国家の関与するサイバー攻撃と戦争免責
―サイバー保険における戦争免責条項の適用をめぐって―

日本大学大学院法学研究科　博士後期課程　黒田　佳祐

Ⅰ　はじめに

近年、テクノロジーが進歩し、デジタル機器が普及することで、我々はデジタルインフラに対する依拠が強まっている。それに伴い、サイバーリスクが拡大・増大している[1]。サイバーリスクは、世界中で様々な問題を発生させており、現代社会において普遍的なリスクとなっている。その具体例としては、ハッキングによる情報流失、ランサムウェア感染による操業停止やロック解除のための身代金の支払い、重要な情報を盗むことなどを目的とした標的型攻撃メールなど様々なものが挙げられる。このように、サイバー攻撃手法は日々高度化・巧妙化しており、コンピュータやインターネットへ更に依存していく事業環境の中、サイバーリスクの深刻度は益々高まる傾向にある。

2022年2月24日に始まったロシアのウクライナに対する軍事侵攻においては、ミサイル攻撃や空爆などによる武力攻撃だけでなく、サイバー空間における攻撃が激化している。ロシア（またはそれを支援する勢力）によるサイバー攻撃は、ウクライナに対してのみではなく、ウクライナを支援するアメリカやヨーロッパ諸国に加え、日本に対しても行われているといわれる。

サイバー攻撃による損害をはじめとした拡大するサイバーリスクへの対応策としては、損害保険の一種であるサイバー保険が存在する。その一方で、戦争による損害は、巨額なものとなる可能性があるため、損害保険ではこれを免責とするのが通例であり、サイバー保険も同様である。したがって、ロシアによるウクライナへの軍事侵攻に伴うサイバー攻撃のような戦時に行われるサイバー攻撃には、典型的な免責規定である「戦争免責」条項の適用があるのかという問題が生じることになる。

国家の関与するサイバー攻撃と戦争免責については、アメリカにおいてその適用が争われた事例

が複数存在する。中でも注目すべきは、ニュージャージー州の裁判所で争われたMerck & Co対Ace American事件[2]である。本件は、これまでに出された第一審・控訴審判決ともに、戦争免責条項の適用を否定し、保険会社に保険金の支払いを命じている。

このような状況に対応するために、ロイズ市場協会は、「サイバー戦争免責条項」などのあらたな免責条項の作成を進めている。

本稿は、サイバー保険の概要、戦争免責の法学的な定義・意義について検討したのち、実際に戦争免責条項の適用が争われた事例、ロイズ市場協会提案のサイバー戦争免責のモデル条項について取り上げ、さらに、日本企業に対するサイバー攻撃への戦争免責の適用について考察することで、戦争免責条項の適用をめぐる「国家の関与するサイバー攻撃と戦争免責」の関係についての検討を行うものである。

Ⅱ　サイバー保険の概要

近年、サイバー保険の需要が高まっているが、サイバー保険は比較的新しい保険分野であり、あまり聞き馴染みのない者が多いのではないだろうか。本章では、サイバー保険の補償内容や市場規模など、サイバー保険とはどのような保険であるのかについて検討する。

1　サイバー保険とは

サイバー保険とは、企業がサイバー攻撃によって生じる損害を包括的に補償する保険のことである。サイバーリスクを対象とする保険商品には、個人を被保険者とする「個人向けサイバー保険」と呼ばれる商品も存在するが[3]、一般的にサイバー保険は事業者向けの保険である。サイバー攻撃の被害に遭うと、個人情報・顧客情報の流出や業務妨害などで巨額の損害が発生する恐れがあるが、サイバー保険に加入することにより、企業はサイバー攻撃に対する経済的な対策を立てることができる。

2　世界のサイバー保険市場規模

世界のサイバー保険市場規模は、2022年に133億3000万ドルと評価され、2023年には166億6000万ドルに増加すると予測されている。さらに、2030年までに846億2000万ドルに成長すると言われている[4]。

ミュンヘン再保険によると、世界のサイバー保険の収入保険料は、2019年に約58億ドル、3年後の2022年には約119億ドルと倍増しており、さらに2025年までに約225億ドル、2027年までに330億ドルに達すると予測されている[5]。また、スイス再保険が2022年11 月に公表した報告書[6]によると、世界のサイバー保険の収入保険料は、2021年に100億ドル、さらに2025年までに230億ドルになるとの予測が示されている。

このように、調査機関によって若干の違いはあるものの、世界全体のサイバー保険市場は拡大しており、今後も大幅に拡大していくと予測されている。

3　日本におけるサイバー保険

日本におけるサイバー保険の成り立ち[7]は、1998年に遡る。この時代、日本における保険の自由化の流れの中で「企業向け保険の自由化」が始まり、東京海上が「ネットワーク賠償責任保険」を開発・販売開始した。本保険は「ネットワークに起因する賠償損害」を補償するものであった。各社もこれに追随したが、大きな市場開拓には至らなかった。

2003年5月に個人情報保護法が成立し、この法律の施行までの間にも大きな個人情報漏洩事故が起きたことから、個人情報漏洩リスクに対する保険へのニーズが高まった。そのような環境の中、損保ジャパンが「個人情報取扱事業者保険」を開発・販売開始した。各社もこれに追随し、情報漏洩保険市場が立ち上がった。本保険は、情報漏洩に起因する賠償損害および事故対応にかかる費用損害を補償し、一定の市場を構築した。

2012年2月に、AIG日本法人が「サイバーエッジ」を発売開始した。翌2015年2月には、東京海上が既存の情報漏洩保険をアレンジした「サイバーリスク保険」を販売開始した。「サイバー」を商品名に入れたことが象徴的であり、これに各社が追随し、日本のサイバー保険市場が拡大していった。

サイバー保険は、企業がサイバー攻撃に遭った際に生じる損害を包括的に補償する保険であるが、主な補償内容としては、① 費用損害（当面の事故対応に係るコスト、初動対応コスト、謝罪広告・詫び状送付・コールセンター設置等費用等）、② 賠償損害（サイバー事故によって生じた賠償責任に関する損害賠償金、弁護士費用等）、③ 利益損害（システムダウンに伴い生じた逸失利益、営業停止時の人件費等）となっている。

しかし、2020年度における日本損害保険協会の調査[8]によれば、日本企業のサイバー保険の認知度は低く、加入率は7.8%である。加入しない理由の第1位は「保険の補償内容や保険料についてよく知らないため」（40.7%）であるが、第3位は「サイバーセキュリティ対策の優先度が低いため」（21%）、第4位は「サイバー被害を受ける可能性が低いため」（18.8%）となっており、危機意識の低さがうかがえると指摘されている。

Ⅲ　戦争免責について

戦争による損害は、巨額なものとなる可能性があるため、損害保険ではこれを免責とするのが通例であり、サイバー保険においても同様である。しかし、近年の戦争では軍事作戦の一手段としてサイバー攻撃が用いられる例もあるところ、国家の関与するサイバー攻撃に対しては、この戦争免責条項の適用があるのかという問題が生じる。本章では、法律による免責事由、約款による免責事

由、ロイズ提案の戦争免責条項を確認したのち、戦争免責条項における戦争とはどのようなものであると考えられているかについて検討する。

1　法律による免責

保険契約において、保険事故によって損害が生じた場合には、保険者は原則として損害てん補責任を負うが、免責事由に該当する場合には損害てん補責任を免れる。そもそも免責とは、一般に責任を免じることを意味し、その事由が免責事由である。そして免責事由とは、「保険事故に該当する事実が発生しても、例外的に保険者が保険給付義務を負わない事由」という定義が通説的理解である[9]。免責条項は、債務者である契約当事者の一方が負担しなければならない相手方に対する責任を免除し、または軽減することを内容として定めた条項であると解される。

損害保険契約における保険者の免責について、保険法17条1項は、前段で、「保険者が保険契約者または被保険者の故意または重大な過失によって生じた損害をてん補する責任 を負わない」ことを定め、後段で、「戦争その他の変乱によって生じた損害についてもてん補する責任を負わない」ことを定めている。

また、保険法17条1項の前身となる改正前商法第640条は、「戦争其他ノ変乱ニ因リテ生シタル損害ハ特約アルニ非ザレバ保険者之ヲ填補スル責ニ任セス」と規定し、戦争その他の変乱によって生じた損害の免責を定めている。続く改正前商法第641条は、「保険ノ目的ノ性質若クハ瑕疵、其自然ノ消耗又ハ保険契約者若クハ被保険者ノ悪意若クハ重大ナル過失ニ因リテ生シタル損害ハ保険者之ヲ填補する責ニ任セス」と規定し、保険の目的の性質若しくは瑕疵、自然の消耗よって生じた損害の免責、および、保険契約者または被保険者の悪意または重大な過失によって生じた損害の免責を定めており、保険法の規定は改正前商法の規定を基本的に維持している[10]。

このように、戦争によって生じた損害を免責とすることは、法律によって規定されているのである。

2　約款による免責

法律による免責事由を見てきたが、法定された免責事由は、損害保険の一般的・典型的な免責事由であり、保険法17条は任意規定である[11]。そのため、約款で法定の免責事由以外の免責事由を定めることが可能である。逆に、法定の免責事由に該当する場合に保険給付を行う旨の約定をすることも、それが公序良俗に反するような場合を除き、一般的には有効であると考えられる。例えば、戦争その他の変乱による損害について、原則として保険者を免責とする旨を定めた上で、例外的に保険料計算の基礎に影響を及ぼさないなどの客観的な条件を満たす場合に限定して、保険金の一部を支払う旨を定めることは可能であると考えられている[12]。

しかし、貨物海上保険や船舶保険などの一部の保険を除き、すべての損害保険において戦争関連リスクは、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。保険法においては、「戦争その他の変乱によって生じた損害」と規定されているが、実際に各社の約款においては、「保険金を支払わない場合」や「てん補しない損害」として「戦争、外国の武力行使、革命、政権奪取、内乱、武装反乱その他これらに類似の事変、暴動に起因する損害」が挙げられている[13]。なお、サイバー保険においても、戦争関連リスクについての免責条項は、一般的な損害保険の約款にみられる条項と同様の文言が規定されている[14]。このように戦争関連リスクを除外している理由としては、戦争や革命などは広い地域で、かつ巨額の損失が生じる可能性があり、損害保険会社が補償を提供できないためである。また、保険料率算定が困難であり、保険数理上の予測困難性からも戦争免責条項が必要であると考えられる[15]。

3　ロイズの戦争免責条項

イギリス勅許保険協会（The Chartered Insurance Institute）によると、ロイズ（Lloyd's of London）におけるノンマリン分野における戦争免責の多くは、NMA464（War and Civil War Exclusion Clause）に由来している。NMA464は、1930年代のスペイン内戦に対応して作成されたものであり、第二次世界大戦前からその文言はほとんど変更されていない。NMA464は、多くの保険種目で採用され、最も広く使用された戦争免責条項の一つである[16]。NMA464の原文およびその日本語訳は以下の通りである[17]。

（原文）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.

（日本語訳）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。

4　戦争免責条項における戦争とは

（1）サイバーリスクの増大

わが国は、日本国憲法第9条において平和主義（戦争放棄・戦力不保持・交戦権の否認）を掲げており、第二次世界大戦以降、直接的な戦争への参加はない。そのため、戦争関連リスクに係る補償の除外が実質的な意義を有することはなかった。

しかし、1990年代初頭のイラクでの湾岸戦争、2001年9月11日のニューヨークでのワールド・トレード・センターへのテロ攻撃、2015年以降のイスラム過激派組織（イスラム国）によるテロ行為など、戦争や戦争に匹敵するようなテロ行為が発生し、世界を震撼させた。また、2010年のイランのウラン濃縮施設に対するStuxnet（スタクスネット）マルウェアによるサイバー攻撃は、国家間のサイバー戦争へと発展し、重大な物理的損害をもたらした。さらに、近年のロシアのウクライナに対する軍事侵攻においては、ミサイル攻撃や空爆などによる武力攻撃に加えて、サイバー攻撃が激化している。このように、現代の戦争は、現実的な武力行使だけでなく、サイバー空間における攻撃を伴うものへと変容している。

（2）戦争の定義

戦争免責に関する約款を解釈するうえでは、「戦争」とは具体的にどのような内容を意味するのかが問題となる。しかし、保険法上にも約款上にも、「戦争」とは具体的にどのような状態を指すのかという、戦争の定義規定は置かれていない。

国際法によれば、戦争は、「一方の国家による戦争宣言などの戦意の表明によって開始され、戦争状態は征服の場合を除き交戦国間の平和条約の締結のような合意によって終了する」とされており、宣戦布告、講和条約や無条件降伏の有無などが要件とされていると考えられる[18]。

また、日本国憲法第9条は、憲法の三大原則のひとつである平和主義について規定するが、第9条第1項で放棄している戦争とは、「国権の発動」によるものであり、「国権の発動たる戦争」とは、国際法上、国の主権の発動として認められていた兵力による国家間の闘争であって、宣戦布告または最後通牒の手続により明示的に戦争の意思表示をするか、あるいは、武力行使を伴う国交断絶の形式で黙示的に表明することを要件とするとともに、交戦法規、中立法規等の戦時国際法が適用される形式的意味での戦争をいうとされる。なお、「国権の発動たる」という形容句は、戦争が伝統的に主権国家に固有の権利として観念されてきたことを表すものであって、国権の発動でない戦争の存在を認め、そのような戦争は放棄しないという趣旨ではないとされる[19]。

一方で、国際法の解釈ではなく、保険法独自の解釈として戦争等の概念を明らかすることが要請される側面があるとの考えから、「戦争とは、宣戦布告の有無にかかわらず、国家間または交戦団体の交戦状態をいい、その他の変乱とは、内乱・一揆・暴動など、戦争とまではならないが人為的騒乱であるとされる」との見解も存在する[20]。

戦争の定義については、上記のような解釈があるが、戦時に行われるサイバー攻撃が戦争免責条項の適用対象となるか否かは判然としない。次章では、アメリカにおいて、国家の関与するサイバー攻撃に関して戦争免責条項適用の可否が争われた事例を取り上げる。

Ⅳ　戦争免責条項の適用が争われた事例

国家の関与するサイバー攻撃と戦争免責条項については、アメリカにおいてその適用が争われた

事例が存在する。本稿では、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て、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 & Co対 Ace American事件」、および「Mondelez International 対 Zurich Insurance事件」について紹介する。中でも、ニュージャージー州の裁判所で争われたMerck & Co対 Ace American事件は、2023年5月に控訴審判決が下され注目を集めている。

1　Merck & Co対 Ace American事件

（1）事実の概要

アメリカのニュージャージー州に本拠地を置く多国籍製薬会社Merck & Co（以下、「原告メルク社」という）は、2017年マルウェア（NotPetya）によるサイバー攻撃を受けた。ビットコインによる身代金を要求するメッセージがコンピュータ上に表示され、被害にあったコンピュータは4万台以上に及び、7,500台のサーバーも被害を受けた。その結果、ワクチンの製造などが滞り、14億ドル以上の損害を被った。原告メルク社はAce American保険会社など複数の保険会社（以下、「被告保険会社」という）との間で[21]、てん補損害額17億5,000万ドルのオールリスク財産保険を締結しており、この財産保険は、コンピュータのデータ及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。本保険契約の存在と補償内容については争いがない。

原告メルク社は14億ドルの損害について保険金を請求したが、被告保険会社はこれを拒絶した。ここでの争点は、このサイバー攻撃がロシア政府によるものであるかであった。原告メルク社は、正式な国家によるものではなく、ランサムウェアの一形態であると主張した。さらに、それがウクライナに損害を与えるためにロシア政府が関与していたとしても、免責条項は適用されないとして、保険金の支払いを求めた。これに対して被告保険会社は、NotPetya攻撃は、ロシア政府がウクライナ政府を揺るがすために行ったものであり、免責条項である敵対的・戦争的行為に該当すると主張し、保険金の支払いを拒絶した。

本訴訟において重要な免責条項である「敵対的／戦争的行為免責（Hostile／Warlike Action Exclusion）条項」の原文およびその日本語訳は以下の通りである[22]。

（原文）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.

（日本語訳）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争的な行為によって引き起こされた損失または損害

a) 政府もしくは主権国家（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ついて、同時または他の順序で損失に寄与する他の原因または事象にかかわらず、補償しません。

原告メルク社は「ITコンプライアンス調査中間報告書（IT Compliance Investigation Interim Summary Report）」の中で、本件のマルウェア攻撃について詳細な説明を行っている[23]。

2017年6月27日、NotPetyaとして知られるマルウェアが原告メルク社のコンピュータとネットワークシステムに感染した。これは、それ以前に何者かが、原告メルク社やウクライナの他の企業が使用する「M.E. Doc」という会計ソフトウェアを開発したウクライナの会社のコンピュータシステムにアクセスしていたためであった。そして、NotPetyaマルウェアは、この会計ソフトウェアに配信された。マルウェア感染の経緯は以下の通りである。

原告メルク社およびウクライナで事業を展開するその他の企業は、請求書、税金、その他の財務データを処理し、ウクライナ政府に送信するために、M.E. Docと呼ばれる信頼できる第三者機関のアプリケーションを使用していた。第三者機関の分析によると、2017年4月14日以前に、脅威アクター[24]がM.E.Docのソースコードとシステムのソフトウェアアップデート配布インフラにアクセスしたことが判明している。このアクセスを利用して、脅威アクターはM.E. Docソフトウェアのアップデートにバックドアを組み込み、脅威アクターがM.E. Docソフトウェアを使用する顧客システムにアクセスすることを可能にした。これらのバックドアを使って、脅威アクターは、M.E. Docソフトウェアを使用している企業のネットワーク上で、アンチウイルスやその他のマルウェア検出ツールやセンサーによって検出されることなく、コードの送信、受信、および実行が可能なコマンド＆コントロールインフラストラクチャ[25]を確立した。

脅威アクターは、M.E. Docソフトウェアの悪意あるバージョンを、標準的なM.E. Docのアップデート方法を使用して、既存のM.E. Docの顧客に送信した。そして、原告メルク社は、ウクライナにあるサーバーを通じて悪意あるアップデートを受け取った。このサーバーは、アップデートの目的でM.E. Docソフトウェアの新バージョンの定期的なチェックを自動的に行っているところ、

このような送信は、M.E. Docのアップデートのための合法的で定期的なチェックに偽装されていたのであった。これらの侵害されたアップデートの結果、2017年6月27日以前に、脅威アクターはコマンド＆コントロール機能を通じて、企業の感染したシステムから指示を送信したり、偵察情報を取得したりすることが可能となった。

両当事者の専門家によるとNotPetyaが、システムまたはネットワークに感染すると、システム上の特定のデータを暗号化しようとするため、データにアクセスできなくなり、ほとんどのユーザーがファイルを復元できなくなる。そして、感染したシステムまたはネットワーク上のデータを暗号化した後、NotPetyaは、身代金の支払いと引き換えにデータを復元するための復元化キーを提供することを提案するメッセージを表示し、自身をランサムウェアとして提示するのである。

原告メルク社のグローバルネットワーク内のコンピュータは、最初の感染から90秒以内に、約1万台がNotPetyaに感染し、5分以内に約2万台が感染した。最終的には、4万台以上のコンピュータがNotPetyaに感染した。原告メルク社は、このマルウェアによって「生産設備や重要なアプリケーションがオフラインになり、製造、研究開発、販売業務を含む原告の業務に大規模な混乱が生じた」と主張している。

2017年7月、原告メルク社はNotPetyaの損害について被告保険会社に通知したところ、被告保険会社は権利留保書面（reservation of rights letter）を提示した。2018年3月、被告保険会社は再度権利留保書面を送付し、今度は敵対的・戦争的行為による免責を明示的に提示した。しかし、被告のうちの一社であるナショナル・ユニオンはこの権利留保書面の提示に参加しなかった。そして、原告メルク社は2018年8月2日に訴えを提起した。これに対し、2018年8月20日、被告保険会社のほとんどは、敵対的・戦争的行為免責条項に基づき、原告メルク社のNotPetya関連の請求に対する保険金の支払いを拒否した。

被告保険会社は、「サイバー・コンサルタント」であるクロール・サイバー・セキュリティ（Kroll Cyber Security、以下「クロール」という）が、原告メルク社のシステムがNotPetyaに感染していたと結論づけたことを指摘した。NotPetyaは、「ウクライナの事務所にあるM.E. Doc（原告メルク社やウクライナで事業を展開する他の企業が使用する税務ソフトウェア・アプリケーション）が稼働するサーバーを通じて原告メルク社に侵入した」とされている。クロールはまた、「NotPetyaによるサイバー攻撃は、ロシア連邦のために、またはロシア連邦の代理として活動する関係者によって組織された可能性が非常に高い」と結論づけた。

同日、被告ナショナル・ユニオンは、原告メルク社に権利留保書面を送付し、「クロールの調査結果およびNotPetyaサイバー攻撃に関する一般に入手可能な情報に基づき、ナショナル・ユニオンは保険契約の『戦争/テロリズム免責』に基づき権利を留保する」と述べた。この免責条項が、他の保険会社の保険契約に含まれる敵対的・戦争的行為免責条項と実質的に同一であることは議論の余地がない。

（2）第一審判決

2021年4月から9月にかけて、広範な証拠開示の後、当事者は敵対的・戦争的行為免責条項の適用可能性を含む様々な問題について略式判決または部分的略式判決を求める申立てと反対申立てを行った。

2021年12月6日、第一審裁判所である、ニュージャージー州上位裁判所（Superior Court of New Jersey）[26]は、NotPetyaによって引き起こされた原告メルク社の損害に対する補償を除外するために敵対的・戦争的行為免責条項は適用されないと判断し、部分的略式判決を求める原告メルク社の申立てを認めた。裁判所は、適用される契約解釈の法原則と判例を分析し、次のように結論づけた。

「免責条項の文言の平易な意味を考慮すると、当裁判所は免責条項が適用されないと判断する。原告らが準備書面で述べているように、本件事実に類似する事例に戦争（または敵対的行為）免責条項を適用した裁判例は存在しない。証拠によれば、これらの保険で使用されている文言は長年にわたって事実上同じである。もちろん、この契約の両当事者が、時には民間から、時には国家から、さまざまな形態の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ことも自明である。そうであるにもかかわらず、被告保険会社は免責条項の文言を変更し、当該被保険者にサイバー攻撃を免責とする意図があることを合理的に知らしめるようなことは何もしなかった。そして、被告保険会社に免責条項を変更する能力があったことは確かである。被告保険会社が保険約款の文言を変更しなかったため、原告メルク社は、免責条項が伝統的な形態の戦争にのみ適用されると予期する権利を有していた。解釈原則[27]を考慮すると、サイバー攻撃に基づく行為に免責条項が適用されることを予期していなかったという原告メルク社の立場は、免責条項が伝統的な形態の戦争にのみ適用されると、被保険者が予期するということを合理的に示している。したがって、提示された事実の下では免責条項は適用されないと判断する。」と判示した[28]。

このように、第一審判決は主として、① 戦争免責条項を、このようなサイバー攻撃に適用することを認めた判例が過去にはないこと、② 国家の関与するサイバー攻撃が過去何年にもわたって増加し、一般的となっていることを保険契約の当事者は認識しており、そのような状況では、被告保険会社はサイバー攻撃による損害を免責とするという意図を被保険者に伝えることができたにもかかわらず、免責条項に変更はなく、従前と同じ文言を用いていたこと、③ 免責条項の文言を変更していなかったことから、ここでいう戦争免責が、伝統的な戦争にのみ適用されると期待する権利を原告メルク社は有していること、④ このようなサイバー攻撃による損害を免責とするためには、サイバー攻撃を免責とする旨を明記した免責条項への変更が必要であることを理由に、被告保険会社に対して保険金の支払いを命じている。なお、中心的な争点となっていた「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、判決では触れられていない。

（3）第一審判決に対する反応

被告保険会社は、この判決を不服として控訴した。控訴審判決によると、第一審判決に対して

は、肯定的な意見も否定的な意見も存在したとされる。

住宅、自動車、企業向け保険会社の主要な全国業界団体である米国損害保険協会（American Property Casualty Insurance Association）は、被告保険会社に同意する立場をとった。米国損害保険協会は、「国家」によって行われたあらゆる性質の非友好的行為によって引き起こされた損害が、敵対的・戦争的行為免責条項に明白に該当すると主張し、第一審判決に反対したとされる[29]。

さらに、第一審判決が言及した過去の裁判例の中には、1953年に「私的な契約や文書で使用される『戦争』という用語は、公的または政治的な根拠に基づいて、法律主義的または技術的な意味で解釈されるべきではなく、その通常の現実的な意味、すなわち、2つ以上の国家の事実上または実質上の武力間の実際の敵対行為が与えられるべきである」と述べた比較的古い裁判例[30]が含まれていたため、「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」との批判もなされた[31]。

その一方で、第一審判決を支持する関係者団体は多数存在する。例えば、ニュージャージー州郡協会（New Jersey Association of Counties）は、敵対的・戦争的行為免責条項に関する保険会社の解釈を受け入れることは、「戦争免責条項の定説的な意味を変更することになり……地方自治体が適切な保険による補償を確保するために歴史的に依拠してきた保険契約解釈規則を根底から覆す恐れがある」と主張したとされる。また、保険法を専門分野とする全米の法学教授からなるグループであるInsurance Law Scholarsは、「保険会社はサイバー関連事象に対する補償を除外または制限するような、容易に利用可能な保険約款を使用しなかったため、裁判の判決は支持されるべきである」と主張した[32]。

（4）控訴審判決

2023年5月1日、ニュージャージー州中間上訴裁判所は、被告保険会社の上訴を退け、「免責条項の平易な文言、およびその適用の状況と歴史を考慮すると、被告保険会社が本件の状況下で免責条項が適用されることを立証しなかった、すなわち、本件サイバー攻撃が免責条項のもとで想定される『敵対的』または『戦争的』行為であったことを立証しなかった」と結論付けた[33]。

控訴審において、被告保険会社は、免責条項が「明確（clear）かつ明白（unambiguous）であり、NotPetyaの攻撃に適用されることは明らかである」ため、第一審が下した略式判決は被告保険会社側に有利に認められるべきであったと主張した。その理由として、被告保険会社は、敵対的・戦争的行為免責条項における「戦争的（warlike）」という言葉が本件に適用されない可能性があることは認めるが、「敵対的（hostile）」という言葉は、「不利な（adverse）」、「悪意や危害を加えようとする意思を示す（showing ill will or a desire to harm）」、「敵対する（antagonistic）」、「非友好的な（unfriendly）」という意味で、可能な限り広義に読まれるべきであると主張した。さらに、被告保険会社は、脅威アクターが政府または主権国家である限り、「脅威アクターによる悪意または危害を加えようとする意思を反映した」いかなる行為も「敵対的・戦争的行為免責」に該当することを主張し、NotPetya攻撃にはロシア連邦が含まれると主張した[34]。

しかし、控訴審において、上訴裁判所は敵対的・戦争的行為免責に関連する長年の判例をとり上げたところ、「これらの判例は、主権国家による『敵対的または戦争的行為』に類似した用語が、戦争に明らかに関連する行為、または少なくとも軍事行為や軍事目的に関連することを意図していることを示すものである」と判示した[35]。このように、上訴裁判所は、敵対的または戦争的行為によって生じた損害の免責には「軍事行為の関与（involvement of military action）」が必要であり、免責条項は適用されないとして、被告保険会社の主張を退けた。

このように、ニュージャージー州上位裁判所は、第一審・控訴審ともに、敵対的・戦争的行為免責条項の適用を否定し、被告保険会社に保険金の支払いを命じたのである。

なお、被告保険会社は、本判決を不服として、ニュージャージー州最高裁判所へと上告している。

2　Mondelez International対 Zurich American事件

アメリカのイリノイ州に本拠地を置く食品・飲料会社のMondelez International（以下、「原告モンデリーズ社」という）は、2017年にNotPetyaランサムウェアによるサイバー攻撃を受けた。その結果、原告モンデリーズ社は1,700台のサーバーと2万4,000台のコンピュータが回復不能なダメージを負い、1億8,800万ドルの損害を受けた。原告モンデリーズ社はZurich American（以下、「被告保険会社」という）との間で、オールリスクの財産保険を締結していたため、保険金を請求した。しかし、被告保険会社は約款に規定されていた、敵対的・戦争的行為免責条項を理由に保険金の支払いを拒絶した。そのため、原告モンデリーズ社は、2018年にイリノイ州クック郡巡回裁判所（Circuit Court of Cook County）に、本保険金の支払いを求めて訴訟を提起した。

本件の争点は、前記のMerck & Co対 Ace American事件と同様に、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であった。原告モンデリーズ社は、「被告保険会社は技術的な証拠を提供していない」と主張したところ、被告保険会社は、「NotPetyaは免責条項に定める敵対的または戦争的行為に該当する」と主張した[36]。

しかし、この裁判は、2022年10月27日の最終弁論（closing arguments）直前に、原告モンデリーズ社および被告保険会社の双方から訴訟の取下げの申立て（motion）が行われたため、最終的には判決まで至らなかった。

Ⅴ　ロイズ市場協会提案のサイバー戦争免責のモデル条項

1　判決に対する保険会社の動向

2017年のNotPetyaによるランサムウェア攻撃やMerck & Co対 Ace American事件判決による保険約款の解釈の在り方は、サイバー保険市場にリアルタイムで影響を与えた。一部の保険会社は、免責条項の修正を行い、補償範囲を狭めようとした。例えば、ロンドン市場の特定の保険会社

が提供する最新のサイバー保険では、政府による宣戦布告の有無に関係なく適用される可能性のある、より広範で具体的な文言を使用した戦争免責条項が採用されている[37]。このように、保険業界においては、国家の関与するサイバー攻撃による損害を明確に免責とする条項を策定する動きがみられている[38]。

2　ロイズ市場協会が提案したモデル条項

ロイズは、17世紀に発足し、300年以上の歴史を持つ英国ロンドンにある保険市場である。そこでは、世界各国の様々なリスクが日々持ち込まれており、各シンジケートに所属する高い専門性を有する引受人によってリスクの評価や料率設定、保険引受が行われている。また、ロイズ市場協会（Lloyd's Market Association）は、シンジケートのマネージング・代理店などで構成された団体であって、ロイズ市場の参加者のために専門的かつ技術的な支援を提供している[39]。

そのロイズ市場協会は、同協会内のCyber Business Panelにおいて検討を重ねた結果、2021年11月にLMA5564（No.1）、LMA5565（No.2）、LMA5566（No.3）、およびLMA5567（No.4）の4つの「戦争、サイバー戦争、およびサイバーオペレーション免責条項（War, Cyber War and Cyber Operation Exclusion、以下『サイバー戦争免責条項』という）」を公表している[40]。この4つのサイバー戦争免責条項は、主要な用語の一貫した定義に基づき、4段階の補償レベルを設定しているところ、この免責条項の重要な特徴は、① サイバー保険自体に「サイバーオペレーション（cyber operation）」の概念を導入したこと、② 責任の帰属を決定するためのプロセスを規定したことである。

ここで注目されるのは、免責条項の中に新たに用いられているサイバーオペレーションという概念であるが、サイバーオペレーションとは、「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）するために、国家が、または国家のためにコンピュータシステムを使用すること」であると定義されている。また、この免責条項は、「戦争（war）」の定義も設けているところ、戦争とは、「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」であると定義されている。このように、「サイバーオペレーション（cyber operation）」という新たな概念は、物理的な武力を用いる一般的な「戦争（war）」とは異なるということが明示されている[41]。

この4つのサイバー戦争免責条項では、「戦争によって引き起こされたあらゆる種類の損失、損害、賠償責任、費用を補償しないこと」および「免責条項適用の立証責任を保険会社が負うこと」が共通して記載されている。しかし、各免責条項は、サイバーオペレーションによる損失を免責とする程度が異なっている。LMA5564（No.1）は、4つの免責条項の中で、免責の対象範囲が最も広く（＝補償の対象範囲が最も狭く）、すべてのサイバーオペレーションによる損失を免責として

いる。LMA5565（No.2）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（中国、フランス、ドイツ、日本、ロシア、イギリス、米国）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[42]または安全保障、防衛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おり、これらに起因しない損失を、特定の支払限度額の範囲で補償するものである。LMA5566（No.3）の免責の対象範囲は、LMA5565（No.2）と同様であるが、支払限度額についての定めはない。LMA5567（No.4）の免責の対象範囲は、LMA5566（No.3）と同様であるが、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（bystanding cyber assets[43]）」に及ぼす影響を補償範囲に含んでいるため、4つの免責条項の中で、免責の対象範囲が最も狭い（＝補償の対象範囲が最も広い）ものである。

その後、2022年8月16日、ロイズは「市場通告（Market Bulletin）Y5381」[44]を公表した。これは、2023年3月31日以降、サイバー保険の契約開始時または更新時に、国家の関与するサイバー攻撃に起因する損害についての免責条項の付帯を義務付けるものである。そして、国家の関与するサイバー攻撃に起因する損害についての免責条項は、①保険契約に個別の戦争免責規定がない場合、戦争（宣戦布告されたか否かを問わない）に起因する損失を免責とすること、②国家の機能または国家の安全保障能力を著しく損なう国家の関与するサイバー攻撃に起因する損失を免責とすること、③国家の関与するサイバー攻撃によって、上記②に示すような影響を受ける国家の国外に所在するコンピュータシステムを補償の対象から除外するかどうかが明確であること、④国家の関与するサイバー攻撃がどのように1つまたは複数の国家に責任帰属するかについて、当事者が合意する強固な基準を定めること、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こと、これら5つの要件を備えておかなければならないとした。

さらに、2023年1月20日、ロイズ市場協会は上記LMA5564～LMA5567のサイバー戦争免責条項をアップデートしたモデル条項（バージョンB）を公表した。新たに策定されたバージョンBの主要な特徴としては、初期バージョン（バージョンA）にある「サイバーオペレーションの国家への責任帰属（attribution of a cyber operation to a state）」に関する条項が省略されていることである。バージョンAにおいては、サイバーオペレーションの国家への責任帰属を判断する際、保険者および被保険者が、入手可能である客観的に合理的な証拠を考慮することとされている。国家への責任帰属を判断する証拠として、ここでは、「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」の政府機関の判断によるとされている。しかし、バージョンBには「サイバーオペレーションの国家への責任帰属」に関する条項がないため、マネージング・エージェント[45]が責任帰属の方法を設定することとなる。

このように、ロイズ市場協会によるサイバー戦争免責のモデル条項の策定を中心に、国家の関与するサイバー攻撃による損失を明確に免責とする動きが進んでいる。

Ⅵ　日本企業に対するサイバー攻撃と戦争免責条項の適用

1　ロシアのウクライナ侵攻に関連する日本企業へのサイバー攻撃

2022年2月24日、ロシアによるウクライナ侵攻が発生した。これを受けて世界中でサイバー攻撃の脅威が高まる中、日本企業が攻撃の標的となり深刻な被害を受けるケースも相次いでいる[46]。

実際に、ロシアのウクライナ侵攻以降、日本企業が標的となり、深刻な被害を受けるケースも出現している。

小島プレス工業（トヨタの取引先）は、2022年2月26日にランサムウェア攻撃を受けたためにシステム障害が発生し、3月1日にはトヨタが国内のすべての工場の稼働を停止する事態となった。2022年2月27日には、タイヤメーカであるブリヂストンのアメリカのグループ会社がランサムウェア攻撃を受け、北米と中南米にある複数の工場が操業を停止した。2022年3月10日には、デンソー（トヨタグループの大手自動車部品メーカー）のドイツの拠点でランサムウェア攻撃を受け、発注書や図面あるいは機密情報などを不正に窃取された。2022年3月13日には、大手菓子メーカーの森永製菓がランサムウェア攻撃を受け、社内のサーバーへの不正アクセスが行われ、複数のシステムがダウンするなどの障害が発生し、商品の製造にも影響が出たとされている[47]。

このような企業に対する攻撃に加えて、2022年9月6日には日本政府のポータルサイトや民間企業のサービスに対してDDoS攻撃が行われ、政府・行政機関のサイトや民間企業のサイトへのアクセスが困難になるという障害が発生した。この攻撃は、ロシア政府を支持するハッカー集団キルネットによる犯行であるとされている[48]。

2　戦争免責の適用の可能性

ロシアのウクライナ侵攻から増加しているとされる日本企業等へのサイバー攻撃であるが、攻撃を受けた企業がサイバー保険に加入していた場合、その損害は保険によってまん補されるのであろうか。それとも戦争免責条項の適用がなされるのであろうか。

これまで検討してきたように、サイバー保険における戦争免責条項は、国家の関与するサイバー攻撃による損害には適用が困難であると思われる。それは、アメリカにおけるMerck & Co対 Ace American事件において裁判所が示した理由にも述べられているが、現行の戦争免責条項にいう戦争とは、従来の武力による国家間の衝突を意味しており、戦争免責条項の適用には軍事行為の関与が必要であると考えられるためである。また、免責条項の立証責任は保険者にあり、サイバー攻撃の主体が国家または国家が関与する機関によるものであると立証することは困難であると指摘できる。さらに、ロイズにおける新しい免責規定導入の動向は、現状の戦争免責規定ではサイバー攻撃によって生じた損害に対する戦争免責条項の適用が困難であることを示しているものと考えられる。

Ⅶ　おわりに

本稿は、戦争免責条項の適用をめぐる「国家の関与するサイバー攻撃と戦争免責」の関係について検討を行った。戦時に行われるサイバー攻撃への戦争免責条項の適用においては、何が「戦争」や「敵対的または戦争的行為」に当てはまるのか、また何がその範囲外となるのかを適切に解釈できるようにすることが求められる。

前述したように、現在の日本のサイバー保険における、戦争関連リスクについての免責条項は、一般的な損害保険の約款にみられる文言と同様であるため、戦時に行われ、国家の関与するサイバー攻撃による損害が補償範囲に含まれるかどうか判然としない。保険会社がこのような損害を補償の対象外とするのであれば、ロイズ市場協会提案のモデル条項のように、国家の関与するサイバー攻撃を免責とする規定を設けることを検討する余地はあると考える。しかし、戦争免責条項の適用範囲を広げすぎてしまうと、サイバー保険の存在意義が薄れてしまう可能性があることは否めない。それでもなお、サイバーリスクは広範囲にわたって巨額の損害を引き起こす可能性があるため、サイバー保険の補償範囲を明確にすることが非常に重要であることに変わりはない。

本稿は、損害保険における戦争免責条項の適用について、国家の関与するサイバー攻撃という新たな問題が存在することを提示し、若干ではあるがその適用の可否を検討した点に意義があると考える。しかし、実際に戦争免責条項の適用が争われた事例として第4章で取り上げたアメリカの裁判例は、オールリスク型の財産保険に関して争われた事例であり、サイバー保険にも妥当しそうであるか、約款文言の違いにより戦争免責条項の適用の可否に影響があるかといった点につき更なる検討を行う必要がある。また、戦争免責条項の適用にあたっては戦争と損害との間の因果関係が求められるところ、このような戦争起因性の判断に関しての考察も必要であり、今後の研究課題として挙げられる。

サイバー戦争という新たな戦争が誕生し、サイバー保険の市場規模が急速に拡大されていく今日、戦争免責条項の内容・解釈を再検討する必要があるのではないだろうか。今後も、サイバー保険と戦争免責の動向に注目していきたいと考える。

---

[1] サイバーリスクを厳密に定義することは困難であるが、一例として、英国の規制当局であるPrudential Regulation Authority（健全性監督機構、PRA）が2017年7月に公表した監督声明（Supervisory Statement）SS4/17において、保険引受の観点から、サイバーリスクについて、「サイバー保険引受リスクとは、有形資産及び無形資産に関する悪意ある行為（サイバー攻撃や悪意あるコードへのITシステムの感染）と悪意なき行為（データの損失、偶然の作為または不作為）から生じるサイバー関連の損失に晒される保険契約を引き受けることから発生する一連の財務上のリスク」と定義されている。サイバーリスクと保険については、榊素寛（2021年）「サイバーリスクと保険の全体構造」、『損害保険研究』第83巻第2号、1-45頁に詳しい。

[2] 第一審：Merck & Co. v. Ace Am. Ins. Co., Docket No.: UNN-L-2682-18 2021 N.J. Super. Unpub. LEXIS 4566（Superior Court of New Jersey, Law Division, Union County. Dec. 6, 2021）
控訴審：Merck & Co. v. Ace Am. Ins. Co., 475 N.J.Super. 420 (App Div. May 1, 2023), 293 A.3d 535（2023）

[3] 個人を被保険者とする「個人向けサイバー保険」とは、火災保険に追加する補償（特約）として提供されるもののことである。例えば、東京海上日動が提供する火災保険「トータルアシスト住まいの保険」では、家庭におけるサイバーリスクに備える「ホームサイバーリスク費用補償特約」を付加することができる。本特約は、住宅内のネットワーク構成機器・設備（パソコン、スマートフォン、IoT機器等）が不正アクセス等のサイバー攻撃を受け、セキュリティ事故に対するために負担した修理費用やデータ復旧費用等を補償する。

[4] “cyber insurance market size”, FORTUNE BUSINESS INSIGHTS, https://www.fortunebusinessinsights.com/cyber-insurance-market-106287（2023年9月24日アクセス）。

[5] “Cyber insurance: Risks and trends 2023”, Munich Re, https://www.munichre.com/landingpage/en/cyber-insurance-risks-and-trends-2023.html（2023年9月24日アクセス）。

[6] “Cyber insurance: strengthening resilience for the digital transformation”, Swiss Re Institute, https://www.swissre.com/dam/jcr:6fd9f6dd-4631-4d9f-9c3b-5a3b79b321c0/2022-11-08-sri-expertise-publication-cyber-insurance-strengthening-resilience.pdf（2023年9月24日アクセス）。

[7] 土井剛（2021年）「サイバー保険概要」、『日本セキュリティ・マネジメント学会誌』35 巻2号、25頁を参照。

[8]「国内企業のサイバーリスク意識・対策実態調査2020」日本損害保険協会、https://www.sonpo.or.jp/cyber-hoken/data/2020-01/pdf/cyber_report2020.pdf（2023年9月24日アクセス）。

[9] 山下友信（2022年）『保険法（下）』、有斐閣、46頁。

[10] 保険の目的の性質若しくは瑕疵、自然の消耗よって生じた損害については、保険法では法定の免責事由とされていない。また、商法641条は「悪意」と規定していたが、一般に悪意は故意を意味するものであると解されていることから、保険法では「故意」と規定された。

[11] 萩本修（2009年）『一問一答保険法』、商事法務、120頁。

[12] 同上、121頁。

[13] 例えばわが国の住宅火災保険普通保険約款3条2項1号や傷害保険普通保険約款3条1項9号において「戦争、外国の武力行使、革命、政権奪取、内乱、武装反乱その他これらに類似の事変または暴動（群衆または多数の者の集団の行動によって、全国または一部の地区において著しく平穏が害され、治安維持上重大な事態と認められる状態）」が掲げられている。

[14] 例えば、三井住友海上が提供するサイバー保険「サイバープロテクター」は、「戦争、外国の武力行使、革命、政権奪取、内乱、武装反乱その他これらに類似の事変、暴動、労働争議または騒擾」に起因する損害に対して保険金を支払わないと規定する。その他、東京海上日動が提供する「サイバーリスク保険」、あいおいニッセイ同和損保が提供する「サイバーセキュリティ保険」などにおいても類似の文言が規定されている。

[15] 甘利公人＝福田弥夫＝遠山聡（2020年）『ポイントレクチャー保険法〔第3版〕』、有斐閣、121頁。

[16] “War exclusions in cyber policies: an overview”, DAC BEACHROFT, https://www.dacbeachcroft.com/en/articles/2023/march/war-exclusions-in-cyber-policies-an-overview/（2023年9月20日アクセス）。

[17] War and Civil War Exclusion Clause（NMA464）の日本語訳については、先行研究である、濵田和博（2022年）「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」、『損保総研レポート』第141号、11頁を参照。

[18] 国際法学会〔編〕（2005年）『国際関係法辞典〔第2版〕』、三省堂、545頁。

[19] 野中俊彦＝高橋和之＝中村睦男＝高見勝利（2006年）『憲法Ⅰ〔第4版〕』、有斐閣、164頁。また、日本国憲法第9条に関する学説については、杉山幸一（2021年）「憲法9条における『国際紛争を解決する手段』について」、『危機管理学研究』第5号、152-161頁に詳しい。

[20] 石田満（1997年）『商法Ⅳ（保険法）〔改訂版〕』、青林書院、191頁。

[21] 本訴訟では、Ace Americanほか、Allianz（アリアンツ）、National Union Fire Insurance（ナショナル・ユニオン・ファイアー・インシュアランス）などの保険会社30社が被告となっている。

[22] Merck & Co. v. Ace Am. Ins. Co. 2021 N.J. Super. Unpub. LEXIS 4566 at 3.

[23] Merck & Co. v. Ace Am. Ins. Co. 293 A.3d 539-540.

[24]「脅威アクター」とは、"Threat Actor"の訳であり、サイバー攻撃を行う主体を指す。

[25]「コマンド＆コントロールインフラストラクチャ（Command and Control Infrastructure）」は、C2またはC&Cとも呼ばれ、サイバー攻撃において用いられるインフラストラクチャで、攻撃者が侵害したシステムと通信し指揮（command）および統制（control）する目的で用いられる。「用語集」SOMPO CYBER SECURITY、https://www.sompocybersecurity.com/column/glossary/a98（2023年9月22日アクセス）。

[26] ニュージャージー州上位裁判所（Superior Court of New Jersey）は、一審裁判所（Trial Court）と中間上訴裁判所（Intermediate Appellate Court）を有している。終審は、州の最高裁判所である「Supreme Court of New Jersey」が担っている。

[27] 解釈原則（Canons of ConstructionまたはRules of Construction）とは、法律解釈の根本原則で、裁判所が契約書などの文言を解釈するときに準拠する原則である。田中英夫〔編〕（1991年）『英米法辞典』、東京大学出版社、121頁。

[28] Merck & Co. v. Ace Am. Ins. Co. 2021 N.J. Super. Unpub. LEXIS 4566 at 13-14.

[29] Merck & Co. v. Ace Am. Ins. Co. 293 A.3d 542.

[30] Stanbery v. Aetna, 26 N.J. Super. 498, 98 A.2d 134 (Law Div. 1953)

[31] "It's War – But not as we know it?", Carter Perry Bailey, https://www.cpblaw.com/publications/2022/it-s-war-but-not-as-we-know-it/（2023年9月23日アクセス）。

[32] Merck & Co. v. Ace Am. Ins. Co. 293 A.3d 542.

[33] *Id*. at 538.

[34] *Id*. at 545.

[35] *Id*. at 551.

[36] "Insurers Pitch Stand-Alone Cyber Policies as 'War Exclusion' Faces Uncertain Future", Best's Review, https://bestsreview.ambest.com/edition/2022/April/Cyberattacks.html（2023年9月23日アクセス）。

[37] "War Exclusion Developments in Cyber Insurance Policies", Latham & Watkins, Latham & Watkins, https://www.lw.com/admin/upload/SiteAttachments/War-Exclusion-Developments-in-Cyber-Insurance-Policies.pdf（2023年9月23日アクセス）。

[38] "Cyber insurers wrestle with war exclusions as state-sponsored attack fears grow", S&P Global Market Intelligence, https://www.spglobal.com/marketintelligence/en/news-insights/latest-news-headlines/cyber-insurers-wrestle-with-war-exclusions-as-state-sponsored-attack-fears-grow-56743302（2023年9月23日アクセス）。

[39] ロイズの組織と仕組みについては、松岡順（2009年）「現代のロイズ －ロイズの組織とその仕組み－」、『損保総研レポート』第90号、51-80頁に詳しい。

[40] 当該サイバー戦争免責条項免責条項の規定内容や免責条項への反応については、濵田（2022年）、16-21頁に詳しい。

[41] サイバー戦争免責条項において、「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、本文中に「サイバー戦争」という用語は登場しない。また、免責条項中の「用語の定義」の項においても、「戦争」や「サイバーオペレーション」の定義規定は置かれているものの、「サイバー戦争」という用語についての説明はない。なお、サイバー戦争の定義については、加藤朗（2013年）「新たな安全保障領域『サイバー空間』の理論的分析」、『国際安全保障』41巻1号、12-26頁に詳しい。

[42]「必要不可欠なサービス（essential service）」とは、金融機関および関連する金融市場インフラ、保健サービス、公共サービスを含むがこれらに限定されない、国家の重要な機能の維持に不可欠なサービス

を指す。

[43]「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る国に所在しないが、サイバーオペレーションの影響を受けるものを指す。

[44] 市場通告Y5381は、「国家の関与によるサイバー攻撃免責条項（State backed cyber-attack exclusions）」というタイトルが付されており、独立型サイバー保険における、国家の関与によるサイバー攻撃免責条項について、ロイズの要件を定めることを目的としている。

[45] マネージング・エージェントとは、シンジケート全体の管理・運営を行う団体のことである。ロイズにおける保険契約の取引に関与する関係者または組織としては、保険責任を負うメンバー、保険引受単位であるシンジケート、主に個人メンバーに対するアドバイスや事務代行を行うメンバーズ・エージェント、メンバーのためにシンジケートの運営を行うマネージング・エージェント、マネージング・エージェントに雇用され保険引受実務を担当するアンダーライター、保険または再保険契約者のためにアンダーライターとの交渉等を行うブローカーなどが存在する。松岡（2009年）、55頁参照。

[46] ロシアが本格的な軍事侵攻を開始した前日である2022年2月24日、経済産業省は「昨今の情勢を踏まえ、サイバー攻撃事案の潜在的なリスクが我が国においても高まっている」ことを指摘し、国内企業や業界団体にサイバー攻撃対策を強化するよう呼びかけた。「昨今の情勢を踏まえたサイバーセキュリティ対策の強化について注意喚起を行います」経済産業省、https://www.meti.go.jp/press/2021/02/20220221003/20220221003.html（2023年9月23日アクセス）。

[47]「サイバー攻撃 日本企業も標的に 深刻な被害受けるケースも」NHK、https://www3.nhk.or.jp/news/html/20220327/k10013554701000.html（2023年9月23日アクセス）。

[48]「日本政府や日本企業に“サイバー攻撃”『キルネット』とは」NHK、https://www3.nhk.or.jp/news/html/20220912/k10013814111000.html（2023年9月23日アクセス）。