寄稿記事

リモート環境での経営の考え方
～経営者はサイバーセキュリティをどのように考えているのか～

Chief Security Officer　萩原健太（はぎはら　けんた）
グローバルセキュリティエキスパート株式会社

1. 日本企業の現実

新型コロナウイルス感染症による社会的混乱が始まったとき，経営者がまず思ったことは「会社を存続させることができるのか」，「今いる従業員を守ることができるのか」といった切実な思いである．残念ながら（当然ながら）サイバーセキュリティではないことは確かだ．

昨今，いわゆる「コロナ関連倒産」が増えているとも言われるが，企業全体の倒産数は減少傾向にある．新型コロナウイルス感染症の影響を受ける前の2019年は，企業の倒産件数は8,383件だが，2021年は6,030件と約3割も減少している．これはまさしく困難を乗り越えようとする経営者や従業員，関係者一人一人の努力の賜物でもあると言える［1］．

表1　倒産件数と負債の推移［1］

年	件数	負債総額
2019年	8,383件	¥1,423,238,000,000
2020年	7,773件	¥1,220,046,000,000
2021年	6,030件	¥1,150,730,000,000

一方で，2020年度通年の実質GDP（国民総生産）は，前年度からマイナス4.5%と個人消費の落ち込みも影響し，日本経済は下火となり，企業が難しい舵取りを行っている状況に変わりはない［2］．

2. 新型コロナウイルス感染症禍の経営

「経営」を語るには烏滸がましいが，現実的かつシンプルに言えば，「入り（収入）を増やすか，出（支出）を減らすか」であり，リモート環境であろうとなかろうと，その考えが変わることはない．つまり，今の事業が維持できるのか．先行きが見通せないようであれば，固定費や人件費などの見直しを行い，資金繰りを考える．また，そもそもこのような検討が行えない環境であれば，キャッシュフローの見える化を行うなど，根本的な考えは新型コロナウイルス感染症禍でも変わることはない．

しかし，不安定な社会情勢から経営そのものの構造の再考，そして可及的速やかに判断をしなければならなくなったのは経営としての変化である．

特に象徴的な対応は，テレワーク増加によって出勤が減少したことによる，オフィスそのものの減少や廃止の検討，そして通勤手当などを始めとした手当の見直しを行ったことであろう．実際に7割近い組織が（検討中を含み）オフィスの見直しを行い，専有面積の縮小などの検討を行っている．その一方で，コワーキングスペースなどの場所の有効利用ができる環境整備を進めた企業も増え，日本の働き方が変化している［3］．

また事業のデジタル化も急務になった．

これまで対面型を中心としていた店舗はネットショップの開設を行ったり，EC（Electronic Commerce）サイトの構築を行ったりするなど，事業のオンライン化が進められている．あるネットショップの作成サービスにおいては，ショップ開設数が2020年2月から2021年9月時点で比較すると，2

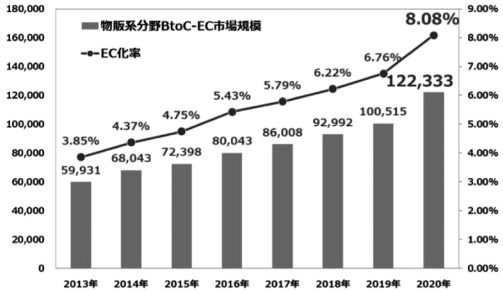

図1　物販系分野のBtoC-EC市場規模及びEC化率の経年推移［6］

倍にも迫る勢いで増加している［4, 5］．また，物販系分野コンシューマ（BtoC）向けのECの市場規模を見ると，2019年は約10兆円だった規模が約12兆円に増加し，伸長率も約22%となっている．さらに約6%のEC化率も2020年には約8%となり，国内においては以前よりも高い水準になっている［6］．

日本のIT推進が叫ばれて20年を超え，デジタルトランスフォーメーション（DX）が叫ばれる昨今において，皮肉にも新型コロナウイルス感染症が日本のデジタル化への道を加速させていると言える．

3. サイバーセキュリティを考えるとき

そのような中で経営者がサイバーセキュリティを考える（余力はないのが正直なところだが）タイミングは大きく3つある．1つ目は緊急事態宣言などによってテレワークを実施しなければならなくなったとき．2つ目は事業のデジタル化（オンライン化）を余儀なくされたとき．そしてインシデントが起きたときの3つである．

まず緊急事態宣言発令後，急にテレワークに移行し，より通信を安全に行うための仕組みであるVPN（Virtual Private Network）を始めとしたネットワーク関連機器の導入やライセンスの追加，自宅パソコンでの業務対応の許可，広くはセキュリティポリシーの見直しなど，さまざまな対応を行った．日本シーサート協議会（NCA）の調査ではテレワーク対応の準備を行っていた組織が9割もあり，スムーズな移行が行われているようにみえる［7］．しかし，NCAは従業員規模の大きい組織（従業員数1000名以上）が7割超加盟しており，規模の大きい企業であったからこそ，スムーズに移行できたと言える［8］．

中小企業はそこまで考える余裕もなく，テレワークに移行した組織，結果的にテレワークの業務に移行できなかった組織もある．

2つ目のデジタル化（オンライン化）はこれまで嫌厭してきた経営者も情報技術の活用の重要性または必然性に気づき，活用を検討した結果として，最後にサイバーセキュリティを考えるタイミングである．なお，経営者が情報技術に明るくなければ，基本的な構成要素は部下や委託先の提案に任せて，最終承認のみを行っている場合もある．先に述べたEC化のように，Webサイト数そのものの推移を見ても2019年は約17億件であったのが，22年1月現在では19億件を超え，2億件超も増加している［9］．この増加はビジネスのデジタル化（オンライン化）が進んでいる1つの証明とも言えるであろう．

表2　テレワーク対応状況［7］

テレワークの対応状況	
準備していた	15%
一部準備していた	77%
準備していなかった	6%
その他	2%

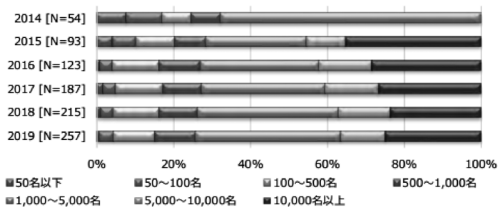

図2　CSIRT母体組織の従業員規模［8］

3つ目はインシデントが起きたときである．例えば，昨今増加するネットワーク機器装置の脆弱性を悪用した攻撃や，Webサイトの改ざん，設定ミス，フィッシングメールやマルウェア付きメール，そしてランサムウェアの攻撃など，サイバー空間は良くも悪くも常につながっている空間であるため，攻撃が減少している傾向は見られない．上記のようなインシデントが自組織で発生した時に，経営者は慌て，サイバーセキュリティを考えるというのが現実である．

なお，他組織で発生した重大なインシデントで，大手の放送局や報道機関に取り上げられたことも多い．その場合も，インシデントとして対応が必要な場合がある．

4. 経営者だからこそ推進する

情報技術やサイバーセキュリティは「難しいからわからない」と避けてきたのが多くの経営者の現実であり，DXは経営者が規模の大きい企業のサイバーセキュリティの意識と小規模事業者のサイバー

セキュリティ意識では大きく意識が異なる．つまり，DXは経営者がこれまで避けてきた現実に向き合わなければならないことになる．もし，情報技術はわからないが，DXを推進したいと言っている経営者がいるとすれば，その組織のDXは間違いなく失敗するであろう．これからの経営は，情報技術の活用こそ事業成長の鍵であり，その流れを止めることは近年の発展を見る限り難しいのは間違いない．しかし，忘れてはならないのは「DX＝デジタル化」ではないということである．DXは組織における事業や風土そのものの改革がもとめられているのであり，そこに情報技術という道具を使って実現することに過ぎない．つまり，深い情報技術の知識や経験がなかったとしても，経営者は一層耳を傾け，これまでの成功に甘んじることなく，DXの推進役になることに変わりはないということである．新しい技術，創造力にあふれる若手，知識が豊富な人員をメンバーとして構成し，自身も学びながら成長をしていく必要がある．経営者は感性や知識など元々秀でているからこそ，その立場にあるのであり「わからない」で逃げる必要はないのである．

5. 検討タイミングの変化の必要性

経営としての基本的な視点は，リモート環境だからと言って変わったわけではないが，よりスピードが求められるようになった．オンラインを基本として開催される会議は，移動時間であった時間も使えるため，数も増加傾向にある．さらには，生き残りのために各組織がしのぎを削って，新しい事業やデジタル化を検討しており，その波に乗らなければ経営としての遅れをとることになる．このように経営者はスピードも質もこれまで以上に必要になった．

サイバーセキュリティについても考えるタイミングや深さは，リモートになったからと言って大きな変化はない．経営者はサイバーセキュリティを考えるタイミングそのものは変わっていないが，ようやく迫ってきたというのは事実である．組織がデジタル化を推進するアクセルと，ブレーキともいえるサイバーセキュリティの存在は欠かすことができない．経済産業省が公開している「デジタルガバナンス・コード」の中でも「戦略の実施の前提となるサイバーセキュリティ対策を推進していること」と記述されており，その重要性が揺らぐことはない．

しかし，このような状況下でも変化がみられない現実において，経営者にサイバーセキュリティを一層考えるように仕掛けていく努力もしなければならない．

この努力の1つの例として，組織における「サイバーセキュリティ」の機能をCSIRT（Computer Security Incident Response Team）や相当の組織として独立させるのではなく，企業の事業継続マネジメント（Business Continuity Management, BCM）及び事業継続計画（Business Continuity Plan, BCP）の中に組み込み，重大なインシデントであればBCPが発動できるようにすることである．

昨今，実空間とサイバー空間の境目はより一層不明瞭になってきており，どの空間にあっても組織としての危機が訪れる可能性があることに変わりはない．昨今のランサムウェアによる被害によって重要インフラ組織が機能不全に陥る重大なインシデントが発生しているが，これはまさしく「災害」であり，組織の事業継続に関係するものである．DXが推進されればされるほど，両輪ともいえるサイバーセキュリティを，経営者がより一層考えていかなければならない．

今，組織で重大なインシデントが発生していなくても，それはある意味運がいいだけであり，決して対岸の火事ではない．事業のデジタル化が欠かせない昨今において，経営者がサイバーセキュリティの思考停止に陥ることは，1つの経営リスクから目を背けてしまっていることを忘れてはらならない．

もし思考停止に陥っている経営者がいたら，本文書をぜひお見せいただきたい．これが，組織のサイバーセキュリティ対策が進む一助になればこれ以上の喜びはない．

リアルな空間でもサイバー空間でもウイルスが猛威を振るっている．しかし，この困難を乗り越え，新しく，輝かしい時代を，皆で作っていきましょう．

頑張ろう日本！

参考文献

[1] 東京商工リサーチ「全国企業倒産状況」，https://www.tsr-net.co.jp/news/status/（*本情報をもとに執筆者にて作成）

[2] 内閣府「国民経済計算（GDP統計）」，https://

www.esri.cao.go.jp/jp/sna/menu.html
［3］ 月間総務「オフィスに関する調査」，https://www.g-soumu.com/news/2020/08/officequestionnaire.php
［4］ BASE「ネットショップ開設数が160万ショップを突破」，https://binc.jp/press-room/news/press-release/pr_20210921
［5］ BASE「ショップ開設数が90万ショップを突破」，https://binc.jp/press-room/news/press-release/pr_20200213
［6］ 経済産業省「電子商取引に関する市場調査」，https://www.meti.go.jp/policy/it_policy/statistics/outlook/210730_new_hokokusho.pdf
［7］ 日本コンピュータセキュリティインシデント対応チーム協議会「新型ウイルス感染リスク禍におけるCSIRT活動で考慮すべきこと」，https://www.nca.gr.jp/activity/imgs/CSIRTcorrespondence%20practice%20collection-ver.1.0.pdf
［8］ 日本コンピュータセキュリティインシデント対応チーム協議会「日本シーサート協議会加盟組織一覧 2019年版」，https://www.nca.gr.jp/imgs/nca_teams_2019.pdf
［9］ internet live status「Total number of Websites」，https://www.internetlivestats.com/total-number-of-websites/

略歴

萩原健太（はぎわら　けんた）
法政大学大学院公共政策研究科修士課程修了．サイバーセキュリティに関する支援や講演などを多数行い，政府や関係団体の委員会やワーキンググループなどの委員も務める．最近では，サイバーセキュリティの関連団体で業界発展のための活動を行う一方で，経営計画の策定支援やマーケティング活動の支援なども行っている．日本シーサート協議会運営委員長，ソフトウェア協会理事，Software ISAC共同代表，情報通信研究機構招聘専門員などを務める．