国家の関与するサイバー攻撃と
サイバー保険の戦争免責条項について

主席研究員　濵田　和博

目　　次

８．　戦争リスクなどへの補償提供策

（1）国家によるバックストップ

（2）カタストロフ・サイバーリスク市場

（3）保険リンク証券（ILS）

９．　おわりに

要旨

近年、世界的にサイバー攻撃が多発、激化しているが、特に2022年2月のロシアによるウクライナ侵攻以降、「国家の関与によるサイバー攻撃」に対する懸念が広まっている。国家の関与によるサイバー攻撃に係るリスクは、一般的に広域に同時多発的に被害をもたらし、巨額の損害を発生させる可能性があり、個々の損害保険会社では、対応が困難なリスクの1つとなっている。

損害保険業界は、これまでサイバー保険のみならず、ソルベンシーに重大な影響を及ぼすリスクを補償対象から除外する対応の一環として、ほとんどすべての損害保険契約に戦争免責条項を付帯している。

2017年に世界的に大損害をもたらしたサイバー攻撃により、被害を受けた保険契約者が、戦争免責条項を根拠として保険金支払を拒絶した損害保険会社を提訴した事例が、米国で複数発生している。既に一部の裁判では、原告（保険契約者）の主張を認め、被告（保険会社）に保険金支払を命じた一審判決が出ている。

このような状況を踏まえ、ロイズ保険協会（LMA）などでは、「サイバー戦争免責条項」など新たな免責条項案を作成しているが、これらも課題が指摘されており、更なる改善が望まれる。

技術革新に伴い、サイバーリスクを巡る状況も常に「進化」していることから、わが国の損害保険業界も、最新のサイバーリスクの動向や、諸外国の保険業界の動向を注視しつつ、約款における戦争免責条項のあり方に関する検討など、適切な対策を採る必要がある。

１．はじめに

情報技術の進展により、個人生活や企業活動のあらゆる領域に、デジタル機器が普及し、それらに対する依存が強まるにつれ、サイバーリスクは拡大・増大している。また2020年以降、新型コロナウィルス感染症への対応として、企業のデジタル・トランスフォーメーション（DX）も、急速に進展しており、さらなるサイバーリスクの増大要因の1つとなっている。

これらの増大するサイバーリスクへの対応策として、サイバー保険への需要が高まっており、これを受けサイバー保険市場は、拡大を続けている。

一方で、欧米では2021年までランサムウェアなどによるサイバー攻撃の件数や被害額の増大に伴い、サイバー保険の保険金支払額が年々増加していることから、各保険会社は、引受キャパシティの制限や、保険料の引上げなど、サイバー保険の損害率改善に向けた各種対応を行っている。

また、サイバー保険に大きな損害をもたらし得る事象の1つとして、2022年2月のロシアによるウクライナ侵攻を機に、「国家の関与によるサイバー攻撃」[1]に関心が高まっている。ロシアとウクライナの紛争は、2014年のクリミア危機[2]の頃から、「武力を用いる軍事行動」[3]に、情報戦やサイバー攻撃を交えて敵を攻略する「ハイブリッド戦争[4]」と言われており、2017年に世界各国において、甚大な損害を発生させたサイバー攻撃も、当該紛争国が関与していると見られている。今回の侵攻以降、戦闘の激化・長期化により、サイバー攻撃の増加・拡大が懸念されている。

当研究所ではこれまで、2019年度上半期に欧米主要国におけるサイバー保険の関連動向について調査[5]し、さらに2021年1月、および2022年2月には損保総研レポートでその後の動向について取り上げた[6]。

本稿では、サイバー保険市場の概況を説明したのち、国家の関与によるサイバー攻撃、従来の戦争免責条項、戦争免責条項の適用を巡る訴訟事例、LMAのサイバー戦争免責条項およびロイズの指示、研究機関による提案、ならびに戦争リスクなどへの補償提供策について取り上げる。

なお、本稿における意見・考察は筆者の個人的見解であり、所属する組織を代表するものではないことをお断りしておく。

---

1 本稿では、英文における「state-backed」や「state-sponsored」を、「国家の関与による」と表記している。

2 ウクライナ南部のクリミア半島の帰属を巡って、ロシアとウクライナの間に生じた、2014年の政治危機を指す。この後、同半島は「クリミア共和国」としてウクライナから独立し、ロシアに編入された。

3 「kinetic military action」を本稿では、「武力を用いる軍事行動」と記載する。

4 イギリスに本部を置く、国際安全保障、サイバーセキュリティ等について分析を行うシンクタンクである国際戦略研究所（International Institute for Strategic Studies）が、2015年5月に公表したArmed Conflict Survey 2015の中で、ロシアがクリミアを併合した手法を「ハイブリッド戦争」と規定した。

5 損害保険事業総合研究所「欧米地域におけるサイバー保険関連動向」（2019.9）

6 林圭一「米国を中心とするサイバーインシデント・サイバー保険市場の動向」損保総研レポート第134号（損害保険事業総合研究所、2021.1）、牛窪賢一「米国を中心とするサイバー保険市場の動向」損保総研レポート第138号（損害保険事業総合研究所、2022.2）

２．サイバー保険市場の概況

本項では、サイバー保険市場の概況として、全世界における市場規模、元受保険業界の状況、および再保険会社等の対応について説明する。

（1）全世界における市場規模

世界全体のサイバー保険市場に関して正確な統計はないが、その市場規模は、ここ数年で大幅に拡大しており、今後もその傾向は継続すると見られている。例えば、ミュンヘン再保険によると、世界全体のサイバー保険の収入保険料は、2018 年には約 47 億ﾄﾞﾙであったが、3 年後の 2021 年には約 92 億ﾄﾞﾙとほぼ倍増し、さらに 2025 年までに約 221 億ﾄﾞﾙに達すると予測されている[7]。また、スイス再保険も、2022 年 11 月に公表した報告書[8]において、世界全体のサイバー保険の収入保険料の規模は、2025 年までに 2021 年比で 2.3 倍になるとの同様の予測を公表している（図表 1 参照）。

図表 1　世界全体のサイバー保険の収入保険料（実績と予測）

企業名	2018 年	2021 年	2025 年（予測）
ミュンヘン再保険	47 億ﾄﾞﾙ	92 億ﾄﾞﾙ	221 億ﾄﾞﾙ
スイス再保険	50 億ﾄﾞﾙ	100 億ﾄﾞﾙ	230 億ﾄﾞﾙ

（出典：Munich Re, “Munich Re Global Cyber Risk and Insurance Survey 2022”（2022.6）、Swiss Re Institute, “Cyber insurance: strengthening resilience for the digital transformation”（2022.11）をもとに作成）

（2）元受保険業界の状況

a. 損害率等の推移

損害率についても世界的な統計はないが、世界最大のサイバー保険市場である米国[9]では、全米保険監督官協会（National Association of Insurance Commissioners：以下「NAIC」）[10]が、同国内でサイバー保険を販売する保険会社から、同保険に係るデータを収集し、報告書[11]として公表しており、この中に損害率のデータも含まれている。これによると、サイバー保険を販売する保険会社のうち、収入保険料で上位 20 社[12]の平均損害率は、図表 2 のとおり 2020 年まで毎年悪化しているが、保険会社による保険料率の引上げ、リスクの選択、または引受条件の厳格化などの対策により、2021 年には

---

7 Munich Re, “Munich Re Global Cyber Risk and Insurance Survey 2022”（2022.6）

8 Swiss Re Institute, “Cyber insurance: strengthening resilience for the digital transformation”（2022.11）

9 IAIS, “Global Insurance Market Report”（2021.11）によると、世界全体のサイバー保険の引受保険料における米国のシェアは、53%である。なお、第 2 位のイギリスのシェアは 34%であり、両国で 87%のシェアを占めている。

10 NAIC は、米国において保険規制・監督を担う各州保険庁長官による意見交換や、各州間の統一的な政策の検討の機能を担う機関である。

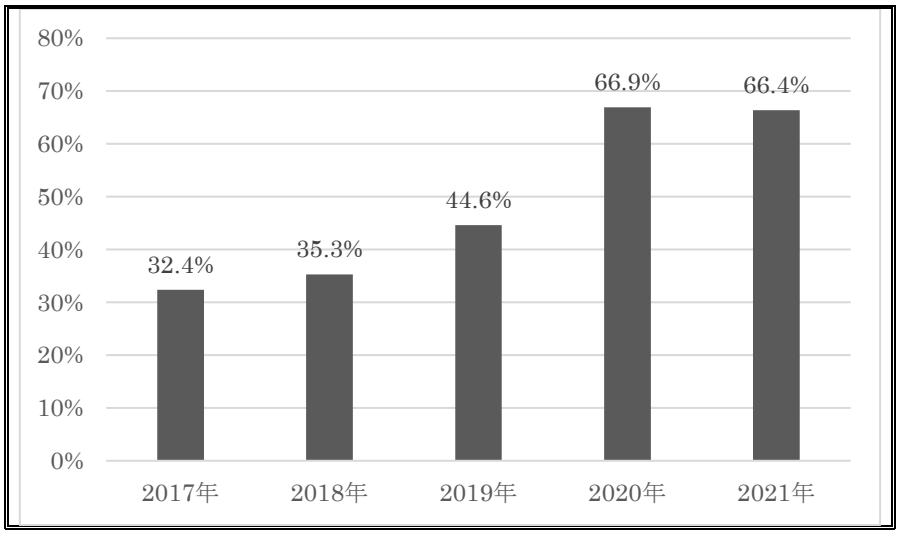
11 NAIC, “Report on the Cyber Insurance Market”（2022.10）

12 2021 年において、上位 20 社のサイバー保険の収入保険料は、全体の 83%を占める。

損害率の改善に至っている。

一方欧州では、サイバー保険の保険金請求件数が急増しているとの状況にはないが、過去に比して保険金請求件数は高水準にある。例えばアリアンツ傘下の企業向け保険会社である Allianz Global Corporate & Specialty（AGCS）によれば、2016 年におけるサイバー保険事故件数は 100 件弱であったが、2020 年および 2021 年は、各年とも約 1,000 件発生している[13]。

図表 2　米国のサイバー保険の損害率の推移



（出典：NAIC, “Report on the Cyber Insurance Market”（2022.10）をもとに作成）

b. 保険料率の引上げ状況

格付会社の S&P Global Ratings が、2022 年 7 月に公表した報告書によると、サイバー保険は、保険市場で急速に成長しているが、最近の保険料増加の大部分は、契約の数や大きさの成長ではなく、大幅な保険料率の上昇が原因であるとされている[14]。サイバーリスクへの需要は高まっているが、その一方で（再）保険会社の提供するキャパシティは、同様には増加していない状況にあり、結果として保険料率引上げにつながっている。

例えば、保険ブローカーのウイリス（WTW）は、2022 年 4 月の時点で、北米保険市場におけるサイバー保険の保険料率上昇は、企業向け保険の中で最も顕著であるとし、前年比 100%から 200%の保険料率上昇を予測している[15]。保険関連情報を提供している Business Insurance の 2022 年 10 月時点の記事によれば、米国のサイバー保険の

[13] AGCS, “We do not expect a major wave of claims: Russia's invasion of Ukraine: Potential impact for insurance and claims”（2022.5）
[14] S&P Global Ratings, “Cyber Risk in a New Era: The Rocky Road To A Mature Cyber Insurance Market”（2022.7）
[15] WTW, “Insurance Marketplace Realities 2022 Spring Update”（2022.4）

料率の上昇は、2021 年に比べると鈍化しているものの、依然として継続しているとのことである[16]。

また、保険ブローカーのマーシュ（Marsh）は、2022 年 6 月に公表した報告書の中で、ロンドン市場を通じて保険を契約する顧客の 90%以上が、2021 年の第 1 四半期以降、サイバー保険の料率上昇を経験し、第 4 四半期までには、その割合が 98%に達しているとしている[17]。サイバー保険の保険料の平均金額は、2021 年の第 1 四半期に前年同期比 28%の上昇であったが、第 4 四半期には同 109%上昇にまで拡大しており、中には保険料が 3 倍以上となった保険契約者もいるとのことである。

（3）再保険会社等の対応

主な再保険会社、および再保険ブローカーの、サイバーリスク、ならびにサイバー保険市場に対する課題認識・見通し・引受スタンスは、図表 3 のとおりである。ほとんどの再保険会社等が、サイバー保険市場の成長性を認めているものの、一方で精緻なリスクモデルが開発されておらず、集積額の把握が困難であることから、キャパシティの拡大には躊躇している状況が窺える。

図表 3　主要再保険会社等の課題認識・見通し・引受スタンス

名称	概要
ミュンヘン再保険	○サイバー保険の再保険市場は安定しているが、リスクを評価するためのより洗練された引受ツールが開発されるまで、大幅に成長する可能性は低い。 ○サイバー保険の再保険料率の水準を維持することを計画しているが、エクスポージャーを測定するためのより優れたコンピュータモデルが必要である。 ○2021 年のサイバー保険の収入保険料はおよそ 14 億ﾄﾞﾙであり、約 14%の市場シェアを占めている。 ○ミュンヘン再保険のコンバインドレシオは約 85%であり、特に欧州は収益性が高い。
スイス再保険	○今後サイバーリスクに関してより多くのデータが利用可能になるまで(注)は、当該リスクの保有を抑えるが、長期的には、自社の主要な事業部門になることを確信している。 ○一方で、システミックリスクが懸念事項として挙げられる。 ○サイバーリスクについて、再保険業界は世界中の政府と連携して、社会により広い範囲で補償を提供できるようにする必要がある。 ○サイバー保険は、歴史が浅いため、データが不足しており、またリスクに係る不確実性レベルが高いため、サイバー保険の成長についてのタイムフレームは提供できない。 ○サイバー保険の元受・再保険全体における市場シェアは、約 6%である。
ハノーバー再保険	○サイバー保険料の収入保険料は、約 5 億 5,000 万ﾄﾞﾙであるが、今後大幅に増加させる考えはない。
SCOR	○サイバー保険の収入保険料は約 2 億ﾄﾞﾙで、収入保険料総額 90 億ﾄﾞﾙに比して、小さな割合である。 ○引受額が増加していないのは、急速に進化するサイバーリスクについて、PML や集積額について確信が持てないことが主な理由である。

[16] Gavin Souter, “Cyber insurance pricing comes off COVID era highs”（Business Insurance, 2022.10）

[17] Marsh, “UK cyber insurance trends 2021”（2022.6）

名称	概要
Gallagher Re	○サイバー再保険市場は急速に拡大しており、2037 年頃までに、グローバルなキャット再保険（property catastrophe reinsurance）市場の規模を超えると予想している。 ○2023 年からは、サイバー保険料の増加、および損害率の低下により、収益性向上を予測している。

（注）スイス再保険は、サイバー保険について、事業部門としては約 5 年間の実績しかないとしている。

（出典：Gavin Souter, “Reinsurers cautious over cyber liability exposures”（2022.9）、Reinsurance news, “Cyber to become a prominent line for Swiss Re in future”（2022.9）、Reinsurance news, “Swiss Re would love to develop cyber ILS market: Group CUO Léger”（2022.9）ほか各種資料をもとに作成）

3．国家の関与によるサイバー攻撃

本項では、近年重大な損害をもたらすサイバーリスクとして懸念が高まっている、国家が関与していると見られる、過去のサイバー攻撃の事例、およびロシアのウクライナ侵攻による影響について、説明する。

（1）過去のサイバー攻撃の事例

国家が関与していると見られるサイバー攻撃は、近年日常的に頻発している。国家の関与によるサイバー攻撃には、例えば以下①から③のように、様々な態様があり、ある程度の（IT）資源を持つほぼすべての国家がサイバー攻撃を行っているとの見方もある[18]。

① 最高指導者による承認と国家による直接指揮がある場合
② 国家が「代理人（proxy）」に財政的・技術的支援を行い、攻撃を奨励する場合
③ 国家が「代理人」による攻撃を看過する場合（消極的関与）

世界的に重大な影響を与えたサイバー攻撃の事例は、図表 4 のとおりである。

図表 4　国家が関与していると見られる主なサイバー攻撃の事例

名称	時期	関与した国家（注 1）	攻撃・被害の概要
WannaCry	2017 年 5 月	ロシア	○Microsoft Windows を標的としたランサムウェアである。 ○大規模なサイバー攻撃により、150 カ国の 23 万台以上のコンピュータを感染させた。 ○身代金として暗号資産ビットコインを要求した。

[18] 川口貴久「国家によるサイバー攻撃からのセキュリティ」（シノドス、2020.3）

名称	時期	関与した国家（注1）	攻撃・被害の概要
NotPetya（注2）	2017年6月	ロシア	○世界全体で、事業中断損害も含め約100億ﾄﾞﾙの損害をもたらしたと言われている。 ○ネットワーク上で急速に拡散し、ハードディスクそのものをすべて暗号化し、使用不能の状態にした。 ○発生した被害を元に戻す方法はなく、基本的にファイルは完全に消し去られ、回復が困難であった。
APT40（注3）	2021年7月	中国	○「APT40」と呼ばれるサイバー脅威主体が、サイバー空間の安全等を脅かしているとして、米英政府などが非難する声明を発表した。 ○APT40は、世界的規模で、知的財産および営業機密の窃取を目的としたサイバー攻撃に関与したとされている。
Maui ransomware	2021年5月	北朝鮮	○医療および公衆衛生部門の組織を標的として攻撃した。

（注１）いずれの事案も、攻撃主体とされた国家は、各事案への関与を否定している。

（注２）2016年に初めて確認されたランサムウェアである「Petya」に類似しているものの、暗号化の方法など異なる点があるため、ロシアのコンピュータセキュリティ企業であるカスペルスキーが「NotPetya」と命名した。なお「Petya」は、1995年公開の映画「007／ゴールデンアイ」に登場するソ連の兵器衛星の名称に由来する。

（注３）APT（Advanced Persistent Threat）は、「特定の相手に狙いを定め、その相手に適合した方法・手段を適宜用いて侵入・潜伏し、数カ月から数年にわたって継続するサイバー攻撃」を指し、世界のセキュリティ業界では、組織名不明の攻撃主体を発見すると、ロシアの APT29、北朝鮮のAPT38のように「APT＋数字」で名称を付けている。

（出典：各種資料をもとに作成）

（2）ロシアによるウクライナ侵攻の影響

欧州連合サイバーセキュリティ機関（EU Agency for Cybersecurity：以下「ENISA」）は、2022年10月公表の報告書[19]の中で、2022年7月までの1年間における、サイバーリスクの主な傾向の1つとして「地政学的影響」[20]を挙げており、その主な内容は、以下のとおりロシアのウクライナ侵攻によるものである。

○ ロシアとウクライナの間の紛争により、ハクティビスト（hacktivist）[21]の活動の大幅な増加、サイバー攻撃者の、武力を用いる軍事行動との連携による作戦の実行、および国家による援助、などがサイバーリスクにおける変化として見られる。

○ 破壊的な攻撃は、国家によるサイバー攻撃の重要な構成要素となっており、ロシアとウクライナの紛争中、サイバー攻撃者が武力を用いる軍事行動に合わせて作

[19] ENISA, “ENISA Threat Landscape 2022”（2022.10）

[20] 地政学は、国の特性や政策を地理的な要素から研究する学問を指す。

[21] サイバー犯罪に関する用語で、社会的・政治的な主張を目的としたハッキング行為や、その傾向をハクティビズム（hacktivism）と言い、その活動家はハクティビスト（hacktivist）と呼ばれる。

戦を実行していることが確認されている。

○　特に 2022 年 2 月、ロシアのウクライナ侵攻以降、新たなハクティビズムの存在が観測されている。

○　偽情報（disinformation）は、サイバー戦争における使用手段の 1 つとなっており、「物理的な」戦争が始まる前から、ロシアのウクライナ侵攻の準備活動として利用されている。

保険業界では、ロイズ（Lloyd's of London）も 2022 年 6 月に、国家が関与し、地政学的に動機付けられたサイバー攻撃のリスクが高まっていると警告している[22]。

また、マーシュは、2022 年 4 月に公表した報告書の中で、多くの保険会社が当該侵攻を機にサイバー保険の契約条件を厳格化したとしている[23]。Aviva は 2022 年 4 月に、ウクライナ侵攻に伴い、サイバー攻撃が増加することを考慮して、中小企業に対し、サイバーセキュリティを強化するよう促すとともに、リスク管理のためのガイドブック[24]を提供している[25]。

４．従来の戦争免責条項

サイバー攻撃による損害に係る保険金請求に対して、一部の保険会社が、「戦争免責条項」を根拠として保険金支払を拒絶した事案が発生している。

そもそも「免責条項」とは、保険料を算定して保険制度として運営するために、保険金支払義務の範囲を定めるうえで、特定の事由を除外する規定である[26]。戦争による損害は、多くの業種・保険契約にまたがり、全体として巨額となる可能性が高く、また保険料率算定も困難である。こうしたことから、戦争関連のリスクは、一般的に保険契約普通保険約款、または特約により、補償の対象範囲から除外されている。戦争リスクに対する補償を得るためには、必要に応じて復活担保する特約条項、または別の保険契約が必要となる[27]。

イギリス勅許保険協会（Chartered Insurance Institute）[28]によると、ロイズにおけるノンマリン分野における戦争免責の多くは、1930 年代のスペイン内戦に対応して作成さ

---

[22] Lloyd's, "Shifting powers: physical cyber risk in a changing geopolitical landscape"（2022.6）
[23] Marsh, "Global Insurance Market Index 2022"（2022）
[24] Aviva, "Cyber Threats in 2022: Managing the risks to your business"（2022.3）
[25] Aviva, "Helping businesses manage their cyber risk"（2022.4）
[26] 中出哲「保険契約における免責条項の意義 −海上保険を題材とする問題提起−」保険学雑誌 654 号（日本保険学会、2021.9）
[27] 船舶、貨物、航空などの各保険では、戦争リスクの補償が提供される場合がある。後記 8.（2）を参照願う。
[28] イギリス勅許保険協会は、自らを「保険およびファイナンシャルプランニングの専門家に対する社会の信頼の構築に注力する専門家団体」としており、保険募集人などの能力向上や資格認定などの役割を担っている。

れた NMA464（War and Civil War Exclusion Clause）[29]に由来している[30]（図表 5 参照）。また現在ロイズには、数多くのバリエーションの戦争免責条項が存在している。

図表 5　War and Civil War Exclusion Clause（NMA464）

原文	日本語仮訳
Notwithstanding anything to the contrary contained herein this Certificate does not cover Loss or Damage directly or indirectly occasioned by, happening through or in consequence of war, invasion, acts of foreign enemies, hostilities (whether war be declared or not), civil war, rebellion, revolution, insurrection, military or usurped power or confiscation or nationalisation or requisition or destruction of or damage to property by or under the order of any government or public or local authority.	別段の定めにかかわらず、本保険証明書は、戦争、侵略、外国の敵の行為、敵対行為（宣戦布告の有無は問わない）、内戦、反乱、革命、暴動、軍事力または権力の奪取、没収、国有化、または政府、公的機関、地方自治体による、またはその命令による財産の徴用、破壊、または損害によって直接的または間接的に引き起こされた損失または損害を補償しない。

（出典：LMA NMA464 をもとに作成）

５．戦争免責条項の適用を巡る訴訟事例

本項では、国家の関与が疑われるサイバー攻撃により発生した被害に係る保険金請求に対し、損害保険会社が、戦争免責条項を根拠として保険金支払を拒絶し、訴訟となった事例として、「Merck 対 Ace American など」、および「Mondelez International 対 Zurich Insurance」について紹介する。

（1）Merck 対 Ace American など

本訴訟の原告である、米国ニュージャージー州に本社を置く製薬会社 Merck & Co（以下「原告」）[31]は、2017 年に、サイバー攻撃により、自社が世界各国で使用していた 4 万台以上の社内のコンピュータ、および 7,500 台のサーバーがマルウェア（NotPetya）に感染し、14 億ﾄﾞﾙ以上の損害を受けた。

原告は、Ace American など[32]（以下「被告保険会社」）との間でてん補限度額 17 億 5,000 万ﾄﾞﾙのオールリスクの財産保険[33]を契約しており、この財産保険は、コンピュータのデータ、およびソフトウェアの破壊・破損に起因する損害を補償対象としていた。

---

[29] LMA の作成するモデル条項の番号は、2003 年以降は LMA（例：LMA5564）を、それより前は NMA を冠している。なお、NMA は、Lloyd's Underwriters' Non-Marine Association の略である。

[30] Mirza Salam Ahmed & Ben Dyson, "Cyber insurers wrestle with war exclusions as state-sponsored attack fears grow"（S&P Global Market Intelligence, 2020.1）

[31] Merck & Co は、北米においてのみ Merck を名乗り、日本を含むその他の地域では MSD（Merck Sharp and Dohme）の名で事業を行っており、世界的に Merck の名称を使用しているドイツの Merck KGaA とは別企業である。これは、第一次世界大戦中に、米国政府が、独 Merck を敵対企業として、その米国拠点を接収した後に、接収された事業が米国内で個別に事業を継続したことによるものである。なお Merck KGaA は、北米においてのみ EMD（Emanuel Merck, Darmstadt）の名称で事業を行っている。

[32] 保険契約の内容の詳細は不明であるが、訴訟では Ace American ほか、アリアンツなどの保険会社 30 社が被告となっている。

[33] 本訴訟では、複数の保険契約が対象となっている。

当該保険契約の存在や、その補償内容ではなく、「当該サイバー攻撃が、ロシア政府によるものかどうか」が主な争点であった。原告は、「正式な国家による行為ではなく、むしろランサムウェアの一種である」と主張し、戦争免責条項は適用されないとして、保険金の支払を求めた。一方、被告保険会社は、「被害をもたらしたマルウェアは、ロシア政府がウクライナに対して用いた敵対行為手段の 1 つである」ので、当該保険契約中の「敵対的／戦争的行為免責（Hostile／Warlike Action Exclusion）条項[34]」（図表 6 参照）が適用されるとして、免責を主張した。

2022 年 1 月、ニュージャージー州高等裁判所（Superior Court of New Jersey）[35]は、原告保険契約者が、契約時にサイバー攻撃に対して、戦争免責条項が適用されるとは想定していなかったとして、被告保険会社に、約 14 億ﾄﾞﾙの保険金支払を命じた（図表 7 参照）。なお判決では、中心的な争点であった「当該サイバー攻撃が、ロシア政府によるものかどうか」については、一切論じられなかった。

なお、この判決において「サイバー攻撃は、「伝統的な（traditional）」敵対的行為を伴わない」としたことに対しては、「「伝統的」という言葉は、当該免責条項には明示的に使用されていない」との指摘がある。また、今回裁判所が言及した過去の判例が、比較的古い[36]ものであるため、「それらの判決が出された時点では、サイバー攻撃は想定されていなかった」との批判もある[37]。被告保険会社は、この判決を不服として上訴している。

[34] 判決文によると、ほとんどの保険契約において、ほぼ同様の記載であるとのことである。
[35] ニュージャージー州高等裁判所は、一審管轄部門（trial court）と中間上訴審管轄部門（intermediate appellate court）を有している。なお終審は、州の最高裁判所である「Supreme Court of New Jersey」が担っている。
[36] 例えば、戦争免責条項における「戦争」に「軍隊の使用が含まれる」とした判例として、1953 年の判決（Stanbery 対 Aetna）が挙げられている。
[37] Carter Perry Bailey, “It’s War – But not as we know it?”（2022.5）

図表 6　Merck の保険契約における敵対的／戦争的行為免責条項の規定（抜粋）

原文	日本語仮訳
A. 1) Loss or damage caused by hostile or warlike action in time of peace or war, including action in hindering, combating, or defending against an actual, impending, or expected attack: a) by any government or sovereign power (de jure or de facto) or by any authority maintaining or using military, naval or air forces; b) or by military, naval, or air forces; c) or by an agent of such government, power, authority or forces; This policy does not insure against loss or damage caused by or resulting from Exclusions A., B., or C., regardless of any other cause or event contributing concurrently or in any other sequence to the loss.	A. 1）以下の主体による、実際の、差し迫った、または予想される攻撃を妨害、戦闘、または防御するための行動を含む、平時または戦争時の敵対的または戦闘的な行為によって引き起こされた損失または損害 a）政府もしくは主権（法律上または事実上）、または陸軍、海軍、もしくは空軍を保持、使用する当局 b）陸軍、海軍、または空軍 c）そのような政府、権力、当局、または軍隊の職員 この保険契約は、免責条項 A、B、または C によって引き起こされた、またはそれらに起因する損失または損害に対して、同時または他の順序で損失に寄与する他の原因またはイベントに関係なく、補償しない。

（出典：ニュージャージー州高等裁判所による「Merck 対 Ace American など」に対する判決文をもとに作成）

図表 7　「Merck 対 Ace American」の裁判の概要

項目	内容
判決が根拠とした判例法の考え方	○曖昧な約款文言や表現については、被保険者の合理的な期待を反映するように、保険契約を解釈する。 ○オールリスク保険は、通常想定されないリスクに適用される特別なタイプの保険であり、保険契約に損害補償を明示的に免責とする規定がない場合、少なくとも被保険者の詐欺やその他の故意の違法行為がない限り、当該保険による補償が一般的に認められる。 ○保険契約の文言に、疑い、不確実性、もしくは曖昧さがある場合、または文言に 2 つの解釈が可能な場合、「補償」に有利な解釈を採用しなければならない。 ○「戦争」は、「軍隊の使用を伴う」と理解するのが合理的である。
判決内容	○適用可能な判例法に照らし、免責条項の文言の平易な意味を考えると、免責条項が適用されないと判断する。 ○戦争免責条項を、このようなサイバー攻撃の事例に適用することを認めた判例は、過去にない。 ○保険契約の両当事者が、国家の関与によるサイバー攻撃が一般的になっていることを認識している状況で、被告保険会社は、サイバー攻撃を免責とする意図を予め被保険者に伝えることができたにもかかわらず、免責条項を変更せず、同じ文言を使用していた。 ○保険契約の文言を変更しなかったことから、「当該免責事項は、伝統的な戦争形態（traditional forms of warfare）のみに適用される」と期待する権利を原告は有する。 ○今回発生した損害を免責とするには、サイバー攻撃を免責する旨を明記した特約条項への変更が必要である。

（出典：ニュージャージー州高等裁判所による「Merck 対 Ace American など」に対する判決文をもとに作成）

（2）Mondelez International 対 Zurich American

米国イリノイ州に本社を置く食品・飲料会社 Mondelez International（以下「原告」）[38]もまた、Merck と同様に、2017 年に NotPetya によるサイバー攻撃を受け、1 億 8,800 万ドルの損害を受けた。同社は、オールリスクの財産保険を契約していた Zurich American（以下「被告保険会社」）から、「敵対的／戦争的行為免責（Hostile／Warlike Action Exclusion）条項」[39]を根拠に保険金支払を拒絶されたため、保険金支払を求め、2018 年 10 月にイリノイ州クック郡巡回裁判所（Circuit Court of Cook County）[40]に提訴した。

本裁判においても前記 Merck の事案と同様に、「NotPetya を使用したサイバー攻撃がロシアによるものであるかどうか」が争点となった。これに関し原告は、「被告保険会社は、技術的な証拠を提供していない」と主張したのに対し、被告保険会社は、「NotPetya は、免責条項に定める、「敵対的または戦闘的な行為」に該当すると主張した[41]。

この裁判は、Merck の事案に続き、サイバー保険への「戦争免責条項」適用の可否を巡る裁判として注目を集めたが、2022 年 10 月 27 日の最終弁論（closing arguments）直前に、原告・被告双方から訴訟の取下げの申立て（motion）が行われ、判決を迎えることなく終了した[42]。両社は、この申立てに関する経緯等を公表していないが、裁判外の和解により解決したと考えられる[43]。

６．LMA のサイバー戦争免責条項およびロイズの指示

前項記載の、2017 年の NotPetya によるランサムウェア攻撃を巡る、企業と保険会社との間の法廷闘争を主な契機として、保険業界において、「国家の支援によるサイバー攻撃による損害を明確に免責とする規定」の検討が開始されている[44]。本項では、LMA の作成したサイバー戦争免責条項、同条項への反応、および同条項と関連したロイズの指示について説明する。

---

[38] Mondelez は、ネスレ、ペプシコに続く世界第 3 位の食品・飲料会社であり、傘下にナビスコやキャドバリーなど著名なブランドを有する。

[39] Brian Corcoran, “What Mondelez v. Zurich May Reveal About Cyber Insurance in the Age of Digital Conflict”（Lawfare, 2019.3）によると、当該免責条項は、Merck の保険契約の「敵対的／戦争的行為免責条項」とほぼ同内容のようである。

[40] 巡回裁判所は、イギリスや米国などに存在する裁判所の一種で、かつて裁判所が未整備な時代に、判事が各地を巡回して法廷を開いたことから名付けられた。イリノイ州では、巡回裁判所が第一審管轄裁判所となっている。

[41] Tom Davis, “Insurers Pitch Stand-Alone Cyber Policies as ‘War Exclusion’ Faces Uncertain Future”（2022.4）

[42] Lauraann Wood, “Mondelez, Zurich Settle NotPetya Dispute Before Trial Close”（2022.10）

[43] 裁判の費用は、双方がそれぞれの支出分を負担するとのことである。

[44] Mirza Salam Ahmed & Ben Dyson, “Cyber insurers wrestle with war exclusions as state-sponsored attack fears grow”（S&P Global Market Intelligence, 2020.1）

（1）LMA のサイバー戦争免責条項

ロイズ市場協会（Lloyd's Market Association：以下「LMA」）[45]は、2 年以上にわたり同協会内の Cyber Business Panel において検討を重ね、2021 年 11 月に、単独型[46]サイバー保険向けの、4 種[47]の「戦争、サイバー戦争[48]、およびサイバーオペレーション免責（War, Cyber War and Cyber Operation Exclusion）条項：以下「サイバー戦争免責条項」）を公表した。

この免責条項における主な新たな試みは、サイバー保険に「サイバーオペレーション（Cyber Operation）」の概念を導入していること、責任帰属（attribution）[49]を決定するためのプロセスを設定していること、サイバー攻撃の対象となる「必要不可欠なサービス」の範囲を部分的にでも明確にしていること、および集積リスクを事実上軽減する構造を設定していることである[50]。

この免責条項の中で新たに使用された文言である「サイバーオペレーション（Cyber Operation）」は、「国家による、または国家のためにコンピュータシステムを使用し、他国の、または他国内のコンピュータシステム上の情報を混乱（disrupt）、拒否（deny）、劣化（degrade）、操作（manipulate）、または破壊（destroy）すること」と定義されており、物理的な武力を用いる「戦争（war）」[51]と区別されている。

4 つの免責条項とも、①免責の規定、②サイバーオペレーションの責任帰属に関する規定、③用語の定義、の 3 つのパートで構成されている。

また、「この免責条項が適用されることの証明責任を保険会社が負っていること」も全免責条項に共通して記載されている。

---

[45] LMA は、シンジケートのマネージング・エージェントなどで構成された団体であり、ロイズ市場参加者のため専門的で技術的な支援を提供している。なお、マネージング・エージェントは、1 つ以上のシンジケートの管理業務を担う企業であり、引受業務などシンジケートの業務全般に管理責任を負っている。

[46] サイバー保険には、単独型サイバー保険と、財産保険や賠償責任保険など従来型の保険にサイバーリスクの補償を付帯した特約型サイバー保険がある。

[47] LMA5564、LMA5565、LMA5566、および LMA5567 を指し、それぞれ No. 1 から No. 4 の番号が振られている。

[48] 「サイバー戦争（Cyber War）」という文言は、モデル条項のタイトルにしか用いられておらず、4 種のモデル条項の本文には一切出てこない。また免責条項中の「用語の定義」の項においても、「戦争」と「サイバーオペレーション」のみが説明されており、「サイバー戦争」については、定義していない。

[49]責任帰属とは、「攻撃に係る因果関係を明らかにすること」や、「攻撃者を特定すること」を指し、国家が関与するサイバー攻撃であれば、「責任ある政府・組織まで遡ること」を意味する。なお、サイバー犯罪の分野において、「attribution」は、単に「帰属」、または「特定」などとも訳されるが、本稿では「責任帰属」との和訳を使用する。

[50] Vincent J. Vitkowsky, "The New LMA War, Cyber War and Cyber Operation Exclusions for Cyber Insurance Policies"（HB Litigation Conferences, 2021.12）

[51] このサイバー戦争免責モデル条項の中で「戦争（war）」は、宣戦布告の有無にかかわらず、①国家による他国に対する物理的武力の行使、または内戦、反乱、革命、暴動の一部、および／または、②政府、公的機関、または地方公共団体による、またはその命令に基づく、軍事力、権力の奪取、没収、国有化、徴用、財産の破壊、または損害と定義されている。

a. 免責条項の規定内容について

LMA の各免責条項の、主要な規定は図表 8 のとおりである。

LMA5564（No. 1）は、4 つの免責条項の中では、免責の対象範囲が最も広く（補償の対象範囲が狭く）、すべてのサイバーオペレーションを免責の対象としている。

LMA5566（No. 3）は、①戦争の過程で行われたサイバーオペレーション、②特定の国家間におけるサイバーオペレーション、および③国の必要不可欠なサービスの提供など安全保障に重大な悪影響を及ぼすサイバーオペレーション、の 3 つの場合に免責の対象範囲を限定している。

LMA5565（No. 2）の免責対象の範囲は、LMA5566（No. 3）と全く同じであるが、保険金支払の対象となる（上記①、②、③以外）のサイバーオペレーションについては、個別に 1 事故および期間中の支払限度額を設定できる方式となっており、LMA5566（No. 3）より保険会社の引受リスクを狭める方式となっている。

LMA5567（No. 4）の免責対象の範囲は、基本的には LMA5566（No. 3）と同様であるが、「バイスタンディング・サイバー資産[52]」を補償対象に含めているため、4 つの免責条項の中では、免責の対象範囲が最も狭く（補償の対象範囲が広く）なっている。

図表 8　LMA のサイバー戦争免責条項（注１）

	原文	日本語仮訳
No. 1: LMA 5564	1. Notwithstanding any provision to the contrary in this insurance, this insurance does not cover any loss, damage, liability, cost or expense of any kind (together “loss”) directly or indirectly occasioned by, happening through or in consequence of war or a cyber operation.	1. 本保険の別段の定めにかかわらず、本保険は、戦争またはサイバーオペレーションに直接または間接的に引き起こされた、あらゆる種類の損失、損害、賠償責任、費用（以下「損失」と総称する）を補償しない。
	2. The insurer shall have the burden of proving that this exclusion applies.	2. 保険会社は、この免責条項が適用されることの立証責任を負うものとする。

[52] バイスタンディング・サイバー資産（bystanding cyber asset）とは、被保険者またはサービス・プロバイダーが使用するコンピュータシステムのうち、物理的に「影響を受けた国」に所在していないが、サイバーオペレーションにより影響を受けたものを指す。

	原文	日本語仮訳
No. 3: LMA 5566	1. Notwithstanding any provision to the contrary in this insurance, this insurance does not cover any loss, damage, liability, cost or expense of any kind (together "loss") directly or indirectly occasioned by, happening through or in consequence of: 1.1. war or a cyber operation that is carried out in the course of war; and／or 1.2. retaliatory cyber operations between any specified states; and ／or 1.3. a cyber operation that has a major detrimental impact on: 1.3.1. the functioning of a state due to the direct or indirect effect of the cyber operation on the availability, integrity or delivery of an essential service in that state; and／or 1.3.2. the security or defence of a state. 2. （No. 1: LMA5564 第 2 条に同じ）	1. 本保険の別段の定めにかかわらず、本保険は、以下の事由により直接または間接的に引き起こされたあらゆる種類の損失、損害、賠償責任、費用（以下「損失」と総称する）を補償しない。 1.1. 戦争または戦争の過程で行われたサイバーオペレーション、および／または 1.2. 特定の国（注2）間の報復的なサイバーオペレーション、および／または 1.3. 以下に記載の内容に、重大な悪影響を及ぼすサイバーオペレーション 1.3.1. 国内の必要不可欠なサービスの可用性、完全性、または提供に対するサイバーオペレーションの、直接的または間接的影響による、国家の機能、および／または 1.3.2. 国の安全保障、または防衛
No. 2: LMA 5565	1. （No. 3: LMA5566 第 1 条に同じ） 2. （No. 1: LMA5564 第 2 条に同じ） 3. Subject to the exclusions above and the other terms, conditions and exclusions contained in this insurance, the following limits shall apply to any other cyber operation(s): 3.1. {response} for any cover in relation to all loss arising out of one cyber operation; 3.2. {response} in the aggregate for the period of insurance. These limits shall apply within the full policy limit and not in addition thereto. Unless an amount is specified in 3.1 and 3.2, there shall be no coverage for any cyber operation(s).	3. 上記の免責条項、ならびに本保険に含まれるその他の条項、および免責事項に従い、以下の補償限度額が、その他のサイバーオペレーションに適用されるものとする。 3.1. 1 つのサイバーオペレーションに起因するすべての損失に関するすべての補償に対して「契約に応じ設定する金額」 3.2. 保険期間中の合計で「契約に応じ設定する金額」。これらの限度額は、保険契約の全限度額の範囲内で適用されるものとし、それに追加するものではない。3.1 および 3.2 で、補償限度額が記載されていない場合は、いかなるサイバーオペレーションも補償されない。

	原文	日本語仮訳
No. 4: LMA 5567	1. Notwithstanding any provision to the contrary in this insurance, this insurance does not cover any loss, damage, liability, cost or expense of any kind (together "loss") directly or indirectly occasioned by, happening through or in consequence of: 1.1. war or a cyber operation that is carried out in the course of war; and／or 1.2. retaliatory cyber operations between any specified states leading to two or more specified states becoming impacted states; and／or 1.3. a cyber operation that has a major detrimental impact on: 1.3.1. the functioning of a state due to the direct or indirect effect of the cyber operation on the availability, integrity or delivery of an essential service in that state; and／or 1.3.2. the security or defence of a state. 2. Paragraph 1.3 shall not apply to the direct or indirect effect of a cyber operation on a bystanding cyber asset.	1. 本保険の別段の定めにかかわらず、本保険は、以下の事由により直接または間接的に引き起こされたあらゆる種類の損失、損害、賠償責任、費用（以下「損失」と総称する）を補償しない。 1.1. 戦争、または戦争の過程で行われたサイバーオペレーション、および／または 1.2. 特定の国（注2）間の報復的サイバーオペレーションにより、2つ以上の特定の国が影響を受けた国（注3）となった場合、および／または 1.3. 以下に記載の内容に、重大な悪影響を及ぼすサイバーオペレーション 1.3.1. 国内の必要不可欠なサービスの可用性、完全性、または提供に対するサイバーオペレーションの、直接的または間接的影響による、国家の機能、および／または 1.3.2. 国の安全保障、または防衛 2. 第1.3項は、サイバーオペレーションが、バイスタンディング・サイバー資産に及ぼす直接的または間接的な影響には適用されないものとする。

（注１）LMA5564 から LMA5564 には、それぞれ免責条項名の末尾に、No. 1 から No. 4 が付されている。なお本図表では、説明の便宜上 No. 2 の前に No. 3 を掲載している。

（注２）「特定の国（specified states）」として、免責条項では、中国、フランス、ドイツ、日本、ロシア、イギリス、および米国の 7 カ国が挙げられている。

（注３）「影響を受けた国（impacted states）」とは、サイバーオペレーションによって、No. 4: LMA5567 第 1.3 項に定める「重大な悪影響を及ぼすサイバーオペレーション」を受けた国を指す。

（出典：LMA, "War, Cyber War and Cyber Operation Exclusion"（2021.11）をもとに作成）

b. 責任帰属の規定について

責任帰属の規定は、4 免責条項とも共通の規定になっている（図表 9 参照）。責任帰属は、原則的に、「サイバーオペレーションにより被害を受けたコンピュータシステムが所在する国」の政府機関の判断によるものとしている。

図表 9　免責条項における責任帰属の規定

原文	日本語仮訳
3. The primary but not exclusive factor in determining attribution of a cyber operation shall be whether the government of the state (including its intelligence and security services) in which the computer system affected by the cyber operation is physically located attributes the cyber operation to another state or those acting on its behalf.	3. サイバーオペレーションの責任帰属を決定する際の主要な要因の 1 つは、サイバーオペレーションの影響を受けたコンピュータシステムが物理的に所在する国の政府（当該国の諜報機関、および安全保障担当機関を含む）が、サイバーオペレーションを他の国、またはその国のために行動する者によるものと判断するか否かによる。
4. Pending attribution by the government of the state (including its intelligence and security services) in which the computer system affected by the cyber operation is physically located, the insurer may rely upon an inference which is objectively reasonable as to attribution of the cyber operation to another state or those acting on its behalf. It is agreed that during this period no loss shall be paid.	4. サイバーオペレーションの影響を受けたコンピュータシステムが物理的に所在する国の政府（当該国の諜報機関、および安全保障担当機関を含む）による責任帰属が確認されるまでは、保険会社は、サイバーオペレーションの責任帰属が他の国、またはその国のために行動する者にあるとの客観的に妥当な推論に依拠することができるものとする。この期間中は、損失に対して、保険金は支払われないものとする。
5. In the event that the government of the state (including its intelligence and security services) in which the computer system affected by the cyber operation is physically located either: 5.1. takes an unreasonable length of time to, or 5.2. does not, or 5.3. declares it is unable to attribute the cyber operation to another state or those acting on its behalf, it shall be for the insurer to prove attribution by reference to such other evidence as is available.	5. サイバーオペレーションの影響を受けたコンピュータシステムが物理的に所在する国の政府（当該国の諜報機関、および安全保障担当機関を含む）が、サイバーオペレーションを他の国、またはその国のために行動する者によるものと、 5.1. 断定するのに不合理に長い時間がかかるか、または 5.2. 断定しないか、または 5.3. 断定できないと宣言する 場合、保険会社は、利用可能な他の証拠に基づいてその責任帰属を証明するものとする。

（出典：LMA, “War, Cyber War and Cyber Operation Exclusion”（2021.11）をもとに作成）

（2）免責条項への反応

a. 免責条項の採用状況

LMA の免責条項の保険会社等による採用状況について具体的な情報はないが、2022 年 7 月に公表されたウイリスの報告書[53]によると、第 2 四半期（4 月から 6 月）においては、ロンドン保険市場に参加する保険会社のサイバー保険の保険約款への対応状況は、以下のとおりに分かれている。

① NMA464 に様々な修正を加えた免責条項の使用
② NMA464 を基にした新たな免責条項案の作成

[53] WTW, “Cyber Insurance Market Update: Q2/H1 2022”（2022.7）

③ LMA が提示した 4 免責条項うちのいずれか 1 つ（大部分は LMA5567（No. 4））の使用

b. 免責条項の問題点の指摘

LMA の公表した免責条項に関して、マーシュは、以下のような問題点があると指摘している[54]。

○ 「重大な悪影響（major detrimental impact）」や「必要不可欠なサービス（essential service）」など、不明確な用語が用いられており、補償の対象となる事象と、そうでない事象との区分ができない。
○ 責任帰属の方法に以下の欠陥があり、保険会社に有利な内容となっている。
①正確性、重要性、または政治的動機に関係なく、サイバー攻撃の影響を受けたコンピュータシステムが、物理的に所在する国の政府の声明により、責任帰属が導き出される可能性がある。
②「影響を受けた政府」が、自ら責任帰属を明確にしない場合、保険会社は、「客観的に妥当（objectively reasonable）」とはどのような場合を指すかを明確に定義しないまま、「客観的に妥当」な他団体による推論に依拠する可能性がある。
③保険会社は最後の手段として、明確な時間的制約なしに、利用可能なその他の証拠によって責任帰属を証明することができる。

また、公的機関（政府や諜報機関など）に責任帰属の証明を要求することには、以下のような問題があると、国際的な法律事務所から指摘されている[55]。

○ 政府は、ほとんどのサイバーインシデントの原因を公表しておらず、決定的な証拠がない、または情報源を危険にさらすことを避けるなど、様々な理由で公表することに消極的である可能性がある。
○ 公に責任帰属を明確にすることより、当該国との良好な政治的・経済的関係の維持を優先する可能性がある。

c. マーシュとミュンヘン再保険による免責条項の作成

マーシュの提起した免責条項の問題点について、LMA、ロイズシンジケート、および保険会社などが論議を行った結果、多くの市場参加者が、何らかの形で、1 つまたは

[54] Marsh, “A cyber continuum: New ‘cyber war’ exclusion language raises concerns”（2022.2）
[55] Carey Olsen, “Reforming the ‘War Exclusion’ in the context of rising Cyber Warfare”（2022.7）

複数の LMA の免責条項を採用することを表明した[56]。また、この論議の中で、マーシュとミュンヘン再保険は、本件に係る問題意識を共有し、共同で LMA5567 を修正する形で、新たな免責条項「戦争およびサイバーオペレーション免責条項（War and Cyber Operation Exclusion）[57]」を作成し、2022 年 6 月に公表した（免責条項については図表 10 を、また責任帰属については図表 11 を参照願う）。この免責条項の作成に際して、両社は、主に以下の観点から検討を行ったとしている。

- ○ 免責条項では、国家の関与によるサイバー攻撃に係る補償範囲を明確にする必要がある。
- ○ 免責条項は、何が戦争を構成するのかを明確にし、「サイバーオペレーション」の概念との混同を避けるべきである。
- ○ 「サイバーオペレーション」、「重大な悪影響」、「影響を受けた国」、「必要不可欠なサービス」などの新たに導入する概念は、文言の意味についての論争を回避、または最小限に抑えるために、できるだけ明確にする必要がある。
- ○ 免責条項は、戦争を構成する、またはその一部として展開される（補償の範囲外の）サイバー攻撃と、戦争に関連していない、免責とされるべきではないサイバー攻撃とを明確に区別する必要がある。

図表 10　マーシュとミュンヘン再保険の免責条項

原文	日本語仮訳
1. Notwithstanding any provision to the contrary in this insurance, this insurance does not cover that part of any loss, damage, liability, cost or expense of any kind (together "loss") resulting: 1.1. directly or indirectly from war; 1.2. from a cyber operation that is carried out as part of a war; or 1.3. from a cyber operation that causes a sovereign state to become an impacted state. Provided, however, paragraph 1.3 shall not apply to the direct or indirect effect of a cyber operation on a computer system used by the insured or its third party service providers that is not physically located in an impacted state but is affected by a cyber operation.	1. 本保険の別段の定めにかかわらず、本保険は、次のいずれかに該当する損失、損害、賠償責任、費用（以下「損失」）を補償しない。 1.1. 直接または間接的に戦争に起因するもの 1.2. 戦争の一部として実施されたサイバーオペレーションによるもの、または 1.3. 主権国家を、影響を受けた国にさせるサイバーオペレーションによるもの ただし第 1.3 項は、物理的に影響を受けた国に所在しないが、サイバーオペレーションの影響を受ける、被保険者またはその第三者サービス・プロバイダーが使用するコンピュータシステムに対するサイバーオペレーションの、直接または間接的影響には適用されないものとする。

（出典：Marsh & Munich Re, "War and Cyber Operation Exclusion"（2022.6）をもとに作成）

[56] Marsh, "A cyber continuum: Cyber war exclusion – moving towards clarity"（2022.8）
[57] LMA のモデル条項のタイトルに用いられていた「サイバー戦争（Cyber War）」の言葉は、マーシュとミュンヘン再保険の作成したモデル条項には使用されていない。

図表 11　マーシュとミュンヘン再保険の免責条項における責任帰属の規定

原文	日本語仮訳
3. In determining attribution of a cyber operation, the insured and insurer shall have regard to whether the government of the impacted state formally or officially attributes the cyber operation to another sovereign state or those acting at its direction or under its control. In the absence of attribution by the impacted state, the insurer may rely upon a reasonable inference as to attribution of the cyber operation to another sovereign state or those acting at its direction or under its control having regard to such evidence as is available to the insurer. In the event that the government of the impacted state either takes an unreasonable length of time to, or does not, or is unable to attribute the cyber operation to another sovereign state or those acting at its direction or under its control, it shall be for the insurer to prove attribution by reference to such other evidence as is available.	3. サイバーオペレーションの責任帰属を判断する際には、被保険者と保険会社は、影響を受けた国の政府が、サイバーオペレーションを、他の主権国家、またはその指示もしくはその支配下で行動する者に公式に責任帰属したかどうかを考慮するものとする。 影響を受けた国による責任帰属がない場合、保険会社は、自らが入手可能な証拠を考慮し、サイバーオペレーションが、他の主権国家、またはその指示もしくはその支配下で行動する者に責任帰属するとの合理的推論に依拠できるものとする。 影響を受けた国の政府が、サイバーオペレーションを、他の主権国家、またはその指示もしくはその支配下で行動する者への責任帰属に、不合理に長い時間がかかるか、または責任帰属しないか、もしくはできない場合、保険会社は、入手可能な他の証拠を参照して責任帰属を証明するものとする。

（出典：Marsh & Munich Re, “War and Cyber Operation Exclusion”（2022.6）をもとに作成）

（3）ロイズの市場参加者への指示

ロイズは、2022 年 8 月に発出した「市場通告（Market Bulletin）Y5381」にて、シンジケートに対して、2023 年 3 月 31 日以降、サイバー保険の新規・更改契約において、国家の関与するサイバー攻撃に起因する損害について免責条項の付帯を義務付ける指示を出した。

この市場通告の中で、ロイズは、サイバーリスクが進化するリスク（evolving risk）であるとし、市場にシステミックリスクをもたらさぬよう適切な管理が必要であるとしている[58]。ロイズは既に、「パフォーマンス管理、補足的要件とガイダンス（Performance Management - Supplemental Requirements & Guidance）」[59]において、戦争リスクを引き受ける条件を定めるとともに、それに該当しない場合には、引き受けるすべての保険および再保険契約に戦争免責条項を含めることなどを定めている。

ロイズは、既に多くのマネージング・エージェント（managing agent）[60]が、国家の関与によるサイバー攻撃リスクに対する免責条項を、個別の保険契約に盛り込んでいることを認識しているとしながら、サイバー保険を引き受けるすべてのシンジケートが、「適切な水準に基づく、堅牢な（robust）文言を使用」した免責条項を保険契約に

[58] 2020 年から段階的に実施したサイレント・サイバーリスクへの対応もこの一環であるとしている。
[59] 2011 年から、マネージング・エージェント等の市場参加者向けに発出される文書で、市場通告や電子メールにて告知した既存の要件やガイダンスを、統合し通告するものである。
[60] マネージング・エージェントについては、脚注 45 を参照願う。

盛り込むことを徹底する意向である。

a. 単独型サイバー保険における免責事項の要件

シンジケートが、戦争や、国家の関与によるサイバー攻撃から生じるエクスポージャーを管理しているとロイズが確信できることが重要であるとし、すべての単独型サイバー保険は、ロイズの同意がない限り、以下に示す要件に従って国家の関与によるサイバー攻撃から生じる損害に対する責任を免責とする適切な条項を含める必要があるとしている。また、この条項は、戦争免責条項（同じ条項内の一部とすることも、別の条項とすること可）に追加するものでなければならず、国家の関与によるサイバー攻撃の免責条項は、最低限、以下の 5 つの要件を備えていなければならないとしている。

① 当該保険契約に個別の戦争免責条項がない場合、戦争から生じる損失を免責とする（宣戦布告されているか否かを問わない）。
② 以下のような、国家の関与によるサイバー攻撃から生じる損失を免責とする（③を条件とする）。
（a）国家の機能を著しく損なう、または
（b）国家の安全保障能力を著しく損なう
③ 国家の関与によるサイバー攻撃により、上記②（a）、および（b）に示すような影響を受ける国の国外にあるコンピュータシステムを、補償の対象から外すかどうかを明確にする。
④ 国の支援するサイバー攻撃の責任帰属の判断において、当事者が合意する強固な基準を示す。
⑤ すべての重要な用語が明確に定義されていることを確認する。

ロイズは 2023 年度の事業計画策定プロセスにおいて、単独型のサイバー保険に使用する条項について、マネージング・エージェントと論議する予定であり、その場でマネージング・エージェントは、採用する約款が上記の要件を満たしていることを説明しなければならないとしている。なお、マネージング・エージェントがこのガイダンスに示された要件から外れた対応を行う場合は、ロイズに対して、当該対応につき十分な説明を行い、承認を得る必要がある。

b. LMA 免責条項について

ロイズは、LMA が作成した 4 つの免責条項のいずれかが採用されれば、上記の要件を満たすと考えているが、マネージング・エージェントがそのいずれかを使用する場合でも、（ロイズから免除（dispensation）を受けない限り）当該条項が前記 a の要件を満たしていることを証明する必要がある。

c. 実施と次のステップ

この要件は、2023 年 3 月 31 日から、各保険契約の契約開始時または更新時から適用される。有効期限が 2023 年 3 月 31 日から起算して 12 カ月超ある場合でない限り、既存の有効な保険契約を変更（endorse）する必要はない。

7．研究機関による提案

サイバー保険における戦争リスクへの対応については、各種研究機関からも提案が行われている。本項では、ジュネーブ協会等による提案、およびカーネギー国際平和基金による提案について取り上げる。

（1）ジュネーブ協会等による提案

世界の保険会社約 80 社の CEO で構成される保険業界のシンクタンクであるジュネーブ協会（Geneva Association）、およびテロリスク（再）保険プール国際フォーラム（International Forum of Terrorism Risk (Re)Insurance Pools：IFTRIP）[61]（以下両団体を総称して「ジュネーブ協会等」）は、サイバー保険において「戦争」などを巡る「約款文言の不明確さ」、や「業界共通の定義の欠如」が、保険会社と保険契約者との紛争や訴訟の原因になっているとして、「テロを超え、戦争には至らない」範疇のサイバー攻撃を、「敵対的サイバー行為（Hostile Cyber Activity：以下「HCA」）」と新たに定義・分類し、サイバー保険の補償対象とすることを提案している。戦争やテロとの比較における、HCA の考え方・定義は、図表 12 のとおりであるが、HCA は、以下の特徴・傾向を有するものであるとしている。また、図表 13・14 は、それぞれ HCA を含むサイバー攻撃のレベルイメージ、およびレベル別の動機等を示している。

○ テロの原因などに関係なく、他の国に深刻な損害を与えることを意図する。
○ 国家によって、国家のために、または国家の財政的（または道徳的）支援によって実行される傾向がある。

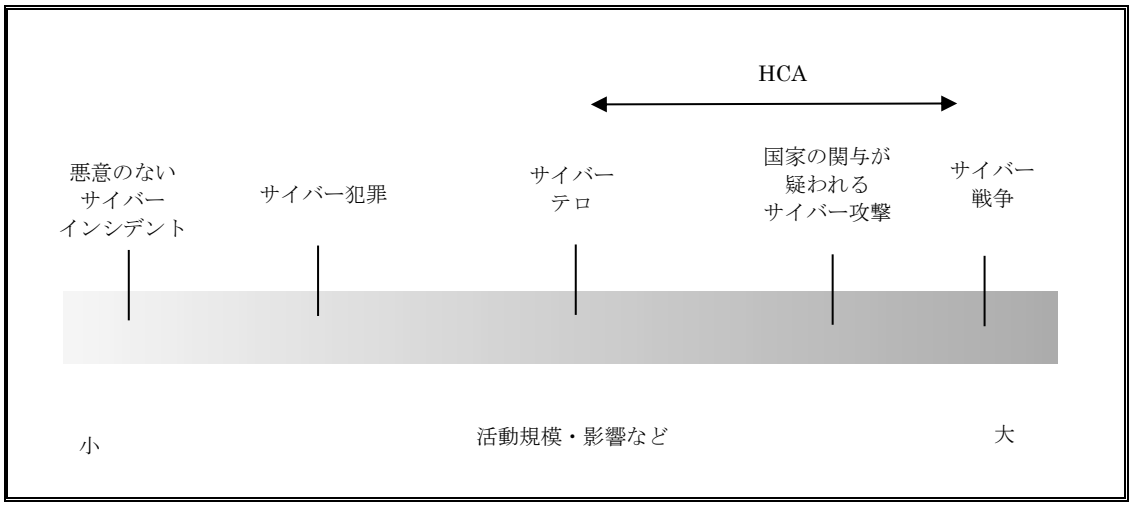
[61] IFTRIP は、グローバルなテロ（再）保険プールの共同イニシアチブである。

図表 12　戦争、テロ、および HCA の考え方・定義

項目	概要
戦争	○保険において「戦争」は、2 つ以上の当事者間の武力紛争状態であると考えられており、一般に、正規または非正規の軍事力を用いた極端な暴力、侵略、破壊、死亡によって特徴付けられる。 ○補償の拒絶は、一方の当事者または別の当事者によって宣戦布告がなされた後、または戦争状態が認識された後に損害事象が発生した場合にのみ可能である。それより前の行為は、単なる「敵対行為」である。 ○国際法の下で、「宣戦布告」については、明確な線引きや客観的基準が存在するが、「宣戦布告をしていない戦争」については、境界線が曖昧である。 ○現在までのところ、純粋にサイバー空間内で発生した宣戦布告の事例はない。 ○ジュネーブ協会は、「宣戦布告された戦争」以外の国家による行為は、HCA に含めることを提案する。
テロ	○現在、「テロ」の概念は、国によって異なっている。 ○歴史的には、テロは 2000 年以上前から存在しているが、テロの性質は近年変化し、テロの定義も変化し、複雑なものとなっている。 ○現代のテロは、まだ進化しているものの、以下のような傾向がある。 ・暴力的または著しく破壊的な行為や影響（人命の損失、重要インフラの物理的な損害や妨害など）を伴う。 ・準備段階で発見されないようにするため、個人または小規模のグループによって実行される。 ・即時的な宣伝効果（publicity）を狙い、テロ組織または個人に、実際のまたは認識される力を与えるものである。 ・政治的、宗教的、またはイデオロギー的な変化をもたらすことを目的として、一般大衆に恐怖を与えるよう設計されている。 ○上記のような特徴を持つ「サイバーテロ事件」は、まだ発生していないが、近い将来発生する可能性が高いと考えられる。
HCA	○HCA とは、一般的に、以下のいずれかを引き起こすことを目的とし、国家によって、国家のために、または国家の実質的支援や道徳的奨励（moral encouragement）によって実行される、サイバー手段や誘因（triggers）を用いて、経済的目標、または公共生活（民主的プロセスを含む）や国民の信頼を損ねたり不安定にしたりすることを目的とする内密の（covert）攻撃を指す。 1. あらゆるレベルの政府に対する混乱 2. 死亡または負傷（身体的または精神的） 3. 物的損害 4. 直接および間接的な事業中断（BI）／混乱 5. 経済的／金銭的損失 6. 環境損害（公害など） 7. 社会的信用の低下または喪失 8. 社会的混乱 9. 政治的紛争 10. 人間関係や評判の低下

（出典：Geneva Association, “Cyber War and Terrorism: Towards a common language to promote insurability”（2020.7）をもとに当研究所にて作成）

図表 13　サイバー攻撃のレベルイメージ



（出典：Geneva Association, “Insuring Hostile Cyber Activity: In search of sustainable solutions”（2022.1）をもとに作成）

図表 14　サイバー攻撃のレベル別の動機等

	サイバー犯罪	サイバーテロ	HCA	サイバー戦争
動機	金銭	カオス／金銭	混乱／破壊／影響力／カオス	支配的立場／影響力
期待	価値（Value）	恐怖／破壊	恐怖／破壊／混乱／力	乗っ取り／破壊
宣伝効果（publicity）	低	高	場合により異なるが、一般的には中程度	低／高

（出典：Geneva Association, “Cyber War and Terrorism: Towards a common language to promote insurability”（2020.7）をもとに作成）

（2）カーネギー国際平和基金による提案

米国のシンクタンクであるカーネギー国際平和財団（Carnegie Endowment for International Peace）[62]の運営する「テクノロジー・国際問題プログラム（Technology and International Affairs Program）」[63]は、Merck などの訴訟を契機として、「保険が国家の関与するサイバー攻撃や、その以外の大規模なサイバーリスクをどのように補償できるのか、または補償すべきかについて不明確であり、この根本的な不確実性が、社会的に有益なサイバー保険の発展を阻害している」として、現在の「戦争免責条項」を廃し、新たに「カタストロフ・サイバーリスク」[64]と、「戦争または国が関与するサイ

[62] 国際的な相互理解と世界平和の推進を目的に，1910 年に「鉄鋼王」アンドリュー・カーネギーにより設立された事業財団である。
[63] テクノロジー・国際問題プログラムは、サイバーセキュリティのほか、金融テクノロジーや AI などのテーマを研究し、提言を行っている。
[64] 民間損害保険での対応が困難な、甚大な被害をもたらすサイバーリスクを指す。

バーリスク」に対応する 2 つの免責条項を導入することなど、保険業界等に対して、各種分析・提案を行っている（図表 15 参照）。

図表 15 カーネギー国際平和財団による主な分析・提案

項目	概要
サイバー保険における従来の「戦争免責条項」の廃止	○免責条項の適用には、責任帰属という非常に難しい問題がある。 ○これらの問題に係る訴訟には、時間と費用がかかるとともに、顧客企業はサイバー保険の有用性を疑う懸念もある。 ○また当該免責条項を修正しなければ、保険会社は、様々な「国家の関与のないカタストロフ・サイバーリスク」にさらされたままである。
「新しい考え方」の導入	○係争中の訴訟（注1）からは、有益なガイダンスを得ることはできず、保険会社、被保険者、または監督当局に、将来の保険契約の文言をどのように作成すべきかを示すことができない可能性がある。 ○多様な保険市場全体に改革を導入するには、幅広い分野の利害関係者による新たな分析と提案が必要である。
補償範囲の定義、明確性、実用性	○保険会社、被保険者、および監督当局は、免責対象について共通の理解を有する必要がある。 ○慎重な免責条項の文言によって訴訟リスクを最小限に抑えることは可能だが、明確性と実用性は、現状十分ではない。
2 つの免責条項の導入	○以下のとおり、免責対象とすべきリスクを、「カタストロフ・サイバーリスク」と、「戦争または国が関与するサイバーリスク」の 2 つに分けて、別々の免責条項で対応する。 ①「カタストロフ・サイバー免責条項」 損害が戦争によるものか、また国家の関与によるものかどうかに関係なく、損害の規模や性質に基づいて、保険による補償が困難なカタストロフ・サイバーリスクを免責とする。 ②新たな戦争免責条項 戦争により引き起こされたサイバーリスクを免責とする新しい戦争の免責条項であり、責任帰属の問題を回避する方法として、地理的アプローチにより、武力を用いる軍事行動（または国家の関与によるサイバーオペレーションのリスクが高い地域）を特定し、加害者の身元に関係なく、これらの地域で被った損失を免責とする（注2）。
政府のバックストップ（注3）	○国家が関与するカタストロフ・サイバーリスクの補償には、政府のバックストップが必要になる場合がある。 ○サイバー保険市場は未だ未成熟なため、保険適用可能性の境界については、合意されたコンセンサスが存在しない。 ○大災害が発生する前に財政的な枠組を整備する必要がある。

（注１）Merck などの訴訟事案を指す。なお本報告書公表時点では、まだ判決は出されていない。

（注２）例えば、地理的アプローチを 2017 年の NotPetya による攻撃」に適用した場合、ウクライナ国内で被った損害のみが免責となり、同国外で被った損害は補償されることになる。

（注３）バックストップ（backstop）は、一般的に野球場等の「バックネット」を指すが、ここでは「安全装置」の意味合いで使用している。因みに「バックネット」は和製英語である。

（出典：Jon Bateman, “War, Terrorism, and Catastrophe in Cyber Insurance: Understanding and Reforming Exclusions”（Carnegie Endowment for International Peace, 2020.10）をもとに作成）

８．戦争リスクなどへの補償提供策

戦争リスクなどの、カタストロフ・サイバーリスクは、一般的なサイバー保険において補償対象とすることは困難であるが、本項では、カタストロフ・サイバーリスクへの

対応手段として、国家によるバックストップ、カタストロフ・サイバーリスク市場、および保険リンク証券（ILS）について説明する。

（1）国家によるバックストップ

民間の損害保険業界による保険化が困難である、カタストロフ・サイバーリスクを補償するための、プール制度、または官民連携制度創設の必要性については、2010 年代半ばから、世界各国で論議されており、ロイズによると、既に 12 カ国以上でテロによる再保険プール制度（以下「テロリスクプール制度」が存在している[65]。2022 年に公表されたウイリスの報告書[66]によると米国、イギリス、ドイツ、スペイン、オランダのテロリスクプール制度においては、サイバーリスクによる財物損壊が補償対象に含まれている[67]。「テロ」の定義や該当範囲は、各国制度により区々となっており、統一的ではない。例えば、米国のテロリスクプール制度である TRIP（Terrorism Risk Insurance Program）は、「議会により宣言された戦争」を補償対象外としている[68]。

（2）カタストロフ・サイバーリスク市場

イギリス最大の独立系 MGA（Managing General Agent）[69]である CFC Underwriting[70]は、「（2022 年 9 月時点で）今後 12 カ月から 18 カ月までの期間に、戦争リスクに関する「カタストロフ・サイバーリスク」の保険市場が生まれる可能性がある」と予測している[71]。同社が想定しているのは、現在、海上保険や航空保険分野において、通常の保険とは別証券で引受を行っている「戦争保険」[72]の「サイバー保険版」である。CFC Underwriting は、サイバー保険の戦争保険市場が生成するためには、サイバー保険において、「戦争リスク」が免責対象として明確に定義されている必要があると考えており、今般発出されたロイズの「国家の関与によるサイバー攻撃に対する免責条項付帯に係る指示」により、サイバー保険から「戦争リスク」が免責される要件が明確になったことから、新たな市場が生まれる可能性があるとしている。

---

65 Lloyd's, "Shifting powers: physical cyber risk in a changing geopolitical landscape"（2022.6）
66 WTW, "The Terrorism Pool Index: Review of terrorism insurance programs in selected countries 2022"（2022.5）
67 オランダでは、非財物損害も対象となっている。また、オーストラリアや、インドなどのテロリスクプーにおいては、サイバーリスクを対象外としている。
68 テロリスク保険法（Terrorism Risk Insurance Act）Sec.102. (1) (B)に基づく。
69 保険引受を除く保険会社機能を有する総括代理店を指す。
70 同社の旧社名は、「ClickForCover.com」であり、インシュアテック企業として、1990 年代からサイバー保険をオンラインで販売している。
71 Harry Curtis, "Analysis: Lloyd's latest cyber directive paves the way for a cyber cat market"（Insurance Post, 2022.9）
72 東京海上日動ウェブサイトによると、例えば「船舶戦争保険」は、被保険利益により、①船舶自体に対する戦争保険、②費用・収益に対する戦争保険、および③船主責任に関する戦争保険の、3 つに分類されている。

（3）保険リンク証券（ILS）

スイス再保険は、モデル化が困難で、分散困難なサイバーリスクへの対応手段の１つとして、保険リンク証券（Insurance Linked Securities：ILS）を挙げている[73]。保険リンク証券は、自然災害などの保険市場のリスクを、資本市場に移転する証券化商品であり、近年自然災害の増加により再保険会社の引受キャパシティがひっ迫する中、利用が拡大している[74]。保険リンク証券の代表例であるキャットボンドを例にとると、ボンド（債券）の発行により投資家より資金を募り、予め定めた要件を満たす自然災害等が発生しなければ、元利を投資家に支払い、災害が発生した場合には、リスク移転者である保険会社等が資金を受け取れる仕組である[75]。

イギリスに本拠を置く保険会社である Beazley も、システミックサイバーリスクをより適切に定義することで、保険リンク証券により新たな保険業界外の資本を呼び込むことが可能であるとしている[76]。

格付会社の S&P Global Ratings は、サイバーリスクに係る保険リンク証券は、投資機会と受け入れられる可能性があるとしながら、サイバーリスクが、完全にはモデル化されていないことなどを理由として、短中期的には、その市場の成長は鈍化するとしている[77]。

９．おわりに

本稿では、サイバー保険市場の概況とともに、国家の関与によるサイバー攻撃、サイバー保険における戦争免責条項の適用を巡る訴訟事例、LMA のサイバー戦争免責条項およびロイズの指示、研究機関による提案、ならびに戦争リスクへの補償提供策について説明してきた。

同時に広範囲にわたり巨大な損害が発生しうるサイバーリスクについて、サイバー保険において、補償範囲を明確に定義することは非常に重要であり、「国家の関与によるサイバー攻撃」も本来免責対象とすべき事象である。

しかし、そのリスクにより発生した損害に対して、もともとサイバー攻撃を想定して作成されていない従来の「戦争免責条項」を根拠として、損害保険会社が保険金を支払わないことには、米国の判例はもとより、多くの批判がある。また、このような条項解釈が、サイバー保険の有用性に対して、保険契約者の疑念を深め、サイバー保険の普及を阻害する要因となることも懸念される。

---

[73] Swiss Re Institute, “Cyber insurance: strengthening resilience for the digital transformation”（2022.11）

[74] 斎藤信也「保険リンク証券の課題と可能性」（野村総合研究所、2021.10）

[75] 従来の再保険キャパシティは、2021 年末の 4,750 億ﾄﾞﾙから、2022 年末には 4,350 億ﾄﾞﾙに減少する見込みであるが、これを補完する形で保険リンク証券市場は、2022 年に約 950 億ﾄﾞﾙの追加的なキャタストロフ再保険キャパシティを提供すると推定されている。（AM Best, “Dedicated Reinsurance Capital Growth of 2021 May Not Continue”（2022.10））

[76] Artemis, “Better defining systemic cyber risks to attract more capital: Beazley CEO”（2022.8）

[77] Artemis, “Cyber ILS market growth to be slow, as investors still hesitant: S&P”（2022.8）

この問題を解決すべくLMAが新たに作成・公表した「サイバー戦争免責条項」にも、責任帰属等解決すべき問題が指摘されており、今後も、戦争、およびサイバーリスク関連の約款文言や用語などについて、（再）保険業界全体で、国際的な明確化・共通化に向けた取組を行う必要がある。また、サイバーリスクについては、リスクの特殊性から、保険業界のみならず、関連他業界の知見を得ることも必要となるであろう。加えて、戦争リスクや、カタストロフ・リスクに対しては、民間の保険会社だけでは対応が困難であることから、被害者救済の観点から官民連携の推進・強化などの検討も必要であると考える。

技術革新に伴い、サイバーリスクを巡る状況も常に「進化」している[78]ことから、わが国の損害保険業界も、最新のサイバーリスクの動向や、諸外国の保険業界の動向を注視しつつ、約款における戦争免責条項のあり方に関する検討など、適切な対策を採る必要がある。

[78] AGCS, “Cyber: The changing threat landscape”（2022.10）

＜参考資料＞

・牛窪賢一「米国におけるサイバー保険の動向」損保総研レポート第 120 号（損害保険事業総合研究所、2017.7）
・牛窪賢一「米国を中心とするサイバー保険市場の動向」損保総研レポート第 138 号（損害保険事業総合研究所、2022.2）
・川口貴久「国家によるサイバー攻撃からのセキュリティ」（シノドス、2020.3）
・金奈穂「サイレント・サイバーリスクを巡る動向－米国・イギリスを中心に－」損保総研レポート第 126 号（損害保険事業総合研究所、2019.1）
・久保寛展「ドイツ保険法におけるいわゆる「戦争免責条項」の解釈について」保険学雑誌 631 号（日本保険学会、2016.1）
・公安調査庁「内外情勢の回顧と展望」（2022.1）
・斎藤信也「保険リンク証券の課題と可能性」（野村総合研究所、2021.10）
・損害保険事業総合研究所「欧米地域におけるサイバー保険関連動向」（2019.9）
・中江俊「米国テロリスク保険の概要―テロリスクの特性と課題を中心に―」損保総研レポート第 107 号（損害保険事業総合研究所、2014.4）
・中出哲「保険契約における免責条項の意義―海上保険を題材とする問題提起―」保険学雑誌 654 号（日本保険学会、2021.9）
・林圭一「米国を中心とするサイバーインシデント・サイバー保険市場の動向」損保総研レポート第 134 号（損害保険事業総合研究所、2021.1）
・松村昌廣「我が国のサイバーセキュリティ戦略の欠点と展望―「平和国家」体制の桎梏への対応を考える」情報通信政策研究第 5 巻 2 号（総務省、2022.1）
・AGCS, “Cyber: The changing threat landscape”（2022.10）
・AGCS, “We do not expect a major wave of claims: Russia's invasion of Ukraine: Potential impact for insurance and claims”（2022.5）
・AM Best, “Dedicated Reinsurance Capital Growth of 2021 May Not Continue”（2022.10）
・Artemis, “Better defining systemic cyber risks to attract more capital: Beazley CEO”（2022.8）
・Aviva, “Cyber Threats in 2022: Managing the risks to your business”（2022.3）
・Aviva, “Helping businesses manage their cyber risk”（2022.4）
・Brian Corcoran, “What Mondelez v. Zurich May Reveal About Cyber Insurance in the Age of Digital Conflict”（Lawfare, 2019.3）
・Carey Olsen, “Reforming the ‘War Exclusion’ in the context of rising Cyber Warfare”（2022.7）
・Carter Perry Bailey, “It’s War – But not as we know it?”（2022.5）
・Coalition, “2022 Cyber Claims Report”（2022.3）
・Coalition, “2022 Cyber Claims Report: Mid-year Update”（2022.9）
・ENISA, “ENISA Threat Landscape 2022”（2022.10）
・Gallagher Re, “Cry cyber and let slip the dogs of war”（2022.6）

・Gavin Souter, “Cyber insurance pricing comes off COVID era highs”（Business Insurance, 2022.10）
・Geneva Association, “Cyber War and Terrorism: Towards a common language to promote insurability”（2020.7）
・Geneva Association, “Insuring Hostile Cyber Activity: In search of sustainable solutions”（2022.1）
・Geneva Association, “Mapping a Path to Cyber Attribution Consensus”（2021.3）
・Harry Curtis, “Analysis: Lloyd’s latest cyber directive paves the way for a cyber cat market”（Insurance Post, 2022.9）
・IAIS, “Global Insurance Market Report”（2021.11）
・Jon Bateman, “War, Terrorism, and Catastrophe in Cyber Insurance: Understanding and Reforming Exclusions”（Carnegie Endowment for International Peace, 2020.10）
・Joseph V. Amodio, “How the Ukraine War Impacts Cybersecurity Insurance”（TANIUM, 2022.3）
・Lloyd’s, “Performance Management - Supplemental Requirements & Guidance”（2020.7）
・Lloyd’s, “Shifting powers: physical cyber risk in a changing geopolitical landscape”（2022.6）
・Lloyd’s, “State backed cyber-attack exclusions” Market Bulletin Ref: Y5381（2022.8）
・LMA, “War, Cyber War and Cyber Operation Exclusion”（2021.11）
・Marsh, “A cyber continuum: Cyber war exclusion – moving towards clarity”（2022.8）
・Marsh, “A cyber continuum: New ‘cyber war’ exclusion language raises concerns”（2022.2）
・Marsh, “Global Insurance Market Index 2022”（2022）
・Marsh, “UK cyber insurance trends 2021”（2022.6）
・Marsh & Munich Re, “War and Cyber Operation Exclusion”（2022.6）
・Michelle Falcucci, “Reforming the ‘War Exclusion’ in the context of rising Cyber Warfare”（2022.7）
・Mirza Salam Ahmed & Ben Dyson, “Cyber insurers wrestle with war exclusions as state-sponsored attack fears grow”（S&P Global Market Intelligence, 2020.1）
・Munich Re, “Munich Re Global Cyber Risk and Insurance Survey 2022”（2022.6）
・NAIC, “Report on the Cyber Insurance Market”（2022.10）
・Rachel Anne Carter, Darren Pain & Julian Enoizi, “Insuring Hostile Cyber Activity: In search of sustainable solutions”（Geneva Association, 2022.1）
・Rachel Anne Carter, & Julian Enoizi, “Cyber War and Terrorism: Towards a common language to promote insurability”（Geneva Association, 2020.7）
・Rachel Anne Carter, & Julian Enoizi, “Mapping a Path to Cyber Attribution Consensus”（Geneva Association, 2021.3）
・Reinsurance news, “Cyber to become a prominent line for Swiss Re in future”（2022.9）
・Reinsurance news, “Swiss Re would love to develop cyber ILS market: Group CUO Léger”（2022.9）
・Renee Kiriluk-Hill, “Gallagher Re: Cyber Reinsurance Premiums Will Surpass Property, Casualty as Demand Grows, Loss Mitigation Improves”（2022.2）
・S&P Global Ratings, “Cyber Risk in a New Era: The Rocky Road To A Mature Cyber Insurance Market”

（2022.7）
・S&P Global Ratings, “Cyber Threat Grows As Russia-Ukraine Conflict Persists”（2022.5）
・Swiss Re Institute, “Cyber insurance: strengthening resilience for the digital transformation”（2022.11）
・Tom Davis, “Insurers Pitch Stand-Alone Cyber Policies as ‘War Exclusion’ Faces Uncertain Future”（2022.4）
・Vincent J. Vitkowsky, “The New LMA War, Cyber War and Cyber Operation Exclusions for Cyber Insurance Policies”（HB Litigation Conferences, 2021.12）
・WTW, “Cyber Insurance Market Update: Q2/H1 2022”（2022.7）
・WTW, “Insurance Marketplace Realities 2022 Spring Update”（2022.4）
・WTW, “The Terrorism Pool Index: Review of terrorism insurance programs in selected countries 2022”（2022.5）

＜参考ウェブサイト＞

・東京海上日動　https://www.tokiomarine-nichido.co.jp/
・米国財務省　https://home.treasury.gov/
・Allianz　https://www.allianz.com/
・AM Best　http://www.ambest.com/
・Artemis　https://www.artemis.bm/
・Business Insurance　https://www.businessinsurance.com/
・Carey Olsen　https://www.careyolsen.com/
・Cybersecurity & Infrastructure Security Agency　https://www.cisa.gov/
・IAIS　https://www.iaisweb.org/
・Illinois Courts　https://www.illinoiscourts.gov/
・Insurance POST　https://www.postonline.co.uk/
・Lloyd’s of London　https://www.lloyds.com/
・LMA　https://www.lmalloyds.com/
・Marsh　https://www.marsh.com/au/home.html
・Munich Re　https://www.munichre.com/en.html
・NAIC　https://content.naic.org/
・Pool Re　https://www.poolre.co.uk/
・PropertyCasualty360　https://www.propertycasualty360.com/
・Reinsurance News　https://www.reinsurancene.ws/
・S&P Global Ratings　https://www.spglobal.com/
・WTW　https://www.wtwco.com/en-US