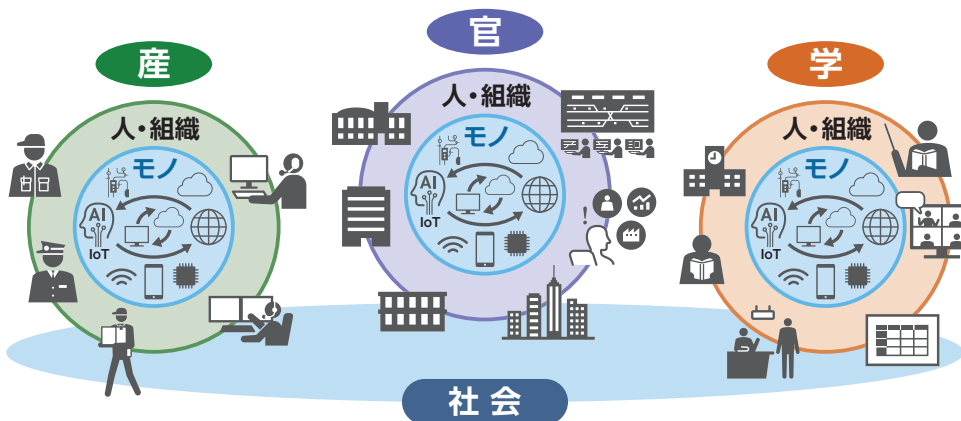
また、つながりは日立の中だけではなく、サイバーセキュリティ対策に取り組んでいる企業、国、学校との脅威情報や対策実行時の課題共有など、枠組みを越えたコミュニティの形成が必要不可欠になっています。各企業や組織が、これらのコミュニティから得られたノウハウを自分たちのセキュリティ対策にフィードバックし、さらに広げるといった、社会が「つながる」活動も、積極的に推進しています。(図表1-2参照)

■ **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せい弱性」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かったりと、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、これからは一人ひとりのセキュリティ意識の向上こそが最後の砦であると考え、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、自分ゴトとして取り組んでいくことをめざしています。

図表1-2 セキュリティエコシステムのイメージ



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

情報セキュリティの方針

日立は、日本を代表するグローバル企業として、セキュリティリスクを経営リスクの一つとして認識し、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、情報セキュリティの確保に努めています。

(1) 情報セキュリティ管理規則の策定および継続的改善

当社は、情報セキュリティを、経営ならびに事業における重要課題の一つと認識し、法令およびそのほかの規範に準拠・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

当社は、当社の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・規範の順守

当社は、情報セキュリティに関する法令およびそのほかの規範を順守する。また、当社の情報セキュリティ管理規則を、これらの法令およびそのほかの規範に適合させる。また、これらに違反した場合には、社員就業規則などに照らして、しかるべき処分を行う。

(4) 教育・訓練

当社は、当社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

当社は、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

当社は、前第1項から第5項に従い、当社および当社グループ会社からなる企業集団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。

情報セキュリティ推進体制

日立グループにおいては、日立製作所 本社（コーポレート）がグループ全体のガバナンスを行います。

日立製作所の各ビジネスユニット（以下、BUと記す）・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。

執行役社長が、情報セキュリティ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、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。

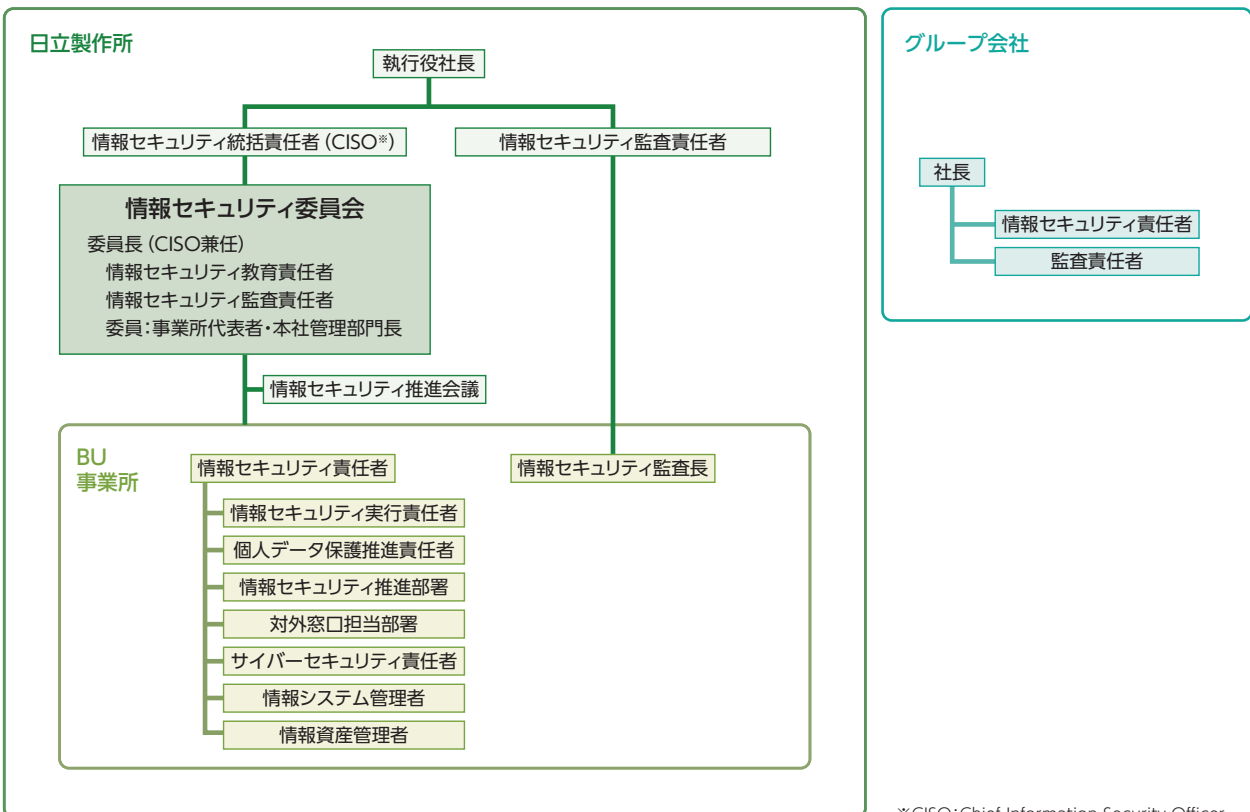
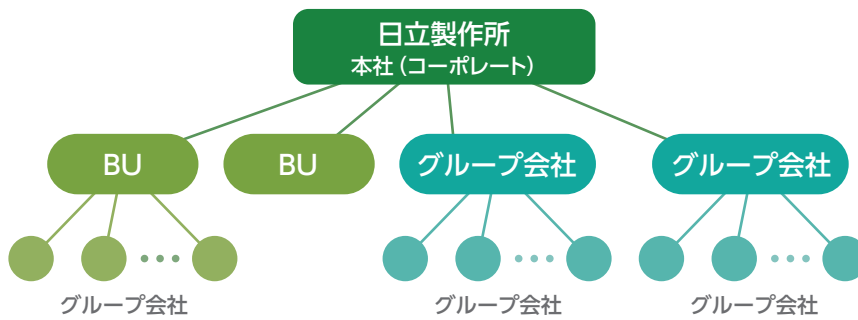
BU・事業所では、原則BU長・事業所長が情報セキュリティ責任者を務めます。情報セキュリティ責任者は、推進をサポートする情報セキュリティ実行責任者、個人データ保護推進責任者を任命し、個人情報保護および情報セキュリティを管理、統括します。

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。また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関する責任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



※CISO:Chief Information Security Officer

情報セキュリティマネジメント

情報セキュリティ規則体系

日立では情報セキュリティの方針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2-②参照)

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順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

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。

■ 個別規則

「Webサイト及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順守すべき事項を定めています。

「入退及び立ち入り制限区域管理規則」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。

情報セキュリティマネジメントサイクル

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ます。

[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ひとりの意識の向上を図ります。

図表2-② 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サイト作成及び情報開示に関する規則
	入退及び立ち入り制限区域管理規則
	個人情報取扱業務委託規準

図表2-③ PDCAのイメージ図



[Check]では、定期的なセキュリティの運用状況の点検、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2-③参照)

また、毎年度、情報セキュリティ施策の成熟度を、経済産業省が発行している「サイバーセキュリティ経営ガイドラインVer3.0」にもとづいて評価し、次年度以降の施策の立案を行っています。

情報セキュリティに関する教育

■ 情報セキュリティに関する教育

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、従業員一人ひとり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。2022年度の日立製作所における受講率は、100%（休職者など受講不可能な者を除く）に達しています。そのほかにも、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2-④参照)

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ひとり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2-④ 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	<ul style="list-style-type: none"> ・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	経営幹部	個人情報保護の動向と日立製作所の取り組み
	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

情報セキュリティマネジメント

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や現場実査などを実施しています。

■ 個人情報保護・情報セキュリティ監査

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回個人情報保護および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、以下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。

■ オンサイトリスクアセスメント

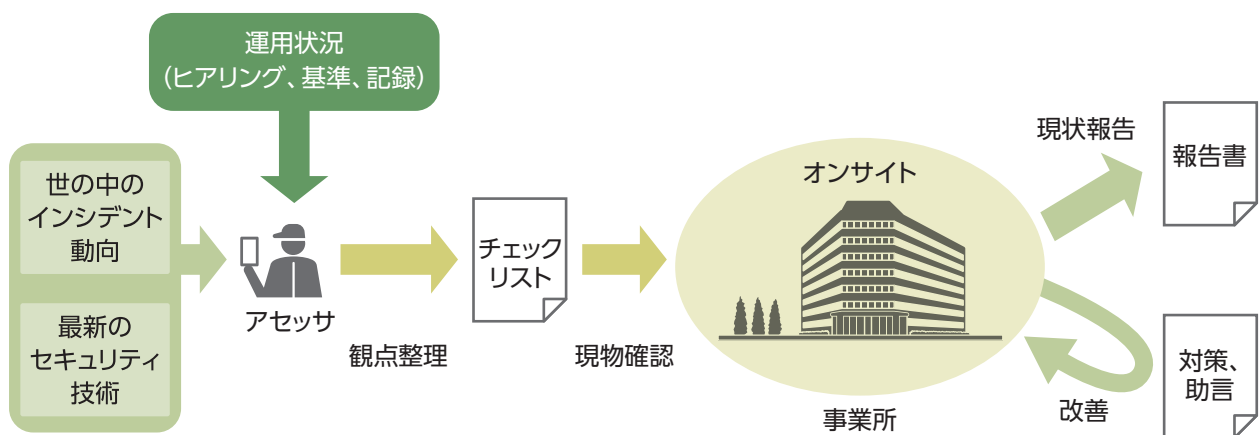
グローバルに事業を展開する日立グループでは、各国・各地域に多くの拠点を構えており、本社機能、営業所、サービスや製造拠点などさまざまな事業形態があります。このような環境下において組織内のネットワークの環境や設備、IT機器などの設置やクラウド環境など、利用環境も多様である一方で、インターネット接続や情報記録媒体（USBメモリ）などを経由した社外とのコミュニケーションを行うため、標的型攻撃やマルウェア感染などのセキュリティリスクへの備えが重要となってきます。

事業を取り巻く環境の変化に伴うリスクに対応するために、セキュリティ専門家チームによるアセスメント体制を強化しています。具体的にはBU・グループ会社の現場を訪問し、次の視点から強化施策に取り組んでいます。

- ① 日立グループのネットワークにつながるすべての製品や社内設備を対象に、セキュリティ専門家チームが最新動向を踏まえたアセスメントを行う
- ② セキュリティ上のリスクとなる課題の抽出と解決に向け現場に対する有効な対策の提言を行う

(図表2-5参照)

図表2-5 オンサイトリスクアセスメントの流れ



2017年度より、延べ約180サイトのアセスメントを行い、セキュリティリスクを多数摘出し、必要な対策についてアドバイスしています。また、全社的な問題については施策にフィードバックを行っています。

2022年度からは、比較的风险が高いと考える海外のグループ会社や、M&Aにより買収した会社に対するアセスメントを強化し、より早い時点でのセキュリティリスクの把握、対策ができるように提言しています。

■ 外見ぜい弱性調査

近年のサイバー攻撃はインターネット上に公開されているぜい弱なサーバを見つけ出し、それらを入口に社内ネットワークへの不正アクセスの試み、ランサムウェアなどのマルウェア感染、個人情報や機密情報の窃盗が企てられます。インターネット上に公開しているサーバがインターネット側からどのように見えているかを調査する取り組みとして、Shodanなどのぜい弱性検索サイトを活用した「外見ぜい弱性調査」を定期的実施しています。サーバの管理者が行うセルフチェックとのかい離がないかを確認することで、セキュリティリスクの低減活動に取り組んでいます。

情報セキュリティマネジメント

セキュリティ人財育成の取り組み

日立グループでは、自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、人財に対するセキュリティの観点での育成を全社において推進しています。

セキュリティ人財育成の考え方

近年のサイバー攻撃の激化に伴い、日立グループでは、自社内のセキュリティ強化、また、お客さまに提供する製品・サービスのセキュリティ確保を目的に、それらを提供する人財へのセキュリティ観点での育成を推進しています。育成する人財は、3つに分類されます。高度なセキュリティ専門家だけでなく、製品・サービスの開発・運用に携わる技術者や社内ITの利用者も対象として人財

育成を進めています。(図表2-6参照)

- 高いセキュリティスキルを持ち、日立グループのセキュリティをけん引するセキュリティ専門人財
- お客さまに提供する製品・サービスの設計・開発・運用、および生産・製造現場のセキュリティ施策を担う人財
- セキュリティの基礎を理解し、セキュリティ事故発生時に適切に対応できるベーシック人財

各人財区分ごとの育成プログラム

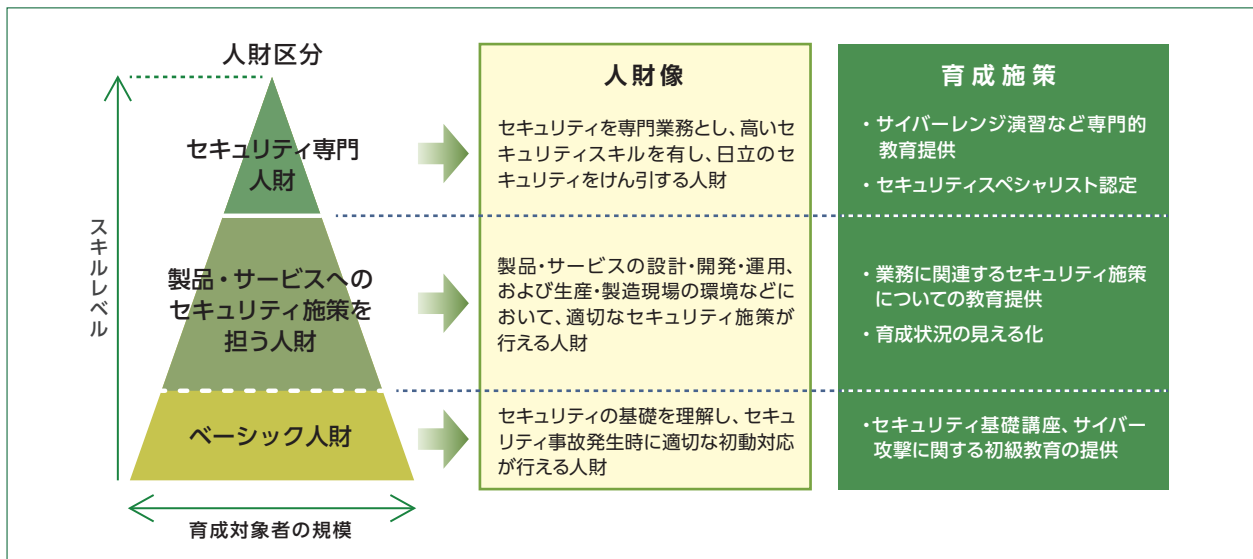
3つの人財区分に合わせた育成プログラムを開発し、それぞれの目的に応じた人財育成を効果的に推進しています。

■ 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、2014年8月より、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、これまでに1,800名を超える人財を認定しています。

図表2-6 3つのセキュリティ人財区分と育成施策



■ 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、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の育成なども実施しています。

■ 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について修得すること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、2016年度より提供を開始した「サイバー攻撃対応基礎知識修得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、これまでに10,000名を超える人財が受講をしています。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。なお、新型コロナウイルス感染症による環境の変化に対応し、集合教育として提供していた教育のオンライン化を行い、ベーシック人財向けにワークショップ形式で提供していた「サイバー攻撃対応コミュニケーション訓練」についても2020年度よりオンライン教育へ移行しています。(図表2-7参照)

図表2-7 ベーシック人財向け教育

サイバー攻撃対応基礎知識修得 eラーニング

✓ サイバー攻撃を受けた際の動きや影響を 修得する研修

【基礎知識】

- ① 日常業務での注意点 ② サイバー攻撃への対処
- ③ 開発時の注意点 ④ ぜい弱性情報の収集と対策検討
- ⑤ インシデント発生時の備え

【体験学習】

- ① 標的型攻撃による情報流出
- ② ランサムウェア感染による業務妨害
- ③ Webアプリケーションのぜい弱性による被害
- ④ マルウェア被害

サイバー攻撃対応コミュニケーション訓練 (ワークショップ)

✓ インシデント発生時の状況把握、 対応内容決定の訓練

【対応プロセス】

- ① Observe (観察) ② Orient (方向付け)
- ③ Decide (意思決定)
- ④ Act (対応・対策) に要求される迅速性、正確性の体験

【コミュニケーションスキル】

- ① 報告 ② 連絡
- ③ 相談において、役割分担の重要性や出来事を5W1Hで正確に伝えることの重要性の理解

情報セキュリティマネジメント

グローバル情報セキュリティ強化の取り組み

グローバルビジネスの拡大に伴い全世界の日立グループにおいて、情報セキュリティの取り組みが重要となっています。日立では、セキュリティ施策の確実な遂行に向け、グローバルセキュリティにおけるガバナンス浸透を向上させるべく、各地域に情報セキュリティエキスパートを設置し、グローバルガバナンス強化に取り組んでいます。

情報セキュリティエキスパートによるガバナンス強化活動

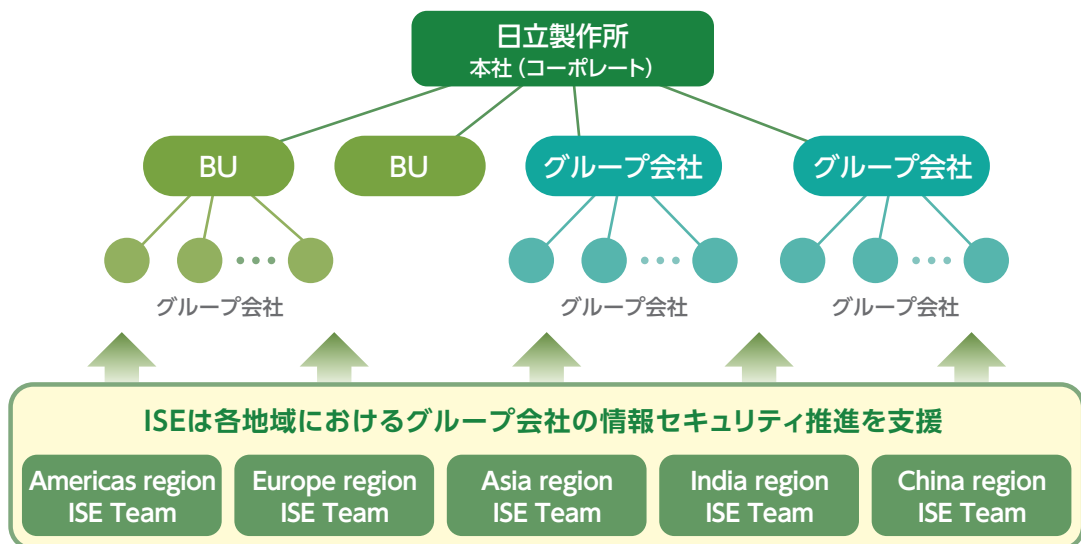
情報セキュリティのガバナンスラインは、日立グループのセキュリティ統括部門より方針・施策を各BU・グループ会社へ共有・指示を行い、各BU・グループ会社はそれぞれ区処する海外法人に対し、その実行を指示します。

グローバルで各社の情報セキュリティ推進を支援するため、2019年より各地域に情報セキュリティエキスパート (ISE:Information Security Expert) を設置し、ガバナンス浸透を向上させる活動を開始しました。2023年現在、米州、欧州、アジア、中国、インド地域に配置し、各地域の現地法人支援を行っています。

情報セキュリティエキスパート (ISE) は、セキュリティ統括組織と一体となり、各地域のガバナンス強化を図っています。(図表2-8参照)

各地域でのコミュニティ確立、コミュニケーション活性化やセキュリティ意識醸成のためISEによるサイバーセキュリティワークショップやウェブセミナーの開催、セキュリティニュースレターの発行を行い、区処会社経由の本来のガバナンスルートを補完する機能として、現地法人へのガバナンス強化支援を行っています。(図表2-9参照)

図表2-8 情報セキュリティエキスパート (ISE) のガバナンス強化体制



図表2-9 情報セキュリティエキスパート (ISE) の主な活動内容

ISEの主な活動内容	
1. セキュリティ統括組織と連携したセキュリティ施策計画策定・実行	5. 「自分ゴト化」を意識したセキュリティ啓発活動支援
2. セキュリティ成熟度・ガバナンス浸透度の把握と各社向上支援	6. 各地域における各種法律・規制への関係部署との連携対応
3. 各地域におけるセキュリティコミュニティの確立	7. 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
4. 海外現地法人のセキュリティ担当を対象としたワークショップの開催	

セキュリティ状況の可視化とPDCA活動

日立グループでは、現場視点のIT&セキュリティ対策実施自己評価および第三者によるアセスメントを実施し、ITガバナンス向上を推進しています。

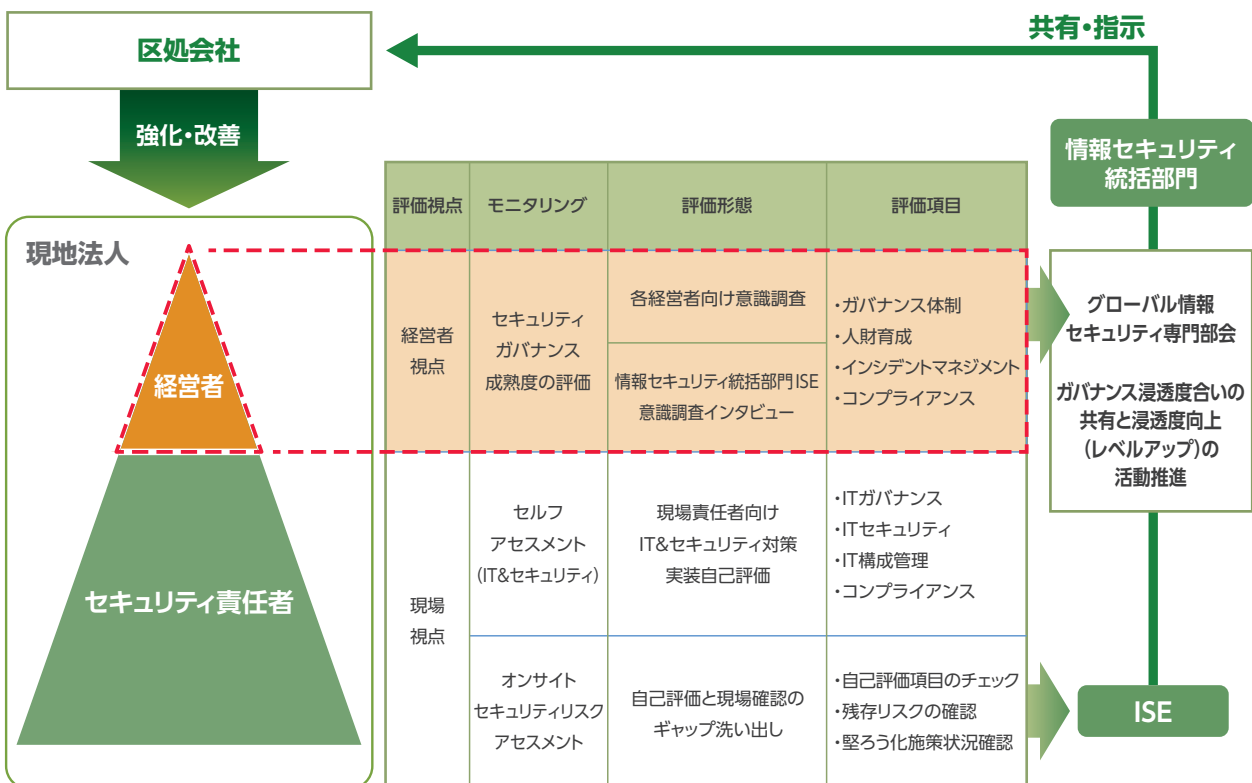
従来の現場視点に加え、経営者視点のセキュリティガバナンス成熟度を把握すべく、海外現地法人の経営者向けにセキュリティガバナンスの取り組み状況について意識サーベイを実施しています。

意識サーベイは、ガバナンス体制、人財育成、社内ITセキュリティ、生産・製造セキュリティ、製品セキュリティ、サードベンダ、コンプライアンスといった多方面をカバーする内容となっています。

海外現地法人経営者向けのサーベイ結果については、データの可視化・分析を行い、ガバナンス浸透度を上げる具体的な活動立案につなげています。また、可視化されたデータについては、BU・グループ会社のセキュリティ管理・統制を行う責任者とも共有し、各社でのセキュリティ活動立案 (Plan)、実施 (Do)、確認 (Check)、評価・改善 (Action) の指標としても有効利用を図っています。(図表2-10参照)

経営者視点、現場視点の両アプローチにより、PDCAの実現を促進しています。

図表2-10 グローバルでのセキュリティ状況モニタリングと評価フィードバックの流れ



情報セキュリティマネジメント

M&Aにおける情報セキュリティ強化の取り組み

日立では、積極的に推進しているM&Aの際のセキュリティリスクを最小化するために、日立グループに新しく加わる会社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における情報セキュリティガバナンス強化の方針

日立グループでは事業拡大を実現するために、積極的なM&Aを実施してきています。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していくことが必要になります。

買収後に情報セキュリティ事故が発覚した場合には、

買収する会社にとどまらず日立グループ全体へ大きな影響（企業価値や営業活動など）を及ぼすリスクが生じるため、情報セキュリティリスクの有無を早期に把握し適切に管理することが不可欠です。買収する会社に対して、M&Aの早い段階から日立ルールを理解および順守を働きかけ、日立のポリシーに基づいた統制管理を実施することが重要となります。

M&A時の情報セキュリティリスク評価

M&A時のリスク評価は、契約締結の前後2フェーズに分けて行います。

① 契約締結 (Day0) 前に実施する「情報セキュリティリスク評価」

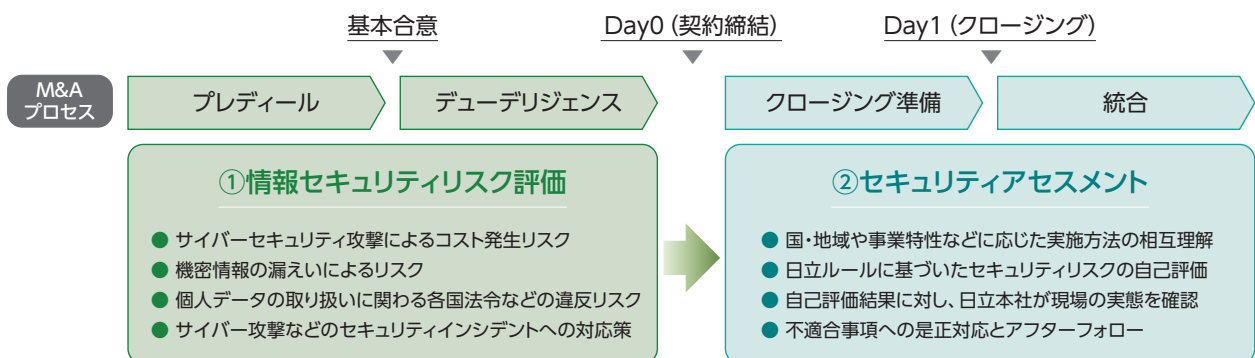
情報セキュリティの組織・体制、規則・ポリシー・基準の整備状況、事業の特性や国・地域における法制度への対応、サイバーセキュリティ事故などの発生有無および事後対応の状況など、公開されている情報および事前提供を受けた情報に基づき、買収する会社の情報セキュリティリスクを分析します。

② 契約締結 (Day0) 後に実施する「セキュリティアセス

メント」

買収した会社が事業を展開している国や地域の状況や特性などを考慮した上で、アセスメントを行う拠点を選定します。次に、日立のルールに基づき対象分野ごとに用意したリスク評価項目により選定した拠点を対象に自己評価を行ってもらいます。その上で、自己評価の結果をさらに詳しく把握するために、日立本社が対象拠点を直接訪問して現場の状況を確認します。最後に、日立ルールに適合していない事項がある場合には、是正計画を作成してもらい是正完了までアフターフォローを行います。（図表2-11参照）

図表2-11 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



■ 情報セキュリティリスク評価の考え方

買収時は会社の規模に関わらず交渉の早い段階で、情報セキュリティリスクの有無を適切に把握することが重要です。事業領域やサービス内容に応じてどのようなリスクがあるか評価する必要がありますが、情報漏えいなどのリスクが明らかな場合には、買収価格やITシステムの移行費用に転嫁することも考えなければなりません。

また、是正が必要な重大な情報セキュリティリスクが確認された場合には、そのリスクを今後どのように低減していくのか、買収会社と具体的な対応方針を協議した上で、計画的に改善策を推進する必要があります。

日立としては、グループ全体への情報共有やフィードバックも並行で行いつつ、全体をふかんにして各社のリスク状況を適切に管理する統制体制を整備しています。

■ セキュリティアセスメントの対象領域と評価項目

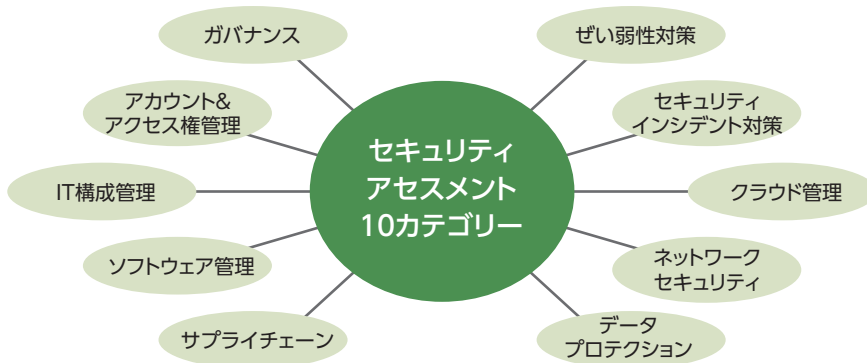
日立では、従業員が普段オフィスで業務に使用するPCやサーバなど（社内IT環境）に限らず、製品開発や製造時に使用する関連機器・装置、お客さまに製品・サービスを提供する環境などを対象に、サイバーセキュリティリスクの対象と捉えています。また、個人情報保護や機密情報管理などに関する管理方法や漏えい対策などについて確認します。（図表2-12参照）

セキュリティアセスメントの評価項目は、ISMSやNIST SP-800シリーズなどを参考に策定した社内のセキュリティ基準（日立規則）から近年の情報セキュリティインシデント状況を考慮して、10カテゴリーから構成されています。（図表2-13参照）

図表2-12 サイバーセキュリティリスクと情報セキュリティリスク

サイバーセキュリティリスク				情報セキュリティリスク
社内IT環境	開発・検証環境	生産・製造環境	製品・サービス	データプロテクション
共通項目 (サプライチェーン・ガバナンス)				
<ul style="list-style-type: none"> 社内ネットワーク 社内ネットワーク未接続機器 社外公開サーバなどの機器 社内IT機器 (PC・サーバなど) <p>情報システム部門管理</p>	<ul style="list-style-type: none"> 開発用機器 検証用機器 デモ用機器 <p>各組織個別管理</p>	<ul style="list-style-type: none"> 生産用機器 製造用機器 検査用機器 <p>各組織個別管理</p>	<ul style="list-style-type: none"> サービス提供環境 <p>各組織個別管理</p>	<ul style="list-style-type: none"> 個人情報保護 GDPR対応 機密情報管理

図表2-13 セキュリティアセスメントの評価項目10カテゴリー



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マネジメント

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、今までの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。

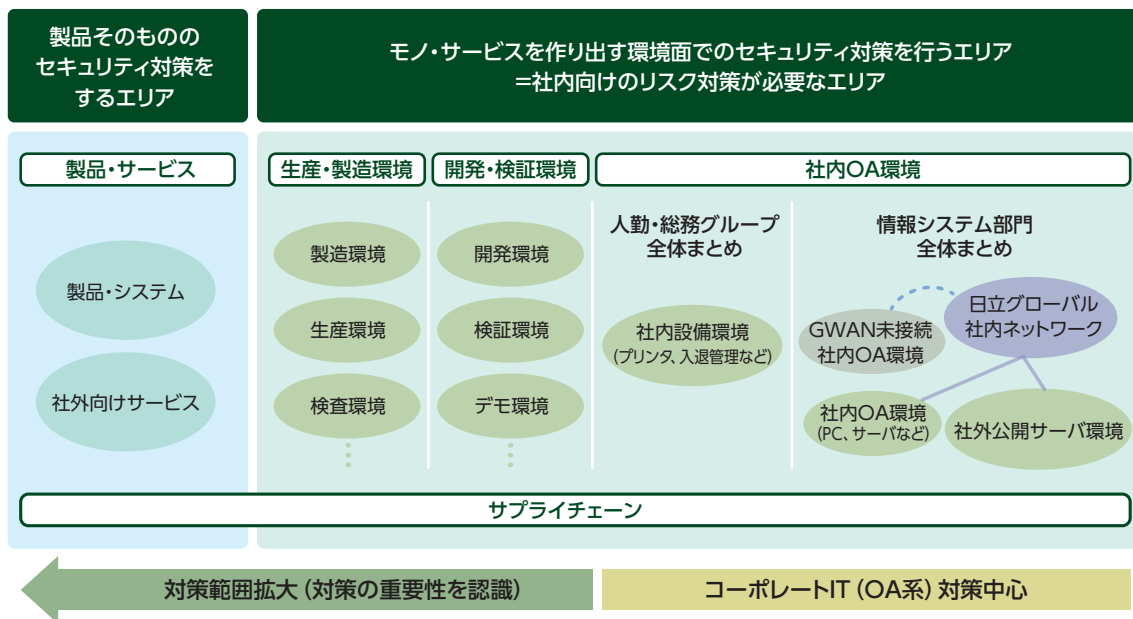
サイバーセキュリティ対策の強化施策

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OA環境以外の攻撃への対応、また、製品・サービスや調達に対するサイバーセキュリティ対策が求められるようになってきました。(図表2-14参照)

このため、2018年から、社内OA、開発・検証、生産・

製造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2-15参照)

図表2-14 サイバーセキュリティ対策範囲の拡大



図表2-15 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OA	IT	・社内OA環境の接続・分離要求事項の策定と展開	
開発・検証	環境面	設計・開発	・社内OA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

推進体制

本社（コーポレート）では、サイバーセキュリティ専門部会内に各領域別に分科会を設置し、サイバーセキュリティの強化施策を立案します。

各分科会での施策は、サイバーセキュリティ専門部会から、グループ内の各BU・グループ会社のサイバーセ

キュリティ対策徹底機能の取りまとめであるサイバーセキュリティ責任者を通じて、各部門へ展開されます。

各部門は、サイバーセキュリティ責任者の指示に基づいてサイバーセキュリティ対策に対する施策の周知徹底を図ります。（図表2-16参照）

環境別のセキュリティ強化の取り組み

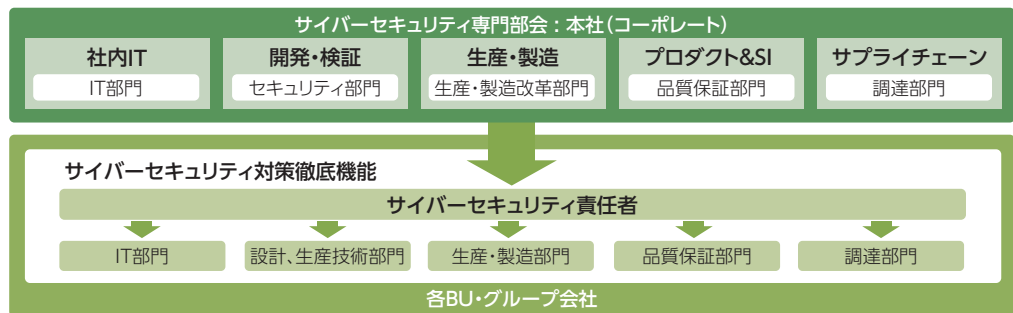
■ 社内OA環境におけるセキュリティ強化

社内OA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/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。

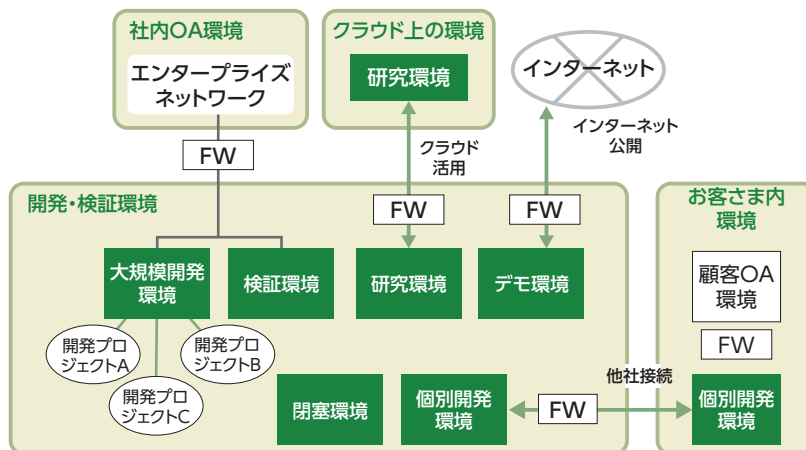
■ 開発・検証環境におけるセキュリティ強化

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2-17参照）

図表2-16
サイバーセキュリティ
推進体制



図表2-17
開発・検証環境の
セキュリティネットワーク



サイバーセキュリティの取り組み

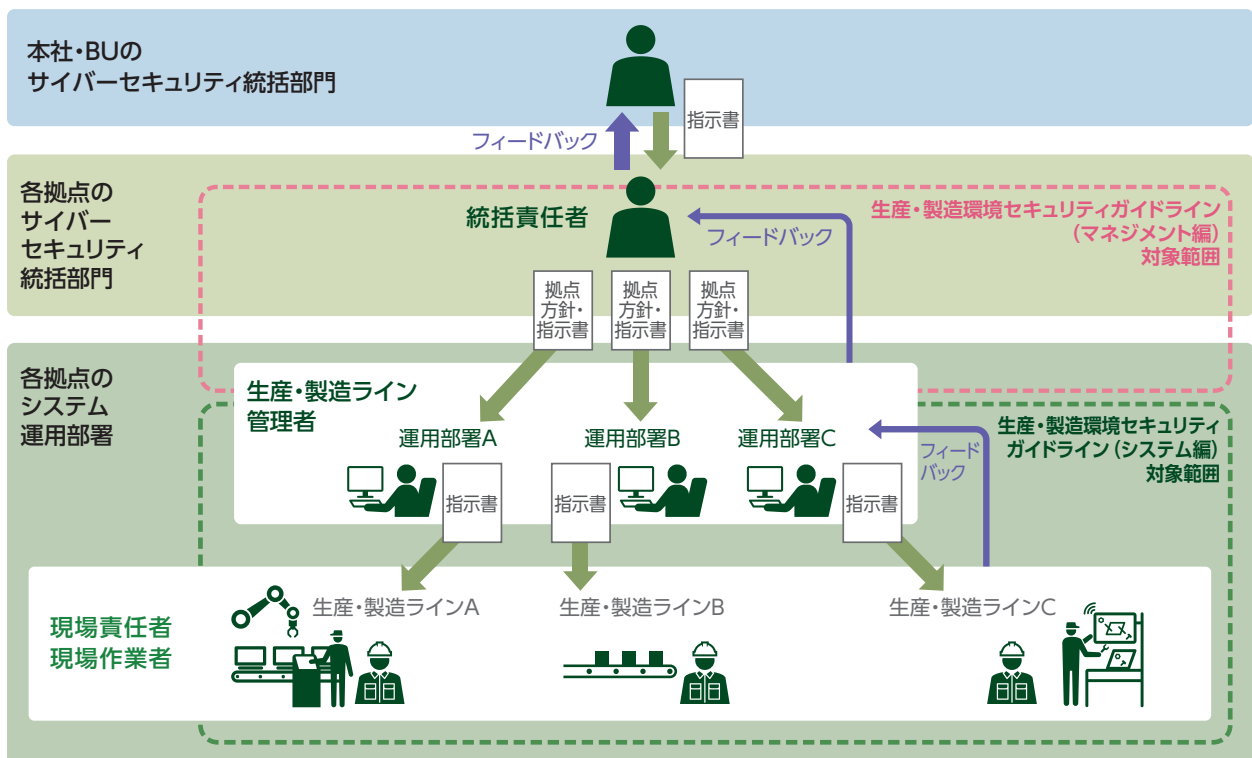
■ 生産・製造環境におけるセキュリティ強化

生産・製造環境は、他環境（社内OA、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2-16参照）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、順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2-19参照）

図表2-19 生産・製造現場向けのポスター・ルール集



図表2-18 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

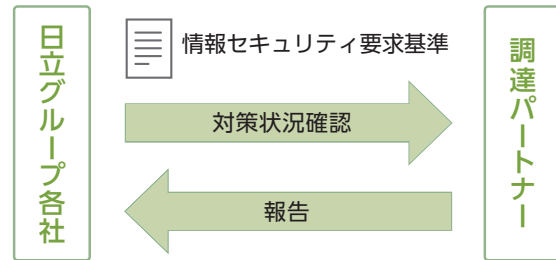


ガイドライン構成	内容	対象者
マネジメント編	マネジメント面（組織・人的管理面としての取り組み）として、組織体制の整備および、拠点全体・部署個別のセキュリティ運用・管理上ルールの策定と見直しについて記載。	サイバーセキュリティ統括責任者
システム編	「IEC62443-3-3」に基づき、現状把握と対策検討としてシステム構成およびその対策方法は、日立グループの代表的なモデルを用いて記載し、各部門・各部署でカスタマイズして利用する。	生産・製造ライン管理者 現場責任者 現場作業員

サプライチェーンにおけるセキュリティ強化の取り組み

セキュリティ上、日立の情報資産に注意を払っていたため調達パートナーに対し業務を委託する際には、あらかじめ日立が定めた情報セキュリティ要求基準に基づき、調達パートナーの情報セキュリティに関する対策状況を確認、審査しています。この情報セキュリティ要求基準には、昨今のサプライチェーンに対するサイバー攻撃に対するセキュリティ対策の項目を付加した「情報セキュリティガイドライン」を追加しています。また、日立としての情報セキュリティに関する要求事項を具体的に示

すことで、調達パートナーに確認いただいています。
(図表2-20)



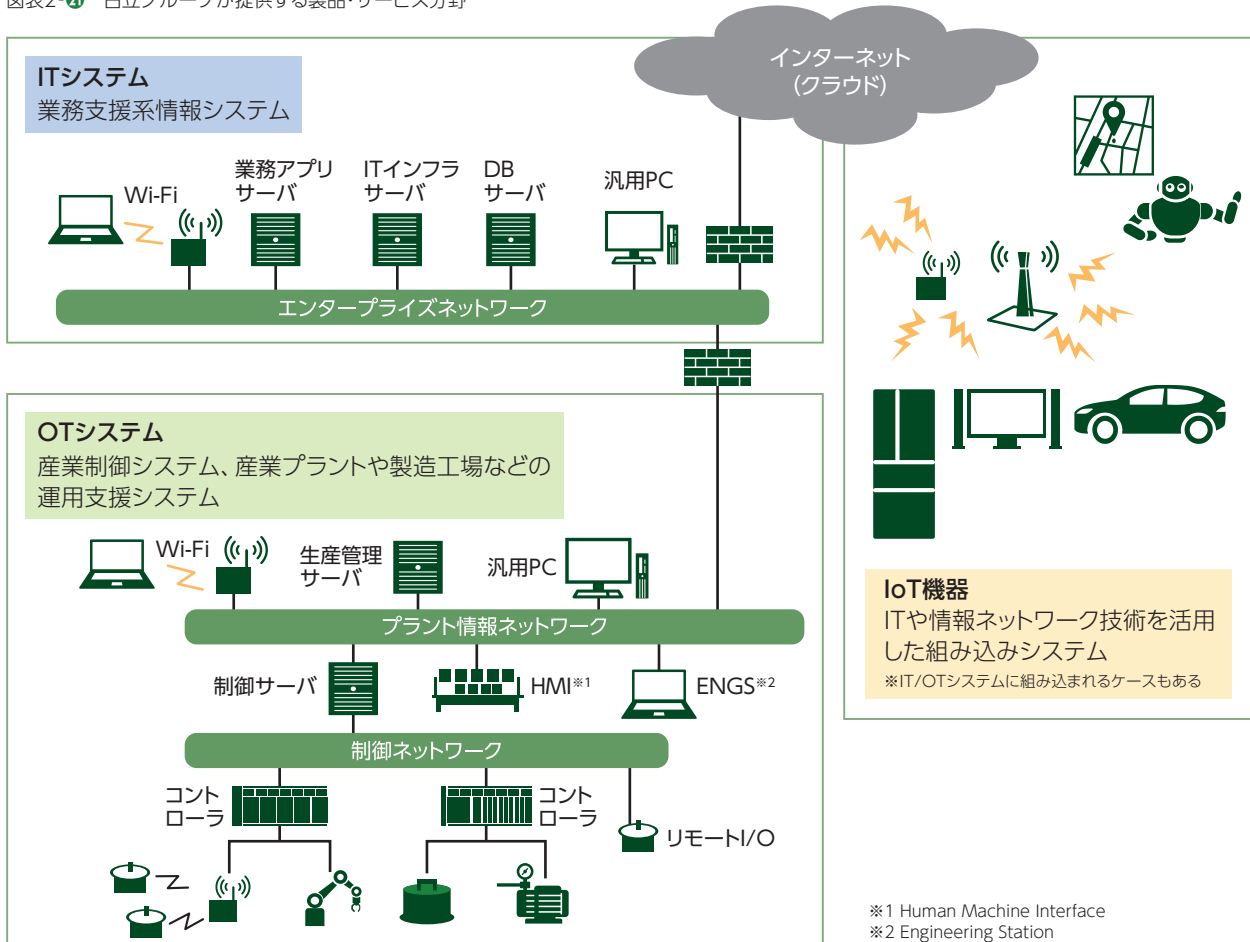
図表2-20 サプライチェーンにおけるセキュリティ強化体制

製品・サービスに関するセキュリティ強化の取り組み

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

図表2-21 日立グループが提供する製品・サービス分野



サイバーセキュリティの取り組み

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2-21参照)

■ 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2-22参照)

各部門は、セキュリティマネジメントに関する部門規程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2-23参照)

■ 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程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。

これらにおいて、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、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、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として、本社（コーポレート）とBU・グループ会社にPSIRT (Product Security

図表2-22 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、製品と記す）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2-23 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		

Incident Response Team)として整備し、各々が連携して、製品・サービスにおける脆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。

■ 製品・サービスのセキュリティ確保に関する先行的な取り組み

日立製作所では、お客さまに提供する情報系製品・サービスのセキュリティを確保するため、セキュリティ対応施策の検討・策定体制を有し、セキュリティマネジメントプロセスに沿ってそれらを運用、改善する活動を推進しています。その長い歴史の中で、先行的に実施している取り組みについて、以下に記します。

(1) セキュリティ対応施策の策定・運用

セキュリティ対応施策の策定・運用を推進しています。例えば、インターネットへの接続は一般に高いリスクを伴うことから、インターネット接続に対する認可制度を設けており、承認を得なければインターネットへの接続や公開などが行えない仕組みを取っています。本活動には、関連するグループ会社も参画しており、連携して策定された施策は、関連する事業部門に展開され、各事業部門において運用されます。

(2) セキュリティマネジメントプロセスに沿った製品・サービスの開発・運用

製品・サービスの開発・運用の各フェーズに、セキュリティマネジメントプロセスを定義し、それを規則化することで組織におけるセキュリティ対策の確実な実施につなげています。リスクの大きさを定義するセキュリティランクの概念を採用し、ランクづけの指標を定義し、セキュリティランク別に開発・運用時のセキュリティ確保に必要なセキュリティマネジメントプロセスを示しています。セキュリティランクの採用は、リスクの高さを認識し適切な対応を取ることを促すだけでなく、リスクとコストのバランスの考慮にもつながります。またそのプロセスは、日立において標準化されている情報システム開発プロセスとも連携した内容となっています。規則化されたセキュリティマネジメントプロセスの内容は、定期にまたは必要に応じて随

時に改訂されます。これは、発生したインシデント、顕在化したリスク、運用した結果などからのフィードバックに基づき実施され、マネジメントプロセスがより適切なものになるよう継続的な改善を行うことを目的としています。

(3) セキュリティ人材の配置に関する施策の推進

製品・サービスのセキュリティリスクに応じたセキュリティ品質の確保を目的として、適切な資格・経験・知識を備えた3種類の人財(①セキュリティリスクアセッサ・②セキュリティシステムアーキテクト・③セキュリティオペレーションズアドミニストレーター)を定義し、レビュー、設計・テスト、運用の各プロセスに配置する施策を推進しています。セキュリティリスクアセッサは、各事業部門の長によって任命され、セキュリティの専門的観点でレビューを実施し、助言・指導をします。セキュリティシステムアーキテクトおよびセキュリティオペレーションズアドミニストレーターは、専門知識を活用して各プロジェクトのセキュリティに関する設計・テストや運用を遂行します。これにより、セキュリティが確保された製品・サービスの開発・運用を実現し、お客さまに提供しています。

(4) ぜい弱性点検の実施

ぜい弱性攻撃による被害の抑止を目的に定期的ぜい弱性診断を実施しています。点検のタイミングは、新規開発時、環境変更時および定期実施としています。点検方法は、チェックリストを用いた定性的なもの、ぜい弱性点検ツールを用いたものがあり、これらを単独または併用することで、システム特性や運用状況に沿った適切な点検が行えるようにしています。

(5) ぜい弱性関連情報のハンドリングとインシデント対応体制の整備

ぜい弱性を悪用したセキュリティインシデントの発生可能性の低減を目的に、情報系製品・サービス提供部門におけるぜい弱性関連情報のハンドリングプロセスをガイドにまとめ、これに基づき活動を推進しています。また、大規模なインシデント発生時の対応体制および対応マニュアルを整備、訓練を実施することで迅速かつ確な対応ができるよう備えています。

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、二重脅迫の脅威など、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。日立製作所では、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2017年10月より設置し、セキュリティ監視・インシデントレスポンス強化を図っています。

■ セキュリティ監視

日立グループでは、グローバル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。2017年より監視対象を拡大しており、グローバルの基幹拠点すべてをカバーしています。また、EDR (Endpoint Detection and Response) の導入により、機器の動作監視や調査・対処も可能となりました。これにより、EDRと基幹拠点からのログを組み合わせることで分析することが可能となり、精度の高い効率的な監視を実現しています。

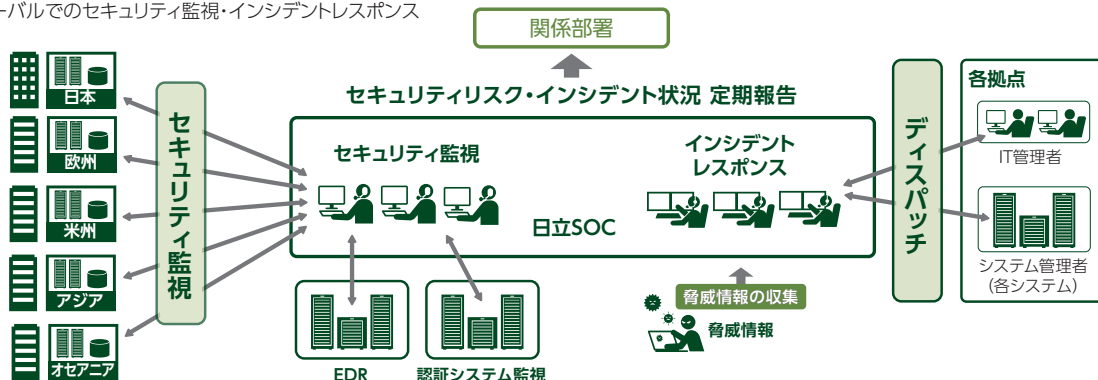
最近の脅威動向として正規の認証情報を不正に取得し悪用する攻撃が増えています。正規の認証情報が利用されており検知が困難なため、認証システムの監視機能を強化することで、第三者によるアカウント不正利用の早期検知を行っています。

■ インシデントレスポンス

日立グループでは、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。2020年からは、基幹拠点のログ監視とEDR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、認証システムの監視を組み合わせることで、昨今の在宅勤務環境における新たな脅威にも対処しています。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2-24参照)

図表2-24 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CISO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、以下に示すようなWeb上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の収集を行っています。

- IPA、JPCERT/CC、CISAなどの社外の公的団体の情報発信サイト
- セキュリティ関連のニュースサイト
- 各種セキュリティベンダのブログサイト、ホワイトペーパー

収集した情報は、情報元が公開する指標（深刻度、CVSS基本値など）から攻撃成功の可能性、社内システムでの利用状況などを基に、脅威を5段階の警戒レベルで分類しています。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、昨今急速に変わりつつあるセキュリティに係る各国法制度等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

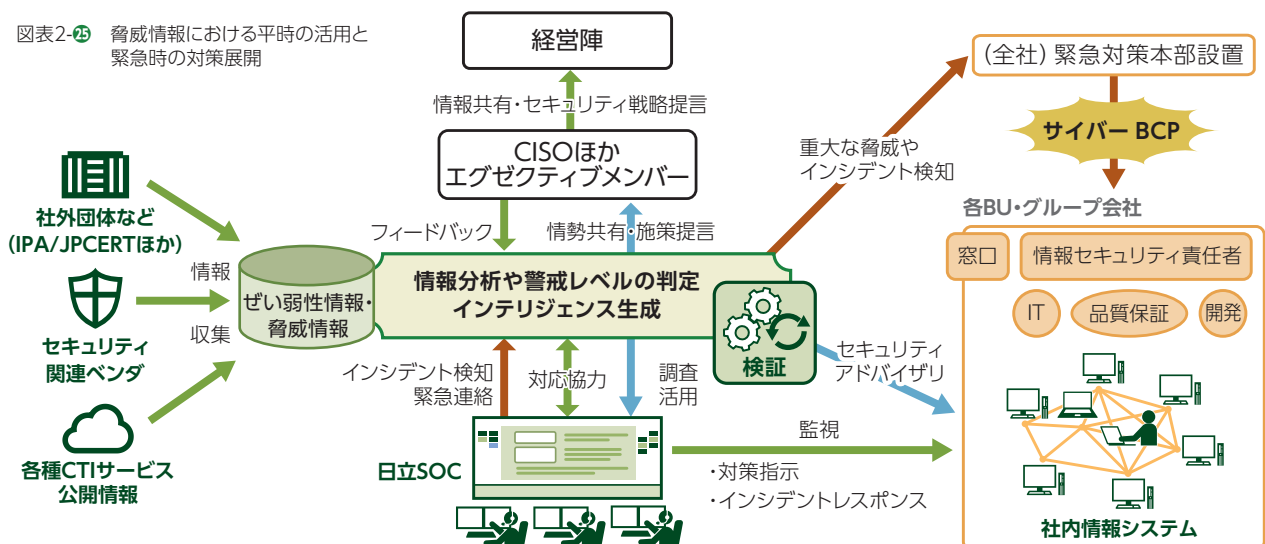
収集した情報は、各BU・グループ会社から選出されたサイバーセキュリティ責任者に対して、即時～週次でのメール配信、社内Webへの掲載などを通じて周知を行っています。また、日立グループ全体に関わる影響範囲の広い脅威に対しては、サイバー BCPの発令に関して検討するとともに、対策を徹底させるためのサイバー警報を発報することで対策強化を図っています。また、社外に公開しているシステムを調査し、被害を受ける可能性のある場合は該当部署へ個別に通知し、対策を促す活動を行っています。これらの収集・分析情報を基に、日立SOCや情報システム部門とも連携し脅威ハンティングを行い、インシデント対応や監視の強化に活用しています。

これらの活動から得られた知見から、日立グループの現状や改善が必要な対策についてを整理し、本社のセキュリティ統括部門やCISOと連携し、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につなげることで、セキュリティ対応実行サイクルの加速を図っています。

■ 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2-25参照)

図表2-25 脅威情報における平時の活用と緊急時の対策展開



サイバーセキュリティの取り組み

日立グループにおける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 (Cyber Security Incident Readiness /Response Team) 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

セキュリティインシデント (以下、インシデントと記す) とは、サイバーセキュリティに関係する人為的事象で、不正アクセス、サービス妨害行為、データの破壊などの行為 (事象) を示します。

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

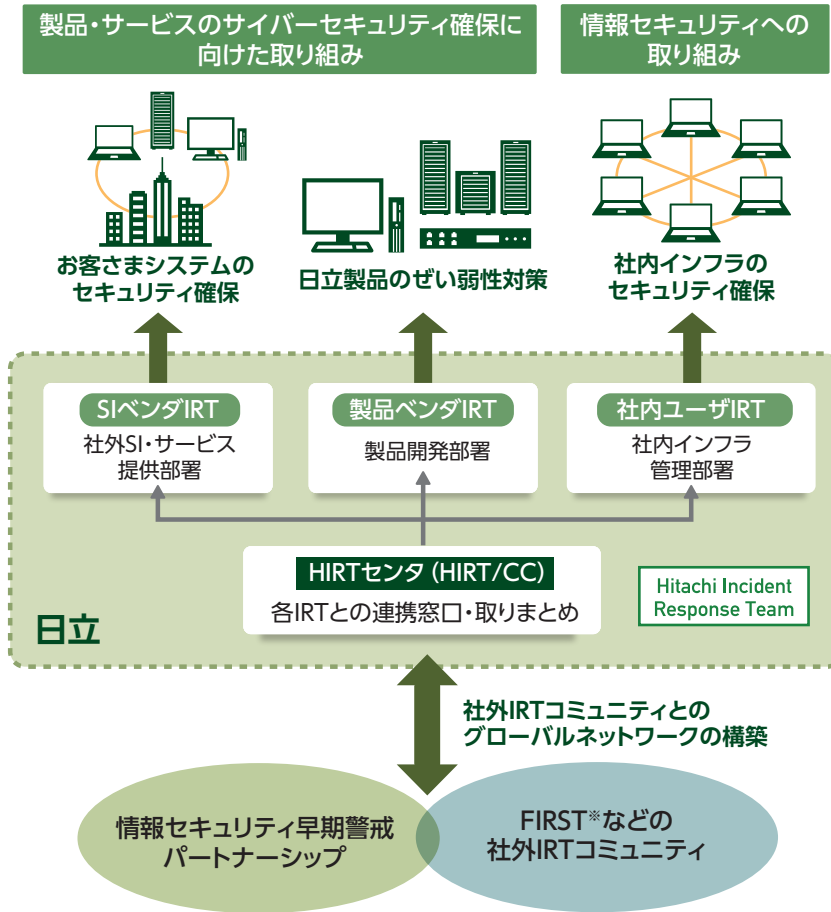
ために、下記のように、4つのIRT (Incident Response Team) という活動モデルを採用しています。4つのIRTとは、

- (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IRT)

の3つとともに、

- (4) これらのIRT間の調整業務を行うHIRT/CC (HIRT センタ) 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2-26参照)

図表2-26 ぜい弱性対策とインシデント対応活動を支える4つのIRT



分類	役割
HIRT/CC*	該当部署: HIRTセンタ FIRST*、JPCERT/CC*、CERT/CC*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。

*HIRT/CC: HIRT Coordination Center
 FIRST: Forum of Incident Response and Security Teams
 JPCERT/CC: Japan Computer Emergency Response Team/Coordination Center
 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ー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

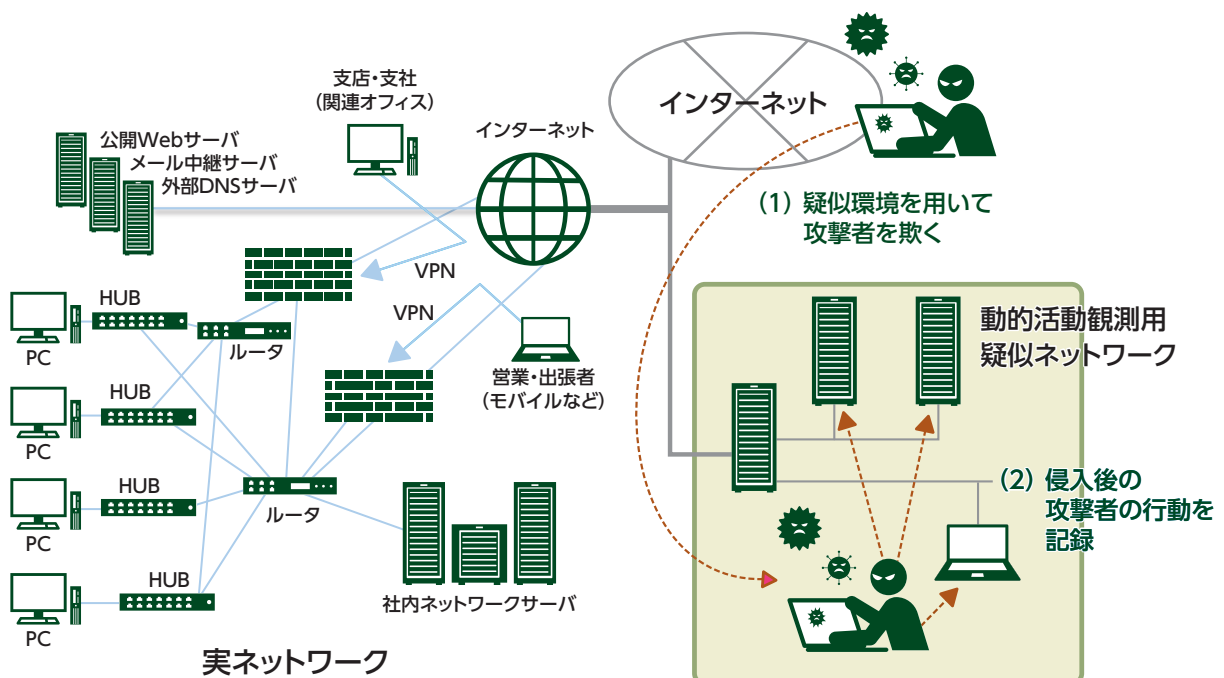
「次の脅威のキャッチアップ」と早期に対策展開を図るための技術として「動的活動観測」に取り組んでいます。動的活動観測は、標的型攻撃などのサイバー攻撃を調査するために構築した組織内ネットワークの疑似環境下で、侵入後の攻撃者の行動を記録し分析する観測手法です。(図表2-17参照)

(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の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

図表2-17 攻撃者の行動を記録する動的活動観測システム



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まいります。

(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、分野に特化したIRT活動の検討と整備を進めています。金融分野における先行的な取り組みとして2012年10月に、HIRT-FIS^{※2}を設置しました。

※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、脅威情報構造化記述形式STIX^{※4}、米国国土安全保障省のAIS^{※5}などを用いた情報利活用基盤の整備を推進しています。

※4 STIX:Structured Threat Information Expression

※5 AIS:Automated Indicator Sharing

(3) 研究活動の整備

マルウェア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、人材育成の場の醸成、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/>

データプロテクションの取り組み

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2-28参照)

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、社内規程が法令、プライバシーマーク準拠規

程である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、4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2-29参照)

図表2-28 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

日立製作所（以下、当社と記す）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、当社の技術情報や、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、当社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まいりました。この考え方に立ち、日立製作所は下記、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/>)

(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。

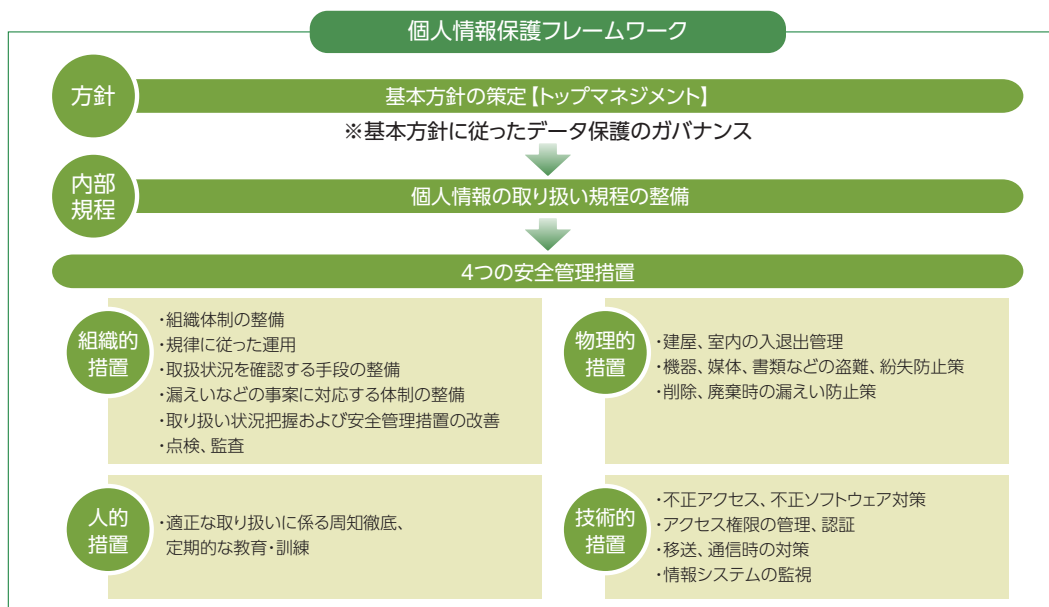
(4) 法令・規範の遵守

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2-10 個人情報保護のフレームワーク



データプロテクションの取り組み

■ 個人情報保護体制

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。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。

■ 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2-30参照)

■ 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、漏えい事故などの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。

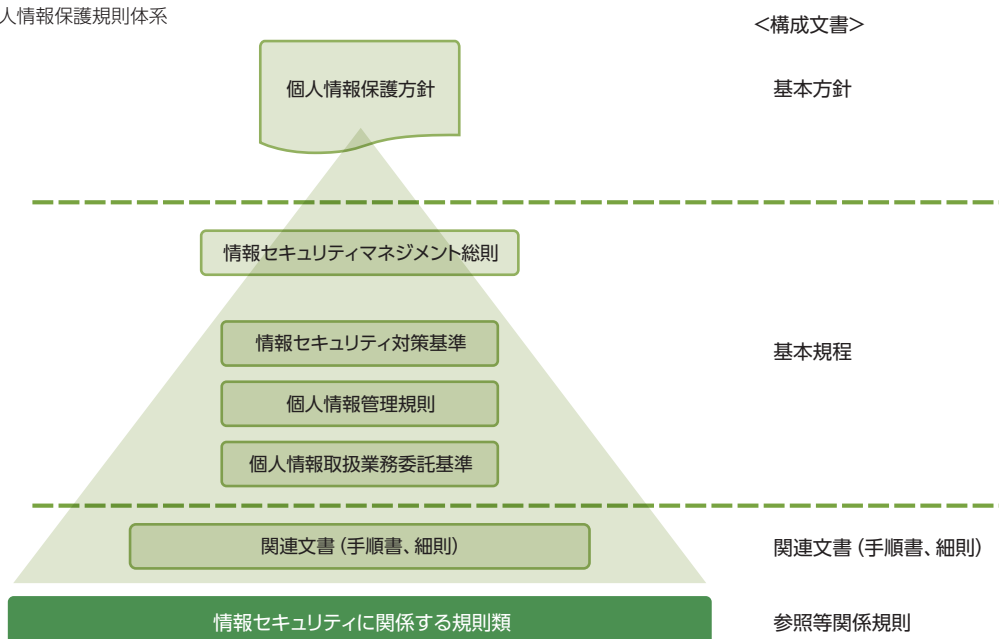
個人情報保護マネジメントシステム

日立の個人情報保護マネジメントシステムはJIS Q15001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、47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

図表2-30 個人情報保護規則体系



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、および関連文書に規定されています。

■ 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定期的な運用の確認、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。

2022年度は、前年度に規則改正した「改正個人情報保護法対応」の推進他について、計画を立て[Plan]、改正内容に基づいて活動を実施[Do]、点検、監査にて推進状況の確認を実施し[Check]、結果を評価し見直しを行いました[Action]。(図表2-31参照)

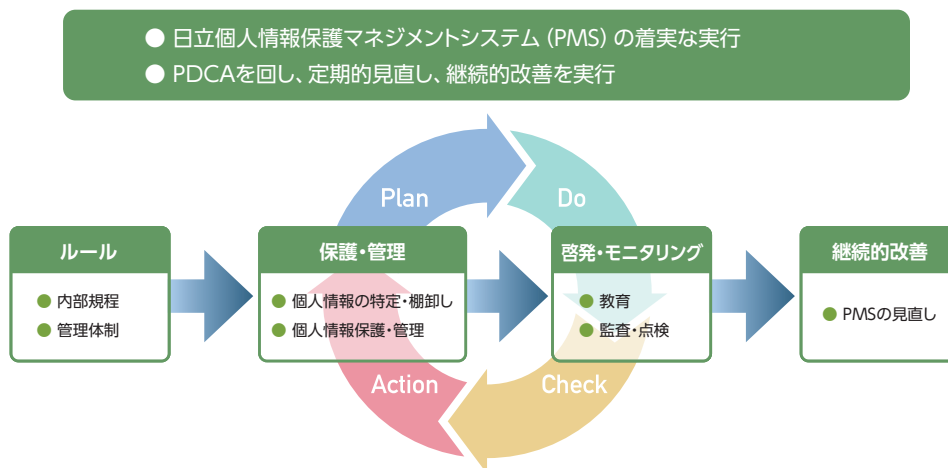
個人情報の管理と適切な取り扱い

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、台帳を管理し、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か月に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

図表2-31 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



データプロテクションの取り組み

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。

■ 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回個人情報保護および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（739業務*）部署門については「個人情報保護運用の確認」を1か月に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。

*2023年3月時点

■ 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、従業員一人ひとりに配布しています。

■ 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

デジタル化の著しい進展を受けてデータの利活用が進んでいる昨今、プライバシーリスクも増大しています。個人情報保護への要請の高まりを受け、世界各国で個人情報保護関連法制度の強化が進んでいます。

国境をまたいだデータ利活用が広く行われる中、各国法制度では自国の個人情報の保護を海外所在事業者に対しても求めたり、他国への個人情報越境移転を規制していたりする場合があります。このため、個人情報保護のコンプライアンス対応では各国法制度の動向を把握した上で適切な対応を進める必要があります。

日立では、グローバルでの個人情報保護法制対応の先駆けとして、欧州一般データ保護規則（GDPR）への対応推進を図ってまいりました。

中国の個人情報保護法をはじめとしたその他の国や

地域のデータ保護法令に対しても、現地の地域統括会社と連携しながら対応を推進しています。

日立グループ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おり、グループ各社での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、日立グループ会社全体の個人情報保護のコンプライアンス対応機能の強化・整備に取り組めます。

日立グループのプライバシーマーク®への取り組み

日立グループでは、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、2022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、2023年3月に9回目の付与適格決定を受け、2025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鑽を重ねています。

※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（2023年7月末時点）。

株式会社 日立製作所	株式会社 日立システムズパワーサービス
株式会社 日立製作所 病院統括本部	株式会社 日立システムズフィールドサービス
日立健康保険組合	株式会社 日立社会情報サービス
沖縄日立ネットワークシステムズ株式会社	株式会社 日立情報通信エンジニアリング
株式会社九州日立システムズ	株式会社 日立総合計画研究所
株式会社四国日立システムズ	株式会社 日立ソリューションズ
株式会社セキュアブレイン	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ICTビジネスサービス	株式会社 日立ソリューションズ西日本
株式会社 日立アーバンサポート	株式会社 日立ソリューションズ東日本
株式会社 日立アカデミー	日立チャンネルソリューションズ株式会社
株式会社日立医薬情報ソリューションズ	株式会社 日立ドキュメントソリューションズ
株式会社 日立インフォメーションエンジニアリング	株式会社 日立ハイシステム21
日立SC株式会社	株式会社 日立パワーソリューションズ
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 日立ビルシステム
株式会社 日立ケーイーシステムズ	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 日立コンサルティング	株式会社 日立保険サービス
株式会社 日立産業制御ソリューションズ	株式会社 日立マネジメントパートナー
株式会社 日立システムズ	株式会社 日立リアルエステートパートナーズ
株式会社 日立システムズエンジニアリングサービス	株式会社北海道日立システムズ

データプロテクションの取り組み

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、多種多量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も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。

パーソナルデータの利活用とプライバシー保護

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2-32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。(図表2-32参照)

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2014年から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。

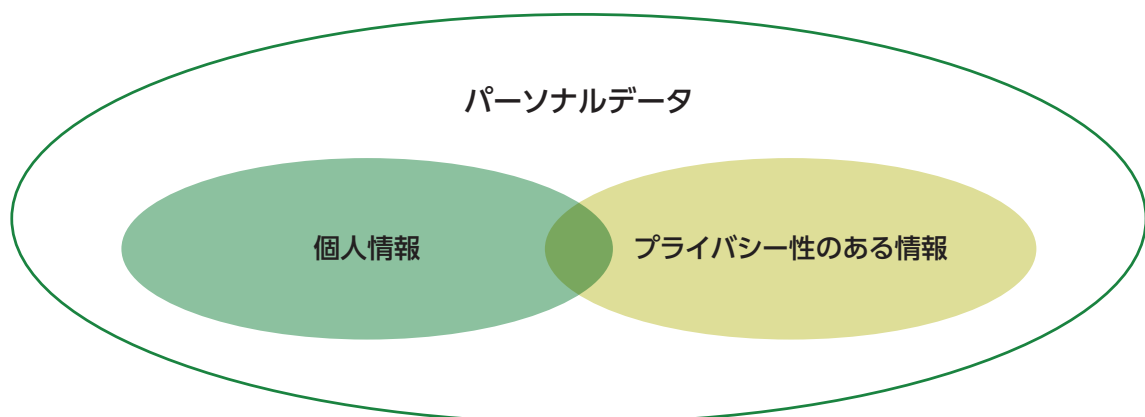
■ プライバシー保護諮問委員会の運営

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パーソナル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」を設置しています。

■ プライバシー保護に関する規則・マニュアルの整備

このような体制のもとでプライバシー保護方針を定め、方針に沿ってパーソナルデータの取り扱い規則を制定し、従業員向けのマニュアルを整備しています。マニュアルでは、プライバシー保護のための具体的なプロセス、留意事項などを解説することで、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。

図表2-32 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



■ プライバシー影響評価の実施

このような規則・マニュアルに従って、従業員はパーソナル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、プライバシーに関わる問題の発生を防ぐための対策を講じています。評価にあたっては法制度や技術の動向、問題化事例、後述する意識調査から得られた知見などから日立が独自に作成したチェックリストを使用します。このとき、従業員だけでは判断が難しい場合や、リスクが高いと評価された場合には、プライバシー保護諮問委員会が対応を支援し、リスクの低減を図っています。

デジタルシステム&サービスセクターにおいては、これまで多くの業務にプライバシー影響評価を適用しており、その件数は2022年度だけで約270件に及びます。対象となった業務分野も金融、公共、社会インフラ、産

業・流通など、多岐にわたっています。さらに、2023年から日立プライバシー(PIA)制度を導入することで日立製作所全社をあげたプライバシー保護の取り組みを加速しています。これらの取り組みを通じて、パーソナルデータを取り扱う業務においてプライバシー影響評価を実施することでプライバシーに関わる問題の発生を未然に防ぐための対策を講じています。

■ プライバシー保護教育

パーソナルデータ利活用とプライバシー保護の両立を図るためには、個々の社員がその重要性を理解し、プライバシー対策を実践する必要があります。そのため、プライバシー保護に関する定期的な教育や情報共有を行うとともに、プライバシー保護のあり方について検討しています。

お客さまの安全・安心をめざして

2022年3月に、一般社団法人 日本経済団体連合会が主催した「個人データの適正利用に向けたシンポジウム」で、「パーソナルデータの利活用とプライバシー保護」と題し、日立のプライバシー保護の取り組みについて講演しました。講演後のパネルディスカッションでは、パネリストの方から日立のプライバシー保護の取り組み

は先進かつ有益であるなどと評価いただきました。

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。

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。

欧州、米州とグローバルで開催しているセキュリティワークショップでは、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としています。また、日本におけるワークショップでは、セキュリティエコシステムというタイトルでのパネルディスカッションを実施しセキュリティ専門家やIT専門家の立ち位置と全く違う視点での気づきや、そこから得られた学びの共有を進めています。

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国、学校、他の企業と、脅威情報や対策実行時の課題共有など、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行い、サイバーセキュリティ対策のノウハウを共有・共感することで、より有益な対策につなげることが可能となります。

そのために、日立では、グローバルなコミュニティに参画をしています。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やサイバーセキュリティ/デジタルリスクのベストプラクティスなどの世界最先端の調査研究を行うISF (Information Security Forum) に加盟し、情報セキュリティに関する最先端の情報交換や共有を行っています。

加えて日立では、従業員それぞれの持つ経験や知識を生かし、以下に示す国際標準化活動、シーサート(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、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及び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おります。

- OASIS CTI

構造化情報標準促進協会 (OASIS) のサイバー脅威インテリジェンス (CTI) では、サイバー攻撃活動を記述し交換するための脅威情報構造化記述形式、検知指標情報自動交換手順に関する規格化が検討されています。

■ シーサート (CSIRT) 活動

日立では、日立グループにおけるシーサート活動に加え、HIRT (Hitachi Incident Response Team) を窓口 (PoC: Point of Contact) として社外シーサート活動に参画しています。また、社外シーサート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。2023年6月現在で、105か国、652チームが加盟しています。

- 日本シーサート協議会 (NCA)

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

団体です。シーサート設立の促進・支援、インシデント発生した場合のシーサート間の連携体制づくりなど、国内のシーサートコミュニティが、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、国内のシーサート活動の普及を推進しています。

■ そのほかの活動

上記活動に加えて、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大脅威執筆委員会 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、制御システムSMS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

- 一般社団法人ICT-ISAC

- 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

- ロボット革命イニシアティブ協議会 産業セキュリティアクショングループ

- 日本セキュリティ・マネジメント学会 (JSSM)

- 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

- 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Japan Automotive ISAC

- 一般社団法人交通ISAC

- 電力ISAC

情報セキュリティ啓発活動

日立では、一人ひとり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」

テレワークの導入が一気に加速、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、テレワークの推進には十分なセキュリティ対策が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、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。

本来、セキュリティ対策は、「IT」、「プロセス」と「ヒト」の3要素でバランスを取る必要があります。

昨今の劇的な環境変化に対応するため、そして、これからの日立としてのセキュリティリスクを低減するため

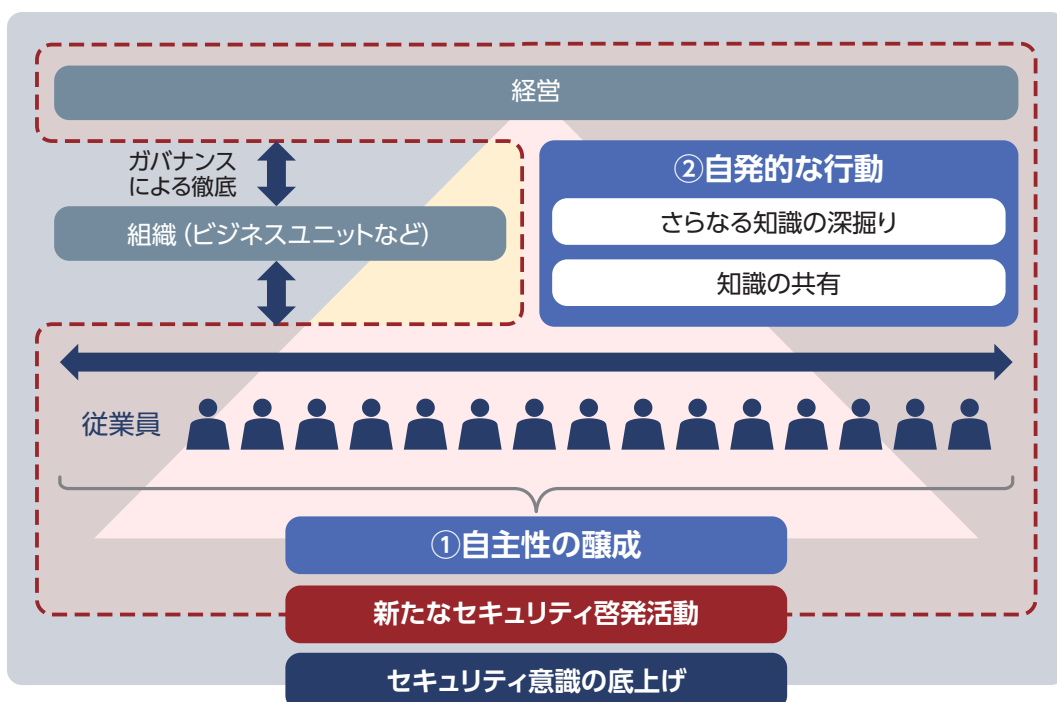
に、従業員への啓発・教育を拡充し、よりバランスの取れたセキュリティ対策の推進に着手しました。「セキュリティ意識の向上こそが最後の砦である」と考え、既存のガバナンス徹底に加え、従業員の自主性の醸成と、自発的な行動により、セキュリティ意識の底上げを図る活動に取り組んでいます。「自分ゴト化」と「従業員が心から共感すること」をキーワードに、従業員が受け身ではなく、自らセキュリティに興味を持ち、自分ゴトとして取り組むことをめざしています。

(図表3-①参照)

図表3-① これからのセキュリティ啓発のめざす姿

既存のガバナンス徹底に加え、
従業員一人ひとりの自主性の醸成と自発的な活動によるセキュリティ意識の創出

一人ひとり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」



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3-②参照)

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、アニメーションやチャットなどを通じて、従業員一人ひとり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。

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3-③参照)

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。

「セキュリティと愉しく関わりながら、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。

※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3-② 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。



図表3-③ 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、従業員一人ひとり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。



社会のレジリエンスを高める 協調型サイバー防衛技術の研究開発

近年サイバー攻撃の見逃しや対応の遅れによる経済や社会インフラへの影響が社会的な問題となっています。日立では、攻撃を受けた組織が、対策ノウハウを他組織と迅速に共有し協調防衛する技術と、デジタルツイン上で対策の影響を評価し適切な対策を選択可能とする技術を組み合わせ、より多くの攻撃への自動対処・復旧の実現をめざします。

社会のレジリエンスを高める協調型サイバー防衛技術の研究開発

近年サイバー攻撃は、分野を問わず数多く発生し、ある組織で発生した攻撃が他の組織でも同様に発生しているケースも多くみられます。日立、慶應義塾大学、中部電力株式会社は、2017年4月から、攻撃への対策ノウハウを記載したインシデントチケット（以下、チケット）といった、これまでの施策では共有してこなかった情報を迅速に共有・活用する「分散型セキュリティオペレーション（以下、分散SOC）」構想の共同研究を推進しています。これにより、攻撃の予防や検知、適切な対処を連携して行うことで、被害の拡大防止をめざしています。

また、日立では保護対象のシステムをサイバー空間上に再現（デジタルツイン化）し、攻撃に対するセキュリティ対策の複数立案・仮想適用や対策によるシステム停止等の副作用を事前評価することで最適な対策を迅速に選択する「セキュリティデジタルツイン（以下、SDT）」技術を開発しています。これにより、システムの安定稼働が特に重要である制御システムといったミッションクリティカルシステムにおいて、本来の業務への悪影響を最小限に抑えた適切なセキュリティ対策を可能とします。

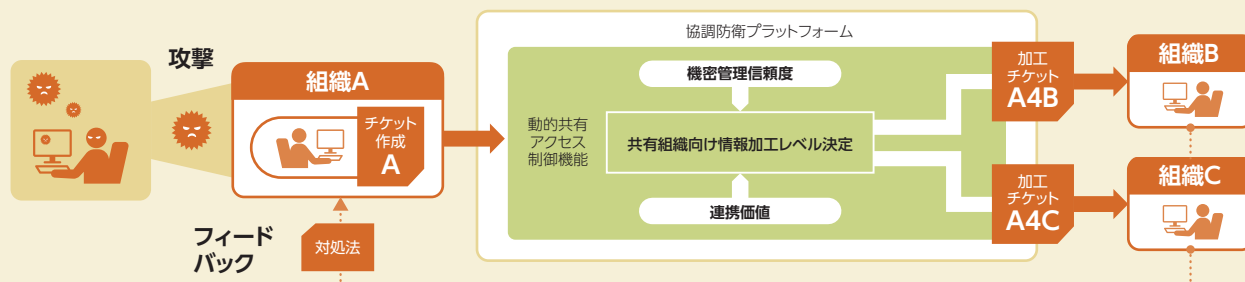
分散型セキュリティオペレーション技術の研究

チケットを共有するにあたり、共有相手の信頼度や連携により期待できる値を基に、開示可能な機微・機密情報の範囲を、相手組織ごとに自動設定する技術、「協調防衛プラットフォーム」を2022年に開発しました。機微・機密情報の範囲を限定（匿名・抽象化処理）することで、安全性と効率性を兼ね備えた対策情報の共有が実現でき、組織間での情報連携の促進が期待されます。開発した技術は、以下2つを特徴とします。

1. 相手組織に応じてチケットの情報加工レベルを決定する「動的共有アクセス制御機能」

本制御機能は（図表①）に示すように、相手組織の機微・機密情報の取り扱いに対する信頼度（以下、機密管理信頼度）、および連携により期待できる自組織の利益（以下、連携価値）を定量化し、それらの値に応じて情報加工レベルを決定します。すなわち、上記機密管理信頼度および連携価値が高い組織には、無加工の状態でチケットが送付され、上記値が低い組織に対しては、IPアドレスやシステム構成情報などの機微・機密情報が削除されて相手と

図表① インシデント対策情報共有技術



共有されます。この機密管理信頼度は、相手組織のセキュリティ体制やセキュリティ担当者のスキル等に基づき決定され、連携価値は、以下に説明する「チケット共有利益算出機能」により決定されます。

2. チケット共有相手からのフィードバックの価値を算出する「チケット共有利益算出機能」

「自組織と同様の攻撃を受けている組織からは、有用なフィードバックを得られる可能性が高い」という仮定のも

と、チケットに記載された攻撃者の識別子（攻撃元のIPアドレスや悪性ドメイン名、不審メールの内容など）を、相手組織で観測された攻撃者の識別子と比較し、共通部分が多いほど自組織が得られる価値、すなわち連携価値が高いと判定します。また攻撃者の識別子自体の機密性が高いことから、本機能では秘密計算を用いて暗号化された状態で識別子の共通部分を特定します。

セキュリティデジタルツイン技術の研究

システムに対してセキュリティ対策を実施する際に、業務継続性を担保したセキュリティ対策を選定するセキュリティデジタルツイン(SDT)技術を開発しています。2022年は、特に業務継続性が重要視されるOTシステムをターゲットとしたデジタルツイン・生産率算出モデルを開発しました。開発した技術は以下の2つを特徴としています。

1. 3層モデルによるOTシステムのデジタルツイン構築技術

OTシステムをアクター、アセット、プロセスの3層のモデルによりデジタルツインとして再現し、セキュリティ対策が業務継続性に及ぼす影響を評価します(図表②)。アクターは、日常の業務を行う作業員、攻撃者、セキュリティ対策者などの挙動を表現したモデルです。アセットは、稼働するコンピュータ機器のモデルであり、ソフトウェアの脆弱性やネットワークの依存性などを表現します。プロセスはOTシステムによって実行される業務を表現したモデルです。各モデルには、時系列で変化する挙動を再現可能な独自の状態遷移プログラムを組み込んでいます。

本技術を活用することにより、デジタルツイン上で攻撃者にアセットを仮想的に攻撃させて、実際のシステムに波及する影響や、弱点(例えば危険度の高い脆弱性など)を特定できます。加えて、攻撃によるインパクトを緩和するセキュリティ対策を複数立案したり、それぞれの

対策の副作用(例えば業務のパフォーマンスへの悪影響など)を実際のシステムに影響を与えることなく事前に評価することが可能です。

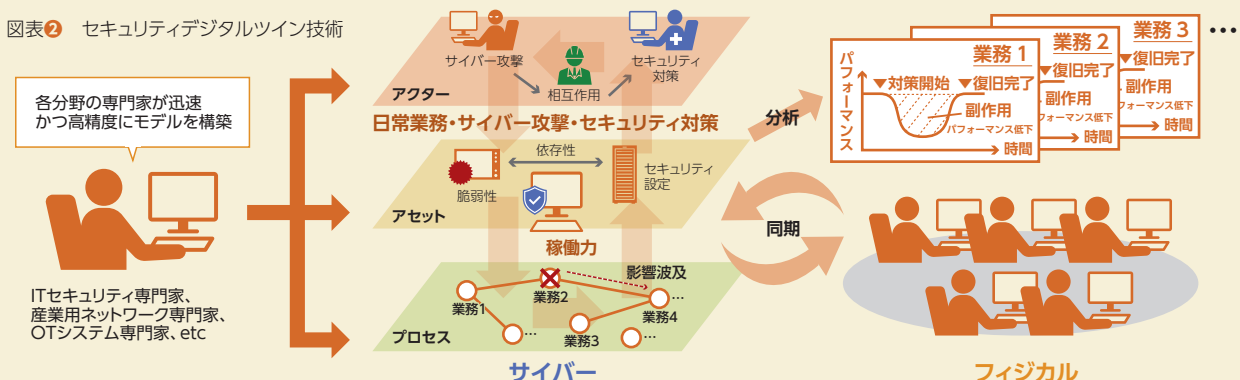
2. 工場環境における生産率算出モデル

前記3層モデルを工場環境に適用するため、特に「ラインにおける生産率を維持すること」を評価目標(KPI)と設定し、セキュリティ対策が生産率に与える影響を算出可能なモデルを開発しました。本技術ではペトリネットを用いて生産業務のデジタルツインを構築し、サイバー空間上でトークンにより表現される製品が複数の工程を経て生産される様子を再現します。これにより、全ての工程が完了したトークンを数えることで、KPIの達成度(生産率)を算出できるようになります。

その他の業務も同様にペトリネットによるモデル化が可能で、危険性の高いぜい弱性に対するセキュリティ対策が複数パターン想定される場合、お客さまのKPIと各対策の副作用を勘案して、最適なセキュリティ対策を導出します。

今後は他組織で発生したサイバー攻撃やその対策を自組織のSDT上で再現することにより、自組織への影響を評価し適切な対策を自動で選択、実行するとともに、ITシステムのみならずOTシステムにおいても自動化をめざします。また、今回開発した技術の社会実装、コミュニティの拡大を進め、安心・安全な社会インフラの実現に貢献していきます。

図表② セキュリティデジタルツイン技術



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 (2023年6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を用いています。

- 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 (社会ビジネスユニット 制御プラットフォーム統括本部)
- 株式会社 日立製作所 (サービス&プラットフォームビジネスユニット サービスプラットフォーム事業本部、アプリケーションサービス事業部 Lumadaソリューション推進本部、デジタルシステム&サービス統括本部 社会イノベーション事業統括本部 Lumada CoE)
- 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およ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 (水・環境ビジネスユニット 水事業部ソリューション事業推進部 デジタルソリューション推進グループ、水・環境ビジネスユニット 環境事業部 情報システムエンジニアリング部、コネクティブインダストリーズ事業統括本部 IT・業革推進本部 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 (インダストリアルデジタル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 (DXクラウドソリューション部))
- 日立チャンネルソリューションズ株式会社
- 株式会社 日立社会情報サービスおよび沖縄日立ネットワークシステムズ株式会社
- 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 (カスタマーサポートセンタ)
- 株式会社 日立インフォメーションエンジニアリング
- 株式会社 日立ICTビジネスサービス (プロダクトサポート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 四国日立システムズ
- 株式会社 日立システムズ (金融プラットフォーム事業部第二サービス本部 ATMサービス部)
- 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ASプラットフォーム設計部)
- 株式会社 日立システムズ (マネージドサービス事業部、ビジネスサービス事業部、セキュリティサービス事業部)
- 株式会社 日立システムズ (マネージドサービス事業部 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 (フィールドサービス (支社統括本部 首都圏支社 首都圏支店))
- 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
- 株式会社 日立ソリューションズ東日本
- 株式会社 日立ソリューションズ
- 株式会社 日立パワーソリューションズ
- 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)
- 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ソリューションズから移管対応中
- 株式会社 日立マネジメントパートナー (事業企画本部、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(2023年6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4-①参照)

図表4-① 「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弱い弱性分析、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水性やソースコード、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、利用者からの正し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 (2023年6月末時点でCMVPIによる“historical list”への掲載を含みます)。(図表4-2参照)

図表4-2 「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 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。

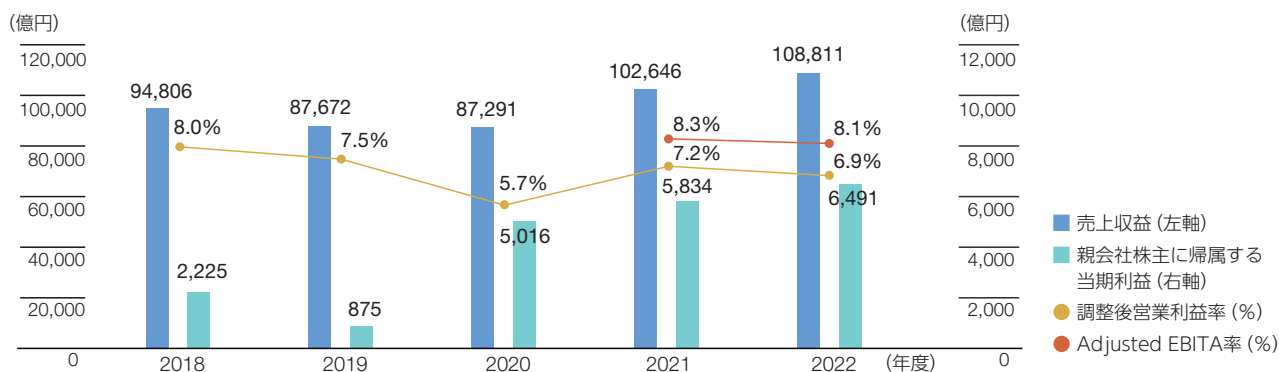
日立グループの概要

会社概要 (2023年3月31日時点)

商号	株式会社 日立製作所	資本金	462,817百万円
設立年月日	大正9年(1920年)2月1日 (創業明治43年(1910年))	従業員数	32万2,525人(国内13万3,762人、 海外18万8,763人)
本店の所在地	東京都千代田区丸の内一丁目6番6号	連結子会社数	696社(国内119社、海外577社)
代表者	代表執行役 執行役社長兼 CEO 小島 啓二	持分法適用会社数	267社

業績ハイライト (2023年3月期連結IFRS)

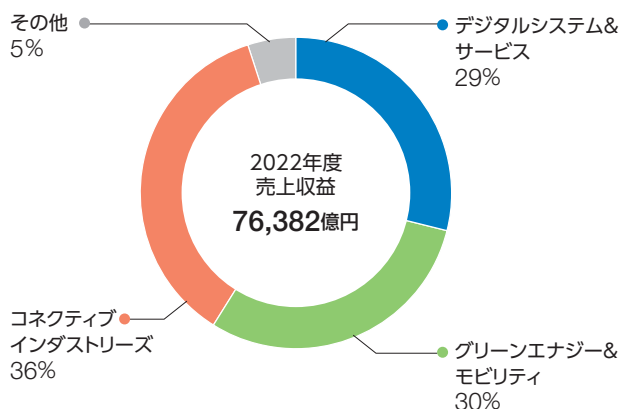
売上収益	10兆8,811億円 (前期比106%)	調整後営業利益率	6.9% (前期比0.3ポイント減)
当期利益(親会社株主帰属)	6,491億円 (前期比656億円増)	Adjusted EBITA率	8.1% (前期比0.2ポイント減)
Adjusted EBITA*1	8,846億円 (前期比292億円増)		



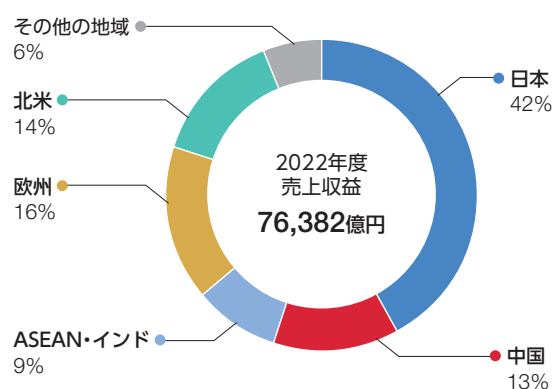
* 当社の連結財務諸表は、国際財務報告基準(IFRS)に基づいて作成しています

*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*



地域別売上収益*



* 2022年度に非連結化した日立金属、日立建機および2023年度に非連結化予定の日立Astemoを除いた今後の連結事業(3セクター)で示しています。

 **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