# 情報セキュリティの推進

## 情報セキュリティ方針

IoTの進展により、さまざまなモノがつながることで、新たな価値が生み出されています。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IoT・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管理は、企業の最重要の課題の一つとなっています。

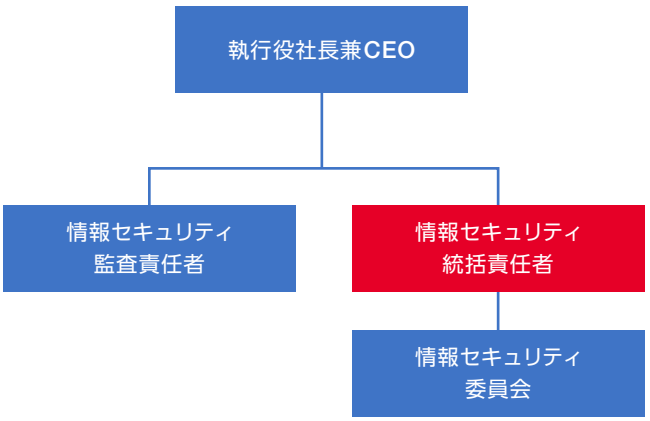
こうした背景のもと、社会イノベーション事業を展開する日立は、情報セキュリティガバナンスを最も重要な経営課題の一つと位置づけています。2018年3月に日本経済団体連合会が発表した「経団連サイバーセキュリティ経営宣言」においても、価値創造とリスクマネジメントの両面からサイバーセキュリティ対策に努めることが経営の重要課題であると述べられており、日立は同じ理念で情報セキュリティのガバナンスに取り組んでいます。

## 情報セキュリティ推進体制

日立製作所では、情報セキュリティおよび個人情報保護の実施・運用に関する責任・権限をもつ情報セキュリティ統括責任者を執行役社長兼CEOが任命します。

従来は、CIO*1が情報セキュリティ統括責任者の役割も担い、情報セキュリティ対策、管理を行ってきました。2017年10月より、日立全体の情報セキュリティガバナンスをさらに強化し、一括して推進するため、新たにCISO*2を任命しました。CISOは、情報セキュリティ統括責任者として、日立のすべての製品や社内設備を対象に情報セキュリティを推進する役割を担い、2017年度は執行役副社長が務めました。

### 情報セキュリティ推進体制図




2017年9月以前　CIOが就任
2017年10月以降　CISOが就任

情報セキュリティと個人情報保護に関する取り組み方針、各種施策は、情報セキュリティ統括責任者を委員長とする「情報セキュリティ委員会」が決定します。決定事項は各事業所およびグループ会社に伝達され、各組織の情報セキュリティ責任者が職場に徹底しています。

*1　CIO：Chief Information Officer
*2　CISO：Chief Information Security Officer

## 情報セキュリティマネジメント

### 情報セキュリティ管理

日立は、国際規格であるISO/IEC 27001に基づく「グローバル情報セキュリティ管理規程」を定め、情報セキュリティ管理の強化に努めています。グローバルには日本の親会社から日本国外のグループ会社に対して展開を行うとともに、米州、欧州、東南アジア、中国、インドなどの地域統括会社によるサポートとセキュリティシェアドサービスの利用を積極的に推進しています。

### セキュリティ監視

日立ではサイバー攻撃の早期検知と迅速な対応のために、SOC*1による24時間365日のセキュリティ監視と、IRT*2によるセキュリティ関連情報の収集・展開とインシデント対応を行っています。

*1　SOC：Security Operation Center
*2　IRT：Incident Response Team

## 機密情報漏えいの防止

日立製作所では情報漏えいを防止するために「機密情報漏えい防止3原則」を定め、機密情報の取り扱いに細心の注意を払い、事故防止に努めています。

**機密情報漏えい防止3原則**

原則1　機密情報については、原則、社外へ持ち出してはならない。
原則2　業務の必要性により、機密情報を社外へ持ち出す場合は、必ず情報資産管理者の承認を得なければならない。
原則3　業務の必要性により、機密情報を社外へ持ち出す場合は、必要かつ適切な情報漏えい対策を施さなければならない。

情報漏えい防止の具体的施策として、暗号化ソフト、セキュアなパソコン、電子ドキュメントのアクセス制御・失効処理ソフト、認証基盤の構築によるID管理とアクセス制御、メールやWebサイトのフィルタリングシステムなどをIT共通施策として実施しています。サイバー攻撃に対しては、防御策を多層化（入口・出口対策）して対策を強化しています。

また、サプライヤーに対しては、日立が定めた情報セキュリティ要求基準に基づき、調達取引先の状況を確認・審査しています。

## 個人情報保護

日立製作所は、「個人情報保護方針」に基づいて構築した、日立製作所個人情報保護マネジメントシステムを運用しています。また、日立製作所ほか日本国内44事業者*がプライバシーマークを取得しています。

なお、2017年度、顧客プライバシーの侵害および顧客データの紛失に関して、個人情報の取り扱いに関する苦情・申し立てなどはありませんでした。

また、2018年5月に欧州で施行されたGDPR（欧州一般データ保護規則）など、個人情報の保護に関する法制化が各国で進んでおり、日立はその動向を注視しながら適切な取り組みを進めています。

＊ 2018年5月末現在

## 情報セキュリティ監査

日立の情報セキュリティは、日立製作所が定めた情報セキュリティマネジメントシステムのPDCAサイクルにより推進しており、すべてのグループ会社および部門に対し、1年に1回情報セキュリティおよび個人情報保護の監査を実施しています。

日立製作所における情報セキュリティ監査は、執行役社長兼CEOから任命された情報セキュリティ監査責任者が独立した立場で実施しています。221社の日本国内の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。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ています。

個人情報保護については、1年に1回、全部門が職場での自主点検として、「個人情報保護・情報セキュリティ運用の確認」を実施しています。併せて重要な個人情報を取り扱う業務（693業務*）については「個人情報保護運用の確認」を1カ月に1回実施し、安全管理措置や運用の状況を定期的に確認しています。

＊ 2018年3月時点の登録業務数

## 情報セキュリティ教育の実施

日立では、すべての役員、従業員、派遣社員などを対象に、情報セキュリティおよび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。日立製作所では約4万人が受講し、受講率はほぼ100%に達しており、そのほかにも対象別、目的別に多様な教育プログラムを用意し、情報セキュリティ教育を実施しています。また、標的型攻撃メールなどのサイバー攻撃への教育として、実際に攻撃メールを装った模擬メールを従業員に送付し、受信体験を通してセキュリティ感度を高める「標的型攻撃メール模擬訓練」を2012年より実施しています。

## サイバーセキュリティは経営課題へ

2017年5月にランサムウェア*1である「WannaCry」に感染し、一部のシステムで障害などが発生しました。日立は、この事案からの学びを踏まえ、経営課題としてサイバーセキュリティ対策のさらなる強化に取り組んでいます。

### ランサムウェア感染に対する初動対応

始まりは2017年5月12日の22時ごろ、データセンター内のシステムの動作が不安定となる事象でした。この時点ではウィルス感染であることは分かっておらず、システムの障害を疑って原因調査を進めていました。1時間後、ランサムウェアへの感染が確認されたため、その情報が速やかに社内のIncident Response Team（IRT）に報告され、攻撃および被害状況の把握を開始しました。

翌13日深夜1時過ぎ、IRTは把握した情報から今回の事案がランサムウェア「WannaCry」への感染によるものであると判断、経営幹部に報告し、被害拡大防止の初動対応に着手しました。同日の5時過ぎに日立グループ全社への緊急対策指示を展開、9時に本社に緊急対策本部を設置して、被害状況の把握と、復旧に向けた対策および感染ルートの分析を開始しました。

### 事案を通して学んだこと

ランサムウェア感染事案への対策を通して学んだことが4点あります。

1点目は、ネットワーク内で一気に拡散するサイバー攻撃の脅威です。社内のネットワークに接続される機器は、パソコンやサーバーなどOA機器だけでなく、現場の開発・生産用設備などのOT機器にまで広がっています。今回の事案では、セキュリティパッチ*2が自動適用されていないOA機器や、そもそも適用が慣習化されていないOT機器など、セキュリティが弱い箇所からウィルスに感染し、ネットワーク内で一気に拡散して被害の拡大につながりました。

2点目は、サーバーなどOA機器のセキュリティ対策徹底の重要性です。業務システムが稼働している場合、業務の調整ができずシステムを止められないといった理由から、タイムリーなセキュリティパッチの適用ができていなかった機器が感染の被害を受けました。

3点目は、OT機器のセキュリティ対策の困難さです。これらの機器にはそもそもセキュリティパッチの適用が想定されていないものも多く、また導入後にシステムをアップデートする必要性を意識していない、という実状がありました。

4点目は、サイバー攻撃を想定したBCP（事業継続計画）強化の必要性です。「絶対の安全はない。有事の際には影響を限定し、いかに早く元に戻すか」という考えのもと、ランサムウェアなどのサイバー攻撃についても、災害などと同様に日ごろから最悪のシナリオを想定して手順書の整備やトレーニングを行い、現場力を向上しておくことが必要です。

このような課題への対応には、技術的な側面に加えて、事業の継続性を観点とする経営視点での総合的なリスク分析と対策の判断が必要となります。

昨今のサイバー攻撃の高度化に加えて、ヒューマンエラー、内部不正、環境変化など情報セキュリティを取り巻く脅威は年々増加し、事案の発生による経営インパクトは大きくなっています。日立は、今後も重要な経営課題の一つとして、組織・運用・システムのバランスを考慮したサイバーセキュリティ対策の強化と耐性の向上に取り組んでいきます。

*1：感染したコンピューターに特定の制限をかけて、その制限の解除と引き換えに金銭などを要求するコンピューターウィルスの一種
*2：コンピューターのプログラムに不具合や脆弱性が発見された際に、それらの問題を修正するために提供されるプログラム