総　論

新時代の中で変わるBCPの考え方

昆 正和

持続可能性への危機感

企業の活動は「持続可能」であることを前提に営まれている。「持続可能」とは、工場でいえば、常に必要な時に必要なだけ原材料や部品が調達でき、加工・処理・組立・検査を行う経験豊かなオペレータや作業員がいて、適切なタイミングで納入する輸送体制がある、ということである。さらにその背景には、常に安定的に工場を稼働させるための電気や燃料が供給され、機械設備が正常に稼働できる仕組みが整っており、これらがすべて同期して永続的な生産サイクルを反復できる、ということである。

ところが、これから見ていくように、近年はそうした企業活動の持続可能性に暗雲の漂う気配が出てきた。世界中のあらゆるものがネットワークで緊密につながり、限りなく利便性が向上し、人とモノの移動や交換が活発かつスピーディになってきてはいる。しかし、その代償として、ひとたび歯車が狂えば、一夜にしてあらゆる方向に影響が波及し、私たちの生活や経済活動を混乱・麻痺させてしまう。その脆さを目の当たりにするような事態が起こり始めている、否、明らかに増えているのである。

思うに、事業活動の歯車を狂わせる突発的なリスクについては、企業はBCP（事業継続計画）の策定を通じて回避すべく努力してきたはずである。しかし、果たしてそのBCPは、今日のリスクにうまく対処できているだろうか。

以下では、これまでのBCPのあり方を振り返るとともに、新たな危機につながる3つのリスクと、それぞれのリスクが企業に与える影響について考えていく。

地震以外のリスクは見えているか？

ここではまず、BCPの原点に立ち戻ってみよう。何のために企業はBCPを策定するのか。中小企業庁のBCP策定運用指針は、BCPの意義と目的について次のように定義している。

「企業が自然災害、大火災、テロ攻撃などの緊急事態に遭遇した場合において、事業資産の損害を最小限にとどめつつ、中核となる事業の継続あるいは早期復旧を可能とするために、平常時に行うべき活動や緊急時における事業継続のための方法、手段などを取り決めておく計画のこと」

これまで多くの企業が、事業運営を脅かす“緊急事態”の典型として「地震リスク」を選定し、地震に特化したBCPを策定してきた。地震が真っ先に選ばれた理由は、さまざまな災害の要素を含んでいるため、地震BCPさえつくっておけば他の災害にもある程度は対処できるだろうとの考えからである。しかしその結果、地震対策を講じることがBCPの終着点であるという錯覚や固定観念が

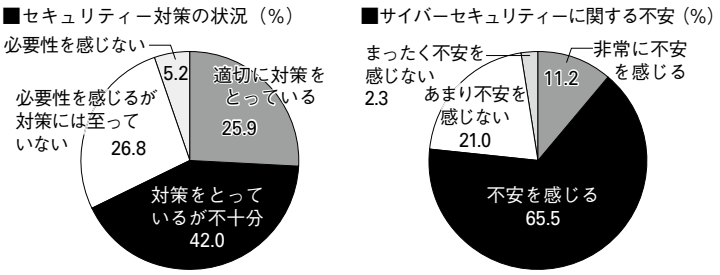
表1　想定しているリスク（一部抜粋）

	地震	津波	洪水（津波以外）	新型インフルエンザなどの感染症	大気・土壌・海洋汚染などの環境リスク	テロ・紛争（国内外）	他国からのミサイル攻撃	インフラ（電力・水道など）の途絶	通信（インターネット・電話）の途絶
大企業	98.1	53.2	43.2	69.1	24.1	34.2	26.3	53.6	61.2
中堅企業	92.6	38.4	30.0	49.5	10.8	11.0	9.5	31.7	46.1
その他企業	89.9	41.1	27.0	43.2	12.7	13.9	8.9	36.4	44.7
全体	92.0	42.3	30.5	49.3	14.0	16.4	11.9	37.8	47.8

内閣府「平成29年度 企業の事業継続及び防災の取組に関する実態調査」より

できてしまって、それ以外の危機対応が疎かになっている嫌いがある。内閣府の「平成29年度 企業の事業継続及び防災の取組に関する実態調査」を見ると「想定しているリスクは何か」という問いに対し、「地震」が圧倒的に多く、大企業で98.1%、中堅企業で92.6%である(**表1**)。中小企業はさらにこの傾向が強いことは筆者の経験からも明らかだ。

図1 製造業のセキュリティ対策調査



経済産業省調べ(4,300社が回答)

では地震以外の危機対応とは何か。たとえば、近年は工場にIoTやAIを導入する動きが加速しているが、その斬新さやメリットだけに目を奪われ、門外不出のノウハウや熟練技術がデータとして可視化されること、そして外部とつながることのリスクを軽く見てはいないだろうか。あるいは、年々その頻度と激しさを増している台風や豪雨災害を、一過性の災害、たまたまの出来事に過ぎないと過小評価してはいないだろうか。こうした観点から、以下では企業の持続可能性(事業継続性ともいえる)を脅かすリスクとして「工場のサイバー攻撃」「パンデミック(新型感染症の世界的流行)」「気候変動のリスク」の概要を述べる。

スマート工場を脅かすサイバー攻撃

近年、製造業では工場のスマート化が進んでいる。「工場のスマート化」とは、工場内の多種多様な装置や設備機械、オペレータの行う作業のデータなどを、IoTを活用して可視化・蓄積してさまざまな形で分析・応用できるようにする技術である。データ化することで自動化が図られ、人材不足の解消や作業の効率化に貢献できる。工場内で取得したデータを最大活用するにはネットワークでつながる必要がある。しかし、もともと閉じた環境で成り立っている工場が外部とつながることについては、無防備な点があると指摘する専門家も少なくない。

経済産業省が製造業のセキュリティ対策について行った調査では、集計した企業の7割近くが対策不十分との結果が出ている(**図1**)。特に、中小企業の危機意識が薄いといわれており、これが中小企業のBCPの策定率の低さとも関連していることはいうまでもない。

製造業では設計図や技術仕様書などのノウハウを扱うことも多く、意図せずして外部へ流出する懸念がある。また、工場がサイバー攻撃を受ければ、機密データが盗み出されたり破壊されたりする危険性があることはもちろん、特に制御系が攻撃を受けると致命的である。情報処理推進機構のホームページには次のような記述が見られる。

「実際にサイバー攻撃によって、2010年にはイランの核施設でウラン濃縮用の遠心分離機が機能不全に陥る事件が、2014年にはドイツの製鉄所で溶鉱炉が損壊する事件が、2015年および2016年にはウクライナで大規模な停電が引き起こされる等の事件が発生しており、制御システムのセキュリティ対策の見直しが急務となっています」

また、2018年8月に発生した台湾での事例がある。工場内の機器がランサムウェアに感染し、他の工場にまで感染が広がった結果、製品の出荷が滞ってしまったのである。ランサムウェアは悪意のあるプログラムの一種で、これに感染したPCはロックされたり、ファイルを暗号化されたりして使用できなくなる。そして元に戻すことと引き換えに「身代金」を要求するのである。

感染した原因は工場内での2つのミスにあるとされる。1つは生産設備の保守業者が持ち込んだ機器をネットワークに接続する際、ウイルスチェックをしなかったこと。もう1つは、そのネットワークに接続しているPC(Windows OS)で適切な脆弱性対策が行われていなかったこと。感染したランサムウェアは周辺の他のPCだけでなく、ネットワークを介して別の工場にも拡散。感染が発