THE GENEVA ASSOCIATION

INSURANCE FOR A BETTER WORLD

サイバーリスクの集積：
保険引受の課題への本格的な取組み

研究要旨2023年11月

ジュネーブ協会 Cyber & Evolving Liability ディレクター**Darren Pain**

サイバー攻撃は、データや IT サービスの機密性、利用可能性、あるいは信頼性を損なう悪意のある行為または偶発的な行為であり、時には同時に、かつ異なる地域にまたがり、多くの人や組織に被害をもたらす可能性があります。このような重大な累積損失の可能性は、通常の財産や責任保険の一部として、あるいは単独のサイバー補償を通じて顧客からサイバー関連リスクを引き受ける保険会社にとっては非常に問題です。

潜在的なサイバー損失の集積に対する懸念は、今に始まったことではありません。しかし、近年の地政学的緊張の高まりにより、サイバー脅威の状況は著しく悪化し、深刻なサイバー事件への懸念が高まっています。2022 年の世界的なサイバー攻撃は、2021 年と比較して 38%増加しており、ランサムウェア攻撃は引き続き脅威となっています。国家レベルの脅威者は、破壊目的のサイバー兵器使用など、現在進行中のロシア・ウクライナ紛争の域を超えて、サイバー空間でますます攻撃的になっています。

私たちはまだ真に壊滅的なサイバー事件を経験していませんが、敵対者は、経済的損失が拡大するおそれのある主要な経路である重要なインフラやデジタルサプライチェーンをますます標的にしています。これには、大規模な攻撃の実行、広く使用されている企業ソフトウェアや脆弱なレガシーサイバーセキュリティプロトコルの未知の脆弱性を悪用した、複数の被害者を対象とした重要なコンピューターシステムやデータの暗号化、およびクラウドベースのサービス妨害などが含まれます。

大規模で永続的なサイバー補償ギャップ

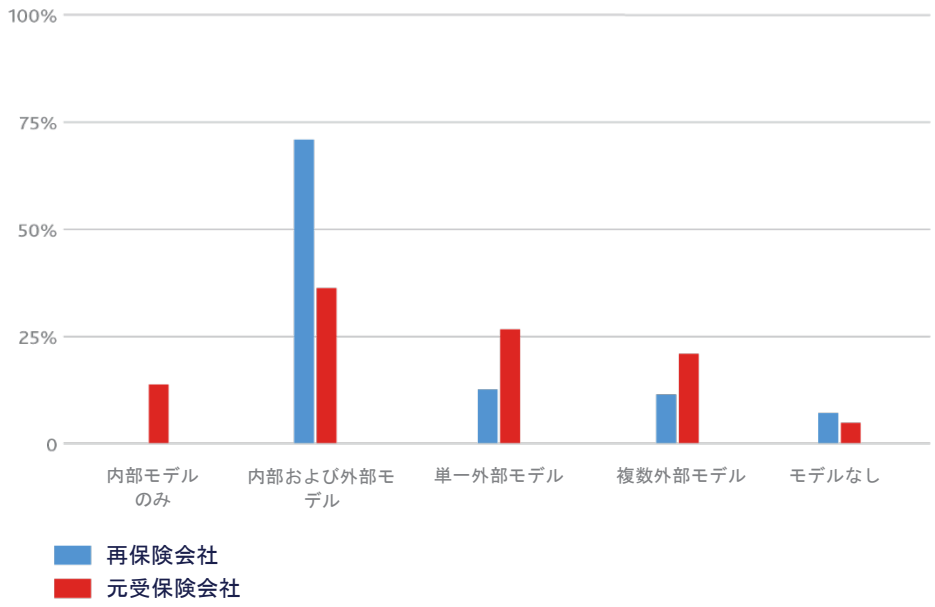
より敵対的なサイバー環境は、サイバーリスクがもたらす保険数理上の課題を浮き彫りにしました。特に、サイバー損失の頻度と損害規模をもたらす要因は必ずしも十分に理解されておらず、通常、標準的な統計的アプローチでモデル化することはできません。サイバーは人為的な危険であり、被害の程度は被害者と攻撃者の両方のインセンティブ、動機、および資源の相互作用によるため、それはたいてい複数要因間の複雑で非線形関係が影響します。

このような背景から、慎重な保険会社が、厳密に定義された契約文言と限定的なリスク吸収力でサイバーリスクを引き受けていることは、驚くべきことではないでしょう。しかし、企業、個人、および政府がデジタル技術にますます依存するようになるにつれて、大規模なサイバー事件や攻撃による総費用は増加し続けています。サイバー犯罪の年間費用は約 1 兆米ドルから最大 8 兆米ドルと幅広く推定されますが、世界のサイバー保険料が 120 億米ドルから 140 億米ドルであることと比較すると、相当な量のサイバー関連損失が無保険であることがわかります。

保険数理の進歩

サイバー保険の規模と範囲をさらに拡大し、想定される補償ギャップを埋めるためには、壊滅的なサイバーリスクを定量化する方法を改善することが不可欠です。サイバー保険市場の成長や成熟に伴い、集積リスクを管理するための引受業務が発達しました。壊滅的なサイバーリスクをモデル化し定量化するための新しいアプローチは、累積損失につながる可能性のある要因や壊滅的なサイバーエクスポージャーを制限する要因についての一般的な理解と並行して進化しています。同様に、サイバーリスクの全体像を把握するのに役立つさまざまな情報源から、より多くの質の高いデータと見識を収集できるようになりました。これには、異なる脅威の実行者、その資金源、動機、および傾向に関する情報が含まれます。これらの情報は、攻撃の見込みだけでなく、複数の被害者の可能性や事件の深刻度も浮き彫りにすることができます。

図 1: 元受保険会社および再保険会社によるサイバーリスクモデルの利用(企業の割合)



内部または外部モデルを持つ元受保険会社および再保険会社 52 社に基づき、サイバー保険料で加重

出典:ジュネーブ協会、Gallagher Re のデータに基づく

初期の保険数理アプローチは異なりますが、多くの場合、3 つの主要なタイプのバリエーションと組合せになります。つまり、応用的な事故頻度・損傷度モデル、ネットワーク波及モデル、および専門家主導のシナリオ分析です。現在、多くの元受保険会社や再保険会社は、正式なモデルを使用してサイバーリスクの評価を行い、エクスポージャー管理の方向性を決定しています。元受保険会社は、内部モデルを持つ再保険会社よりも外部ベンダーに依存する傾向があります(図 1)。これには、複数の外部モデルからの洞察の比較が含まれますが、実際には異なるモデル設定がそれを困難にし、厳しいライセンス契約は法外に高い費用になる可能性があります。

しかし、サイバーモデルは未成熟のままであり、その結果は不安定で一貫性がない場合もあります。いくつかのシミュレーションでは、めったにない業界全体のサイバー事件が、一部の自然災害にほぼ匹敵する保険損失を生み出す可能性があることを示唆していますが、推定値は採用された仮定に大きく影響されます。より広範なサイバー関連の保険クレームを対象とする他の決定論的シナリオ分析も、はるかに大規模な壊滅的損失の可能性を示しており、元受保険会社や再保険会社は、多くの企業に無差別に影響を与えたり、主要なインターネットアーキテクチャーを破壊したりするマルウェア攻撃による大きな脅威に特に警戒しています(表 1)。

表 1: 壊滅的サイバーシナリオに関する元受保険会社および再保険会社のランキング

壊滅的サイバーシナリオ	シナリオの平均ランキング
サービス妨害や業務中断	
ワーム型マルウェアの流行	1
広範なランサムウェア攻撃	2
大量のデータ漏えい	
顧客やサプライヤーに広範な影響を及ぼす主要な組織や機関における機密情報(個人情報や暗号化されたパスワードなど)の流出	4
重要なインフラの障害	
産業用制御システムの監視制御システム(SCADA)ネットワークの脅迫	4
業界やセクターの重要な参加者に対するサイバー攻撃(たとえば病院、食品製造業者、および販売業者など)	5
主要な公益事業会社(電力や水道など)に対するサイバー攻撃	2
州および地方自治体のサービス侵害	5
セクターを超えた IT 障害	2

調査回答者によるランキングスコアの中央値を示す(1 は最高ランクのシナリオ) 。ジュネーブ協会会員のサイバー元受保険会社および再保険会社 11 社の調査結果に基づく

出典:ジュネーブ協会

このことは、あらゆる点から見て、ひとつまたは複数モデルのリスク指標を過信しすぎないように留意することを指摘するものです。また、サイバー集積モデルがリスク評価の情報提供に広く使用されているにもかかわらず、これまでのところ元受保険会社や再保険会社の引受および資本管理に部分的にしか統合されていない理由でもあります。

優れたモデルを超えて

リスクモデルの改善は必要ですが、リスク吸収資本を大幅に増やすには十分ではないでしょう。サイバーの不確実性は依然として残っており、認識できることや確実なモデル化が制約されているため、元受保険会社や再保険会社はより大きなサイバーリスクを引き受ける意欲が低下しています。したがって、保険契約者の将来の補償ニーズに対応できる、より大きく、持続可能なサイバー元受保険または再保険市場を育成するためには、他の制度的イノベーションが必要かもしれません。これには、次のような取組みが含まれます。

- 標準化された保険クレームデータの収集と、サイバーリスクとエクスポージャーに関する情報共有と知識交換。これには、進化する脅威や脆弱性について独自の洞察を持っている可能性のある政府セキュリティ機関や大手テクノロジー企業などの主要な利害関係者との協力の強化が含まれるでしょう。クラウドサービスプロバイダーと元受保険会社および再保険会社間の近年のパートナーシップの多くは、このような協力体制の潜在的なメリットを示しています。
- リスクキャリアの中でサイバーエクスポージャーをプールするとともに、投資家の需要により適合し、ピーク時のサイバーリスクのより大きな移転を可能にする革新的な手段により、サイバーリスクを資本市場に移転する仕組みの促進。最近は、サイバー保険リンク証券(ILS)市場が小さいながらも成熟してきており、投資家の関心が高まっています。
- IT 企業がサイバー攻撃に対してより堅固なハードウェアとソフトウェアを開発することを奨励するための、法的責任制度の強化。このような取組みは、米国の国家サイバーセキュリティ戦略の中核的な柱であり、サイバーリスクを軽減し、サイバーセキュリティの脆弱性を最も影響を受けやすい人々から遠ざけることを目的としています。

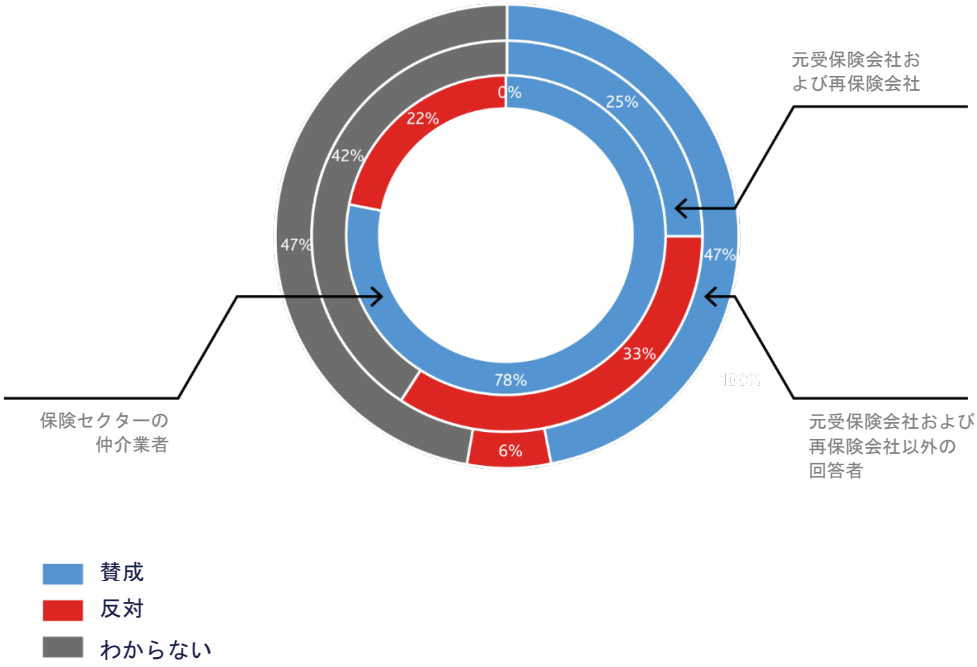
最終的には、重大なサイバー補償ギャップに対処するために、元受保険や再保険の極端な損失を防ぐための政府の資金調達も必要になる可能性があります。これにより、元受保険および再保険セクターは下振れ損失が限定されていることを認識できるため、より多くのサイバーエクスポージャーの引受を奨励し、支援することができます。最近行われた米国財務省のパブリック・コンサルテーション・エクササイズ(市民からの声を集める公開協議)に対する回答は、壊滅的なサイバー事件に対する連邦保険プログラムを一定程度支持するか、少なくともさらなる可能性を検討するべきことを、元受保険および再保険セクターの内外ともに支持しております。その一方で、保険会社を含む回答者のかなりの割合が、サイバーに対する官民保険の取り決めが現時点で適切であるとは確信していません(図 2)。

懐疑的な人々(および確信を持てない一部の人々)の間で共通するテーマは、政府の支援策が意図しない結果をもたらすかもしれない、という懸念です。これには、保険契約者がサイバーセキュリティに対して手薄になるだけでなく、保険会社が優れたサイバー衛生を促進し、革新的な保険ソリューションを開発するインセンティブを弱める可能性も含まれています。市場参加者の中には、政府の支援策が、現在無保険のものも含めて、保険会社がすべてのサイバー危機に対する補償を提供する義務を負うことになるのではないか、と懸念する者もいます。

しかし、納税者は最終的に、サイバーによる大災害で巨額の無保険損失の相当額を負担することが求められる可能性が高いため、大規模な事件の最中にその影響に対処するよりも、元受保険や再保険市場の機能を促進する措置に目を向けることが賢明であるように思われます。適切に設計され、調整され、そして実装されたサイバー対策は、政府が合意された基準を超える極端な損失に対してのみ責任を負うことを保証するとともに、サイバー保険の継続的な開発と導入を促進し社会のレジリエンスを高めるインセンティブを与えることができます。これには、政府が保証するための費用をカバーする保険料や、大規模なサイバー事件の後に税金で賄われた損失を取り戻すための手続きが含まれます。

図 2: サイバーリスクに関する米国連邦保険制度に対する業界の見解

壊滅的なサイバー事件に対する連邦保険の可能性は?



55 名の個人の回答に基づく。個別の組織を代表して提出された共同回答は、個別に集計。また、保険会社には元受保険会社や再保険者を代表する業界団体からの回答を含み、仲介業者はブローカー、格付け機関、およびモデル販売会社からの回答を指す

出典:米国財務省コンサルテーション・エクササイズに対する公表回答のジュネーブ協会分析