HITACHI
Inspire the Next

情報セキュリティ報告書 2024

Information Security Report 2024

日立グループ

INDEX

〈本報告書の概要〉

●報告範囲・期間：2023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：2024年11月発行

情報セキュリティを
グローバルかつスピーディーに
“One Hitachi”で加速化する。

国や地域、企業間のボーダーを超えて、サイバー攻撃はますます高度化・巧妙化し、社会全体の脅威となっています。企業は情報漏えいやシステム停止だけでなく企業価値の失墜の危機に常にさらされ、セキュリティ対策は待ったなしの状況にあります。

日立がLumada事業を中心に広くグローバルビジネスを推進していく上で、情報セキュリティを世界規模で考え、いつどこで起きるか予測不能なサイバー攻撃に備える仕組みづくりがますます重要になってきています。日立グループが掲げる「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」明日に向けて、事業に関わるすべての部門、すべての従業員が同じ目的をめざし、“One Hitachi”として情報セキュリティに取り組んでいきます。

株式会社日立製作所
執行役常務　CISO

加賀田 美朗

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2020年からCPO兼バリュー・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。2024年執行役常務、CISO就任。

ますます重要になる情報セキュリティの取り組み

昨今、加速度的に頻発するサイバー攻撃は、攻撃の種類や手法が多様化し、かつ被害が表出するまでの時間が短くなってきています。ランサムウェアの攻撃や窃取した情報の公開など、企業を脅かす事案も後を絶ちません。ITシステムの重要な要素となっているクラウドサービスを狙ったもの、事業プロセスの一部であるサプライチェーンを狙ったものなど、より現場に近いターゲットを狙った攻撃も顕著です。

一方、世界各国で企業に対するデータ保護規制、サイバーセキュリティ関連法制の整備が進んでいます。

欧州一般データ保護規則（GDPR）、中国デジタル三法をはじめ、EU Data Act発効も控えています。日立グループでも、グローバルビジネスを展開する上では、各国の法規制に準拠しながら、セキュリティリスクをマネジメントしていく必要があります。

目まぐるしい世界情勢の変化や自然災害の激甚化など、企業を取り巻くさまざまなリスクを把握し、有事にはスピード感をもって対応することは、企業にとって重要な経営課題です。情報システムを取り巻く環境の変化によって、サイバー攻撃やデータ漏えいも大きなコーポレートリスクの一つとなっており、そのリスクに適切に対応できるか否かは、企業価値に大きな影響を与えます。

情報セキュリティは社会イノベーションを提供する企業としての使命

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」ことをめざす姿として掲げ、IT※1、OT※2、プロダクトによる社会イノベーション事業を進めています。また、今や、海外での売上高は日立グループ全体の約6割にのぼり、広くワールドワイドで製品・サービスを提供しています。まさに、私たちの事業は、世界中のさまざまな国や地域で、ビジネスや暮らしを支える社会インフラに関わっているといえます。

万が一、サイバー攻撃によって、情報漏えいを起こしたり、提供する製品・サービスに不具合が生じたりすることがあれば、社会に及ぼす影響は計り知れません。お客さまや、生活者の皆さまに決して被害が及ぶことがないように、現状をしっかりと掌握し、情報セキュリティを重要な経営課題の一つとして認識する必要があります。情報セキュリティは、グローバルに社会を支えるビジネスを展開する日立グループの使命と考え、取り組みを進めていきます。

対象範囲を拡大するサイバー攻撃に着実に対応

一つは、サプライチェーンも含めた広い範囲でのセキュリティ対策の実施です。今まで以上に、社内IT領域のみならず、製造や開発の現場も、製品・サービスも、そしてサプライチェーンも対象にして、平時/有事を意識したセキュリティ対応が重要になってきていると考えています。

製品・サービスのセキュリティを確保するために、事業部ごとにセキュリティ責任部署を設置し、ソフトウェアのぜい弱性を管理し、問題が発生した場合に適切に対策していけるようにするなど、手順を整備しています。また、サプライチェーンのパートナー企業の皆さまは、同じ船に乗って同じゴールをめざすパートナーとして、実現の可能性を見極めながら、納得していただきながら、情報セキュリティの取り組みを実行していきます。進めていく上で日立グループが支援できることがあれば、一つ一つ解決しながら一緒にやっていきたいと考えています。

グローバルの法規制に対応してデータ保護を確実に実行

次に、各国や地域の法規制に対応したデータ保護の強化です。お客さまの重要なデータを共有させていただき、製品やサービスに反映することで、お客さまの成長をサポートし、ひいてはサステナブルな社会の実現

※1 IT：Information Technology
※2 OT：Operational Technology

に貢献するLumada事業においては、お客さまのデータのセキュアな利活用が極めて重要です。Lumada事業を中核にお客さまにソリューションを提供している日立グループは、グローバルで強化が進むデータ保護に関する法令や規制に確実に対応していきます。

データ保護・プライバシー保護の観点から、各国や地域の法令にのっとった管理を行うことは言うまでもなく、お客さまの資産である機密情報が棄損したり、漏えいしたりすることが決してないように、社内での運用、管理方法を盤石なものにするにとどまらず、お客さまに提供するところまでカバーするセキュリティプロセスと統制の仕組みづくりを進めていきます。

即応性をめざしグローバル推進体制を強化

そして、グローバルでの情報セキュリティに関する体制強化です。サイバー攻撃への対策をいかに迅速に行うことができるかが問われるなか、スピーディーに攻撃を検知し対策を打てるよう、また、平時においても、いち早く施策の徹底を行えるよう、グローバルでの情報セキュリティに関する体制強化を進めています。

グローバル事業を展開していくためには、国や地域ごとのビジネスの考え方や法令をしっかり理解した上で、それらに合った形でそれぞれの地域にきちんと受け入れていただくことが不可欠です。情報セキュリティにおいても、米州、欧州、アジア、インド、中国に設置した本社直轄のセキュリティ担当部門を中心に、各地域で法令をモニタリングしている部門とも連携しながら、最新動向を捉えて、早め、早めに各地域に合った形で、情報セキュリティ施策を推進していきます。

社外との「オープンな協創」、社内での「共感できる意識向上」を大切に

組織化が進むサイバー攻撃に対しては、一企業での取り組みだけでなく、企業間で手を携えて、さらには産官学の連携を強化していくことも重要だと考えます。社会全体の情報セキュリティのレベルが上がることが、日立の情報セキュリティのレベルアップにもつながります。こうしたオープンな考え方のもとに、さまざまな業界団体や学会への積極的な参加と議論を推進していきます。

そして、日立グループ内においては従業員がセキュリティ意識をもって正しく行動できるセキュリティ文化の醸成が不可欠です。火災報知器が煙を察知するように、「何かおかしい」と一人一人が感じ、対応する習慣が大切です。日立グループでは、「損得より善悪」という考え方が定着しています。情報セキュリティにおいても、この考え方に基づいて、何のために行うのか、その先に何をめざしているのかを、全員で共有していきます。共感が生まれ、納得感をもって一人一人が取り組めるように、従業員の情報セキュリティ意識の向上を図っていきます。

「グローバル」に、「即応性」をもって情報セキュリティを推進

これまでのさまざまな業務経験のなかで、私は常に、人間の集団であることを前提に仕事をする大切さを学びました。国籍や年齢など個々人のバックグラウンドに関係なく、人間である以上は、残念ながらミスはあり得ます。失敗は起こり得ることを前提として事を進めていく姿勢が欠かせません。情報セキュリティにおいても、常に100%の対策はないことを念頭において取り組んでいきます。

日立グループは社会を支える事業を展開しています。万が一の場合は、世界規模での社会的影響は甚大です。このことを、決して忘れてはなりません。本年は、創業者小平浪平の生誕150年にあたります。小平が掲げた「和」「誠」「開拓者精神」を、情報セキュリティにおいても胸に刻み、絶えず変化する脅威に対して、あらゆるケースを想定して果敢に向き合い、その対策を真摯に考えて実行していきます。「グローバル」に、そして、「即応性」をもって、日立グループの一人一人が力を合わせて“One Hitachi”で、お客さまと社会のために、情報セキュリティを力強く推進していきます。

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、新たな価値が生み出される一方で、日々巧妙化するサイバー攻撃による情報漏えいや操業停止など、事業そのものの継続に支障をきたすリスクが大きくなっています。このリスクを最小化するため、情報セキュリティに関わるリスクマネジメントは、企業の最重要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、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1-❶参照)

図表1-❶　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

日立グループでは2017年のWannaCry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、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

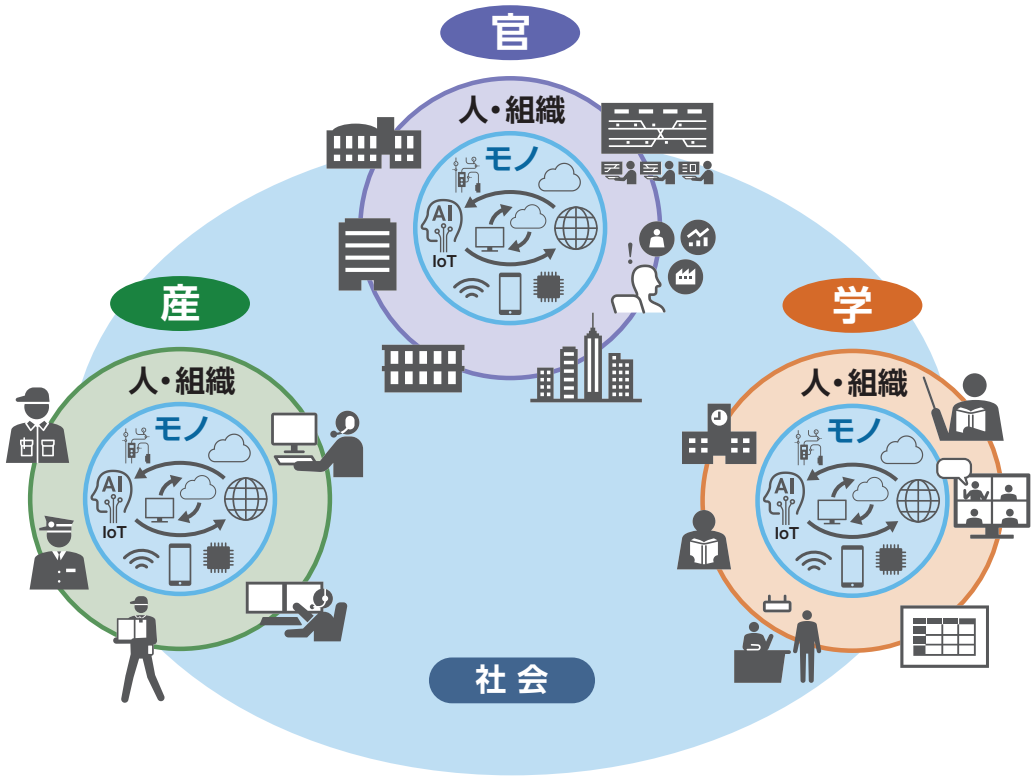
セキュリティにおける有事の際の対応では、IT部門に加えて広報、人事・勤労、法務などのあらゆる部門と連携が必要です。また、セキュリティ対策の対象範囲が拡大している中、モノづくり部門や品質保証部門、調達部門などともしっかりとした連携をしないと、対応はうまく機能しません。日立では、このようなセキュリティエコシステムが重要と考え、その構築を推進しています。

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1-❷参照）

図表1-❷　セキュリティエコシステムのイメージ



日立の情報セキュリティの考え方

■ 自分ゴト化：新たなセキュリティ啓発に向けた取り組み

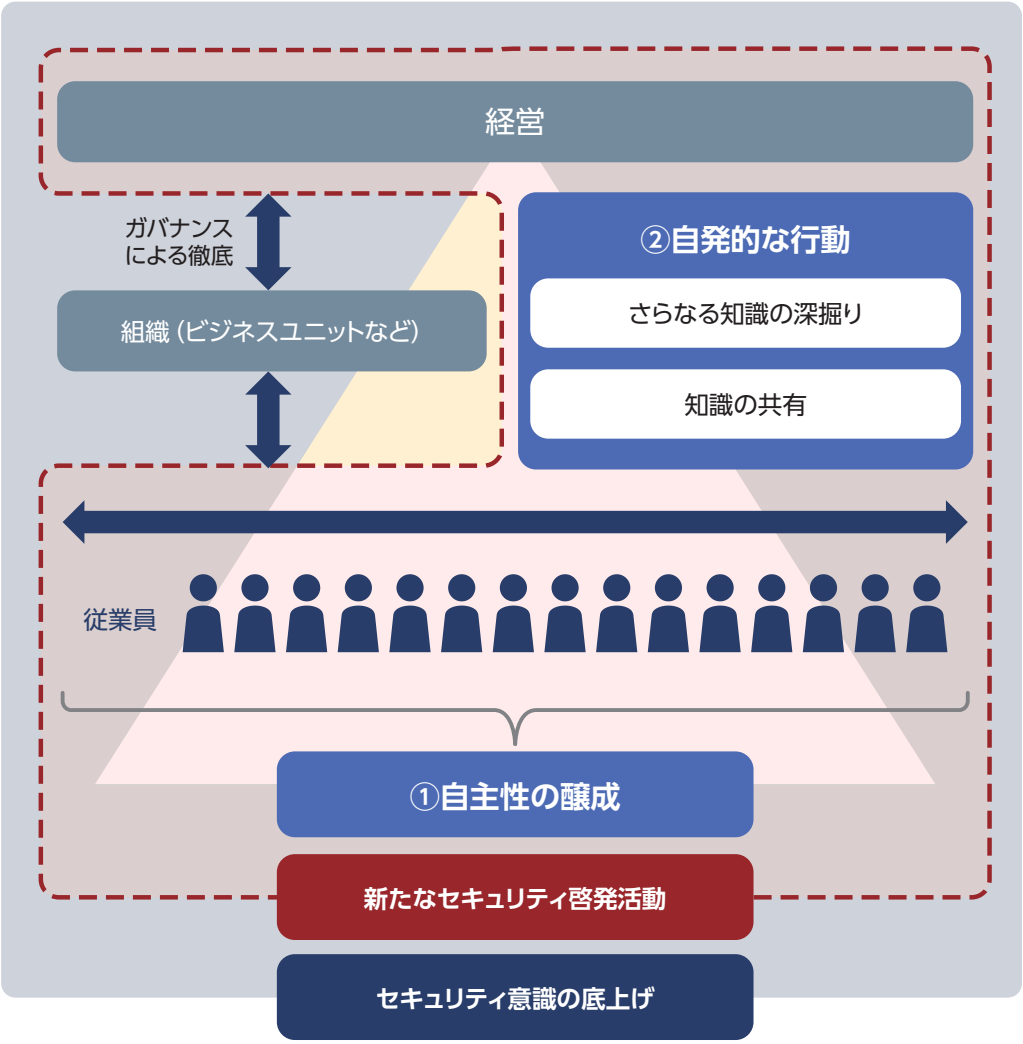
ここ数年で定着したテレワーク中心の働き方においては、「セキュリティ意識のぜい弱性」が狙われることが想定されます。オフィス以外で仕事をすることにより、近くに相談できる相手がいなかったりと、誰しもがリスクと隣り合わせになってきているのが現状です。

そのために、これからは一人一人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1-❸参照）

図表1-❸　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、
従業員一人一人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

一人一人のセキュリティ意識の向上こそが重要
キーワード：「自分ゴト化」、「従業員が心から共感すること」



日立の情報セキュリティ戦略と重点テーマ

日立では、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、データ保護の法規制動向を踏まえ、セキュリティ戦略を立案し、施策を展開しています。

昨今のセキュリティインシデントの特徴としては、アタックサーフェスの拡大と、情報窃取やランサムウェアなどの金銭を目的とした攻撃が活性化し、これらの攻撃で、各社で事業影響が発生していることがあげられます。特にサプライチェーン被害により事業停止が発生する事案が発生しています。また、アタックサーフェスの拡大に関しては、クラウドサービスへの攻撃増加が目立っています。加えて、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、身代金を要求する攻撃が顕著です。

グローバルでのセキュリティ、データ保護の法規制動向については、ヨーロッパの規制強化の動きが顕著になってきています。セキュリティ関連では、喫緊で重要インフラに係る製品サービス提供時に必要となるセキュリティ要件であるNIS2指令に加え、まだ数年は先ですが、さらに規制対象の範囲がひろがるサイバーレジリエンス法、データ保護関連では、EU Date Actの施行が迫っています。また、加えて、データ保護関連では、7割の国で、データ保護法の規定・整備が進み、ベトナム・インドなどアジア地区でも整備が活性化している状況です。

こういった状況を踏まえ、日立では、以下の4点を重点テーマとして取り組んでいます。

1. 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5つの地域に本社直轄の情報セキュリティ担当部門として、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をもつリージョンブランチを設置し、ワールドワイドでのSecurity One Teamによるインシデントへの迅速な対応、そして変化する地域法制への準拠を推進しています。あわせて、現状のデータ保護部隊の強化を行い、グローバルで、本社をヘッドとした一体運営を行っています。

2. 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共に、インテリジェンス情報のグローバルでの活用推進を促進しています。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を推進しています。また、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の再チェックを進めています。

3. 製品・サービス/サプライチェーンセキュリティ加速化

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き仕組み構築を進めています。また、製品・サービスセキュリティに関しては、各BU・会社に設置されたPSIRTをより効果的に機能させるために、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ています。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図っています。

4. データ保護強化

グローバルデータガバナンス強化を進めるとともに、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を進めています。また、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、施行が決定したEU Date ACTに関して、各種対応を進めています。

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の情報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・規範の遵守

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遵守する。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。

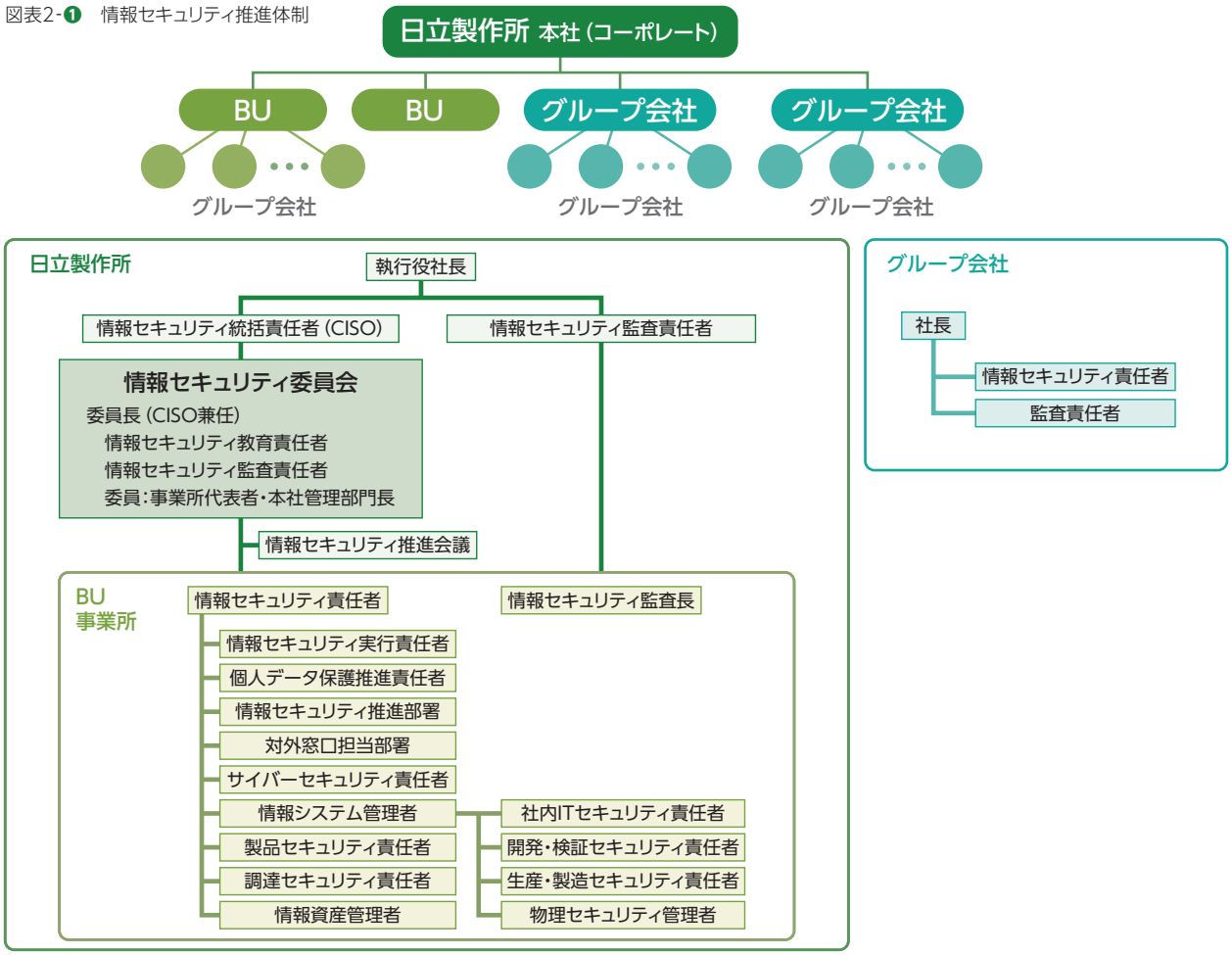
BU・事業所では、原則BU長・事業所長が情報セキュリティ責任者を務めます。情報セキュリティ責任者は、推進をサポートする情報セキュリティ実行責任者、個人データ保護推進責任者を任命し、個人情報保護および情報セキュリティを管理、統括します。加えて、サイバー攻撃の対象範囲が拡大していることから、情報システム管理者のもとに、社内IT環境、開発・検証環境、生産・製造環境、オフィスの入退室などの物理セキュリティ環境における各責任者を設置しています。さらに、お客さまに提供する製品・サービス、取引先などのサプライチェーンのセキュリティを強化するため、製品セキュリティ責任者、調達セキュリティ責任者も設置しています。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2-❶参照)

2022年度から米州、欧州、アジア、インド、中国の地域統括会社に個人データ保護に関する現地グループ会社サポート機能を設置し、個人データ保護コンプライアンスの確保に努めています。

また、2023年度には、米州、欧州、アジア、インド、中国に本社直轄の情報セキュリティ担当部門である「リージョンブランチ」を新設することで、各地域のグループ会社へのサポートを行い、グローバルでのマネジメントの強化に努めました。

図表2-❶　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2-❷参照)

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、OECDプライバシーガイドラインを参照し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一人の意識の向上を図ります。

図表2-❷　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

図表2-❸　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2-❸参照)

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」に基づいて評価し、次年度以降の施策の立案を行っています。

情報資産管理の取り組み

さまざまな脅威から狙われている情報資産が漏えいしたり使用不能になったりしないよう、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無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他、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、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。

情報セキュリティマネジメント

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2-❹参照)

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、日立本社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。

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。2023年度の日立製作所における受講率は、100% (休職者など受講不可能な者を除く) に達しています。その他にも、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2-❺参照)

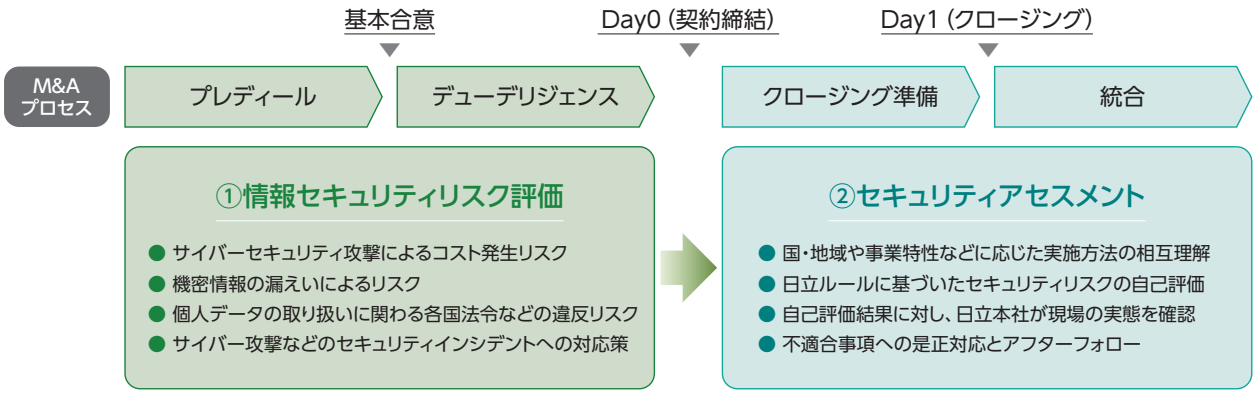
日立製作所の教育コンテンツは国内外のグループ会社にも公開しており、日立グループ全体として情報セキュリティ・個人情報保護教育に積極的に取り組んでいます。

■ 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2-❹ 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



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。

■ 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。

図表2-❺　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

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2-❻参照)

- 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

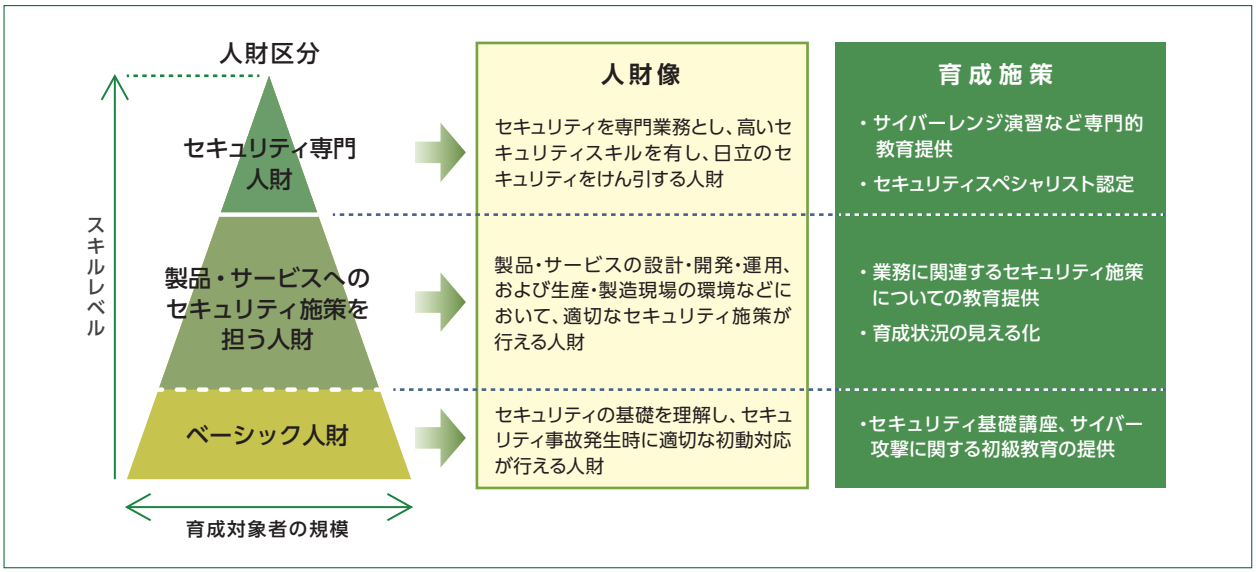
各人財区分ごとの育成プログラム

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、認定しています。

図表2-❻ 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・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、リモートワークによる就業環境に対応し、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。

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、情報セキュリティへの取り組みが、さらに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担当部門（リージョンブランチ）を新設し、グローバルガバナンス強化に取り組んでいます。

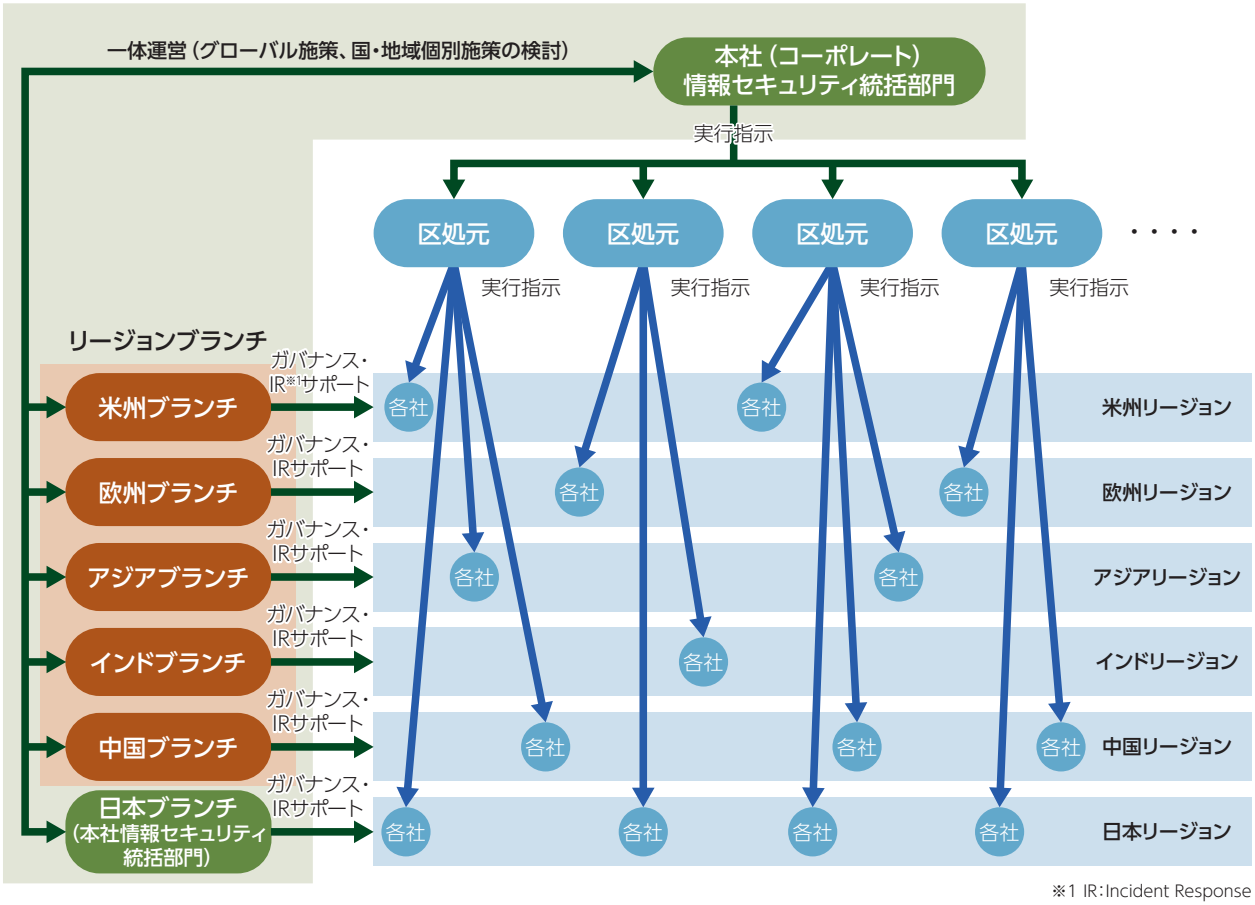
リージョンブランチによるガバナンス強化活動

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。

Security One Teamによるインシデントへの迅速な対応、変化する地域法制への準拠を目的に、23年度より、米州、欧州、アジア、インド、中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区処元BU・会社から各グループ会社への縦軸ラインに加え、ブランチより各地域現地法人へ横軸ライン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。尚、日本においては、本社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きます。

各地域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

図表2-❼　リージョンブランチによるガバナンス強化体制



※1 IR：Incident Response

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2-❼)

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着実な基本施策の実行を促進しています。(図表2-❽参照)

図表2-❽　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。

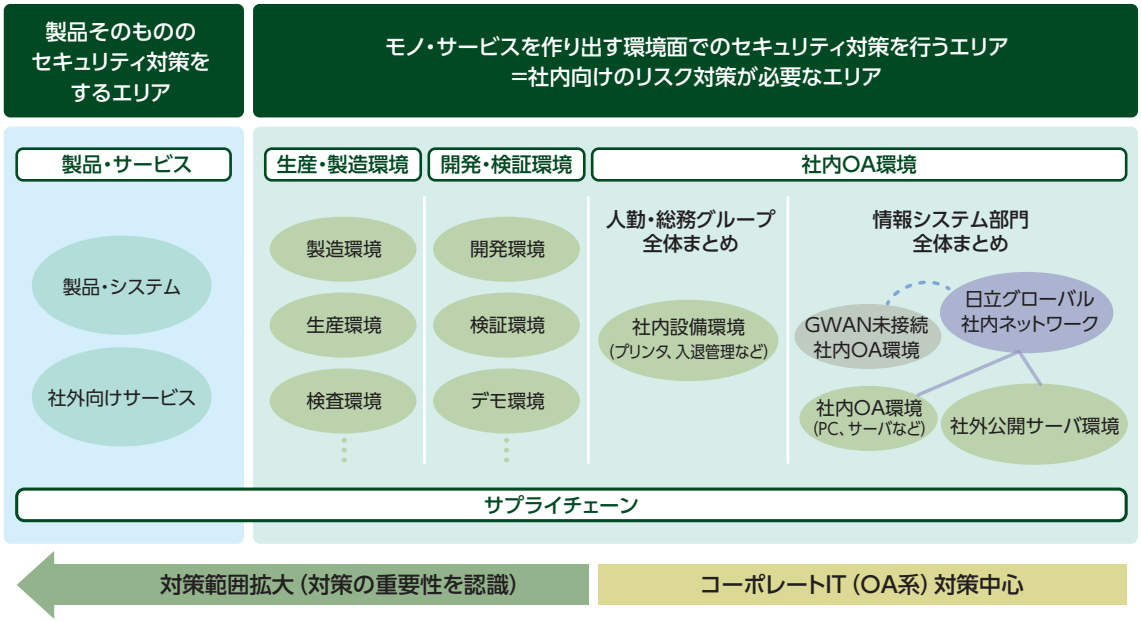
サイバーセキュリティ対策の強化施策

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2-❾参照)

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2-❿参照)

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、開発・検証環境、生産・製造環境、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、本社がこの自己点検結果をモニタリング、最後に第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2-❾　サイバーセキュリティ対策範囲の拡大



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。

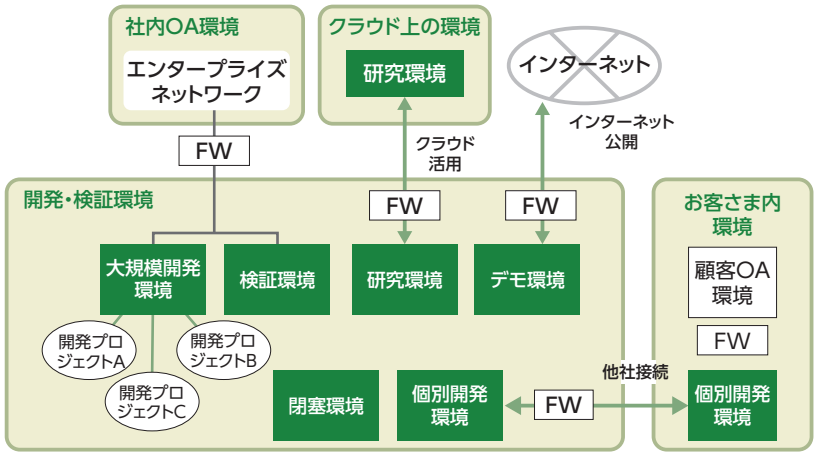
■ 開発・検証環境におけるセキュリティ強化

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2-⓫参照)

図表2-⓾　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	環境面	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		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

図表2-⓫　開発・検証環境のセキュリティネットワーク



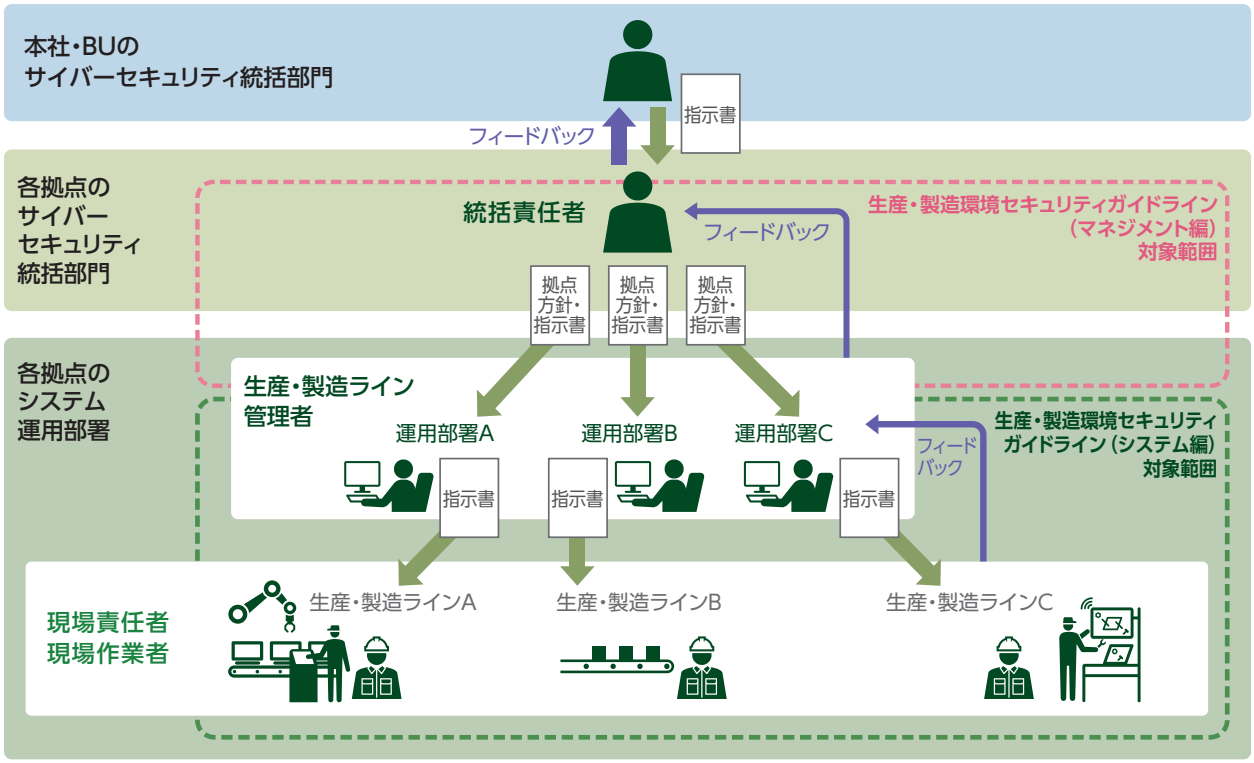
サイバーセキュリティの取り組み

■ 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2-⑫参照）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

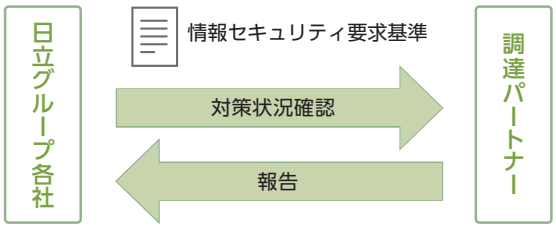


ガイドライン構成	内　容	対象者
マネジメント編	マネジメント面（組織・人的管理面としての取り組み）として、組織体制の整備および、拠点全体・部署個別のセキュリティ運用・管理上ルールの策定と見直しについて記載。	サイバーセキュリティ統括責任者
システム編	「IEC62443-3-3」に基づき、現状把握と対策検討としてシステム構成およびその対策方法は、日立グループの代表的なモデルを用いて記載し、各部門・各部署でカスタマイズして利用する。	生産・製造ライン管理者
		現場責任者
		現場作業者

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だく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2-⓮)

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。

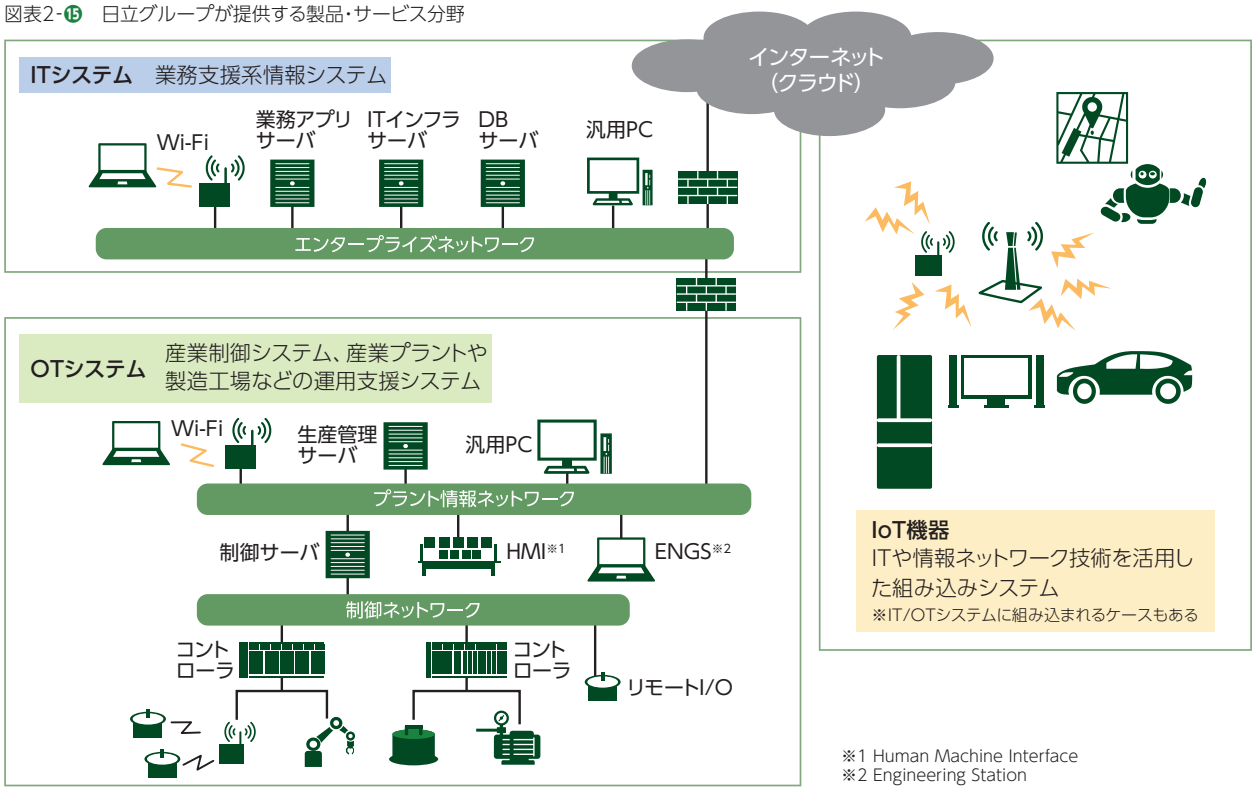


図表2-⓮　サプライチェーンにおけるセキュリティ強化体制

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2-⓯参照)

図表2-⓯　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

サイバーセキュリティの取り組み

■ 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2-⑯参照)

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、本社(コーポレート)とBU・グループ会社にPSIRT(Product Security 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

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2-⑰ 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		

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、本社（コーポレート）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。

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

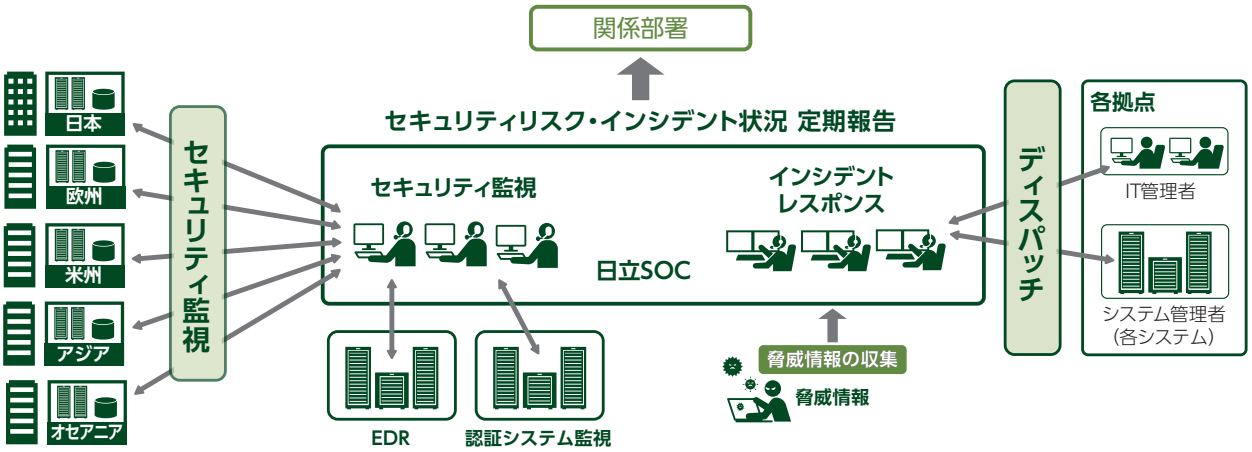
標的型攻撃やランサムウェア、二重脅迫の脅威など、複雑かつ巧妙なサイバー攻撃により、個々の企業や組織にとどまらず、サプライチェーン全体のセキュリティリスクが増大しています。このようなサイバー攻撃に対峙するためには、その脅威をいち早く発見し、被害拡大を防止することが重要です。日立グループでは、マルウェア感染や不正アクセスなどの脅威を早期に検知し、インシデント発生時の初動から対策までを迅速に対応し、サイバー攻撃に対する被害を最小限に抑えるための24時間365日体制の日立セキュリティオペレーションセンター（日立SOC）を2017年10月より設置し、セキュリティ監視・インシデントレスポンス強化を図っています。また欧州、米州地区との連携を強化することでグローバルでの対応力強化を進めています。

■ サイバーセキュリティ監視

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。

また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あります。正規の認証情報が利用され検知が困難なため、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を行っています。これらの施策により在宅勤務などの新たな働き方における新たな脅威にも対応しています。

図表2-⓲　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



■ 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、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。

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)

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の発令を検討するとともに、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。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整理し、本社のセキュリティ統括部門やCISO、リージョンブランチの統括部門と連携し、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。

サイバーセキュリティの取り組み

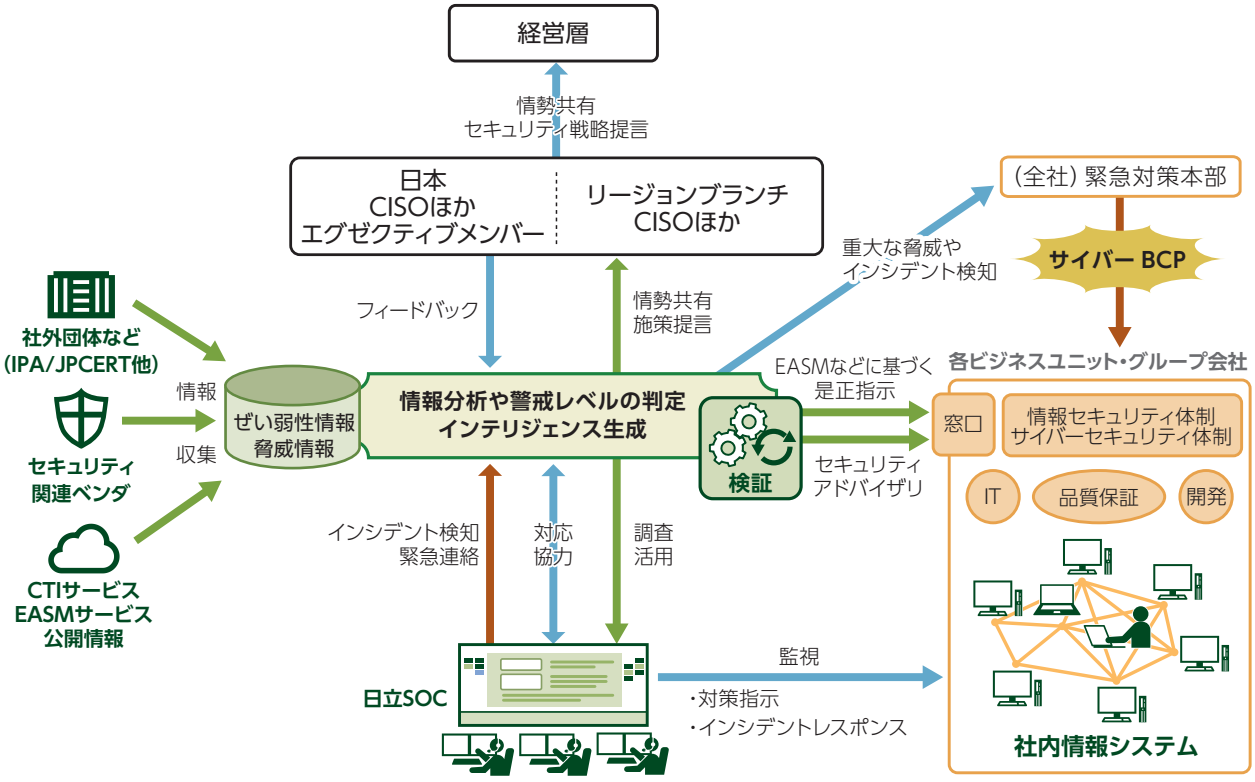
■ 外部からの攻撃への対処

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。それらを構成するソフトウェア、ハードウェアは毎日のようにぜい弱性が発見され公開されています。攻撃者はこのようなぜい弱性を利用して不正アクセス、ランサムウェアなどのマルウェア感染、機密情報の窃盗を試みます。これらに対応するために、アタックサーフェス管理（EASM）を行い、被害を受ける可能性のある場合は該当部署へ個別に是正指示を行うことで、外部からの攻撃リスクの低減と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）

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



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。

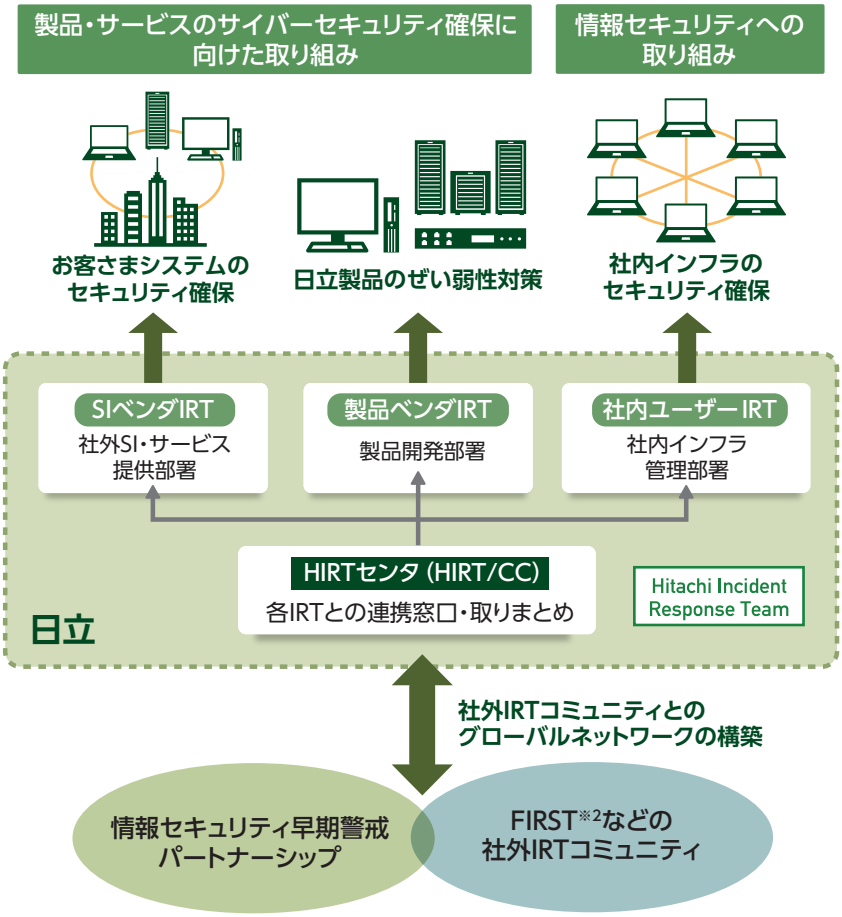
HIRTは、ぜい弱性対策とインシデント対応とを推進するために、下記のように、4つのIRT (Incident Response Team) という活動モデルを採用しています。4つのIRTとは、

(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 (社内ユーザー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2-⑳参照)

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4つのIRT



分　類	役　割
HIRT/CC※1	該当部署：HIRT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

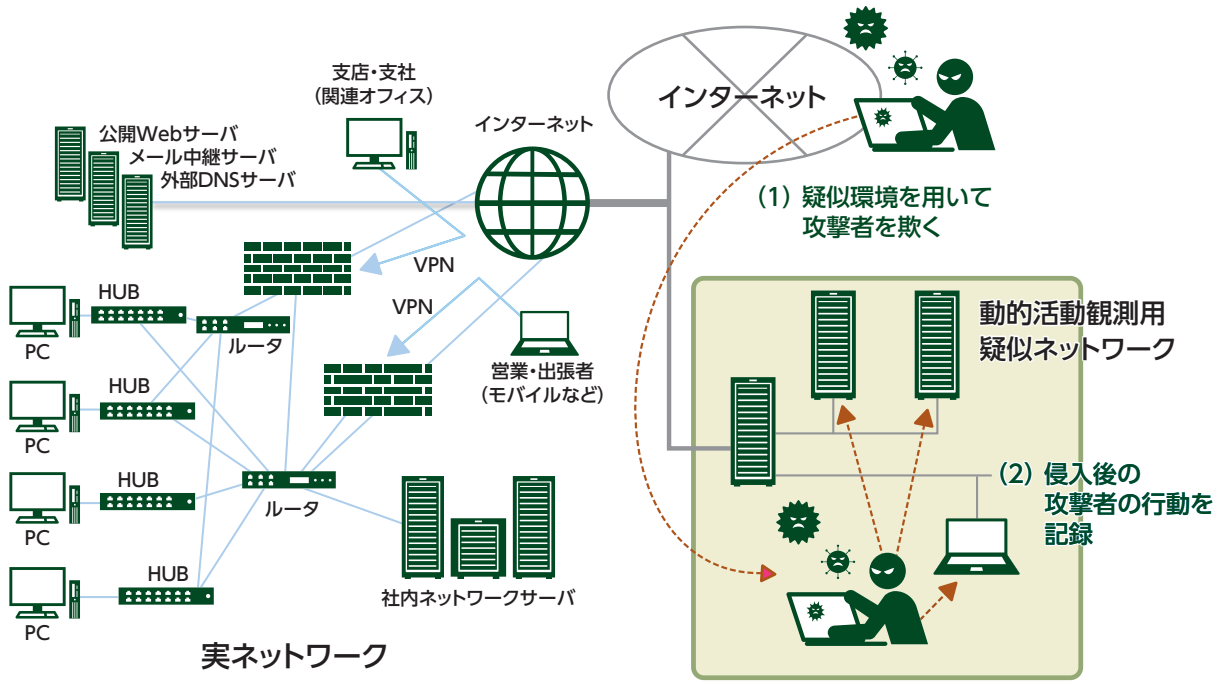
「次の脅威のキャッチアップ」と早期に対策展開を図るための技術として「動的活動観測」に取り組んでいます。動的活動観測は、標的型攻撃などのサイバー攻撃を調査するために構築した組織内ネットワークの疑似環境下で、侵入後の攻撃者の行動を記録し分析する観測手法です。(図表2-㉑参照)

(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2-㉑ 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/

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2-㉒参照)

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、社内規程が法令、プライバシーマーク準拠規格であるJIS Q 15001に適合しているかを確認、評価する仕組みを整備しています。このような規程の整備とともに、実際に個人情報を取り扱うにあたり、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2-㉓参照)

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。

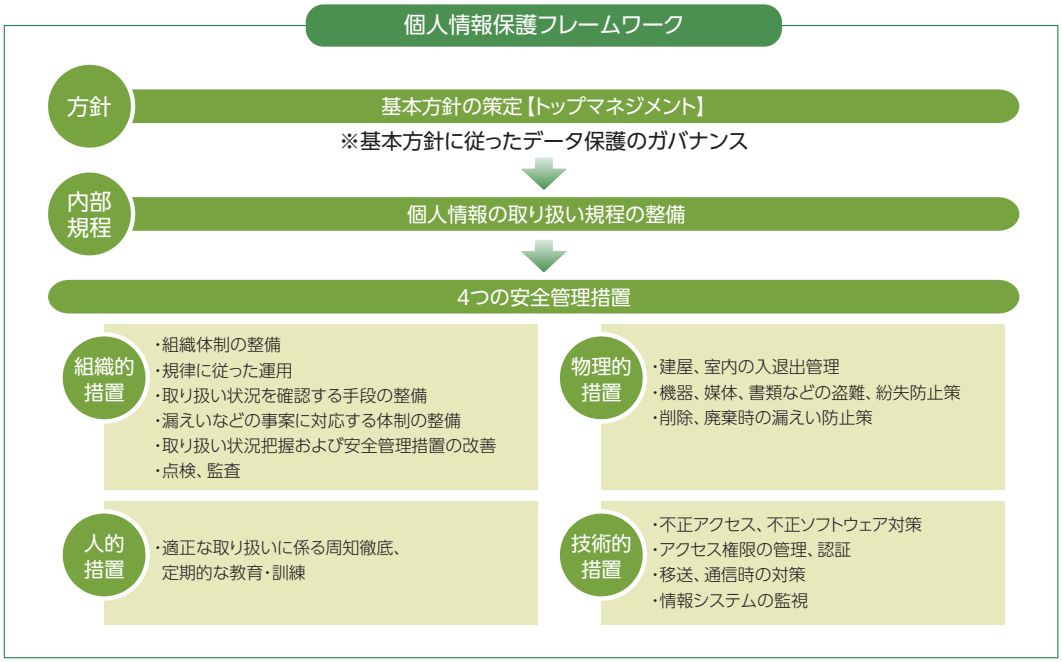
（4）法令・規範の遵守

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2-㉓　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2-㉔参照)

■ 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。

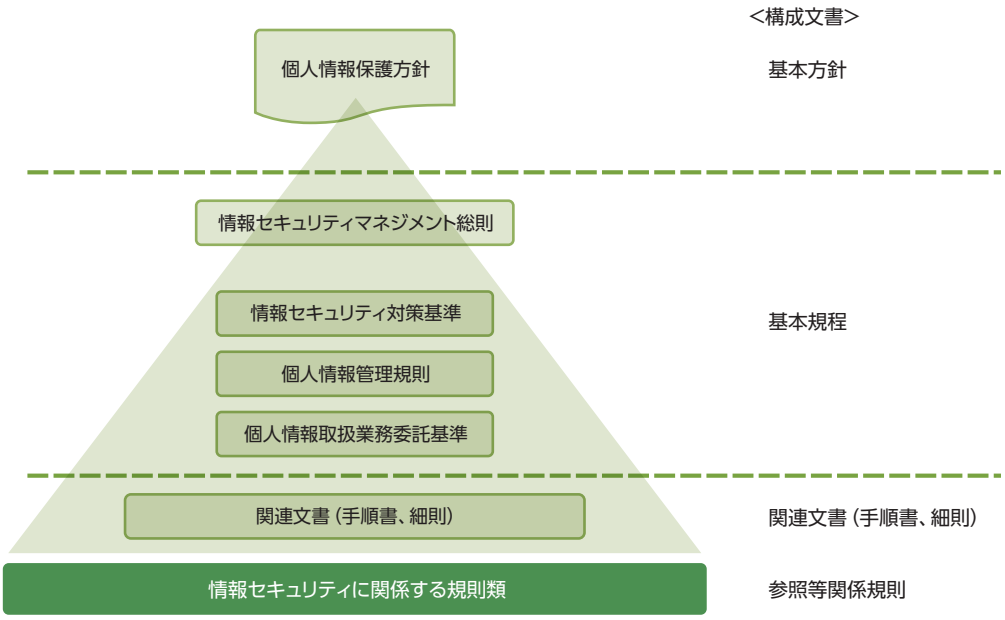
技術的安全管理措置では、情報システムに対する不正アクセス、不正ソフトウェア対策の実施などを行っています。また、取り扱う個人情報の重要度に応じてアクセス権限の管理、認証、移送、通信時の対策、情報システムの監視などを行っています。

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 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

図表2-㉔　個人情報保護規則体系



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。(図表2-㉕参照)

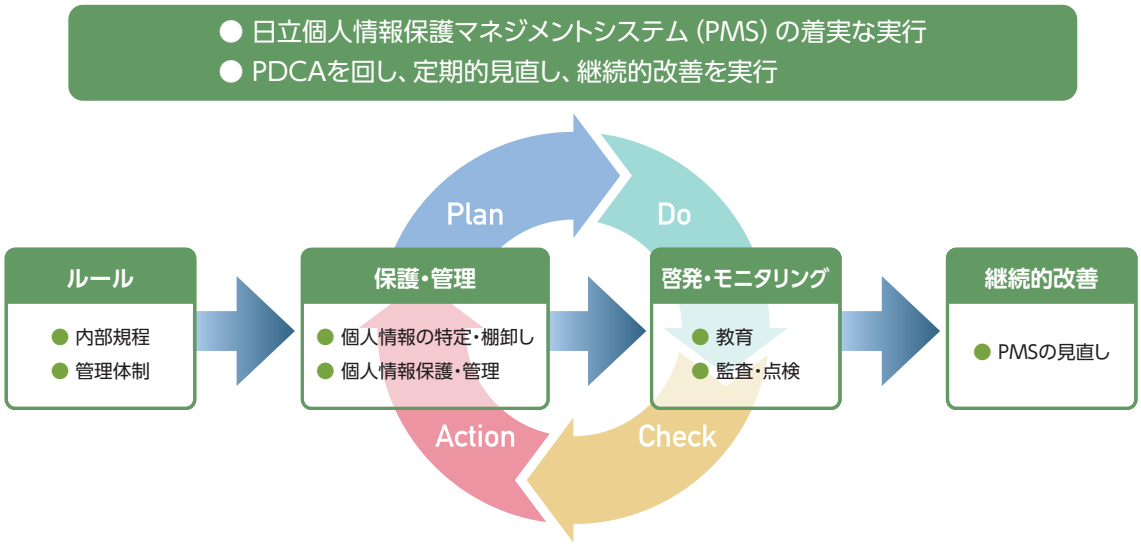
個人情報の管理と適切な取り扱い

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) 相当の社内規程を制定し、規則にのっとり、厳格な管理と適切な取り扱いに努めています。職場ごとに個人情報管理の責任者 (情報資産管理者) を置き、業務で取り扱う「すべての個人情報」を特定し、当該個人情報の重要性およびリスクに応じて管理し、適切な措置を講じています。

個人情報の取り扱い業務ごとにリスクの認識、分析実施し、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



データプロテクションの取り組み

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を有する部門については「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。

■ 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。

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、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機能を設置し、各国での法令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、2024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、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（2024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
株式会社 日立インフォメーションエンジニアリング
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

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。

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。(図表2-㉕参照)

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。

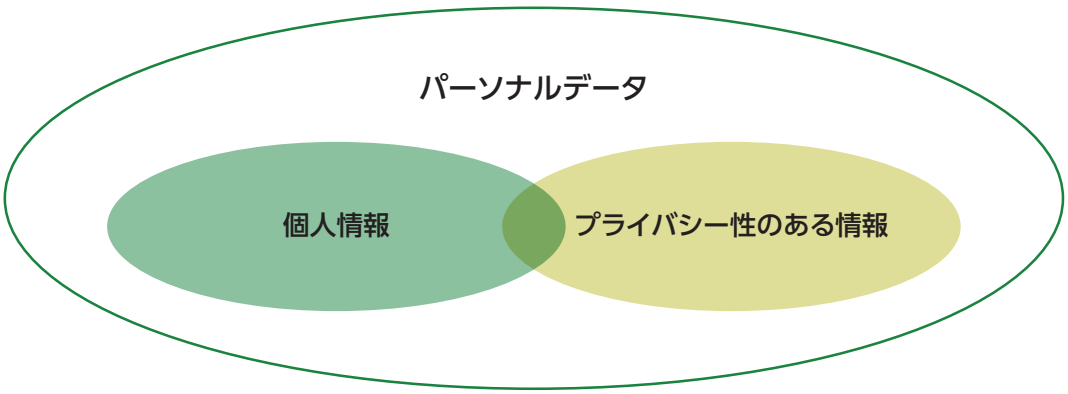
日立のプライバシー保護の取り組み

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。

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、2023年から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することで、プライバシー保護施策に取り組んでいます。

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。

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



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。

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としています。また日本においては、パネルディスカッションやワークショップを通じてセキュリティの専門的な知識を学ぶ機会の提供や、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。2024年10月現在で、111か国、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
- 一般財団法人日本データ通信協会、テレコム・アイザック推進会議
- 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「ヒト」の3要素でバランスを取る必要があります。

昨今の社員の働き方の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。

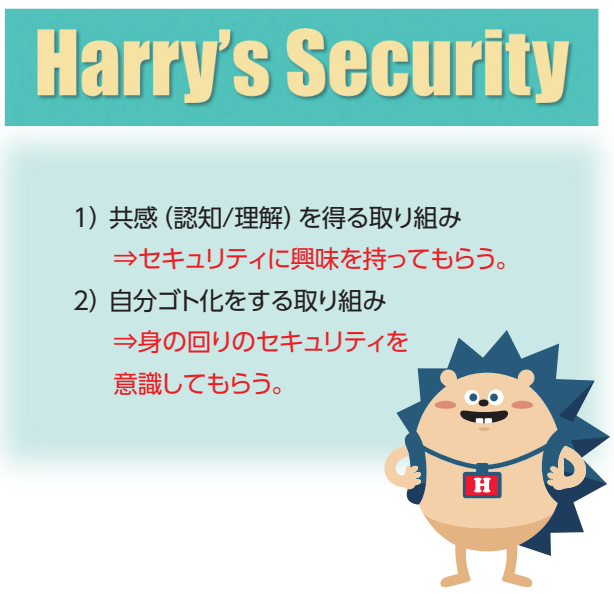
自主性の醸成に向けた活動：Harry's Security

「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3-❶参照)

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。

図表3-❶ 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3-❷参照)

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Micosoft Teams※1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。

※1 Micosoft 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3-❷ GREEN AEGISの活動

トピックス

社員参加型で危険予知トレーニング（KYT）教材を作成

2023年から、セキュリティのキャラクターである「Harry」が登場する危険予知トレーニング（KYT）の教材の作成に着手しました。KYTとは、ある状況において、どのような危険があるかを考えるためのトレーニングです。その作成プロセスにおいては、社員に参加してもらいながら進めてきました。どのようなシーンにどのような危険が潜んでいるかを、社員からアイデアを募集しました。そのアイデアをもとに作成したテーマ候補から、最終的に、社員からの投票によって、「メールの誤送信」「公共の場での会話」をテーマに定め、作成しました。できあがった教材は、イントラネットでの公開や、情報セキュリティ e-ラーニングにも取り込んで、広く活用してもらえるように展開しています。社員が作成に参加することで、セキュリティについて普段から考えてもらう機会を提供し、併せて、できあがった教材を身近に感じてもらうことをめざしています。

コラム
COLUMN

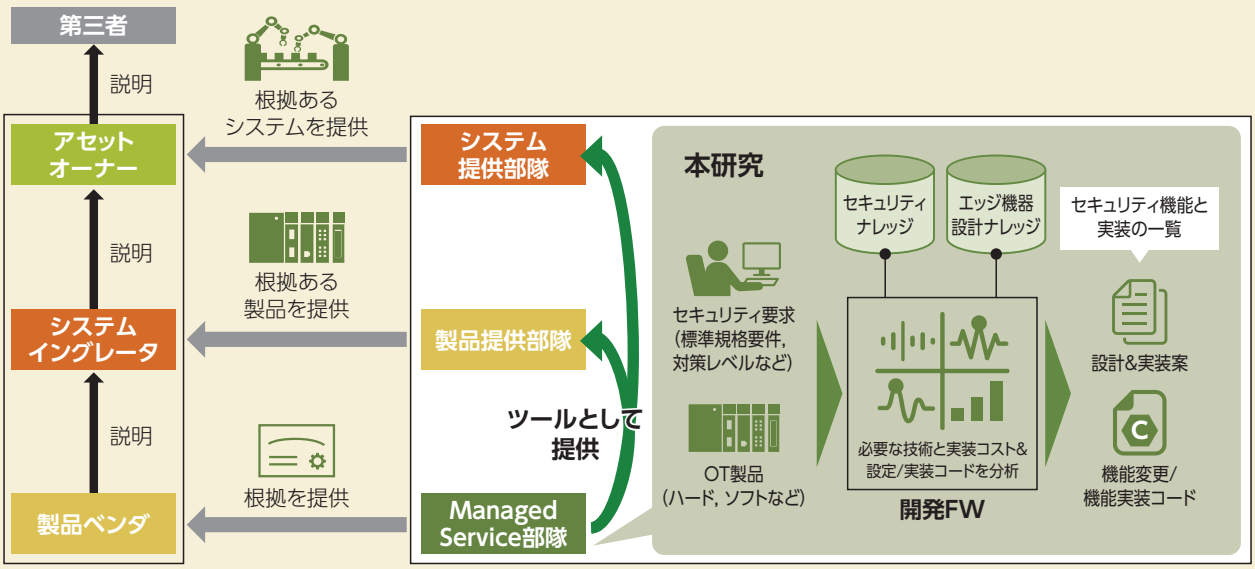
目前に迫る セキュリティ法規制対応に向けた技術開発

近年、欧州Cyber Resilience Actをはじめとしたセキュリティ対応の法規制化がグローバルで進んでいます。事業者は、法規制に対応できなければ市場から排除されることになります。そのため、適切な対応を効率良く行うことが重要となってきます。日立では、セキュリティ法規制要件に説明可能な形で対応するための技術や、運用フェーズ、サプライチェーンのセキュリティ対応を効率化する技術を開発しています。

アカウンタブルセキュリティ技術

IIoT (Industrial Internet of Things) へのサイバー攻撃の脅威が顕在化しています。これに伴い、IoT製品を取り扱う企業はセキュリティ法規への準拠とシステム、装置の性能などを両立した妥当な対策の実施と、それらの対外的な説明が求められます。対策が説明可能 (アカウンタブル) であるためには、「システムを構成する装置へ実装する対策の妥当性」が重要となります。図に示すようにアセットオーナーは、自身の資産のセキュリティが担保されていることを第三者に対し説明するために、システムインテグレータの提供するシステムのセキュリティが担保されていることを説明できなければなりません。システムインテグレータや装置ベンダも同様です。すなわち、装置ベンダの提供する装置のセキュリティが説明可能であることが、“アカウンタブル” であることの起点であり、システムインテグレータやアセットオーナーにとっての説明性の担保にもつながります。日立は「OTシステム、装置に必要なセキュリティ機能や要件が説明可能であること」を “アカウンタビリティ” と定義し、装置に対する具体的な設計案や実装案を提示することでそれらの説明性を担保することをめざしています。具体的には、セキュリティ法規の要求事項を、システム、装置の性能などを制約として捉えた「制約充足問題」として解くことで、考慮すべき条件をすべて満たした上で、妥当性があり、かつ装置へ実装可能なセキュアな対策を導出します。対策の導出工数を評価するため、OSSを活用したプロトタイプを作成し、対策の妥当性を第三者へ説明する工数を1/20以上削減できることを確認しました。(図表4-❶参照)

図表4-❶　アカウンタブルセキュリティ技術の概要



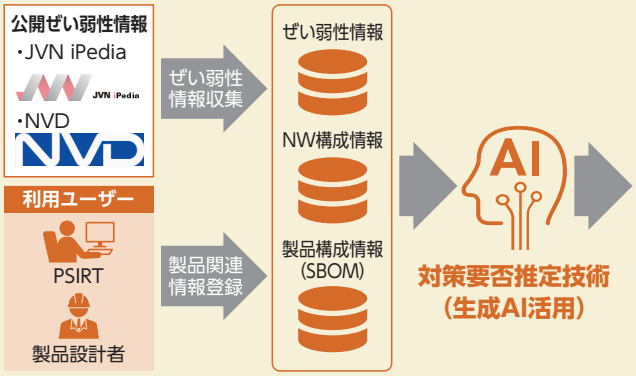
運用フェーズのぜい弱性管理とSBOM活用

運用フェーズのプロダクトセキュリティを守るため、各企業においてPSIRT組織（Product Security Incident Response Teams）の設立が進んできています。PSIRTにおけるぜい弱性ハンドリング業務は、ぜい弱性情報を日々収集し、自社製品やサービスに関わる可能性が高くなおかつ危険性も高いと見込まれるぜい弱性を選別します。選別されたぜい弱性は詳細に分析され、そのぜい弱性の悪用による自社製品やサービスへの攻撃可否に基づき対策の要否が決定されます。

昨今のOSSの利用増加や発見されるぜい弱性の増加にともない、PSIRTにおけるぜい弱性ハンドリングの工数は増大していますが、専門家の数は限られており、業務遂行が困難になりつつあります。これまでにも分析すべきぜい弱性の絞り込みにつながる技術を開発してきましたが、一方で、絞り込んだ後の各ぜい弱性の対策要否に関わる詳細分析には依然として多大な工数を要することが課題でした。

これに対して日立は、ぜい弱性の説明文から悪用に必要な条件を抽出し、製品構成情報（SBOM、NW構成情報など）と突き合せることで条件の該否判定結果および調査観点を提示する技術を開発しました。この提案手法によって、既存技術のみの場合に比べてぜい弱性ハンドリング業務の工数を最大4割程度まで削減できる見込みを得ました。（図表4-❷参照）

図表4-❷　ぜい弱性対策要否推定技術の概要



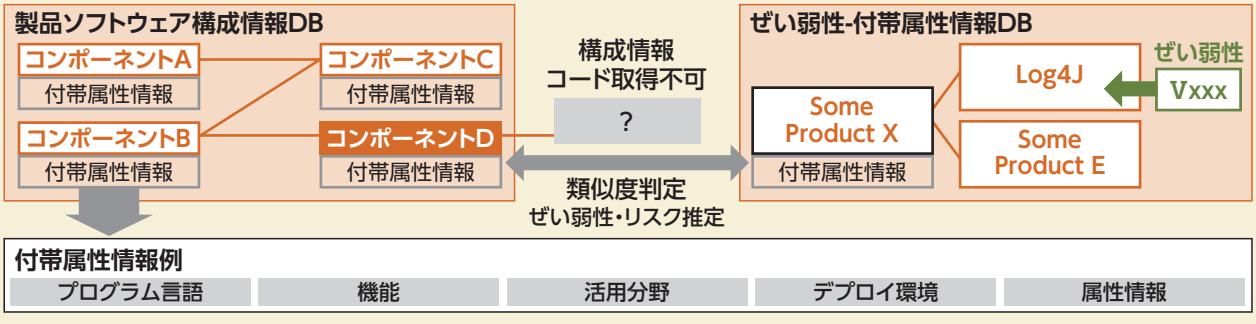
優先順	観点	攻撃到達条件	根拠／サジェスト	該否
1	Software	zlib	SBOM(xxx.spdx.json)に該当ソフトが存在します	該当
2	Version	1.2.12	SBOM(xxx.spdx.json)に該当ソフトが存在します	該当
3-1	Function	inflateGet Header	該当関数を呼び出す機能は存在しません	非該当
3-2	Source file	inflate.c	該当するソースファイルは存在しません	非該当
4	NW path existence	-	装置Aから対象装置CへのNWパスが存在します	該当
…	…	…	…	未確認

・対策要否判断において作業者がチェックすべき観点を、ぜい弱性情報から網羅的に自動抽出
・抽出したチェック項目の観点ごとに「確認工数の低さ」や「顧客への説得力」に基づき優先度付けし、作業優先度を提示

ソフトウェアサプライチェーンのセキュリティ

近年のソフトウェアは、OSSや商用ソフトウェアが数多く組み込まれ、難読化や開示情報の制約がある構成要素が含まれます。ソースコードや、ソフトウェア構成情報が取得できない構成要素については、ぜい弱性や、リスク発現の判定が困難であり、ソフトウェアサプライチェーンにおけるセキュリティ対策の課題となっています。ソフトウェア構成情報が不完全である場合にも有効に不正機能を検証する手法として、ソフトウェアの構成要素の、プログラム言語、デプロイ環境、ソフトウェアの活用ドメイン情報などといった付帯属性をデータベース化し、既にリスク情報が判明している他のソフトウェアの付帯データとの類似度によって、対象が内包するぜい弱性と、リスクを推定する技術を開発しています。この技術により、サプライチェーンを跨いだソフトウェアのセキュリティリスク低減に貢献します。
（図表4-❸参照）

図表4-❸　ソフトウェアの類似度に基づくぜい弱性リスク推定技術の概要



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（2024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（クラウドサービスプラットフォームビジネスユニット・マネージドサービス事業部・デジタルプラットフォーム事業部 デジタルエンジニアリングビジネスユニット・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・Data & Design・Business Development）
- 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 バリューチェーンTSS事業開発本部 DX推進部、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）
- 日立チャネルソリューションズ株式会社
- 株式会社 日立社会情報サービス
- 日本スペースイメージング株式会社
- 株式会社 日立情報通信エンジニアリング（マネージドサービス部）
- 株式会社 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（金融DX事業部第二本部 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 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 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
- 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（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(2024年9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5-❶参照)

図表5-❶ 「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（2024年9月末時点でCMVPによる“historical list”への掲載を含みます）。（図表5-❷参照）

図表5-❷　「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

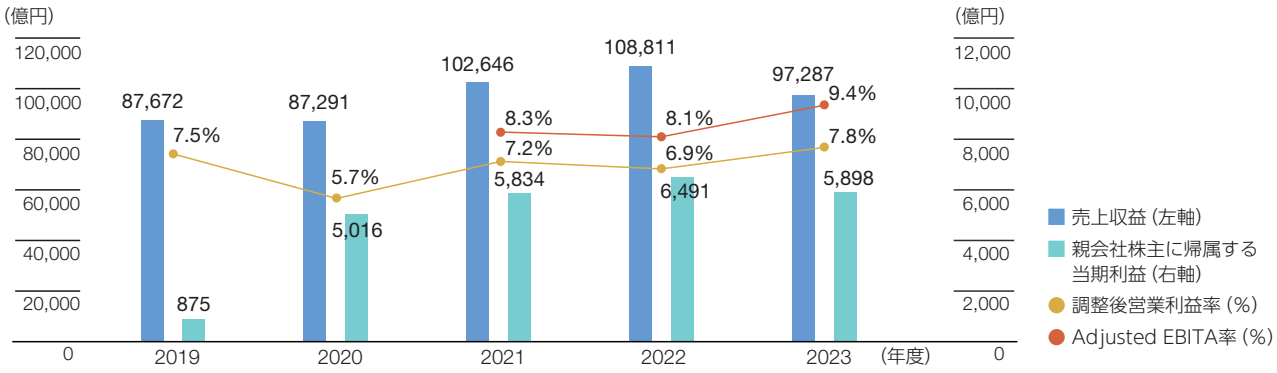
会社概要 (2024年3月31日時点)

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 小島 啓二
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**	463,417百万円
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**	26万8,655人 (国内11万3,737人、 海外15万4,918人)

業績ハイライト (2024年3月期連結IFRS)

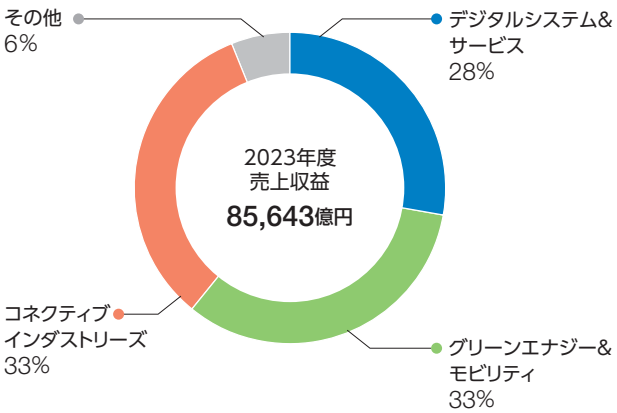
当社の連結財務諸表は、国際財務報告基準 (IFRS) に基づいて作成しています

売上収益	9兆7,287億円	(前期比89%)			
当期利益 (親会社株主帰属)	5,898億円	(前期比593億円減)	**調整後営業利益率**	7.8%	(前期比0.9ポイント増)
Adjusted EBITA※1	9,181億円	(前期比335億円増)	**Adjusted EBITA率**	9.4%	(前期比1.3ポイント増)

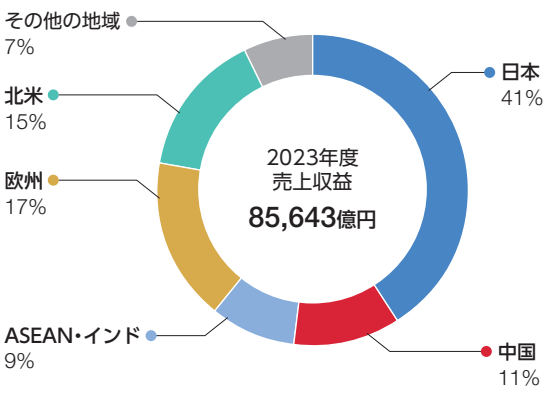


※1 Adjusted EBITA (Adjusted Earnings before interest, taxes and amortization):調整後営業利益に、企業結合により認識した無形資産等の償却費を足し戻した上で、持分法による投資損益を加算して算出

■ 日立グループの事業構成※2



■ 地域別売上収益/構成比※2



※2 「日立グループの事業構成」「地域別売上収益/構成比」の業績は、日立金属、日立建機および日立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

Printed in Japan (H) (2024.11)