◎ 巻頭エッセイ ◎

イノベーションを支えるサイバーセキュリティー

梶浦 敏範
Kajiura Toshinori

日本経済は厳しい環境にある。これを打開する鍵は生産性の向上や付加価値の増大にあって、それを実現する手段としては「デジタルイノベーション」が一番手に挙げられる。日本政府は、あらゆるものがサイバー空間でつながった社会を “Society 5.0” と呼んで社会全体の発展を促している。これは、狩猟社会・農耕社会・工業社会・情報社会という段階を経てたどり着く5番目の「超スマート社会」を指している。社会全体がコンピューターになったような世界で、社会のそこかしこにあるデータを有効に活用して、社会的課題の解決と経済発展を同時に成し遂げようというものだ。産業界もこれに賛同し、むしろ自分たちが “Society 5.0” 実現の主役だと意気込んでいる。

サイバー空間でつながるメリットは、必要とされる物やサービス、情報などがどこにあるかが非常に簡単にわかることである。サイバー空間でのコミュニケーションは、コストが極めて安価でありリアルタイムで迅速に行ないうることが、広範なニーズとシーズのマッチングを可能にしている。「飢餓は食料の不足というよりは、その流通過程が破壊されることによって起こる」という意見もあるように、物やサービスがあっても必要とされているところに届かなければ意味がない。供給サイドとしてはニーズがあることにすら気づかないこともあり、これが社会全体からみると大きなロスになっている。このような課題を解消した社会を “Society 5.0” と言うのである。

「超スマート社会」では、出かけようと思えば自動運転車がやってくるし、頼んだ宅配物は帰宅時間に合わせて届く。地球の裏側にいる仕事仲間とは隣席にいるような感覚で議論ができるし、参照したいデータがあればすぐにディスプレイに表示される。「働き方改革」の究極の姿かもしれない。公的機関への届け出なども実際に足を運ぶことはほぼなくなり、自宅から24時間対応で手続きを済ますことができる。食卓上にある好物も、スマホをかざせば原産地や加工方法、アレルギー素材の有無も確認できる。遠隔診療や遠隔手術の可能範囲も広がるし、需要と供給のバランスを制御できるので、地方の医師不足の解消なども期待できるだろう。

*

「超スマート社会」は、社会のなかでデジタルデータが正しく生成・流通・活用されることで機能を維持している。昔のコンピューター業界のことわざに “Garbage in,

garbage out” というものがあり、入力データが間違っていれば計算結果は信用できないとデータの重要性を指摘していた。だから社会全体がコンピューターになったような「超スマート社会」では、上記の「正しく」が非常に重要な意味をもつ。

データを正しく運用するには条件がある。機密性（confidentiality）・完全性（integrity）・可用性（availability）の3つである。連携すべき機関以外に漏れるようでは機密性が保てないし、間違っていたり改ざんされるようでは完全性があるとは言えない。不正に暗号化されたりデータファイルを破壊されるなどして使えなくなれば、可用性に欠けるものになってしまう。

従来、システム運営者は、データへのアクセス制限をかけ、二重チェックをして間違いを防ぎ、バックアップを定期的にとるなどしてこれらの3条件を満たすよう努力していた。しかしこれらの対策をかいくぐる技術も一方には存在し、セキュリティー意識の高い企業・団体では、より強度の高いファイアウォールや暗号化技術を開発・導入したり、従業員教育を繰り返し行なうなどの努力を重ねてきた。

21世紀になると、地球規模でのデジタル化が進みインターネットが広く普及して上記のリスクは増大した。当初、企業・団体のホームページを書き換える愉快犯や、金銭をだましとる窃盗犯などだったサイバー空間の犯罪者たちは、やがて大規模かつ高度に組織化され、一部には国家権力を背景にするものも現われた。「サイバー攻撃」という脅威の登場である。

最初に大規模なサイバー攻撃が観測されたのは、2007年のエストニアでのこと。デジタル先進国であるエストニアの基幹であるITインフラに組織的で継続的な攻撃があったものだ。その後、ジョージアではロシアの軍事侵攻に先だつサイバー攻撃があり、ウクライナでは電力網が攻撃され大規模な停電が少なくとも2度発生している。

被害はこの地域にとどまらない。2014年には米国でSony Pictures Entertainmentが攻撃され、大量の未公開映像や個人情報が流出した。2016年にはバングラデシュ中央銀行から、約90億円の不正送金が為されている。この2件は北朝鮮の関与が疑われ、前者については米国当局が「北朝鮮の組織的犯行」と断じている。

2017年には、文字どおり世界中を “WannaCry（ワナクライ）” というランサムウェア（身代金要求型のマルウエア）が荒らしまわり、多くの企業・団体に被害が出た。英国では国民保健サービスが攻撃され医療機器や関連施設が影響を受け、約40の医療機関が被害を被った。予定されていた手術が中止となり、救急搬送された患者の手当てができないこととなった。日本企業も日立製作所や本田技研などでの被害が確認されるなど、多くの人の目に「サイバー脅威」が新しい段階になったことをみせつけた。これまでサイバーセキュリティーは重要だと思ってはいても具体的な行動に結びついていなかった企業・団体も、人員を強化したり組織を改編するなどの対応を始めるようになる。

これらの攻撃は金銭を狙ったものもあるのだが、国の重要インフラの機能を停止させて市民生活を脅かす可能性も含んでいる。つまりサイバー攻撃は、ある国家が他の国家に対する攻撃に使えることが実証されたとみていい。軍事行動の舞台が陸・海・空から宇宙・サイバー空間にまで広がったことによって、重要インフラの大半を民間部門が担っている現在の日本では、民間企業の責務は従来より一段と重いものになったと考えられる。日本を狙う攻撃者がいたとすると、相手は経済基盤・優位技術・市民生活を支えるインフラなどのなかで、一番弱いと思われるところに攻勢をかけてくる公算が高い。これを防ぐには、官民の垣根を越えた対策が求められる。

国家を背景にした組織の攻撃に、一企業で対応するのは難しい。したがって企業は自社を自分で守る「自助」に務めるだけでなく、業界内や業界を横断して連携する「共助」や政府からの支援による「公助」も得、さらには「国際連携」も行なうことによって、社会の耐久力を高める努力を続けなくてはならない。「共助」や「公助」を有効なものにするためだけでなく、「自助」の段階においてもサイバーセキュリティーに関する情報の開示や共有は不可欠である。かつては自社への攻撃を認識しても、諸般の事情でこれを隠す企業が多かった。本来は被害者である企業をメディアが厳しく糾弾することもあって、その傾向は強かった。しかし昨今は被害にあったことを進んで公表する企業も増えてきて、社会全体のセキュリティー性強化に貢献すべきだとの風潮があることは頼もしい。

*

日本でも、大量の個人情報流出、ランサムウェアによる機能停止、仮想通貨の盗難など被害が積み重なってきたこともあり、企業・団体の特に経営層の危機意識は高まっている。以前はサイバーセキュリティーと聞くと「技術課題だからCIO（Chief Information Officer、最高情報責任者）やCISO（Chief Information Security Officer、最高情報セキュリティー責任者）を置いて仕事を任せたよ」とする経営者が多かったのだが、昨今「サービス停止に追い込まれるようでは、お客様や社会に迷惑をかける。サイバーセキュリティーは経営課題だ」と捉える人も増えてきた。

「共助」としても、サイバーセキュリティ基本法改正に伴って、今年度、内閣サイバーセキュリティセンターが設立した「サイバーセキュリティ協議会」では、専門的な知識・能力を有する企業・団体やこれをとりまく企業群の連携により、ある会社への攻撃を検知したら同業他社や一般企業に注意を促すような体制は整いつつある。日本政府もサイバーセキュリティーにかける予算は増やしており、「公助」も強化されることが期待される。

しかし米国や英国の政府・企業・シンクタンクなど先進的な取り組みをしている団体と意見交換すると、日本の産業界側の課題もみえてくる。元来現場が力をもっている日本企業は、セキュリティー対策も“Event Driven”（攻撃を受けるなど何かが起きた

ら対応する）でボトムアップの傾向が強い。これはこれで重要なのだが、事件・事故は起きてしまったら何らかの被害は避けられない。一方英米の先進的な企業では、“Intelligence Driven”（あらかじめ得られた情報で攻撃などを予測し準備をする）でトップダウンなのだ。リスク管理に高い能力をもつ経営者が自ら情報を収集して予防にあたる。たとえば、「最近この種の攻撃手法でこういう情報が狙われる」といった情報を得て自社のその部分を強化しておくから、予備攻撃や攻撃準備の段階で攻撃者の意図を捉え、被害を未然に防ぐことが可能になる。

デジタルイノベーションを興し、“Society 5.0” を実現すべく活動するのは産業界の必然的な姿勢である。そうでなければ、業種にかかわらず現在および将来の国際競争に勝ち残れない。かつては国際競争には勝てなかったが、ある地域ではシェア1位を得て安定経営する企業もあった。しかしデジタルエコノミーの世界には国境も地域の壁もない。優れたものが世界市場を総取りすることが、しばしば起きる。しかしシェア1位になったからといってサイバーセキュリティー対策を怠って信用を失墜するようなことになれば、すぐに市場から追われてしまうことも考えなくてはいけない。世界中に競合他社はいるのだ。

“Society 5.0” は、事実上サイバー空間で成り立つ社会である。そこでの最大の脅威は「サイバー攻撃」であると言っても過言ではない。これへの対処能力を高めること、その努力を続けることは、これからの国・企業・団体、ひいては個人に至るまで社会の一員に加わる以上は必要なことと言えよう。

かじうら・としのり　日本サイバーセキュリティ・イノベーション委員会代表理事／
（株）日立製作所上席研究員
https://www.j-cic.com/
kajiura@j-cic.com