特集
Special Feature

［ディジタルエコノミー時代のサイバーセキュリティ―ディジタルトランスフォーメーション促進の基盤確立に向けて―］

① ディジタル化とデータ活用により進化する社会インフラセキュリティ

応用

宮尾　健 （株）日立製作所　谷本順一 （株）日立製作所

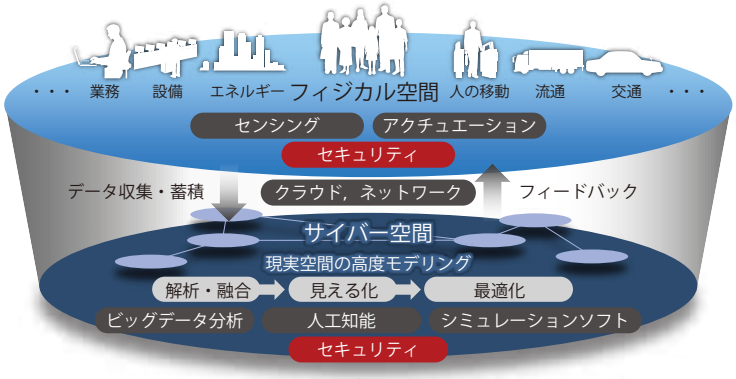
データ活用とセキュリティの脅威

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，カメラなどを用いて，ヒトやモノの動向はデータ化され，インターネットにつながる．Society 5.0 では，フィジカル空間をディジタルとしてモデル化し，サイバー空間上で人工知能等を用いてデータを分析，シミュレーションソフトを用いて試行・最適化することで，これまでにないスピードで新たな価値を発見し，フィジカル空間へフィードバックすることが可能となりつつある（図 -1）．このようなデジタライゼーションの動きは，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 Society 5.0 への取り組みは，データ活用することにより新しい価値を生み出す光の部分がある反面，そのデータ活用に伴う新たなセキュリティ脅威を生み出している．これは，活用するデータそのものの確からしさが前提となっており，たとえば，ヒトやモノの動向のデータが誤っていたり改ざんされていたりすると，そこから導き出される結果も誤ったものになるリスクがあることを意味する．

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．たとえば，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経験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，（一社）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，官民連携した取り組みが活発化している[2]．

このような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．



■図 -1　Society 5.0 の実現に向けたデータ活用

ランサムウェア事案で得た教訓

サイバー攻撃の概要

実際，筆者の所属する日立製作所においても，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．2017年5月12日，WannaCryと呼ばれるワーム型ランサムウェアが欧州から世界中に感染拡大した．本ウィルスはWindows[☆1]の脆弱性を悪用して，自分自身を他の脆弱なWindowsシステムにネットワークを経由して拡散させる．

また感染したシステムはデータが暗号化され，その暗号解除の鍵と引き換えに金銭を要求する脅迫文が表示される．日立グループでも欧州の現地法人の検査機器から社内ネットワークのサーバなどに次々と感染し，グローバルで被害が発生した．

影響範囲

被害範囲は，社内ネットワークに接続されている機器である業務システムサーバ，OA（Office Automation）用PCなど情報システム部門が管理しているものから，工場にある製造・生産システム，制御や倉庫システム，ファシリティの入退室管理システムまで多岐にわたった．

図-2は，2017年5月12日からの社外へのファイアウォールにおけるWannaCryの拡散パケットの廃棄数を表したものである．20：00頃に感染が始まり，3時間後の23：00にはほぼ飽和状態になり，脆弱性が対策されていない機器すべてに対して拡散が終わっている．その後，アンチウィルスソフトによる検疫や脆弱性対策によりパケット数は減少していった[3]．

ランサムウェア事案から得た教訓

ランサムウェア事案から得た教訓には，以下の2点が挙げられる．

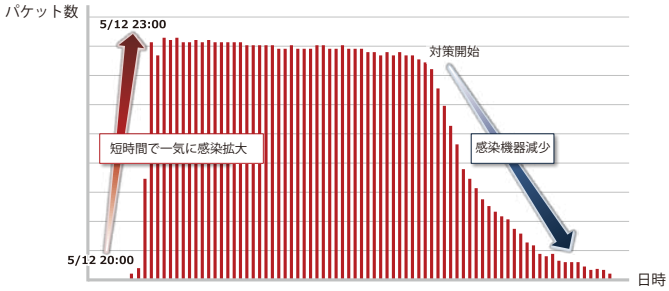
(1) IoT時代における大規模システムの運用の在り方を見直すこと

(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

1つ目の「IoT時代における」の意味は，今回のランサムウェア「WannaCry」のパケットの最初の発信源（今回はこれを「感染源」と表す）が，「検査機器」であったことである．このようなIoT機器では，IT機器とは異なり組込みOS，たとえば組込みWindowsが使われており，パッチ適用が元々想定されていないことが多い．さらには，そもそも現場に設置されている各種IoT機器はアセットとして構成が管理されていない場合すらあった．そのためセキュリティ上のリスクを正しく把握できていなかったことになる．

また，「大規模システムの運用」の意味は，今回の感染源の場所が欧州であったにもかかわらず，社内ネットワークの全体に感染が及んでしまったことである．これは，ネットワークのポリシーの問題であるが，社内と社外の間を壁でしっかり守っておく，言い換えれば，エンドポイントのセキュリティを十分対策しておけば，社内ネットワークの内部については，性善説に基づき，利便性を優先し，セグメント化を排除してよいという考え方に基づいて設計していた点である．そのため，いったんエンドポイントで感染が発生してしまうと，社内ネットワークには関所がなく，一気に感染が起こってしまう状況であった．

2つ目の教訓は，「事業継続計画（BCP）は，自然災害とサイバー攻撃の両面から検討」する必要があることである．自然災害にかかわるBCPについては，2011年の3.11東日本大震災をきっかけに世の中的にもBCPが見直された．大震災時の見直しにおいては，たとえば，バックアップサーバは自然



■図-2　WannaCryの拡散速度

☆1 Windowsは，米国Microsoft Corporationの米国およびその他の国における登録商標である．

災害を想定した場合，同じ場所にバックアップサーバを置くと同時に被災してしまうため，地理的に離れた場所に設置するよう対策したものの，今回のようなウィルスの場合には地理的な位置関係は関係なく，ネットワークにつながっているとバックアップサーバまでウィルスに感染してしまい，バックアップデータが暗号化されてしまった事例があった．また，BCP に従い緊急対策本部を設置したものの，結果として，感染拡大が防げなかったことは課題として残った．

課題への対応

これらの経験から導き出した課題として，事業継続を考える場合には，自然災害だけでなく，サイバー攻撃を考慮した事業継続計画（ここでは「サイバー BCP」と表現する）の策定と事業の観点からのリスクアセスメントが重要である．

このサイバー BCP が大変重要であると考えるに至った出来事を事例として紹介する．日立製作所は製造業であり，製造現場を持っている．その現場には各種製品の製造を行うための制御システムがある．製造現場において，生産計画の情報，つまりどういう製品をいくつ作れというデータは，多くの場合，上位の計画系のシステムから与えられて製造する．昨今は特に，世の中の多様なニーズに対応していくため，そのデータの入手する周期がどんどん短くなっている．ところが，今回の場合，その計画系のシステムがランサムウェアで問題が発生してしまったため，製造現場側から見ると上位の計画系からの入力データがなく，稼働できなくなった．つまり，制御システムをサイバー攻撃からしっかり守るだけでは，事業継続の観点から見ると不十分だということに気付いた．サイバー BCP を検討・見直しする上で，システムの接続相手，言い換えると入力データがサイバー攻撃等が原因で入ってこなくなった場合でもどのように事業継続を考えておくか，要はデータフロー，および業務フローの観点から見直すことが肝要である．そのためには，いわば，サプライチェーンの観点で広く捉えることが大切である．サプライチェーンにおけるセキュリティは一事業者では対応しきれない問題でもあり，社会として取り組むべき課題であると考える．

このような観点からサイバー BCP を策定したとしても，それを実行に移す上での課題が残る．その課題は，組織面，技術面，人材面に渡る（表 -1）．

組織面で課題となるのは，多くの場合，事業継続の責任を持つ部門とセキュリティ対策・運用の責任を持つ部門が異なることである．事業責任を持つ現場の長が事業継続可否の判断ができるよう，セキュリティの責任部門がタイムリーに状況を報告できることが重要である．そのための体制を BCP として事前に決めておくことが大切である．

また，技術面では情報システム，制御システムを含め，セキュリティの監視･検知･分析･対処をサポートし，事業継続および迅速復旧を実現するためのセキュリティシステム構築が大切である．図 -2 のグラフから分かるように，事業継続のためには，まずは発生を早く検知し，いかに早期に封じ込めできるかが大切である．その対応は，人間が対策本部を作って検討していては間に合わず，技術面での対応が必須となる．

人材面では，セキュリティと業務・制御システムの両方に精通した人材を育成する必要がある．今回のランサムウェア事案にあてはめると，感染の状況を把握した上で事業継続の観点で翻訳できる人材をあらかじめ育成することが必要であり，社会的にも大きな課題となっていると認識している．

■表 -1　サイバー BCP を実行に移す上での課題

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（サイバー BCP）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を育成

アセット管理とディジタルエビデンス

セキュリティ統合監視

前章で述べたように，ランサムウェア事案で得た教訓を活かし，統制・組織・技術・人材の各観点からの対応が必要であるが，本章では特に技術面からの課題解決について述べる．

社会インフラシステムをセキュリティの脅威から守るためには，情報システムだけでなく，制御システムまで含んだセキュリティの監視が必要である．情報と制御を統合的に監視するという意味で，セキュリティ統合監視と呼ぶ．セキュリティ統合監視では，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（Security Operation Center）/CSIRT（Computer Security Incident Response Team），現場 SOC と表現した（図 -3）．

このセキュリティ統合監視の中で，特に重要と考える機能が，アセット管理とディジタルエビデンスである．

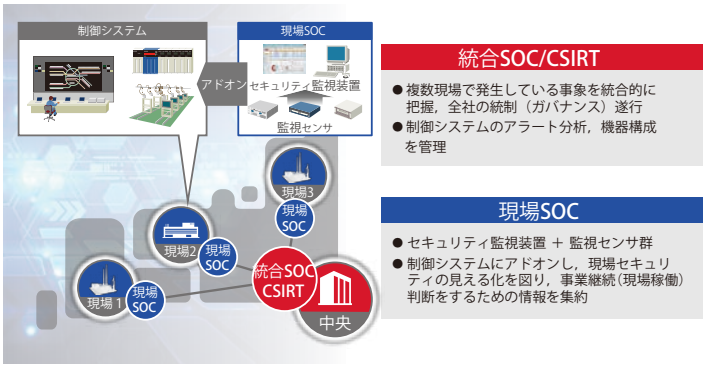
アセット管理

今回のランサムウェア事案において，感染源が IT 機器ではない現場の検査機器であるが，この種の機器には自動的にセキュリティパッチを当てる仕掛けはなく，そもそも IT 機器としての管理対象の範囲に入っていなかったことが課題である．そのため，多種多様で，IT 機器ではない現場機器（たとえば，制御コントローラや検査機器といった IoT 機器）の構成を管理するアセット管理が非常に重要になる．

サーバや端末などの構成を把握するアセット管理は，これまでは IP アドレスをキーにして管理されてきた．そのため，現場設備は，サーバや端末などの IT 機器ではないという理由からアセット管理の対象外であったり，また IP アドレスからは，フィジカル空間でどこの場所に存在するかの情報がないため，ネットワークが切り離された状態でセキュリティ対策を実行する上で課題となることがある．

そのため，サイバー空間とフィジカル空間を結びつけるアセットデータを作成し，管理していくことが重要である．現場設備と IP アドレスとを関連付けし，制御システムを構成する制御機器まで含めた形で管理する．OS の種別やバージョン，セキュリティ対策状況などを把握しておくことで，万一，インシデントが発生した場合でも，対象機器がネットワークから切り離された状況においても現地でセキュリティ対策を迅速に実施したり，対策全体の中でどこまで対策が進んでいるかの進捗把握ができるようになる．

現場設備のアセットデータを収集するための仕掛けとして，現場のネットワーク機器のミラーポートに専用の分析機器をつけて，ネットワーク通信の分析をするなどして，現場機器のアセット管理のベースとなるデータを作り上げる．このアセットデータは，現場だけでなく，中央とも共有し把握できるようにする．さらには，世の中の脆弱性などのインテリジェンス情報が現場機器にどこまで対策が必要なのか，その対策がどこまで進んでいるのかを把握す



■図 -3　セキュリティ統合監視の概要

るために使う．

このような取り組みは，セキュリティ統括組織が，事業上の残存リスクがどれだけ残っているかを正しく把握し，継続的に対策を進めることで，IT だけでなく現場機器まで含め，組織全体としてのリスク把握，その低減に活用することができるようになる効果がある．

さらに，アセット管理は，インシデントの封じ込めのためにも有効である．インシデントが発生したときに，それが機器の故障なのか，またはセキュリティインシデントなのかの切り分けを実現する．制御システムでは，多くの場合，警報情報が定義されており，その警報情報の定義の中に，セキュリティインシデントを追加して，実際の制御システムに対してサイバー攻撃があったときにどのような現象として現れるかを分析する．たとえば，ワーム型のウィルスの場合はどう見えるか，機器故障の場合はどうなのかといった分析をする．その上で，制御システムを監視するオペレータが，発生した事象をアセットデータと照らし合わせながら事象を把握し，現場機器の切り離し等の一次対処を実行することで，事業継続の観点から被害を最小限に抑え，事業を継続することが可能となる．

ディジタルエビデンス

ディジタルエビデンスは，ディジタル署名やブロックチェーン，画像処理技術などを応用してディジタルデータが本物であることを証明するための手法であるが，この手法をサイバー空間とフィジカル空間をつなぐデータの証跡管理に活用し，セキュリティ統合監視の中で監視することで，インシデントが発生した場合でも原因分析に役立てられる．

特に，ディジタルエビデンスに使うディジタルデータに，これまでの IT やネットワークのログ情報だけでなく，ヒトやモノのフィジカル空間での振る舞いを映像や制御データとして残すことで，これまで IT 系のデータだけでは原因究明の難しかった事象を迅速に分析できる可能性がある．たとえば，保守メンテナンスを実行している映像をディジタルエビデンスとして残しておくことで，インシデントが発生した場合でも，保守メンテナンス作業が問題なかったことをエビデンスとして証明することができるメリットがある．

サイバー・フィジカル連携フレームワーク

サイバー・フィジカル連携

Society 5.0 は，フィジカル空間をディジタル化し，サイバー空間においてデータ分析･シミュレーションを実施し，これまでにないスピードでフィジカル空間にフィードバックすることで新たな価値を生み出す．これを実現するために，フィジカル空間を構成するアセットをディジタル化し管理するアセット管理と，フィジカル空間でのヒトやモノの行動や振舞いを証拠性を持った形で管理するディジタルエビデンスが，基盤技術としてサイバー・フィジカル連携のセキュリティ確保に欠かせない要件と考えている．

この要件は，単に単一組織で実現するにとどまらず，たとえばサプライチェーンを構成する組織群で実現することで価値が高まり，社会として実現すべき課題と考えている．そのためには，サイバー空間とフィジカル空間をつなぎ，ヒト・モノ・データをサプライチェーンを含め組織間で共有するために，ある種のフレームワークを構築することが有効であると考える．

フレームワーク

サイバー・フィジカル連携のフレームワークは，異なる事業者間，異なる事業分野間をまたがった場合でも，サプライチェーン全体の信頼を確保するための技術である．このようなフレームワークを開発･構築することで，フィジカル空間とサイバー空間を

社会としてデータでつなぐことができ，そのデータを分析･活用することにより，新たな付加価値やサービスを創出し，社会に多大な恩恵をもたらすことが期待できる．

フィジカルセキュリティ統合プラットフォーム

このようなフレームワークの一例を，フィジカルセキュリティ分野において考えてみる．これまで，監視カメラや入退室管理システムなどの各種フィジカルセキュリティシステムのデータは，それぞれのシステム内で独立して扱われていた．

一方，複数のシステムが導入されることが多い監視や入退室管理業務などの現場では，異なるシステム間でのデータ共有ができず，監視情報の分断やオペレーションコストの多重化などの課題が生じていた．また近年の IoT の進展により，各種センサデータを収集・分析するとともに，業務改善や経営課題の解決に活用するニーズも高まっている．

こうしたニーズに応える実用例の１つとして，日立製作所が開発したフィジカルセキュリティ統合プラットフォームが挙げられる．このプラットフォームには，各種のシステム・装置・機能と連携する標準プラグインモジュールを多数用意しており，必要なセキュリティ対策や世の中のニーズ・課題に合わせ，各フィールドにモジュールを選択実装することでソリューション提供を行う．フィジカル空間にはフィジカルセキュリティシステム・IoT センサ・映像解析機能などと連携するモジュールを実装し，サイバー空間にはレポート出力・設備制御といったヒトやモノの動態の見える化･分析･制御するモジュールを実装する．

そして，データフィールドでは，データの収集・蓄積を行うとともに，フィジカル空間とサイバー空間を連携させることで動態管理や現場側へのフィードバックを可能とする（図 -4）．

■図 -4 フィジカルセキュリティ統合プラットフォームによるデータ活用

今後の展開

本稿では，Society 5.0 の実現に向け活用データの確からしさを確保し，さらにはランサムウェア事案の教訓から課題を整理し，今後求められる技術として，特にアセット管理およびディジタルエビデンスについて概説した．これらはサイバー・フィジカル連携フレームワークとして，単一組織だけでなく，サプライチェーンを構成する組織群，さらには社会全体のニーズとして実現すべき課題と考える．今後は，その課題解決に向け，技術開発や社会実装を通して，継続して社会に貢献していきたい．

参考文献

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（Oct. 2017），http://www.meti.go.jp/press/2017/12/20171226004/20171226004.html
2) （一社）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（Oct. 2017），http://www.keidanren.or.jp/policy/2017/103.html
3) 日立評論，Vol.100，No.3（May 2018）．

(2018 年 9 月 7 日受付)

宮尾　健　takeshi.miyao.ch@hitachi.com
1987 年東京大学工学部電子工学科卒業，1996 年ボストン大学コンピュータサイエンス科（修士）修了．1987 年（株）日立製作所に入社．社会インフラ向け制御システムの開発，経済産業省への出向等を経て，現在セキュリティ事業開発に従事．

谷本順一　junichi.tanimoto.xp@hitachi.com
1989 年広島大学大学院工学研究科博士課程前期システム工学専攻修了．同年（株）日立製作所に入社．公共・社会分野のシステムエンジニアリング等を経て，現在セキュリティ事業の企画業務に従事．