HITACHI
Inspire the Next

情報セキュリティ報告書 2022

Information Security Report 2022

日立グループ

INDEX

〈本報告書の概要〉

●報告範囲・時期：2021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：2022年10月発行

いかにしなやかに、いかに迅速に対応していくか “One Hitachi”で情報セキュリティに取り組む

ー ここ最近、ランサムウェアによる企業、自治体や病院への攻撃をニュースでもよく見かけます。このような状況をどのように見ていますか。また、対策を講じるうえで、セキュリティに携わる人にとって大事なことは何でしょうか。

この1年でランサムウェアによる攻撃は、ますます高度化・多様化しています。誰もが世界中のどこからでも攻撃される危険にさらされ、企業においては手薄なサプライチェーンが攻撃起点となる事例も増えています。さらに、昨今の緊張した国際情勢も攻撃頻度を加速させていると言えるでしょう。

対策を講じるにあたり、情報セキュリティも、国際情勢やその歴史的背景など全体の中で捉えることが重要です。なぜ日本がサイバー攻撃されるのか、なぜ日立が標的とされるのか。日立という会社が、単なる一企業のビジネスを超えた、社会的に重要な役割を担っている会社であることを認識したうえで、攻撃の実態を把握し、対処することが必要になってくると思います。

先日も、日本を代表するメーカーのサプライヤーでサイバー攻撃によるシステム障害が発生し、国内の全工場が稼働停止を強いられる事例がありました。日々高度な対策を行っているにもかかわらず、深刻な状況を招いた原因は何だったのか。我々にも起こりうることだという認識を持ったうえで、セキュリティのあり方を考えていく必要があります。

ー製品やサービスのぜい弱性を狙った攻撃は、Lumada事業を推進していくうえでどのような影響がありますか。

世の中で起きているような製品・サービスをターゲットとした攻撃は、Lumada事業によるデータ利活用や協創型ビジネスを一層拡大・推進していくうえで、今後さらにさまざまなケースにおいて遭遇することが考えられます。お客さまごとに、売り切りのビジネスもあれば、ソリューションを提供し続けるサービスもあると思いますが、各事業の特性ごとに、日立がどこまで責任を持つべきか、しっかりとした仕組みを構築していかなければなりません。一定のぜい弱性が見つかった場合は、お客さまに連絡を取り対処していただく、もしくは対処させていただくということは、既に実行しています。日立がお客さまに提供したソリューション

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。

いかにしなやかに、いかに迅速に対応していくか “One Hitachi”で情報セキュリティに取り組む

やソフトウェアに関して、情報セキュリティをどのような形で維持していくのか、社会的責任の観点からも、企業として大きな課題を提示されていると認識しています。

ー 情報漏えいはサイバー攻撃でなく、人的な側面でのリスクもあると思いますが、どのような対応が必要でしょうか。

人的なリスクについては、故意によるものと過失によるミスの2つがあります。故意のリスクは、徹底的に倫理教育を施すことで、個々人の意識を高めていただくしかありません。過失によるミスについては、人間はミスを起こすものですから、そのミスが極力起こらないようにするための仕組みを会社として提供することが責務だと考えます。セキュリティPCの支給や、安全なネット環境の構築など、従業員が安心安全に業務を行えるように整備することが会社としての役割です。

加えて、日本の企業には恥の文化が根づいていますが、セキュリティに関しては恥ではありません。もし自分のPCが原因になるようなことがあれば、すぐ申告できるようなオープンな風土を築くことが被害の拡大防止につながります。

ー さまざまな要因で情報漏えいのリスクが高まる中、欧州のGDPR※1をはじめ、各国がデータ保護規制を強化するグローバルな動きをどう捉えていますか。

サイバー攻撃が企業や社会に与えるインパクトを考えるうえで、コンプライアンスの観点も不可欠になってきます。そして、データが国や地域を超えて連携しあうことを考えると、日立グループ全体として、グローバルでどう対応するかを考えなくてはなりません。例えば、GDPRに関しては、グローバルの各国や地域に日立グループの会社がありますが、各社でGDPRの解釈が異なってしまっては意味がありません。そこで、日立グループとしての統一した解釈を明確にし、共通の対応方針を持ち、そのうえで、地域ごとにスペシャリストチームを配置することで、地域の専門性をもったネイティブスタッフにチェックしてもらいます。すなわち、グローバルで守るべきこと、地域の範囲で守るべきこと、国の範囲で守るべきこと、大きくはこの3つのレイヤーで、各国や地域の法令に対処していけばよいと考えています。

ー こうした広範化・複雑化するサイバー攻撃、データ保護規制の動向を踏まえ、セキュリティマネジメントの根本として大事なことは何でしょうか。

リスクは必ず入ってくる、セキュリティは必ず破られるという前提を持つことが大事です。そして、堅ろう性だけを追求するのではなく、攻撃を受けた時の対処をあらかじめ決めておき、さまざまなリスクに対して柔軟に対応できるセキュリティを敷いておくことです。

大相撲で小兵力士が巨漢力士に多彩な技で立ち向かい、打ち負かすことがありますが、セキュリティマネジメントにも同じことが言えます。大きなリスクに真正面からぶつかっても跳ね飛ばされるだけです。跳ね飛ばされないようにちゃんと考えて、横から行くのか、上から行くのか、下から行くのかというシナリオを持って、まさに「柔よく剛を制す」発想で対応する必要があります。柔軟性のあるセキュリティが、そのしなやかさによって剛強なリスクに打ち勝つのです。さらに、リスクによってさまざまな対処法を練って準備しておくとともに、消防訓練のように日々鍛錬を重ねることによって、とっさの状況判断と対処ができるようになります。消防士の皆さんは、消火活動の現場で起こるさまざまな状況を想定し、繰り返し訓練されることにより、とっさの判断が早くなります。このスピード感も、リスクによるダメージを極小化するうえで、しなやかさとともに重要なポイントとなります。

ー スピードアップのために組織に求められることは何ですか。

特にグローバル体制下では、事故が発生した最初の段階で、いかに迅速に情報共有できるかがポイントです。火事が起きた時に初動対応が重要なように、万が一、世

界の日立グループのどこかで事故が起きても、すぐ連絡が行き届き、グループ全体で共有して、リスクを止める迅速さが必要です。しかし、従来のピラミッド型の組織体系に基づいた情報共有では、ある意味、情報がバケツリレーの状態で、上がりにくく、上がるうちに情報量がどんどん少なくなり、迅速性も落ちていきます。できるだけフラットな体制で、事故の現場から経営陣まで情報を一気通貫させていくことが必要です。そして、もう一つ必要なことは、地域単位での情報共有の横連携の強化です。例えばヨーロッパのある国で事故が起きたら、ヨーロッパの中のグループ会社で迅速に情報共有できるようにすることです。現在、米州、欧州、中国、アジア、インドの各地域の拠点にISE※2を配置していますが、その機能をベースに発展させていければと思います。まだ、道半ばですが、本社起点の”縦軸”と地域の拠点起点の”横軸”による2つの方向で情報共有の迅速化をめざしていきたいと考えています。

ー 日立グループの2024中期経営計画における情報セキュリティの位置づけについて教えてください。

2024中期経営計画では「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社会を支える」ことをめざす姿として新たに掲げています。社内と社外の垣根がなくなりつつある現状を踏まえてセキュリティマネジメントを考えなくてはなりません。製品・サービスのセキュリティをどう強化していくか、サプライチェーン全体のセキュリティをどう向上させていくかなど課題は山積ですが、一つずつ真摯（しんし）に向き合ってまいります。

サイバー攻撃をはじめ、故意や過失による情報漏えいなど、あらゆるリスクが、世界のどこで起こるか分かりません。ですから、基本的には何が起きても対処できるような準備をしっかり行うことと、それをいかに早く検知するか、そして、再び起こさないための分析と対策をそのつど行うことが必要です。かつ、一社だけの対策では十分とは言えませんので、他の会社と横連携することも大事です。

こうした情報セキュリティのリスクは、目に見えないところが厄介です。サプライチェーンも含めて全く同レベルのセキュリティを実行していくことは、難しい一面もありますが、パッチをきちんとあてる、多要素認証にする、パスワードを定期的に変える、生体認証を取り込むなど、社外のパートナーに対して、日立としてお願いすべきことは発信し続ける必要があります。

ー 今後の日立グループのセキュリティ戦略の方向性と決意をお聞かせください。

日立グループは数多くの会社が集まって構成される企業グループですが、今後は“One Hitachi”のもと、一つの会社として事業を推進してまいります。この事業方針と呼応して、情報セキュリティに関しても、“One Hitachi”として取り組むことがいちばん大事なことだと思います。各社でバラバラに行うのではなく、日立全体の方針にのっとり、共通の施策に基づいて、共有化と迅速性を十分に検証しながら、最適なセキュリティ構築を加速化させていきたいと考えています。

※1 GDPR：General Data Protection Regulation（一般データ保護規則）
※2 ISE：Information Security Expert

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順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、昨今のコロナ禍において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1-❶参照)

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

日立グループでは、世の中の潮流や高度化・複合化しているサイバー攻撃への対応として、セキュリティ対策を継続的に、かつ、着実に実行していきます。その中で、IT基盤の対策として、ITプラットフォームのクラウド化に伴う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、業務システムのクラウド化の活性化や働き方改革の動向を踏まえ、今後のアーキテクチャーの主流であるクラウドをベースとし、今までの境界型も併せたハイブリッドな構成での最適なセキュリティをめざしています。これらのクラウドベースITアーキテクチャーを基準とするゼロトラストセキュリティを実現する上で、重要な要素となる、「認証」「エンドポイント」「サイバー統合監視」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。

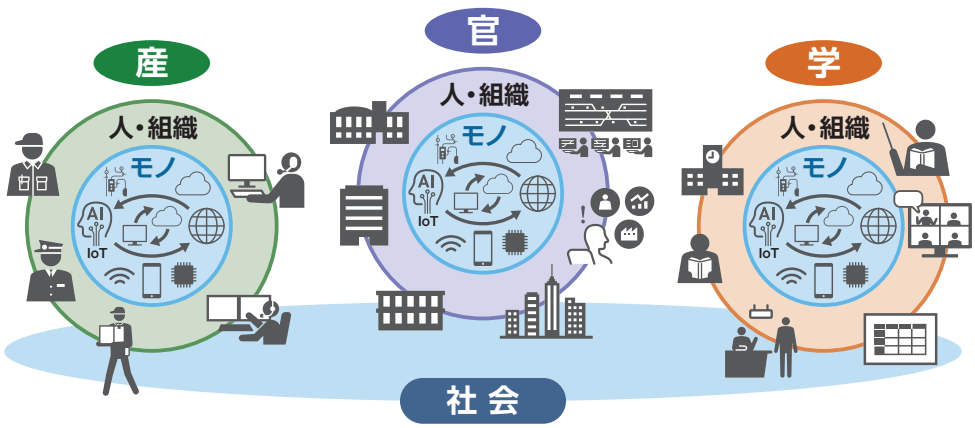
また、つながりは日立の中だけではなく、サイバーセキュリティ対策に取り組んでいる企業、国、学校との脅威情報や対策実行時の課題共有など、枠組みを越えたコミュニティの形成が必要不可欠になっています。各企業や組織が、これらのコミュニティから得られたノウハウを自分たちのセキュリティ対策にフィードバックし、さらに広げるといった、社会が「つながる」活動も、積極的に推進しています。(図表1-❷参照)

■ 自分ゴト化：新たなセキュリティ啓発に向けた取り組み

昨今の新型コロナウイルス感染症拡大による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、慣れない環境の中、つい気が緩んだり、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1-❷　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、情報セキュリティの取り組みを、経営ならびに事業における重要課題の一つと認識し、法令およびそのほかの規範に準拠・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管理体制を確立し、これを着実に実施する。加えて組織的、人的、物理的および技術的な情報セキュリティを維持し、継続的に改善していく。

(2) 情報資産の保護と継続的管理

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。

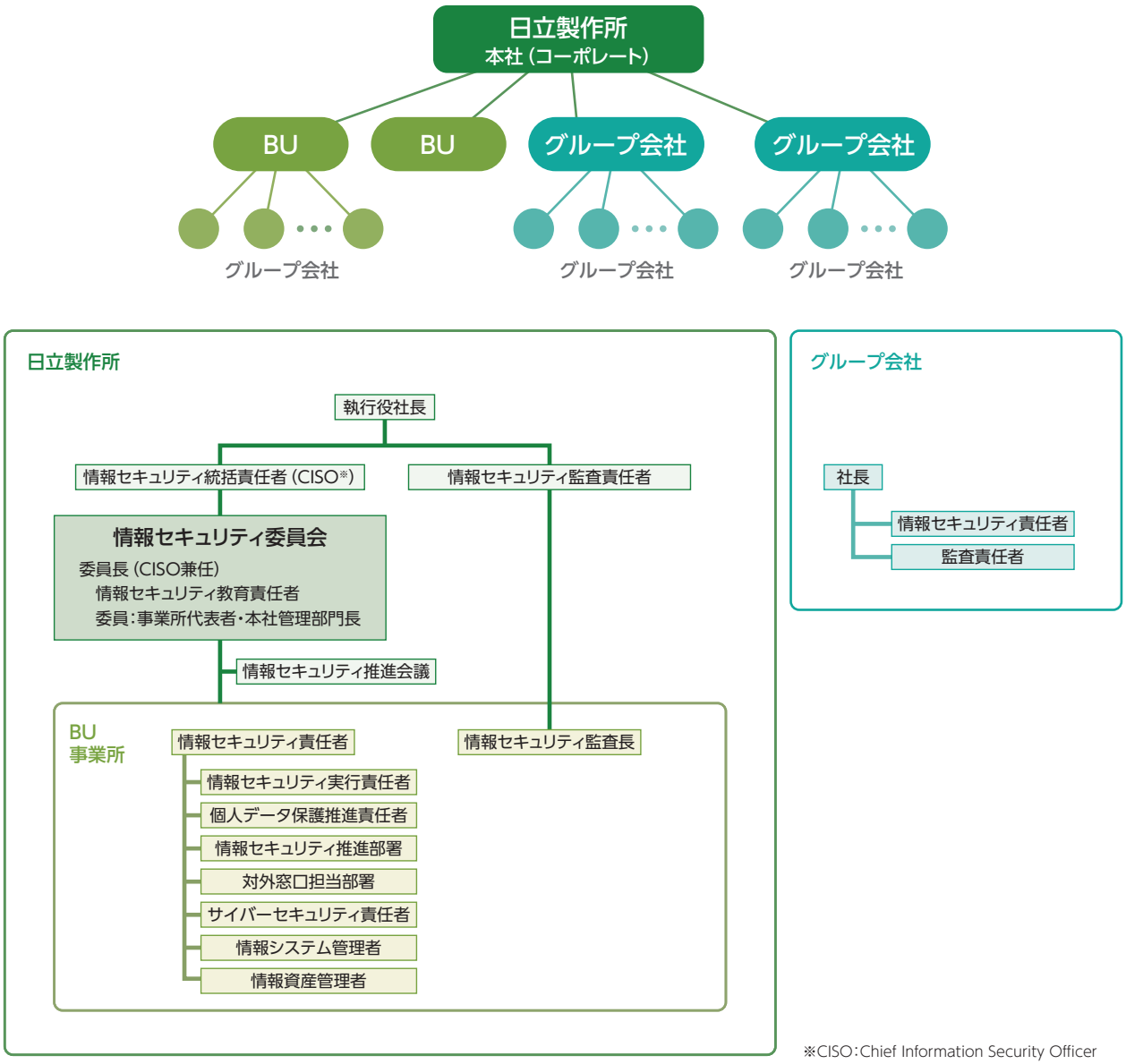
情報セキュリティ委員会の決定事項は、全BU・事業所実務者が出席する情報セキュリティ推進会議を通じて、各組織に徹底されます。

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2-❶参照)

図表2-❶　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2-❷参照)

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。

2021年に個人情報保護に関する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」を定めました。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2-❷　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サイト作成及び情報開示に関する規則
	入退及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)

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。日立製作所では従業員など約3万5千人が受講し、受講率は100%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2-❹参照)

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実施しており、2020年度より、グローバルまで拡大し、現地法人に対する訓練教育も開始しています。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	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。

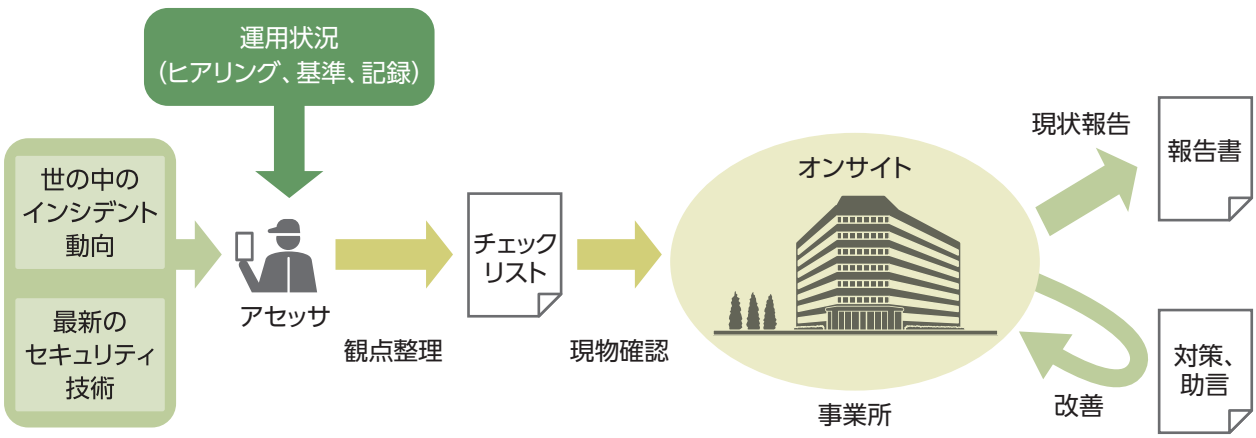
事業を取り巻く環境の変化に伴うリスクに対応するために、セキュリティ専門家チームによるアセスメント体制を強化しています。具体的にはBU・グループ会社の現場を訪問し、次の視点から強化施策に取り組んでいます。

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2-❺参照）

図表2-❺　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年度は新型コロナウイルス感染症の影響の軽減が見込まれ、比較的セキュリティリスクが高いと考える海外のグループ会社に対する訪問と現場確認を再開し、アセスメントを実施しています。

また、2022年度よりM&Aで買収した会社に対するアセスメントも開始しています。より早い時点でセキュリティリスクを把握し、対策ができるよう提言していきます。

■ 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」を定期的に実施しています。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、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、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、下の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
- お客さまへ提供する製品・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

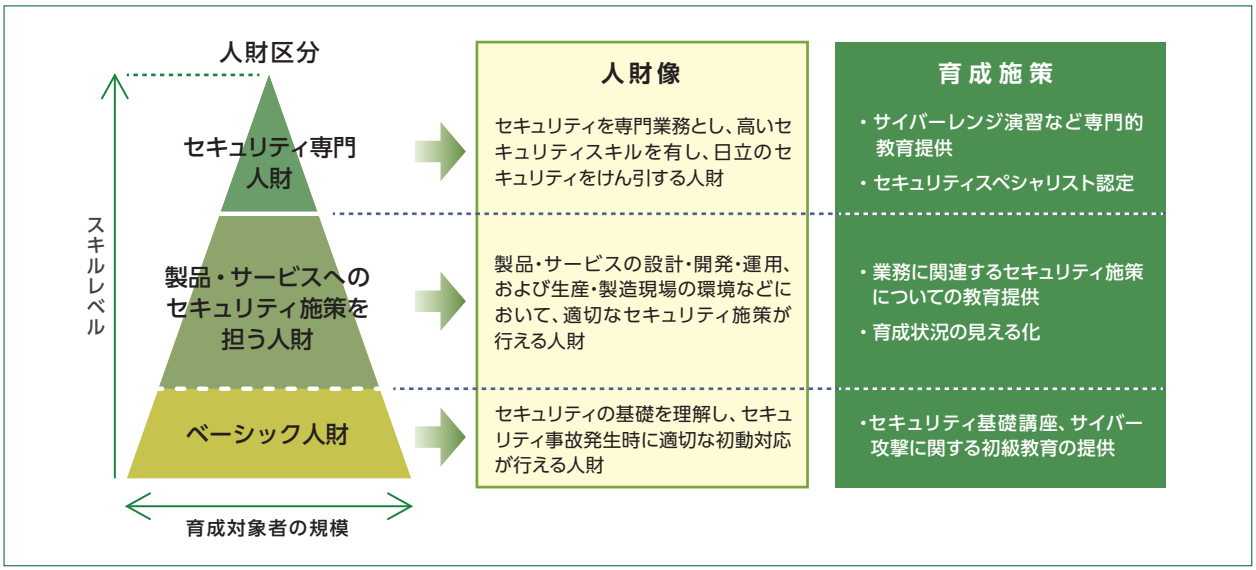
各人財区分ごとの育成プログラム

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材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 ITProfessional)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1,300名を超える人財を認定しています。

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要員の育成なども開始しています。

■ 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6,000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推進しています。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2-❼参照)

図表2-❼　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
③Web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】
①Observe (観察)　②Orient (方向付け)
③Decide (意思決定)
④Act (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

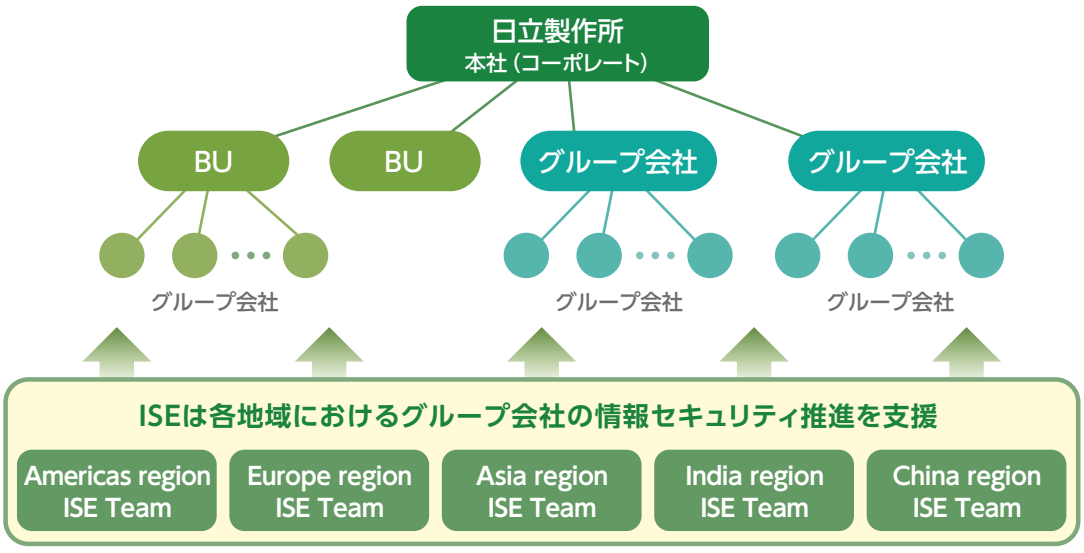
情報セキュリティのガバナンスラインは、日立グループのセキュリティ統括部門より方針・施策を各BU・グループ会社へ共有・指示を行い、各BU・グループ会社はそれぞれ区処する海外法人に対し、その実行を指示します。

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。2022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2-❽参照）

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2-❾参照）

図表2-❽　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2-❾　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」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。

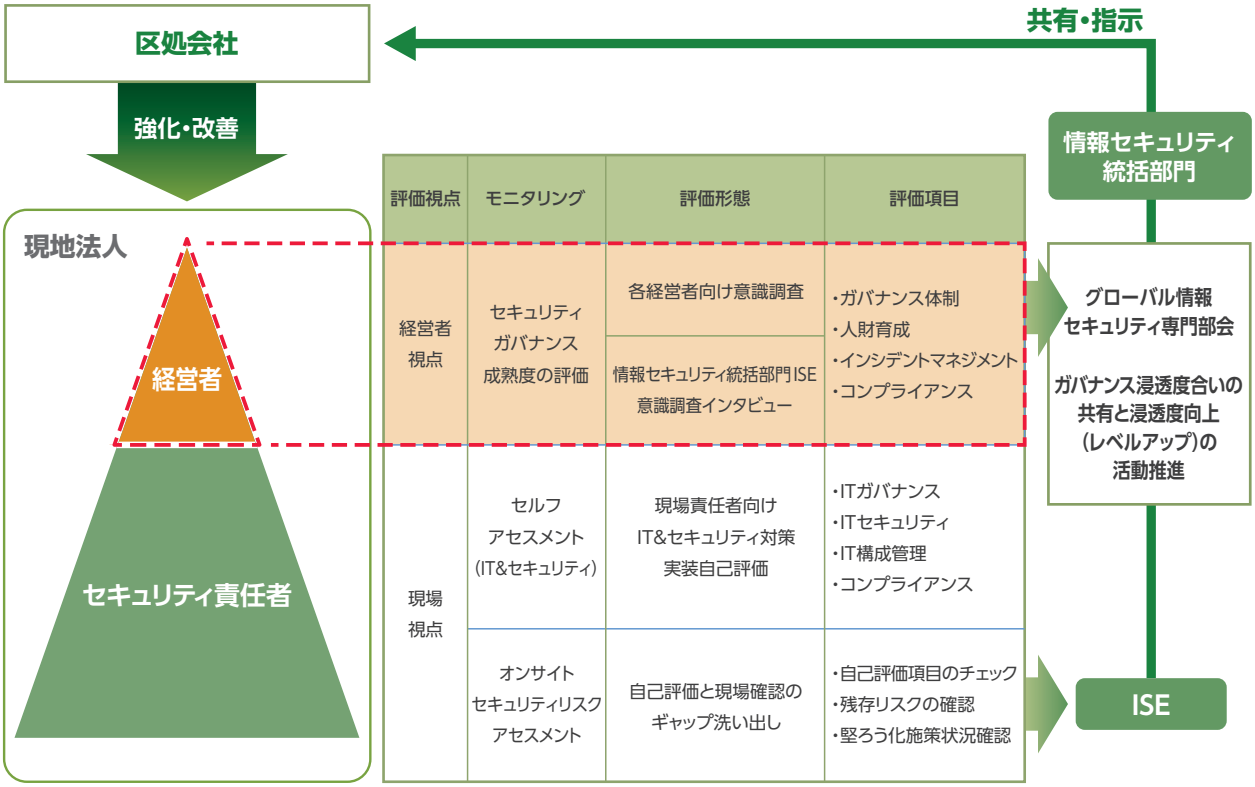
従来の現場視点に加え、経営者視点のセキュリティガバナンス成熟度を把握すべく、海外現地法人の経営者向けにセキュリティガバナンスの取り組み状況について意識サーベイを実施しています。

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の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。

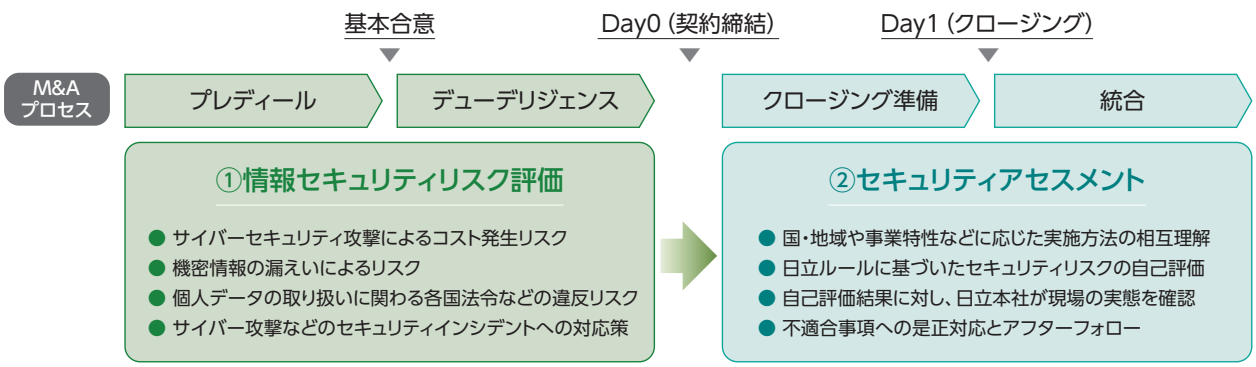
① 契約締結（Day0）前に実施する「情報セキュリティリスク評価」

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に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2-⓫参照）

図表2-⓫　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。

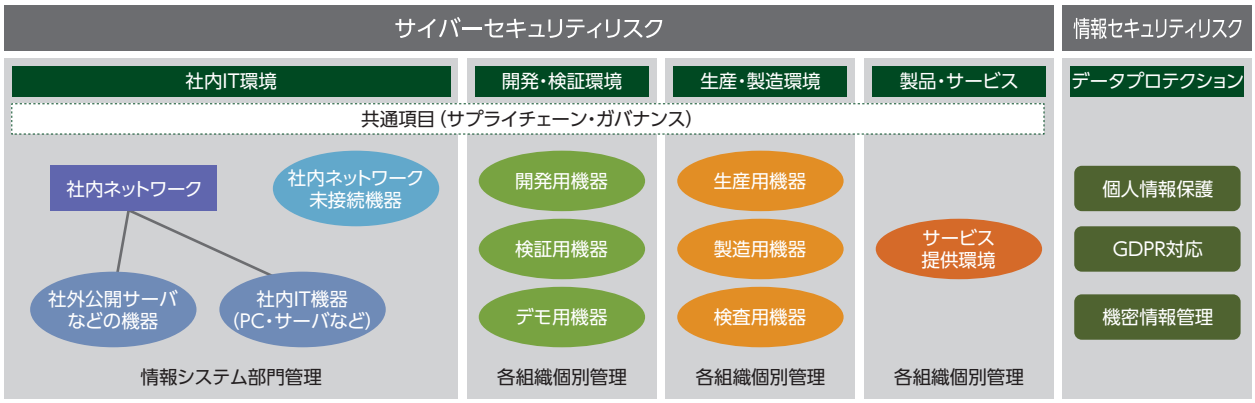
日立としては、グループ全体への情報共有やフィードバックも並行で行いつつ、全体をふかんして各社のリスク状況を適切に管理する統制体制を整備しています。

■ セキュリティアセスメントの対象領域と評価項目

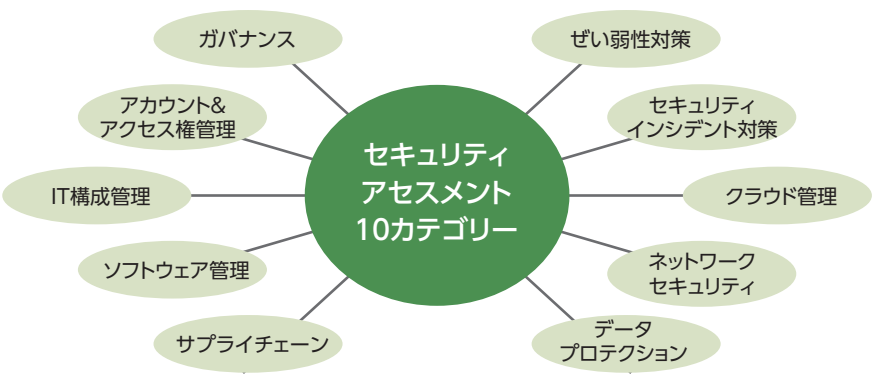
日立では、従業員が普段オフィスで業務に使用するPCやサーバなど（社内IT環境）に限らず、製品開発や製造時に使用する関連機器・装置、お客さまへ製品・サービスを提供する環境などを対象に、サイバーセキュリティリスクの対象と捉えています。また、個人情報保護や機密情報管理などに関する管理方法や漏えい対策などについて確認します。（図表2-⓬参照）

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2-⓭参照）

図表2-⓬　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



図表2-⓭　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

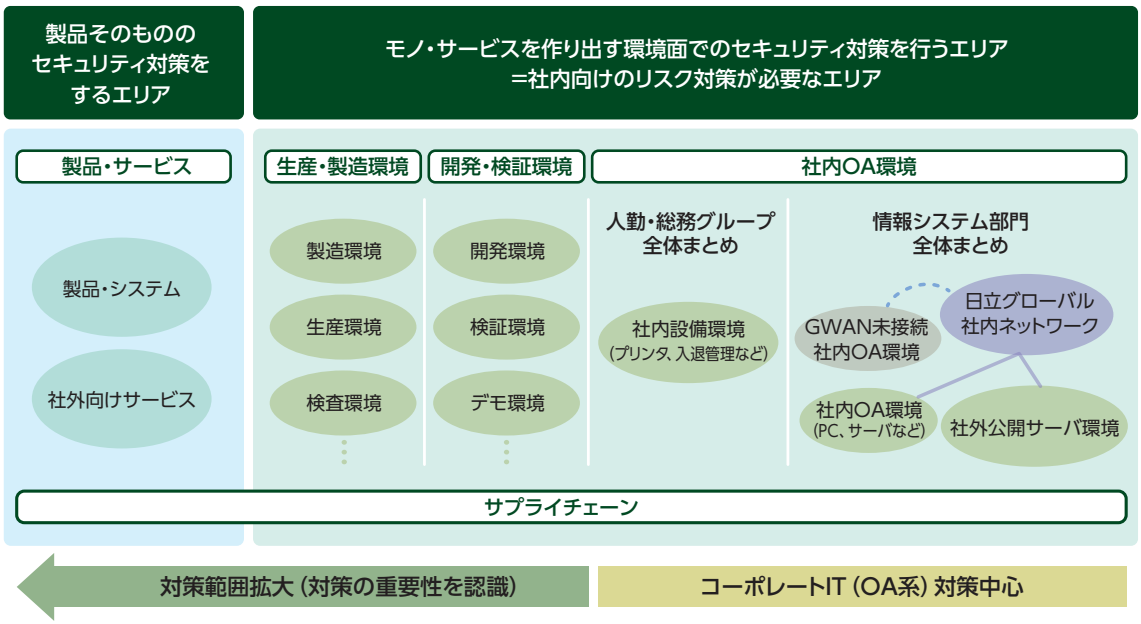
サイバー攻撃手法の多様化に伴い、インシデントの発生源や影響が拡大する中、こうしたリスクに対応するため、今までのOAで利用する社内IT環境の対策が中心であったセキュリティリスクのマネジメント範囲を拡大し、製品・サービスを作り出すための開発・検証環境や生産・製造環境、サプライチェーンや製品・サービスの開発プロセスに対しても対象を広げ、事業のリスク低減に取り組んでいます。

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2-⓮参照)

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2-⓯参照)

図表2-⓮　サイバーセキュリティ対策範囲の拡大



図表2-⓯　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

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

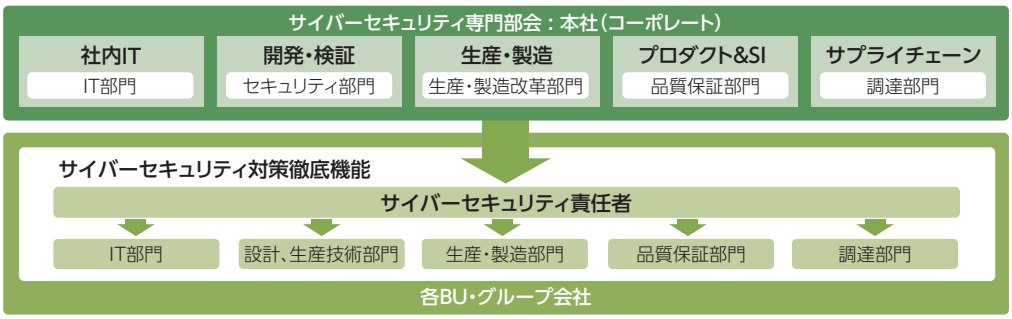
■ 社内OA環境におけるセキュリティ強化

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。

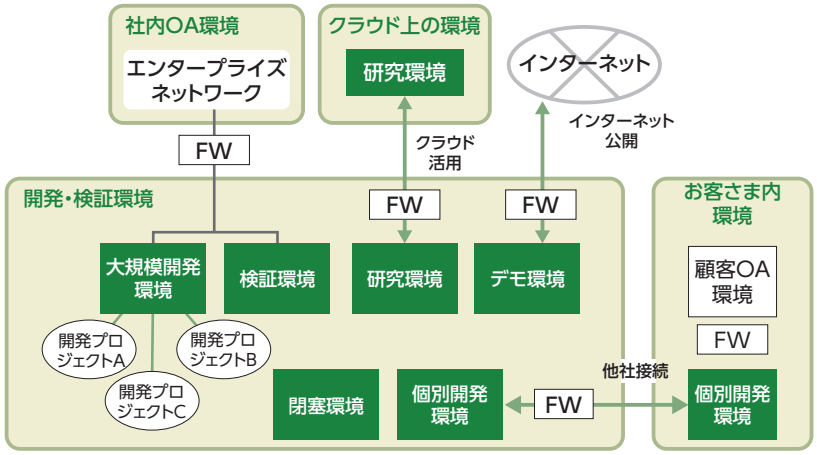
■ 開発・検証環境におけるセキュリティ強化

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



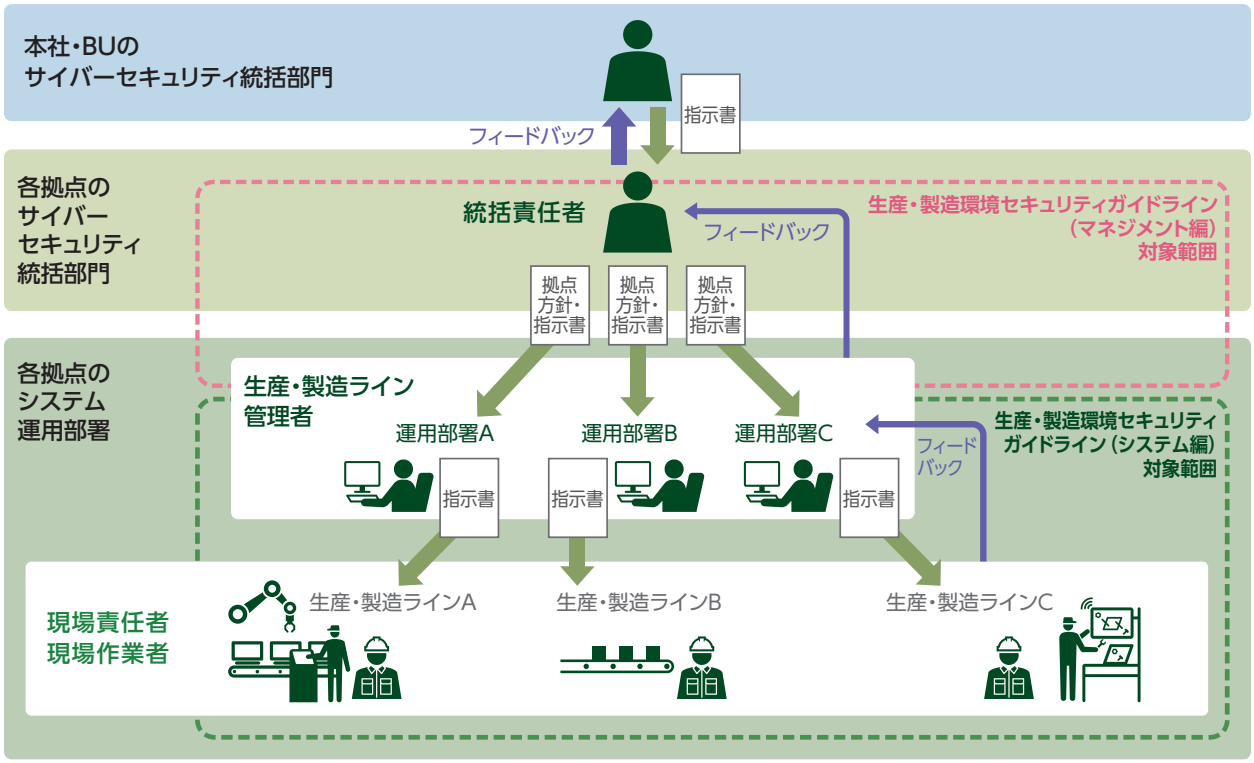
サイバーセキュリティの取り組み

■ 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2-⑱参照）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

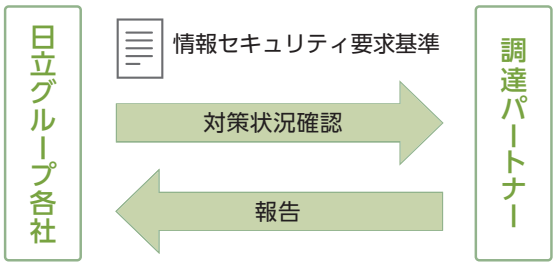
図表2-⑱　生産・製造環境におけるガイドラインの内容と活用イメージ



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2-⑳)

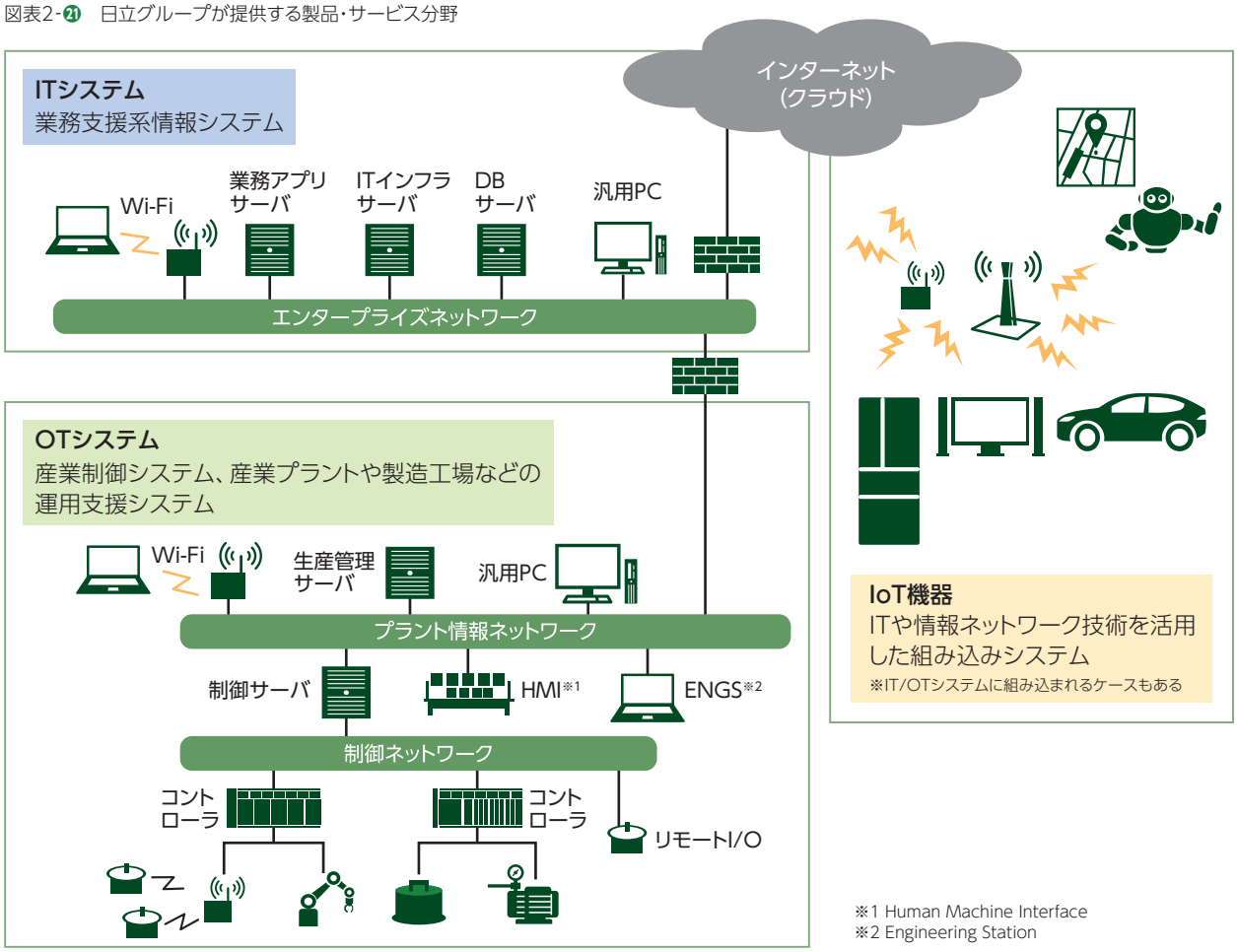


図表2-⑳　サプライチェーンにおけるセキュリティ強化体制

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



※1 Human Machine Interface
※2 Engineering Station

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)

2022年度より新たに各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、製品・サービスセキュリティの強化に取り組むセキュリティマネジメント体制の構築を推進しています。合わせて、本社(コーポレート)とBU・グループ会社にそれぞれセキュリティの技術的な対応を行うためのPSIRTを整備し、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います。

■ 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2-㉓参照)

■ 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。

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		

■ 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、お客さまへ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。リスクの大小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) セキュリティ人財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と、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的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て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。

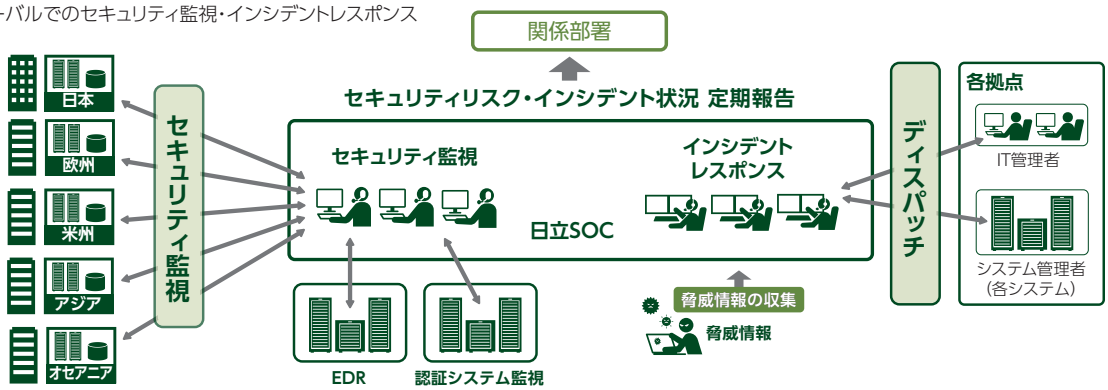
最近の脅威動向として正規の認証情報を不正に取得し悪用する攻撃が増えています。正規の認証情報が利用されており検知が困難なため、認証システムの監視機能を強化することで、第三者によるアカウント不正利用の早期検知を行っています。

■ 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へ提供する製品・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。

■ 警戒情報の配信

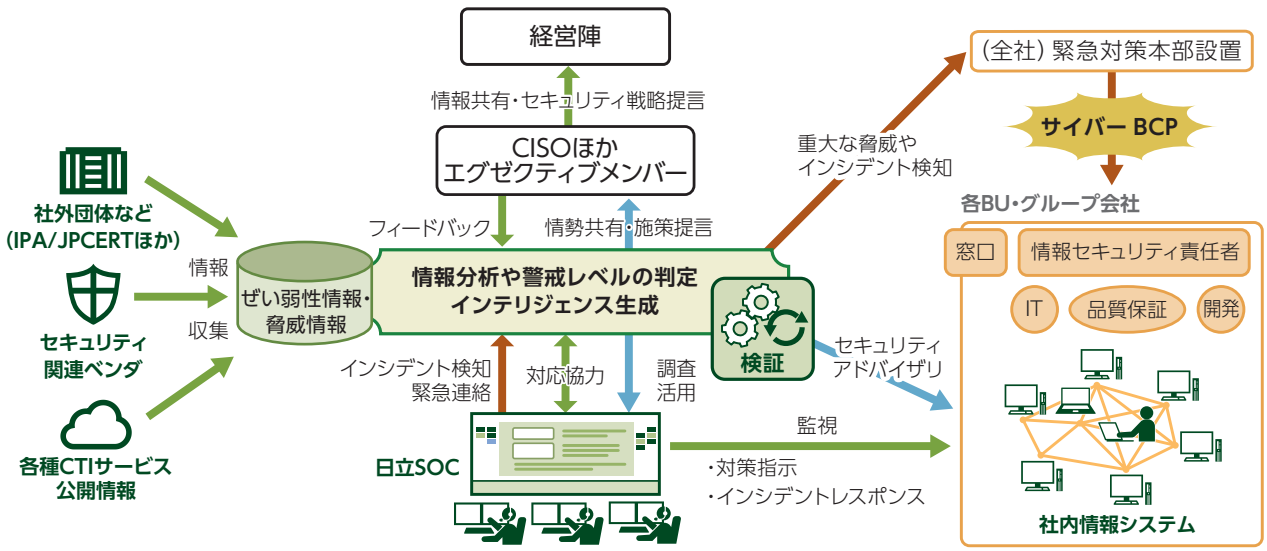
収集した情報は、各BU・グループ会社から選出されたサイバーセキュリティ責任者に対して、即時～週次でのメール配信、社内Webへの掲載などを通じて周知を行っています。また、日立グループ全体に関わる影響範囲の広い脅威に対しては、サイバー BCPの発令に関して検討するとともに、対策を徹底させるためのサイバー警報を発報することで対策強化を図っています。また、社外に公開しているシステムを調査し、被害を受ける可能性のある場合は該当部署へ個別に通知し、対策を促す活動を行っています。これらの収集・分析情報は、日立SOCや情報システム部門とも密に連携し、インシデント対応や監視の強化にも活用しています。

これらの活動から得られた知見を基に、日立グループの現状や改善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。

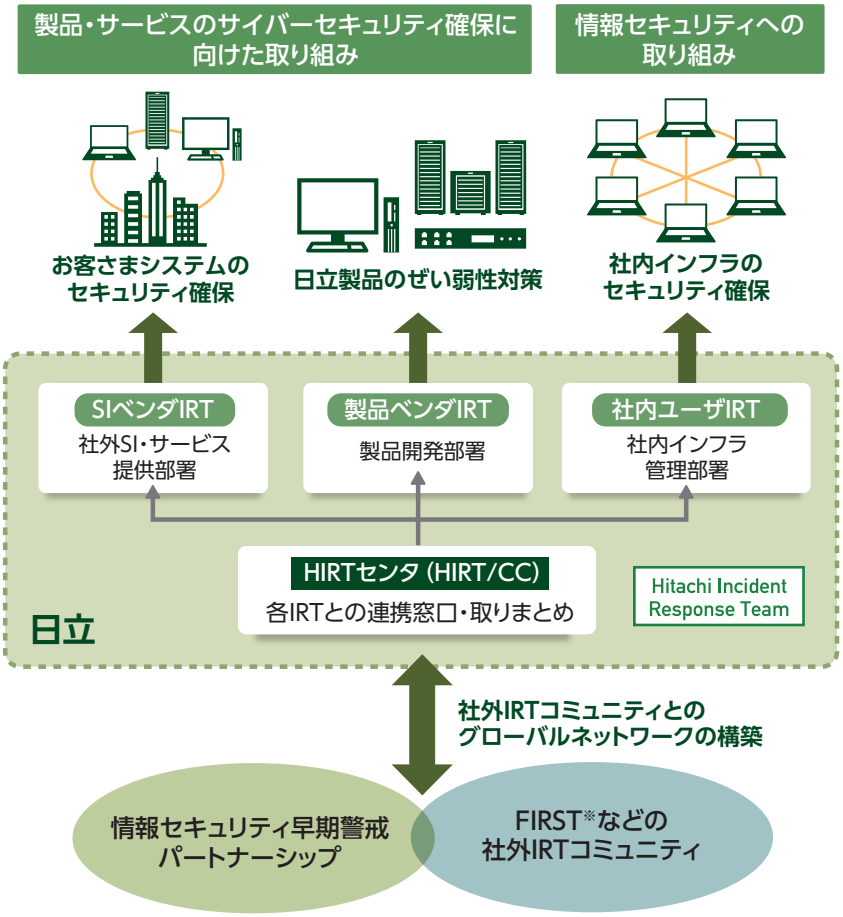
HIRTは、ぜい弱性対策とインシデント対応とを推進するために、下記のように、4つのIRT (Incident Response Team) という活動モデルを採用しています。4つのIRTとは、

(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

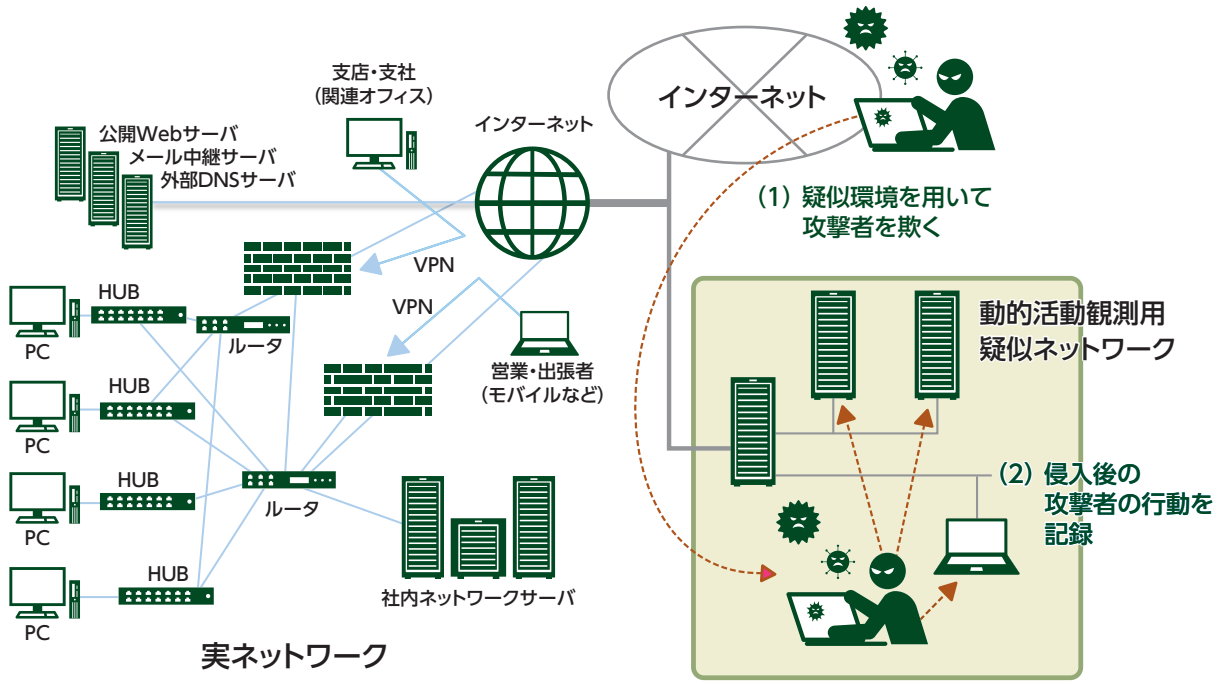
「次の脅威のキャッチアップ」と早期に対策展開を図るための技術として「動的活動観測」に取り組んでいます。動的活動観測は、標的型攻撃などのサイバー攻撃を調査するために構築した組織内ネットワークの疑似環境下で、侵入後の攻撃者の行動を記録し分析する観測手法です。(図表2-㉗参照)

(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2-㉗ 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)の順守により、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。

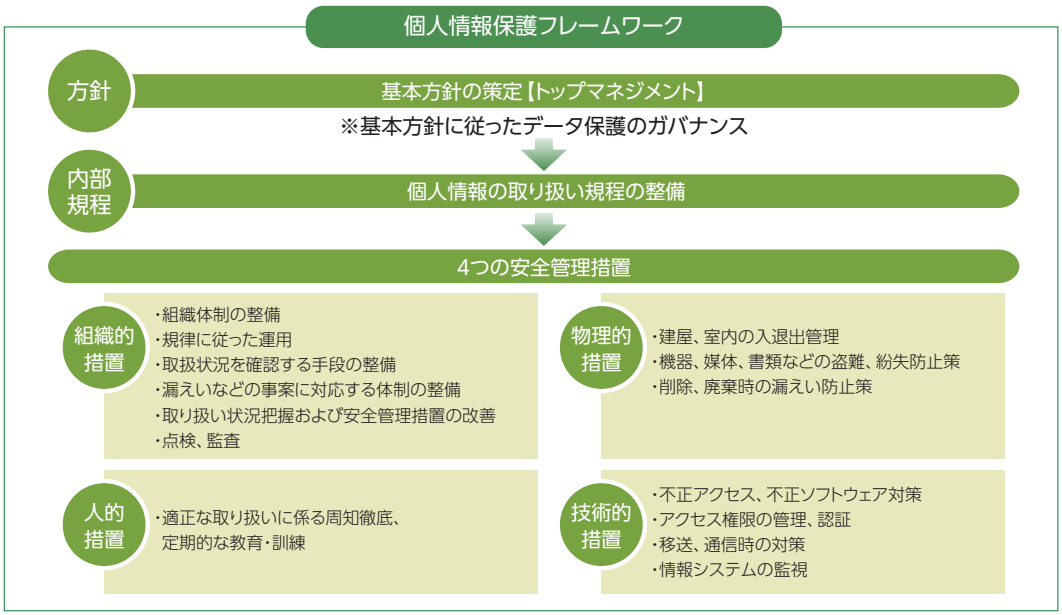
（4）法令・規範の順守

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順守します。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2-㉙　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。

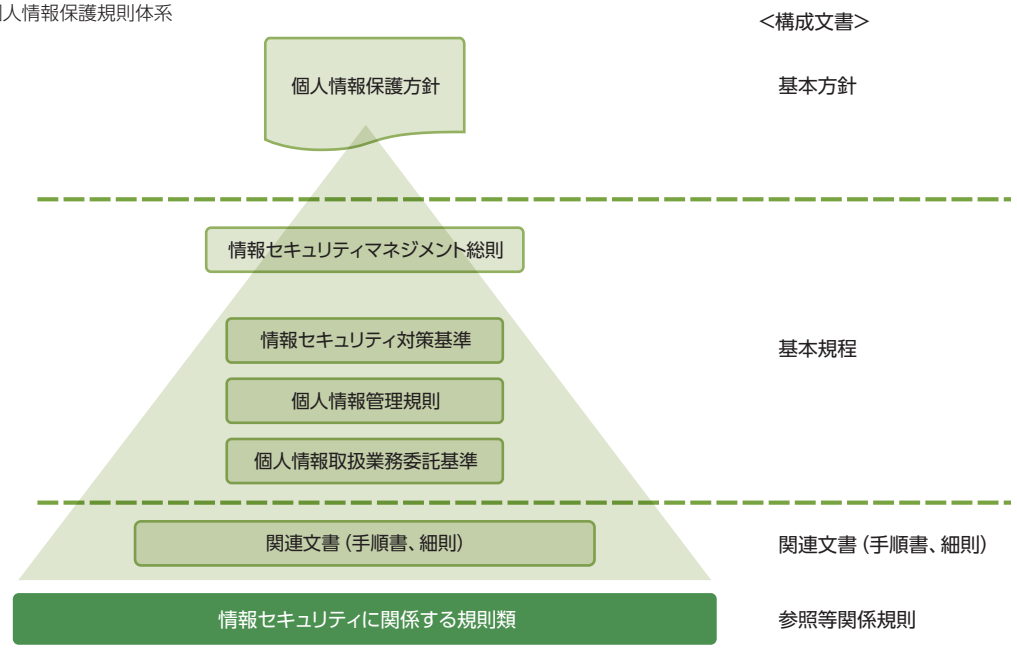
技術的安全管理措置では、情報システムに対する不正アクセス、不正ソフトウェア対策の実施などを行っています。また、取り扱う個人情報の重要度に応じてアクセス権限の管理、認証、移送、通信時の対策、情報システムの監視などを行っています。

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 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



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。

2021年度は、改正個人情報保護法対応について、計画を立て[Plan]規則類を改正しました。現在各所にて推進中であり[Do]、2022年度は点検、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す[Action]。(図表2-31参照)

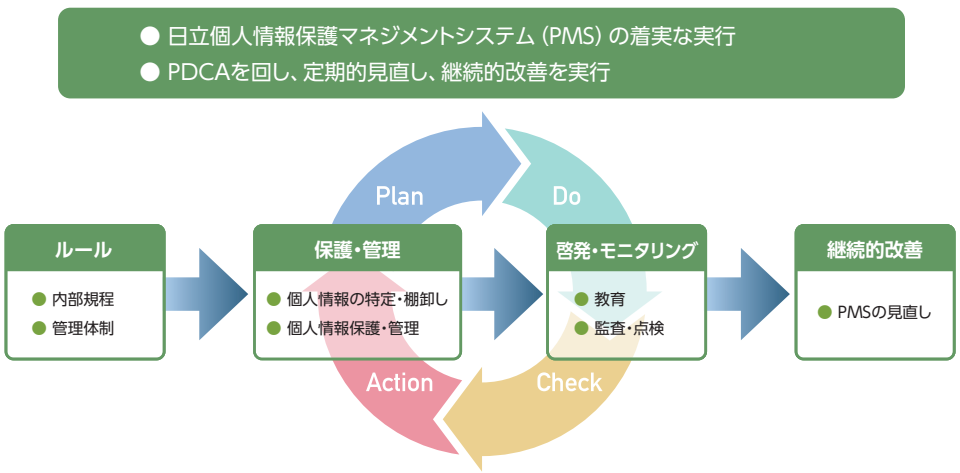
個人情報の管理と適切な取り扱い

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、分析を実施し、取り扱いに関するルールを定めて運用する「個人情報取扱業務」は、全社一括管理を行っており、定期的に見直しを実施しています。

また、個人情報取扱者には、当該業務の取り扱いルールの周知徹底を行い、署名を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2-31　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

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、管理の順守事項を確認し、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を実施 し、日立全体として監査・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（740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。

※2022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おり、個人情報保護への要請も高まっています。この状況下、世界各国で個人情報保護関連法制度の制定・改定の動きが活発になっています。

国境をまたいでデータの利活用がなされることもあり、各国法制度では保護対象となる個人情報が自国内のものに限定されなかったり、他国への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。

そのほか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などと連携しながら対応を推進しています。

2021年には個人情報保護に関する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、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を推進するため、各国の対応機能の強化・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、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、2021年3月に8回目の付与適格決定を受け、2023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（2022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
株式会社四国日立システムズ
株式会社セキュアブレイン
株式会社 日立ICTビジネスサービス
株式会社 日立アーバンサポート
株式会社 日立アカデミー
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SC株式会社
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
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 日立ハイテクソリューションズ
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。

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&サービスセクターが中心となって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。

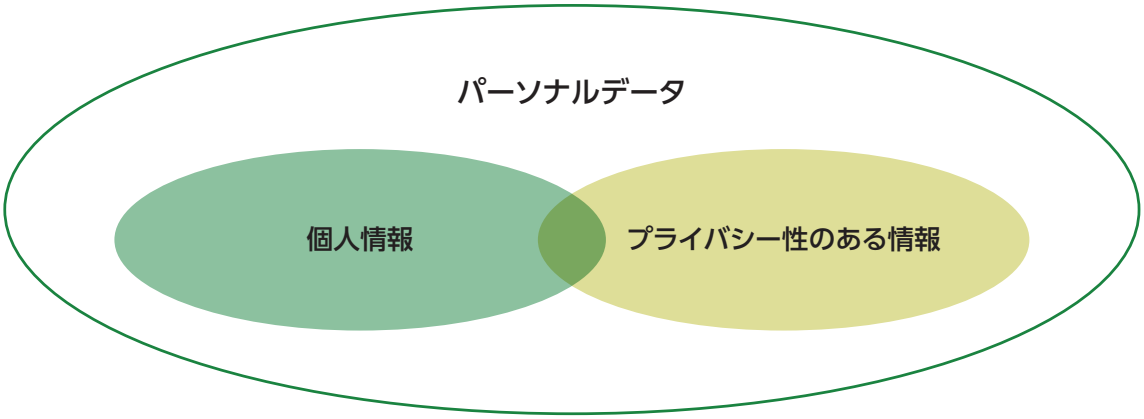
■ プライバシー保護諮問委員会の運営

日立は、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

日立では、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。

日立は、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2021年度だけで約230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。

■ 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。

生活者およびお客さまの安全・安心をめざして

日立は、プライバシー保護に関する生活者の期待に対応するため、2020年に株式会社 博報堂の協力を得て「第五回 ビッグデータで取り扱う生活者情報に関する意識調査」を実施しました※1。このような調査から得た生活者の意識の変化をプライバシー保護対策に反映しています。そして、本調査のような生活者の意識を継続的に調査し、施策の評価・改善に役立てる取り組みは、総務省と経済産業省による「DX時代における企業のプライバシーガバナンスガイドブックver1.2」※2においても重要であると記され、日立の取り組みが事例として取り上げられています。

2022年3月には、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。

※1「第五回 ビッグデータで取り扱う生活者情報に関する意識調査」(2020年12月公表)
https://www.hitachi.co.jp/New/cnews/month/2020/12/1222a.html
※2「DX時代における企業のプライバシーガバナンスガイドブックver1.2」(2022年2月公表)
https://www.meti.go.jp/policy/it_policy/privacy/guidebook12.pdf

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。

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, WG20
  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、制御システムにおけるネットワークと制御装置のセキュリティに関する規格化が検討されています。また、WG20では、制御システムにおけるセキュリティと機能安全の両立に関する規格化が検討されています。
- 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。2022年9月末現在で、101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、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 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

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」

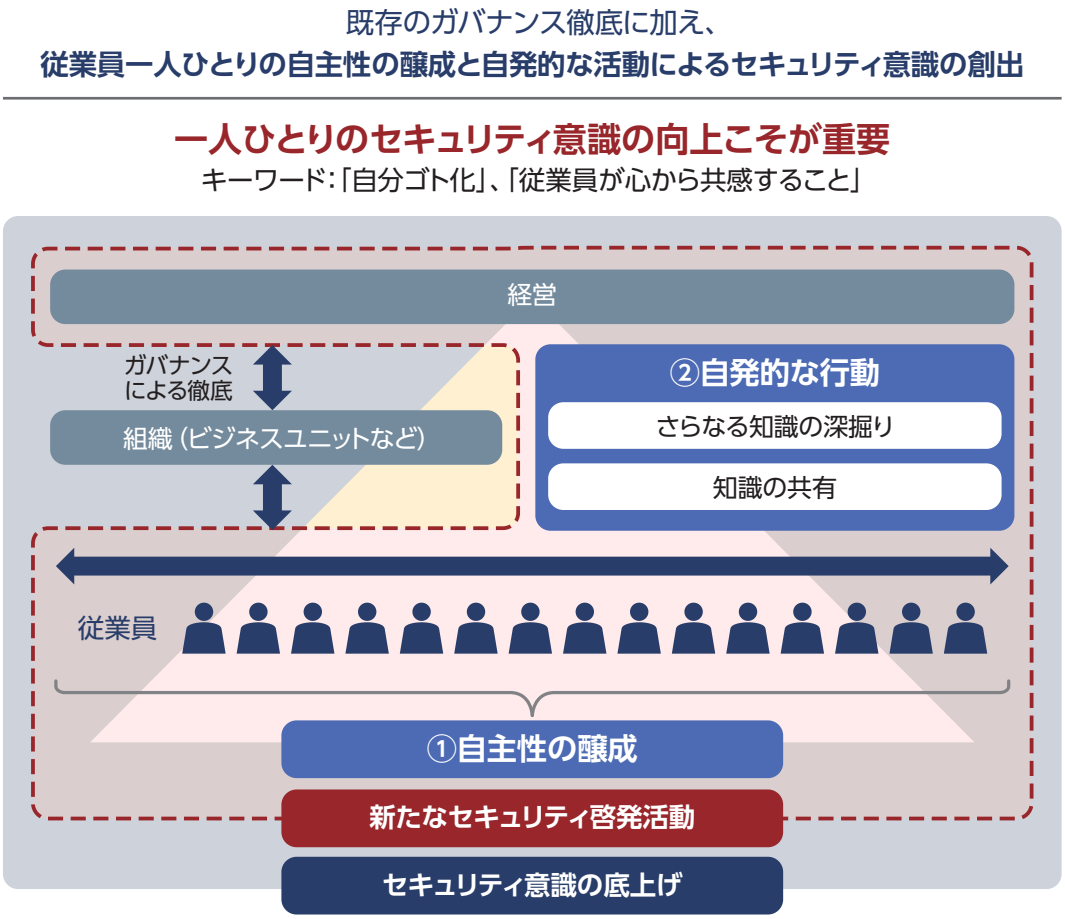
昨今の新型コロナウイルス感染症拡大により、テレワークの導入が一気に加速、定着する一方で、サイバー攻撃の脅威はますます高まっており、テレワークの推進には十分なセキュリティ対策が不可欠となっています。今まで攻撃者の主なターゲットは組織のITのぜい弱性でしたが、テレワーク中心の働き方においては、「セキュリティ意識のぜい弱性」が狙われることが想定されます。

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3-❶参照)

図表3-❶　これからのセキュリティ啓発のめざす姿



自主性の醸成に向けた活動：Harry's Security

2020年12月より、まず「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3-❷参照）

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

2021年5月より、「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」をスタートしています。（図表3-❸参照）

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Micosoft Teams※を活用し、実施している取り組みを紹介したり、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。

※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　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3-❸　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。

コラム
COLUMN

お客さまのビジネスを守るプロダクトセキュリティ技術

昨今のサイバー攻撃はコネクテッド化が進むプロダクトやOTシステムを対象としており、その被害も深刻化しています。各業界でプロダクトセキュリティの法規制化や規格化が急速に進んでおり、その対応がお客さまのビジネスにとって不可欠となっています。日立はお客さまのビジネスを守るさまざまなセキュリティ技術開発に取り組んでいます。

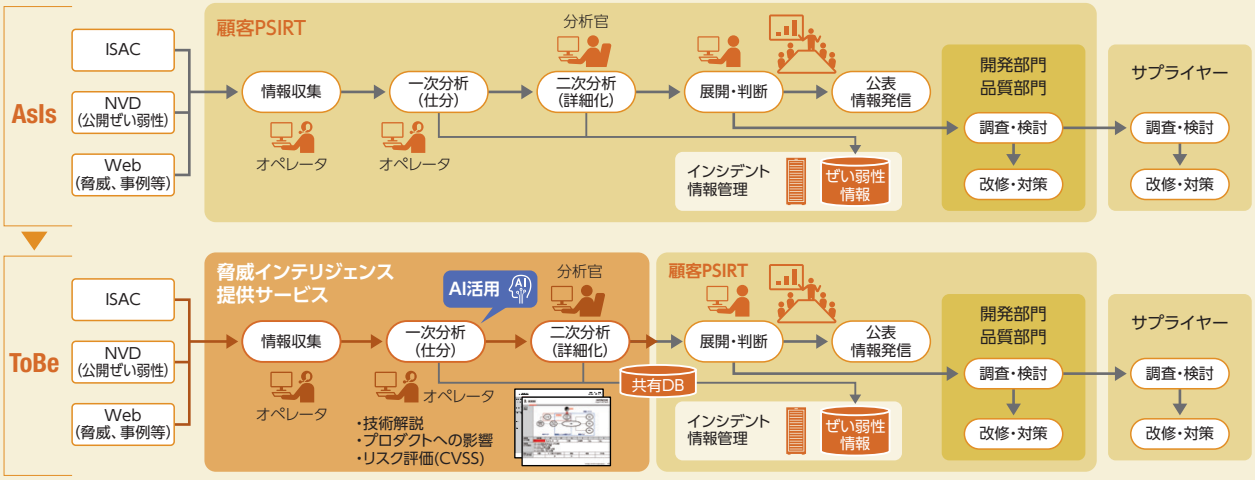
お客さまのビジネスを守るプロダクトセキュリティ技術開発の推進

サイバー攻撃と言えば、ひと昔前まではいわゆる「ITシステム」が対象でした。一方近年は自動車や家電といった「プロダクト」や、工場や社会インフラといった「OTシステム」が、インターネットなどを介して他とつながるようになり、かつてないサイバー攻撃の脅威にさらされています。これらのいわゆるIoT（Internet of Things）システムは、人々の生活や安全に直結するものも多くあり、販売・運用の責任主体となるお客さま企業にとって、自社のプロダクトのセキュリティを守ることは極めて重要になります。各業界ではプロダクトセキュリティに関する法規制・ガイドラインの施行・義務化が急激かつグローバルに進行しており、ビジネスを担うお客さま企業にとってこれらへの対応が不可欠となっています。プロダクトは設計・開発・運用といったライフサイクルすべてにおいてセキュリティが考慮される必要がありますが、近年は、長期運用されるプロダクトのコネクテッド化や、搭載されるソフトウェアの複雑化を背景に、運用フェーズのセキュリティに対するニーズが特に高まっています。日立では、PSIRT向け脅威インテリジェント分析技術、自動車向けセキュリティオペレーション技術など、運用フェーズ向けプロダクトセキュリティ技術の開発を進めています。

PSIRT向け脅威インテリジェント分析技術

運用フェーズのプロダクトセキュリティを守るため、お客さま企業はPSIRT組織（Product Security Incident Response Teams）を設立することが求められています。PSIRTはプロダクトに関するぜい弱性情報を監視し、それらに対するプロダクトへの影響を判断し対応の意思決定を行います。PSIRTにはインターネットや外部組織などから日々大量のプロダクトセキュリティに関する情報が集まります。これらを適切に仕分けし影響を判断する必要がありますが、そのためにはセキュリティと自社プロダクトの両方に詳しいエキスパート人財が不可欠です。

図表❶　PSIRT向け脅威インテリジェント分析の概要



プロダクトのIoT化は加速し、セキュリティ情報は日々増え続ける一方で、これらエキスパート人財の育成・維持が難しく、スケーラビリティを確保しにくいという課題がありました。

これに対し日立では、AIを活用したPSIRT向け脅威インテリジェント分析技術を開発しています。この技術は収集されたセキュリティ情報が当該の分野やお客さま企業に関係あるか否かについて、AIを用いて自動で判定します。IT関連および業界特有のセキュリティ情報によって学習された判別モデルをAIに用いることで、PSIRTのエキスパート人財が見るべき情報の8割を削減することが可能となりました。この技術は日立が提供する脅威インテリジェント提供サービスにて活用され、お客さま企業や業界向けに特化した分析レポートのタイムリーな提供に役立っています。(図表❶参照)

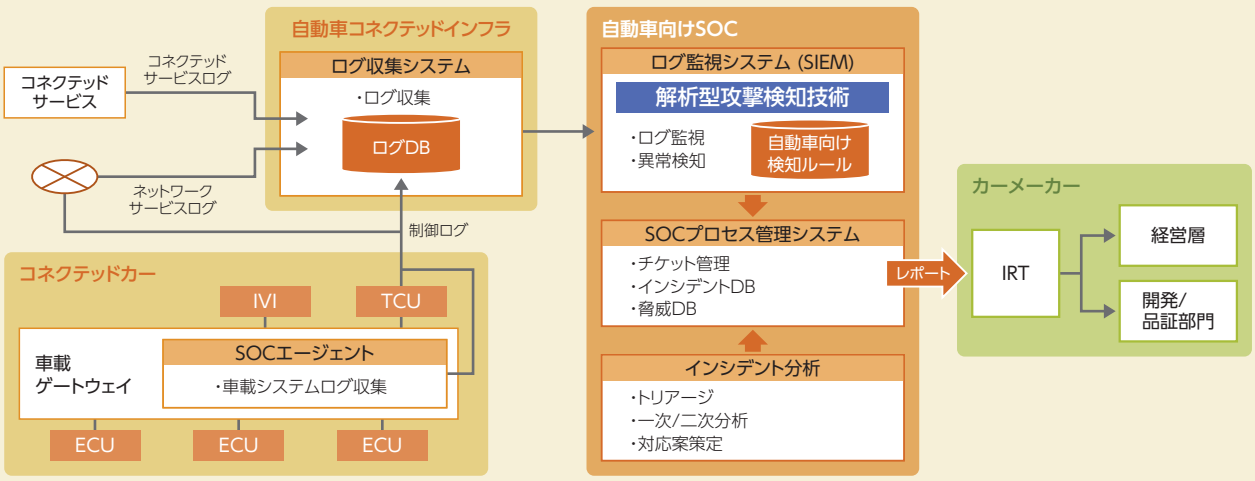
自動車向けセキュリティオペレーション技術

サイバー攻撃のリスクはコネクテッドカーなどの自動車に対しても増大しています。自動車サイバーセキュリティに関する法規制が国連WP29で制定され、製造時の対策に加え、運用時のセキュリティ維持も求められています。これを受け、カーメーカー各社は自動車を監視して攻撃を検知・対処する自動車セキュリティオペレーションセンターの立ち上げを進めています。日立はIT向けSOC (Security Operation Center) の実績と車載機器開発に関する知見に基づき、自動車向けSOCに関する技術開発およびソリューション提供を行っています。

日立の自動車向けSOCでは、車両、センター、モバイルなどのログをリアルタイムで監視し、攻撃の発生を迅速に検知して被害を抑制します。日立は車載システムからクラウド側のシステムまでをソリューションとして提供し、インシデント対応を迅速かつ確実にサポートします。特に車両サイドでは、車載システムならではの特徴を捉え、監視ログを設計・配置し、車両から監視システムへのログ収集を効率的に行うソフトウェアを提供します。車載ゲートウェイで収集したログを統合的に分析することで攻撃シナリオを推定し、攻撃者が車外から侵入した初期の段階で攻撃の兆候を検知します。

監視システムでのログ解析を効果的に行うためには、適切な攻撃検知ルールの作成が不可欠です。従来のIT向けSOCにおける攻撃検知ルールの作成には攻撃事例の蓄積が必要でしたが、車への攻撃事例は蓄積が少なく、そのまま適用することが困難であるという課題がありました。事例がなければあらゆる攻撃を網羅的に想定する必要がありますが、一方で車両モデルのリリースタイミングに間に合うように効率的に検知ルールを設計しなければなりません。そこで日立では、攻撃事例が少ない中でも検知ルールを作成する手法である自動車SOC向け解析型サイバー攻撃検知技術を開発しました。この手法では、日立の持つセキュリティ設計技術を活用して解析的に抽出した車両への脅威に対して、IT分野の蓄積された攻撃事例から類推できる攻撃者の行動を割り当て、さらに、ITと自動車での攻撃者の行動の違いを踏まえて攻撃者行動を変換します。これにより漏れのない検知ルールを効率的に作成することが可能となりました。本技術は日立の自動車向けSOCソリューションにおいて活用されています。(図表❷参照)

図表❷　自動車向けセキュリティオペレーションの概要



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（2022年8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、Lumada CoE、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）
- 株式会社 日立製作所（社会システム事業部　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 交通情報システム本部）
- 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 システム&サービスビジネス営業統括本部 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）
- 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、クラウドサービス事業部、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 日立システムズパワーサービス（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（経営企画本部総務本部財務本部公共・社会事業部企業サービス事業部　事業企画部 システム事業本部 システム第1部 第1グループ 第2グループ システム第2部　プラットフォーム事業第1本部　ファシリティ事業推進部 ファシリティサービスグループ　プラットフォーム事業第2本部営業統括本部　営業企画本部　公共・社会営業本部 営業第1部 営業第1グループ　営業第2部　企業営業本部 営業第1部 営業第1グループ　営業第2部生産技術管理本部品質保証本部）
- 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、金融第1ソリューション本部 第3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
- 日立SC株式会社（本社）
- 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）
- 株式会社 日立ハイテクソリューションズ（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(2022年8月末時点[認証製品アーカイブリストへの掲載を含みます])。(図表4-❶参照)

図表4-❶ 「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（2022年8月時点[CMVPによる“historical list”への掲載を含みます]）。（図表4-❷参照）

図表4-❷　「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 (2022年3月31日時点)

商号	株式会社 日立製作所	**資本金**	461,731百万円
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**	36万8,247人 (国内15万6,768人、海外21万1,479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**	853社 (国内157社、海外696社)
代表者※1	代表執行役 執行役社長兼 CEO 小島 啓二	**持分法適用会社数**	287社

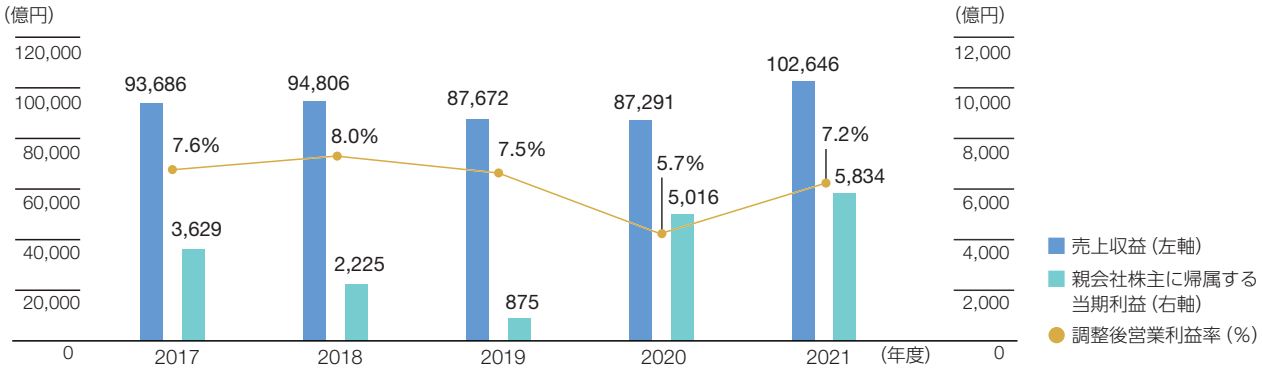
※1 2022年6月23日時点

財務ハイライト (2022年3月期連結IFRS)

売上収益	10兆2,646億円　(前期比118%)	**当期利益 (親会社株主帰属)**	5,834億円　(前期比818億円増)
調整後営業利益率	7.2%　(前期比1.5ポイント増)	**ROIC**※3	7.7%　(前期比1.3ポイント増)
EBIT※2	8,509億円　(前期比6億円増)		

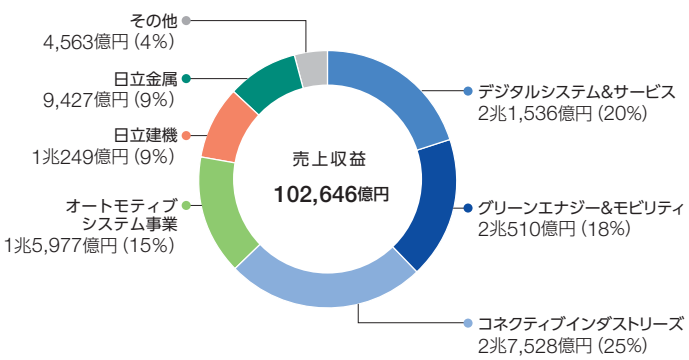
＊ 当社の連結財務諸表は、国際財務報告基準 (IFRS) に基づいて作成しています
※2 EBIT:継続事業税引前当期利益から、受取利息の額を減算し、支払利息の額を加算して算出した指標
※3 ROIC:Return on invested capitalの略で「投下資本利益率」の意。「ROIC=(税引後の調整後営業利益率+持分法損益) ÷投下資本×100」により算出。
なお、税引後の調整後営業利益=調整後営業利益×(1−税引負担率)、投下資本=有利子負債+資本の部合計

■ 売上収益／調整後営業利益率／当期利益の推移



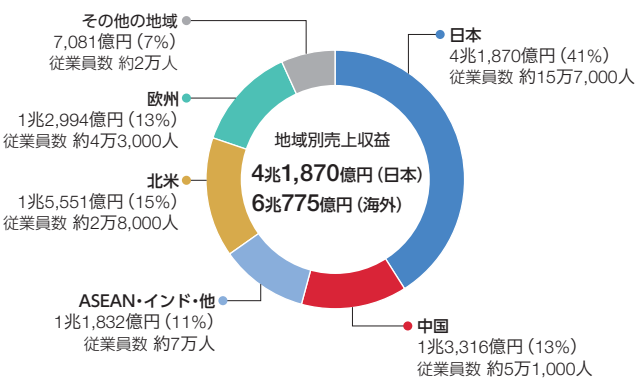
■ セグメント別売上収益／構成比

(2022年3月期 連結IFRS)



■ 地域別売上収益／構成比

(2022年3月期連結IFRS)



＊ 各部門の売上収益は、部門間内部売上収益を含んでいます

株式会社 日立製作所
情報セキュリティリスク統括本部
〒100-8280 東京都千代田区丸の内一丁目6番6号
TEL.03-3258-1111

Printed in Japan (H) (2022.10)