フォーサイト・ニュースレター11月号

November 1, 2020

カテゴリー: サイバーリスク, パンデミック, 新型コロナウィルス

タグ: RIMS, Wannacry, サイバーリスク, サイバー保険

コロナ禍が拍車を掛けた サイバーリスク対応の重要性

テニスの前に中止された高地のイベント

8月号で、コロナ禍でウィンブルドンテニス等の様々な大型イベントが中止に追い込まれた事に触れたが、リスクマネジメントの分野でも、今年は議論が深まる事が期待されていたサイバーリスク関連の大型イベントが中止に追い込まれていた。
今年の5月上旬には、世界中の企業や組織のリスクマネジメントの関係者、保険業界、キャプティブ保険関係者やキャプティブ設立地の金融当局関係者が、ロッキー山脈の目と鼻の先の米国コロラド州デンバー市で行われる、サイバーリスク祭りと形容できそうなRIMS（※）2020年次総会に大集合していたはずだった。
※RIMSは本部をニューヨークに置く、北米を中心に世界60か国から3500社・1万人以上が会員となっている、1950年創立の世界最大のリスクマネジメント団体である。

- *RIMSの年次総会は毎年4日間に亘って開催され、同じ時間帯に同時並行で複数のセミナー・講演・研修会等が常に実施されることから、講演者数は毎年4日間合計で300人以上という大掛かりなものである。*

注目すべきなのは、RIMS年次総会では企業や組織による講演も多く、リスクマネジメントにおいて今後の重要なテーマや分野を毎年俯瞰できる機会になる点である。RIMS2020の参加者向けに事前配布された時間割表（4日間・毎日6時限）を眺めると、今年はサイバーリスク関連の講演に専用の「CTR」という略称コードをわざわざ設定するほどの力の入れよう

で、ほとんどの時限に「CTR」というコードが振られているか、別の分野ながらサイバーリスクに関連するセミナーや講演が予定されていた。各講演の題名だけ見ても、「ランサムウェア」「ウェアラブルデバイスの法的リスク」「囚われのデータ」「職場でのSNS」「戦争危険免責とサイバーリスク」「地震とサイバーリスク」「生体情報プライバシーと団体訴訟リスク」と、一日中議論ができそうなトピックがずらりと列挙されていた。

RIMSの年次総会のテーマや内容の構成は1年前（つまり、前回の年次総会開催前後）の時期から協議が行われ、またその協議のための基礎材料である市場調査等は更に前の時期から進められていることから、サイバーリスクは2018年頃には既に重要なテーマになりつつあったと言える。

「おうちで〇〇」「巣籠」の裏返しはサイバーリスク

サイバーリスクの根幹にある機密情報の取得・管理・利用や、それらの盗用リスクは、目新しいものではない。情報技術の発展と同じくらい歴史が古く、表裏一体であるとも言える。映画の題材[(1)]にもなった数学者アラン・チューリングが1930年代から開発に関わった初期コンピュータの原型やその理論は、無線傍受で入手したドイツの暗号解読という機密情報の抽出が目的だった。1世紀前と違うのは、一般人の生活や経済活動自体がその仕組みに大きく依存しつつあり、またトラブルが発生した際の被害と規模が大きくなりやすいことにある。

コロナ禍はRIMS年次総会を中止に追い込んだ一方で、その年次総会がテーマにしようしていたサイバーリスク対策の重要性を非常に速いペースで更に高めている。

テレワーク・巣籠・ネット注文・遠隔医療等、コロナ禍は企業や組織に多くの業務を前倒しで集中的に電子化・オンライン化させる潮流を生み出している。一般消費者によるデジタル化も進んでいる。JCBが8月に発表した「キャッシュレス決済に関する調査～コロナ禍におけるキャッシュレス決済事情～」の調査結果では、B2C分野での電子決済の浸透が速いペースで進んでいることが示唆されている[(2)]。Eコマース分野においては決済承認技術の進化が生体情報の取得と管理に繋がり、それが新たなリスクを生み出す[(3)]との指摘もされており、こうしたシステムや金融インフラに関わる事業者にとって、サイバーリスクは避けて通れないものである。経済活動の電子化・オンライン化が進む昨今におけるサイバーリスクの理解とその対策の確立の重要性は益々高まる状況にある。

また、情報技術の発展の中核になりつつあるAIやビッグデータ等の活用も、その活用自体に伴うリスクとは無縁ではない。例えば、2019年10月に米科学誌Scienceに掲載された医療用AIに関する論文 では、治療方針の検討支援のために用いられ米国内で既に広く普及している医療用AIが、特定の人種に対して偏った治療方針の提案（或いは治療を不要とする提案）を提示するに至っていたという報告がされている。AIが提示する内容を検証せずに流れ作業的にAIの提案通りの診断を行った結果、第三者の健康、財産、権利等に対して損害や損失が発生するというシナリオも今後のリスクとしては考えられるであろう。

まさに前述の講演の題名自体が問題提起した事柄が「もし」ではなく現実となり、「何時起こるか、その時のためにどのような対策を立てておくべきか」という状況に進みつつあると言える。サイバーリスク事象が発生した際は費用や賠償の発生を伴うケースが非常に多いため、その財務的対応をどうすべきかという課題は必然的に検討事項として出てくる。

サイバーリスクのためのファイナンス対応は「保険を買う」だけなのか？

サイバーリスクのための財務的な対策となると、大抵の場合はRIMS年次総会の保険業界による講演やパネルディスカッションでも語られるように、サイバーリスク保険の手配という話になることがある。一般的に保険契約というのは、保険料という対価を差し出す代わりに、有事の際には合意された条件（＝保険契約の約款等）に基づいて第三者（つまり保険会社）の資本を使うというものである。

但し、これがサイバーリスク対応のためのリスクファイナンス上の万能薬かというと、その限りに非ずというのが実際のところである。10月19～20日にハワイ州からライブ配信されたハワイキャプティブ保険協会（Hawaii Captive Insurance Council）のヴァーチャル・フォーラム(5)において、全世界のキャプティブ保険会社(6)による引受種目の中で追加または増額された種目のトップがサイバーリスクという結果が報告されている。こうした調査報告は、キャプティブ保険子会社の設立や活用が最も多い欧米における傾向を強く反映するもの

の、欧米で普段キャプティブの利用目的のトップになりがちな従業員福利厚生や賠償責任リスクを抑えての結果であることを考えると、サイバーリスクへのリスクファイナンス手段として、キャプティブというグループ内の資本の有効活用手段が非常に重視されていることを示唆している。

サイバーリスクは財務的にも重要性がトップレベルでありながら、情報技術や利用方法自体が常に変化するという特徴を持ち、また潜在的なリスクの集積や範囲が大きくなる傾向が強い。このため、第三者である保険会社は、企業や組織のリスクファイナンスに対していつも満額回答ができるとは限らず、場合にはよってはゼロ回答になることもある。

2017年に大きなニュースとなったランサムウェアの「WannaCry」の騒動では、保険業界が支払った保険金は限定的なものであったと考えられるものの、保険業界が事後に再検討や議論した事として「企業／組織がこうした既知のセキュリティ脆弱性問題への対応を怠った場合に、サイバー保険ポリシーにおいて過失怠慢による損害賠償責任を補償の対象とするか」というものがあった(7)。また補償範囲が維持されたとしても、補償額には上限があり、保険金の請求時に期待通りの保険金（つまり、キャッシュ）が確保できるかどうかについても、保証があるわけではない。企業や組織にとってみれば、サイバーリスク保険単体では、補償範囲やその対価の保険料が毎年安定的に確保できるとは限らない局面が多々あると言える。

自社グループ内の資本を有効活用し、グループとして必要なサイバーリスクへの財務的補償体制の確保とグループ内でのキャッシュの循環を車の両輪的に達成する手段として、キャプティブは多くの可能性を秘めており、海外においては既に実例も増えつつあると言える。多くの企業や組織での基幹業務の電子化・オンライン化に伴い、コストや資本効率をバランス良く追求できるキャプティブを通じたサイバーリスクの確保は、今後重要な選択肢となると考えられる。

キャプティブ保険を通じたサイバーリスクのためのリスクファイナンス設計

では、サイバーリスクのために、グループ内の資本を活用してキャプティブ保険会社を使うというのは具体的にどうなるのか。代表的な例を基に、その基本的な仕組みを紹介する。

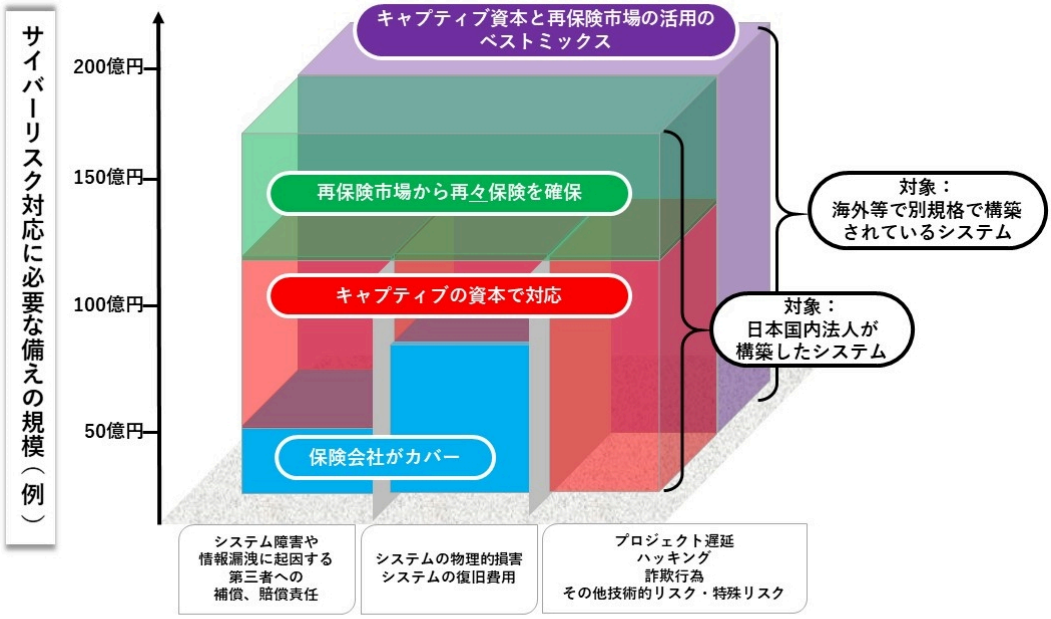
- リスクファイナンスの対象となるサイバーリスクが日本国内所在のもの（例：対象とする企業は国内法人）という前提を置くと、まずサイバーリスク保険という金融商品自体は、日本国内の保険会社を通じて手配することになる。

- 一旦保険会社が引き受けたリスクとその対価の保険料は、再保険の形でキャプティブに移転（これを出再と呼ぶ）が可能である。ここでポイントとなるのが、キャプティブを持つことにより、再保険市場に直接アクセスする手段が手に入る事になる点である。キャプティブは法制度の整備された国や地域（シンガポール、ミクロネシア連邦、米国ハワイ州等）に設立するため、海外の再保険会社として活動ができる。

- 再保険会社として、サイバーリスクを含め様々な保険の開発と改良が最も進んでいるロイズ（英国）、欧米の再保険会社、アジアの再保険市場（特にシンガポール）に直接アクセスし、自社グループに必要な保険の交渉と設計が可能となる。再保険市場におけるコストである再保険料は、キャプティブの資本（つまり自社グループの資本）とのバランスや、再保険の契約方式次第で、様々なパターンの設計も可能である。

- 或いは、自社グループの資本の使い方次第で、「自分専用の保険」を設計することも可能になる。この場合は再保険市場に頼る必要もなくなる。
- このようにして、キャプティブの資本と再保険を組み合わせ、理想とした保険を設計し、その補償内容を総額ベースで日本国内での保険契約に反映させることにより、グループにとって最適なリスクファイナンス体制の確立が可能となる。

- 上記のような手順をベースに設計したサイバーリスクのためのキャプティブ保険を活用したリスクファイナンスを視覚化すると、次のような図にまとめられる。この中で、青以外の部分は企業や組織自身が、キャプティブを通じて検討を含め、多くの部分をコントロールできる利点があり、柔軟性が高く臨機応変の対応が可能になると言える。



リスクファイナンス対応の対象となるサイバーリスク

参考文献

1. The Imitation Game　イミテーション・ゲーム／エニグマと天才数学者の秘密 (2014)
2. https://www.global.jcb/ja/press/20200821140457.html
3. 2019年11月20日付 Financial Times紙「Ecommerce turns to biometrics to validate shoppers」
4. Obermeyer Z, Powers B, Vogeli C, Mullainathan S. (2019) “Dissecting racial bias in an algorithm used to manage the health of populations”. Science. https://science.sciencemag.org/content/366/6464/447
5. https://hawaiicaptives.com/hcic-2020-virtual-forum/
6. キャプティブ保険会社の基本的な仕組みについては、http://www.foresightmgt.co.jp/captive/　を参照
7. 独立行政法人情報処理推進機構（2017）「米国におけるサイバー保険の現状」