知創の杜

2019 Vol.3

FUJITSU

デジタル社会をしなやかに生き抜くために
―サイバー・レジリエンスを高める企業経営―

shaping tomorrow with you
社会とお客様の豊かな未来のために

株式会社 富士通総研
FUJITSU RESEARCH INSTITUTE

富士通総研のコンサルティング・サービス

社会・産業の基盤づくりから個社企業の経営革新まで。
経営環境をトータルにみつめた、コンサルティングを提供します。

個々の企業の経営課題から社会・産業基盤まで視野を広げ、課題解決を図る。
それが富士通総研のコンサルティング・サービス。複雑化する社会・経済の中での真の経営革新を実現します。

お客様企業に向けたコンサルティング

課題分野別コンサルティング

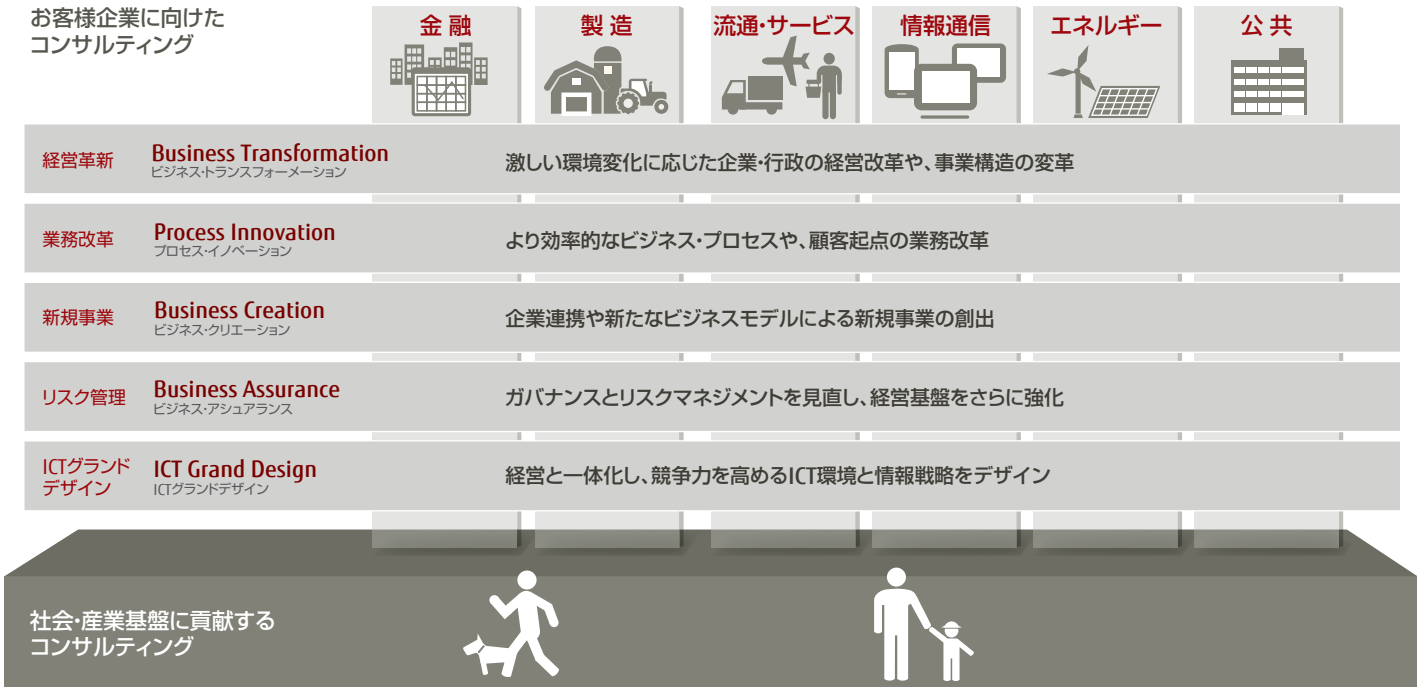
お客様のニーズに合わせ、各産業・業種に共通する、多様な業務の改善・改革を図ります。経営戦略や業務プロセスの改善などマネジメントの側面、そしてICT環境のデザインを通して、実践的な課題解決策をご提案します。

業種別コンサルティング

金融、製造、流通・サービスなど、各産業に特有の経営課題の解決を図ります。富士通総研は、幅広い産業分野で豊かな知識と経験を蓄積しており、あらゆる業種に柔軟に対応するコンサルティング・サービスが可能です。

社会・産業基盤に貢献するコンサルティング

国や地域、自然環境などの経営の土台となる社会・産業基盤との全体最適を図ることで、社会そのものに対応する真の経営革新、業務革新を実現します。



知創の杜

2019　Vol.3

CONTENTS

4 イントロダクション
デジタル社会をしなやかに生き抜くために
―サイバー・レジリエンスを高める企業経営―

5 特集
デジタル時代のレジリエンス経営

10 フォーカス
デジタル社会におけるレジリエンスとは

20 あしたを創るキーワード
データ保護に係る標準化と制度化の動向

25 ケーススタディ1
スマートファクトリーを実現するための
サイバー・レジリエンス

30 ケーススタディ2
AI×レジリエンス

デジタル社会をしなやかに生き抜くために
―サイバー・レジリエンスを高める企業経営―

近年の急速なデジタル技術革新によって、人々の生活やビジネスに破壊的な変化がもたらされています。このような変化の激しいデジタル時代においてビジネスの成長を続けるために重要な要素は、「アジリティ」と「レジリエンス」であると私たちは考えます。

「アジリティ」、いわゆる機動性や俊敏性を伴う変革が欠かせないことは、すでに多くの経営者の方々が認識され、自らの業界のデジタル・ディスラプションに向けた行動を起こされています。実際、多くの企業でデジタル部門や新規ビジネス部門を設置し、変化への適応や変革の推進のチャレンジに取り組まれています。

一方で、デジタル技術の活用はビジネスを新たな脅威に曝す側面も持つことに気をつけなければなりません。世界経済フォーラムが毎年発表しているグローバルリスク報告書においても、サイバー攻撃などのテクノロジーリスクは中長期なリスクとして近年は上位に挙げられています。

自然災害が近年多発し、改めてBCPに注力される企業も増えていますが、サイバー空間でも「危機の常態化（Crisis is the new normal.）」を前提とした「レジリエンス」の強化を経営アジェンダとして取り組む必要があります。それが、“サイバー・レジリエンスを高める企業経営”です。

本誌では、デジタル時代のレジリエンス経営をテーマに、安全保障や社会インフラ分野における動向から、製造現場における今後のセキュリティ・レジリエンスの姿、さらにはレジリエンスにおけるAI活用の可能性まで幅広くご紹介しています。デジタルトランスフォーメーションを支えるレジリエンス経営について、皆さまの理解の一助になれば幸いです。

特 集

デジタル時代のレジリエンス経営

株式会社富士通総研
ビジネスレジリエンスグループ
グループ長 藤本　健

グローバル規模で、経済活動から政府・社会インフラまで広く、クラウドやIoT、AIなどのデジタル技術が浸透していく動きが現在加速しています。いわゆるデジタル革新（デジタルトランスフォーメーション：DX）です。

DXは、Society5.0[注1]を実現する手段でもあり、サイバー空間とフィジカル空間が融合する社会では、ヒトやモノがすべてつながり、新たな脆弱性となり得ます。つまり、デジタル技術の活用が、企業活動を事業継続リスクやレピュテーションリスクに曝すことにもなるのです。

このようにDXによって変化するリスク環境の中で、経営にとって“レジリエンス”というテーマは、ますます重要になってきます。本稿では、これからの「レジリエンス経営」はどうあるべきかについて考えます。

執筆者プロフィール

藤本　健（ふじもと　たける）

株式会社富士通総研 ビジネスレジリエンスグループ グループ長

1996年 富士通株式会社入社後、コーポレート部門を経てコンサルティング部門に異動、2007年より株式会社富士通総研。主な専門はリスクマネジメント・危機管理。電力・ガスシステム改革のIT対応にも従事。近年は、事業継続やサイバーセキュリティに関するコンサルティング活動に注力している。

1. デジタル化によって変化するリスク環境

最初に、デジタル化によって変化するリスク環境について考えていきます。

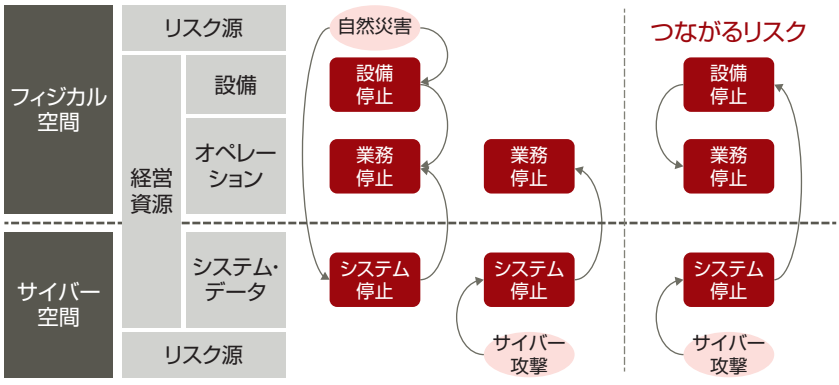
DXに伴うリスク環境の一番の変化は、セキュリティにおいて守る対象が“システム”に加えて、“データ”まで広がることです。これまでもプライバシー保護として、個人情報の保護については取り組まれてきましたが、個人情報のデータ化や、IoT・AIの活用拡大により、データが爆発的に増加するだけなく、データの価値が高まるに伴い、それらのデータの機密性や完全性が毀損されることによるビジネスへのインパクトは著しく大きなものとなります。また、AIやIoTにより生成されるデータについては、本当に信用できるのかという信頼性のリスクについても考えていく必要があります。デジタル社会、データ駆動型社会において、データの安全・安心・品質の確保は企業経営にとっても重要なテーマです。

また、デジタル化の流れにおいて、パブリッククラウドの活用は前提と考えるべきでしょう。欧米を中心に政府調達においては、クラウドファーストを掲げ、さらにはクラウドサービスの認証制度を導入するなど、パブリッククラウドの採用は世界的な潮流になりつつあります。日本においても、2018年に「政府情報システムにおけるクラウドサービスの利用に係る基本方針」において、“クラウド・バイ・デフォルト原則”を採用するとともに安全性評価の仕組みの検討に着手しています。

実はこれらのクラウドサービスに係る認証制度や安全性評価の議論は、一方でクラウド活用における潜在的なリスクを示唆しています。実際、SoE（System of Engagement）などは現場部門主導でパブリッククラウドを活用するシーンが増えていますが、IT部門の立場からすると、これらはいわゆるシャドーITの増加であり、統制が難しいシャドーITの増加は潜在的なリスクの高まりとして認識されることも多くなってきています。

もう1つは、“つながるリスク”です。IoTの活用により、現場から収集したデータをサイバー空間で分析したうえで、フィジカル空間の高度化として適用する、サイバーとフィジカルの融合はデジタル社会では当たり前になっていきます。

しかし、IoTが導入される工場系や制御系のネットワークは、これまではクローズドなネットワークとして運用されてきたため、オープンな環境に耐えられる構造になっていません。つまりオープンなネットワークとつながることで、それまで露呈していなかった脆弱性が狙われることになるのです。さらには情報システムの停止とは違い、サイバー攻撃により設備の稼働そのものが停止するなど、影響はフィジカル空間にまで及び、ひいては重要産業・重要インフラ企業のオペレーションまでもが停止し、国民生活の安心安全を脅かすことにもなりかねません。



●図1　フィジカル空間とサイバー空間におけるリスク源と経営資源の関係

2. デジタルリスクマネジメントに必要な取り組みとは

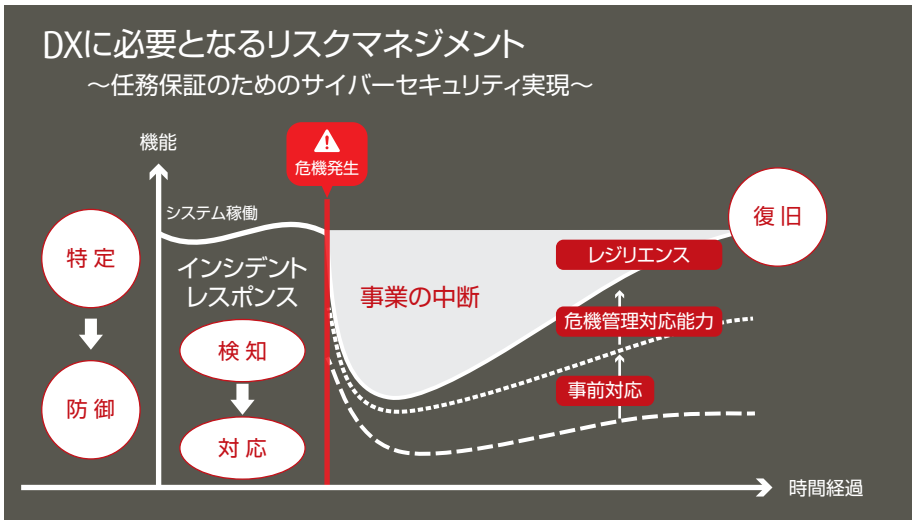
それでは、デジタル革新に必要なデジタルリスクマネジメントでは、どのような取り組みが必要になるでしょうか？

1つは、「検知」、「対応」、「復旧」の3つのレジリエンスの機能強化です。NIST（National Institute of Standards and Technology：米国国立標準技術研究所）のサイバーセキュリティフレームワーク、通称CSF（Cyber Security Framework）では、サイバーセキュリティの5つの機能、「特定」、「防御」、「検知」、「対応」、「復旧」が定義されています。この中でもCSFの特徴でもある、攻撃者による侵入を前提とした「検知」・「対応」・「復旧」の3機能は、レジリエンスの構成要素であり、近年の組織に求められるサイバーセキュリティの基本能力でもあります。デジタル革新を進めるに際しては、同時にデジタルリスクへの備えは不可欠であり、侵入前提でいかに被害を極小化するか、事業の中断時間をいかに短期化し、早期復旧させるか、などについて経営層が関与して取り組む必要があります。

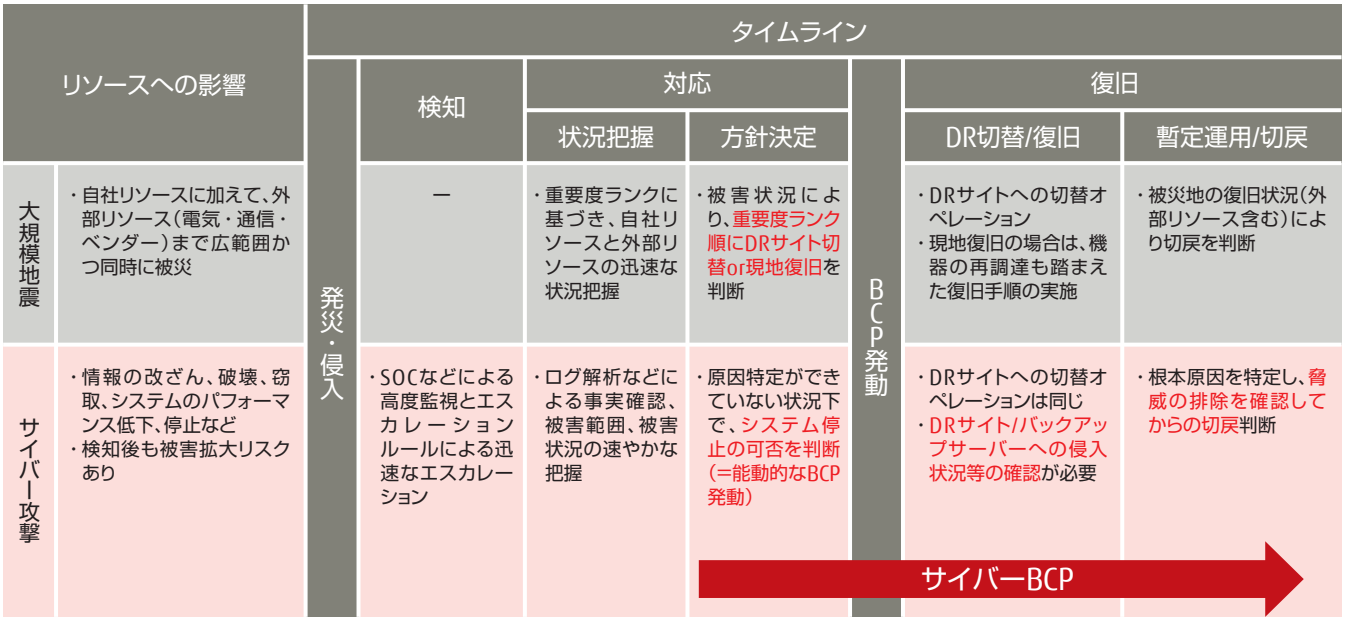
「検知」では、SIEM（Security Information and Event Management）などを用いた統合監視・分析基盤を全社的に整備するとともに、SOC（Security Operation Center）業務の自動化により、デジタル時代にさらに爆発的に増加すると考えられるセキュリティイベントからサイバー攻撃行動を検知、対処要否判断のさらなる迅速化が必要となってくると考えられます。このようなセキュリティ基盤は今後、より高度化が求められるため、自組織で整備する余力がない場合は、外部からサービスとして調達する選択肢も考慮すべきです。

「対応」では、訓練などを通じたCSIRT（Computer Security Incident Response Team）の実効性の向上に加えて、危機対策本部との連携構築など、経営層が関与する有事のセキュリティガバナンス整備が肝要となります。特に、IoTが増える現場においては、ITの現場と異なり、「対応」のプロセスや体制、いわゆるインシデントレスポンス体制が未整備なケースが多く、サイバー攻撃に対する組織・プロセスの脆弱性から被害拡大を招きかねません。具体的には、工場などにおいてもCSIRTの工場版としてのFSIRT（Factory Security Incident Response Team）の整備がデジタル化と並行して必要になります。

また、デジタル化後は、サイバー攻撃が重要インフラや重要産業のオペレーションを停止させるリスクも一層高まるため、「復旧」の機能として、BIA（Business Impact Analysis：ビジネス影響分析）に基づくデジタ



●図2　デジタルリスクマネジメントにおける取り組み



●図3　大規模地震とサイバー攻撃によるBCP/ICT-BCPの違い

ル資産（システム・データ）の仕分けと、それらの結果を踏まえたサイバー版BCP（Business Continuity Plan）の整備が必要です。日本では多くの企業がBCP/ICT-BCPを整備しているので、これらのナレッジを活用して、サイバー版BCPに補完的にアップデートすることが可能でしょう。

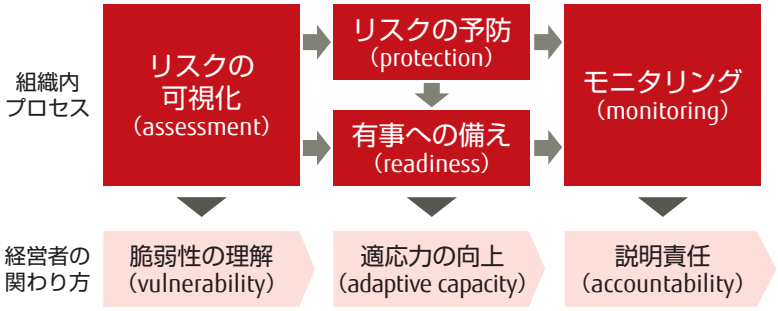
加えて、デジタルリスクの認識と評価がさらに重要になります。これまでは、BIAでは自然災害を前提にした重要システムの可用性の観点でのリスク分析でしたが、ここにデジタルリスクとして、データの完全性侵害がシステムの信頼性を脅かし、物理的な事故をも引き起こす脅威を理解・認識し、その重要度を評価する取り組みが必要です。これがNIST CSFでいうところの「特定」の機能となります。

もう1点、今後想定されるのがレギュレーションの強化です。いわゆるコンプライアンスリスクへの対応です。具体的には、防衛産業分野において、米国では国防総省（DoD）が政府調達の条件として、サプライヤーに対してNIST SP800-171[注2]への準拠を義務付けました。NIST SP800-171では、セキュリティの統合監視や環境分離、インシデント確認後72時間以内の報告など、従来よりも一段高いセキュリティレベルが、特にレジリエンス機能の領域で求められています。この流れは、他の重要インフラ産業へも拡がり、日本国内にも波及することが見込まれます。また、NIST SP800-171が求めるセキュリティ強度の議論は、現時点では特定の重要情報を包含するシステムに求められる話ですが、長期的にはグローバルスタンダードになることが予想されますので、DXを推進する企業は、NIST SP800-171レベルへのアップデートを視野に全社的なサイバーセキュリティ戦略の策定と実行にも取り組んでいく必要があると言えるでしょう。

3. レジリエンス経営への昇華

最後にデジタルリスクに対するレジリエンス強化をどのように企業経営への取り組みに組み込んでいくべきかについて触れたいと思います。

まず、重要であるのはデジタルリスクマネジメントのプロセスを組織内に実装する際、各プロセスにおいて経営層の関与の仕方と責任を明確にすることです。**図4**はデジタルリスクマネジメントのプロセスと経営者



●図4　デジタルリスクマネジメントのプロセスと経営者の関与

の関わりを示したものです。例えば、「リスクの可視化」は前述のデジタルリスクの評価を指しますが、経営者はこの評価結果から、自組織はどのようなデジタルリスクに曝されていて、どのような脆弱性があるのかを理解します。そのうえで、「リスクの予防」と「有事の備え（いわゆるレジリエンス強化）」において、デジタルリスクに対する適応力を向上させるために、経営者がリソース（ヒト・カネ）を投入する判断を行い、実行します。また、DXを進める企業において、サイバーセキュリティなどのデジタルリスクマネジメントをコーポレートガバナンスの一環として位置づけ、対外的な説明責任を果たすことも今後は考えていくべきです。そこで、やりっ放しにならないよう、自組織のデジタルリスクと脆弱性をモニタリングのうえ、アップデート（補強）していく、いわゆるPDCAの取り組みも必要となってきます。

このようなデジタルリスクマネジメントをコーポレートガバナンス・システムとして実装する取り組みをグループ会社やサプライヤーまで適用していくことで、真のレジリエンス経営へ昇華させることが可能となるでしょう。

また、レジリエンス経営へのデジタル技術の適用も今後のテーマとして考えていくべきです。例えば、AIを活用してサイバー攻撃を検知する技術はすでに実用化が進んでいますが、自然災害においても近年常態化している大型台風による災害は、AIを活用した被害予測により事前の備えが可能となり、被害拡大の抑制にもつながります。

デジタル時代のレジリエンス経営のもう1つのテーマとして、デジタル技術を活用したプロアクティブな活動、プレディクティブな活動にも積極的に取り組んでいくべきではないでしょうか。

（注1）　Society5.0：日本政府が提唱する科学技術政策の基本指針の1つ。狩猟社会、農耕社会、工業社会、情報社会に続き、新たな社会として提唱されているSociety5.0は、サイバー空間とフィジカル空間を高度に融合させ、経済発展と社会的課題の解決を両立することを目指している。

（注2）　NIST SP800-171：米国政府機関が定めたセキュリティ基準を示すガイドライン。政府機関だけでなく、取引企業からの情報漏洩を防ぐため、業務委託先におけるセキュリティ強化を要求する内容で、米国防省と取引している全世界の企業に対してNIST SP800-171への準拠が要求されている。準拠しない企業とその製品やサービスはグローバルサプライチェーンからはじき出される恐れがある。
「連邦政府外のシステムと組織における管理された非格付け情報の保護」
https://www.ipa.go.jp/files/000057365.pdf

フォーカス

デジタル社会におけるレジリエンスとは

グローバル規模で経済活動から社会インフラまで広く、クラウドやIoT、AI等のデジタル技術が浸透していく動きが加速しています。いわゆるデジタル革新（DX）です。

本対談では、デジタル化の進展により変化するリスク環境で「レジリエンス経営」はどうあるべきかについて、名古屋工業大学の渡辺教授、富士通株式会社の太田シニアエバンジェリスト、富士通総研（以下、FRI）の山口マネジングコンサルタントに語っていただきました。進行役はFRIの藤本ビジネスレジリエンスグループ長です。

（対談日：2019年10月18日）

対談者（敬称略 左から）　※所属・役職は対談当時のもの
山口　貴詩：株式会社富士通総研 ビジネスレジリエンスグループ マネジングコンサルタント
渡辺　研司：名古屋工業大学 大学院工学研究科 教授
太田　大州：富士通株式会社 シニアエバンジェリスト
藤本　　健：株式会社富士通総研 ビジネスレジリエンスグループ グループ長

1. デジタル×レジリエンスに関連した最近の活動

藤本　グローバル規模で経済活動から政府・社会インフラまで広く、クラウドやIoT、AIなどのデジタル技術が浸透していく動きが加速しています。いわゆるデジタル革新（デジタルトランスフォーメーション：DX）です。Socaiety5.0[注1]の実現手段でもあるDXが進む中、サイバーとフィジカルが融合して様々なものがつながるのに伴い、新しいリスクが顕在化しています。DXにより変化するリスク環境でレジリエンス経営はどうあるべきでしょうか？　渡辺先生には重要インフラのレジリエンス強化を推進される立場から、太田さんにはデータの安心・安全について提言活動されている立場から、山口さんにはNISCなどの公共事業や様々な重要インフラ事業者向けにレジリエンスコンサルティングを行う立場から、お話しいただきたいと思います。まず、デジタル×レジリエンスというキーワードに関連して最近の活動をご紹介いただけますか？

渡辺　「サイバー・フィジカル」[注2]は流行り言葉ですが、元々サイバーの片側面だけ考えればよいわけではなく、どんなビジネスも物理的なサービスや機器につながっているので、サイバーもフィジカルも両面考えなければならないということで、ようやく融合が始まったのだと思います。重要インフラにもすでにサプライチェーンリスクはあり、自動車産業などフィジカルの世界でも露呈している問題です。DXが進むとサイバー空間においても同様に、デジタルサプライチェーンリスクのような問題が起こります。デジタル化された調達の構造においてはデータやソフトウェアにボトルネックがあって、さらにそこに脆弱性があれば、そこから攻撃されます。サプライチェーンリスクのマネジメントについてはフィジカルの方が先行しているはずなので、新しい枠組みを作る話ではないし、サイバー空間の問題でも活用できる話です。そういう意味でも今まで別々だったサイバーとフィジカルがレジリエンスというキーワードでようやく統合された気がします。

太田　サイバーセキュリティについては日本では情報漏洩という観点で見ている経営者が多く、防御中心の対応でした。2012年頃から、米国のサイバーセキュリティへの動きが単に防御ではなく、検知から対処・復旧するというレジリエンスの考え方に基づいているとわかりました。この辺を調査・研究してみると、NIST（National Institute of Standards and Technology：米国国立標準技術研究所）がきちんと機能して、その基準を政府が活用して自身のレジリエンス力を高める政策を実施、民間企業にも適用を拡げるという、国としての戦略論が明確に見えたので、これは日本も倣うべきだということで、私は活動をしてきました。「No Security, No Digital」と講演していますが、サイバーセキュリティの考え方をグローバルな基準でしっかりやっていかなければということと、GDPR（General Data Protection Regulation：一般データ保護規則）が始まって、データの利用だけでなく保全もしっかりやらないとペナルティが来るので、経営のリスクになると捉えています。サイバーセキュリティでは米国やイスラエルの技術に頼っているので、安全保障面から独自技術を持つべきという技術研究開発と人材育成の課題もあり、国への提言や民間企業への啓発活動をしています。

山口　私はリスクマネジメントの専門家として、コンサルティングサービスを提供しています。最近はサイバーセキュリティマネジメントをメインテーマに活動していますが、これまでもBCP/BCMや内部統制など、リスクマネジメント分野全般で活動してきました。また、富士通本社のリスク管理部門で約3年にわたり、リスクマネジメントの実務にも携わった経験を活かしています。

2. 重要インフラ事業者に学ぶデジタル時代のレジリエンス

藤本　DXが進むと、従来のシステムの可用性という観

点から、今後はデータをいかに守るかが非常に重要になってきます。今後IoTやAIが増えて、かつデータの価値が高まると、データが損失した際のビジネスインパクトが大きいと思います。今後DXを進める企業はどういうリスクに気をつけていくべきか、それぞれのお立場でお話しいただけますか？

渡辺　重要インフラ事業者の多くは制御システムを持っているので、政府の重要インフラ専門調査会等では悪い奴がいる前提でサイバーセキュリティの議論を進めていました。しかし、今は自然災害も含め、悪い奴がいなくても脆弱性がある部分に手を加えなければいけないし、攻撃される以前の脆弱性自体の問題も議論されています。重要インフラ事業者は、元々国民生活や社会経済活動に対するサービスを維持する義務があるので、デジタルで始まった議論にフィジカルが入ってバランスがとれてきました。サービスについてもレジリエンスの考え方が入ってきて、時と場合により能動的に止めなければいけないというモードに変わってきています。サイバー攻撃を受けて、止めないとコントロールできなくなる状態に陥った場合、能動的にサービスを止める判断ができるか、経営レベルの問題として議論しています。IT-BCPでもいかに継続するか、という可用性が重んじられてきましたが、場合によっては止めることがレジリエンスなのです。

渡辺　研司（わたなべ　けんじ）
名古屋工業大学
教授・リスクマネジメントセンター防災安全部門長
1986年 京都大学卒業、同年 富士銀行入行、米国駐在（ストラクチャード・ファイナンス）、システム開発・企画他。1997年プライスウォーターハウスクーパースに移籍、国内外企業向け金融ビジネスに関わるコンサルティングに従事。2003年 長岡技術科学大学准教授（経営情報系）。2010年4月より現職。内閣重要インフラ専門調査会・会長、国土交通省運輸審査会運輸安全確保部会・専門委員、経済産業省ISOセキュリティ統括委員会・委員、ISO/TC292（Security and resilience）・エキスパート、日本政策投資銀行BCM格付けアドバイザーなどを兼務。工学博士、MBA。

藤本　確かに重要インフラはフィジカル面で従来もレジリエンスに取り組まれてきているので、能動的に止めるという議論は、DXを進める企業は参考にできるかもしれません。一方で、重要インフラの方々は絶対停止させない使命感をお持ちなので、能動的に止める難しさもあると聞きますが、いかがですか？

渡辺　難しいですが、電力分野の一部では制御権をとられるくらいなら止める判断をしなければならないと考えるようになりつつあります。ビジネスインパクトだけでなくソーシャルインパクトを考慮して、止めるまで2時間稼げるなら、その間、例えばメディアや政府広報を使うなどして、世の中にコミュニケーションして皆に備えてもらうというモードで考える人たちも出てきました。止まらないようにすることだけをいくら頑張っても、それを突破されて止まった瞬間に人々や都市が混乱するだけなので、止めないようにすることにも限界を感じていると思います。北海道のブラックアウトのようにオートメーション化し過ぎたものが突然落ちてしまうのは、技術的にコントロールし得ない状況が起こり得るということです。だからこそ、能動的な安全停止のような考え方が重要かと思います。

藤本　能動的に止めるメリットは、止めるまでの時間を確保して準備できるのと、リスクコミュニケーションがとれることで、そこをプロアクティブにやることが大事ということですね。

太田　今まで人間は必ずコントロールできるという前提に立って動いてきたものが、2011年に福島の原発がコントロールできなくなって、重要インフラではそういうことが起こり得るという価値観が業界で共有され始めたという理解でよろしいですか？

渡辺　少なくとも現場では「最悪の事態」は起こり得るという前提が共有されたと思います。そのうえで、「自分たちはここまではリスクをコントロールしている。そして残存するリスクはこうである」と言っておかないと、後で無限責任を問われるような事態になりかねません。

3. 安全保障としてのデジタルレジリエンス

藤本　次に冒頭に太田さんからお話がありましたNISTのガイドラインの動向について伺います。米国では、NISTガイドラインへの適合が義務化される動きが政府や防衛産業、重要インフラ企業中心に進んでいるようですが、この辺について教えてください。

太田　米国、イスラエル、オーストラリアなどでサイバーセキュリティを社会でどう回しているかというと、「サイバーセキュリティは安全保障のためにやる」という価値観が共通しています。安全保障の一環としてやっているので、人材のローテーションもファンドもきちんと回っています。実は日本はそれをなかなか真似できていません。なぜならセキュリティ・クリアランス(注3)という日本では非常に超え難い壁があるので、国防を民間と一緒にやるという概念も生まれてこないのです。そんな環境だったので、一度はビジネスに対する熱意を失いかけたのですが、そんな時に、「ルール」ってあるよね、と気づきました。それは2010年に米国がNISTに作成を依頼したルールで、NISTが作るのは政府調達のための基準書ですが、これを社会実装して、ルールとしていかに社会全体の安全性を高めるか、という安全保障としての戦略論がしっかりしていたのです。そこで、ルール形成が非常に重要なのだと認識しました。最も注目すべきは2017年12月にDFARS（米国防総省調達規則）でDoD（米国防総省）の指令によりDoDに納める業者はSP800-171(注4)への適合が義務化されたことです。米国の航空・宇宙業界から発注を受ける日本企業を救わなければと、富士通でもクラウドサービスを立ち上げると同時に、日本の防衛産業も適合できるようにした方がいいと防衛省にお話しました。現在、防衛省でも米国と同様の仕組みの準備を進められています。

太田　大州（おおた　たいしゅう）
富士通株式会社
シニアエバンジェリスト
1980年 富士通株式会社入社。複合情報通信システム分野の商品開発、東京シティホールや東京国際フォーラムなどインテリジェントビルシステム構築に従事。1995年 消防指令管制システムの開発、お客様サポートを担当。2005年より情報セキュリティ、事業継続（BCM）のビジネスを担当し、お客様・社会の安心安全イノベーションを促進。2015年6月より初代エバンジェリストとして、社会的な視点でのサイバーセキュリティの課題解決に向けて、「国産セキュリティ自給率の向上」を目標に国産技術の醸成・普及、人材育成支援に関する活動を強化推進中。

藤本　米国は安全保障の観点で戦略的に進めているという話でしたが、日本の重要インフラ周りの方向性はいかがでしょう？

渡辺　サイバー・フィジカルと並行してサプライチェーンリスクについての議論が展開されていますが、SP800-171では完成品メーカーにサプライヤーのセキュアな状態を保持するコスト負担義務があります。防衛

分野まで強くないにしても、重要インフラのサービスを提供しているのは重要インフラ事業者自身ですので、サービスの安定供給のためにサプライチェーンの安全を確保する義務があり、取引関係で下請けを圧迫するのではなく、一緒に訓練やトレーニングなどを能動的にやらないといけません。様々な企業から調達していても何かあれば、責められるのは重要インフラなので、積極的・主体的にサプライチェーンを構成する企業群と協力して強くしていく必要があります。

太田　そのお話を聞いて思いましたが、先日の台風15号の時はサプライチェーン含めて様々な人たちが協力し合ったわけですが、電力の復旧は結局、東京電力に頼るしかないわけですよね。そう考えると、代替が可能な企業と不可能な企業とがあって、代替不可能な企業に対しては、安全保障の文脈で考えるべきではないでしょうか。

渡辺　ナショナルセキュリティの観点からすると、重要インフラ事業は国営に戻すか、最後は国が責任をとるような考え方もあります。今さら国営に戻す議論はないでしょうが、発電・送配電が分社化で組織が分かれてしまっても、危機管理、防災やサイバーセキュリティは一体的にやるべきです。加えて、ファンダメンタルな部分での国のサポートやセーフティネットは、国民生活の安心・安全のためにも必要だと思います。

太田　中国が全体国家主義で自由経済主義を取り入れている内容はEconomic Statecraft(注5)で、安全保障の観点で全部コントロールする考え方であり、民間企業も国が支援しています。日本において民間のみで稼ぐのは限界に近いと思います。米国の30年間のGDPはリニアに伸びていて、中国も2008、9年頃から盛り上がって日本を抜いていますが、日本は1993年以降、横ばいです。リニアに伸びる戦略こそ国家の戦略論で、米国も中国もそれを通じて国力を強くしているのです。

4. コンサル現場に見るデジタルリスク

藤本　フィジカルでは経済活動と安全保障のバランスをどうとるかは事業者側に委ねられているきらいがありますが、DXの推進においては、事業者や一企業に委ねるのではなく、国が戦略を持つべき、ということですね。では、コンサル現場のトレンドについてはいかがでしょうか？

山口　交通インフラのお客様では、ICT部門で把握している情報システムは重要インフラを支えるシステムのごく一部で、大半は各事業部門が所管する制御システムです。これらシステムのリスクアセスメントをしてみると、情報システムと違い、制御システムを運用する事業部門はセキュリティリテラシーが高くないという状況がわかりました。デジタルとフィジカルの融合により、制御システムもインターネットや他のシステムにつながる部分が増えていて、サイバーリスクが高まっていますが、サイバーセキュリティ対策が十分でないのが実態です。制御システムはどうしてもメーカーや

山口　貴詩（やまぐち　たかし）
株式会社富士通総研
ビジネスレジリエンスグループ マネジングコンサルタント
2003年 富士通株式会社入社、コンサルティング部門に配属、2007年より株式会社富士通総研。主な専門はリスクマネジメント、事業継続マネジメント、サイバーセキュリティなど。近年はBCP/BCM整備、危機対応教育・演習支援、リスクマネジメント構築、サイバーセキュリティに関するコンサルティングに従事。

運用会社などのパートナーに依存せざるを得ないので、インシデントが起きた場合の体制整備を外部パートナーと共同で実施する必要があります。

藤本　最近、FSIRT（Factory Security Incident Response Team）という単語を初めて聞きました。今まで工場はクローズドネットワークを前提に運用されていたので特にセキュリティレベルが低く、IoTやスマートファクトリーでつながることで、曝されるリスクがあります。交通系のインフラも大きなプラントと同じようなものですね。

渡辺　ある交通系の重要施設で同じスイッチの下に空調と対顧客用の通常業務システムがぶらさがっていて、そこから攻撃すれば空調が止められることがわかってしまいました。意外なところでIoT機器がつながっていて気づかないです。

山口　現場にヒアリングすると、クローズドだと主張しても実はつながっているケースが割とありますね。部門縦割りで、システム間連携も把握できていないといったことが原因です。

太田　それは設計段階でサイバー攻撃のリスクが考慮されていないということですか？

山口　そうですね。そこまで考慮されずに設計されて、運用されています。あと、ネットワークの専門家からすると、従来の工場ネットワークはただの配線でネットワークセキュリティの概念がないそうです。

太田　ローカル5G[注6]になったら、こっちにもあっちにもつながっているとなるので、防衛線を超えられたら大変ですね。

渡辺　フィジカルだと配線で見えますが、デジタルになると、つながっているところが見えないというのは怖いです。

藤本　制御系では保守ルートからの侵入はよく聞く話です。IoTが増えて、現場のDXが進むと、現場でのサイバーリスクが増大するので、認識を改める必要があると思います。

5.「強靭性」ではなく、「しなやかな復元力」・「弾力性のある回復力」

藤本　次にレジリエンス経営というお題で、経営層をいかに巻き込むかについて議論を進めたいと思います。

渡辺　レジリエンス経営の考え方は、やられる時はやられるので、それをどう戻していくかということだと思います。政府系ではレジリエンスを「強靭性」と訳すケースが多いのですが、それは本来ロバストネス（robustness）だと思います。以前、経産省が定義していた「しなやかな復元力」とか「弾力性のある回復力」が、本来の意味合いを表した訳だと思います。重要インフラの経営も民営化により効率化されましたが、その一方で、安全も担保しながら収益も上げなければいけないことについて限界を感じていますし、それが露呈するような事案も自然災害による事案では散見されるようになりました。止める時は止めるし、自らが認識している残存リスクをコミュニケーションしながらユーザーにも備えてもらうことをお願いせざるを得なくなってきています。

藤本　全部コントロールできるという考え方を変えていかなければということですね。

渡辺　いくら強靭性を求めても、それだけでは、やられた時にお手上げ状態になりますが、やられた時にはモードを変えて、どちらの方向にどのスピードで戻っていくか、残されたリソースを見ながら、「あと何時間」といった猶予を適時に公表すれば、世の中はその時間軸で備えていきます。最近の台風で交通機関が計画運休する

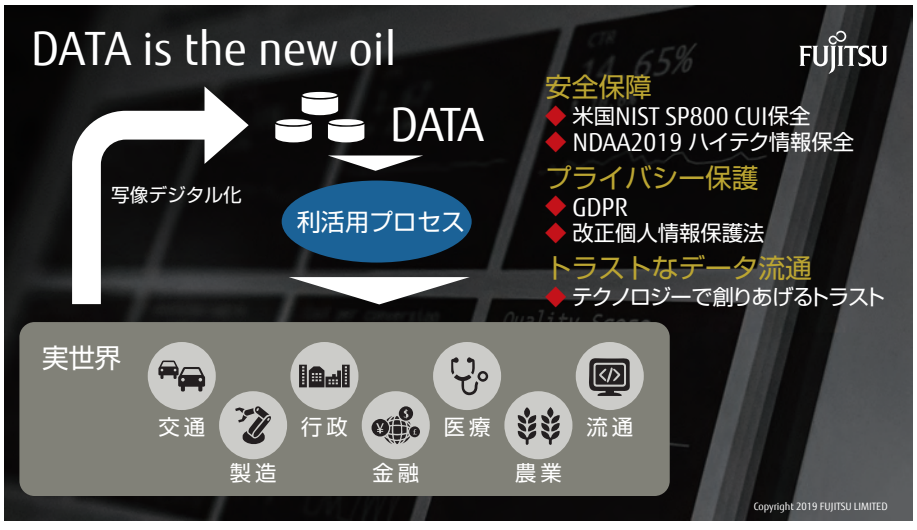
のと同じ議論です。止めてはいけないと頑張って突然止まるのが一番困るので、あと何時間でダメです、という報告を社長に上げて記者会見したり、ユーザーに迷惑かけないようその時間内にやるべきことを伝えたりする義務が重要インフラ事業者にはあります。止めざるを得ない状況は政府からもアナウンスしてもらい、その時間内で国民も備える、といった構図が国全体のレジリエンスだと思います。

藤本　台風や大雨の際のダムの緊急放流も同じですか？

渡辺　そうです。ある程度の時間の余裕をもってデータをダウンロードし、システムを止める人は止め、バックアップに切り替え、皆で備えていく。正面から立ち向かうより、やり過ごす。そういうことを重要インフラが率先して社会を巻き込んでやっていく。その時政府によるフォローは不可欠です。交通機関の計画運休も社会で認知される4、5年前は苦情が出ました。でも、最後まで動かすから皆帰れなくなるのです。重要インフラは能動的に勇気をもって止めなければいけない判断力を持ち、社会はそれに応えて活動を「縮退」すべきです。

6. レジリエンス経営を支える「トラストな社会」

太田　レジリエンス経営はそういう最悪の状態をプロアクティブに発見することに力を向けた方が現実解として有効ですね。今までセキュリティは静的情報を守ることを考えていましたが、デジタル時代のデータはダイナミックです。「データは21世紀のオイル」と言われますが、原油は利用目的に応じて精製するテクノロジーと、それを安全に使って保管・流通させるルールとがマッチして運用されています。DXは現実世界から来るデータが常時書き換えられていくデータ利活用のプロセスが回り始めることなので、データに関連する安全保障やプライバシー保護のルールやトラストなデータ流通を支えるテクノロジーの内容を細かく確認していく必要があります。1つは安全保障観点からNISTで要求されるCUIや国防権限法のハイテク情報で、下手に扱って出てしまうと制裁金が課せられます。もう1つは企業間取引と同様に経営インパクトが大きい情報です。さらにGDPRや個人情報保護法、ペナルティを伴うプライバシー情報が各国にあり、このプロセスで個人情報を回すと、リスクがどんどん入ってくることを認識しなければなりません。データをやり取りする相手を信頼できる相



●図　データ利活用プロセスに関連するルールとテクノロジー

手として認識する必要もあります。それらが克服された社会を私たちは「トラストな社会」と呼んでいますが、インターネットの中に信頼できる者だけつながる仮想ネットワークを構築してデータを流通させ、レギュレーションや法律で求められるものを保全できる空間をシェアして使う考え方です。ガバナンスも含め、データの真正性や完全性を担保する考え方も必要になると思います。

藤本　従来は機密性や可用性ですが、デジタルでつながる世界では完全性、真正性が重要だという意味で、信頼できる人たちのインビテーションネットワークなのですね。

藤本　健（ふじもと　たける）
株式会社富士通総研
コンサルティング本部
ビジネスレジリエンスグループ グループ長
1996年 富士通株式会社入社後、コーポレート部門を経てコンサルティング部門に異動、2007年より株式会社富士通総研。主な専門はリスクマネジメント・危機管理。電力・ガスシステム改革のIT対応にも従事。近年は、事業継続やサイバーセキュリティに関するコンサルティング活動に注力している。

太田　日本はマイナンバーも法人番号もきっちり定義されているので、チャンスがあります。しっかり社会実装できるインフラとして空間を作っていくことが次の目標です。

7. BCPのナレッジをベースとしたレジリエンス経営

山口　BCP/BCMの対象脅威は自然災害で、多くは大規模地震を想定して作られています。予防的に対策しても防ぎきれないから事後対応が重要という意味では、サイバーセキュリティとBCP/BCMの親和性は高いです。そういった文脈で「サイバーBCP」という言葉を使うことがありますが、BCP的な考え方でセキュリティ対策をどうやるかを考えなければなりません。大規模地震対象のBCPとサイバーBCPの違いは、地震は起きたことが明白で、ある程度被害は固定化されますが、サイバーセキュリティのインシデントは発生しているかもわからないところからスタートするので、検知が重要なことと、原因もわからない状況で能動的にシステムを停止する意思決定が必要になることです。そこがポイントです。

藤本　「サイバーBCP」というのは正しいでしょうか？

太田　BCPの考え方をサイバーセキュリティに当てるのは賛成です。マネジメントプロセスを回していることに対しては、可用性の観点で見れば、原因はともかく止まる結果は同じなので、その箇所へのサイバー攻撃をどうするのかという観点で見ればいい。「サイバーBCP」と言わず、BCPのリスク要件としてサイバーセキュリティがあるという位置づけにすればよいのではないでしょうか。「サイバーBCP」と普通のBCPがあるのではなく、経営リスク要件として位置づけたいです。BCPはレジリエンス経営に絶対必要です。今後、その対象をIoT時代は広げるべきだと思います。

渡辺　位置づけや背景をきちんと説明しないと、IT-BCPのITがサイバーになっただけになります。BCPの継続戦略や復旧目標時間などとは無関係に、ITやネットワークは二重化してデータはバックアップすればいいという時代の不幸を繰り返したくないので、BCPの枠組みにサ

イバーをはめ込む方がいいです。

太田　SP800-171でも可用性の話はしていて、データが回り始めると、回らなくなった瞬間に現場プロセスが止まってしまう脅威があるので、その意味でも可用性も大事です。

藤本　そこはスタティックなデータですか？

太田　フローし始めるからダイナミックです。

山口　レジリエンス経営ではコーポレートガバナンスの観点もあります。経産省が6月に公開した「グループ・ガバナンス・システムに関する実務方針」では、コーポレートガバナンス・コードの趣旨を踏まえて、グループ全体でのガバナンスのあり方を示しています。その中の「有事対応のあり方」がレピュテーションマネジメントで、「問題を把握した初動として事案の重大性を見極めて、公表が必要と判断した場合には迅速な第一報を優先させて誠実な謝罪と正確な説明を心掛けるべきである」とあります。レジリエンス経営という意味では、コーポレートガバナンスとして有事対応も含めたあり方を実装していくことが求められると思います。

渡辺　有事にもグループ全体でガバナンスを効かせなければいけないということですかね。早く告知して、シャットダウンして、「ここまでやられました、しかしここからはやられていません」といった状況を刻々と能動的に対外発信していかないと、プレスが先に出るのはまずいですからね。

藤本　能動的に止めつつ、リスクコミュニケーションしていく中で伝えていくということですね。

渡辺　大丈夫と言っていながら突然止まると、レピュテーションは地に落ちます。「ダメになる可能性が高まりましたが、あと〇〇時間頑張るので、その間にこう備えてください」といった残存リスクをユーザーに伝える義務を果たさなければなりません。千葉の停電の復旧見込みが何度もずれ込んだケースも電力会社とユーザー、さらには政府との間で認識のギャップが生じて、レピュテーションにも大きな影響がありました。

8. 今後に向けたメッセージ

渡辺　デジタル時代になっても、デジタルばかりやっていると、フィジカルが疎かになるので、統合しなければいけないモードになってきました。サイバー・フィジカルというフレームは有効なので、デジタルとフィジカルのバランスを考えなければならないことを忘れないことです。入口や途中はデジタルでも、最後の出口はフィジカルなので、出口もきちんと担保しないと、データやネットワークだけ守っても仕方ありません。世の中全体がデジタルにシフトしていますが、フィジカルと融合してバランスをとることを考える時代に来たと思います。

太田　DXの世界は日本が挑戦すべきテーマだと思うので、それを実現するための技術開発とルール形成と人材育成をしっかりとやっていけるように取り組んでいきたいと思います。

山口　デジタル化は業種問わず進み、サイバーとフィジカルの融合も進行する中、セキュリティの確保とレジリエンスの向上が必要だと思います。現状はお客様の意識の温度差が業界や個社、情シス部門と事業部門、現場と経営層であります。その解決には、リスク感覚や危機意識を浸透させて共通認識にする土壌を作るために共通言語と場を備えることが必要です。そこで専門知識を持つコンサルタントとして貢献したいと思います。

藤本　データだけでなく、その先の出口まで考えることが重要だと思います。技術、ルール形成、人材育成

も対応する必要があります。人材育成としてリスク感度、共通認識を図る共通言語を作ることも肝要です。本日はありがとうございました。

（注1） Society5.0：日本政府が提唱する科学技術政策の基本指針の1つ。狩猟社会、農耕社会、工業社会、情報社会に続き、新たな社会として提唱されているSociety5.0は、サイバー空間とフィジカル空間を高度に融合させ、経済発展と社会的課題の解決を両立することを目指している。

（注2） サイバー・フィジカル：実世界（フィジカル空間）にある多様なデータをセンサーネットワーク等で収集し、サイバー空間で大規模データ処理技術等を駆使して分析/知識化を行い、そこで創出した情報/価値によって、産業の活性化や社会問題の解決を図るもの。

（注3） セキュリティ・クリアランス：職務上、機密情報を取り扱う必要のある人物に対し、職歴や家賃等の滞納歴、犯罪歴等を確認し、ふさわしい人物であることを証明するプロセスのこと。欧米では、政府機関だけでなく民間企業でも導入されている。日本でも、機密情報にアクセスできる人物に対し、セキュリティ・クリアランスを実施し、認定する制度の創設が検討されている。

（注4） NIST SP800-171：米国政府機関が定めたセキュリティ基準を示すガイドライン。政府機関だけでなく、取引企業からの情報漏洩を防ぐため、業務委託先におけるセキュリティ強化を要求する内容で、米国防省と取引している全世界の企業に対してNIST SP800-171への準拠が要求されている。準拠しない企業とその製品やサービスはグローバルサプライチェーンからはじき出される恐れがある。
「連邦政府外のシステムと組織における管理された非格付け情報の保護」
https://www.ipa.go.jp/files/000057365.pdf

（注5） Economic Statecraft：経済的手段によって安全保障上の目的＝地政学的な国益を実現すること。

（注6） ローカル5G：大手通信事業者ではない一般企業や自治体等が主体となり、個別ニーズに応じて構築する局所的な5G（第5世代移動通信システム）ネットワーク。

あしたを創るキーワード

データ保護に係る標準化と制度化の動向

株式会社富士通総研
ビジネスレジリエンスグループ
コンサルタント　小泉　早優佳

IoTやAI等のデジタル技術が浸透し、社会が変革していくデジタルトランスフォーメーション（DX）の動きが加速しています。このデジタルトランスフォーメーションの進展によって、サイバー空間とフィジカル空間が高度に融合したSociety5.0[(注1)]が、現実のものとなりつつあります。Society5.0のような社会では、データが動力となり、価値を持ちます。そのような価値あるデータを保護しようとする動きが世界的に出てきています。本稿では、米国によるセキュリティガイドラインNIST SP800-171を中心に、データ保護に係る標準化と制度化の動向についてご説明します。

執筆者プロフィール

小泉　早優佳（こいずみ　さやか）
株式会社富士通総研 ビジネスレジリエンスグループ コンサルタント
2018年 株式会社富士通総研入社。国や民間企業のサイバーセキュリティやリスクアセスメント、リスクマネジメントに関わるコンサルティング業務に従事。NISTをはじめとするセキュリティガイドラインや法規制、また関連する社会動向に関する調査にも取り組む。

1. データ利活用の動き

2019年1月、ダボス会議で、「Data Free Flow with Trust」という概念が日本政府によって提言されました。公平かつ安全で信頼性のあるデータの国境を越えた自由な流通を意味するこの概念は、日本政府が目指す新たなIT政策の1つで、データ利活用の促進に向けた取り組みでもあります。データを収集、蓄積、加工、分析し、それを活用することで新たな価値を生み出そうとするデータ利活用の動きは、今あらゆるところで加速しています。デジタル時代において、新しい価値を生み出すデータは、今や「21世紀の石油」と言われるほど価値のあるものと考えられています。一方、価値あるデータを取り扱うことにはリスクが伴います。個人情報にはプライバシーの問題、機密情報には企業経営や安全保障の問題がつきまといます。

2. データ保護の流れ

米国が英国等と共同開発した最新鋭ステルス戦闘機「F35」。この設計に関する機密情報が中国のサイバー攻撃によって漏洩していたことが発覚しました。攻撃を受けたのは請負業者であるオーストラリアの防衛企業であり、近年リスクの懸念が高まっているサプライチェーンからの情報漏洩でした。戦闘機の設計に関する情報のような機密情報の漏洩は国家の安全保障を揺るがす問題です。このようなサプライチェーンからの情報漏洩が引き起こす安全保障への影響を懸念し、米国は法規制をかけました。2018年に国防権限法（NDAA：National Defense Authorization Act）を成立させ、ファーウェイ等、一部の中国企業による製品の調達を禁じたのです。

このように、今、データを保護しようとする動きが世界的に出てきています。米国では、2010年11月の大統領令（Executive Order 13556）を皮切りに、データ保護の取り組みが強化されています。2015年には、管理すべき重要情報（CUI：Controlled Unclassified Information）の保護を目的として、米国国立標準技術研究所（NIST：National Institute of Standards and Technology　以下NIST）によるセキュリティガイドラインNIST SP800-171が施行され、グローバルスタンダードになりつつあります。EUでは、NIST SP800-171で求められている内容と整合をとる形で、一般データ保護規則（GDPR：General Data Protection Regulation）が施行されました。

データ保護の動きは他産業に先駆け、とりわけ防衛産業で進んでいます。米国国防総省（DoD：Department of Defense）は国防総省調達規則（DFARS：Defense Federal Acquisition Regulation Supplement）によって、管理すべき重要情報（CUI）を開示する取引企業に対し、NIST SP800-171への適合を義務化しています。元請企業だけでなく、下請け等のサプライチェーン上のすべての企業が対象で、適合できていない場合は取引先から除外される可能性もあり、米国国防総省（DoD）のサプライチェーン上にある日本企業も対応を求められている状況です。

NIST SP800-171への適合状況の確認は、米国国防総省（DoD）との契約時に請負企業が自己申告する形で行われてきましたが、2020年度からは米国国防総省（DoD）による認証制度（CMMC：Cybersecurity Maturity Model Certification）が開始されることが公表されました。この認証制度は、企業のサイバーセキュリティレベルを5段階で評価するもので、レベル3までは、NIST SP800-171の要件をすべて満たす必要があると思われます。この評価制度は現在検討段階にあり、正式な公開は2020年1月を予定しています。認証は第三者機関によって行われ、2020年6月からは情報提供依頼書（RFI）、2020年秋からは提案依頼書（RFP）への応札の際に、認証書の提示が求められるようになる見込みです。

日本でも、NIST SP800-171と同レベルまで強化された防衛装備庁による新セキュリティ基準が2021年度から導入される予定です。また、適合状況を監査する仕組みも検討されています。

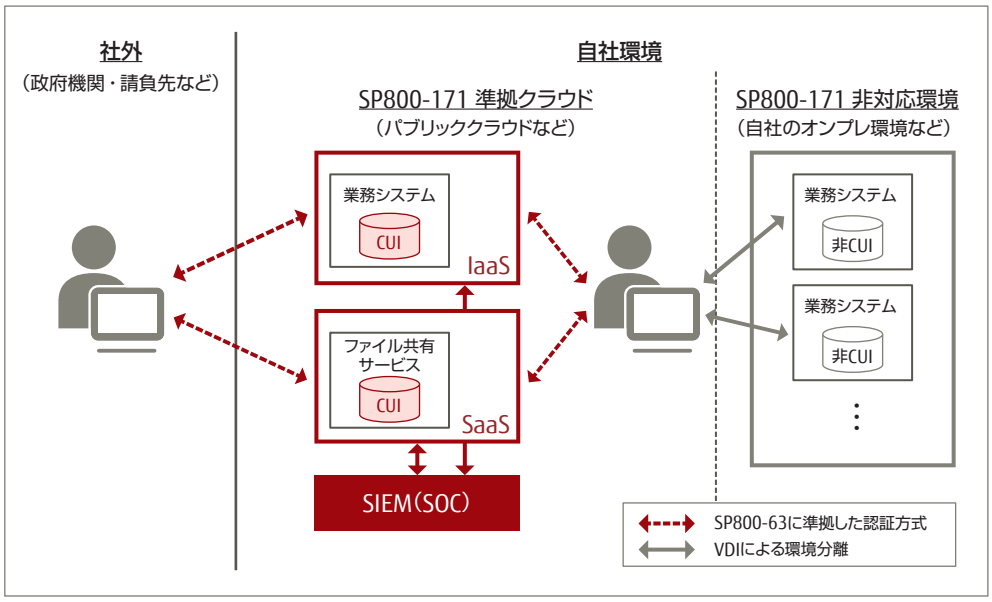
3. NIST SP800-171で求められていること

NIST SP800-171には、先述の管理すべき重要情報（CUI）という概念が定義されており、例えば、製品の設計図や、インフラ施設のセキュリティ情報、個人の健康情報等がこれに当たります。定義は分野ごとに各省庁が定め、米国国立公文書記録管理局（NARA：National Archives and Records Administration）が管理、公開していますが、記載が曖昧であるため、管理すべき具体的な重要情報（CUI）を定義する際は、契約元の政府機関と協議する必要があります。

NIST SP800-171は、14のファミリーと呼ばれる項目と、技術要件と非技術要件の全110要件からなっています。中でも特徴的なのは、暗号化、環境分離、多要素認証、ログの統合監視を求めている点であり、具体的には、情報を輸送する際には暗号化を実施すること、ネットワークの物理的または論理的環境分離を行うこと、認証には2つ以上の異なる要素を組み合わせる多要素認証を用いること、ログの横断的分析を可能にするための統合監視を行うことが要件として記載されています。本稿では、認証とログの統合監視について、次に解説いたします。

認証においてポイントとなるのは、アイデンティティ認証です。アイデンティティ認証とは、本人確認（プルーフィング）と資格証明（クレデンシャル）によって認証を行うことです。例えば、ユーザー登録を行う際は、ある人物が本当にその人物であるということ、すなわち本人確認を、パスポートや運転免許証等によって行います。本人であることが確認された後、その人物の職務や与えられている権限等に応じて、資格証明（クレデンシャル）を発行します。データにアクセスする際は、この資格証明（クレデンシャル）を用いて認証を行うことで、アクセスしている人物が本人であること、また資格を持ったふさわしい人物であることを担保することができます。NIST SP800-171では、誰がどの情報にアクセスできるかを厳格に管理することが求められていますが、アイデンティティ認証を行うことで、これを実現することができます。またアイデンティティ認証は、機密情報を取り扱う人物に対し、その適格性を判断するために行う、セキュリティ・クリアランス(注2)のような役割を果たしていると言えます。なお、具体的な管理策については、NIST SP800-63という電子認証に関するガイドラインを参照する必要があります。

ログの統合監視におけるポイントは、SIEM（Security



●図1　NIST SP800-171適合のイメージ

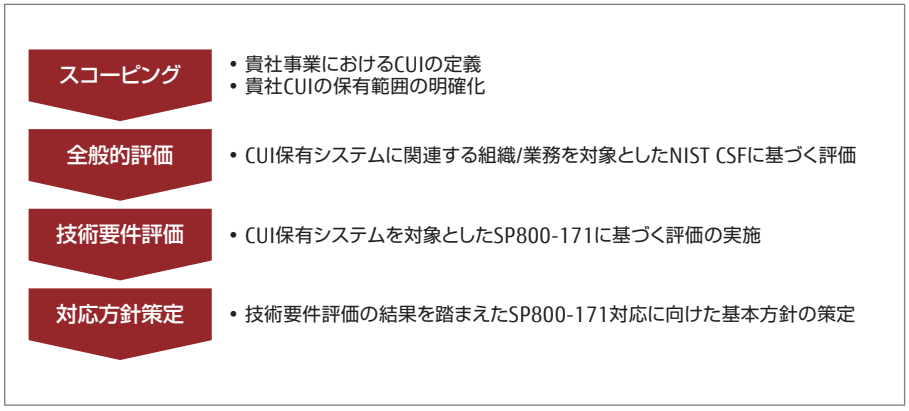
Information and Event Management）と呼ばれるネットワークの監視・検知システムの導入です。これは、ログの統合監視を人間の手で行うには限界があるためです。また、国防総省調達規則（DFARS）では、セキュリティインシデントを検知してから72時間以内に決められた方法でインシデント報告を行うことが求められており、インシデント発生時に限られた時間の中で状況を把握するため、また迅速に対応するためにも、SIEMの導入は不可欠です。ログの統合監視がNIST SP800-171において求められている理由には、セキュリティ対策の変化が背景にあると考えます。これまでのセキュリティ対策は防御を中心に考えられてきました。しかし、防御だけでは完全に防ぎきれないほど日々複雑化・巧妙化しているサイバー攻撃に対して、攻撃を受けた後の検知、対応、復旧における対策、いわゆるレジリエンスを高めることも求められるようになってきているのです。この考え方は、NISTによるサイバーセキュリティフレームワーク（CSF：Cybersecurity Framework）で提唱されている5 functions（特定、防御、検知、対応、復旧）に則ったものであり、攻撃を受けることを前提として対策を行う考え方はグローバルスタンダードになりつつあります。

4. これからのデジタル時代に向けて

データ保護の強化の流れは防衛産業に限ったことではありません。2016年の米連邦調達規則（FAR：Federal Acquisition Regulations）では、管理すべき重要情報（CUI）を保有するすべての業界においてNIST SP800-171を調達基準とする旨が明記されており、防衛産業に続き他産業もこの流れに追随していくと考えられます。実際にニューヨーク州金融サービス局によるサイバーセキュリティ規則（23 NYCRR Part 500）では、金融機関を対象に保護すべき非公開情報（NPI：Non Public Information）として、事業者のビジネスに重大な悪影響を及ぼす情報や個人の特定が可能な情報を保護することを求めています。

さらに電力業界でも、北米電力信頼度評議会（NERC：North American Electric Reliability Corporation）によるセキュリティガイドライン NERC CIP Standardが大規模電力システムに関する情報を保護するように求めています。これは、大規模電力システムに関する情報が漏洩し、サイバー攻撃を受けた場合、電力の安定供給に支障をきたす可能性があるためです。このガイドラインは、北米の電力会社が大規模発電および送電設備に対して行わなければならないセキュリティ対策について記載しており、対策が不十分な企業には罰金が科せられるという強制力のあるガイドラインです。

データ保護の流れは日本においても、北米同様、防



●図2　NIST SP800-171適合の流れ

衛産業から始まり、他産業が追随していくと考えられます。防衛装備庁による新セキュリティ基準のように、NIST SP800-171と同程度のセキュリティ強度を求めるガイドラインが他産業でも今後作られていく可能性があります。しかし、データ保護の強化というのは、単にレギュレーション対応という意味合いだけではありません。データが価値を持つ時代、それをセキュアな環境で保護することは企業にとって重要な経営課題です。NIST SP800-171で求められていることは特別なことではなく、これからのデジタル時代において、データを保護するために妥当なレベルです。NIST SP800-171への適合は、一層のセキュリティレベルの強化へ向けて有効な手段と考えます。

適合までのステップとしては、初めにスコーピング作業として、自社事業における管理すべき重要情報（CUI）を定義し、保有範囲を明確化します。次に、NISTのサイバーセキュリティフレームワーク（CSF）に基づいて、管理すべき重要情報（CUI）について保有システムに関連する業務の全般的なセキュリティ評価を行います。そして、NIST SP800-171に基づき、データの保護に重点を置いた評価を実施し、その結果を踏まえ、具体的な基本方針を策定していきます。富士通総研では、お客様のレジリエンス向上をご支援するため、NIST SP800-171適合に向けたコンサルティングサービスを今後提供していきます。

（注1） Society5.0：日本政府が提唱する科学技術政策の基本指針の1つ。狩猟社会、農耕社会、工業社会、情報社会に続き、新たな社会として提唱されているSociety5.0は、サイバー空間とフィジカル空間を高度に融合させ、経済発展と社会的課題の解決を両立することを目指している。

（注2） セキュリティ・クリアランス：職務上、機密情報を取り扱う必要のある人物に対し、職歴や家賃等の滞納歴、犯罪歴等を確認し、ふさわしい人物であることを証明するプロセスのこと。欧米では、政府機関だけでなく民間企業でも導入されている。日本でも、機密情報にアクセスできる人物に対し、セキュリティ・クリアランスを実施し、認定する制度の創設が検討されている。

ケーススタディ 1

スマートファクトリーを実現するための サイバー・レジリエンス

スマートファクトリー化が進む製造現場では、今まで露呈していなかった脆弱性が狙われると、設備の停止や誤作動といったフィジカル面に影響が及びます。スマートファクトリーのセキュリティ対策は、「工場内ネットワークの可視化による早期検知」と「サイバーリスクを想定したインシデント対応体制とBCPの確立」がポイントです。

執筆者プロフィール

岡本　登（おかもと　のぼる）

富士通株式会社 ネットワークサービス事業本部 ネットワークインテグレーション事業部 シニアエキスパート

交換機ソフトウェアの開発から電力、警察、金融、流通などの様々なシステム開発に携わり、インターネットの世界へ足を踏み入れる。特にセキュリティには長年従事し、その間、NPO活動などで社外発表も多数。4年前から工場セキュリティの実証実験とソリューション開発を中心に活動中。

告野　信輔（つげの　しんすけ）

株式会社富士通総研 ビジネスレジリエンスグループ マネジングコンサルタント

2001年 富士通関西中部ネットテック株式会社入社。サーバ構築・保守やセキュリティポリシーの策定、教育講師等を経て、2005年 富士通株式会社に異動。2007年より株式会社富士通総研。事業継続、情報セキュリティ等、主にリスク管理分野のコンサルティング業務に従事。現在はセキュリティに関する対応体制構築支援や訓練・演習を通じた組織の対応能力向上の支援、専門家の育成に従事。

はじめに

近年、製造業では、様々な領域でデジタル化が進んでいます。とりわけ、製造現場である工場においては、さらなる効率化や柔軟性を実現するため、工場内の様々なデータをIoTで取得・収集し、そのデータを分析して予測等に活用することで新たな付加価値を生み出すスマートファクトリー化が進められています。

一方で、様々なモノがつながるということは、それまで露呈していなかった脆弱性が狙われるということとなります。特に、製造設備と“つながる”ことによって、設備の稼働そのものが停止したり、誤作動を起こしたりといったフィジカル面にまで影響が及びます。

工場のネットワークはこれまでクローズド環境で運用されることが多かったため、あらゆるモノがつながるオープン環境に耐え得る構造になっていないのが実情です。スマートファクトリーを実現する際は、オフィス環境と同様の防御対策ができないこと（工場の防御対策の限界）を理解したうえで、「工場内ネットワークの可視化による早期検知」と「サイバーリスクを想定したインシデント対応体制とBCP（Business Continuity Plan）の確立」を行うことがポイントとなります。

1. 工場におけるセキュリティ対策（防御）の限界

オフィス環境でこれまで積み上げてきた数々のセキュリティ対策は、工場内ではインフラ環境が異なるため、その効果はほとんど期待できません。以下の実情を踏まえ、防御の限界を認識する必要があります。

(1) 設計されていないネットワーク

通常のオフィス環境で使用される情報系ネットワークでは、その用途やセキュリティの観点からネットワークをセグメントに分割して管理していますが、工場内ではこうした設計が行われずに数珠つなぎに接続され、結果的にすべてがつながる広大な1つのネットワークを形成していることが多く見られます。

(2) エンドポイントセキュリティの不在

情報系ネットワーク内では端末や装置にパッチの適用やアンチウイルスソフトの導入といったレベルのセキュリティ対策を施すことは通常行われていますが、工場内ネットワークの端末や装置では、動作に影響が出る可能性もあり、パッチの適用やソフトウェアの導入などは実施できません。さらに、古いWindows OSが使われているケースも多く、結果として脆弱性を抱えた装置が多数存在しています。

(3) 監視されない現在状況

工場内のネットワークでは、ネットワークセキュリティの概念はなく、単純な物理的配線にとどまっています。したがって、ここを流れるデータの量や通信内容、通信相手はもちろん、マルウェアの拡散活動すら監視されていません。

2. スマートファクトリーの必須要件としてのレジリエンス強化

前述のような防御面での課題を全面的に解消するためには、スマートファクトリーを一から設計する必要があり、既存工場をスマート化・デジタル化するには、防御面での限界を認識し、インシデントの発生前提の考え方に基づいた対応、すなわち残留リスクを想定した備えが必要です。

具体的には、サイバー空間におけるリスクに対する「検知」、「対応」、「復旧」の3つのレジリエンスの機能強化です。工場においては、サイバーリスクが設備の停止や誤作動、さらには人命に関わる事故にもつながりかねないため、レジリエンス強化は重要テーマです。

(1) 検知：工場内ネットワークの可視化による早期検知

現状の工場では、そもそも対策のベースラインが明確になっていません。工場のネットワークにはどの機

●表　工場のセキュリティ強化のSTEP

STEP	項目	目的	内容	対応手段
1	工場内ネットワークの現状把握	接続される端末・機器の把握	・既存の機器一覧 ・L2SWのMACテーブル	・ネットワークセンサー（接続装置の探査） ・ネットワーク情報収集ツール ・SNMPによる情報収集 ・ワーム拡散活動検知センサー
		物理的なネットワーク構成の把握	・既存のネットワーク構成（SW等の接続状態など）	
		通信量の把握	・L2SWの送受信カウンター	
		ワーム感染の把握	・潜伏しているワームの検知	
2	工場内ネットワークの変化把握	管理ルールの見直し	・構築ルール ・接続ルール	・工場内ネットワーク構築ガイドライン ・工場内ネットワーク利用ガイドライン
		異常の検知	・不正機器接続の検知 ・疑わしい通信の検知	・可視化情報のリアルタイム分析
3	工場内ネットワークの最適化	管理できるネットワークへの変革	・ネットワーク構成の見直し ・アドレス体系の見直し	・インテリジェントスイッチの導入 ・セグメンテーション
		可用性の向上	・データフローを考慮した最適化 ・止まらないネットワーク	・業務特性、通信特性に応じた、冗長性/QoS等の機能の適用
		運用性の向上	・インシデントレスポンス対応 ・集中管理	・被害局所化機能の導入（自動遮断） ・工場向けNOC/SOC/CSIRT

器がどこに接続され、どのような通信を行っているのか、ネットワークには入口や出口はあるのか、すでにマルウェアが潜伏しているようなことにはなっていないのか、これらを明らかにします。

そのために、ネットワークに接続されている機器の情報や流れているデータなどを自動的に収集し、最新状態を細かく可視化します。これにより、ワームの拡散活動や不正な端末の無断接続なども検知することができます。

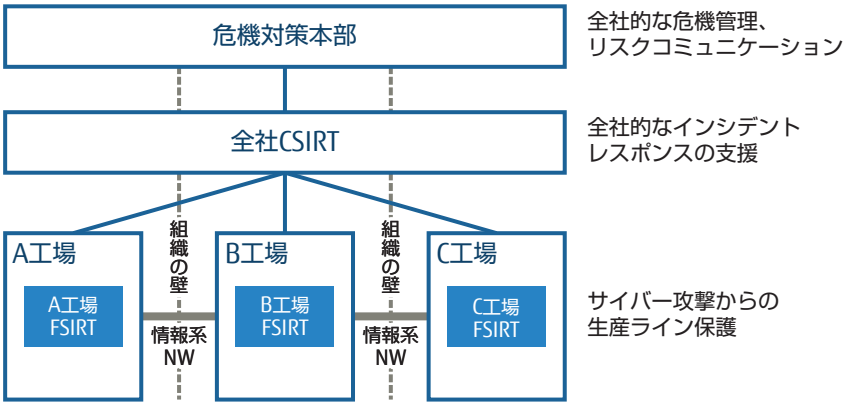
これらを統合的に監視・分析する機能を備えた基盤と、それらを運用するFSOC（Factory Security Operation Center）が、工場のデジタル化と並行して、今後取り組むべき重点テーマです。

(2) 対応：インシデント対応体制（FSIRT）の確立

さらに、FSOCにおいて異常が検知されても、それらの情報をどう扱うかのインテリジェンス機能が必要です。例えば、異常が検知され、危機が迫っている可能性がある状況においても、工場全体の稼働への影響、さらには取引先への影響などのビジネス面を考慮する必要があるため、原因となる装置の通信をすぐに遮断すべきかどうかの判断が難しい場面が想定されます。そのために必要となるのが、FSOCからエスカレーションされる情報や不足している情報を能動的に集約し、それらを踏まえた情勢判断を行い、さらには生産管理部門や経営層にエスカレーションする対応体制、つまりFSIRT（Factory Security Incident Response Team）の確立です。

一般的なオフィス環境でのインシデント対応については、CSIRT（Computer Security Incident Response Team）が旗振り役を担いますが、工場の場合は対象が制御系システムであることから、パッチ適用の可否判断や稼働への影響などについて情報システム部門で対応するには限界があります。そこで、全社的に工場設備を担当する生産管理部門などを主体としたFSIRTを構築し、役割の明確化、対応プロセスや判断基準等の整備が必要となります。

また、暫定対処として生産ライン停止や他工場への二次被害拡大防止のために、異常が検知された工場を全社ネットワークから切り離すといった、事業への影



●図1　FSIRTと危機管理対応体制

響とのトレードオフで判断が求められるケースもあるため、経営層を中心とした危機管理対応体制との連携なども整備しておく必要があります。

(3) 復旧：サイバー版BCPへのアップデート

スマートファクトリーに対してサイバー攻撃が行われると、設備稼働停止など、物理的な被害に直結するため、「BCP」が必要となります。

すでに多くの組織でBCP/ICT-BCPは整備されているため、事業を復旧・継続するうえで優先的に復旧すべき設備や重要システムの抽出、それらに対する対策実施状況を把握していると思われます。しかし、多くのBCP/ICT-BCPは地震等の自然災害を想定脅威としており、停止時、つまり可用性観点で経営に及ぼす影響の大きさを評価しています。サイバー攻撃を想定する際には、損なわれる危険性のある工場内の制御系システムおよびデータの完全性や機密性の重要度を改めて評価する必要があります。

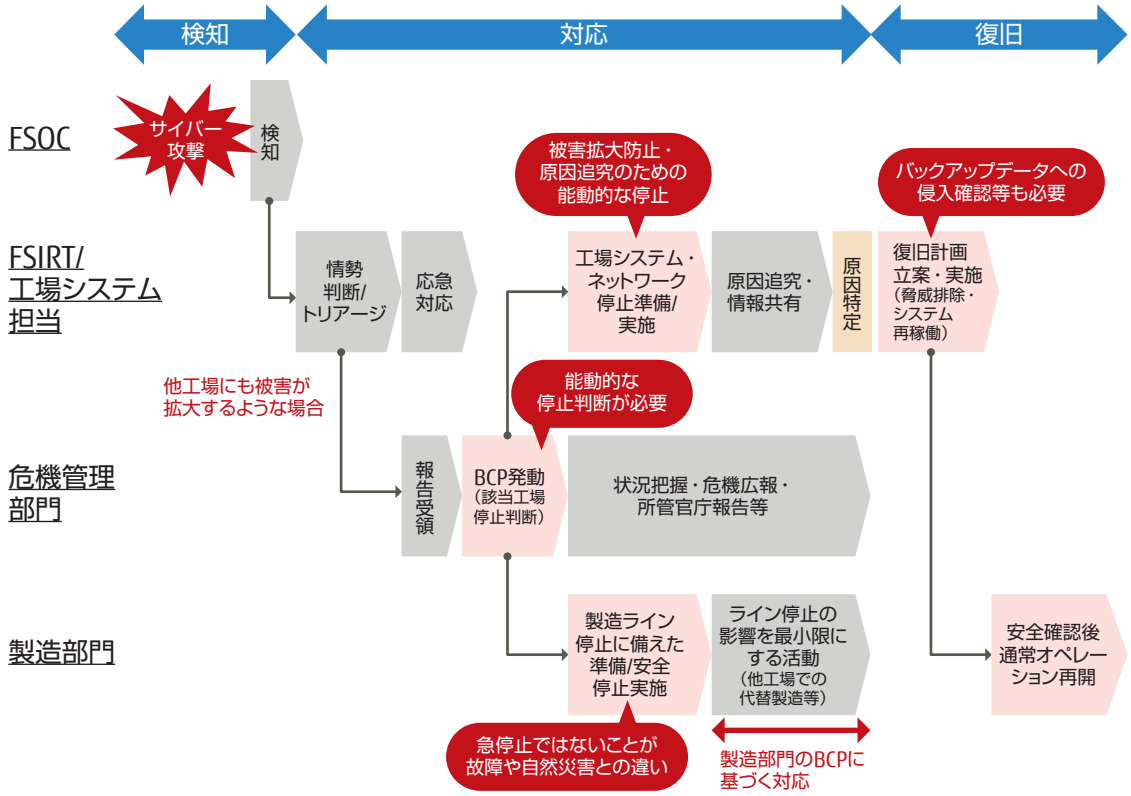
また、実際の対応においても、検知イコール停止となる故障や自然災害と違い、能動的な停止判断（BCP発動）や再発防止のための原因追究、脅威排除後の再稼働、復旧時に用いる各種データの被害確認等、サイバー攻撃ならではの復旧プロセスを考慮する必要があります。

3. セキュリティとレジリエンスのリテラシー向上に向けて

本稿でご紹介した「工場内ネットワークの可視化」、「FSIRTの整備」、「サイバー版BCP」に私たちは現在、着手しています。「工場内ネットワークの可視化」については、実際に大手製造業様のいくつかの工場において実践し、可視化を行ううえでの課題抽出や解決策の検討、可視化項目の有効性検証を実施しました。例えば、可視化に向けて、まずは工場内のネットワーク機器をインテリジェントスイッチ(注)に変えることや装置の情報収集のためにネットワークセンサーを導入するなど機器の整備を進め、そのうえで工場内通信の特徴を把握し、早期検知に有効な可視化項目を選定すること、などです。

また、可視化を行って早期検知した後のFSIRTの整備は、CSIRTなどの数多くのインシデント対応、クライシス対応のプロセス整備を通じて得た知見をベースに進めているほか、サイバー版BCPについてもBCPやICT-BCPの策定ノウハウに基づくご支援を実施しています。

今後もスマートファクトリーが砂上の楼閣とならないように、これらの工場セキュリティのソリューションからインシデント対応体制整備やBCP策定などのレジリエンス強化コンサルティングまでワンストップでご支援してまいります。



●図2　工場における対応プロセス例

（注）　インテリジェントスイッチ：LANスイッチの製品分類の1つで、SNMP（Simple Network Management Protocol）のリモートによるネットワーク管理機能を持たせたスイッチ製品。

ケーススタディ 2

AI×レジリエンス

株式会社富士通総研
ビジネスサイエンスグループ
シニアコンサルタント　佐藤　文孝

AIの技術要素や活用目的は多岐にわたり、業種・職種を問わず適用が可能である。レジリエンス向上に対するAI活用という観点で活用事例を製造業中心に紹介する。

執筆者プロフィール

佐藤　文孝（さとう　ふみたか）
株式会社富士通総研 ビジネスサイエンスグループ シニアコンサルタント
データサイエンティストの視点により、様々な課題をデータ分析で解決に導くAI活用のコンサルタント。

概要

昨今、様々な分野でAIの名を冠したシステムやサービスが多く生まれている。

一口にAIと言っても、その技術要素や活用目的は多岐にわたり、業種・職種を問わず適用が可能である。

本稿では、レジリエンス向上に対するAI活用という観点でサイバーセキュリティ以外の活用事例と導入の際の注意点などを製造業中心に紹介する。

活用事例

昨今のAIの進化は目覚ましく、特定分野においては人間の認識や思考を超える振る舞いを達成している。「人工の知能」とまで呼ばせるその言葉の響きからは、今までのシステムにおける自動化や高速化にとどまらない、ルールベースのコンピュータ処理を超えるもの、つまりは人間の思考、判断を同等の精度で代替し、人間では気づかないような新たな価値を生み出すことが期待されるのではないだろうか。

レジリエンスという観点では、AIが現状のリスクを自ら判断、評価、対応したり、未知のリスクに気づいたりといったことに活用できるのではないかと期待される。

例えば、工場における生産品の品質予測や、生産設備の故障予兆などがわかりやすい取り組みではないだろうか。生産ラインが生み出す大規模な多次元データの処理はAIの得意分野と言えるであろう。シンプルな相関関係では発見できない、複雑に絡まりあった多次元データ間の関係性を学習していき、そこから品質の低下や故障の前兆を発見し、アラートをあげ、実際のトラブルを未然に防止する。現在ではエッジコンピューティングの技術の向上もあり、毎秒生まれるセンシングデータをネットワークに乗せることなく処理することが可能になってきている。

AIの別の強みの1つとして、センシングデータのような数値化されたデータではない言語や画像などの非構造化データに対する処理が挙げられる。画像や言語はそれを受け取った個人によって認識が一定ではなく、ルールベースの処理に組み込むのが難しいデータであったが、昨今のアルゴリズムでは、そのような特徴の定義が難しい非構造化データから最適な特徴量を含めて機械的に学習することが可能になってきている。これにより、画像認識は、単純なパターンマッチングによらない製品の異常検知や作業員の転倒検知などを高精度で実現する。言語データの活用事例で言えば、過去に起こったトラブルとその対処履歴を学習させることにより現在起こっているトラブルに類似した過去の対処事例を高精度に検索、参照することが可能になり、トラブルへの早期対処と対応品質の向上を実現する取り組みが多く行われている（専門分野別意味検索活用事例[注1]）。さらにセンシングデータと対応履歴を紐づけることができれば、異常が起きた瞬間に対応策を提示し、機械が自動で適切な運転へと舵を切るということも可能である。

AI活用の課題

実際にAIを使ってリスク対策を行ううえでの注意点を以下に挙げる。

(1) データ品質の不足

コンピュータサイエンスの分野で有名な慣用句に「GIGO（Garbage In, Garbage Out）」という言葉がある。アウトプットの品質はインプットの品質によるという意味で使用されるが、これはAIの構築でもよく使われる。自動車の燃費性能の予測を行うために食べログの口コミデータを使用する必要はないであろうし、口コミデータをいくら分析したところで自動車の燃費予測はできないはずである。工場内の機器からは様々なセンサーデータが取得されるが、それらが何に対して有用なデータなのかを理解することは重要になる。具体例を挙げると、現在取得されているセンサーデータは製造品の品質を知るためのものなのか、製造機器の異常を知るためのものなのか、作業員の安全を知るためのものなのか、

機器の稼働状況をモニターするためだけのものなのかなど、その活用目的は様々であり、活用ケースによって最適な情報というのは異なってくる。とりあえず、今取得できているデータがたくさんあるからやってみるという方針では、うまくいかない場合が多いことを認識し、必要に応じて意味のあるデータ取得の方針から検討する必要がある。

(2) 異常系教師データの不足

特異な異常事態に対する予測では異常系教師データ不足が問題になる。現状のAIモデルで大きな成果を上げているモデルのほとんどは、「教師あり学習」という手法を用いている。この手法は、インプットデータと実際に予測や分類をしてほしい正解ラベルのペアを学習用データとして準備し、アウトプットをできるだけ正解ラベルに近づけていくという方法で学習を行っていく。この手法では教師データの量が非常に重要になる。

日々の品質変化のデータなどは様々なパターンが十分な量で蓄積されていることが多いが、大型製造装置の思わぬ故障停止などの重篤な事故は頻発するわけではないため、学習用の事例数として不十分であることが多い。しかし、そのような重篤なレアケースこそ、未然に防ぐ価値が高いというジレンマが存在する。

(3) 説明可能性のトレードオフ

近年大きな話題になっているDeep Learningに代表されるように、そのアルゴリズムが複雑になればなるほど難しい問題に対応できる一方、アウトプットの説明可能性が失われていくという問題が存在する。十分な学習データが存在し、複雑なアルゴリズムを選択すれば、昨今のAIはおそらく高精度の予測を行ってくれるであろう。しかし、ある日突然、品質予測AIが製造品の品質劣化の予測アラートを出してきたとしても、なぜそうなったか、どう対処したらいいかを教えてくれなければ、作業者は混乱するだけである。予測問題だけ高精度に解けるようになったとしても、そこからどのように行動を起こすべきかについてはまた別の問題設定にするか、業務モデルで吸収することが必要になってくる。

解決策

適切で効果的なAI活用のためには、今ある環境の一部にAIを入れるというような考え方ではなく、そのパフォーマンスを最大限に発揮するためのデータ設計から業務モデルまでをトータルで設計することが必要である。

予測や予兆のために必要となる物理的に意味のあるデータは存在しているのか、そのようなデータがないのであれば、どのように取得し、運用していくのかを検討する。現状で取得できているデータでトライしてみるのも1つの方針としては悪くはないが、最善の結果が得られるわけではないということは認識しておくべきである。

教師データに不足がある場合の解決策としては、様々な方針が考えられる。可能な問題設定は限られるが、教師データを人工的に増やす水増しや、データが豊富に存在する類似領域での学習結果を流用する転移学習、一部の教師データに教師無しデータを紐づける半教師あり学習などがあるが、どれも必ず効果を上げられるとは限らない。教師データが不足するケースでの異常検知系の処理方針は正常系の振る舞いを学習し、その正常パターンと外れたものを異常系として検出する（異常系を教師として使用しない）ものが現実的な運用方針となっていることが多い。

AIのアウトプットの説明可能性の問題はAI関連研究では古くから存在し、説明可能AI（XAI：Explainable AI）の開発は大きな研究テーマの1つである。現状、一部の限られた領域においては有効性が示されているものも存在するが(注2)、汎用的なものは存在せず、業務モデルとともに検討・設計する必要がある。説明可能性が失われると述べてきたが、AIのアルゴリズムの中にも変数の重要度等を評価できるものは存在するため、そのようなロジックを活用するか、あるいは、予測問題と要因分析問題を完全に分けて運用し、AIのアウトプットはあくまでも検査のトリガーとして使用し、外れること

を見越した業務設計を行うことが必要になる。

おわりに

本稿では簡単ではあるが、製造現場を例にAI活用事例を紹介してきた。今話題のAIはデータが豊富に存在する限られた問題設定においては強力にその力を発揮するが、現実世界は必ずしもそのような環境にあるとは言えない場合が多い。今後の研究の発展による解決も期待されるが、現状は、まだ、人がAIに寄り添って共に助け合うことで課題を解決していく必要がある。これまで述べてきたようにAIのアルゴリズムを知っているだけでなく、物理的対象に対する知識や業務、ビジネスへの理解も必要不可欠であり、全体を俯瞰した課題解決モデルの設計が肝要である。

（注1） Zinrai専門分野別意味検索：
https://www.fujitsu.com/jp/solutions/business-technology/ai/ai-zinrai/services/platform/domain-specific-semantic-search/

（注2） 説明可能なAI：
富士通研究所2017年9月20日【プレスリリース】「AIの推定理由や根拠を説明する技術を開発「Deep Tensor」とナレッジグラフを融合」
http://pr.fujitsu.com/jp/news/2017/09/20-1.html
富士通研究所2017年12月21日「当社先端技術「説明可能なAI」が英Nature誌に掲載」
http://www.fujitsu.com/jp/group/labs/resources/news/topics/2017/topics-20171221.html

知創の杜バックナンバーご紹介

知創の杜　検 索

https://www.fujitsu.com/jp/group/fri/knowledge/magazine/

メルマガ会員登録

知創の杜メールニュース　検 索

https://www.fujitsu.com/jp/group/fri/resources/news/FRImailnews.html

トレンドや事例など、お客様のビジネスに役立つ情報を毎月お届けします。

- オピニオン
- コンサルティング事例
- 研究レポート
- サービス紹介
- セミナー案内
- 最新トピックス

www.fujitsu.com/jp/fri/

株式会社 富士通総研
FUJITSU RESEARCH INSTITUTE

〒105−0022　東京都港区海岸1丁目16番1号　ニューピア竹芝サウスタワー
TEL：(03) 5401−8391　FAX：(03) 5401−8395

通巻第41号