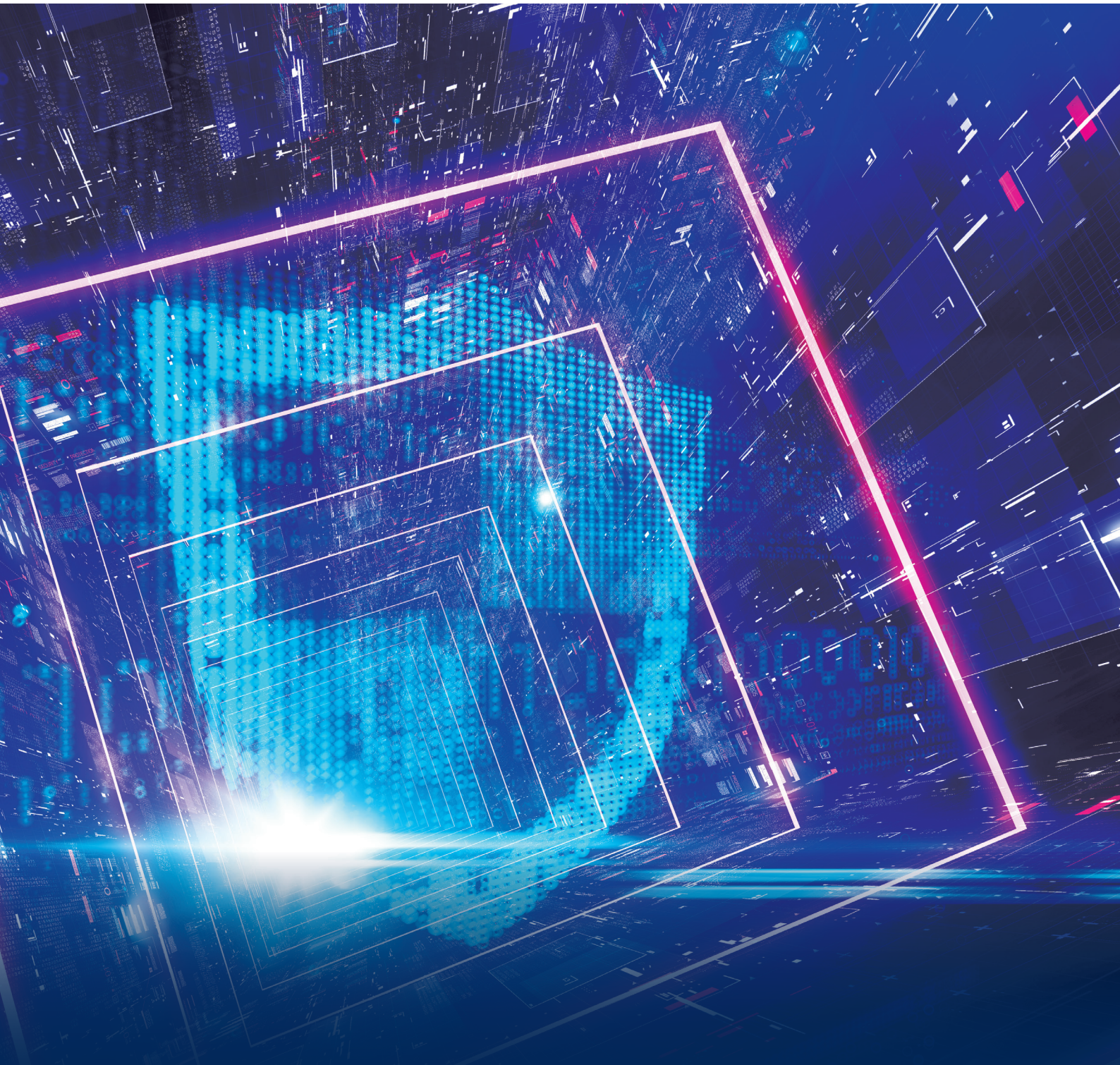


# 情報セキュリティ報告書 2021

Information Security Report 2021





# INDEX

CISOインタビュー	1
トピックス	4
情報セキュリティガバナンス	7
情報セキュリティマネジメント	8
日立グループにおけるCSIRT活動	13
サイバーセキュリティ対策	16
グローバル情報セキュリティの取り組み	18
セキュリティ人材育成の取り組み	20
サイバーセキュリティマネジメントの取り組み	22
個人情報保護に対する取り組み	28
<b>コラム</b> 日立グループのプライバシーマークへの取り組み	35
プライバシー保護の取り組み	36
情報セキュリティ実現のための研究開発	38
情報セキュリティに関する社外活動	40
第三者評価・認証	42
日立グループの概要	45

---

## 〈本報告書の概要〉

- 報告範囲・期間：2020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：2021年12月発行
-

## ニューノーマル、協創、グローバル展開が進行 そのインフラを支えるのが情報セキュリティの使命

— この一年を振り返ると、新型コロナウイルス感染症の拡大によって働き方が大きく変わりました。企業のセキュリティに対する影響をどう捉えていますか。

企業のさまざまな部門やビジネスシーンにおいて、非接触、非対面が進み、ニューノーマル下の働き方が定着してきました。オンラインは非常に便利なシステムで、その利点にばかり目が行きがちですが、便利さの裏にある怖さを認識しなければなりません。

ビジネスを行う時、コロナ禍前までは出社することが当たり前でしたが、もはや場所ありきではありません。目標とする業務が達成されるなら、極論するとどこにいてもいいわけです。日立でも社会機能を維持するための業務、製造に関わる業務、お客さまと直接行わねばならない業務など、出社せざるを得ない業務以外は、幅広い職務で在宅勤務を標準とした働き方を推進しています。物理的に離れて業務を行うにはITシステムやツールの整備が必要です。そのインフラ構築は会社がすべきことであり、そのインフラを安心で支える情報セキュリティはとても重要です。

— 働き方の変化に伴いITシステムのクラウド化が加速していますが、このような変化におけるリスクをどのように認識されていますか。

クラウドを活用したシステムでは、インターネットを経由するため、情報漏えいや不正アクセスなど、セキュリティ面でのリスクも高くなります。従来の社内ネットワークを中心としたシステムと異なった発想でのリスク対策が必要になってきます。監視ツールの導入などを進めるとともに、並行して、従業員一人ひとりの行動も重要になりますので、リスクを想定した一定のルールを設けることが必要です。

— そのルールとは何でしょうか。セキュリティリスクと常に隣り合わせにいる従業員は、どんなセキュリティ意識を持てばいいでしょうか。

コロナ禍によって働き方が変わり、日立もリモートワークのための環境づくりを前倒しで進めています。会社が構築したシステムにのっとり、ルールを守って業務を行うことが不可欠です。急いでいたから、経験が浅いから、デジタルに疎いからといった理由で許されること



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。

## ニューノーマル、協創、グローバル展開が進行 そのインフラを支えるのが情報セキュリティの使命

ではありません。社会の中で、我々が最低限のルールを守りながら生活をしているように、情報セキュリティに関しても、ルールを破った場合にはしかるべき措置をとる厳しい態度で臨むことも必要です。

また、個人のパソコンやスマートフォンがウイルス感染したら一大事なのに、なぜ会社の物だと困らないと思えるのでしょうか。会社から貸与された全ての備品は個人の持ち物と同じ価値、意味合いを持つという意識を持ってほしいと思います。

### — データ利活用をベースとした協創型ビジネスにおいて、情報セキュリティをどう位置づけていますか。

日立グループでは、お客さまのデータに光を当て、輝かせることで新たな知見を引き出し、お客さまの経営課題の解決や事業の成長に貢献する「Lumada事業」を拡大しています。協創のためにデータを利活用するわけですが、協創とは価値だけでなく、同時にリスクも共有することだと考えます。

万全と思われる情報セキュリティも、サイバー攻撃はわずかな穴を突いてきます。そうさせないために必要なのは、スピード感と透明性です。協創のパートナーに抹茶アイスクリームをお出しする時に、辛いワサビを紛れ込ませてはいけません。

### — 抹茶アイスクリームにワサビ! それはセキュリティにおける何を意味するのでしょうか。

ビジネスには決して隠し事をしてはいけない側面があります。こと情報セキュリティにおいてはお互いに隠し事をせず、透明性をもって臨まなくてはなりません。不都合なことでもオープンにすることが重要です。若いころ、私は調達部に所属し、海外赴任もして多種多様なビジネスパーソンと仕事をしてきましたが、ビジネスの推進力は人と人との信頼であることを実感してきました。

協創における情報セキュリティを、確かなものにするのも信頼だと思います。

### — 日立グループではグローバル規模での大型M&Aが加速していますが、情報セキュリティの観点で留意するポイントは何でしょうか。

M&A推進に伴うシステム統合によって思わぬセキュリティリスクが生じる場合があり、情報セキュリティレベルの維持は極めて重要な経営リスクであると言えます。システム統合を行ってから対策をスタートするのでは遅いのです。統合の前に、相手企業の状態をしっかりと把握しておく必要があります。

リスクというものは、一見小さな穴かもしれませんが、そこで何事か起きると相手企業のみならず、日立グループ全体、お客さま、さらには、社会にまで影響を及ぼします。ですから、新しく日立グループの一員になった会社には、事前にヒアリングしたり、対策をお願いしたり、場合によっては現地へ赴いて確認することも必要になってきます。同様にサプライチェーンについても、外部の委託先企業の不正アクセスによって機密情報が流出することなどがないように、一枚岩となってセキュリティを構築する必要があります。

### — ますます激しさを増すサイバー攻撃に対して、防御策としてどんなことが必要でしょうか。

2021年度に入って、ランサムウェアを用いた企業脅迫の事例が頻繁に起きています。そして、その攻撃は、ますます高度化し、巧妙化しています。私たちとは異なる価値観をもって、こういった攻撃が常に社会や企業に対して行われているということを、改めてしっかり認識することが重要です。その存在を認めただけで、こちらの懐を深くして、対策をとっていく。どれだけセキュリティシステムの堅ろう性を上げても、高度化、巧妙化された





攻撃を100%は防げないと考えておく必要があります。「完璧」な情報セキュリティ対策はもはや存在しない。セキュリティインシデントは常日頃発生するものであるとの認識を持つべきであると考えます。従って、我々がなすべきことは、徹底した監視と多様な対策を取りつつ、万一の際にはできるだけ短い時間で回復する抵抗力、サイバーレジリエンスを身に付けていけるような取り組みを常日頃から行っていくべきであると考えています。

#### — 人の意識の隙やぜい弱性が狙われるデジタル環境で、切り札として期待するものは何ですか。

切り札は、従業員一人ひとりの自発性だと思っています。長期にわたるコロナ禍でのリモートワークを通して、従業員の方々のセキュリティ意識は高まっています。また、製造に携わっている方々、現地で工事に携わっている方々、お客さまの横で常に働いている方々を含め、あらゆる場面での職場の意識を向上させようと活動を立ち上げて、先頭に立ってけん引してくれる人も増えてきています。情報セキュリティの担当者だけでなく、職場ごとにリーダーが生まれてくるのが理想です。かつて、「日立工場」の大火事を二度と起こすまいと職場消防隊が発足し、現在もその意志を受け継ぎ、日立のあらゆる拠点には自衛消防隊が存在します。同様に、各職場に「職場セキュリティ消防隊」のような存在が生まれ、自発的に情報の安全を見守って、何かが発生した際にはいち早くイン

シデント発生を通報するような文化が根付けば、日立グループの情報セキュリティは大きく飛躍することになるでしょう。

#### — 今後の日立グループとしての方向性と決意をお聞かせください。

近年のサイバー攻撃はますます高度化・複雑化しており、一社だけで対策するのは限界があると感じています。他企業の責任者の方々と話をしても、皆さん、同じ課題を持っていらっしゃる。そろそろ、会社間の垣根を越えた、情報セキュリティのコミュニティづくりを推進する段階かもしれません。これまでも一部で行っていましたが、点と点、線だったものを面で展開するようなダイナミックなつながりが必要です。

サイバー攻撃は業界にかかわらず、ぜい弱なところに入ってきます。利害ではなく、善悪の関係を構築するコミュニティづくりを、私たち日立グループがリーダーシップを取って進めていきたいと考えています。



## 社会の変化に対応した サイバーレジリエンス向上に向けて

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かたも大きな変革が必要となってきています。そして、セキュリティの脅威は、今まで以上に標的型攻撃は高度化、多様化し、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。

### 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。  
ゆえに、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、更には、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

### ●ゼロトラストセキュリティにむけた取り組み:統制

日立グループでは、過去からの取り組みに加え、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、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、いま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は、「認証」「エンドポイント」「サイバー統合監視」が重要な要素になってきます。



## 認証

昨今のクラウド利用において、多要素認証のないクラウドシステムは、不正アクセスを受ける確率が非常に高くなっています。そのために、クラウドベースでの認証のありべき姿を考え、特権管理強化、個々のユーザの認証強化を推進しています。

## エンドポイント

パソコンやサーバー、スマートフォンだけでなく、クラウドシステムやアプリケーションまで含めたトータルシステムとしてのエンドポイント強化を目標に取り組んでいます。2020年度においては、日立グループ全体でPC端末へのEDRの導入を推進しました。また、併せて、ネットワー

クゲートウェイやデータそのもののセキュリティを含め、検討を推進しています。

## サイバー統合監視

これまでは境界型のネットワークにおける各種ログを分析・対応を中心に行ってきました。今後は、クラウド、エンドポイント等あらゆるログを収集・相関分析し、インシデント対応をしていく必要があります。そのために、いままでのサイバーセキュリティ監視を発展させた監視システムおよび体制の検討を開始しています。

## ●セキュリティエコシステム構築に向けた取り組み:協創

一般的にはセキュリティというとIT部門との連携と思いがちですが、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となってきます。また、セキュリティ対策の対象範囲が拡大しているなか、モノづくり部門や品質保証部門、調達部門等ともしっかりとした連携をしないと、これらの対応はうまく機能しません。WannaCry以降、会社一丸となってサイバー脅威へ対抗するために、このようなセキュリティエコシステムの構築が重要と考え、推進しています。このエコシステム構築の要素となるのが、「モノ」「人・組織」、「社会」が「つながる」という考え方です。

### モノが「つながる」

DXにおいて、もたらされる新たな付加価値の創出や社会課題の解決を実現するために、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。これに対し、日立は、あらゆる環境において網羅的なサイバーセキュリティ対策に取り組んでいます。

### 人・組織が「つながる」

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には、異なる組織が相互に協力して対策を推進することが必要になります。「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行い、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、人・組織が「つながる」活動を推進しています。

### 社会が「つながる」

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国、学校、企業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きます。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マネジメントサイクル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きます。

## 社会の変化に対応した サイバーレジリエンス向上に向けて

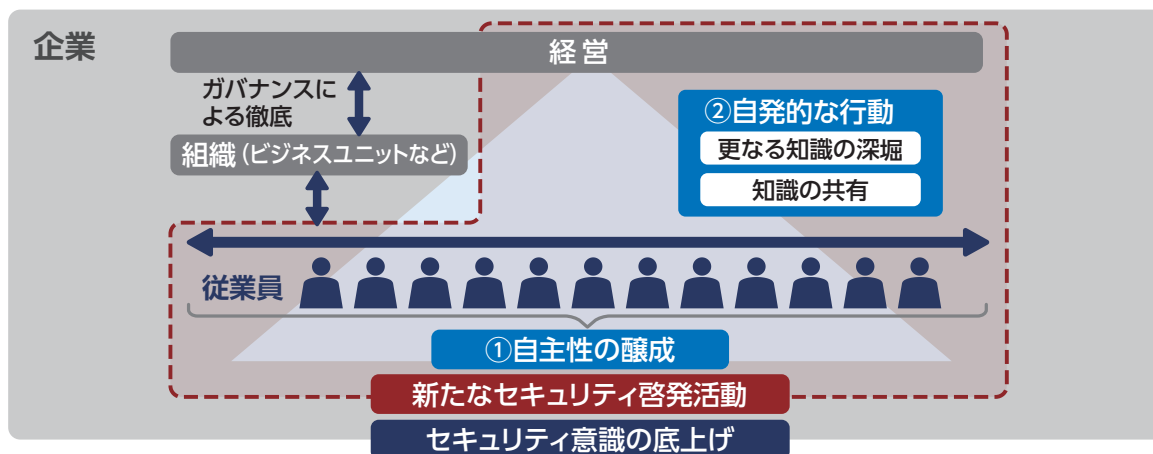
### ●新たなセキュリティ啓発に向けた取り組み:自分ゴト化

昨今の新型コロナウイルス感染拡大によるテレワークの中心の働き方においては、「セキュリティ意識の脆弱性」が狙われることが想定されます。オフィス以外で仕事をするにより、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しました。これは、セキュリティを義務感ではなく、自ら興味をもってもらい、従業員が心から共感し、自分ゴトとして

取り組むことをめざすものです。2020年12月より、従業員がセキュリティを身近に感じて、まず、自発的に触れてもらうための社内コミュニケーションの推進をしています。そして、2021年5月より、従業員が自発的に知識の取得や深堀をし、従業員同士が共有することできるような活動の場として、社内コミュニティ活動をスタートしました。

### 従業員の自主性の醸成と自発的な行動 → セキュリティ意識の底上げ



日立では、自社における「統制」をしっかりと行うとともに、社外への活動などを通し、産・官・学が「協創」した社会全体でのセキュリティエコシステムの構築を進めていきます。また、組織を守る大きな砦をつくるために、「自分ゴト化」を推進し、従業員一人ひとりがセキュリティを正しく理解し、あるべき姿に向かって働くことができる意識づくりをめざします。これら「統制」「協創」「自分ゴト化」を実現することで、新しい日常をより安全・安心で快適に過ごせるように、また、そこに潜むリスクを回避できるように、日立はサイバーレジリエンスの向上に取り組んでいきます。



# 情報セキュリティガバナンス

## 情報セキュリティガバナンスの基本的な考え方

IoTの進展により、さまざまなモノがつながることで、新たな価値が生まれています。その一方で、日々巧妙化するサイバー攻撃の対象も従来のITからモノのインターネットといわれるIoTや、制御・運用技術であるOTの分野にまで広がっています。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を最小化するため、情報セキュリティにかかわるリスクマネジメントは、

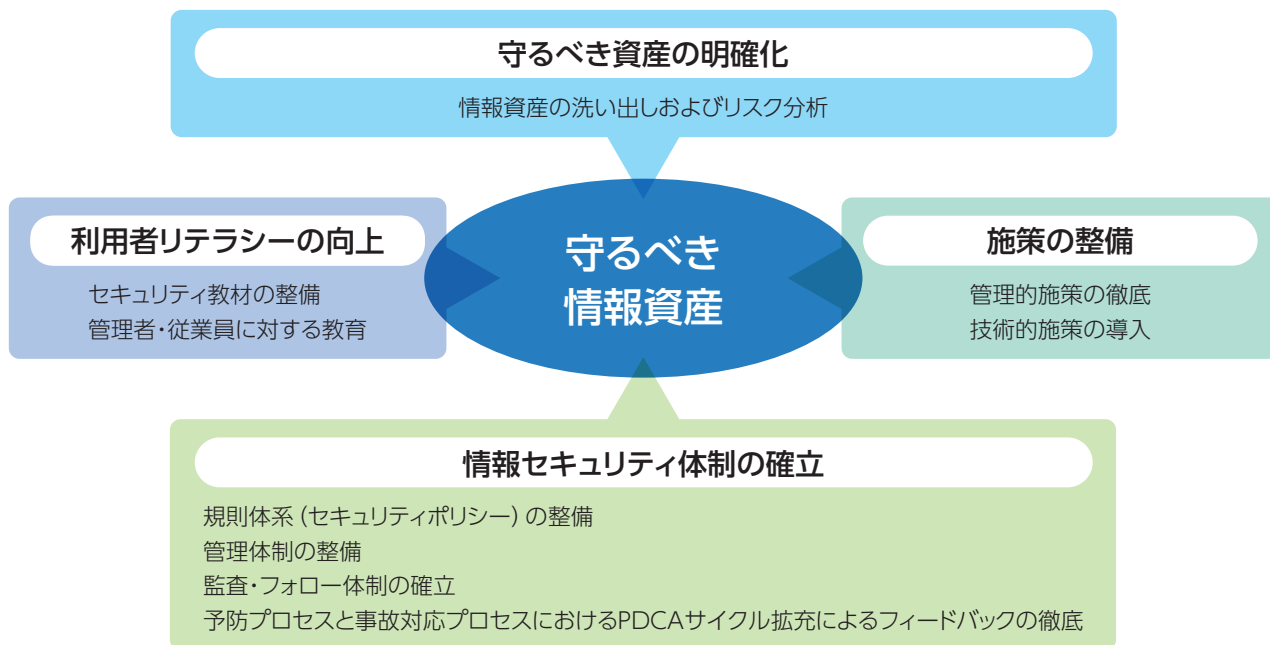
企業の最重要の課題の一つとなっています。

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付け、情報セキュリティのガバナンスに取り組んでいます。

## 情報セキュリティの取り組み

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、事故は「必ず起こるもの」という前提に立ち、4つの観点で情報セキュリティに取り組んでいます。また、日立製作所

主導により、日立グループの情報セキュリティマネジメントシステムのPDCAサイクル（継続的改善活動）を推進し、世界各国の日立グループでセキュリティレベルの向上に取り組んでいます。



# 情報セキュリティマネジメント

日立の情報セキュリティに関する方針、推進体制、規則、マネジメントサイクルなどの概要について紹介します。

## 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ひとつと認識し、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。





## 情報セキュリティマネジメント

### 情報セキュリティ規則体系

情報セキュリティの方針に基づき、下表の規則を定めています。  
また、グループ会社も同等の規則を定め、情報セキュリティを推進しています。

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
	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

#### ●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。「情報セキュリティ対策基準」は従来の規則に対してNIST SP800を元に全面見直しを行いサイバーセキュリティ対策を強化しています。

「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]啓発・モニタリングを行い、[Action]継続的改善を通じて、半年サイクルで実行します。





## 情報セキュリティに関する教育

### ●情報セキュリティ教育

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事が重要です。

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4万人が受講し、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。

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。

分類	対象者	内容
全従業員教育	<ul style="list-style-type: none"> <li>・全従業員</li> <li>・派遣社員</li> <li>・出向受入者</li> </ul>	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
	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

情報システムや情報セキュリティに携わるより専門的な教育については「セキュリティ人材育成の取り組み」に記載しています。

### ●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

開始しております。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。

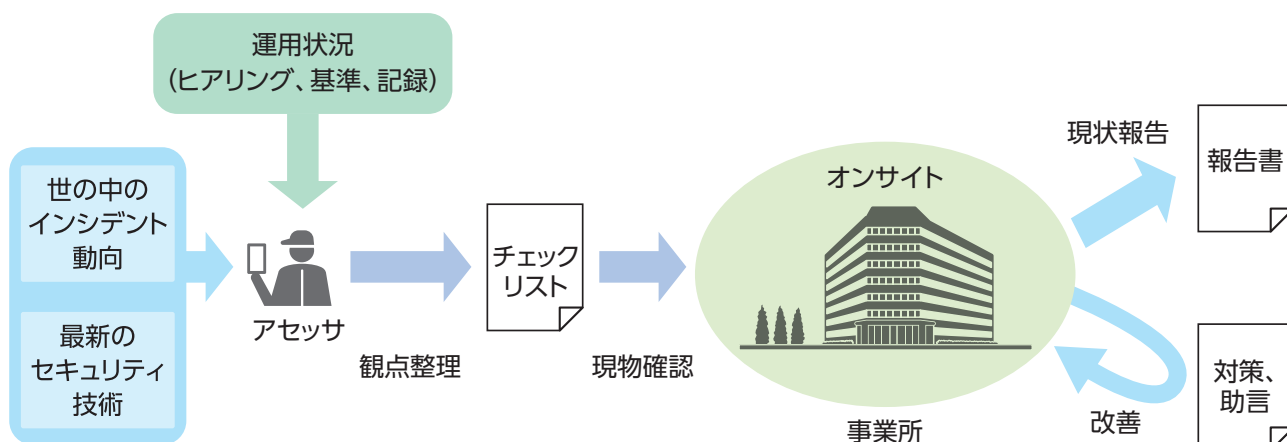
## オンサイトセキュリティリスクアセスメント

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機器などの設置や利用環境も多様である一方で、インターネット接続やリムーバブルメディア（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し有効な対策の提言



2017年度より、延べ約120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抽出し、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。

2021年度も新型コロナウイルスの影響によって現場確認ができないため、リモート確認を併用したアセスメントを実施しています。

# 日立グループにおけるCSIRT活動

日立インシデントレスポンスチーム (HIRT:Hitachi Incident Response Team) 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) 組織です。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

な視点で押し量り、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もち、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

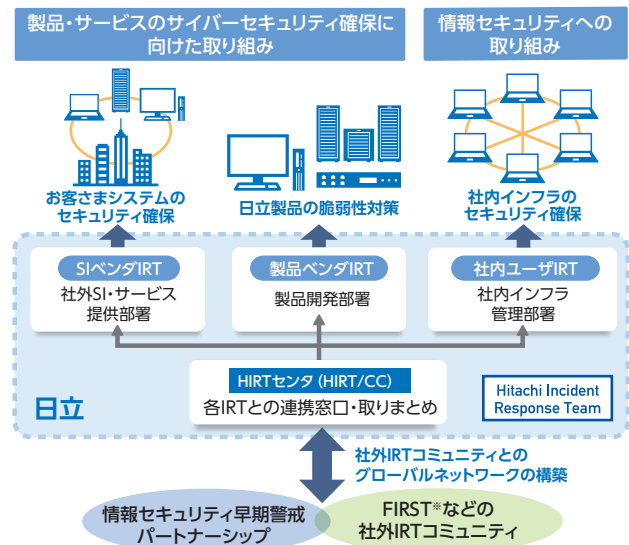
HIRTの役割は、「脆弱性対策:サイバーセキュリティに脅威となる脆弱性を除去するための活動」と「インシデント対応:発生しているサイバー攻撃を回避ならびに解決するための活動」を通じて、「組織単体活動:自身の企業情報システムを対象とする『情報セキュリティへの取り組み』」と「組織連携活動:お客さまの情報システムや制御システムを対象とする『製品・サービスのサイバーセキュリティ確保に向けた取り組み』」の視点から、日立のサイバーセキュリティ対策活動を支援していくことにあります。さらには、「次の脅威をキャッチアップする」過程の中で早期に対策の展開を図ることによって、安全・安心なインターネット社会の実現に寄与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

HIRTは、脆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センター) 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。



分類	役割
HIRT/CC*	該当部署:HIRTセンター 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間の連携を通して脆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 公開された脆弱性について、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脆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 公開された脆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、日立製品の脆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脆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



# 日立グループにおけるCSIRT活動

## HIRTセンターが推進する活動

HIRTセンターの活動には、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・グループ会社への脆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<sup>※1</sup>の推進などを通じて、脆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サイトに関する脆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。

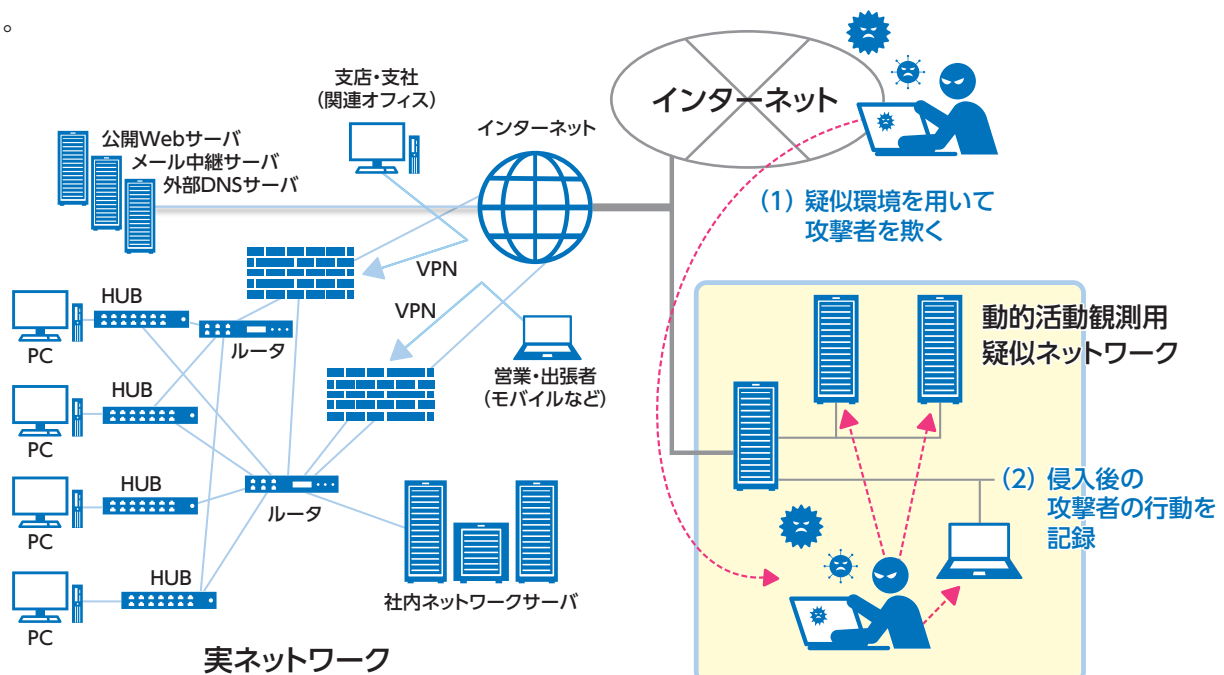
#### (3) 製品・サービスのセキュリティ技術の向上

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

#### (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<sup>※2</sup>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脆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<sup>※3</sup>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 (脆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<sup>※4</sup>、米国国土安全保障省のAIS<sup>※5</sup>などを用いた情報利活用基盤の整備を推進しています。

※4 STIX: Structured Threat Information Expression

※5 AIS: Automated Indicator Sharing

#### (3) 研究活動の整備

マルウェア対策研究人材育成ワークショップなど学術系研究活動への参画を通じて、人材育成の場の醸成、専門知識を備えた研究者や実務者の育成を推進しています。

### ■ Hitachi Incident Response Team

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

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

# サイバーセキュリティ対策

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

## セキュリティ監視・インシデントレスポンス強化

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

### ●セキュリティ監視

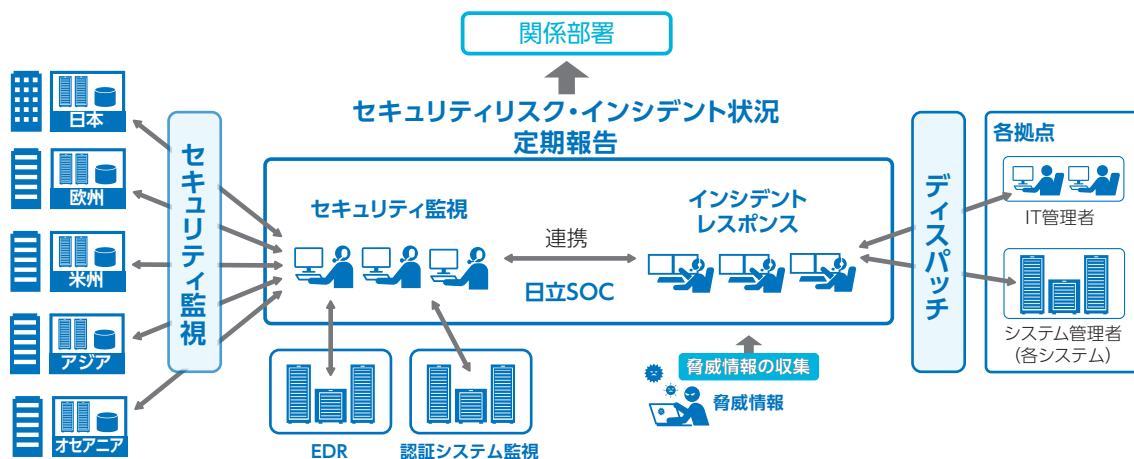
日立グループでは、グローバルにおいて対象とするシステムおよびネットワークの監視ポイントを定め、ログの連携・分析・監視を行っています。2017年より監視対象を拡大しており、グローバルの基幹拠点すべてをカバーしています。また、EDR(Endpoint Detection and Response)の導入により、機器の動作監視や調査・対処も可能となりました。これにより、EDRと基幹拠点からのログを組み合わせることで分析することが可能となり、精度の高い効率的な

監視を実現しています。

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

### ●インシデントレスポンス

日立グループでは、インシデント発生時に備えた対応手順、連絡体制を整備しており、インシデント発生時には、迅速に原因究明や影響範囲の特定、事態の収束を行っています。2020年からは、基幹拠点のログ監視とEDRによる調査を組み合わせることで、より迅速にインシデントの詳細を把握することを可能としています。これにより、対応優先度や対応要否の判断も行うことが可能となり、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対処することが出来ました。また、インシデントレスポンスから得られたノウハウを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。





### 脅威情報の収集・分析と警戒情報の配信

日立製作所では、社内で利用している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・分析と、警戒情報の配信を行っています。

この活動は、グループ会社とも連携して推進しています。

#### ●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脆弱性・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などの社外団体の発信サイト
- ・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

収集した情報については、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のほか、CTIサービスを利用して配信対象の選定と3段階の警戒レベルの判定を行っています。また一部の脅威に関しては、模擬環境での検証作業を通して社内システムへの影響や対策・被害調査に寄与する情報を整理し、対策活動に活用しています。

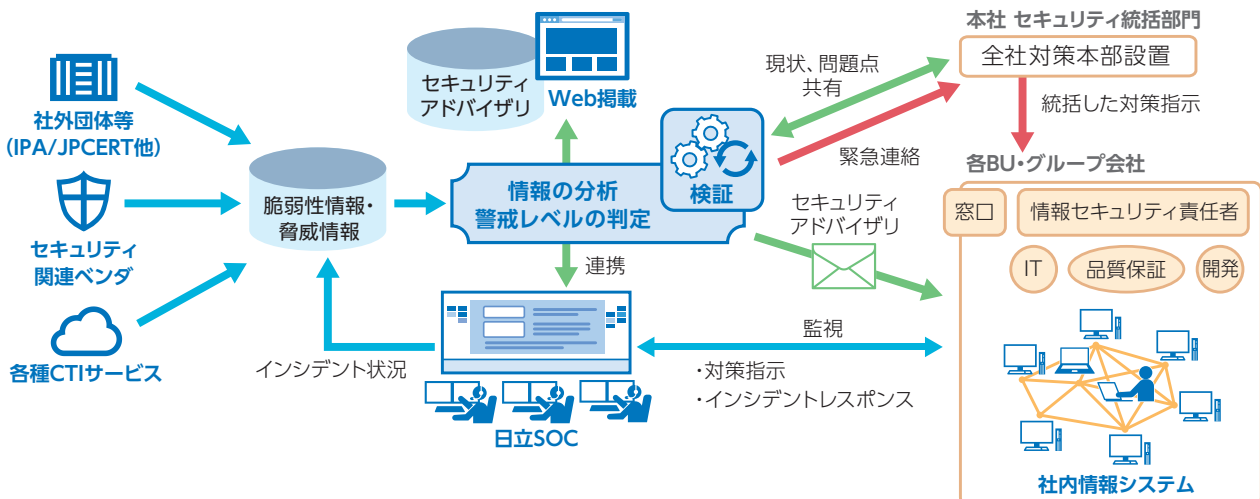
#### ●警戒情報の配信

収集した情報は、警戒レベルに応じ、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、セキュリティアドバイザリとして注意喚起を促すとともに、必要に応じてサイバー警報を発報して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・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連携し、対策確認・監視強化へ活用しています。

これらの活動の積み重ねから、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(コーポレート)セキュリティ統括部門と連携のうえ、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、統括したセキュリティ対策指示を行います。



# グローバル情報セキュリティの取り組み

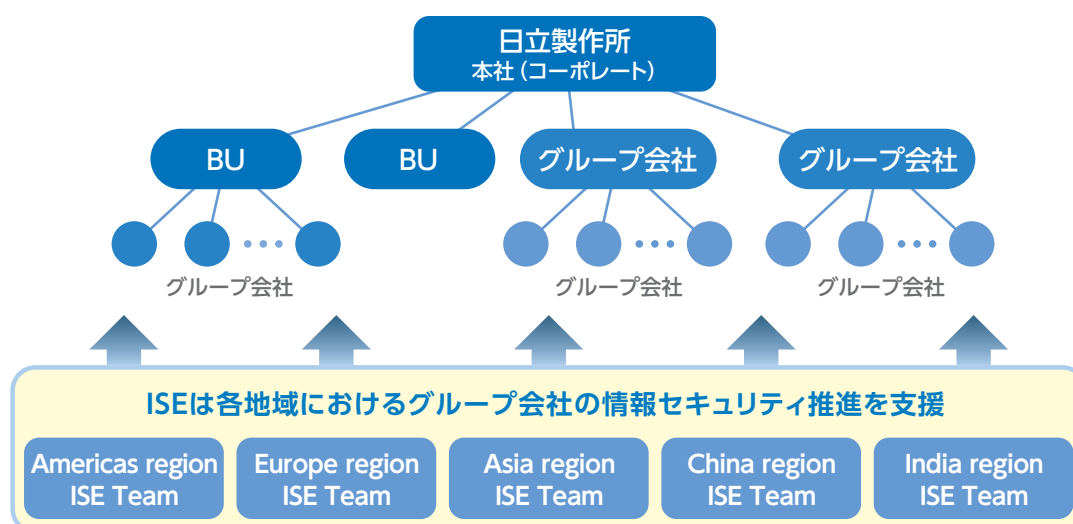
グローバルビジネスの拡大に伴い全世界の日立グループにおいて、情報セキュリティの取り組みが重要となっています。日立では、セキュリティ施策の確実な遂行に向け、グローバルセキュリティにおけるガバナンス浸透を向上させるべく、各地域に情報セキュリティエキスパートを設置し、グローバルガバナンス強化に取り組んでいます。

## グローバルセキュリティガバナンス

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。2021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によるガバナンス強化活動

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。

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を開催し、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。

### 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
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
3. 各地域におけるセキュリティコミュニティの確立
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
5. 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
6. 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

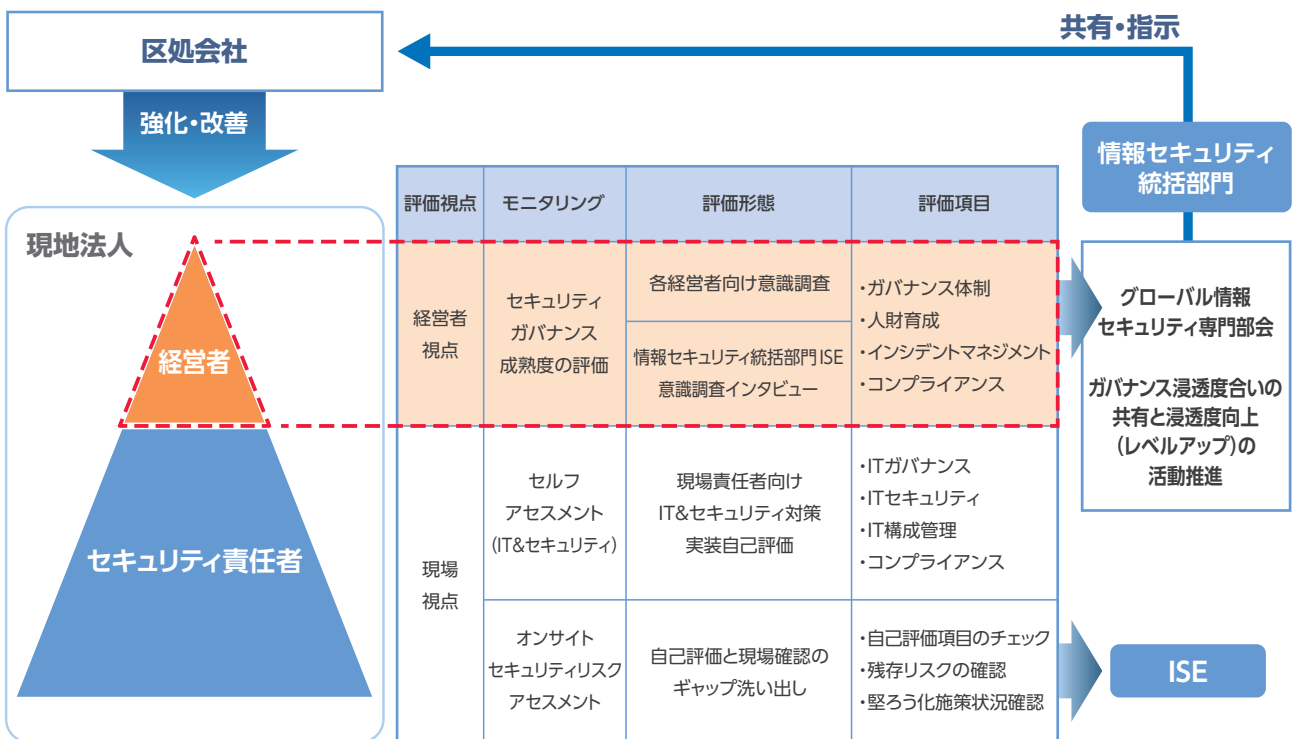
経営者意識調査の実施

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おります。



サーベイ結果の可視化とPDCA活動

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

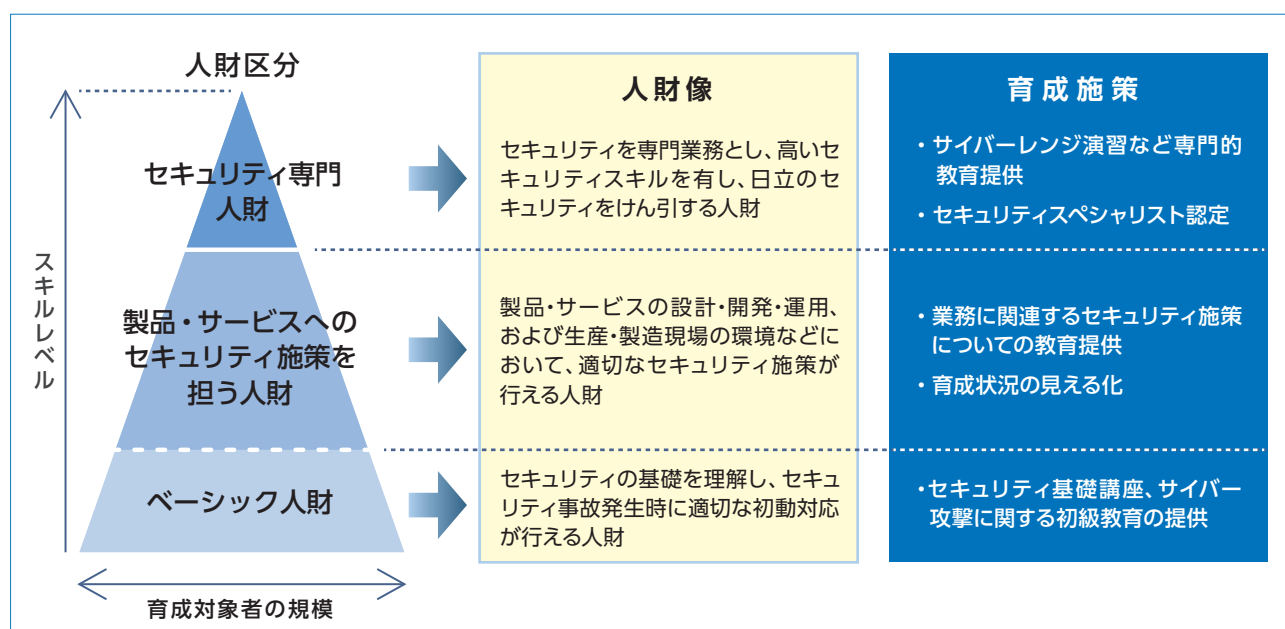
活動立案 (Plan)、実施 (Do)、確認 (Check)、評価・改善 (Action) の指標としても有効利用を図っています。

# セキュリティ人材育成の取り組み

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、人材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。

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材へのセキュリティ観点での育成を推進しています。育成する人材は、右の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材育成を進めています。

- 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材
- 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材
- 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材



セキュリティ専門人材向けには、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材間の情報共有・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材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材を発掘・育成・評価し、これまでに1,300名を超える人材を認定しています。製品・サー

ビスへのセキュリティ施策を担う人材とは、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材です。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材の育成です。また、生産・製造の現場にフォーカスしたセキュリティ人材の育成も重要です。これら人材に対しては、社内規定などで示されたセキュリティ施策の理解を促進するための教育を提供しています。製品・サービスの設計・開発と生産・製造現場はそれぞれ安全を確保しつつお互いに悪い影響を及ぼさぬよう環境を構築・運用しなければならないため、IT/OTに関わるセキュリティ対策を実施するためのさまざまなスキルアップに取り組んでいます。



ベーシック人材の育成は、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材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。ベーシック人材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名を超える人材が受講をしています。また、さら

なる導入教育が必要な人材向けに、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。ベーシック人材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。

### 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脆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脆弱性による被害、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

# サイバーセキュリティマネジメントの取り組み

サイバー攻撃手法の多様化に伴い、インシデントの発生源や影響が拡大する中、こうしたリスクに対応するため、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。

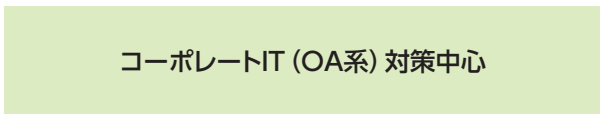
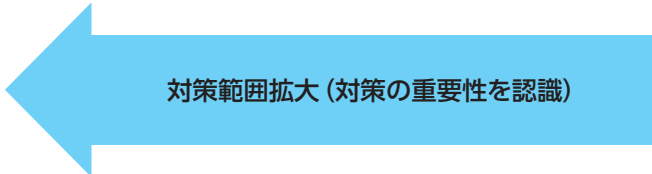
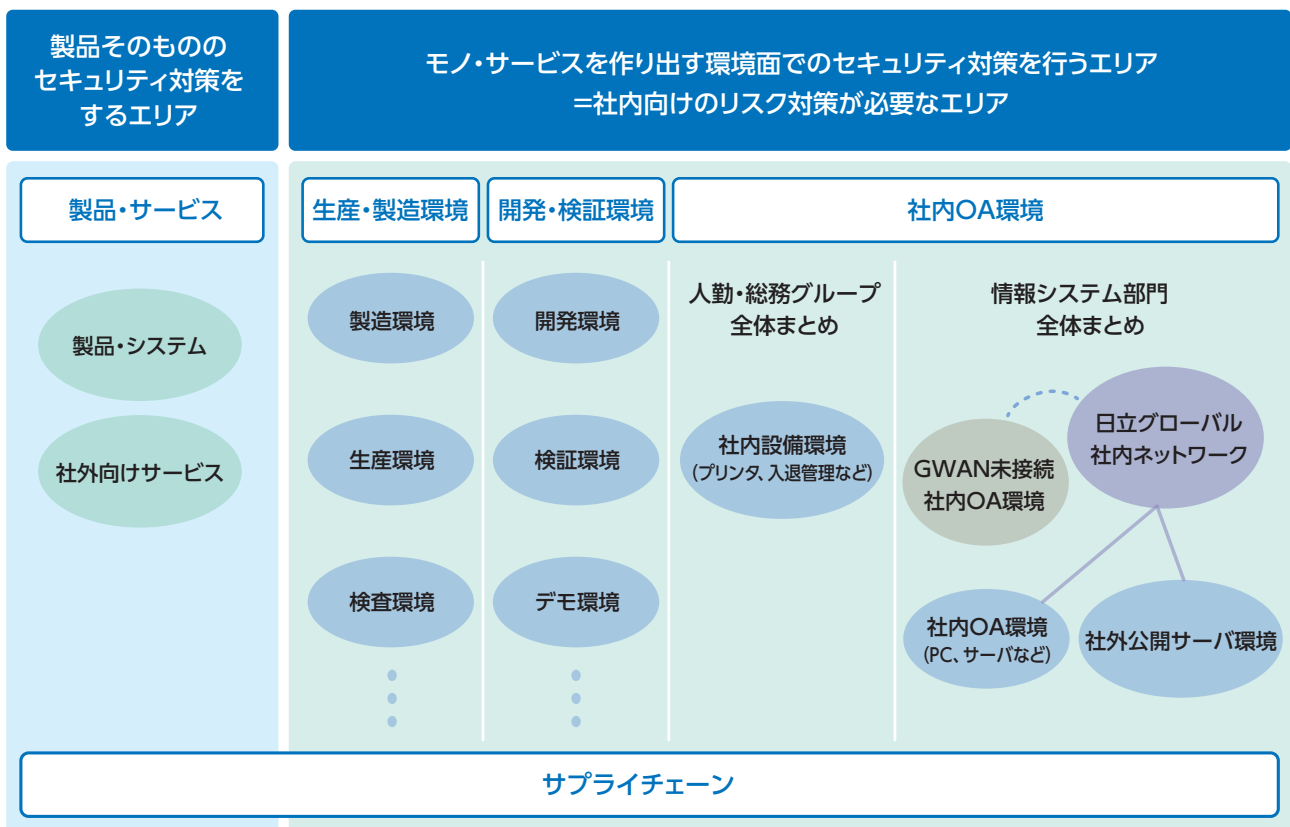
## 背景と目的

2017年5月、製造現場の検査機器がランサムウェア (Wanna Cry) に感染し、日立グループ全体に被害が拡大しました。

この教訓から、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。

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。



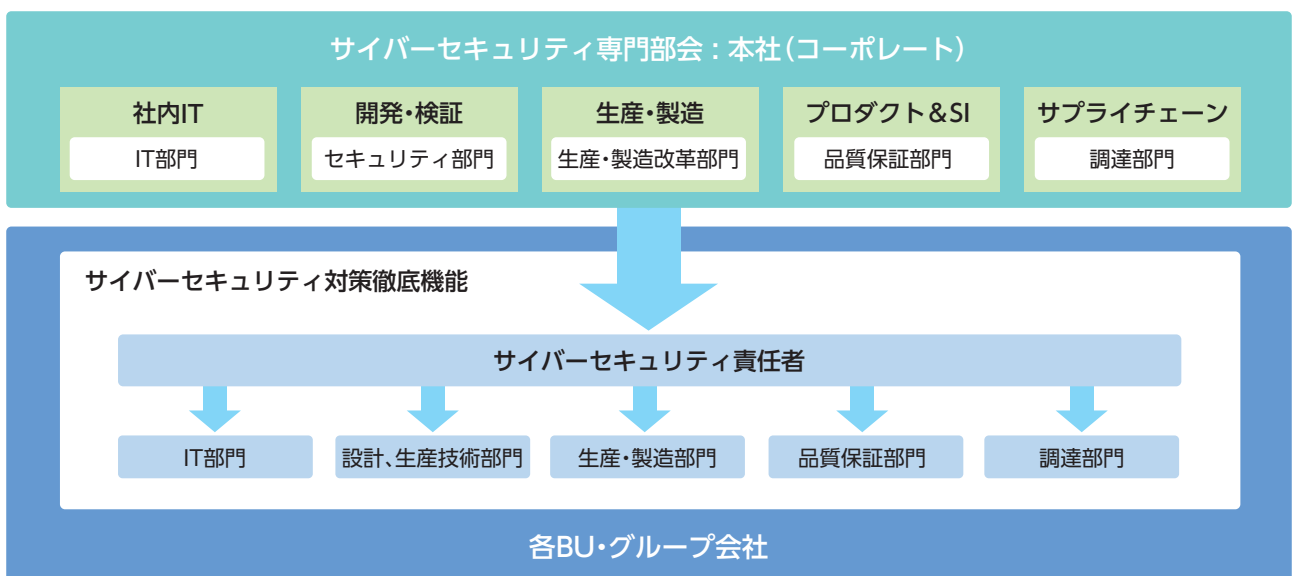
### 推進体制

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。



### サイバーセキュリティ対策の強化施策

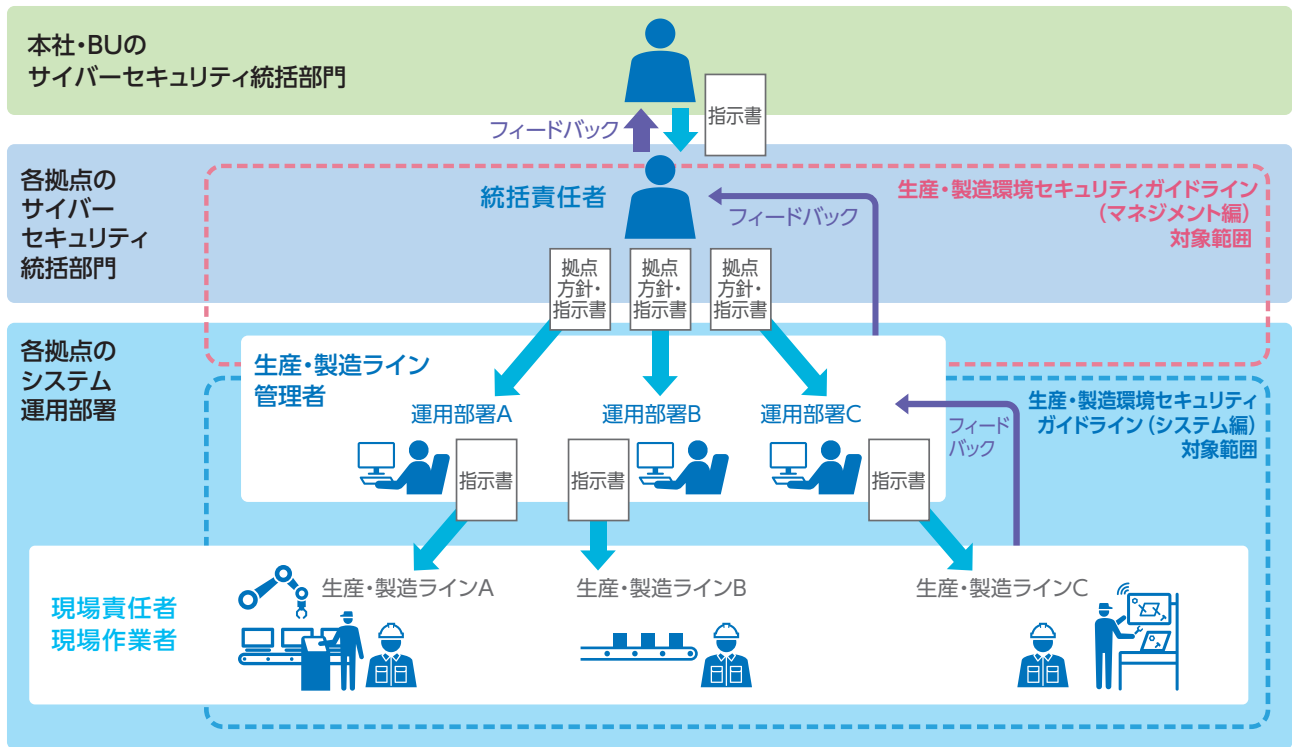
各領域のサイバーセキュリティ対策の強化について、下表の取り組みを進めています。

領域	対象部門	取り組み概要
社内OA	IT	・社内OA環境の接続・分離要求事項の策定と展開
開発・検証	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	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

# サイバーセキュリティマネジメントの取り組み

## ●生産・製造現場におけるセキュリティ強化の取り組み

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。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。

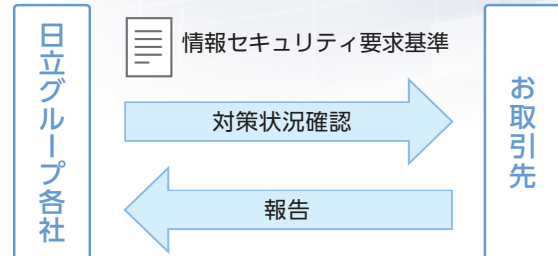


ガイドライン構成	内容	対象者
マネジメント編	マネジメント面（組織・人的管理面としての取り組み）として、組織体制の整備および、拠点全体・部署個別のセキュリティ運用・管理上ルールの策定と見直しについて記載。	サイバーセキュリティ統括責任者
システム編	「IEC62443-3-3」に基づき、現状把握と対策検討としてシステム構成およびその対策方法は、日立グループの代表的なモデルを用いて記載し、各部門・各部署でカスタマイズして利用する。	生産・製造ライン管理者 現場責任者 現場作業員



● サプライチェーンにおけるセキュリティ強化の取り組み

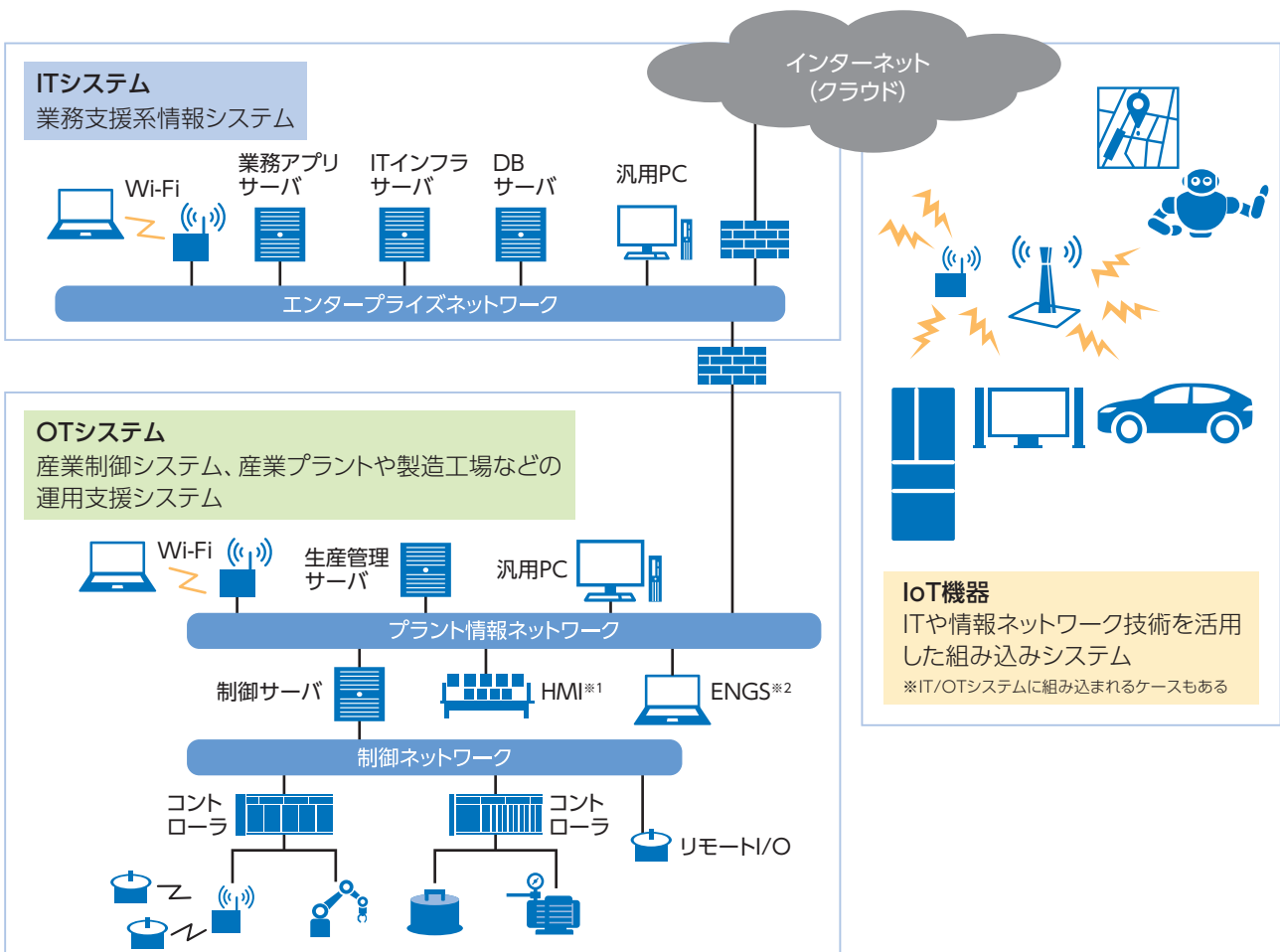
業務を委託する際には、あらかじめ日立が定めた情報セキュリティ要求基準に基づき、お取引先の情報セキュリティに関する対策状況を確認、審査しています。この情報セキュリティ要求基準には、昨今のサプライチェーンに対するサイバー攻撃に対するセキュリティ対策の項目を付加した「情報セキュリティガイドライン」を追加し、日立の情報セキュリティに関する要求を具体的に示し、お取引先へ確認頂いています。



製品・サービスに関するセキュリティの取り組み

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。



※1 Human Machine Interface ※2 Engineering Station

## サイバーセキュリティマネジメントの取り組み

### ●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。

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渡るセキュアプロセスの実装を推進しています。

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等を整備する。
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。

### ●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等について、セキュリティ対策が先行している部門の取り組みを実践事

例として、日立グループ全体でノウハウの蓄積と共有を図っています。

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



### ●製品・サービスのセキュリティ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とっています。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、ランク付けの指標を定義し、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とることを促すだけでなく、リスクとコストのバランスの考慮にもつながります。またそのプロセスは、日立において標準化されている情報システム開発プロセスとも連携した内容となっています。規則化されたセキュリティマネジメントプロセスの内容は、定期にまたは必要に応じて随時に改訂されます。これは、発生したインシデント、顕在化したリスク、運用した結果などからのフィードバックに基づき実施され、マネジメントプロセスがより適切なものになるよう継続的な改善を行うことを目的としています。

#### (3) セキュリティ人材によるレビューの制度化

製品・サービスがセキュリティリスクに対応できていることを確認し、セキュリティ品質を確保することを目的として、開発運用プロセスの各工程でのセキュリティ人材による専門的観点でのレビューを制度化しています。インターネットに接続している製品・サービスを対象に、各事業部門で育成し、事業部門の長が任命したセキュリティ人材が事業部門の代表としてレビューを実施します。これにより、セキュリティが確保された製品・サービスを開発し、お客さまに提供しています。

#### (4) 脆弱性点検の実施

脆弱性攻撃による被害の抑止を目的に定期的脆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、脆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) 脆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

脆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脆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。

# 個人情報保護に対する取り組み

デジタルテクノロジーの進展に伴いデータの利活用が急速に進む中、個人情報保護への関心も高まっています。EUをはじめ130以上の国と地域が個人情報に関する権利保護を目的とした法律を制定しています。

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」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

### 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。

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。

## 個人情報保護方針

日立製作所は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。  
(<http://www.hitachi.co.jp/utility/privacy/index.html>)

### ●個人情報保護に関する当社の考え方

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は

めざまざまな情報を取り扱っております。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参りました。



●個人情報保護方針

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

当社は、役員および従業員に個人情報保護の重要性を認識させ、個人情報を適切に利用し、保護するための個人情報管理規則を策定し、個人情報保護マネジメントシステムを着実に実施します。更に、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共に、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) 安全対策の実施並びに是正

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則り、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等の対策を実施し、個人情報の漏洩、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、誠意をもって対応します。

個人情報保護カード

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。

**(株)日立製作所**  
個人情報保護に対する当社の考え方



**HITACHI**  
Inspire the Next

制定日 2005年4月 1日  
改定日 2010年4月 1日

株式会社 日立製作所 代表執行役 執行役社長  
東原 敏昭

株式会社日立製作所(以下「当社」という。)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はじめ様々な情報を取扱っている。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きた。このような経緯を踏まえ、当社における個人情報保護について、規則の制定及び管理体制の確立を図ると共に、個人情報保護方針を定め、役員及び従業員に周知させるとともに、一般の方が、容易に入手できる措置を講じるものとする。そして、この方針に従い個人情報の適切な保護に努める。

---

**(株)日立製作所 個人情報保護方針**

- 1. 個人情報管理規則の策定及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、役員及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する。更に、維持し、継続的に改善していく。
- 2. 個人情報の収集・利用・提供及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共に、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扱う。また、目的外利用は行わない、及びそのための措置を講じる。

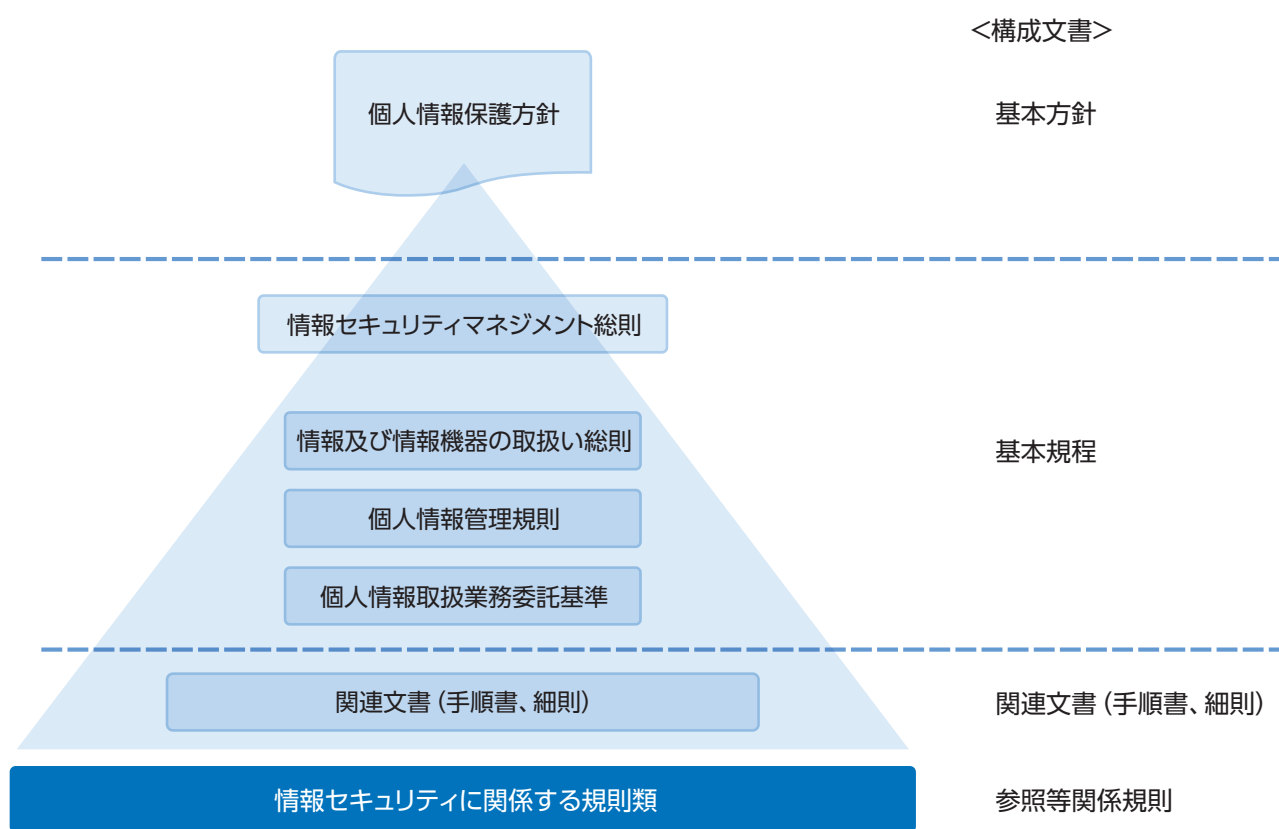
## 個人情報保護に対する取り組み

### 個人情報保護体制

個人情報保護に関するビジョンを実現するため情報セキュリティに関する全社体制を構築しています。詳細は「情報セキュリティ推進体制」をご参照ください。

### 個人情報規則体系

日立が取得、お預かりした個人情報は、個人情報保護規則する規則群に従って、適切に管理いたします。



### 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、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、63条で規定される個人情報管理規則および12条で規定される個人情報取扱業務委託基準、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。(「個人情報の管理と適切な取り扱い」を参照)

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。(「個人情報保護に関する監査」を参照)

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。

- 日立個人情報保護マネジメントシステム (PMS) の着実な実行
- PDCAを回し、定期的見直し、継続的改善を実行



## 個人情報保護に対する取り組み

### 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。

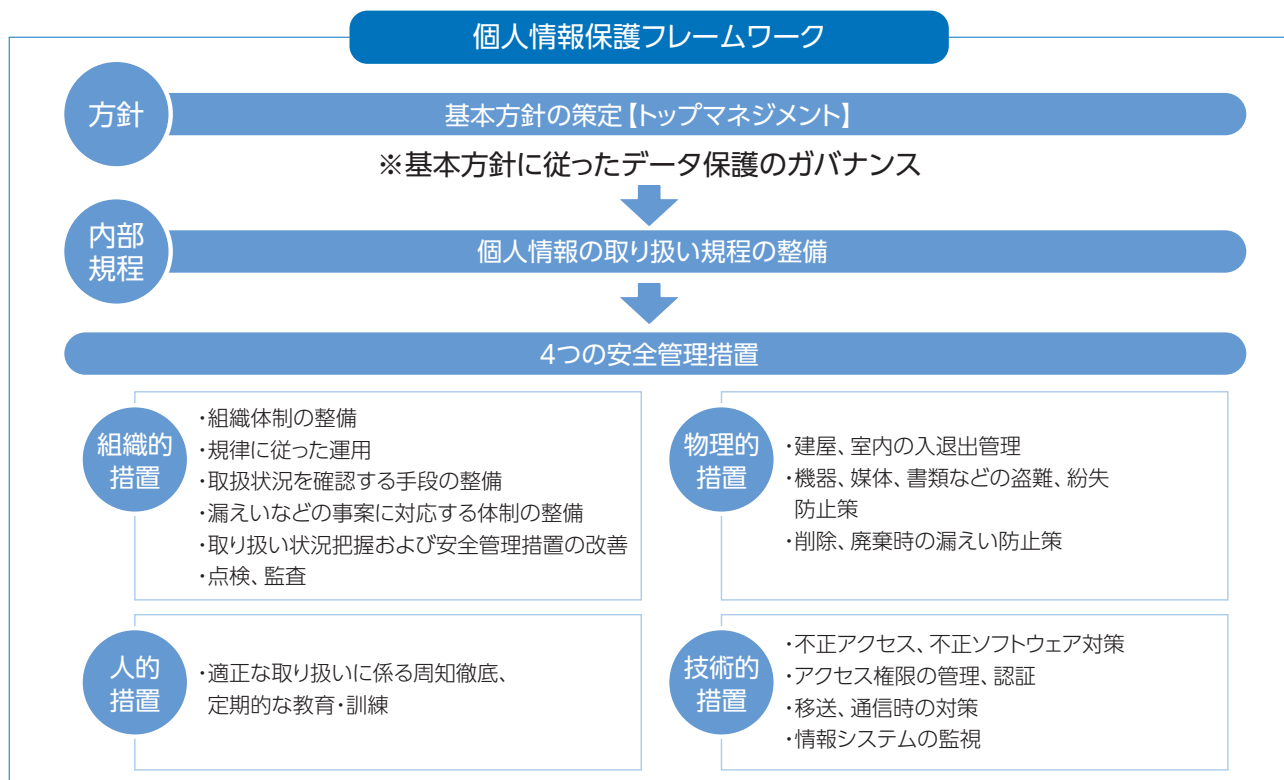
組織的安全管理措置では、個人情報保護責任者を設置し、個人情報保護体制を整備しています。（「個人情報保護体制」を参照）

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。（「個人情報保護に関する教育」を参照）

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。

### マイナンバー制度への対応

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

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。

日立製作所を含む国内の全グループ会社(153社)については、日立製作所と同等の監査を実施し、その結果を日立製作所が確認しています。

情報セキュリティ監査では、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。

### 個人情報保護に関する教育

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。

詳細は「情報セキュリティマネジメント」の「情報セキュリティに関する教育」をご参照ください。

## 個人情報保護に対する取り組み

### 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うえで、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。欧州の地域統括会社、欧

州事務所を含む日立グループ全体で連携し、GDPRの適用を受ける業務の特定とそのリスク評価、リスクに応じた適切な安全管理措置の実行、全従業員を対象とした教育などを実施しています。

また、そのほか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。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、適切な対応を進めるため、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、海外グループ会社の個人情報保護のコンプライアンス対応を支援するため、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、2021年10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、2021年3月に8回目の付与的決定を受け、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<sup>けんざん</sup>を重ねています。



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/>)

※ 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 (2021年10月末時点)。

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

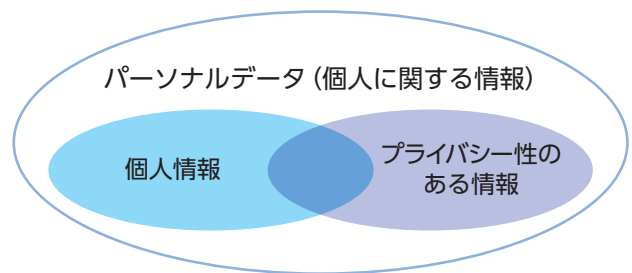
# プライバシー保護の取り組み

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、個人に関する情報がパーソナルデータと総称され、その利活用による価値創出が期待される一方で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、プライバシーにかかわるリスクも変化しています。右図に示す通り、パーソナルデータには、個人情報と一部重複して、「位置情報」や「購買履歴」などのプライバシー

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



## 日立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、IT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IT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。

### ●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、プライバシーにかか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2020年度だけで約220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。また、2020年度は、オフィスや商業施設での体温検知など、新型コロナウイルス感染症 (COVID-19) 対策感染対策を目的としてパーソナルデータを取り扱う業務が増加しました。このような新たな種類の業務に対しても、プライバシー保護対策を講じています。

### ●プライバシー保護教育

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



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。2020年度の調査では、パーソナルデータの利活用に関する期待と不安の比較において、不安が大きいと回答する層が減少し、期待と不安が「同じくらいである」と回答した中間層の割合が増加しました。また、パーソナルデータを利活用した新型コロナウイルス感染症 (COVID-19) 拡大防止対策が生活者から期待されているなど、昨今の社会情勢に起因すると想定される傾向が明らかになりました。人々の意識が多様化し、きめ細やかなプライバシー対策の必要性が浮き彫りになっており、これら生活者の意識の変化をプライバ

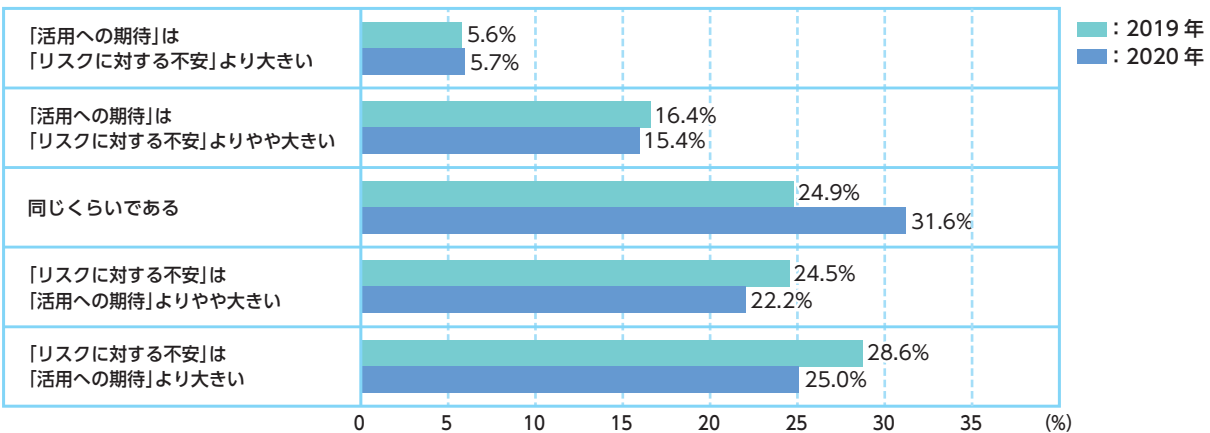
シー保護対策に反映しています。そして、本調査のような生活者の意識を継続的に調査し、施策の評価・改善に役立てる取り組みは、総務省と経済産業省による「DX時代における企業のプライバシーガバナンスガイドブック ver1.1」\*2においても重要であると記され、日立の取り組みが事例として取り上げられています。

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良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。

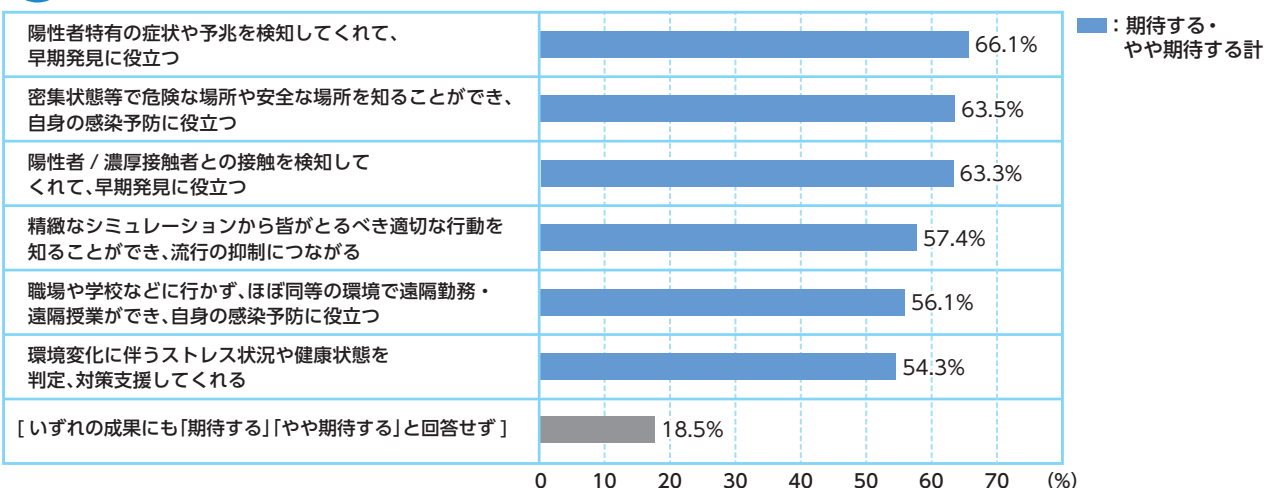
\*1 「第五回 ビッグデータで取り扱う生活者情報に関する意識調査」(2020年12月公表)  
<https://www.hitachi.co.jp/New/cnews/month/2020/12/1222a.html>

\*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ver1.1」(2021年7月公表)  
[https://www.meti.go.jp/policy/it\\_policy/privacy/guidebook11.pdf](https://www.meti.go.jp/policy/it_policy/privacy/guidebook11.pdf)

Q 企業や公的機関などによるパーソナルデータの利活用に関してどのように感じますか。「活用への期待」と「リスクに対する不安」のどちらが大きいとお答えください。



Q パーソナルデータを活用した新型コロナウイルス感染拡大防止対策について期待することは何ですか。次の想定される対策について、あなたの期待の度合いをお答えください。



# 情報セキュリティ実現のための研究開発

昨今のサイバー攻撃の高度化、巧妙化の進展、クラウドベースのITシステムの普及など、社会や企業を取り巻く環境は大きく変化しています。日立では、そういった変化が生み出す新たなセキュリティの在り方に寄与できるよう、さまざまな技術開発に取り組んでいます。特に、2020年度以降の新型コロナウイルス感染の拡大に伴うニューノーマルな働き方、生活様式への転換や定着化の中、注目されている非接触でセキュアな生体認証の技術開発を積極的に推進しています。

## コロナ禍で求められる情報セキュリティ技術開発の推進

新型コロナウイルス感染の拡大に伴い、ニューノーマルな働き方、生活様式への転換や定着化が求められています。キャッシュレス決済や手ぶらでの入退管理、リモートワーク、ハンコレス業務などの適用拡大に向け、非接触でセキュアな生体認証が注目されています。その一方で、取得された生体情報の漏洩・濫用への不安などが市場普及を阻害しているという課題がありました。

これに対し日立では、オープンネットワーク上にセキュアで便利な共通認証基盤を実現する公開型生体認証基盤

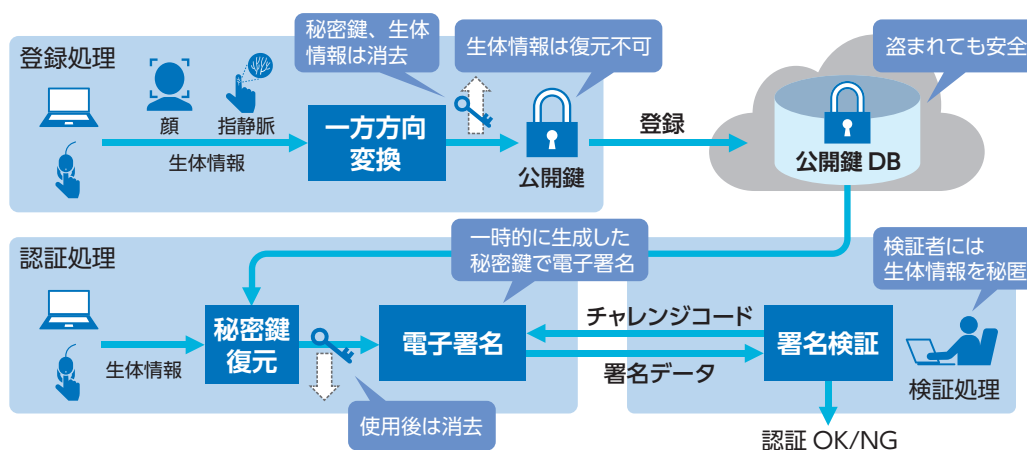
(PBI:Public Biometric Infrastructure)の研究開発と事業化を進め、2020年10月より「生体認証統合基盤サービス」として提供を開始しました。研究開発グループでは、コロナ禍で求められている非接触の指静脈認証装置や汎用カメラ指静脈PBI認証技術、PC内蔵カメラを使った生体認証で社内外のシステムへのアクセスを安全・便利に実現する顔PBI認証技術など、金融、ヘルスケア、オフィス、リテールなど様々な分野のニーズに応える生体認証技術の開発を進めています。

### ●公開型生体認証基盤 (PBI) 技術

公開型生体認証基盤 (PBI) は、生体認証に用いる静脈や顔等の生体情報を、元データに復元できない公開鍵の形に変換して登録し、生体情報を用いた電子署名により本人認証を行う仕組みです。電子署名は、公開鍵暗号基盤 (PKI※) に基づくもので、公開鍵とその持ち主の対応関係を保証する仕組みです。公開鍵暗号基盤 (PKI) では、クライアントの保持した秘密鍵による電子署名と、対応

する公開鍵による検証で本人認証が可能となります。

PBIでは、この秘密鍵を生体情報で置き換え、認証時にクライアント上で一時的に使用するのみのため、情報漏えいのリスクを極限まで削減することができます。本技術を用いることで、さまざまなデバイスで利用される生体情報をオープンなネットワークで安全に活用でき、多岐に渡る認証サービスが展開できるようになります。



公開型生体認証基盤 (PBI) の概要

※ Public key Infrastructureの略で、公開鍵暗号基盤。インターネットによる通信で、公開鍵暗号やデジタル署名を安全に運用する技術。

●非接触指静脈認証技術

指をかざすだけで、手ぶらで認証が可能な認証装置 C-1を開発しました。従来の指静脈認証装置は、安定した静脈パターンを取得するため、装置に指を載せ固定する必要がありました。そこで今回、新たに赤外と可視の反射光を用いた2波長同時照射方式を開発し、非接触の指を安定的に検出すると共に、同時に撮影する3本指の生体特徴を併用することで認証精度を向上しました。さら

に認証時には、圧縮した生体特徴により候補ユーザーを高速検索することで、数百万人規模のユーザーで使える手ぶらPBI認証を実現しました。これにより非接触でかつ大規模な登録者数に対応することが可能になり、手ぶらキャッシュレス決済などBtoBtoC向けに幅広く適用することが可能となります。

●汎用カメラPBI認証技術

非接触で低コストな生体認証方式として、PCの内蔵カメラ等を用いた汎用カメラPBI認証技術を開発しました。指静脈や顔情報を復元不可能な形に変換して認証に用いるため、安心して利用することが可能です。

システムのシングルサインオン、電子署名まで一連の本人認証をセキュアに行うことが可能です。

(1) 汎用カメラ指静脈PBI

PCの内蔵カメラや外付けカメラに指をかざすだけで本人認証が可能となる指静脈PBI認証技術を開発しました。汎用カメラを用いて指静脈認証をする上での課題は、可視光の画像から静脈パターンだけを安定的に抽出すること、かざされた複数指の位置を正確に検出して高精度に認証することです。前者については色情報を用いた静脈パターンの抽出技術を開発し、後者については深層学習を用いて自由背景に写る指領域を検出する技術を開発しました。また指静脈保護安全性を保ったままPBI照合を高速化する技術を開発し、汎用カメラ指静脈PBI認証技術を実現しました。これにより、PCや業務システムに適した環境上で、Windowsサインインから、業務シ

(2) 汎用カメラ顔PBI

PCの内蔵カメラに顔を写すだけで本人認証が可能となる顔PBI認証技術を開発しました。指静脈PBI開発で蓄積した生体認証セキュリティに関する知見と、深層学習に基づく最新の顔認証技術を融合させて、顔認証PBI認証技術を開発しました。さらに、多様な人種への対応、登録画像判定、高速推論といった課題の抽出と技術改良を行い、2020年9月に製品化しました。2021年7月には、PCを使って社内外システムへの安全で簡便なアクセスを実現する「Biometric Signature サインインソフトウェア」の提供を開始しています。自宅やサテライトオフィス、コワーキングスペースなど、オフィス以外の勤務でも、生体認証を使った高いセキュリティを低コストで実現することが可能となります。



日立指静脈認証装置 C-1



日立カメラ生体認証 SDK for Windows フロントカメラ



ニューノーマルな生活や働き方を支援する非接触の指静脈認証装置とPCカメラ向け生体認証ソフトウェア開発キット

# 情報セキュリティに関する社外活動

日立では、従業員それぞれの持つ経験や知識を生かし、情報セキュリティに関する各種社外活動に参画することにより、よりセキュアなIT社会の実現のために活動しています。

## 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) 等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) のひとつである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、脆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に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。2021年10月末現在で、98か国、598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作りなど、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。

## その他の活動

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

- 独立行政法人情報処理推進機構 (IPA) 10大脅威執筆委員会 ほか
- 一般財団法人日本情報経済社会推進協会 (JIPDEC) ISMS専門部会、制御システムSMS専門部会 ほか
- 一般財団法人日本サイバー犯罪対策センター (JC3)
- 特定非営利活動法人日本セキュリティ監査協会 (JASA)
- NPO日本ネットワークセキュリティ協会 (JNSA)
- 日本セキュリティオペレーション事業者協議会 (ISOG-J)
- デジタルトラスト協議会 (JDTF)
- 一般社団法人日本電気計測器工業会 (JEMIMA) PA・FA計測制御委員会、セキュリティ調査研究WG
- 技術研究組合制御システムセキュリティセンター (CSSC)
- 一般社団法人電子情報技術産業協会 (JEITA) 情報セキュリティ調査専門委員会 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

# 第三者評価・認証

日立では、情報セキュリティマネジメントに関する第三者評価・認証の取得を推進しています。

## ISMS認証取得状況

日立が、一般社団法人情報マネジメントシステム認定センター (ISMS-AC) から情報セキュリティマネジメントシステム国際規格 (ISO/IEC 27001) に基づくISMS認証を

取得した組織は、以下のとおりです (2021年9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 (サービス&プラットフォームビジネスユニット 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、Software CoE)
- 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、インダストリー事業統括本部 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 日立アドバンスシステムズ (本社)
- 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
- 日本スペースイメージング株式会社
- 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 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SC株式会社 (本社)
- 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 (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)
- 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 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
- 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 (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
- 日立チャンネルソリューションズ株式会社
- 株式会社 日立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 日立パワーソリューションズ
- 株式会社 日立フーズ&ロジスティクスシステムズ
- 株式会社 北海道日立システムズ (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 日立マネジメントパートナー

## 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/IEC 15408に基づく「ITセキュリティ評価および認証制度」に  
11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]  
よって認証された主な製品は、次のとおりです (2021年)

製品	TOE種別 <sup>※1</sup>	認証番号	評価保証レベル <sup>※2</sup>
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といいます。関連する管理者およびユーザーの手引書 (利用者マニュアル、ガイドンス、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ド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脆弱性分析、製造から運用開始まで、製品の完全性の観点から評価が追加されます。通常の開発ライフサイクルにセキュリティ的な視点を加味しています。
- ・EAL3は、EAL2で得られる保証に加えて、テストの網羅性や開発時の製品の改ざんを防止するための開発環境の評価が実施されます。
- ・EAL4は、一般的な商用製品として最高位とされており、開発環境での開発資産の保水性やソースコード、要員の信頼性など開発ライフサイクル全般にわたって評価されます。
- ・ALC\_FLR.1は、製品にセキュリティの欠陥が発見された場合、必要なパッチを提供する基本的な手続きを客観的に評価します。規格では規定のEALに含め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、利用者からの脆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/IEC 19790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 (2021年11月時点[CMVPによる“historical list”への掲載を含みます])。

製品	認証番号	レベル
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版 および Windows版)	JCMVP #J0007	Level 1
Keymate/Crypto JCMVPライブラリ	JCMVP #J0005	Level 1



# 日立グループの概要

## 会社概要 (2021年3月31日時点)

**商号** 株式会社日立製作所  
**設立年月日** 大正9年(1920年)2月1日  
 (創業明治43年(1910年))  
**本店の所在地** 東京都千代田区丸の内一丁目6番6号  
**代表者\*1** 代表執行役 執行役社長兼 COO 小島 啓二

**資本金** 460,790百万円  
**従業員数** 35万864人(国内15万8,194人、  
海外19万2,670人)  
**連結子会社数** 871社(国内159社、海外712社)  
**持分法適用会社数** 345社

\*1 2021年6月23日時点

## 財務ハイライト (2021年3月期連結IFRS)

**売上収益** 8兆7,291億円(前期比100%)  
**調整後営業利益率** 5.7%(前期比1.8ポイント減)  
**EBIT\*2** 8,502億円(前期比6,666億円増)

**当期利益(親会社株主帰属)** 5,016億円  
 (前期比4,140億円増)  
**ROIC\*3** 6.4%(前期比3.0ポイント増)

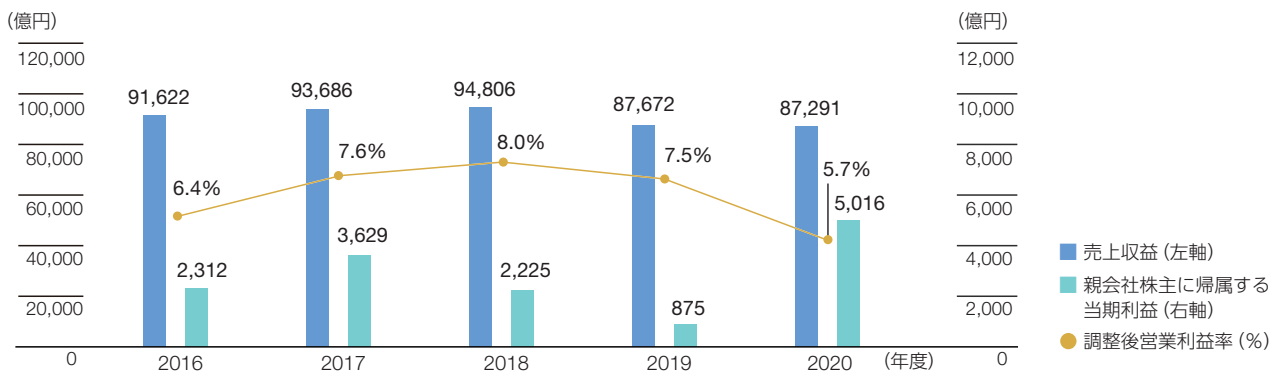
\* 当社の連結財務諸表は、国際財務報告基準(IFRS)に基づいて作成しています

\*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

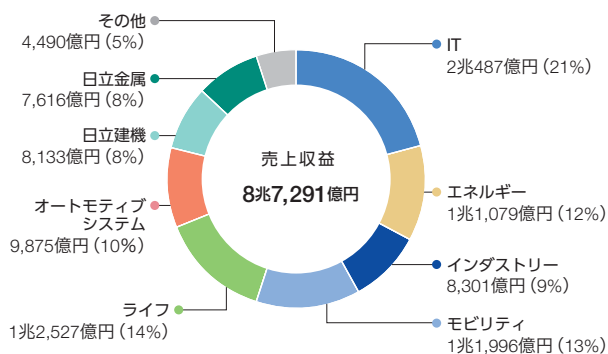
\*3 ROIC: Return on invested capitalの略で「投下資本利益率」の意。「ROIC=(税引後の調整後営業利益率+持分法損益)÷投下資本×100」により算出。

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

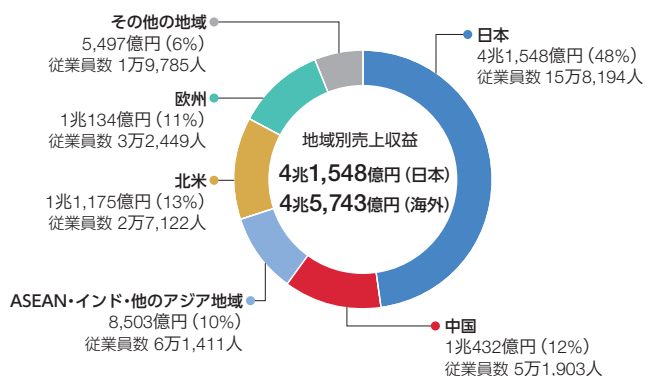
## ●売上収益/調整後営業利益率/当期利益の推移



## ●セグメント別売上収益/構成比 (2021年3月期 連結IFRS)



## ●地域別売上収益/構成比 (2021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