連載 第2回

セキュリティ(危機管理)の本質と課題

執筆／江崎 浩

「安全」は存在しない

まず、安全と安心の正しい理解が必要である。2004年に文部科学省がまとめた「安全・安心な社会の構築に資する科学技術政策に関する懇談会」[1]がまとめた報告書では、以下のように定義されている。

安全: 人とその共同体への損傷、ならびに人、組織、公共の所有物に損害がないと客観的に判断されることである。リスクを社会が受容可能なレベルまで極小化している状態を安全であるとする。安全を高めようとすればするほど、利便性や経済的利益、個人の行動の自由等が制約され、プライバシーが損なわれる可能性がある。

安心: 安心については、個人の主観的な判断に大きく依存するものである。人が知識・経験を通じて予測している状況と大きく異なる状況にならないと信じていること、自分が予想していないことは起きないと信じ何かあったとしても受容できると信じている状態である。人々の安心を得るための前提として、安全の確保に関わる組織と人々の間に信頼を醸成することが必要である。

「安全」は実際には存在せず、世の中には「安心」しか存在しないことを、我々は忘れがちである。また、日本では「安全」が存在すると(勘違い)して、危機管理の施策を適用している場合が少なくない。これこそが、安全な国とされる日本の「落とし穴」であることを十分に認識しなければならない。

安心は「誰かが解決してくれるもの」ではなく、「関係するすべてのステークホルダ間による協調・協働」によって実現されるものであることを念頭に置かなければならない。その結果、「まずは自助、次に共助、最後に公助」の考え方が基本となる。「共助」においては、機器・ソフトウェア提供者、サービス提供者、サービス利用者にまたがる垂直方向の関係者と、提供者間及び利用者間という水平方向の関係者の両軸での協調・協働が実現されることが重要となる。関係するすべてのステークホルダが、自分のシステムの安心度(トラスト)を向上させ、さらに自分のシステムに関係するシステムを運営する方々と協調・協働することで、サービスの品質が向上し、市場での競争力向上につながることになる。すなわち、サービスや製品の提供者が主導のWater-Fall型(=PUSH型・一方向型・非対称型)のサプライチェーンではなく、ステークホルダが対等に相互作用する双方向のNetwork型(=対称型)あるいはユーザーの要求・需要に応じたPULL型のデマンドチェーンの形成である。日本においては、Water-Fall型のサプライチェーンによる品質管理や製品企画が行われている場合がほとんではないだろうか。アマゾンやナイキなど、最先端のグローバル企業においては、ネットワーク型のデマンドチェーンを形成し、しかも、社内のすべてのセクションが顧客や取引先とのコミュニケーションをデジタルネットワーク技術を用いて実現している。“Connected Company”である。

セキュリティ対策は疎かにすると生き残れないし、事業経営に貢献しないと意味がない

さて、安全・安心の確保がセキュリティであるが、以下では、特に、サイバーセキュリティを議論する。そもそも、我が国おいては、「モノづくり」「匠」に象徴されるアナログを尊敬し重要視する傾向にあり、大きくデ

江崎 浩(えさき ひろし)
東京大学大学院 情報理工学系研究科教授
1987年九州大学工学部電子工学科修士了。同年4月東芝に入社。1990年米国ベルコア社。1994年コロンビア大学にて客員研究員。1998年10月東京大学大型計算機センター助教授。2001年4月東京大学大学院情報理工学系研究科助教授。2005年4月より同研究科教授、現在に至る。WIDEプロジェクト代表/Internet Society理事/データセンター協会理事・運営委員長。

ジタル化・オンライン化が後れている状態にある。早急に、全社会・産業システムのデジタル化・オンライン化を進める必要があるが、そのためには、しっかりとしたサイバーセキュリティ対策を確立しなければならない。すなわち、サイバセキュリティ対策を、社会・産業界において重要視されている「安全衛生対策」と同レベルで取り組まなければならない。ポストコロナで実現されるオンライン・ファーストの社会においては、サイバーセキュリティの品質がユーザーに提供されるサービスや製品の品質に直結するものであると捉えなければならない。

セキュリティ対策は、ユーザー・顧客への安全・安心環境の提供だけでなく、事業の継続と発展も目的としている。ただし、現実では事業の継続のためのセキュリティ対策には難しい問題がつきまとう。なぜなら、事業の発展のように新たな収入に貢献する可能性を持っていないからである。新たな収入の獲得よりも、インシデント発生時の支出(減収)を小さく抑えることが主眼となり、積極的な投資対象にはなりにくくなってしまう。特にインシデントが発生しないときには、事業の継続のためのセキュリティ投資は削減の対象となる傾向にある。すなわち、セキュリティは「常時は邪魔者である」、「無事故が続くとやめてもいいと思う」、そして「さぼっても利益構造に変化がない」というわけで、しだいに疎かになっていく。一方、事業の発展と品質の向上を目的としたセキュリティ対策、そのなかでも創造的活動を促すためのセキュリティ対策にはポジティブな面があるが、成功する創造的活動が出てこないと、こちらも投資意欲が減退してしまう。

さらに、政府によってサイバーセキュリティーインシデントは、企業にとって重要なインシデントであり、企業トップ(CTO/CEO)への報告が義務化された。その結果、現場の人たちは、インシデントの発生にも関わらず、その隠蔽工作[2]を行う場合が少なくない。これは、上司への忖度の結果でもある。事務作業の発生ばかりではなく、生産ラインの長時間の停止が発生してしまうことを回避させたいと考えてしまうのである。

このように、現実の事業環境でセキュリティ対策を適切に実施・継続していくことは、決して容易ではない。さて、江戸時代に地域の財政を数多く再建させたことで有名な二宮尊徳は、次の言葉を残している。

『道徳を忘れた経済は罪、経済を忘れた道徳は寝言』

「道徳」を「セキュリティ」(危機管理)、「経済」を「事業経営」に置き換えると、セキュリティ対策を疎かにする組織は生き残れないし、事業経営に貢献しないセキュリティ対策は意味がない、ということなる。短期利益を最重要のKPIとする経営においては、インシデントが発生しない時には、セキュリティ対策(=“道徳”)が利益貢献をしないので、削減あるいは切り捨ての対象となってしまったため、インシデント(COVID-19)が発生した時の、危機管理能力・対応能力を失っていたことが、今回のコロナ禍で顕在化したのではないだろうか。

1「安全・安心な社会の構築に資する科学技術政策に関する懇談会」…安全・安心な社会の構築に資する科学技術政策に関する懇談会、「第2章　安全・安心な社会の概念」2004年4月。
http://www.mext.go.jp/a_menu/kagaku/anzen/houkoku/04042302/1242079.htm

2 サイバーインシデントではなく、対称機器の瑕疵や機能不全として処理。