【米国保険法判例】

サイバー攻撃、サイバーセキュリティ、そして経済安全保障…？立ち止まって考える

大江橋法律事務所 外国法事務弁護士
橋本 豪
▶ PROFILE
go.hashimoto@ohebashi.com

第1 はじめに

経済安全保障をめぐる議論が喧しくなっています。第二次世界大戦後、経済活動に注力し、「平和ボケ」ともいわれるほど安全保障について真剣な議論をする必要を回避してきた、又はそうすることが可能であった我が国においても、昨令和4年に「経済施策を一体的に講ずることによる安全保障の確保の推進に関する法律（経済安全保障推進法）」[注)1]が成立し、経済安全保障に関する議論も百家争鳴の様相を呈してきています。そして、そのような経済安全保障をめぐる議論において、サイバーセキュリティに関するそれが重要な部分を占めていることに、恐らく異論はないでしょう。

筆者は、米国において長期にわたり法律実務に米国の弁護士として従事いたしました。そして、そこでの陪審裁判を含む訴訟の経験を通じ、法律と技術の交錯について考える機会を得たのち日本に戻り、我が国におけるサイバーセキュリティに関する議論の黎明期から、いろいろなかたちでそこに関わる機会を頂戴してきました。そのような経験を踏まえると、経済安全保障に関する議論の活発化と、そこでのサイバーセキュリティの重要性に関する認識の浸透を見るにつけ、まさに隔世の感を覚えます。

しかしながら一方で、日本と米国との間で実務に携わってきた身としては、サイバーセキュリティに関する議論が急速に進展しつつある今、日本としては米国を中心とする海外でのサイバーセキュリティに関する情勢の展開に追い付くことに精一杯で、次々に導入される新しい概念についての理解が追い付いていないのではないか、と感じられることが無いわけではありません。筆者の経験に拠れば、そのような場合に大切なことは、概念の解説に触れそれを咀嚼するとともに、事実を自ら確認する、ということであるように思われます。

そこで、本稿においては、サイバーセキュリティに関する論点のうち民間企業の経済活動に関するものに焦点を当て、民間企業がサイバー攻撃を受けた際に対応策の一つとして重要となる、サイバー保険に関する米国の近時の判例について紹介いたします。そうすることにより、民間企業にとって、また国家経済にとって、サイバー攻撃がどのような脅威を与え、サイバーセキュリティがなぜ重要なのかを浮き彫りにするとともに、サイバーセキュリティの安全保障における位置づけについても考えてみたいと思います。

本稿のニュースレターとしての性格に鑑み、参照した文献等は、直接に名称やその内容を言及、引用する場合を除き、文中に注を設けることはせず、文末に「参考文献等」として列挙しました。本稿内の特定の記述についてより詳細な説明をお望みの場合には、ご遠慮なくご連絡を頂戴できれば幸いです。また、本稿の内容は筆者個人の意見であり、その内容についての責任はひとり筆者の身にあることは、勿論であります。

注)1　令和4年法律第43号。

第2 米国におけるサイバー攻撃と保険

「サイバー犯罪」、「サイバーテロ」、「サイバー戦争」など、サイバー空間における脅威については、明確な定義がなされているとは言い難いにもかかわらず、いろいろな言及のされ方があり、国内法、国際法それぞれとの関係で誤解をはらみ得る用語法も多く見られます。それぞれに関する分析と論評を行い、正確な用語法を提案することは、そもそもそれが可能であったとしても本稿の射程を超えるので、ここでは、サイバー空間における脅威全般について、暫定的にこれを「サイバー攻撃」と称することといたします。

企業がサイバー攻撃を受けそれにより損害が生じた場合には、どのような対処が考えられるでしょうか。もちろん、その損害により、個人を含め当該企業の顧客に損害が生ずる場合もあるでしょうから、その場合にはそのような第三者に対する補償を行わねばならないでしょう。また、監督官庁をはじめとする諸方への連絡も必要となってくるでしょう。一方、当該企業が営利企業として存続し発展していくためには、そのような損害のうち少なくとも経済的な損害については、それが何らかのかたちで補填されることが望ましいことも、十分に理解されることと思われます。

そのためには、サイバー攻撃を行った攻撃者を特定し、その攻撃者を刑事罰に処し、またそれに対して求償できることが解決策としては最も簡明であること、これも異論はないでしょう。ここで、サイバー攻撃の特徴として指摘される、アトリビューション（“attribution”、攻撃者の特定）の困難さが立ちはだかることとなります。すなわち、サイバー攻撃を行った攻撃者の特定は、少なくとも現段階では技術的にも困難を伴うので、結果として、損害を生じさせた行為者に対する刑事罰の適用も民事上の損害賠償の請求も、実効性を持ちにくいものとなってしまうのです。

そのため、いわゆるサイバー保険という解決策が注目されることとなります。そこで、本稿においては、米国弁護士である筆者が分析している米国のそれについて見てみることといたします。まず、サイバー攻撃による損害をカバーするにあたっては、米国においては、いわゆる戦争・テロ保険（“war and terrorism risk insurance”）またはテロリズム保険と呼ばれるもの[注)2]の適用があるかどうかが検討されることとなります。これについては、米国の保険業界の団体であるIII（“Insurance Information Institute”）のウェブサイトに簡明な記述があります[注)3]。それによると、一般論としては、サイバー攻撃によって様々な損害が生ずる可能性があることは認識されている一方、それが物理的な損害を生じさせることはまれであると理解されているため、サイバー攻撃は“violent”ではないから「テロ行為」ではなく、そのため戦争・テロ保険に拠ってそこから生ずる損害もカバーされない、と理解されているようです。従って、サイバー攻撃から生ずる損害をカバーしようとすると、別途サイバー保険（“cyber insurance”）を購入する必要がある、ということになる場合がほとんどであるとされています。

ここで、上述の「テロ行為」の定義については、紙幅の関係もあり背景についての説明を省略しましたが、それ自体も、サイバー攻撃も含め時代とともに変容を遂げていくものであろうと思われます。本稿においては、これまで、“Terrorism Risk Insurance Act of 2002”（“TRIA”）や“Terrorism Risk Insurance Program Reauthorization Act of 2015”（“TRIPRA”）といった連邦法や多くの判例などにより、“terrorism”、“acts of terror”などの定義がなされてきており、精緻に理論化がなされていること、サイバー攻撃の増加に伴い、立法論的観点からの議論も盛んにおこなわれており、そこではテロ行為の定義の再考を迫る議論も一定数あることを指摘するにとどめたいと思います。

注)2　多様な名称が存在するものの、最も一般的と思われるこの名称を本稿においては使用することとします。

注)3　*Does my business need terrorism insurance,* Insurance Information Institute
（https://www.iii.org/article/does-my-business-need-terrorism-insurance 2023年8月27日閲覧）

第3 米国におけるサイバー保険

サイバー保険には、サイバー攻撃の特性によって生ずる、付保可能性に関する難しさが存在します。それは、テロ保険にも通ずるものであろうと筆者は考えていますが、テロ保険に関してよく挙げられるのは、以下の三点です。

① 保険料率計算にあたって保険数理的判断を行うに必要な、損害の発生頻度と損害の重大性に関する歴史的なデータが不足していること。
② テロは意図をもって故意に行われるため、付保可能なリスクの特性とされる偶然性（“fortuity”）を欠くこと。
③ テロによる損害は、地理的に集中することがあり得、保険によるリスクの社会化を阻害しかねない要因となりうること。

ご覧いただくと、上記のテロリズム保険にまつわる困難さは、サイバー保険にも当てはまることが見て取れるかと思います。

それでは、そういった困難さを内包するサイバー保険ですが、米国におけるサイバー保険は何をカバーするのでしょうか。例えば、大手損害保険会社のChubbのウェブサイトに拠れば、以下のような付保の範囲が想定されています[注)4]。

(1) 被保険者の付保範囲

① 弁護士費用、デジタルフォレンジック費用、監督官庁等への通知費用、クレジットスコアの監視、PR関係費用等。
② サイバーインシデントにより生じたビジネスの中断にかかる諸費用と逸失利益。
③ 消失したまたは毀損した電子データやソフトウェアの回復や代替に関する費用。
④ 強要された支払やサイバーインシデントによる問題の解決のための交渉に関する費用。

(2) 第三者に対する責任の付保範囲

① ネットワークセキュリティ不全と個人情報、機密情報漏洩に関する責任。
② サイバーインシデントにより生ずる支払用カード関連の契約上の支払責任。
③ 監督官庁に対して生じる罰金や課徴金（ただし、法律上許容される限度内）。
④ 名誉毀損や知的財産権侵害から生じるメディア関連の費用。

(3) サイバー犯罪（裏書条項による）

① コンピュータ詐欺による被保険者のコンピュータを経由した金銭的損失。
② 被保険者の銀行口座からの詐欺的資金移動。
③ 被保険者の従業員を誤信させて行わせる資金移動。

日本の場合、損害保険協会のウェブサイトに日本におけるサイバー保険の典型的な付保範囲の説明がありますが、付保範囲については、日米で似通ったものであると言ってよさそうです。

そして、このようなサイバー保険にも、戦争除外条項または戦争免責条項が含まれていることがほとんどです。戦争免責条項とは、保険料率の算定が難しく損害も巨額となりがちな戦争による損害を付保対象から除く、という保険約款上の条項であり、多くの保険約款に含まれているのが通常です。この戦争免責条項を巡って近年米国において訴訟が発生しており、判例も見られるようになってきているので、次節においてはそのような判例について見てみることといたします。

注)4 *Cyber Insurance Coverage & Products*, Chubb (https://www.chubb.com/us-en/business-insurance/products/cyber-insurance/cyber-insurance-products.html 2023年8月27日閲覧)

第4 近時の判例

2017年に、ロシアの政府機関であるロシア連邦軍参謀本部情報総局（“GRU”、ロシア語では“Главное разведывательное управление”）によるものとされる、“NotPetya”と呼ばれるランサムウェアを装ったマルウェア注)5による攻撃が行われ、全世界で、30億ドル超とも100億ドル超ともいわれる被害が発生しました。このマルウェアによる被害を受けた企業により、米国においてサイバー保険約款に基づく保険金の支払請求がなされたところ、保険会社側が戦争免責条項を理由として保険金の支払いを拒絶するということが起きており、それを巡って訴訟が提起されているのです。

その中でも注目を集めたものとして、オレオやリッツのクラッカーなどのブランドを有する、世界有数の食品コングロマリットであるMondelezが提起した訴訟注)6と、製薬会社であるMerckが提起した訴訟注)7とがあります。そのうち、Mondelezの事件については和解が成立した一方、Merckの事件については、事実審と上訴審で判決が下されているため、ここでは、Merckの事件について、判決の戦争免責条項に関する部分について見てみましょう。

この事件の事実関係ですが、Merckがウクライナ企業の開発した会計ソフトウェアを利用していたところ、実はそのソフトウェアにNotPetyaが仕込んであった結果、40,000万台以上のコンピュータが当該マルウェアに感染し、データ喪失などの損害を被ったというもので、本判決により、Merckは約14億ドル（1ドル＝145円の為替レートで約2,030億円）の賠償請求を認められました。

争点となったのは、Merckが購入していたサイバー保険の約款中にあった、以下の戦争免責条項でした。

“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.”

この文言をもって、保険会社側は、ロシア政府機関（GRU）が関与していたNotPetyaに拠るサイバー攻撃は、“hostile or warlike action”にあたる、とし、サイバー保険適用が除外されると主張しました。それに対して判決は、当該文言の通常の意味（“plain meaning”）によれば、この戦争免責条項がサイバー攻撃をその対象とするものでなかったことは明らかである、としたうえで、本保険が全危険担保保険（“all-risk insurance”）であったことを指摘し、戦争免責条項の適用を否定しました。

この判決の意味するところは何でしょうか。被保険者に有利な判決が出されたことで、事業会社がさらされているサイバー攻撃の脅威に対する有効な手立てが確保された、ということを意味する

注)5 「ランサムウェアを装ったマルウェア」との表現は、NotPetyaが身代金を要求するにもかかわらず、身代金の支払い後にあっても、復号によりデータの回復ができないように設計されていたことによります。
注)6 Mondelez International, Inc. v. Zurich Insurance Company (https://s3.documentcloud.org/documents/5759256/3972657 56-Mondelez-Zurich.pdf (October 10, 2018) 2023年9月11日閲覧)
注)7 Merck v. Ace American Insurance Company et al. (https://s3.documentcloud.org/documents/21183337/merck-v-ace-american.pdf (December 6, 2021)または https://www.njcourts.gov/system/files/court-opinions/2023/a1879-21a1882-21.pdf 2023年9月11日閲覧)

のでしょうか。筆者は必ずしもそうではないのではないか、と考えています。例えば保険料率の動きを見てみると、本年後半に落ち着きを見せる見通しとは言われているものの、それでも保険料率は近年騰勢を保っており、そこにはサイバー保険に対する旺盛な需要とともに、サイバー保険のもとでの保険金の支払の増減が重要なファクターとして介在していることは疑いないでしょう。

従って、被保険者への保険料支払いがより広範に認められることによって保険料が騰貴することは、十分想定し得ることであると考えられます。そうであれば、保険料の支払いの増加が保険料の上昇を招き、それによりサイバー保険購入がより困難になるというかたちで、企業側の負担が増大するという負の影響も考えておかねばならないということではないでしょうか。次節では結びに変えて、サイバー保険を巡るこのような展開が、経済安全保障との関わりで何を意味するのかについて、若干の考察を試みたいと思います。

第5 サイバーセキュリティと安全保障

上記のとおり、サイバー攻撃による被害がより広範に意識されるようになり、また損害の規模も拡大していく結果保険料が上昇すると、本来であればサイバー保険を購入し被保険者となるべき企業が、そのすべを失ってしまうという可能性について考えてみました。その結果、このように影響を受けた企業は、サイバー攻撃の脅威にさらされながらも、それに対する有効な経済的手立てを奪われることになります。それはとりもなおさず、それらの企業の活動に萎縮効果をもたらすこととなり、中長期的にはこれら企業が存在する国家の国力を削いでいく、ということになるでしょう。

そして、これがまさにいわゆるグレーゾーンにおける敵対的競争、とでも言うべき事態であると言ってよいのでしょう。その観点からすると、現在では、国家間の競争は武力を用いた国家間の争いや政治・外交といった手立てだけではなく、技術革新に伴って利用が可能となったサイバー攻撃といったツールまでを用いた、間断なき敵対的環境という様相を呈してきていると言ってよいでしょう。そして、今日においては、企業もそのような環境の中に否応なく巻き込まれていくこととなっており、それが経済安全保障を考えていく際の一つの重要な視点であると言えるのではないでしょうか。

本稿においては、サイバーセキュリティについて、経済安全保障という大きな枠組みの中でそれがどのように位置づけられるのかについて、若干の考察を試みました。サイバーセキュリティが良い例ですが、急速な事態の展開に追い付こうとするあまり、生硬なカタカナ語、外来語が氾濫し、その結果概念的な理解、咀嚼が不十分なままに、目前の事態を理解することが精一杯である、という方々も多いのではないでしょうか。その結果、大局を見ること、本質を見ることに困難が生じているとすれば、微力ながら、そこに一石を投じてみたいと筆者は考えています。まず、来年一月に、サイバー保険について、より詳細な論考を書籍（共著）のかたちで出版する予定であることを申し添えて、本稿を終えることとさせていただきます。

以上

《参考文献等》

書籍

- 堀田一吉、『現代リスクと保険理論』（東洋経済新報社 2014年）
- 近見正彦・堀田一吉・江澤雅彦、『保険学（補訂版）』（有斐閣 2016年）
- 廣瀬陽子、『ハイブリッド戦争−ロシアの新しい国家戦略』（講談社 2021年）

論文等

- Nehal Patel, *Cyber and TRIA: Expanding the Definition of an "Act of Terrorism" to Include Cyber Attacks,* Duke Law & Technology Review, 19, 2020-2021, pp.23-42
- Baird Webel, *The Terrorism Risk Insurance Act（TRIA）*（Congressional Research Service, updated February 10, 2022 https://crsreports.congress.gov/product/pdf/IF/IF11090/5 2023年8月25日閲覧）
- Abraham, Kenneth S. and Daniel Schwarcz. *"Courting Disaster: The Underappreciated Risk of a Cyber Insurance Catastrophe."* Connecticut Insurance Law Journal, Vol. 27, no.2, Spring 2021, pp. 407-473.

ウェブ記事等

- 川口貴久、「国家が支援するランサムウェア:2017年のWannaCryとNotPetyaの意図に関する分析（前編）」（笹川平和財団、2021年3月19日）（https://www.spf.org/iina/articles/kawaguchi_02.html 2023年8月25日閲覧）
- 篠原拓也、「サイレントサイバーリスクの増大ーサイバーリスクの引き受けは、サイバー保険にとどまらない!?」（ニッセイ基礎研究所、2022年10月11日）

(https://www.nli-research.co.jp/report/detail/id=72584?pno=2&site=nli 2023年8月25日閲覧)
●濱田和博、「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(2022年12月)1−33ページ//(http://www.sonposoken.or.jp/reports/wp-content/uploads/2022/12/sonposokenreport141_1.pdf 2023年8月25日閲覧)。
●Kieren McCarthy, *Cyber-insurance shock: Zurich refuses to foot NotPetya ransomware clean-up bill – and claims it's 'an act of war'*, The Register (January 11, 2019)
(https://www.theregister.com/2019/01/11/notpetya_insurance_claim 2023年8月25日閲覧)
●Alexander Martin, *Mondelez and Zurich reach settlement in NotPetya cyberattack insurance suit* ,The Record (October 31, 2022)
(https://therecord.media/mondelez-and-zurich-reach-settlement-in-notpetya-cyberattack-insurance-suit 2023年8月27日閲覧)
●*Six Russian GRU Officers Charged in Connection with Worldwide Deployment of Destructive Malware and Other Disruptive Actions in Cyberspace*, Office of Public Affairs, US Dept. of Justice (October 19, 2020)
(https://www.justice.gov/opa/pr/six-russian-gru-officers-charged-connection-worldwide-deployment-destructive-malware-and 2023年8月25日閲覧)
●Angus Liu, *Merck entitled to $1.4B in cyberattack case after court rejects insurers' 'warlike action' claim ,* FIERCE Pharma (May 2, 2023)
(https://www.fiercepharma.com/pharma/merck-entitled-14b-payout-cyberattack-case-after-judge-refutes-insurers-warlike-action-claim 2023年8月25日閲覧)
●Jim Sams, *N.J. Appeals Court Rules War Exclusion Doesn't Apply to NotPetya Attack,* Claims Journal (May 4, 2023)
(https://www.claimsjournal.com/news/east/2023/05/04/316786.htm 2023年8月28日閲覧)
●*US Cyber Insurers See Favorable Premium Growth, Results in 2023,* FitchRatings (April 13, 2023)
(https://www.fitchratings.com/research/insurance/us-cyber-insurers-see-favorable-premium-growth-results-in-2023-13-04-2023 2023年8月24日閲覧)
●*Background on: Terrorism risk and insurance*, Insurance Information Institute
(https://www.iii.org/article/background-on-terrorism-risk-and-insurance 2023年8月27日閲覧)
●*Cyber Insurance Coverage & Products,* Chubb
(https://www.chubb.com/us-en/business-insurance/products/cyber-insurance/cyber-insurance-products.html) (2023年8月27日閲覧)
●*Cyber liability risks*, Insurance Information Institute
(https://www.iii.org/article/cyber-liability-risks 2023年8月27日閲覧)
●*Does my business need terrorism insurance,* Insurance Information Institute,
(https://www.iii.org/article/does-my-business-need-terrorism-insurance、2023年8月27日閲覧)
●*Five Facts to Know About History's Most Destructive Cyberattack,* HYPR (https://www.hypr.com/security-encyclopedia/notpetya 2023年8月27日閲覧)