求められるサイレントサイバーリスクへの対応

「サイレントサイバーリスク」は、既存の財物保険や賠償責任保険等における潜在的なサイバー関連の損失リスクを指し、保険会社にとって巨大なシステミックリスクとなりうる。保険会社は、補償範囲の明確化やリスクエクスポージャーの特定を進めるとともに、顧客に対してサイバーリスクの理解を促すことが求められる。

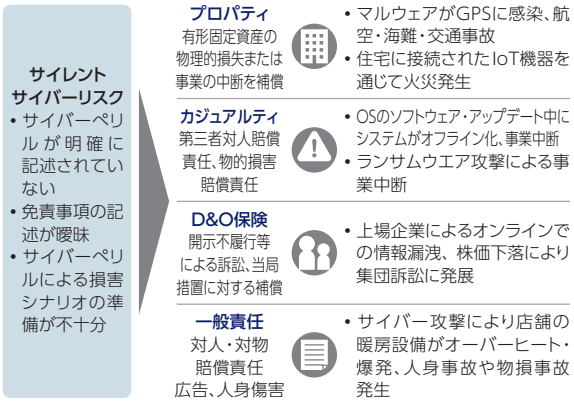
既存保険に潜むサイレントサイバーリスク

サイバーリスクの脅威が高まる中、「サイレントサイバーリスク」の管理が、保険会社にとって重要性を増している。「サイレントサイバーリスク」とは、既存の財物保険や賠償責任保険等における潜在的なサイバー関連の損失を指す[1)]。サイバーリスクの補償に特化していない保険に内在し、IoTや自動運転車など、技術発展に伴いリスクが増大することが懸念される。

具体例として、マルウェアに感染したGPSが航空・海難・交通事故を引き起こしたり、サイバー攻撃によって住宅に接続されたIoT機器が火災を引き起こしたりするリスクなどが挙げられる（図表）。商品設計段階ではサイバーリスクが考慮されておらず、補償範囲や免責事項が具体化されていないため、保険会社は意図せぬ補償を求められる可能性がある。

2017年に発生したNot-Petyaによるマルウェア攻撃では、被害総額30億ドルの90%以上がサイレントサイバーリスク関連の損失とされている。さらに補償請求を行う企業に対して、一部保険会社が戦争排除条項を根拠に保険適用に意義を唱えたことで、訴訟案件に発展するなどの混乱が生じた[2)]。

図表　想定されるサイレントサイバーリスクの例



(出所) MARSH "Silent Cyber" —Frequently Asked Questions (2020年9月) 等を基に野村総合研究所作成

リスク把握に乗り出した監督当局

欧州の監督当局はいち早くサイレントサイバーリスクの対応に着手した。例えば英国の健全性監督機構（PRA）は2019年、サイバーリスク管理のための活動計画策定を保険会社に指示し、「悪意あるサイバー行為」と「悪意ないサイバーインシデント」に対する補償提供の明確化を求めた。さらに欧州保険・企業年金監督局（EIOPA）はサイレントサイバーリスクに関し2022年9月に、「保険会社は健全な引受慣行を目的としてリスクのエクスポージャー特定や測定を行うべき」とし、当局としてもリスクモニタリングや管理を確実なものとすべきとの声明を出している[3)]。

サイレントサイバーリスク把握の難しさ

保険会社がサイレントサイバーリスクに対応するには、①保険約款において免責事項を設定する、②既存契約の補償上限額や補償内容を見直す、③補償範囲を明確にしたサイバーリスクをカバーする商品・サービスを提供する等が挙げられるが、依然として多くの課題がある。

第一に、サイレントサイバーリスクのエクスポージャーの測定や損害シナリオの準備が困難なことだ。サ

NOTE

1) 「サイレントサイバー」は、“non-affirmative cyber”と表記されることもある。出所）Silent Cyber: What you need to know (Willis Towers Watson, 2021年2月1日)
2) 例えば、2017年に製薬大手のMerck & Co. Merckは、NotPetyaによってコンピューター内のデータが破壊され、当初推定8億ドル以上の損失を被った。同社は17億ドル以上の保険に加入していたが、一部の保険会社が、NotPetya攻撃がウクライナに対するロシアの敵対行為の一部である「戦争行為」であるとして損失の補償を拒否したため、訴訟に発展した。
3) “Supervisory statement on the management of non-affirmative cyber exposures” (EIOPA, 2022年9月8日)
4) Cyenceは2014年に設立され、サイバーリスクと確率を定量化するリスクモデリングプラットフォームを損害保険会社に提供している。2017年Guidewire Software社に買収された。
5) 例えば、東京海上日動火災保険は2022年1月、賠償責任保険契約において、サイバー攻撃危険不担保特約を自動付帯している。出所）「賠償責任保険（専門職業用）の約款、2022年1月1日以降始期用（東京海上日動火災保険）」https://www.tokiomarine-nichido.co.jp/hojin/pdf/senmon_yakkan_20220101.pdf
6) 日本では2015年頃から、損害保険会社がサイバー保険の販売を開始している。なお日本能率協会総合研究所は、市場規模は約200億円（2018年）→700億円規模（2023年）まで拡大する見通しを示している。出所）「サイバーリスク意識・対策実態調査2020」（日本損害保険協会、2020年12月9日）、「サイバー保険市場　2023年に700億円規模に」（株式会社日本能率協会総合研究所、2019年1月21日）。

イバー攻撃が複雑化する一方、保険会社は実際に起こった過去のイベントをもとにリスク算定やプライシングを行わざるを得ない。適切にプライシングされていない契約は膨大な請求コストにつながる。

第二に、保険契約者と保険会社の間に大きな認識ギャップがあることだ。多くの契約者が既存の財物・賠償保険のポリシー内で、サイバーリスクがカバーされると想定している。保険契約者が契約内容を十分理解していないままに保険会社が補償範囲を変更すれば、更新可能性を低下させることになろう。

サイレントサイバーリスクに対応するアリアンツ

独保険会社アリアンツ・グローバル・コーポレート・アンド・スペシャルティは2019年に、顧客に対して明確で透明性の高いサービスを提供すべく、すべての保険契約のサイバーリスクを確認し、補償内容の明確化と更新に着手した。具体的には、①従来の保険契約でのサイバーリスク補償範囲の設定、②サイバー専用保険が必要となるシナリオの明確化を進めた。例えばハッカーの攻撃で産業用ソフトウェアが工場の爆発を引き起こした場合、物理的な損害は従来の保険契約でカバーされる一方、売上減少等の経済的な損失はサイバー保険のみでカバーされることとした。これにより保険契約者に補償内容を確実に伝え、新たなサイバー専用保険の提案につなげている。また、引受に際しては明確なレビュープロセスを設け、顧客のサイバーリスク対策意識を促している。

また、アリアンツは2018年に、グループ内のサイバー専門ノウハウを集約し、「センターオブコンピテンスフォーサイバー」とよばれる専門組織を設立した。同組織はグループ横断でのサイバーエクスポージャー管理を担い、各事業拠点に対して引受ガイドライン、研修施策、プライシングモデルなどを提供している。各拠点の約款変更には同組織の承認を必須とすることで、保険ポートフォリオのリスク管理を効率化し、引受ケイパビリティの有効活用や、大規模なサイバー損害シナリオに備えるための資本準備を進めている。また、外部のサイバー関連サービスプロバイダーとのネットワーク構築にも取り組んでおり、米国Cyence[4]と連携してサイバー攻撃による事業中断リスクに対する新しい予測モデリングツールの開発等を進めている。

求められる顧客への明確な説明

日本では2022年1月、一部保険会社がサイバー攻撃危険不担保特約を既存保険契約に自動付帯し、サイバー攻撃等に起因する損害の賠償責任保険等の保険金は支払対象外とするなどの対応が進められている[5]。

保険会社には、契約者のプロテクションレベルを向上させることが期待されている。保険契約でカバーされる補償内容を明確にすることにとどまらず、既存契約に潜むサイレントサイバーリスクの理解や対策を促すことが保険会社のリスクエクスポージャーの管理適正化やさらなるサイバー保険事業の拡大につながるだろう[6]。

Writer's Profile

小野 亜樹 Aki Ono
金融デジタルビジネスリサーチ部
エキスパートコンサルタント
専門はリテール金融
focus@nri.co.jp