サイバー傭兵を規制できるか
―サイバーセキュリティにおける企業の役割―

掲載日：2024 年 5 月 7 日

慶應義塾大学 SFC 研究所 上席所員
小宮山 功一朗

サイバー傭兵という問題

「サイバーセキュリティにおける企業の役割」を論ずるというと多くの読者は、企業をサイバー攻撃からいかに保護するのかについての議論を連想されるのではないだろうか。確かに、企業は多くのサイバー攻撃の被害者であり、またサイバー攻撃の舞台となるインフラを保有し、運営している。それだけにとどまらない。企業はまた、雇われて、サイバー攻撃を直接的・間接的に行うことがある。本稿はこれまで日本においてあまり意識されてこなかった、「私企業による営利目的のサイバー攻撃」という問題をとりあげ、その実情と規制へ向けた動きを紹介する。

インターネット黎明期から、サイバー攻撃を行う者は政治的なメッセージを発することを目的とした集団や、金銭の詐取を目的とした反社会的組織であることが多かった。そして 2010 年代からは国家が、自国の情報機関や軍隊にサイバー空間上での活動を命ずるようになった。目的は治安の維持、国家安全保障上の要請に応えるなど様々である。

反社会的集団や犯罪グループによるサイバー攻撃については、それらを規制するための国際条約の議論が行われ、国際的な犯罪グループ摘発の協調が東西を超えて行われている。情報機関や軍隊が自ら遂行するサイバー作戦については、既存の国際法がサイバー空間にも適用されるという、世界に共通の理解を土台にして、国家の責任を明確化するための議論が活発に行われている。

日本においても、2022 年 12 月の新国家安全保障戦略策定以降、そこに実現すると謳われた「能動的サイバー防御」を巡る議論が加速している。その中で、自衛隊や警察がサイバー空間でどのような活動を行うべきか、どのような活動が可能か、などが検討されている。ここでも国家の役割が中心的な関心であると言える。

そこに近年、企業がサイバー攻撃を直接的・間接的に実施するサイバー傭兵という新たな問題が浮上してきた。例えば 2024 年 2 月に中国の i-soon(上海安洵)という企業の内部文書が何者かによってリークされた[1]。その内容によれば、同社は中国の公安部や情報機関に対して、様々なサービスを販売していた。取得した大量のメールの送受信記録から人物間の関係を分析するソフトウェア、Twitter(X)での投稿を大規模に監視し分析するためのソフトウェア、対象者のパソコンを遠隔から気づかれずに操作するソフトウェアなどである。リーク文書には米国、英国、NATO、タイ、カンボジア、パキスタン、モンゴル、ネパール、エジプトなど多数の国名と、標的となる組織（政府組織、大学・研究機関）の名前が挙がっていた。これらのソフトウェアが中国国外の組織に対して実際使われ、情報が盗まれていたことを強く疑わせる。日本の警察やサイバーセキュリティ対策組織がこれまで対応してきた、中国発とみられるサイバー攻撃のいくつかも、i-soon 社のような企業が開発し、実際に運用していた可能性がある。

高度な技術を持つこのようなサイバー企業はサイバー傭兵(Cyber Mercenary)と呼ばれ[2]、それがもたらす国家間の相互不信や緊張について一部の研究者が警鐘を鳴らしてきた。本稿はサイバー傭兵がサイバー空間の安定にどのような影響をもたらしているかを述べ、その上でその規制へ向けた動きを紹介する。

被害者であり、中立の舞台であり、サイバー傭兵である企業

本稿の分析において、企業は 3 つの役割を部分的に、あるいは同時に担っていることとする。3 つの役割とはすなわち、被害者であり、中立の舞台の提供者であり、サイバー傭兵である。順に説明する。

いうまでもなく、企業はサイバー攻撃の被害者である。そもそも、軍隊と軍隊が正対し正面から交戦することが減ってきており、サイバー空間においてはその傾向が顕著である。したがって、サイバー空間における戦いは、相互に相手側の重要なインフラに対してのサイバー攻撃を行うという形がとられる。重要なインフラとは、時に携帯電話網であったり、金融

[1] Sharwood, Simon. 2024. “Giant Leak Reveals Chinese Infosec Vendor I-Soon Is One of Beijing’s Cyber-Attackers for Hire.” The Register. Retrieved March 8, 2024 (https://www.theregister.com/2024/02/22/i_soon_china_infosec_leak/).

[2] Maurer, Tim. 2017. Cyber Mercenaries - The State, Hackers, and Power -. Cambridge University Press.

システムだったりする。つまり重要なインフラを抱える企業は、サイバー空間における戦いの前線ともよべる場所にいる。2010 年に発覚したグーグルの中国支社に対する中国政府が支援したとされるサイバー攻撃、2014 年 11 月に発生した北朝鮮ハッカーのソニー・ピクチャーズ・エンタテインメントへの攻撃、2021 年 5 月の米国のコロニアルパイプラインへのランサムウェア攻撃など、企業に対する、国家が支援するサイバー攻撃の事例は枚挙に暇がない。企業は自らが持つ情報資産の価値の高さゆえに、被害を受け続けている。

同時に、企業はサイバー空間の多くのインフラを保有し、管理している。サイバー空間を巡る競争において、中立の舞台の提供者でもある。とりわけクラウドサービス、半導体などの電子部品、データセンター、通信回線などを提供するグローバル企業は、世界中に顧客を抱えている。彼らグローバル企業は、特定の国の国益を追求することが、必ずしも自社の利益とならないことを認識している。そのため米系企業であっても、中国系企業であっても、自らの中立性を対外的に強くアピールする傾向にある。

最後に、企業は、サイバー傭兵としてサイバー攻撃を実施することがある。サイバー傭兵としての企業の行動は、サイバー作戦の民営化と、商用スパイウェア販売という 2 つのサブカテゴリーに分けて考えたい。サイバー作戦の民営化は、国家が企業の持つ技術力などを必要とした場合に、フォースマルチプライヤーとしての参加要請をし、契約書を取り交わし、国家がその成果を監視するものである。この場合の企業は、国家にとってのエージェントである。後者の商用スパイウェア販売は、企業が様々なサイバー攻撃ツールを開発し、これを関係する機関、軍隊に販売するパターンである。本稿冒頭の中国 i-soon 社がその典型である。

サイバー作戦の民営化について、強く印象に残るのは 2010 年に発覚したスタックスネット事件である。米国サイバー軍、NSA とイスラエルが共同で準備したとされる、極めて高度なコンピューターウイルス「スタックスネット」が用いられ、イランのウラン濃縮施設の機器の誤動作を引き起こし、遠心分離機の物理的な破壊をもたらした。コンピューターウイルスが情報空間を超えて、物理的な被害をもたらしたという点で、大きな転換点だった。

このウイルスの作成には企業が加わったとみられている。作戦に用いられたコンピューターウイルスはファイルのサイズが大きく、技術的に高度な部分と、そうでない部分が混在した。解析者は少なくとも 3 つのグループが分担して作成したとみている[3]。ドイツ企業製の産業制御システムを欺き、遠心分離機を破壊する部分のプログラムは高度な技術を持つハッカーでなければ実現不可能なものであった。対して、ウイルスが定期的に攻撃者からの命令を

[3] Zetter, Kim. 2014. Countdown to Zero Day: STUXNET and the Launch of the World's First Digital Weapon. Crown Publishers.

受信したり、自身の痕跡を秘匿したりするための部分のプログラムは技術水準が低かった。後者は、現実の世界でいえば「的を選んで銃の引き金を引く」プログラムであり、軍が自ら開発せざるを得なかった、そして前者は軍が契約を結び、その道のエキスパートに開発を外注したと考えるのが自然である。

商用スパイウェアの拡散

スパイウェアとは本来コンピューター上で、ユーザにその存在を意識させることなく、例えば Web サイトの閲覧履歴等を収集するプログラムのことであった。最近では iPhone や Android などのスマートフォン上で動き、メッセージや写真などをこっそり外部に持ち出すだけでなく、GPS の位置情報を盗みだしたり、ユーザの知らないところでカメラを起動し動画を撮影したり、マイクを起動し録音をしたり、と機能が付加されている。

その情報収集能力の高さゆえに、ある国において、裁判所の命令に基づき、人身売買組織のメンバーのスマートフォンにスパイウェアを忍ばせ、組織の情報を一網打尽に得るといった使われ方をしていた。

商用スパイウェアの販売については、10 年ほど前から度々問題視されてきた。フランスやイタリアやイギリスの企業が、使い方によっては市民のプライバシーを侵害する、多くの国で利用が違法とされかねない侵入機能を持つソフトウェアを販売していたからだ。それらの企業が、もしソフトウェアを闇雲に販売すると、やがて言論の自由や思想の自由といった民主主義の根幹が掘り崩されかねないという懸念があった。

残念ながら懸念は現実のものとなる。おそらく、商用スパイウェアの販売価格が下がったのだろう、2018 年頃から、複数の途上国で商用スパイウェアの利用が確認された。とりわけイスラエル企業 NSO グループ社製(以下、NSO 社)のペガサススパイウェアという商用スパイウェアの利用拡大は顕著だった。

ペガサススパイウェアについて簡単に説明する。2019 年春、NSO 社は WhatsApp という世界的に人気のメッセージングアプリにセキュリティ上の問題を発見した。そして、この問題を攻撃するプログラムを作成した。通常のサイバー攻撃では、標的となる人物がメールやファイルを開かなければ攻撃は成功しない。しかし、WhatsApp の問題を利用すると標的となる人物が WhatsApp で通話のリクエストを受けるだけで、持ち主が何もしなくとも、監視のためのスパイウェアをスマートフォンにインストールされてしまう。NSO 社はこの

WhatsApp の問題にかこつけた侵入手法を含めて、同社の顧客であるところの各国政府に販売した。結果、ルワンダの野党リーダー、インドの法律家、スペイン・カタルーニャ州の政治家、トーゴの神職者など多くのジャーナリスト、人権活動家、政治家、宗教指導者が攻撃を受けた。

被害者の 1 人であるメキシコのジャーナリストによれば、このようなスパイウェアの被害は深刻である。彼女はメキシコ政府における汚職を長年調査しており、当局からの嫌がらせが日常的に行われている中で、ある日商用スパイウェアによる攻撃を受けた。「家族が危篤である」というメッセージにかかれていたリンクをクリックしたことがきっかけでペガサススパイウェアに感染した。メールやメッセージングアプリのやり取り、連絡先はもちろん写真までが盗み見された。調査報道をするジャーナリストにとって、内部情報などをもたらす協力者の保護と秘匿は生命線である。彼女がペガサススパイウェアを使った攻撃にあったという事実が明るみになった瞬間に、これまでの協力者は全て彼女との連絡を絶ち、以来彼女は取材困難な状態にある。

商用スパイウェア販売が世界各国で深刻な人権侵害を引き起こしているという批判に対して、NSO 社は「弊社の製品は、テロリストや犯罪者を追跡し、逮捕することに貢献している」と応じた。この言葉自体に嘘はないはずである。違法薬物取引、人身売買などの摘発のために、各国の法執行機関は、スパイウェアを必要としている。自国で類似の製品を開発する能力がない途上国において、このような製品が手に入ることは福音である。

一方で同社の、「製品は各国の政府にしか販売していない」という発言については、疑問の声が上がっている。メキシコで大手企業の食料品、飲料品をボイコットする活動をしている市民が軒並みペガサススパイウェアの攻撃を受けるなど、特定の企業や団体の利益のためにペガサススパイウェアが使用されるケースも確認されているからだ。

規制の取り組み

このような背景をふまえると、核兵器や生物化学兵器の不拡散と同様に、商用スパイウェアの不拡散の機運が高まることに大きな驚きはない。西側先進国も、「途上国において、治安維持のためにスパイウェアが必要なのはわかるが、濫用は看過できない。目立たないように使って欲しい」というのが本音ではなかろうか。

ペガサススパイウェアが契機となり、米国のバイデン政権は 2023 年 3 月に、一部の商用

スパイウェアの利用を禁ずる大統領令を出した[4]。本稿の文脈で言えば商用スパイウェア販売の規制である。大統領令は、外国製の商用スパイウェアを、米国政府が使用しないという方針を打ち出した。あわせて各省庁が保有する外国製の商用スパイウェアの情報の集約、商用スパイウェアを製造・販売している企業の調査などを命じている。

これに呼応する形で、2024 年 2 月に、英仏両国が共同で、ポール・モール・プロセス(Pall Mall Process)という、国と企業が一堂に会し、商用スパイウェアの責任ある利用の仕方を議論するための会議体を立ち上げた[5]。英仏の呼びかけに応じて、日本を含めた 27 の国や連合、メタやグーグルを含めた 14 の企業や団体、12 の市民団体がこの動きに賛同する旨を表明している。湾岸諸国や、実際に商用スパイウェアを開発している企業もこの動きに加わっているからだろうか、合意文書は「ポール・モール・プロセスを通じて、国家、市民社会、合法的なサイバーセキュリティ、および産業界の関係者による、合法的かつ責任ある使用のパラメータを探求することを決意する」としており、商用スパイウェアの規制という目的達成までには、壁がいくつもあることを感じさせる。

ポール・モール・プロセスは英仏両国が提案し、それに民間企業が同調したという見方は早計である。民間企業は、サイバー傭兵や商用スパイウェアの問題を以前から警告し続けていた。2018 年にマイクロソフトなどが中心となり、テックアコードという規範を提示した[6]。この規範の重要な点は「政府が仕掛けるサイバー攻撃は支援せず、自分たちの製品やサービスの改ざんあるいは悪用を防止する」という文書にあらわれるとおり、国家によるサイバー攻撃やサイバースパイ活動の増加を受けて、企業の中立性を保つための、線引きをしようとしている点にある。本稿執筆時点で、NEC、NTT、日立、パナソニック、シャープなどの日本企業も賛同し、議論に参画している。テックアコードに参加するような企業は、各国や国連などの議論の場で情報を提供し、議論の方向性に少なからず影響を与えている。

---

[4] Executive Order on Prohibition on Use by the United States Government of Commercial Spyware that Poses Risks to National Security | The White House https://www.whitehouse.gov/briefing-room/presidential-actions/2023/03/27/executive-order-on-prohibition-on-use-by-the-united-states-government-of-commercial-spyware-that-poses-risks-to-national-security/

[5] The Pall Mall Process. 2024. “The Pall Mall Process Joint Statement.” Retrieved March 3, 2024 (https://www.diplomatie.gouv.fr/en/french-foreign-policy/digital-diplomacy/news/article/the-pall-mall-process-tackling-the-proliferation-and-irresponsible-use-of).

[6] Cybersecurity Tech Accord. 2018. “Cybersecurity Tech Accord.” Retrieved December 4, 2019 (https://cybertechaccord.org/accord/).

日本の次の一手。まとめにかえて。

本稿では、サイバーセキュリティの世界における企業の役割の複雑化を指摘した。企業は、単に被害者であるだけでなく、時にインフラという中立の舞台の提供者であり、時にサイバー傭兵となることを解説した。サイバー傭兵はさらに、サイバー作戦の民営化を担うパターンと、企業が商用スパイウェアの販売供給に関与するパターンに分けて考えられると主張した。そしてサイバー傭兵を規制する動きが並行して動いていることを確認した。企業のコンソーシアムにおいて、英仏主導の多国間協議の場において、規制の議論が行われている。米国における大統領令発令もそのような機運に乗じたものだった。

最後に、サイバー傭兵について日本が留意すべき点について述べ、まとめにかえたい。

まず、能動的サイバー防御がどのようなものになるにせよ、日本はサイバー空間における商用スパイウェアの規制に、つまり軍縮に積極的に貢献するべきである。少なくとも現時点で攻撃的サイバー能力を持たない日本にとって、自国の安全を高めることにつながる。サイバー空間においても情報はなるべく自由に流通するべきであるし、あまつさえ人権の侵害は許されないという、当たり前の主張を繰り返していくことが必要である。岐路の多い道のりにおいて、流されず本流を歩み続ける意志が求められる。

同時に、日本の安全保障の観点からは、サイバー傭兵規制に向かう主要国の動きを虚心坦懐にうけとめることも必要であろう。軍備縮小への動きは、残念ながら、世界の平和に直結しない。例えば 1923 年に米英日仏伊が戦艦や空母の保有比率について合意したワシントン海軍軍縮条約がある。これによって艦船の建造競争を抑えるという明確な目標のもとに各国が条約に署名をした。しかしこの条約が、すでに戦術的に無用の長物と化していた軍艦を廃棄するにあたり、それが米国の財政と世界平和に同時に貢献するというストーリーを広めるための装置だったという見方もある[7]。軍縮が、あるいは規制が誰を利するのかを慎重に見極めたい。主要国が、このタイミングでサイバー傭兵の規制に向けて動いていることの裏に、もはやそれらの国においてサイバー傭兵を必要としない体制が確立済みであるから、と捉えることもできるのだから。

[7] 小野塚知二、 2014 年「第 5 章 戦間期海軍軍縮の戦術的前提―魚雷に注目して―」『軍縮と武器移転の世界史』横井勝彦編、 日本経済評論社。

執筆者プロフィール

小宮山 功一朗（こみやま こういちろう）
慶應義塾大学 SFC 研究所 上席所員

専門分野はサイバーセキュリティと安全保障、サイバー空間の規範、インシデント対応組織 CSIRT など。JPCERT コーディネーションセンターの国際部部長として、セキュリティインシデント対応に従事する。著書に、『偽情報戦争　あなたの頭の中で起こる戦い』（共著、ウェッジ、2023 年）などがある。博士（政策・メディア）。