日本保険学会関東部会　2022年12月16日報告

サイバーリスクと戦争リスクの交錯

―　ウクライナ事態と戦争保険の視点からの考察　―

東京海上日動火災保険株式会社
海上業務部　貨物業務グループ
新谷　哲之介

はじめに

- 近年は、武力紛争とサイバー攻撃が密接な関係にあり、サイバー戦の重要性が増している。武力紛争とサイバー攻撃とが、密接または不可分となると、保険契約上で、武力紛争の危険とサイバー攻撃の危険を、担保または免責としている場合の解釈が問題となり得る。たとえば、海上保険のように戦争リスクが担保される保険契約においてサイバー攻撃リスクを免責とする場合の解釈、反対に、サイバー攻撃リスクを担保する保険契約において戦争リスクを免責とする場合の解釈などもある。
- 今日の軍事的行動にデータ情報通信やコンピュータの使用は不可欠であり、敵の軍隊、政府、経済に対するサイバー攻撃は有効な手段となる。こうしたことから、今日においては、戦争リスクとサイバーリスクには概念的な重複部分がある。ロシアによるウクライナ侵攻はこうした問題について考える契機となった。
- 本報告では、伝統的に戦争リスクを保険の対象とする海上保険と、近年、国際的に普及しているサイバーリスクの免責との関係について考える。また、戦争リスクとサイバーリスクの重複は、単に部分的に重なるということだけではなく、今後は「サイバー攻撃のみの戦争リスク」という事象の可能性もあり、この場合には戦争リスクとサイバーリスクが全面的に重複することになる。こうしたケースについても触れていく。

戦争保険約款の担保内容

- 保険契約が国際的に譲渡されることが多い貨物海上保険では、英国の約款が実質的な国際標準として位置付けられている。わが国でも貿易実務上の要請から英国の約款が使用され、外国語の普通保険約款を使用することが保険会社の事業方法書に記載され、監督官庁から認可されている。
- 往時は、貿易において捕獲や襲撃などの加害行為が大きなリスクであったことから、貨物海上保険は伝統的に戦争危険を担保している。今日わが国では、英国の約款であるInstitute War Clauses (Cargo) 1/1/2009が使用されているが、同約款のもとでは、武力紛争にともなう攻撃や触雷などの危険の他に、捕獲、拿捕、抑留などの危険による損害が填補される。

（抜粋）
1. This insurance covers, except as excluded by the provisions of Clauses 3 and 4 below, loss of or damage to the subject-matter insured caused by
1.1 war civil war revolution rebellion insurrection, or civil strife arising therefrom, or any hostile act by or against a belligerent power
1.2 capture seizure arrest restraint or detainment, arising from risks covered under 1.1 above, and the consequences thereof or any attempt thereat
1.3 derelict mines torpedoes bombs or other derelict weapons of war.

（和訳）
第1条　この保険は、下記第3条および第4条の規定により除外された場合を除き、以下の事由によって生じる保険の目的物の滅失または損傷をてん補する。
1.1　戦争、内乱、革命、謀反、反乱もしくはこれらから生じる国内闘争、または敵対勢力によってもしくは敵対勢力に対して行なわれる一切の敵対的行為
1.2　上記第１条１項で担保される危険から生じる捕獲、拿捕、拘束、抑止または抑留およびそれらの結果またはそれらの一切の企図
1.3　遺棄された機雷、魚雷、爆弾またはその他の遺棄された兵器

サイバー免責約款の内容

- 民間企業や政府機関に対する大規模なサイバー攻撃が発生するようになり、海運や貿易に対するサイバー攻撃によって、保険者が想定していない大きな損害が生じることの懸念が、保険者の間で生じた。とりわけ、再保険者が集まるロンドンマーケットは、サイバー攻撃の波及効果による損害の巨額化について強い懸念を示し、その結果、ロンドンの再保険者を中心に、サイバー攻撃による損害を明示的に免責する特別約款の導入が2019年頃に始まった。再保険契約におけるこうした制限は、必然的に元受保険者の引受能力への連鎖を招来し、わが国を含めた世界各国でサイバー免責約款の導入が行われた。
- わが国で使用されているものは、国際的に一般にみられる英国の特約形式であり、要旨は以下。
- 1条：サイバー攻撃によって生じた損害について保険者は填補責任を負わない旨を規定。（実際の約款は、「サイバー」という包括的な語句を用いるのではなく「コンピュータ、コンピュータシステム、コンピュータソフトウェアプログラムその他の電子システム」と具体的に列挙をしている）
- 2条：サイバーに起因する事象であっても、それが危害を加える手段として使用または操作されない限りは保険者が填補責任を負うことを規定。これは、免責となるのは、加害の意思がある場合のみであって、たとえば誤操作やプログラム上のバグなどは免責の対象としないことを意図する。
- 3条：戦争危険やテロ危険についての例外規定。戦争危険やテロ危険を担保する保険に本特約が付帯される場合に、兵器やミサイルの発射・誘導システムおよび発射メカニズムにおけるサイバーの使用に起因する損害には1条の免責規定が適用されないことを規定する。現代の兵器の多くは、何らかの形でコンピュータやソフトウェア（＝サイバー）が使用されているので、1条によって危害を加える意図のあるサイバーとして免責されると、兵器等による加害行為である戦争やテロ攻撃による損害の多くが保険者免責となってしまい、戦争やテロの保険の意味が実質的に失われかねないために本条がある。

サイバー免責約款原文

MARINE CYBER ENDORSEMENT

This endorsement shall not apply when the Assured is an individual (An individual shall not include a sole proprietorship in this endorsement.).

1 Subject only to paragraph 3 below, in no case shall this insurance cover loss, damage, liability or expense directly or indirectly caused by or contributed to by or arising from the use or operation, as a means for inflicting harm, of any computer, computer system, computer software programme, malicious code, computer virus, computer process or any other electronic system.

2 Subject to the conditions, limitations and exclusions of the policy to which this clause attaches, the indemnity otherwise recoverable hereunder shall not be prejudiced by the use or operation of any computer, computer system, computer software programme, computer process or any other electronic system, if such use or operation is not as a means for inflicting harm.

3 Where this clause is endorsed on policies covering risks of war, civil war, revolution, rebellion, insurrection, or civil strife arising therefrom, or any hostile act by or against a belligerent power, or terrorism or any person acting from a political motive, paragraph 1 shall not operate to exclude losses (which would otherwise be covered) arising from the use of any computer, computer system or computer software programme or any other electronic system in the launch and/or guidance system and/or firing mechanism of any weapon or missile.

（和訳）サイバー攻撃危険に関する特別約款

本特別約款は被保険者が個人となる契約には適用しない。（本特別約款において個人には個人事業者を含まないものとする）

第1条　第3条の規定に従い、この保険では、いかなる場合においても直接であると間接であるとを問わず、コンピュータ、コンピュータシステム、コンピュータソフトウェアプログラム、悪意のあるコード、コンピュータウイルス、コンピュータプロセス、またはその他の電子システムが、危害を加える手段として使用または操作された場合、その使用または操作によって生じたいかなる損害もてん補する責任を負わない。

第2条　コンピュータ、コンピュータシステム、コンピュータソフトウェアプログラム、コンピュータプロセス、またはその他の電子システムが、危害を加える手段として使用または操作されないかぎり、その使用または操作によって生じた損害をこの保険証券記載の普通保険約款、特別約款および他の特別条項に従ってもてん補する責任を負う。

第3条　この特約が、戦争、内乱、革命、謀反、反乱もしくはこれらから生じる国内闘争、敵対勢力によってもしくは敵対勢力に対して行なわれる一切の敵対的行為、テロ行為、または政治的動機から活動する一切の者による危険を担保する保険証券に付帯される場合、本特約第1条は、兵器もしくはミサイルの発射・誘導システムおよび発射メカニズムにおけるコンピュータ、コンピュータシステム、コンピュータソフトウェアプログラムその他の電子システムの使用に起因する（本来補償されるべき）損害には適用しない。

サイバー攻撃危険に関する約款上の問題

- サイバー免責約款3条は、「兵器もしくはミサイルの発射・誘導システムおよび発射メカニズムにおけるコンピュータ、コンピュータシステム、コンピュータソフトウェアプログラムその他の電子システムの使用に起因する損害」には本免責規定が適用されないと規定する。
- この規定が指す具体的内容は何か？＝火砲・ミサイル・魚雷等におけるサイバーの使用については免責としないことであると考えることができる。今日は、誘導式のミサイルもあれば、火砲の弾道や魚雷の射角を手計算するわけでもないので、これらにはコンピュータやソフトウェアプログラムが関係しており、戦争保険やテロ保険の本旨を踏まえれば、サイバーが復活的に担保される必要がある。しかし、問題は、復活担保されるべきは、果たして「兵器もしくはミサイルの発射・誘導システムおよび発射メカニズムにおける」サイバーだけで良いのかという点である。
- たとえば、触雷というリスクを考えた場合に、古典的な触発の機雷であればサイバーは無関係かもしれないが、今日では磁気、音響、水圧、電流などによって起爆するいわゆる感応機雷が多用される。こうした機雷は、センサーが情報を感知し、その情報が、設定された起爆条件と合致することで起爆するので、何らかのソフトウェアやプログラムが機能しているといえる。

サイバー攻撃危険に関する約款上の問題（続き）

- また、前掲のInstitute War Clauses（Cargo）1/1/2009は、その1条2項でcapture（捕獲）危険を担保している。
- 捕獲とは、海上武力紛争法上の措置であって、交戦国が、敵国や中立国の船舶や貨物を臨検し、必要に応じてこれらを拿捕し、その後に捕獲審検所における審決を経て、船舶や貨物を没収するまでの一連の行為。
- こうした捕獲権の行使は、海軍力によって行われるが、海軍艦艇が捕獲を遂行する上で、コンピュータを使用しないことがあるだろうか。☞　今日の操船技術や、海上における他船の動向収集においてコンピュータ、ソフトウェア、プログラムなどが使用されないことはおよそ考えられない。
- ここで例として掲げた触雷や捕獲の危険による損害が生じた場合に、これらについて復活担保せずに引き続き免責とすることを約款起草者が企図していることは考えにくい。火砲・ミサイル・魚雷に限って復活担保し、機雷等の危険を免責のままに残すことには、合理的な理由が見出せず、3条の趣意に照らしても不自然であり、これは起草者の見落とし（想定不足）であることが推測される。

因果関係

- サイバー免責約款3条で復活担保される危険は、実質的に火砲とミサイルと魚雷によるものであるから、たとえば復活担保の対象とされていない捕獲を例として考える場合に、捕獲のオペレーションにコンピュータ等のサイバーが手段として関与することは想定されても、「捕獲損害はサイバーによるものである」とまで認定できるかという因果関係上の問題がある。
- 換言すれば、サイバーと損害との間に因果関係が認められなければ、そもそも1条の免責に該当しないので、損害填補される可能性があるのではないか、ということ。
- ところで、1条には、因果関係の決定方法を規定する文言があり、危険と損害の関係についてdirectly or indirectly caused by or contributed to by or arising fromと定める。つまり「directly or indirectly caused by」「contributed to by」「arising from」という３つの因果関係が示されている。わが国で引き受けられている外航貨物海上保険は、準拠法条項が付帯され、同条項によって文言解釈の準拠法は英国法となる。

因果関係（続き）

- 英国保険法では、因果関係決定に近因原則が適用される。英国の諸々の保険約款で多用されるcaused byという語句は、近因原則の適用を示す一般的な表現と解釈される。一方、本件のように、caused by以外の語句が使用される場合、それは近因原則とは異なる因果関係を規定することが目的であり、そのため、「directly or indirectly caused by」「contributed to by」「arising from」という語句は、それぞれどのような因果関係を示すのかが問題となる。
- まず、「directly or indirectly caused by」であるが、この表現において特に重要な語句がindirectly caused byである。indirectly caused byは、因果関係を最も広く柔軟にとらえることを可能にするための表現であり、危険との関係性が僅かであっても、損害との因果関係を認めることを可能とする。本条は免責規定であるので、危険と損害との因果関係上の縁が遠くとも、間接的に因果関係が認められる限り、保険者を免責する効果がある。
- そうすると、先述の復活担保の対象とされていない捕獲を例として考えると、捕獲のオペレーションにコンピュータやプログラムが関与し、損害の成立に僅かな影響でも与えていれば、免責となる可能性がある。要するに、indirectly caused byと規定することで、海軍艦艇のコンピュータによる索敵行動が捕獲損害に寄与していれば、当該コンピュータ使用は損害の主因でなくとも、一因であれば足り、その原因としての影響力の強弱は問われない。したがって、触雷や捕獲以外にも、Institute War Clausesに列挙されている敵対的行為、拿捕、抑留などの危険、あるいはInstitute Strikes Clausesに規定されるテロリズムなどであっても、コンピュータやプログラムの使用があれば、コンピュータやプログラムが損害に及ぼした影響の度合いとは関係なく保険者免責と解釈されるべきことになる。

因果関係（続き）

• 次に「arising from」であるが、この表現は、Institute Cargo Clausesの核兵器免責を規定する際に使用されている。ここでもdirectly or indirectly caused byと並列して使用され、核免責条項の趣意からは、免責の効果を確実にするために、因果関係を規定する語句を列挙することで、その関係を広範に定める意図の推定が可能である。一方で「arising from」の法律的効果については諸説がある。caused byと同様に近因を指すという見解がある一方で、attributable toと同等の効果を持つという解釈がある。attributable toは、故意免責の規定に適用されている表現であって、損害の原因が複数あって競合する場合に、寄与割合の少ない原因であっても、その原因を有効とすることを可能とする（従って故意は主因でなくとも、わずかでも故意が寄与していれば免責とする効果がある）。

• このように「arising from」については確定的な解釈がないが、「directly or indirectly caused by」および「contributed to by」と並列されることで、これらのいずれの因果関係も適用される。そうすると、因果関係を最も広く柔軟にとらえることを可能にするとされるindirectly caused byによって、因果関係は常に最大限に認められることとなるので、「arising from」の解釈に異なる見解があっても実質的に問題にはならない。

• 最後に「contributed to by」であるが、これについては意義を確定する判例、または傍論における言及はない。一方で、海上保険契約には、契約文言の解釈原則があることから、語句に固有の解釈が確立していないのであれば、解釈原則にしたがって解釈を行うべきものとなる。しかし、上述のとおり、因果関係を最も広く柔軟にとらえることを可能にするための表現であるindirectly caused byが並列されることで、実質的に最大限の因果関係が認められることとなるので、「contributed to by」の解釈が実務上の問題になることは考えにくい。

因果関係（続き）

- 以上を要するに、サイバー免責約款１条は、サイバーの使用または操作を原因とする損害について、その因果関係を、近因に留まらない広範囲にわたり認めており、たとえ捕獲、拿捕、抑止、抑留などのように、必ずしもサイバーが損害の主因とはなりにくい事象であったとしても、間接的にサイバーの使用が寄与していれば、免責となるように構成されている。
- その結果、いざ事故が発生した際に、保険者・被保険者の双方にとって、想定外の免責が発動する可能性があり、不意打ち的な規定となり得る。

考察　①問題の整理

- そもそもサイバー免責約款は、ハッキングやウイルスなどのサイバー攻撃による損害を免責するためにある。そして、約款は、サイバー攻撃について「コンピュータやプログラムが危害を与える目的で使用される」などの表現を用いるところ、現代の兵器がコンピュータやプログラムを多用するために、「コンピュータやプログラムが危害を与える目的で使用される」ことに偶々相当してしまう結果となっているだけであり、そのため、戦争やテロの危険を担保すべき保険が無意味にならないように復活担保の規定が置かれている。
- そうであれば、戦争やテロの保険には、はじめからサイバー免責約款を付帯しなければよい、という考え方もあるかもしれないが、そのような方法は適当とはいえない面がある。
- なぜなら、近年は、正規の軍隊にサイバー部隊が設置され、サイバーが軍事的攻撃手段として用いられるようになっているので、武力が行使されないサイバーのみの攻撃も想定される。こうした武力が行使されないサイバー攻撃は、伝統的な戦争保険およびテロ保険では想定されていないことから、たとえば「戦争危険による損害を填補する」という約款規定のもとであっても填補対象とならないことを示す意味がある。つまり、戦争保険やテロ保険は、物理的な損傷や滅失による損害を填補するものであって、物理的損害が伴わない純粋なる経済的損害を填補するものではないので、サイバー免責約款はこれを明確化する役割も果たしている。ところが、現行のサイバー免責約款では、およそサイバーリスクと観念しがたい触雷、捕獲、拿捕、抑止、抑留などの危険も不意打ち的に免責にしてしまう可能性がある。
- では、どうしたら良いのか？

考察　②約款文言のアンダーライティングによる対応

- こうした戦争保険に対するサイバー免責の適用問題を解決する方法は、幾つか考えられるが、たとえば因果関係の規定をcaused byに代えることで、サイバーが近因と認められる場合のみの免責とすることができる。サイバーが近因と認められる場合のみの損害填補に限定すれば、たとえば火力打撃による損害についてサイバーを近因と認めることは想定しにくく、その結果、戦争保険の実質的効果が減じられることがなく、反面、サイバーが近因と認められる攻撃で免責となるのであれば、サイバー免責の本旨を曲げることもない。触雷や捕獲の損害において、サイバーが近因と認められることも想定しにくいことから、既述の問題は解消されると考えられる。
- あるいは別な方法として、因果関係を近因に限定せずに広く認める規定を維持するのであれば、その場合には、サイバーによる物理的損害は填補し、純粋な経済的損害のみについては免責するよう規定することも一つの方法である。結局のところ、兵器の使用であれ、捕獲や抑留などの行為であれ、サイバーの寄与効果が避けがたいことを前提とするならば、これらは填補の対象とすることを明確化し、純粋な経済的損害の排除を明定すれば良い。

考察　②約款文言のアンダーライティングによる対応（続き）

- なお、サイバーリスクに関する免責条項付帯が国際的に普遍化しているなか、これを復活担保するいわゆるwrite back clause (buy back clause)がある。write back clauseは、サイバー攻撃による火災、爆発、座礁、転覆、衝突、共同海損犠牲、投荷、盗難等の危険による単独海損、共同海損および救助料の填補を約するものであって、戦争危険は対象としない。write back clauseの背景には、近年アンダーライターの間で着目され、IUMIでも研究されたサイバー攻撃による物理的損害惹起の想定がある。これは、たとえば船舶の航行に関わる機器がサイバー攻撃を受け、船舶が制御不能に陥って衝突するとか、コンテナターミナルを制御するシステムがサイバー攻撃を受けて機能不全に陥り、温度管理ができなくなった貨物が爆発事故を起こすなどの想定である。これらは、正規の軍隊のサイバー部隊による攻撃であったとしても、保険上の戦争危険には該当しないのでInstitute War Clausesなどではもとより填補対象とならないが、write back clauseが付帯されている場合、同約款では加害者を限定していないので、正規の軍隊たるサイバー部隊による攻撃であったとしても、上述の列挙危険に該当すれば填補対象となり得る。

考察　③ウクライナで見られたロシアのサイバー攻撃

- 2014年のロシアによるウクライナ侵攻開始の後、2017年にはロシアによるウクライナを狙ったサイバー攻撃といわれるNotPetyaと呼ばれるマルウェアが欧州で猛威を振るった。NotPetyaによる被害は、原子力発電所のモニタリングシステムをダウンさせるなどの衝撃的なものも報じられたが、民間企業の被害についても報じられ、とりわけ世界最大級の船社であるマースクの被害は大きく取り上げられた。同社の端末がウクライナのオデッサ港でNotPetyaに感染したのを皮切りに、その感染が同社の各国の拠点におよび、最低でも300ないし400億円程度の被害を被ったとされた。
- その後、英国外務大臣が、NotPetyaによるサイバー攻撃を分析した結果として、ロシア軍によるものと判断したと発表した。同様に大きな被害を被った製薬大手のメルクが、米国の大手保険会社エースに対して同サイバー攻撃の被害について填補を求めた裁判においても、当該サイバー攻撃がロシアの国家としての実行であったとの主張がエース側からなされた（この点は、結果的には裁判上の争点にならなかった）。
- 2022年2月24日に、ロシアによるウクライナ侵攻が再び始まったが、この侵攻に先立つ同年1月14日にウクライナ政府機関の70の公式サイトが乗っ取られるサイバー被害が発生しており、極めて破壊力の強いウイルスが検出された。このウイルスは、2月24日午前２時にウクライナ軍とウクライナ政府との連絡に使用される衛星電波の基地局のシステムを破壊し、その３時間後の午前5時のロシア軍の侵攻が開始された。こうしたウクライナの政府や軍に対するサイバー攻撃については、ロシアからの攻撃であることを英国NCSC（National Cyber Security Centre=国家サイバーセキュリティ・センター）が報告しており、改めて軍事的な害敵手段としてのサイバー攻撃という側面が浮き彫りになっている。また、ここで保険者としても注目すべきは、サイバー攻撃が通常戦力による攻撃と共同して行われている点である。

考察　④サイバーと通常戦力との協同作用下での保険のあり方

- 武力紛争において、サイバー攻撃が通常戦力による攻撃と協同し、一体化した作戦が行われるようになると、伝統的な戦争危険にとどまらないサイバー攻撃も含んだ軍事行動に対する保険上のニーズも増大していくことが予想されるが、同時にサイバーによる損害と通常兵器による損害との判別が難しくなることが想定される。
- こうした場合には、ニーズとして、「どういう場合でもカバーできるように」という要望がされがちである。一方で保険契約は、予め定めた危険によって被保険者に生じる損害を填補する契約であるから、被保険利益の存在を前提に、危険および損害について画定を要する。
- また、民間保険会社による引受は、プロフィットを前提とする。アンダーライティングとは結局のところ、こうした被保険者のニーズに応えつつ、保険者のプロフィットも確保する枠組みを拵えることであり、料率算定、条件策定、文言起草が鍵となる。戦争危険やサイバー危険のように、損害が広範囲に及ぶことで巨額化する可能性があるものについては、保険者はその許容リスクの画定を慎重に行う必要があり、そのためには料率や支払限度額の画定もさることながら、契約文言の起草・策定はとりわけ重要となる。すなわち、危険および損害をそれぞれどう規定するか、その因果関係をどのように決定するか、という保険の基本的事項の策定が重要となる。いきおい、保険契約の文言は、誤解や曲解が無いように厳密である必要があり、客観的で一義的でなければならない。反対に、「どんな場合でもカバーできるように」という不明瞭な条件では、保険者の填補責任を画定できない。保険が契約である限り、幾ら時代が進んでも不明瞭な事象を総括的に対象とするような保険は現実的ではない。

考察　④サイバーと通常戦力との協同作用下での保険のあり方（続き）

- また、戦争危険なのかサイバー危険なのかという判断が複雑化する場合においても、単に複雑だからという理由で、異なる二つの重大な危険を同一視してアンダーライティングすることは適当でない。なぜなら、サイバーリスクは、非物質的であり、その結果として損害も物理的な滅失・損傷を伴わない経済的損害に終始する可能性が高く、武力の行使に伴う物理的損害を対象とする戦争危険とはアンダーライティングは異なる。
- 一方で、現実に武力紛争においてサイバー戦の重大性が増し、物理的な損害に対する原因としてのサイバーの寄与度が増大するのであれば、それはサイバーリスクの損害に対する因果関係の規定方法によりコントロールされれば良い。すなわち、サイバーと物理的な武力行使は併存し、協同的に作用するという前提に立ち、サイバーが一つの要因であったとしても、近因が武力の行使であるならば損害てん補責任を認めることが考えられる。
- 反対に、サイバーが近因であるならば免責とするという方法もあり得る。
- または、write back clauseのように、サイバーに起因する物理的損害の填補を復活的に担保する枠組みを設けることも、被保険者のニーズと保険者のアンダーライティング上の要求の両者を満たす対処法である。

考察　⑤サイバー戦と電子戦の異同

- 付言しておくべき事項として、サイバー戦と電子戦の異同がある。その理由は、たとえば、海上保険契約における国際的慣習として、Extended RACE と呼ばれる特約が至上約款として付帯される。本約款は放射能免責を規定するINSTITUTE RADIOACTIVE CONTAMINATION EXCLUSION CLAUSE（通称RACE）を拡大した免責規定であり、CHEMICAL, BIOLOGICAL, BIO-CHEMICAL AND ELECTROMAGNETIC WEAPONS、すなわち、化学兵器、生物兵器、生物化学兵器および電磁気兵器についても保険者免責を規定する。
- 電磁的兵器とは、近年軍事的に重視されている電子戦における攻撃兵器であるが、ここに至上約款としての電磁的兵器免責が規定されているので、たとえばサイバー攻撃の危険を担保する意図がある場合に、電磁的兵器による免責が優先することでサイバー危険の担保を打ち消す可能性がないかという問題がある。とりわけ電磁的兵器の免責規定はdirectly or indirectly caused by or contributed to by or arising fromという因果関係の規定方法を用いることで、その免責規定としての効果を非常に強いものとしている。そのため、電磁的兵器とサイバーとの関係が問題となる。
- 電磁的兵器とは、レーザー光や電子ビームなどの電磁波エネルギーを使用した指向性エネルギー兵器、また強力な電磁パルスによって広範囲にわたり電子機器を故障させるEMP兵器などである。したがって、これらは電磁波などによって人や物を直接的に攻撃することができるが、一方でサイバー攻撃は、プログラムやソフトウェアなどの非物理的な攻撃であるので、基本的に両者は異なるものである。しかし、電磁波の使用はサイバーとも関係がある。敵国の各種通信に対してのEMP兵器による電磁パルス攻撃や、ジャミング（妨害電波の発信）は電磁波を利用した電子戦に分類されるが、同時にサイバー空間に対する攻撃ともなる。なぜなら、サイバーは電子機器と通信を前提とするので、これらが使用できなければサイバー空間は成立し得ない。このようにサイバーと電磁はその関係性が深く、概念的には重なる領域が存在している 。現在、それぞれのリスクについて保険者が有無責を規定しているのは、全く異なる背景を持つものであるが、結果としては、電磁的リスクまたはサイバーリスクのいずれに起因する損害であるかの判別を行わなくてはならない。両分野は、いずれも進展が著しく、今後の技術の発展に伴う両者の関係性については、海上保険者として注視を要する。

最後に

- 2022年にロシアがウクライナ領内へ侵攻するに先立ち実施した大規模なサイバー攻撃を考えると、将来において「サイバー攻撃のみの戦争リスク」という想定も視野に入れるべきであろう。たとえば電力、通信、輸送などの重要インフラの機能をサイバー攻撃によって停止させることは、人や財物に対する間接的な攻撃ともなり得る。
- 「サイバー攻撃のみの戦争リスク」について、次のような政府見解がある；「サイバー攻撃のみであっても、例えば、物理的手段による攻撃と同様の極めて深刻な被害が発生し、これが相手方により組織的、計画的に行われている場合には武力攻撃に当たり得る」（第198回国会衆議院本会議録第24号（令和元年5月16日）13頁（安倍晋三内閣総理大臣答弁））
- 講学上も、サイバーのみの戦争リスクについて次のような見解がある；「サイバー攻撃のうち、正規の軍隊などによるものはもとより、正規軍隊以外の行為であっても、国に帰属し『生命あるいは財産の破壊』を生じさせるものについては、それ単独で行われるものであっても（サイバー攻撃のみが行われ、武力紛争の第一撃となったり、すでに開始されている武力紛争のなかで行われるわけでなくとも）、国連憲章２条４によって禁止される武力行使に該当すると考えることができよう」（黒崎将広・坂元茂樹・西村弓・石垣友明・森肇志・真山全・酒井啓亘『防衛実務国際法』（弘文堂・2021）244頁）。こうした国際法上の見解は海外で主張されている。

最後に（続き）

• しかし、こうした直接的な武力が使用されないサイバー攻撃を「武力行使」と観念することは、普遍的通念といえるであろうか。

• 2022年8月に英国のロイズは、単独のサイバー保険（ノンマリン保険）について、通常の戦争危険免責に加えて、新たにstate-backed cyber attacks（国家によるサイバー攻撃）に関する免責条項付帯の指示を出したが、こうした免責規定を導入する必要性に鑑みても、武力が発現しないサイバー戦を戦争危険とみなすことについては、少なくとも保険法上は見解が対立する余地があるものと考えられる。

• 一方で、今後戦争におけるサイバーの役割が進展していく可能性は充分あり、これに伴い社会通念が変容していく可能性もある。海上保険の事故においては、複数の危険の要因が競合することも多く、保険関係者はサイバーリスクおよび戦争リスクに関する知識を常にアップデートしておくことが求められよう。

以上

ご清聴ありがとうございました。

新谷　哲之介（しんや　てつのすけ）
東京海上日動火災保険株式会社
海上業務部　貨物業務グループ　専門次長
東京都千代田区大手町2-6-4 常盤橋タワー27階
TEL 03-6704-4113
tetsunosuke.shinya@tmnf.jp