# CFO 視点で考えるサイバー攻撃対策 ―事業運営におけるリスクコスト―

東京理科大学大学院 教授　加藤晃

## サイバー攻撃の実態

世界経済フォーラムの「グローバルリスク報告書2024年版」では、「サイバー犯罪やサイバーセキュリティ対策の低下」は、「今後2年間に起こりうる影響（深刻さ）」において、挙げられた34件中第4位、「長期的（今後10年間）な深刻度」においても8位にランキング入りし、人工知能（AI）技術がもたらす悪影響のリスク要因が挙げられている。

昨今、二重脅迫型ランサムウェア、サプライチェーンを狙ったサイバー攻撃事件などの報道に接する機会が増えている。他方、サイバー攻撃はリスクマップ上では、第2象限（低い発生頻度、高い損害額）にプロットされる。誰しも、「まさかわが社が狙われるなど…」と思いたい心理は理解できるが、これは正常性バイアスと呼ばれる。犯罪者は、システムの脆弱なところを攻撃する。また、その攻撃手法は刻々と進化している。ゆえに、どんなに対策をとっても完璧はなく、一度問題が起きると強い批判に晒されるのはご存じの通りである。インシデントが発生すると、信用失墜、顧客／取引先への被害を引き起こす可能性がある。他方、表面化せずに知的財産などの企業秘密を盗まれることもある。

## CFOの視点

最高財務責任者（CFO）は、企業の中長期的な成長や収益性を向上させるために必要な資金計画や投資判断など、企業の財務面に特化した役割を果たしており、サイバー攻撃の脈絡では、万一、攻撃を受けた場合でもその被害を最小限に抑える使命がある。

事業は必ずリスクを伴い、経営行動を取ると一定期間に何らかの損失が生じる可能性がある。事前に、将来的に発生しうるリスクを発見、その発生頻度と財務的な影響度（強度）を推定して、経営に影響を及ぼすと判断された潜在的リスクに備える処理手段として、リスクコントロール（潜在危険の回避、損失予防・損失軽減、分離、結合、移転）とリスクファイナンス（保有、移転）があり、最適な手段を選択して実行し、その成果を監視し改善を行う。これら一連のリスクマネジメントの目的は、企業のリスクコストを最小化することによって、企業価値を最大化することである。

それでは、リスクコストにどれ位の準備（投資・支出）をすれば良いのか、他社はどうしているのか、という疑問が湧いてくるのではないだろうか。結論から先に言えば、絶対的な基準は存在しない。何故なら、業界が異なればリスクは全く違うし、企業によっては多角化している場合もある。大きな資産を保有する老舗と起業したばかりの企業では経済的な蓄積が違う。仮に大きな資産を持っていても換金性が低いようであれば、条件が異なってくる。

そして何より事業リスクに対する経営者の考え方（リスク選好、リスクアペタイトと言う）に大きく依存する。リスクマネジメントに関わるリスクファイナンスとリスクコントロールの費用合計がリスクコストである。英語では、Total Cost of Risk（TCOR）と表記される。米国のリスク・保険マネジメント協会（RIMS）によれば、調査した大企業のリスクコストは、約1％（2019年版）であり、中堅・中小企業は、その数倍と推測されている。訴訟大国である米国の数値なので割り引いてみる必要があるが、参考になるデータではないだろうか。ただし、リスクコストは、事業全体をカバーするコスト概念なので、本稿の文脈ではサイバー攻撃を対象として、費用対効果を十分に検討した投資・支出を議論しなければならない。換言すれば、経営者（特にCFO）は、リスクコントロールとリスクファイナンスという2つの手法のバランスを考える必要がある。

## リスクコントロール

サイバー攻撃対策の基本はリスクコントロールである。自社の従業員へのリテラシー向上教育（強固なパスワードの採用、ソフトウエアのアップデート、怪しいメールは開かない等)、取引先企業へのデューディリジェンス、ベンダーの選別、事業継続計画（BCP）の策定、セキュリティレベルのプロによるチェック、最高情報セキュリティ責任者（CISO）の採用・育成などが考えられる。実際、川上から川下まで長大なサプライチェーンを考えるとどんなにネット上で対策を講じても、最も脆弱なところから侵入される可能性は排除できない。そこで、ゼロトラスト・セキュリティが講じられるようになってきた。

他方、サイバーセキュリティ対策組織の陣容と規模については、79.0％の組織が不足していると回答している。いずれにせよ、どんなに対策を講じてもサイバー攻撃の手法は間断なく高度化・巧妙化している以上、リスクをゼロにすることは不可能と思った方が良いだろう。

なお､リスク対策の情報開示については､しっかり対策をしていることをアピールすることで取引先や投資家に安心感を与え、かつ攻撃対象リストから外れることを期待する意見がある一方、攻撃側に防御体制のヒントを与えることになるとの理由から否定的な意見の両方が存在する。

## リスクファイナンス

サイバー攻撃を受けて金銭的な損害が発生した場合、主に二つの方法がある。1つは、利益剰余金やキャプティブ（自社専属の再保険会社）など、保有する資産で支弁する方法である。もう一つは、外部へのリスク移転、サイバー保険への加入である。サイバー攻撃は、大数の法則が効き難く、かつ、攻撃に遭った場合の損害が非常に大きくなる可能性が高いことから、いわゆる内部留保の大きい企業と言えども損害保険の活用をお薦めする。副次的な効果として、損害保険会社は引き受けにあたって、当該企業のリスクコントロール体制を審査する。また、インシデントの発生確率を下げるために効果的なアドバイスを行うかもしれない。

サイバー保険の補償内容としては、①賠償損害（損害賠償金、争訟費用等)、②費用損害(原因調査費用、コールセンター設置費用、広報対応費用、見舞金支払い)、③事業停止損害(利益損害､営業継続費用)が挙げられる。一度、サイバー攻撃が発生すれば、これらの給付項目はほぼ全て補償対象となるだろう。リスクは確実に集積している。

## DXの推進と見直しも

日系企業は、本業へのデジタル・トランスフォーメーション（DX）の取り組みが遅れていると言われているが、その推進過程でサイバー攻撃対策が見過ごされていることはないか｡長年行われてきた基幹システムのシステム･インテグレーター（SIer）への丸投げで良いのか、という論点もある。

CFOは経営財務の最高責任者として、情報技術の専門職位である最高情報責任者（CIO)･CISOと協力体制を築き、リスクコストを意識した、費用対効果に優れた意思決定（リスクコントロールとリスクファイナンスの組み合わせ）を行う責務を負っている。金融・資本市場のプロフェッションは静観しているようで、株価算定に必要な加重平均資本コスト（WACC）にリスクコストを密かに反映しているかもしれない。見直しされては、いかがだろうか。

＜参考文献＞
加藤晃『CFO視点で考えるリスクファイナンス』保険毎日新聞社、2018年。
加藤晃・安岡祥吾「製薬企業の情報セキュリティ開示－サイバー攻撃Ⅱ－」『国際医薬品情報』通巻第1229号､国際商業出版、2023年7月10日。
教学大介「サイバー保険の開発と日本企業のセキュリティ実態」『日本セキュリティ・マネジメント学会誌』Vol.35, No.2、2021年。
薩摩貴人「サイバーセキュリティ最新動向 2022 ～サーベイ結果を読み解く～」KPMGジャパン、2022年5月26日。
日本損害保険協会「サイバーリスク意識・対策実態調査2022」2023年。
World Economic Forum, “Global Risk Report 2024,” January 10, 2024.