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。

* IoT:Internet of Things

情報セキュリティ推進体制

従来、日立製作所では、経営戦略に沿った情報戦略やIT投資計画の策定などに責任を持つ、情報統括責任者であるCIO*1が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・権限の役割も担ってきました。しかし、2017年10月からは、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、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っています。推進にあたっては、CISOを委員長とする「情報セキュリティ委員会」が方針・施策などを決定し、各事業所およびグループ会社に伝達し、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、情報セキュリティ統括責任者

情報セキュリティマネジメント

情報セキュリティ管理

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強化のための継続的な情報セキュリティマネジメントシステムをグローバルに推進しています。また、従来日本の親会社から日本国外のグループ会社に対して各種施策を展開していましたが、2019年度からは、米州、欧州、東南アジア、中国に新たに情報セキュリティエキスパートを設置し、グローバルに一層のセキュリティ強化を開始しました。

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、CSIRT*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 CSIRT:Computer Security 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。

情報漏えい防止の具体的施策として、PCの暗号化、認証基盤の構築によるID管理とアクセス制御、サイバー攻撃への防御策の多層化(入口・出口対策)を行っています。

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。そして、日立製作所ほか日本国内42事業者* でプライバシーマークを取得し、個人情報の保護に努めています。

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います。日立では、GDPRに対する取り組みとして、GDPRの適用を受ける業務の特定、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。

* 2019年3月末現在

情報セキュリティ監査

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。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。これらは、1年に1回すべての部門およびグループ会社で実施しています。

情報セキュリティ教育

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。その他にも対象別、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、「標的型攻撃メール模擬訓練」を2012年より実施しています。

サイバーレジリエンス強化に向けた「セキュリティエコシステム」の構築

新たなセキュリティ戦略　「セキュリティエコシステムの構築」

昨今、サイバー攻撃の手口は以前にも増して高度化し、攻撃の量も増加かつ攻撃対象の範囲も拡大の一途をたどっています。これらに対処するために、日立は新たな戦略を開始しました。それは「セキュリティエコシステムの構築」です。

「エコシステム（生態系）」とは、動植物や環境が互いに依存して生態を維持する状態のことです。これをセキュリティの分野に置き換えてみたところ、本来の業務が異なる部門であっても、セキュリティ活動という1つの目標に向かって相互に協力し合うことが、結果的に組織における事業活動の維持・拡大を可能にするという考えに至りました。

セキュリティエコシステムにおける3つの「つながる」

1　モノが「つながる」

日本において、将来的にめざすべき未来社会であるSociety 5.0[*1]は、さまざまなつながりが新たな付加価値の創出や社会課題の解決をもたらします。これらを実現するために、IoTに代表される、機器やシステムなどのモノが「つながる」環境になります。

2017年5月、日立はランサムウェア[*2]であるWannaCryに感染しました。これは「セキュリティ対策の必要性が認識されていなかった」検査機器から発生したもので、国内外のあらゆる現場まで影響が及ぶ事案となりました。このことから、従来の社内IT環境に加えて、閉鎖的な環境であった生産・製造現場などを含めたセキュリティ対策の必要性を学びました。

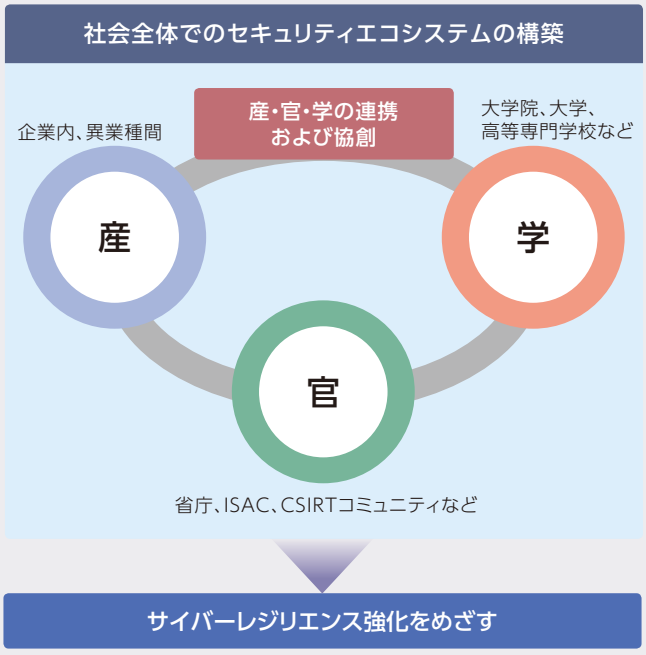
このような背景のもと、日立では、さまざまなモノが「つながる」ことへの対策として、あらゆる環境における網羅的なサイバーセキュリティ対策（環境ごとの指針・ガイドラインの策定など）をグローバルで開始しました。

2　人・組織が「つながる」

いままでつながっていなかったモノをつなげ、セキュリティを確保するには、企業内において各事業部門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。そのために、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、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。

3　社会が「つながる」

また、つながりは日立の中だけに限ったことではありません。サイバーセキュリティ対策推進に取り組んでいる国、学校、ほかの企業との脅威情報や対策実行時の課題共有など、枠組みを超えたコミュニティの形成が必要不可欠になると考えています。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マネジメントサイクルにフィードバックし、さらに新たな共有を広げるといった、社会が「つながる」活動も、日立は積極的に開始しています。



社会全体でのサイバーレジリエンス強化をめざして

日立では、Society 5.0の実現に向けて、より人々が安全・安心に暮らすために、企業内だけでなく産・官・学が連携および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推進し、サイバーレジリエンス[*3]強化をめざして取り組んでいきます。

*1　Society 5.0：サイバー空間（仮想空間）とフィジカル空間（現実空間）を高度に融合させたシステムにより、経済発展と社会的課題の解決を両立する、人間中心の社会（内閣府ホームページより）
*2　ランサムウェア：感染したコンピュータに特定の制限をかけて、その制限と引き換えに金銭などを要求するコンピュータウイルスの一種
*3　レジリエンス：複雑かつ変化する環境下における組織の適応能力（一般財団法人日本規格協会 JIS Q 22300より）