Overview

社会インフラのデジタライゼーションを支えるセキュリティ

宮尾 健 | Miyao Takeshi
谷本 順一 | Tanimoto Junichi

1. デジタライゼーションとセキュリティの脅威

IoT（Internet of Things）の出現により，あらゆるものがインターネットにつながる世界になりつつある。スマートフォンやセンサー，カメラなどを用いて，モノやヒトの動向はデータ化され，インターネットにつながる。現実世界をデジタルとしてモデル化し，サイバー空間上で分析・試行することで，これまでにないスピードで新たな価値を発見し，現実世界へフィードバックすることを可能にするデジタライゼーションは，産業の在り方，社会インフラ自体の在り方までも大きく変えようとしている。

こうした変革をもたらすデジタライゼーションは，新しい価値を生み出す光の部分がある反面，新たなセキュリティ脅威が出現している。

このような社会課題に対し，政府や業界団体において課題解決に向けた取り組みが進められている。例えば，経済産業省において，これらのサイバーセキュリティの課題を洗い出し関連政策を推進していくため，産業界を代表する経営者，インターネット時代を切り開いてきた学識者などから構成される「産業サイバーセキュリティ研究会」を設置した[1)]。また，一般社団法人日本経済団体連合会においても，これらの課題解決に向けて産業界自らが取り組むべき事項や政府が取るべき施策などについて，「Society 5.0 実現に向けたサイバーセキュリティの強化を求める」提言を出しており[2)]，官民連携した取り組みが活発化している。

この取り組みを進めている状況において，セキュリティの脅威が顕在化した事案が発生した。2017年，世界的に猛威を振るったランサムウェア「WannaCry」がその一例である。

2. 日立の取り組みとセキュリティビジョン

実際に日立においても，上述のランサムウェアに感染し被害を受けることとなった。この事案に対応していく中で，以下の2点の必要性が見いだされた。

(1) IoT時代における大規模システムの運用の在り方を見直すこと
(2) 事業継続計画を，自然災害とサイバー攻撃の両面から検討すること

今回の事案はIoT機器が発信源となっており，IT機器だけでなく，社会インフラシステムにおいて実際に稼働している制御装置もセキュリティの脅威にさらされていること，およびサイバー攻撃に対する防護だけでなく，事案発生時に事業継続の観点からどのように対応すべきか，さらにはどのように事前に予防措置を講じておくかが重要であると気付かされた。これらの気付きに実際に対処していくためには，統制・組織・技術・人材の観点より対応が必要である（**表1**参照）。

統制の観点では，自然災害を想定した事業継続計画をサイバー攻撃を含めた計画に発展させることが必要である。組織面では，事案発生時に事業継続の判断を下すために，セキュリティの技術を保有する情報部門と実際の事業を進めている現場部門の双方が連携できる横断組織体制を構築することが重要である。技術面では，自己拡散機能を持つウイルスの封じ込めを行うために，監視・検知・分析・対処をサポートし，事業継続および迅速な復旧を実現するためのセキュリティシステムを構築して

表1｜サイバー攻撃を想定した事業継続計画を実行するための課題

ランサムウェア事案での気付きに実際に対処していくためには，統制・組織・技術・人材の観点より対応が必要である。

統制	自然災害だけでなく，サイバー攻撃を想定した事業継続計画の策定とリスクアセスメントの実施
組織	インシデント発生時に事業継続の判断を下すため，情報・現場部門の双方が連携できる横断組織体制の構築
技術	インシデント監視・検知・分析・対処をサポートし，事業継続および迅速な復旧を実現するためのセキュリティシステム構築
人材	セキュリティと業務・制御システム両方に精通した人材の育成

おくことが肝要である。さらに人材面では，セキュリティと業務・制御システム両方に精通した人材を育成し，事案発生時にも事業継続の観点から対策を推進できるようにすることが大切である。

以上のような課題に対処するため，日立ではセキュリティのビジョンとして，「Evolving Security for changing IoT world.」を掲げ，セキュリティを進化させる。その進化の方向性について以下に紹介する（**図1**参照）。

2.1
進化1：ITセキュリティをOT/IoTセキュリティへ

日立は，電力，鉄道，ガス，水，製造，情報通信，金融，公共などの社会インフラシステムを構築し，顧客に提供している。この経験と実績は，セキュリティ対策を実施するうえで重要な要素と考える。社会インフラシステムのセキュリティ対策は，セキュリティ技術のみならず，システムがどのように運用されているか，そのうえでどのように守ればよいかを理解して初めて有効だと考える。特に，OT（Operational Technology）/IoTセキュリティには，「安全」と「事業継続」が重要となる。システムが正しく動き，サービスを安全に，かつ継続的に提供することが大切であり，インフラ構築の経験がセキュリティ適用に生かされるポイントである。

図1｜日立のセキュリティビジョン

社会インフラの事業継続を支えるために，図中に示す3つの方向にセキュリティを進化させる。

注：略語説明
IoT（Internet of Things），OT（Operational Technology），AI（Artificial Intelligence）

2.2
進化2：日立社内で実証を重ねたセキュリティを顧客へ

日立では，多種多様なセキュリティの実証環境を構築・保有している。IT系においては，日立グループ約30万人の社内ユーザーに対するITインフラを運用し，日々のセキュリティ運用監視を実施するとともに，世界4拠点，4つの言語（英語，フランス語，スペイン語，日本語）をサポートしたSOC（Security Operation Center）サービスを45か国の顧客へ提供している。さらに，今回のランサムウェア事案で得た気付きを生かし，社内インフラでの改善を推進している。

また，日立は社会インフラシステムを開発・製造していることから，OTセキュリティにおいても社内で実証を繰り返し，実績を積み重ねているところである。

2.3
進化3：セキュリティ対策コストを経営課題解決につなげる投資へ

日立は，AI（Artificial Intelligence）やアナリティクスの技術をセキュリティに応用することで，セキュリティを単なるコストではなく，業務効率化など経営課題解決への投資に進化させていく。

例えば，セキュリティの監視運用は膨大なログを常にチェックしなければならないといった大変な作業であり，さらにセキュリティの技術を持った人材でないと対応が難しいところである。こうした場合に，AI技術を

ログ解析に活用することで業務の効率化を図ることができる。

また別の例では，同時に大量発生する映像データを人がリアルタイムに監視することは難しいが，AI技術を活用することでリアルタイムに監視することが可能となる。さらには人の動作を分析することで安全性を高めたり，作業効率を上げたりすることができる可能性がある。

加えて，AI技術を活用した予兆検知，行動分析により，セキュリティインシデントへの対策を事前に準備できるようになる。事故発生後のシステム・サービス停止からの復帰，経営品質のリカバリーにかかる費用は膨大である。小さな異変を検知し，先手を打って対策することが事業継続性を高め，経営の品質を守っていく。

3. サイバー・フィジカル セキュリティソリューション

日立は，ランサムウェア事案での気付きを生かし，セキュリティビジョンに従いサイバー・フィジカル両面からのセキュリティソリューションの提供を開始した。

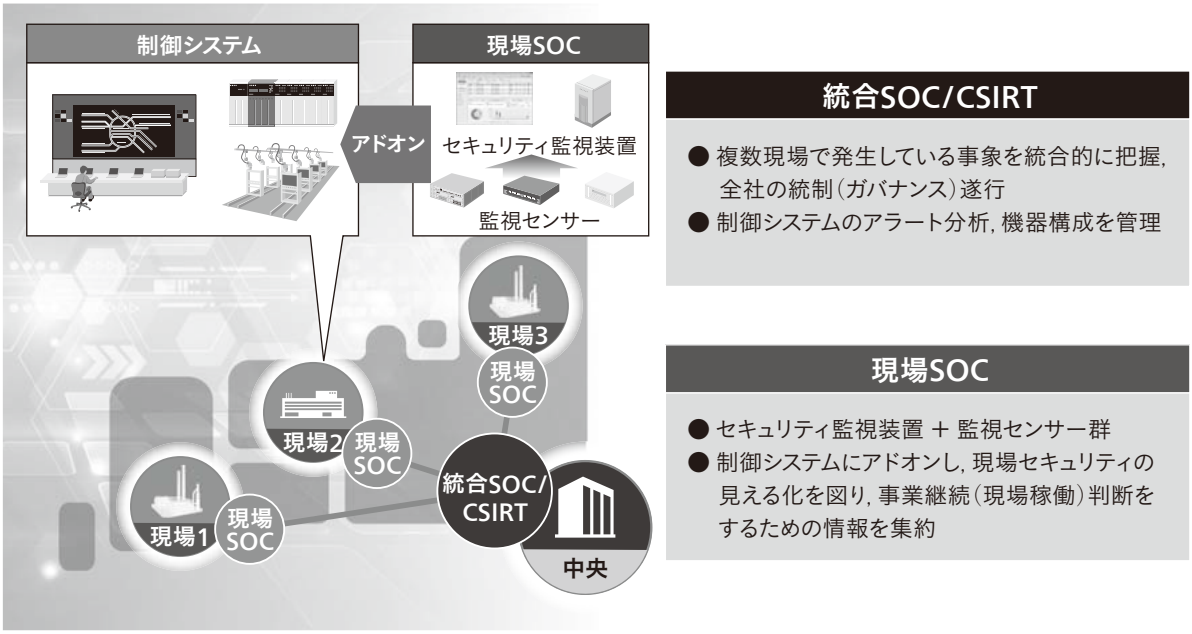
サイバー攻撃を想定した事業継続計画の実現とIoT機器をサイバー攻撃から守るため，セキュリティ統合監視，IoTセキュリティ（IoT機器管理），およびエリアセキュリティのソリューションを提供している。

セキュリティ統合監視は，ITシステムだけでなく，OT/IoTシステムまで含めたセキュリティ運用を実現し，社会インフラ事業の事業継続を支援するためのソリューションである。まず，中央組織と現場組織の役割分担を明確化する。中央の役割としては，統制（ガバナンス）の遂行や複数現場での事象把握，インテリジェンス情報およびセキュリティ人材の集約を図る。一方，現場の役割としては，事業継続（現場稼働）の判断のため，従来の監視業務にセキュリティ監視を追加，現場セキュリティの見える化を図る。これらの役割を実現するために，統合SOC/CSIRT（Computer Security Incident Response Team），現場SOCというソリューションの提供を開始した（**図2**参照）。

IoTセキュリティとしてのIoT機器管理の課題は，ロングライフサイクルで24時間稼働のため停止することが難しい状況で，どのようにセキュリティ対策を実行していくかということである。そのためにはゾーン設計の考え方を推奨する（**図3**参照）。パッチを当てることが難しい制御装置を囲む形で，例えば不正侵入防止装置や不正接続検知装置などを設置することを想定する。これらを製造分野へ適用したシステム構成事例を**図4**に示す。

エリアセキュリティは，ある領域（エリア）を守るため，映像や生体認証などを応用し，セキュリティ情報を収集・蓄積することにより，防犯・防災用途だけでなく，

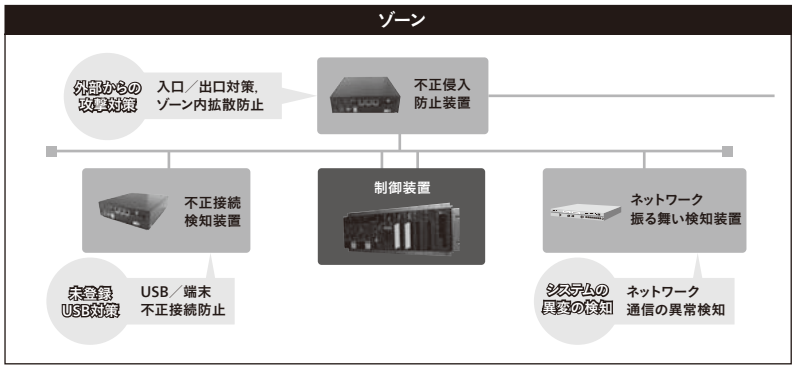
図2｜セキュリティ統合監視における中央と現場の役割
中央の役割を実現するための統合SOC/CSIRT，現場の役割を実現するための現場SOCというソリューションを提供する。



注：略語説明
SOC（Security Operation Center），CSIRT（Computer Security Incident Response Team）

図3｜ゾーン設計の例

OS（Operating System）アップデートやセキュリティパッチを当てるといった通常のセキュリティ対策が困難な制御装置には，それを囲む形で不正侵入防止装置や不正接続検知装置などを設置して，ゾーンでセキュリティを確保する。



注：略語説明
USB（Universal Serial Bus）

エリア全体を見える化するとともに画像解析・AI連携によるセキュリティ強化，さらには安全確保や業務最適化といった経営課題解決まで活用できるソリューションである。なお，このソリューションの要素技術の一つである日立の指静脈認証は，認証精度，認証スピードなどが高く評価され，海外でもフィジカルセキュリティ分野への適用が拡大している。

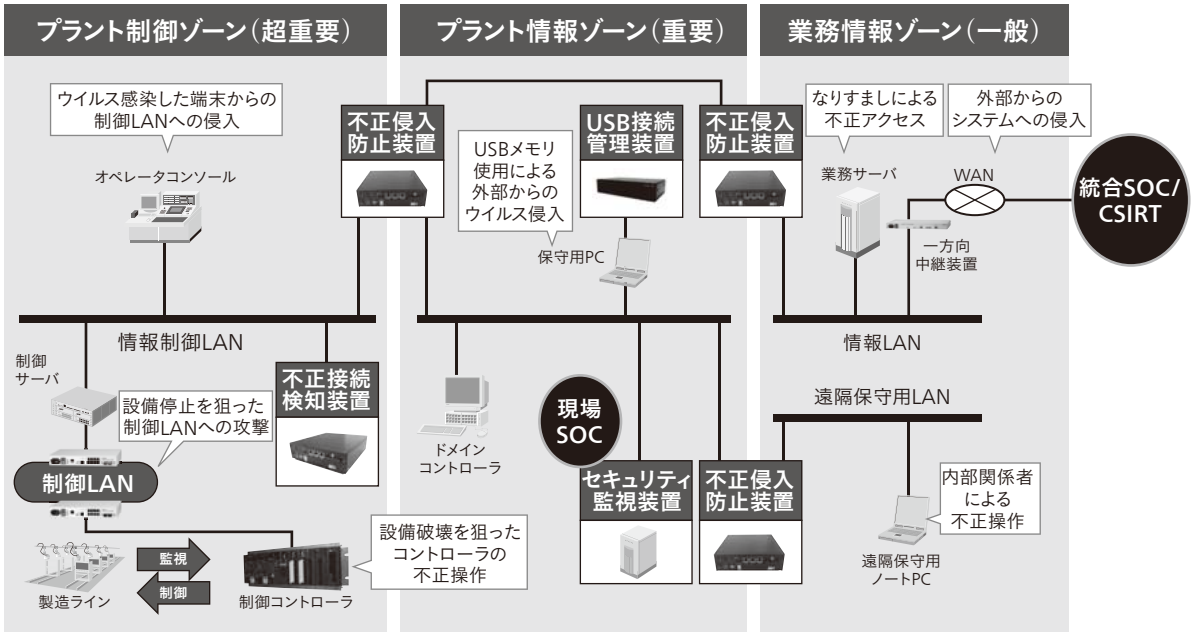
4. 人材育成とサイバー防衛訓練

セキュリティ人材を育成していくための取り組みは各所で実施されている。例えば，独立行政法人情報処理推進機構（IPA：Information-technology Promotion Agency, Japan）は，2017年4月に「産業サイバーセキュリティセンター」を発足した。7月から実際のカリキュラムに従った人材育成に着手しており，日立からも参加し人材育成に努めている[3)]。

また，実際の演習を通した人材育成としては，社会インフラシステムの開発・製造を担当している日立製作所大みか事業所において，社会インフラ事業者の実システムを模したシステムを構築･活用したプログラムにより，組織運営，システム運用におけるサイバー攻撃を想定した事業継続計画の確認，改善の検証をしている。また，

図4｜製造分野におけるセキュリティ統合監視の例

ゾーン設計とセキュリティ統合監視を製造分野へ適用したシステム構成事例を示す。



注：略語説明
LAN（Local Area Network），WAN（Wide Area Network）

セキュリティ技術と業務・制御システムの両面に精通した人材を育成するためのサイバー防衛訓練サービスの提供を開始している。

5. 顧客との協創と経営課題解決

日立は，デジタライゼーションに合わせてセキュリティを進化させ，顧客の提供するサービスや事業を守っていく。これは，顧客が提供するサービスがどのように構築・運用されているかを知ったうえで，顧客と共に考え，進化させることで真の経営課題の解決に努めるということである。

セキュリティは単なるコストではない。顧客の課題解決を通して業務効率化や品質向上に貢献し，投資の一環として経営に貢献する。投資の極小化・最適化を図るため，社会インフラシステムの構築・運用のノウハウを生かし，どのレベルまで対策すればよいかを短期・中期・長期に分けて提案していく。特に初期投資を抑え，スモールスタートをしながら将来的にシステムの段階的構築ができるように，そのためのプラットフォームを提供している。

日立は，セキュリティを経営者の視点で捉え，顧客のすぐそばでその事業を進化させていく。

6. おわりに

本稿では，デジタライゼーションが進む中，社会インフラシステムに求められるセキュリティに対する取り組みについて説明した。

これらの取り組みに基づく具体的なソリューションについて，本特集掲載の別論文で，サイバー・フィジカル両面から詳述しているので参照されたい。

参考文献など

1）経済産業省，ニュースリリース：「産業サイバーセキュリティ研究会」を開催します（2017.12），
http://www.meti.go.jp/press/2017/12/20171226004/20171226004.html

2）一般社団法人日本経済団体連合会，提言：Society 5.0 実現に向けたサイバーセキュリティの強化を求める（2017.12），
http://www.keidanren.or.jp/policy/2017/103.html

3）独立行政法人情報処理推進機構，プレス発表：産業サイバーセキュリティ人材育成施設7月始動，受講者を2月20日より募集開始（2017.2），
https://www.ipa.go.jp/about/press/20170208.html

執筆者紹介

宮尾 健
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
セキュリティ事業統括本部 所属
現在，セキュリティ事業の統括業務に従事

谷本 順一
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 セキュリティ事業統括本部
マネジメント本部 事業管理部 所属
現在，セキュリティ事業の企画業務に従事