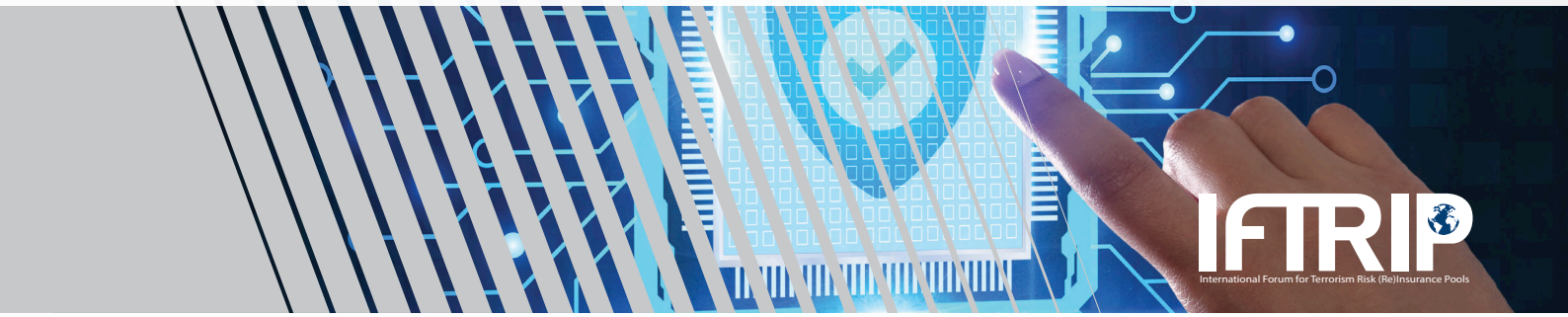
# 研究要旨

# 敵対的サイバー活動に対する保険:持続可能な解決策を探る

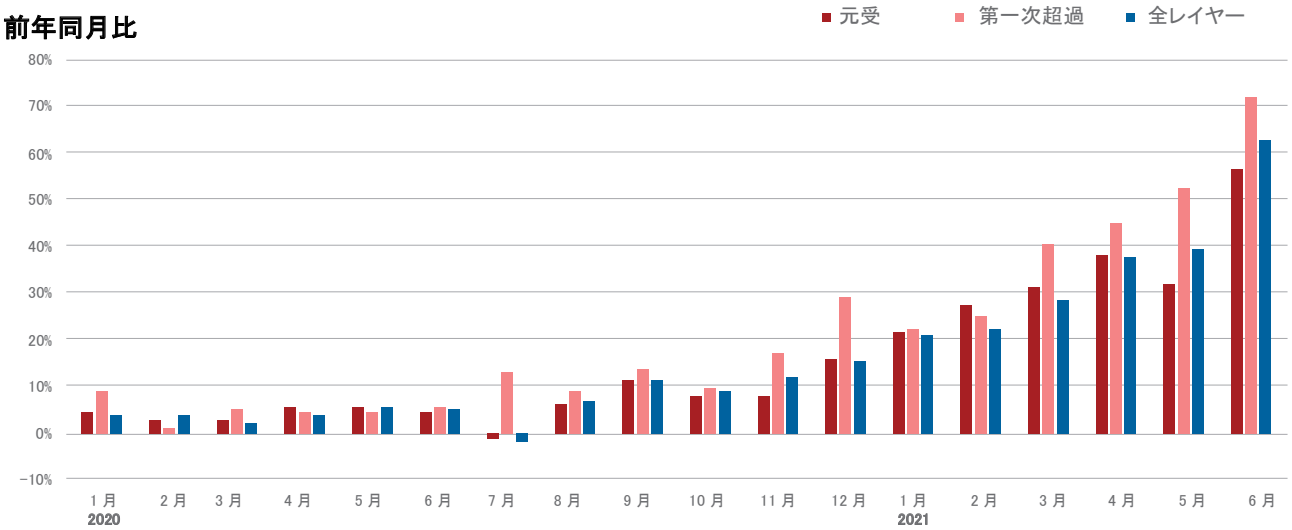



カーター・インシュランス・イノベーション マネージングディレクター **Rachel Anne Carter**
ジュネーブ協会 Cyber & Evolving Liability ディレクター **Darren Pain**
プール再保険CEO兼国際テロリスクフォーラム(再)保険プール(IFTRIP)事務局長 **Julian Enoizi**

サイバー環境は急速に進化しており、デジタル化によるさらなる脅威や脆弱性が増大しています。これは、コロナ危機によってもたらされた労働およびビジネス慣行の変化によって増幅されており、その一部はパンデミック後も続く可能性があります。特にランサムウェアやサプライチェーン攻撃は、パンデミック後にさらに増加しており、悪意のあるサイバーインシデントにより、大規模な経済的混乱が起きる可能性が広く認識されています。

サイバー保険の専門市場は、ファースト・パーティおよびサード・パーティ損失の両方をカバーするリスク分類の漸進的な拡大など、時間の経過とともに発展してきました。しかし、スタンドアローンサイバー保険の特化した積極的な補償などにより、近年は損失率が急激に増加しており、再保険および保険会社がサイバーリスクを再調整するようになりました。従来の損害保険(サイレント・サイバー)から意図しないサイバー・エクスポージャーを補償対象外とする取り組みと相まって、市場の再保険および保険の引受能力は低下しています。これにより、引き続き強い需要があるなかで、サイバー保険のコストの急激な再評価と条件の引き締めが行われました(図1)。

***図 1:契約更新月別、引受けレイヤー別のサイバー保険料率の上昇率の推移***




*米国などにおけるサイバー保険市場では、1000万ドルまたは1500万ドル以上の保障を希望する保険契約者は、通常レイヤー保険またはスタック保険に加入します。ファースト・レイヤー(または元受保険)は、保険設計全体の一般的な契約条件を定めます。超過保険は、必要に応じて追加限度額を設定します。元受保険会社は、限度額まで損失リスクの100パーセントを負担します。そして、第一次超過の保険会社は、そのレイヤーの100パーセントを負担します。*

*出典:エーオン1*

1　エーオン2021

## 敵対的サイバー活動(HCA)と保険

最近の深刻なサプライチェーンへの侵入やランサムウェアインシデントは、サイバー保険を提供する保険会社の長年にわたる問題を浮き彫りにしています。それらのサイバー攻撃の実行者が国家と結びついている場合、保険会社はどの程度の保障を提供できるのか、また提供すべきなのかという問題があります。従来の保険契約は戦争または戦争に準ずる事柄に対し免責条項を設けていますが、サイバー攻撃の動機が不明な場合は特に、国家が攻撃の背後にいる、あるいは少なくともハッカーを保護していると疑われる状況を適切に把握することができません。このような帰属と特性の問題は、保険会社にとって深刻な契約上の不確実性を生み出しており、このことが最近のサイバー保険市況の引き締めに拍車をかけています。

サイバーインシデント(現在広く使用されている定義よりも国家の関与の立証責任が低いHCA用語を含む)を詳細に分類することで、保険会社はより明確な情報やリスクに対する安心感を得ることができます。しかし、市場がサイバーインシデントにかかる保険の難しい約款文言を受け入れるには時間がかかり、たとえ受け入れたとしてもそれ以上進展しないことが考えられます。

最近のサイバーインシデントは、敵対的サイバー活動(HCA)に何が正当に該当し何が該当しないかについて、明確かつ決定的な境界を作ることの難しさを浮き彫りにしています。

国家の関与は多岐にわたり、洗練かつ使いやすいマルウェアを開発するための環境整備を含む暗黙の支援(例えば、コロニアル・パイプラインに対するダークサイドの攻撃)から、主権国家政府によるハッキングキャンペーンの監督やリソース提供(ソーラーウィンズの例)に至るまで様々です。このような状況では、敵対的サイバー活動(HCA)の直接的な帰属を明確にすることが困難な場合があります。特に、犯罪組織に関連する国家関係者が偽旗作戦を用いて痕跡を隠したり、他者を非難したり、あるいはその他の方法で攻撃の最終的な原因に関する国際的合意を妨げている場合はなおさらです。

## 依然として困難なサイバーリスクの定量化

サイバーリスクのモデル化や定量化の進歩、およびリスクを共有するための再保険の有用性やその他のしくみは、既存および将来の保険会社双方が、敵対的サイバー活動(HCA)やその他の悪意あるサイバー活動に対する保険適用範囲の拡大を推進するための鍵となります。例えば、ハリケーンなどの自然災害やテロ攻撃のような人為的災害の危険とは異なり、サイバーの危険には地理的境界がありません。全世界が一つのサイバー災害ゾーンになる可能性があります。
帰属と特性の問題を超えて、敵対的サイバー活動(HCA)の頻度や深刻さ、特に潜在する莫大な集積損害を評価することは、さらに重要な課題であり続けています。

*表 1:既存のサイバーリスク・シナリオ分析*

| シナリオ | 広範な影響 | 保険引受能力 | 損失見積りの不確実性 | 経済的損失の推計(10億米ドル) | 保険損害額の推計(10億米ドル) |
|---|---|---|---|---|---|
| **感染性の高いマルウェアが蔓延[2]** | 破壊的 | サイバー市場による保険対象/保険可能 | 高い | 193 | 27 |
| **大規模なクラウド停止[(1)]** | 破壊的 | サイバー市場による保険対象/保険可能 | 高い | 53 | 8 |
| **インフラの中断または障害(停電など)[(2)]** | 破滅的/破壊的 | サイバー市場やリスクの保険対象外/保険不可能 | 非常に高い | 1,024 | 71<br>(主に資産の非肯定的なリスクによって左右される) |

*注記:(1)技術的障害、分散型サービス妨害(DDoS)攻撃、およびマルウェア感染など使用できない原因は数多くあります。さらにこのシナリオでは、影響を受けるお客様が自身でサービスを復元できないことも考慮しています。[3](2)停電の原因としては、よく知られている物理的な危険(暴風雨や地震など)、人為的ミス、および悪意のある行為が考えられます。[4]*

*出典:ジュネーブ協会およびミュンヘン再保険*

2 ロイズおよびケンブリッジ大学2019
3 ロイズおよびサイエンス社2017
4 ロイズおよびケンブリッジ大学2015

決定論的シナリオ分析によると、クラウドサービスの一時的な中断などの悪意のあるサイバーインシデントは、歴史的な自然災害にほぼ匹敵する経済的損失を引き起こす可能性があります(表1)。しかし、ITや運用インフラの広範な機能停止や障害など、より極端で長期にわたるサイバー攻撃により、予想損失が大幅に増大する可能性があります。さらに、このような推計値の不確実性は非常に大きくなるため、潜在的損失の額がこれらの「推定値」を大幅に上回る可能性があり、再保険および保険会社のリスクの引き受け能力を超えてしまう可能性があります。これは、ハッカーの動機、戦略、脅威ベクトルに対する曖昧さ、および比較的小規模で孤立した攻撃が全面的なサイバー戦争へとエスカレートする可能性と同様に、敵対的サイバー活動(HCA)インシデントに当てはまり、サイバーリスクの定量化の複雑さを増幅しています。

## 政府による安全策の役割

企業や政府間の協力を含むサイバー脅威インテリジェンスの収集の進歩により、サイバーレジリエンスを構築するうえで重要な要素であるリスクの認識と対策が促進されます。このような情報により、保険会社は脆弱性を発見し、サイバーリスクのモデル化の改善を促進することができます。同様に、取り締まり当局による攻撃の実行犯の追跡や追及、および脅迫された資金の回収が進展することにより、サイバー犯罪者を抑止することができるため、保険会社が安心してリスクの引き受け能力の範囲内で保険を提供することができます。

ただし、一部のサイバーリスクの体系的な特徴、特に単一の事象または敵対的サイバー活動(HCA)に関連した複数の攻撃によって生じる損失の可能性は、集積損害の規模が民間の再保険部門および保険部門によって安全かつ合理的に許容できるレベルを最終的に超える可能性があることを意味します。
大規模で悪意のあるサイバー攻撃を受けた場合には、付随的な被害がしばしば発生し、意図していない標的も損失を被ります。近年の一連の攻撃もニアミスであったと言えますが、もし状況が異なっていた場合、損失はさらにひどくなっていたかもしれません。

したがって、パンデミック関連のリスクについての現在の議論を反映し、経済全体のレジリエンスを高めるためには、サイバーリスクの巨大損害に資金を提供するような政府支援の解決策を検討する必要があります。適切に設計された官民連携(PPP)は、保護能力を向上させ、サイバー市場の革新を促進して、敵対的サイバー活動(HCA)リスクの保障を拡大することができます。これは単なる財政的な解決策ではなく、保険会社との協力を通じて、適切な保険加入を含むサイバーセキュリティのベストプラクティスの採用を促進し、こうしたリスクに対する社会的脆弱性を軽減することを目指すべきです。

## 官民連携(PPP)の策定

このような政府支援ソリューションの策定は複雑です。官民連携(PPP)に関する重要な考慮事項には、スキームが強制か任意か、適用範囲がパラメトリックか補償ベースか、あるいはスキームが相互または連帯の原則に基づいているかが含まれます。また、財政的および実現可能性の観点から、スキームに資金を提供するために適切な措置が採用され、事象発生前または発生後に十分な資本を確保する必要があります。特定のスキームを採用する際にはトレードオフがあり、保険契約者、民間の再保険会社や保険会社、および政府の間でピーク損失をどの程度分担すべきかを調整することは困難です(表2)。

このような設計上の課題は、国際的に拡大しています。サイバーリスクの相互関連性やグローバル性を考えると、敵対的サイバー活動(HCA)リスクを保障するための国際的な協調的解決策が理想的な選択肢となるでしょう。しかし、法的な制約、文化の違い、資本へのアクセス、および各国政府が異なる法域でリスクを共有する意思があるかなどの点で、グローバルな解決には未だ至っておらず、少なくとも短期的には実行不可能でしょう。したがって、大規模なサイバーリスクに対する国内官民連携(PPP)ソリューションの策定を優先する必要があります。

保険業界は、サイバーテロ、敵対的サイバー活動(HCA)、およびサイバー戦争を理解し、そのようなリスクを保障するための評価において、長い道のりを歩んできました。保険会社は、保険引受能力を拡大するために、官民連携(PPP)を通じた政府とのリスク共有を含め、サイバーリスクを共有するための実行可能な選択肢を積極的に評価していく必要があります。保険会社と政府間のこのような協力的な取り組みにより、サイバー補償のギャップを埋め、サイバー空間の最大限の社会的利益を実現できるようになります。

***表 2:官民連携(PPP)スキーム特性の長所および短所の要約***

| スキーム特性 | 想定される長所および短所 |
|---|---|
| **複合危険**<br>(対単一危険) | ***長所:*** 多様化の機会<br>***短所:*** 高い管理コスト |
| **強制**<br>(対任意) | ***長所:*** 保険プールの拡大と逆選択の回避<br>***短所:*** 複雑なコンプライアンスの監視と適用 |
| **事前出資**<br>(対事後出資) | ***長所:*** リスクの予防や軽減の促進、および支払いの際の手元資金の確保<br>***短所:*** 不測の事態に備えるための政治的支援の困難さ |
| **パラメトリック**<br>(対補償ベース) | ***長所:*** 保険事故後の迅速かつ効率的な流動性の提供<br>***短所:***実際の発生損失と異なる可能性 |
| **連帯**<br>(対相互主義) | ***長所:*** 金銭的余裕がない人々に対するサイバー保険の強化<br>***短所:*** 多くの場合包括性と強制が必要 |
| **永続的**<br>(対一時的) | ***長所:*** 長期的な資金調達や資本蓄積戦略の策定<br>***短所:*** 潜在的な民間市場参加者の締め出しや将来のイノベーションの抑制 |

*出典:ジュネーブ協会*

## 参考資料


エーオン2021. *Cyber Insurance Snapshot. A Focused View of 2021 Risk and Insurance Challenges.*

ロイズおよびサイエンス社2017. *Counting the Cost.Cyber Exposure Decoded.*

ロイズおよびケンブリッジ大学2015. *Business Blackout.Insurance Implications of a Cyber Attack on the US Power Grid.*

ロイズおよびケンブリッジ大学2019. *Bashe Attack. Global Infection by Contagious Malware.*