防衛研究所
The National Institute for Defense Studies

国家のサイバー攻撃とパブリック・アトリビューション

：ファイブ・アイズ諸国のアトリビューション連合と SolarWinds 事案対応

瀬戸 崇志　政策研究部グローバル安全保障研究室

NIDSコメンタリー
第 179 号　2021 年 7 月 15 日

はじめに：SolarWinds 事案にみる国家のサイバー攻撃と同盟国・同志国連携による対応

日本政府が 2021 年 5 月に公開した「次期サイバーセキュリティ戦略の骨子」（以下「次期 CS 戦略骨子」）は、国家安全保障政策の観点での情勢認識が特に注目される。同骨子の概要資料 4 頁では「サイバー空間は、地政学的緊張も反映した国家間競争の場となっている。中国・ロシア・北朝鮮は、サイバー能力の構築・増強を行い、その関与が疑われるサイバー攻撃を行っているとみられている。」とし、続けて「このようなサイバー攻撃やサイバー空間に関する国際ルール等を巡る対立等に対して同盟国・同志国等が連携して対抗している。」と明記した[1]。骨子本文 22 頁では「国家の関与が疑われるものも含め、サイバー空間における脅威について、平素から同盟国・同志国と連携し、政治・経済・技術・法律・外交その他の取り得る全ての有効な手段と能力を活用し、断固たる対応を取る。」とまで踏み込んだ[2]。

本稿では、国家の関与が疑われるサイバー攻撃[3]への政策対応の中で、各国政府が実施するパブリック・アトリビューション（public attribution）と呼ばれる取り組みに着目し、直近の海外事例も含めて動向と論点を分析する。この取り組みは日本でも公安調査庁が 2021 年 3 月に紹介したほか、同年 4 月の警視庁による中国系ハッカー集団 Tick の協力者の書類送検や、5 月の「次期 CS 戦略骨子」の記述[4]などに照らしても、今後重要性を増す可能性がある。パブリック・アトリビューションは、日本では「特定」や「帰属」と訳されるサイバー攻撃のアトリビューション（attribution）の派生概念だが、特に近年の各国政府の動向や学術研究の発展ぶりを把握するうえで有益となる。そのため、あえてパブリック・アトリビューションの概念を用いて、今後の論点整理を試みる。

直近の事例として、米国の IT 企業 SolarWinds のネットワーク管理ソフト Orion Platform の更新プログラムに偽装したマルウェア（悪意のあるプログラム・コードの総称）により、米国を中心に世界各国に影響を与えた SolarWinds 事案への対応に着目する。同事案は 2020 年 12 月上旬に発覚し、約 5 か月後の 2021 年 4 月 15 日に米国と英国がロシア対外諜報庁（SVR）の関与を非難し、米国が経済制裁を発動した点は日本でも知られる[5]。しかし、実は 4 月 15 日から翌 16 日の 2 日間で、カナダ[6]、オーストラリア[7]、ニュージーランド[8]もロシア政府の責任を同時に非難している（ロシア政府は事案への関与を否認した）。この 5 か国はインテリジェンス機関の相互協力の枠組みを有し、日本でもファイブ・アイズ（Five Eyes）の通称で知られる（以下ファイブ・アイズ諸国）[9]。

このファイブ・アイズ諸国を軸とした同盟国・同志国連携（以下同志国連携）による SolarWinds 事案への対応は、近年の研究ではアトリビューション連合（attribution coalition）[10]とも呼ばれるパブリック・アトリビューションの実施方式の特徴を備える。以下ではパブリック・アトリビューションをめぐる各国の政策動向や、近年の学術研究の展開などを整理し、アトリビューション連合による SolarWinds 事案対応の特徴や論点を分析する。

1.　パブリック・アトリビューション：「誰がやったのか」の（非）公表とコミュニケーション

スイス工科大学のエグロフ（Florian Egloff）とスミート（Max Smeets）の共同研究は、パブリック・アトリビューションを「悪意あるサイバー空間における活動の使用機器、特定の攻撃の実行者、そして最終的な責任を有する敵対国（responsible adversary）の情報を公表する行為[11]」と定義した。「パブリック」とは攻撃の実行者やその背後にいる国家の「公表」を意味し、民間企業や研究者も行い得る[12]。ただし、この概念が「公的機関の対応」を念頭に議論されることもある。例えば 2021 年 3 月、日本の公安調査庁の刊行物は「攻撃実行者と背後にいる国家機関を特定した上で、公開の場（起訴や制裁を含む）で当該国を名指しで非難する（中略）取組[13]」とし、米国や英国

をはじめとする各国政府によるパブリック・アトリビューションの事例を紹介している。

パブリック・アトリビューションの定義には、先行研究上も依然論争がある。本稿の趣旨からは各国の政策対応に焦点を当て、論点整理のため概念の射程を広めにとりたい。以下では、パブリック・アトリビューションを「各国政府が、サイバー攻撃の実行者（以下攻撃者）ないしは責任を負う国家（以下攻撃国）を名指しする政治的判断を公表し、そのうえで必要に応じ、関連情報の公表や、相手方への非難や懸念の表明などを伴う政策対応」として議論する。各国が攻撃者や攻撃国を名指しする政治的な判断（judgement）の公表を重視し、判断の裏付けとなる証拠の多寡や非難の文言は問わず、また同志国の情報（評価）を参照し相手方を名指しする対応も含む[14]。ただし各国が、自らは攻撃者や攻撃国を名指しせず、攻撃の被害国や同志国の立場への支持や連帯（solidarity）の表明にとどめる程度の対応（以下支持・連帯表明）は、パブリック・アトリビューションとは区別して扱う。

各国政府のパブリック・アトリビューションは、基本的には攻撃者や攻撃国に対する非難や懸念を示す声明（以下公式非難声明）の形を取るが、必ずしも公式非難声明にのみ形式が限定されるわけではない。例えば米国の国際法学者であるアイケンサー（Kristen Eichensehr）は、米国政府の対応を例に、政府機関が公表するサイバー攻撃の手口の情報と注意喚起（以下脅威情報アラート）、攻撃者の刑事訴追、攻撃に関与した他国政府機関の関係者や関係法人の資産凍結・渡航禁止などのスマートサンクション（以下制裁）など、公式非難声明に続く政策対応とも一体化し攻撃者や攻撃国を名指しする行為も類型に含む[15]。本稿でも公式非難声明のほかに、上記の類型も含めて議論する。ただし刑事訴追や制裁を概念の射程に含み得るかは論争があり、この点は第 2 節で触れる。

パブリック・アトリビューションは、アトリビューションの派生概念である。アトリビューションとは、攻撃の痕跡や手法などの技術的解析から、攻撃者の意図をめぐる地政学的背景まで、多様な状況証拠の収集と分析を通じ、匿名性が高いサイバー攻撃の攻撃者や背後の攻撃国を特定（判断）していくプロセスである[16]。日本では「特定」や「帰属」とも訳され、「誰がやったのか（who did it）」の問題と呼ばれてきた[17]。やや単純化すれば、パブリック・アトリビューションは「誰がやったのか」の判断の公表と、攻撃者や第三者とのコミュニケーションに着目する。主な学術研究も判断の公表やコミュニケーションをアトリビューションの一部に含め議論してきたが[18]、近年パブリック・アトリビューションが派生概念として登場した背景には、次の 2 つの要因が指摘できる。

第 1 に、国家の関与が疑われるサイバー攻撃に対する各国政府のパブリック・アトリビューションの活発化である。後でみる通り、この取り組みは特に 2017 年以降、平素からの同志国連携の形で実施される傾向を強めた[19]。その後、2018 年 9 月の米国の「国家サイバー戦略[20]」、同年 11 月のオランダの「国防サイバー戦略 2018[21]」、2021 年 4 月のオーストラリアの「サイバー・重要技術国際関与戦略[22]」など、政府のサイバーセキュリティ戦略で、パブリック・アトリビューションや同趣旨の用語を政策手段の 1 つと明記する国家も登場する。パブリック・アトリビューション概念の登場は、攻撃者や攻撃国の公表を政策手段とみる近年の各国政府の認識を反映する。

第 2 に、アトリビューションの結果の公表、または非公表の事例増加に応じた学術研究の発展である。近年では（困難かつ時間を要するにせよ）民間のセキュリティ専門家または被害国政府によって、サイバー攻撃に対する特定国の関与が指摘される事例は増加傾向にある[23]。しかし、攻撃発覚から時間が経過し、民間企業や専門家の調査、関係者のリークを含む報道を通じ、特定の国家の攻撃への関与を強く示唆する情報が公開された後も、被害国政府が攻撃者や攻撃国をめぐる公式の判断の公表や非難を控えることがある[24]。また、国境をまたぐサイバー攻撃事案の被害国間で、アトリビューションの結果の公表の有無や非難の文言に差が出ること[25]や、その逆に自国の被害や保持する証拠が乏しい国が、同志国の情報（評価）に依拠して攻撃者や攻撃国を非難する事例[26]もある。

こうした事例を受け、近年の主要な学術研究では（1）攻撃の事実関係を立証する証拠の収集と分析による攻撃者や攻撃国の特定、特定結果やその根拠などの関連情報の公表、そして公表した結果に基づく相手方への非難は、時に別個の問題として存在し得ること、（2）各国政府と、企業などの非国家主体のアトリビューションの（非）公表は、それぞれ異なる独自の動機や機能が伴うこと、の 2 点を視座として有している[27]。そのうえで、学術研究におけるパブリック・アトリビューション概念は、アトリビューションの結果の公表や、その逆に意図的に公表しないことの動機と機能、さらには（非）公表をめぐる国内・対外政策過程の分析概念として用いられている。

2. ファイブ・アイズ諸国によるアトリビューション連合

2017 年以降、国家の関与が疑われるサイバー攻撃へのパブリック・アトリビューションは、これまでの主な実施国であった米国政府以外にも広がりをみせ、かつアドホックな同志国連携の形で実施される傾向を強めた。その先駆けは、2017 年 5 月のランサムウェア WannaCry の世界各国への感染拡大をうけて、約半年後の 2017 年 12 月 19 日から 20 日に、ファイブ・アイズ諸国・日本・デンマークが、Lazarus Group と呼ばれる攻撃者（集団）と、背後にいる北朝鮮政府の責任を非難した事例である。WannaCry 事案への対応後も、主にファイブ・アイズ諸国を中心に、同志国が時期を揃えて国家の関与が疑われるサイバー攻撃に対するパブリック・アトリビューションを行う取り組みは継続し、こうした傾向をして、近年の研究ではアトリビューション連合とも呼ばれる（表 1 参照）。

表 1：2017 年以降のアトリビューション連合の主要事例

対応の契機となった事案概要 [ ]内は攻撃の時期 （－は開始時期と発覚時期の差を示す）	連合の 形成時期	上段：名指しされた攻撃者と背後の攻撃国[※1] 中段：許容し得ない行為の性質（各国の声明要旨） 下段：公式非難声明や支持・連帯表明を発した国・機関 ：赤字：声明で攻撃者または攻撃国を名指しで非難 [※2][※3]	刑事訴追 制裁の同時提起 [※4] [※5]
WannaCry事案[2017年5月] ランサムウェアWannaCryが全世界150か国以上に感染拡大。英国国民保健サービスの機能停止や日本企業の欧州での事業にも影響。	2017年 12月19日-20日 （事案発生から） [約7か月後]	**北朝鮮（Lazarus Group→朝鮮人民軍偵察総局）** **官民問わず無差別に破壊的影響をもたらす活動** **米・英・加・豪・ニュージーランド**（以下NZ）・**日**・**デンマーク**	× **（時間差で提起）** 米：訴追（2018年6月） 米：制裁（2018年9月） EU-英：制裁（2020年7月）
NotPetya事案[2017年6月] ウクライナの重要インフラへの攻撃が主目的と見られたマルウェアNotPetyaが、欧州はじめ各国に感染拡大。米国の物流大手やデンマークの海運大手などにも甚大な損害。	2018年2月 2月15日-16日 （事案発生から） [約8か月後]	**ロシア（ロシア軍 ※18年2月発表時点。米英は後にSandworm→GRUと断定）** **官民問わず無差別に破壊的影響をもたらす活動** **米・英**・加（※）・**豪**・NZ（※）・**デンマーク**・ノルウェー・**エストニア**・**ラトビア**・**リトアニア**など （※加・NZは攻撃への非難は行いつつも、攻撃者や攻撃国を名指しせず）。	× **（時間差で提起）** 米：制裁（2018年3月） 米：訴追（2020年10月） EU-英：制裁（2020年7月）
化学兵器禁止機関（OPCW）事案[2018年4月] 2018年4月、同年3月の英国内での化学兵器使用事案の調査を担当していたハーグの化学兵器禁止機関（OPCW）事務局に、何者かが施設近傍からハッキングを試行。蘭政府の防諜部門が犯行現場を急襲し、実行犯の身柄を拘束して物的証拠を押収。押収した証拠などから、実行犯は過去にも複数のサイバー攻撃に従事したロシアのインテリジェンス機関の要員と判明（実行犯は18年4月に国外追放となった）。	2018年 10月4日-5日 （事案発生から） [約6か月後]	**ロシア（APT28 →ロシア連邦軍参謀本部情報総局[GRU]）** **国際機関や民主的政治過程への干渉** **英**・**蘭**・仏・**デンマーク**・フィンランド・ノルウェー・**エストニア**・**ラトビア**・**ポーランド**・**スロヴァキア**・**EU**・**NATO**など **米・英・加・豪・NZ のみ**：2016年以降の世界反ドーピング機関（WADA）への攻撃、国際サッカー連盟（FIFA）への攻撃、米国大統領選挙への干渉など、OPCW事案のほかにも、過去に行われた国際機関や民主的政治過程へのサイバー攻撃事案も抱き合わせで、APT28とGRUの責任を公式に断定し名指しで非難。	△ **（米国のみ同時）** 米：訴追（2018年10月） 米：制裁（2018年12月） EU-英：制裁（2020年7月）
APT10事案[2016年－2017年頃]（※諸説あり） 中国系ハッカー集団APT10による、各国の民間企業が利用するクラウド・サービスを踏み台にした大規模サイバー知財窃取（通称クラウド・ホッパー作戦）。発生・発覚時期は諸説あるが、特に2016年から2017年にかけて活発化し、遅くとも2017年4月には民間企業の調査がAPT10の関与を指摘。少なくとも世界12か国以上の防衛産業などを標的に展開。	2018年 12月20日-21日 （事案発覚から） [1年以上後]	**中国（APT10→中国国家安全部[MSS]）** **産業競争力強化目的の民間企業の知財窃取（国家の産業スパイ活動）** **米・英・加・豪・NZ・日・独・蘭・デンマーク**・フィンランド・スウェーデン・ポーランド	△ **（米国のみ同時）** 米：訴追（2018年12月） EU-英：制裁（2020年7月）
ジョージア事案[2019年10月] ジョージア（旧グルジア）で予定されていた議会選挙に先立ち、2019年10月末に同国の政府機関・国営放送・NGOなどを標的に行われた大規模なDDoS攻撃事案。同国内でのTV放送や政府のHPの閲覧などに大規模な障害が発生。	2020年 2月20日-21日 （事案発生から） [約4か月後]	**ロシア（Sandworm→GRU）** **民主的政治過程への干渉や主権の毀損を伴う破壊活動** **米・英・加・豪・NZ・蘭・デンマーク**・ノルウェー・**エストニア**・**リトアニア**・**ポーランド**・**チェコ**・**ウクライナ**・**ジョージア**・EU（※）など （※EUは攻撃への非難は行いつつも、攻撃者や攻撃国は名指しせず）	× **（時間差で提起）** 米:訴追（2020年10月）
SolarWinds事案[2020年3月－同年12月] 米国のIT企業SolarWindsの製品の更新プログラムに偽装したマルウェアSUNBURSTの世界各国への感染拡大と大規模情報窃取の総称。SUNBURSTの拡散は2020年3月から開始され、同年12月に発覚した。ただし、攻撃者による実際の情報窃取の被害は、米国を中心とした政府機関やセキュリティ企業などの重要目標に限定されたとの分析も存在。	2021年 4月15日-16日 （事案発覚から） [約5か月後]	**ロシア（APT29 →ロシア対外諜報庁[SVR]）** **民間企業が大規模な巻き添え被害を被るサイバー諜報（？）** **米・英・加・豪・NZ**・フランス・**デンマーク**・フィンランド・**エストニア**・**ラトビア**・**リトアニア**・**ポーランド**・ルーマニア・EU・NATOなど	△ **（米国のみ同時）** 米:制裁（2021年4月）

[※1]全ての事例で、名指しされた国家は、攻撃への関与を否認している。また名指しされた**攻撃者（グループ）**につき、**複数の名称がするものは最も著名な名称を記載。**
[※2]各国や国際機関の声明は、閣僚声明や報道発表のほか、政府機関や閣僚・各国大使の公式Twitterを経由して発出されたものも含む。2021年7月現在、インターネット上で1次資料にアクセスが可能な国・機関の名称のみを明記し、複数の2次資料でのみ確認できる公式非難声明などの発出国が存在する場合には、「など」として表内に含めている。
[※3]先行研究において、アトリビューション連合の事例におけるパブリック・アトリビューションと支持・連帯声明を区分する基準は確立していない。そのため本稿では便宜上、**赤字**を**公式非難声明を通じたパブリック・アトリビューション**とみなす。**赤字**は、**原則**は（a）**自国が攻撃者や攻撃国を明確に名指しのうえで「非難（condemn）」や「懸念（concern）」を表明し、攻撃の停止や規範の遵守を求める**場合だが、**例外**として（b）ファイブ・アイズ諸国の**「アトリビューション（attribution）の結果を支持（support）」や「評価を共有（share assessment）」などの文言を声明で用いるか、ファイブ・アイズ諸国のアトリビューションの結果（URLなど）を引用しつつ、非難・懸念表明などを行う場合**も含む。他方で（c）**支持・連帯表明**は、攻撃者や攻撃国を明示せずに被害国や同志国の立場への支持や連帯や事案への憂慮を示したもの**とする。なお（b）を、（a）と（c）のいずれに含むか判断に迷う場合は（c）**の支持・連帯表明に準ずるものと扱い、表内に別途注釈**を付す。なお、**国際機関の声明も同様の基準で整理**するが、**欧州連合外務・安全保障政策上級代表声明など、公式制度上は当該機関や加盟国の（パブリック・）アトリビューションとは異なる地位を持つものも含む。**
[※4] EUのサイバー関連制裁制度は、加盟国共通のサイバー外交政策対応を定める「サイバー外交ツールボックス」に基づき、**2019年5月に制度が発効。**制裁対象の**EU加盟国圏内への渡航禁止や資産凍結**が主たる内容。**EU**は、**2020年7月**に**WannaCry事案、NotPetya事案、APT10事案、OPCW事案**に関与した**自然人と法人**に同制裁を初めて発動した（制裁対象には、GRU長官のコスチュコフ[Igor Kostyukov]氏や、GRUの特別技術メインセンター[GTsST: 別名GRU74455部隊]も含む）。制裁はEU規則であり加盟国は履行義務を有する。また**英国はBREXIT移行期より、EUの制裁を国内法で履行**してきた。
[※5]米国やEUの措置は例示であり、**訴追・制裁事由に問題となったサイバー攻撃事案を含むものに限る。**なお**訴追・制裁事由には、同一の攻撃者の過去の余罪や他の制裁事由も含まれることもある。**

出典：各国政府発表ならびに各種 2 次資料に基づき筆者作成（2 次資料は文末注[28]を参照）。

アトリビューション連合は、次の 3 つの特徴を持つ。第 1 に、ファイブ・アイズ諸国は、事案発覚から平均 5 か月から 7 か月程度の期間をあけ、攻撃者や攻撃国を名指しした公式非難声明を 1 日から 2 日以内で同時発表する（特に 5 か国は、攻撃国まで具体的に名指しする傾向が強い）。第 2 に、特にファイブ・アイズ諸国は、各国のインテリジェンス機関（対外情報機関や治安情報機関）が、攻撃国の特定から公式非難声明、さらには後述の攻撃手法の公表などのプロセスで重要な役割を果たす。第 3 に、他の同志国や国際機関（以下同志国・パートナー）も、ファイブ・アイズ諸国と同時期に攻撃者や攻撃国への公式非難声明を公表し、またはパブリック・アトリビュー

ションに至らずとも、5 か国の取り組みへの支持・連帯表明を行う。

このアトリビューション連合の特徴は、次の背景による。ファイブ・アイズ諸国は公開情報の分析と官民連携での情報共有に加え、5 か国のシギント（SIGINT：通信・電波傍受による諜報活動）で収集した機密情報や分析結果（評価）の共有を通じ、攻撃国特定の確度の向上や、公表までの時間短縮を試みている[29]。ただし、インテリジェンス機関の機密情報に依拠した攻撃国の特定は、その結果の公表段階で判断の根拠となった証拠の開示を難しくする。証拠開示は、他国に自国の水面下でのサイバー空間における諜報活動の手法を察知させるなどして、インテリジェンス機関の能力基盤を危険に晒すからである[30]。そのためファイブ・アイズ諸国は、攻撃国の特定結果を裏付ける詳細な証拠を開示できないなかで、公表した特定結果の信頼性を維持する必要があり、よって多くの同志国・パートナーにパブリック・アトリビューションや 5 か国の取り組みへの支持・連帯表明を求める[31]。

以上の点で、ファイブ・アイズ諸国にとっては、より多くの同志国・パートナーが 5 か国のパブリック・アトリビューションの結果（評価）を共有し、同様の対応を取ることが好ましい。しかし国により事案の被害状況や、特定国の攻撃への関与についての判断のための保有情報（とその評価）は異なり、相手国との外交関係もさまざまである。そのためファイブ・アイズ諸国は、おそらくアトリビューション連合形成時の同志国・パートナーの対応に裁量を認め、より多くの国・機関との連携を模索してきたとみられる。ファイブ・アイズ諸国以外の同志国・パートナーのパブリック・アトリビューションは、名指しの程度、根拠として公開する情報、非難の文言も異なり、また同志国・パートナーへの支持・連帯表明にとどめ、攻撃者や攻撃国への名指しは回避する例もある。

ここで、アトリビューション連合形成時のパブリック・アトリビューションの形式の問題にも触れておきたい。各国政府は、基本的に 1 日から 2 日以内に時期を揃えて公式非難声明を発出する。発出媒体は閣僚声明や報道官談話などのほか、政府機関や閣僚・各国大使の公式 SNS アカウントに声明を掲載することもある。すでに述べたとおり、パブリック・アトリビューションは、刑事訴追や制裁と一体化しても行い得る。しかし従来のアトリビューション連合の形成時には、刑事訴追や制裁を同時提起できる国は事実上米国のみであったし、この点でファイブ・アイズ諸国の間でも攻撃国への対応は完全には揃わない。

その背景の 1 つに、他国政府を名指しする公式非難声明と、刑事訴追および制裁との間で、次のように法的な実施条件が異なることが指摘できる。まず、相手国政府を直接名指しした非難は国際法で規律されるが、その際に要求される証拠の質や量をめぐる具体的な基準（証拠水準）や証拠開示の義務は確立していない[32]。そのため、攻撃国の特定でインテリジェンス機関の機密情報に依拠し、非難に際して証拠を開示しないことや、他国の情報（評価）に依拠した非難も可能となる[33]。他方で刑事訴追や制裁は、事実上は国家を名指ししても、国内法制度上は対象となる自然人や法人の基本権の制約を伴う手続となる。よって刑事訴追はもちろんのこと、制裁も対象者が反訴した場合には国内裁判所の司法審査に服し得る。その場合、被疑者や制裁対象の権利保障のために要求証拠水準が厳密となり、裁判所への証拠開示も求められる[34]。

つまり各国政府の刑事訴追や制裁は、原則としては司法審査に耐え得る緻密かつ公開可能な証拠を揃える必要がある[35]。国際司法共助や官民の情報共有などを通じた、長期間の捜査が必要となり、国によってサイバー攻撃被害や法執行機関や制裁実施官庁の入手可能な証拠に差があるなかで、アトリビューション連合形成時にすべての国がタイムリーに提起し得る措置ではない。この点との関連で、例えば 2019 年から発効したサイバー攻撃を事由とする EU 加盟国共通の制裁制度も、あくまでも自然人と法人が対象である。EU は、制裁が国家機関の関係者や関連法人を対象としても、EU とその加盟国による他国へのパブリック・アトリビューションを法的には意味しないとの立場を取る[36]。また、制裁は欧州連合司法裁判所（CJEU）の司法審査対象となり、制裁事由や証拠が不十分な場合は、違法ないしは取消対象ともなる[37]。このような実行に照らしても、刑事訴追や制裁をパブリック・アトリビューションの形式に含み得るか否かは、各国や専門家の間でもなお見解が分かれる。

3. パブリック・アトリビューションの主要機能：抑止、対処・防御、規範設定の 3 つの柱

単独実施か同志国連携かを問わず、特に攻撃国を名指ししたパブリック・アトリビューションは実施に伴い安全保障上のさまざまなコストとリスクを伴う。例えば証拠として開示する情報の種類や実施のタイミングによっては、パブリック・アトリビューションは自国や同志国の諜報活動の基盤を危険に晒す[38]。相手国を公然と非難することは、非難された国が攻撃者を積極的には支援していなかった場合、攻撃者を取り締まるための国際司法共助や、水面下の外交的な問題解決の可能性を狭めるし、相手国とのエスカレーション管理にも影響する[39]。

各国で実施のコストやリスクへの認識が異なるためか、パブリック・アトリビューションへの姿勢は基本的価値観を共有する国の間でも一枚岩ではない。アトリビューション連合への対応は G7 諸国間でも事案により是々非々であり、EU 加盟国間でも各国の脅威認識に応じ積極派と消極派が分かれる。この点でファイブ・アイズ諸国や、逆に EU 加盟国でもオランダやエストニアなどの積極姿勢の強い国家[40]は、パブリック・アトリビューションに明確な意義を見出し、アトリビューション連合を形成してきたとみられる。以下では単独実施か同志国連携かを問わず、「攻撃国」と「同志国以外の第三国」との関係でのパブリック・アトリビューションの主要機能を、3 点に絞り紹介する。なお自明ではあるが、アトリビューション連合の場合は同志国間の関係強化の側面もある[41]。

1 つ目の機能は、抑止である。相手方の意図（intentions）に働きかけ、将来の攻撃を思いとどまらせる機能であり、米・豪・蘭のサイバーセキュリティ戦略や日本政府の文書[42]でも、パブリック・アトリビューションの目的として記される。各国の文書の要諦は、攻撃国を名指しで非難すること、または非難を国際法上ないし政治的根拠とし、サイバー攻撃による反撃、刑事訴追や制裁、後述の攻撃手法の公表[43]など、あらゆる手段で相手方にコスト（cost）を課し続け、将来のサイバー攻撃を行う意図を挫くことにある。特に 2017 年は、サイバー空間に適用される国際規範を議論してきた国連の政府専門家会合（UNGGE）では、サイバー攻撃の被害国が国際法上取り得る対応の範囲をめぐる米国の同志国と中露との間の合意形成が失敗に終わる。それと同時に、国際法上の自衛権の行使要件たる武力攻撃（armed attack）の烈度には至らないが、なお看過し難いサイバー攻撃事案への対応が各国の喫緊の課題となった[44]。この時期に登場したアトリビューション連合とは、こうした武力攻撃の閾値以下のサイバー攻撃事案にも抑止を及ぼす取り組みでもあった。同志国連携を通じて、攻撃国に「武力攻撃の閾値以下の事案にも同志国は国際法に基づき対処し得る」と伝達し、同時に課し得るコストの総量を底上げする狙いがある[45]。

ただし抑止機能は、コストの強要で将来の行動を変化させる対象を「国家」とみた場合、次の懐疑論もある。例えば攻撃国への非難がコストとみる議論は、ネーム・アンド・シェーム（name and shame）と呼ばれる概念を念頭に、非難は攻撃国の国際社会での評判の低下に繋がり、それがコストのため将来の行動を変えるとの前提に立つ[46]。しかし、北朝鮮やロシアといった国際社会からの非難に耐性が強く、自国のサイバー空間での影響力顕示に誘因を持ち得る国には、非難がコストと認識されない可能性もある[47]。仮に、非難自体が攻撃国の行動を変えるコストにならない場合、制裁や攻撃手法の公表などの後続の政策対応がコストの源泉となる。この前提に立つ場合、各国が公式非難声明の後に、相手方がコストと認識し得る烈度の対応をとれない場合、攻撃国に「被害国は自国に十分なコストを課す能力と意思を欠く」とのシグナルを伝達し、むしろ抑止の信頼性を損ねかねない[48]。

2 つ目の機能は、対処・防御である。攻撃側の意図に作用して将来の行動を変える抑止の成否を問わず、相手が脅威を提起する能力（capabilities）自体の無力化や、攻撃の被害の軽減を目指す[49]。例えば米国や英国のインテリジェンス機関の発する脅威情報アラートは、攻撃国や、国家が運用に関与する「高度で持続的な脅威（Advanced Persistent Threats：以下 APT グループ）[50]」と呼ばれるグループを名指しのうえ、セキュリティ用語で「戦術・技術・手順（Tactics, Techniques and Procedures：以下 TTPs）[51]」とも呼ばれる攻撃手法を公表する。この取り組みは、攻撃国や APT グループの攻撃の動向や利用しうる対策手法を政府機関や民間企業のセキュリティ担当者に周知することで、各組織による現在の攻撃の検知と被害の局限や、将来の標的となり得る組織のセキュリティ対策の向上をうながす[52]。こうした TTPs の公表に加え、攻撃者の刑事訴追、攻撃国の外交官（身分のインテリジェンス・オフィサー）の国外追放は、サイバー攻撃を手段に含み、しばしば被害国内からも展開する攻撃国の諜報活動などを阻害するカウンターインテリジェンスの一環ともなる[53]。

3 つ目の機能は、規範設定である。各国による攻撃国への非難は、攻撃国が従事した特定のサイバー攻撃が、サイバー空間に適用される既存の国際法に照らして違法、または国連や G7 でも確認されてきた、責任ある国家の行動規範（norms of responsible state behavior）などに照らし、国際法上は合法であれ許容し得ないとの評価を示す[54]。国際政治学者のフィネモア（Martha Finnemore）と国際法学者のホリス（Duncan B Hollis）の研究によれば、こうした非難は既存の規範を実践し、新たな規範設定の布石となり、将来の慣習国際法の形成にも影響する[55]。

パブリック・アトリビューションの意義を規範設定機能でとらえた場合、制裁や詳細な TTPs の公表などの政策対応を伴わず、また仮に、非難それ自体が攻撃国のコストとはならない場合でも、相手国を名指しで非難することは一定の意義を持つ。なぜならばこの機能の本質は、侵害された規範やその遵守の必要性、さらに規範侵害に対し取り得る措置を、攻撃国以外も含む各国に周知することであり、その効果は非難した攻撃国の反応に左右されないからである[56]。なおサイバー空間をめぐる規範の範囲には各国間で論争があり、公式非難声明で国際法違反には触れずに、責任ある国家の行動規範の侵害や、より簡潔に「許容できない （unacceptable）」などの文言で攻撃国を非難する場合もある。よってパブリック・アトリビューションが設定する規範とは、既存の国際法に加え、国際法上は合法でも、国家の行為として許容し得ない一定のサイバー攻撃をめぐる共通理解も含む立場が強い[57]

そのような、合法であれ許容し得ないサイバー攻撃をめぐる共通理解も含めて、サイバー空間における規範の機能には次のとらえ方がある。第 1 に、規範が抑止やエスカレーション管理の前提となる機能を果たすとの議論である。例えばサイバー攻撃への抑止を論じる立場は、規範をレッドラインとみたて、規範侵害にコストを課し抑止が作用するとみる[58]。また米国では、国際法上の武力攻撃の閾値を超えない烈度のサイバー攻撃は抑止が困難とし、むしろサイバー空間における攻勢作戦で相手国の能力を消耗させる戦略を支持する立場もある。その場合、他国とのサイバー空間での継続的衝突を念頭に、衝突の烈度を管理する手段として規範の意義が論じられる[59]。

第 2 に、一定の標的に対するサイバー攻撃をタブーとする規範は、将来の安全保障環境の予見可能性を高めるとの議論がある。この議論は、各国へのサイバー攻撃能力（offensive cyber capabilities）の拡散と「保有」自体の阻止が困難な安全保障環境を念頭に、各国のサイバー攻撃能力の「運用」を規範に沿う穏健なものに誘導することの意義を説く[60]。例えばエグロフは、パブリック・アトリビューションは非難にコストを感じない攻撃国は抑止できないと認めつつ、許容し得ないサイバー攻撃をめぐる規範の設定により、同志国や国際社会の非難に敏感な第三国のサイバー攻撃能力の運用に影響を与えることで、将来の作戦環境の形成（shape）につながると指摘する[61]。

4. SolarWinds 事案へのアトリビューション連合対応：3 つの機能からみる継続性と論争点

SolarWinds 事案は、米国の IT 企業 SolarWinds が全世界に提供するネットワーク管理ソフト Orion Platform の更新プログラムを装ったマルウェア SUNBURST の感染拡大と、これによる各国での情報窃取事案の総称である。SUNBURST は感染した標的にバックドア（不正規の侵入経路）を開き、自身の挙動を Orion Platform の正規の機能に偽装しつつ、標的のネットワーク内の情報収集、外部通信、マルウェアの追加注入などを可能とする機能を備えていた。そのため SUNBURST の感染拡大は 2020 年 3 月頃から進展しつつ、同年 12 月初旬まで誰にも検知されず、攻撃者は水面下での情報窃取を行うことが可能となった。SUNBURST の感染拡大の範囲は 2021 年 12 月の SolarWinds の公式発表では最大で 1 万 8,000 の製品利用者とされ、その後の調査や各国発表によれば、2021 年 5 月までに米国、英国、オーストラリア、カナダ、EU 関係機関や複数の NATO 加盟国で感染が確認された[62]。

SUNBURST の感染は、2020 年 3 月から Orion Platform の更新プログラムをインストールした全世界の政府機関や民間企業に拡大した。その一方、セキュリティ専門家の調査により被害状況や攻撃手法をめぐる状況証拠が開示されていくにつれ、攻撃者は SUNBURST による実際の情報窃取対象を、各国の政府機関やセキュリティ企業などの少数の重要標的に絞り込んでいたことも明らかになった[63]。特に感染と情報窃取の被害が集中した米国では、報道や世論ではロシアへの強固な対応を求める声が加熱する一方で、専門家の間では、攻撃者の意図が、各国政府の外交・安全保障政策の意思決定のための情報収集を目的として、各国政府間で平素から行われている伝統的なサイバー諜報（cyber espionage）との分析が徐々に強まっていった[64]。一連の分析の背景には、攻撃者が、感染

した標的の識別とバックドアの事後封鎖を可能とする SUNBURST の機能を駆使し、検知され易い無差別な情報窃取や破壊活動を避け、少数の重要標的からの長期の情報窃取を優先したこと[65]や、TTPs の特徴から早期に容疑者となった APT29（別名：Cozy Bear）が、ロシアのインテリジェンス機関のなかでは伝統的なサイバー諜報を重視する傾向の強い SVR 系統の APT グループと目されていたこと、などがある[66]。

米国政府が、最終的に SolarWinds 事案における APT29 と背後にいる SVR の責任を断定し、「広範なサイバー諜報作戦（broad scope cyber espionage campaign）」との咎により名指しで非難したのは、事案発覚から約 5 か月後の 2021 年 4 月 15 日となった[67]。同日を起点とする各国の SolarWinds 事案への対応は、次の点で従来のアトリビューション連合の特徴を備えている（各国の主要措置は以下表 2 を参照）。第 1 に、4 月 15 日と翌 16 日の 2 日間で、ファイブ・アイズ諸国は SVR またはロシア政府に対する公式非難声明を集中させた。第 2 に、5 か国はシギントを担う対外情報機関や、国内捜査やカウンターインテリジェンスを司る治安情報機関も、公式非難声明のほか、（米英の場合）脅威情報アラート発出などで関与した。第 3 に、NATO と EU を含む少なくとも 9 つの同志国・パートナーも、4 月 15 日からの 2 日間で米国や同志国の SolarWinds 事案対応への支持・連帯表明などを行った。以下ではファイブ・アイズ諸国の対応を例に、パブリック・アトリビューションの 3 つの主要機能を読み解く。

表 2：SolarWinds 事案へのアトリビューション連合対応の概要

国・機関 実施日	実施措置 関連する政府機関など	措置の概要・特徴
米 4/15	公式非難声明＋制裁 ホワイトハウス（制裁を授権する大統領令発出） 財務省（制裁の実施官庁）	● **ホワイトハウス**が発表した**「ロシア政府の有害な対外活動 」に対する制裁を授権する大統領令のなかで、APT29とSVRの責任を名指しの上で非難。国際法違反に言及なし。**なお**同大統領令に基づく制裁の事由・対象はSolarWinds事案に限らず、**アフガニスタンにおける米軍兵士暗殺のための工作活動や、ロシアの野党指導者ナワルヌイ（Alexei Navalny）氏の毒殺未遂なども含む。 ● **大統領令**では、**SolarWinds事案を「広範なサイバー諜報作戦（broad scope cyber espionage campaign）」**と表現。**財務省による制裁事由の説明**は、**（SUNBURSTによる侵入の）「規模と範囲（scale and scope）」の要素を問題視**し、（SUNBURSTの感染による）世界の**（ソフトウェア）サプライチェーンへの悪影響や、対応のため民間企業のコスト**などについて言及。
	公式非難声明＋外交官の国外追放 国務省	● 上記の大統領令と同様に「ロシア政府の有害な対外活動」を非難。**米国内のロシア政府機関要員10名の国外追放**を発表。**SolarWinds事案につき国際法違反に言及無し。**一般論としてサイバー空間における規範の重要性に言及し、**パブリック・アトリビューションのための各国政策当局者用の訓練プログラムを発表（**2021年5月17日から21日に実施**）。**
	脅威情報アラート 国家安全保障局（NSA） 米国サイバー軍（USCYBERCOM） 連邦捜査局（FBI） サイバーセキュリティ・インフラセキュリティ庁（CISA） （CISAは国土安全保障省[DHS]の外局）	● **NSA、FBI、CISAが連名**で、**SVRへのパブリック・アトリビューションに伴う措置として共同勧告書（joint advisory）発表。SVRとその系統のAPTグループが攻撃に活用する脆弱性情報**（共通脆弱性識別子：Common Vulnerabilities and Exposures[CVE]）**を公開。** ● **USCYBERCOMとCISA（DHS）**は、**SVRの用いるマルウェアのサンプルを、マルウェア検査機能を持つ公開データベースVirus Totalに登録**（当該サンプルはHunt Forwardとも呼ばれる、USCYBERCOMと同志国との共同作戦を通じて収集したものとの説明）。
英 4/15	公式非難声明＋脅威情報アラート 外務・英連邦・開発省（FCDO） 国家サイバーセキュリティセンター（NCSC） （NCSCは英国政府通信本部[GCHQ]の一部）	● **FCDOの公式声明内**で、**APT29とSVRのSolarWinds事案の責任を米国と共に暴露**したと発表。APT29とSVRを含め、**ロシアのインテリジェンス機関とAPTグループの指揮統制関係の図を公表。国際法違反に言及なし。サイバー諜報との表現は用いず。SolarWinds事案で、SVRの行為の規範侵害や許容し得ない要素が何であったかについては言及せず。** ● **NCSC**は、同日発表の**米国NSA、FBI、CISAの共同勧告書に言及。米国との協力**を発表。
加 4/15	公式非難声明 グローバル連携省（Global Affairs Canada）（外務省） 国防省（通信保安局[CSE]所管） 公安・緊急事態対策省（安全情報局[CSIS]所管）	● グローバル連携省、国防省、公安・緊急事態対策省の所管大臣が連署した公式非難声明でSolarWinds事案における**APT29とSVRの責任を名指しで非難。国際法違反に言及無し。** ● **本事案を「サイバー諜報作戦（cyber espionage campaign）」と表現。**（実際の情報窃取対象以外も含め）**感染した組織に対応のコストを強い、ソフトウェア更新への公衆の信頼性を毀損した点**を問題視。
豪 4/15	公式非難声明 外務・貿易省（DFAT） 国防省（信号総局[ASD]所管） 内務省（保安情報機構[ASIO]所管）	● 外務・貿易省、国防省、内務省の所管大臣が連署した公式非難声明で、**ロシアの国家主体（Russian state actor）の責任を非難。国際法違反に言及無し。サイバー諜報との表現は用いず。**ただし、**各国への感染拡大を通じ、民間企業が被った被害**について問題視。
NZ 4/16	公式非難声明 政府通信保安局（GCSB）	● 政府通信保安局所管大臣の公式非難声明で**ロシアの国家主体の責任を非難。国際法違反に言及無し。サイバー諜報との文言は用いず。**ただし、**無差別な感染被害を全世界の数千のPCにもたらし、これにより民間企業が対応を強いられた要素**を問題視。
その他 4/15 - 4/16	同志国への支持・連帯表明 （公式非難声明に近いもの含む） NATOおよびEUを含む9の国・機関。 下線：外交当局のHPなどに声明を掲載。 （その他は、政府機関・閣僚などのTwitterで声明を掲載）	● フランス、デンマーク、エストニア、ラトビア、リトアニア、ポーランド、ルーマニア、NATO（北大西洋理事会声明）、EU（欧州理事会－欧州連合外務・安全保障政策上級代表声明）が、米国や同志国の取り組みへの支持（support）や連帯（solidarity）を表明を実施。 ● デンマーク、エストニア、ラトビア、リトアニア、ポーランドなどは**米国や同志国のアトリビューションの結果に言及し、SolarWinds事案に対するロシア政府の関与を名指し。**このうち、**エストニア、デンマーク、ポーランド**は、**SolarWinds事案におけるロシアの行為が許容し得ないことや、サイバー空間における責任ある国家の行動規範や国際法を遵守すべき旨を抽象的な形で言及。**
米-英 5/7	脅威情報アラート NSA、FBI、CISA、NCSC	● **米国のNSA、FBI、CISAと英国NCSCの4機関が共同勧告書**を発表。**SVRと関連するAPTグループが用いる戦術・技術・手順（Tactics, Techniques and Procedures[TTPs]）を追加で公表。**また2020年7月における米英加3か国共同でのAPT29のTTPs公表などの過去の取組にも言及し、一連の対応が**SVR系統の攻撃者のTTPsの変化をもたらした旨**に言及。

出典：各国政府発表に基づき筆者作成。

第 1 の抑止機能は、データの制約から一般的に効力測定は困難である。ただし「どのように抑止が作用するか」をめぐる各国の認識は、例えば 2021 年 5 月 12 日の英国国家サイバーセキュリティセンター（NCSC）のイベントでのラーブ（Dominic Raab）外務・英連邦・開発大臣の基調講演が参考となる。ここでは SolarWinds 事案対応を例に、サイバー攻撃の阻止と抑止（disrupting and deterring）に向けた同志国連携によるパブリック・アトリビューションの意義に触れている。具体的には TTPs の公表と対処・防御機能の向上に触れ、この取り組みが「持久走（marathon）かつ消耗戦（war of attrition）であり、今後も（英国は）攻撃者を白日の下に晒し続ける」と言及した[68]。英国が公式非難声明や脅威情報アラートで SolarWinds 事案に対応した点でも、同国は、非難や対処・防御機能向上の継続が、長期的に相手方のコストとして蓄積されることで抑止に寄与するとの認識であるとみられる[69]。

第 2 の対処・防御機能は、以上の英国の認識を踏まえれば、4 月 15 日以降の米英両国の脅威情報アラートなどに見出せる。米国政府は 4 月 15 日、SVR と APT29 のパブリック・アトリビューションに伴う措置として、SVR 系統の APT グループが攻撃に用いる脆弱性情報、マルウェアのサンプルなどの TTPs を公表し、攻撃の被害局限のための対応策を提示した[70]。また 5 月 7 日の米英両国政府合同の脅威情報アラートは、従来の TTPs 公表による被害側の対処・防御機能向上に触れ、SVR が自身の利用する TTPs を変化させてきたとの認識も示している[71]。

最後に、規範設定機能である。この点は、ファイブ・アイズ諸国がロシア政府の責任を明確に非難し、かつ米国とカナダがサイバー諜報との咎での非難に踏み切ったことは、専門家の間で大きな注目を集めた。なぜならば、サイバー諜報の国際法上の地位について各国間で依然論争があるなかで、この 5 か国は従来から、平素（平時）のサイバー諜報は国際法違反ではなく、各国政府間で正統な行為として許容され得るとの立場を取ってきたからである。攻撃国の特定から他国へのサイバー攻撃能力の運用まで、5 か国が享受するサイバー安全保障上の優位は、自身も平素から他国に行うサイバー諜報に立脚する。よって各国は産業競争力強化のための国家の産業スパイ活動は許容し得ないとの一線は引きつつ、（その過程で民間企業を踏み台や巻き添えとするものであれ）他国政府機関などを主な標的とした伝統的なサイバー諜報を縛り得る規範の設定には慎重な立場にあった[72]。

近年のパブリック・アトリビューション研究も、米国などの一部の国が、自国に対する他国政府の伝統的なサイバー諜報の存在を認識しても、攻撃国を名指しした公式の非難は回避する傾向があると指摘してきた[73]。無論、他国のサイバー諜報が発覚した場合に放置する訳ではなく、被害国は攻撃者の刑事訴追、外交官追放、攻撃者の TTPs 公表など、国内法執行とカウンターインテリジェンスの範疇として各国間で均衡性があると認められてきた対応はとる[74]。しかし、ファイブ・アイズ諸国のなかで、今回の米加両国のように「サイバー諜報」の咎で攻撃国に対して公式の非難に至ったことや、米国のように制裁まで課したことは異例の対応であった[75]。よって専門家の間では、SolarWinds 事案を契機にファイブ・アイズ諸国が、サイバー諜報が国際法上合法かつ許容され得るとの立場から決別し、自国のサイバー諜報の抑制も伴う新たな規範の設定を試みたのか否かが論争を呼んだ。

5. 専門家の論争の背景：SolarWinds 事案が問うサイバー諜報を許容するリスクと規範設定の是非

SolarWinds 事案対応と規範設定機能をめぐる専門家の論争は、サイバー諜報のなかでも一定の例外的性質を備えたものを許容し得ないとする規範が、長期的には米国を含む各国の安全保障にも資するとの発想が背景にある。

サイバー空間におけるインテリジェンス機関の活動は、各国が国際規範のもとでは相互に許容してきた、平素における伝統的な諜報活動と、許容し得ない活動の間のグレーゾーンともいえる状態を生じさせ易い。例えば情報窃取のために標的のネットワークへの侵入を伴うサイバー諜報は、ペイロード（payload：悪意ある動作を実行するコード）の差を除けば許容し得ない破壊活動（destructive cyber attack）と類似の手順を踏み、両者はペイロードの実行まで識別困難[76]なことがある。また攻撃者は政府機関からの窃取情報をリークし、選挙などの民主的政治過程に対する干渉も行い得る。被害国としては、平素からのサイバー諜報の外形で、許容し得ない活動（またはその準備行為）が野放しとなるリスクは看過し難いが、一方で各国が従来は相互に許容してきたサイバー諜報にカウンターインテリジェンスの範疇を超える報復を課せば、短期的なエスカレーションのリスクはもとより、将来的に自国のサイバー諜報もまた、同様の烈度の高い対応に晒されるリスクもある[77]。

以上のように、サイバー空間における各国のインテリジェンス機関の活動には、物理空間でのスパイを駆使した伝統的な諜報活動には無い特有のリスクが伴う。そのため、ランド研究所のリビッキ（Martin Libicki）を含む米欧の専門家は、SolarWinds 事案の以前から、原則は合法かつ許容され得る平素のサイバー諜報のなかでも、その標的や手法などの面で例外的に許容し得ない条件を明示する規範の戦略的意義や、その実現可能性を議論してきた[78]。また、こうした議論を体現するように、米国のバイデン（Joe Biden）政権の高官達も、SolarWinds 事案が「諜報と攻撃のグレーな領域[79]」や「破壊活動につながる懸念から、単一の諜報事案とはみなせない[80]」といった認識を示してきた。この点で SolarWinds 事案はファイブ・アイズ諸国に対して、サイバー諜報を国際規範の下で許容し得るとする従来の立場を貫くか、逆に自国の将来のサイバー諜報の自由を狭めても、規範設定を通じてサイバー諜報と許容し得ない活動のグレーゾーンのリスクの問題に向きあうかを問う事例でもあった。

以上の背景を踏まえたうえで、SolarWinds 事案への対応をめぐる専門家の解釈は、大きく 2 つの立場に分かれる。第 1 の立場は、例外規範設定説である。特に米国とカナダがサイバー諜報との文言でロシア政府を非難した事実などに着目し、SolarWinds 事案はサイバー諜報のなかでも例外的な性質を持ち、今後は同質の行為を許容し得ないとの新たなレッドラインを引いたと分析する。アイケンサーを始めとしたこの立場は、米国とカナダの公式非難声明の分析も踏まえ、SUNBURST の世界的感染拡大、サイバー諜報の踏み台とされた米国や各国企業の対応コスト、民間のソフトウェア・サプライチェーンの信頼性の毀損などが、許容し得ない例外的な性質とみる[81]。

第 2 の立場は、規範設定回避説である。各国は公式非難声明のなかで、侵害された規範や許容し得ない攻撃の性質といったレッドラインを踏み越えた要素への明確な言及を避け、将来の自国のサイバー諜報を制約し得る規範の設定を回避したとみる。例えば米国のサイバー安全保障法制の専門家のチェスニー（Robert Chesney）や、英国王立防衛安全保障研究所 （RUSI）のマコール（Jamie MacColl）は、それぞれ米英の SolarWinds 事案への対応を分析し、両国はサイバー諜報をめぐる規範的な立場や新たなレッドラインを明確にしなかったと結論付けた[82]。

専門家の解釈が真逆に割れる中で、SolarWinds 事案への対応のみでファイブ・アイズ諸国がサイバー諜報に歯止めをかける規範設定を試みたのかは断定し難い。5 か国の公式非難声明の内容を比較（前掲表 2 参照）すると、共通してロシアの行為が国際法違反とは言及していない。5 か国は今後とも、サイバー諜報を国際法で規律する意思はもたないとみられる。そのため議論の焦点は、規範を合法であれ許容し得ないサイバー攻撃をめぐる共通理解としてとらえたときに、5 か国が例外規範設定説の立場を取ったのか、仮にそうであれば、SolarWinds 事案におけるロシアの行為の、例外的に許容し得ない性質とは何であったのか、に集約される。

この評価は 5 か国の場合分けが必要となる。英国は、米国と共に SVR の活動を暴露した事実を述べたのみであり、SolarWinds 事案による規範侵害や許容し得ない性質を示さなかった[83]。レッドラインを踏み越えた要素への言及は、近年アトリビューション連合が形成されたジョージア事案や APT10 事案に対する英国政府の公式非難声明と比べても絶無に等しい[84]。これらの前例に照らせば、同国は規範設定回避説の立場を取ったとみられる。

英国以外の 4 か国は、例外規範設定説の解釈を取る余地がある。「サイバー諜報」との文言を用いたのは米加 2 か国のみだが、4 か国とも標的への情報窃取に至る過程での SUNBURST の拡散の無差別性や、被害状況の調査や対策を強いられた民間企業のコストを挙げた。つまり、本命の情報窃取の過程で生じた民間企業の巻き添え被害を問題視し、同種の手法や規模のサイバー諜報を今後許容しないとのレッドラインを引いたとの見方はとりうる。

ただし、米英の専門家の間では、SolarWinds 事案はその手法や規模に照らしても、各国政府がこれまで相互に正統なものと許容し、今後も外交・安全保障上の必要性から許容せざるを得ないだろうサイバー諜報の範疇との指摘も多い。2013 年に米国国家安全保障局（NSA）の文書漏洩で暴露された数多の事例や、2020 年の調査報道で判明した、スイスの暗号技術会社 Crypto AG を利用した米独のインテリジェンス機関の諜報活動など、民間企業を踏み台ないし巻き添えとするサイバー諜報は米英や欧州諸国も実施してきた[85]。被害規模や攻撃の無差別性も、英国政府通信本部（GCHQ）傘下の NCSC 長官であったマーティン（Ciaran Martin）は、SolarWinds 事案でロシアは精密に情報窃取の標的を限定しており、NSA や GCHQ の前歴に比べても無差別性は低いと指摘した[86]。

仮に、SolarWinds 事案のような手法や規模のサイバー諜報が、ロシアのみならず、今後もファイブ・アイズ諸

国や各国のインテリジェンス機関の活動とサイバー安全保障上の優位に不可欠だとすれば、各国にとって自国の活動の抑制を伴う規範の遵守は現実的ではなく、レッドラインとして有名無実化し得る。よって SolarWinds 事案対応のみで、ファイブ・アイズ諸国のサイバー諜報への規範的な立場につき評価を下すことは時期尚早であろう。

むすびにかえて：同志国とアトリビューションを議論する共通の「ものさし」の必要性

本稿の分析から日本への含意を述べるとすれば、アトリビューションのプロセスにおけるパブリック・アトリビューションの論点や目的（機能）をふまえ、日本と同志国との間でアトリビューションを議論する前提を揃えていく必要があるということである。もちろんアトリビューションにおける「誰がやったのか」の特定、特にサイバー攻撃への国家の関与の特定は、各国にとって依然厄介な課題である。「次期 CS 戦略骨子」の骨子本文 22 頁から 23 頁に記載された「状況把握力の強化」は今後も重要となる。また同一の箇所で状況把握力を「防御力ひいては抑止力の基盤」と位置づけ、「国家の関与が疑われるサイバー攻撃等に対応するため、政府内関係省庁及び同盟国・同志国との情報共有を推進する」と明記した点は、今後の日本の取り組みをみるうえで注目に値する[87]。

そのうえで、日本が次期 CS 戦略のもとで同志国連携のさらなる強化にコミットするのであれば、日本と同志国の間の（パブリック・）アトリビューションをめぐる現状の能力や課題認識の差を踏まえ、今後の対応を議論していくことが何よりも大切である。特に 2017 年以降、各国は平素から、国際法上の武力攻撃の閾値を超えない（グレーゾーンの）事態における国家のサイバー攻撃への政策対応の 1 つとして、攻撃者や攻撃国の特定結果の「公表」を戦略的に活用してきた。同時に SolarWinds 事案へのアトリビューション連合対応や専門家の論争に照らせば、各国政府や専門家がこの施策がもつ複数の機能を念頭に、事案毎のパブリック・アトリビューションの実施の是非、形式、公表する情報やメッセージの内容などを議論しているとみられる点も留意すべきである。

パブリック・アトリビューションは、単独実施か同志国連携かを問わず各国の政策手段の 1 つに過ぎない。日本にとってのパブリック・アトリビューション実施の是非は、次期 CS 戦略などが掲げる目標が決めるものである。また、冒頭に挙げたエグロフとスミートが指摘する通り、事案の性質によりパブリック・アトリビューションを控えることも重要な政策オプションである[88]。そうした判断にあたっては、各国がパブリック・アトリビューションで意図する目的を、日本として過小評価も過大評価もせずに把握することが必要となる。この取り組みで先行してきた米国や英国といった同志国が念頭に置く施策の機能への理解は、将来の日本単独での取り組みはもちろん、例えばアトリビューション連合方式で同志国と連携する際に、日本に対して求められる能力や関与の形式の見積もりにも影響し得るからである。

パブリック・アトリビューションは、2017 年以降のアトリビューション連合の活発化や、その後の研究の発展ぶりを反映したアトリビューションの派生概念であり、各国のアトリビューション研究や政策対応の最新の論点をとらえる「ものさし」となる。それを携えておくことは、次期 CS 戦略策定後の日本のサイバー安全保障政策と、その手段の 1 つとしての同志国連携の在り方を、国内外で議論していくうえでも有益であろう。

（2021 年 7 月 5 日脱稿）

プロフィール profile

政策研究部
グローバル安全保障研究室
研究員　　瀬戸　崇志
専門分野：サイバーセキュリティ
：安全保障論

防衛研究所企画部企画調整課
直　通：03-3260-3011
代　表：03-3268-3111（内線 29171）
ＦＡＸ　：03-3260-3034
※ 防衛研究所ウェブサイト：http://www.nids.mod.go.jp/

[1]内閣サイバーセキュリティセンター「資料 1－1『次期サイバーセキュリティ戦略』（骨子）の概要 」2021 年 5 月 13 日、4 頁、https://www.nisc.go.jp/conference/cs/dai28/pdf/28shiryou01.pdf.
[2]内閣サイバーセキュリティセンター「資料 1－2『次期サイバーセキュリティ戦略』の（骨子）」2021 年 5 月 13 日、22 頁、https://www.nisc.go.jp/conference/cs/dai28/pdf/28shiryou01.pdf.
[3]「サイバー攻撃（cyber attack）」の用語は報道や情報セキュリティでの総称概念としての含意と、外交・安全保障政策の文脈での含意が異なる。本稿では媒体の性質上、サイバー攻撃と表記する場合は前者の総称概念として用い、国際法上の最広義の定義の「サイバー行動 （cyber operations）」と同様の意味で用いる。サイバー攻撃（サイバー行動）のなかで、さらに細分化された特別の国際法または安全保障政策上の事態類型を示す場合、初出時に英文を明記し、各国の戦略文書や国際合意の文言も同様に扱う。国際法上のサイバー行動とサイバー攻撃の定義は次を参照。黒崎将広他 『防衛実務国際法』弘文堂、2021 年、240 頁-248 頁。
[4]内閣サイバーセキュリティセンター「資料 1－2『次期サイバー』」、22 頁。特に同頁記載の注 20 および注 21 を参照。
[5]「英『米へのサイバー攻撃、ロシア関与』」『日本経済新聞』2021 年 4 月 16 日。
[6]Global Affairs Canada, “Statement on SolarWinds Cyber Compromise,” April 15, 2021, https://www.canada.ca/en/global-affairs/news/2021/04/statement-on-solarwinds-cyber-compromise.html.
[7]Marise Payne, “Attribution of Cyber Incident to Russia,” Foreign Minister's Office of the Department of Foreign Affairs and Trade, April 15, 2021, https://www.foreignminister.gov.au/minister/marise-payne/media-release/attribution-cyber-incident-russia.
[8]Government Communications Security Bureau, “SolarWinds Compromise Attributed to Russian State Actor,” April 16, 2021, https://www.beehive.govt.nz/release/solarwinds-compromise-attributed-russian-state-actor.
[9]例えば次を参照。鶴岡路人「ファイブ・アイズと日本：参加より連携を」nippon.com、2020 年 11 月 26 日、https://www.nippon.com/ja/in-depth/d00654/#.
[10]Florian J. Egloff, “Public Attribution of Cyber Intrusions,” *Journal of Cybersecurity,* Vol. 6, No. 1, September 2020, p. 9; Dennis Broeders, Els De Busser, and Patryk Pawlak, “Three Tales of Attribution in Cyberspace: Criminal Law, International Law and Policy Debates,” *The Hague Program for Cyber Norms Policy Brief,* Institute of Security and Global Affairs at Leiden University, April 2020, p. 10, https://www.thehaguecybernorms.nl/research-and-publication-posts/three-tales-of-attribution-in-cyberspace-criminal-law-international-law-and-policy-debates. このほか、文献によっては「キャンペーン型対応（public attribution campaign）」、「集団的アトリビューション（collective attribution）」、「調整型アトリビューション（coordinated attribution）」といった用語が用いられることもある。
[11]Florian J. Egloff and Max Smeets, “Publicly Attributing Cyber Attacks: A Framework,” *Journal of Strategic Studies,* Published Ahead of Print, March 2021, p. 3, DOI: 10.1080/01402390.2021.1895117.
[12]Florian J. Egloff, “Contested Public Attributions of Cyber Incidents and the Role of Academia,” *Contemporary Security Policy,* Vol. 41, No. 1, January 2020, pp. 55-81.
[13]公安調査庁「サイバー空間における脅威の概況 2021」2021 年 3 月、7-9 頁、http://www.moj.go.jp/content/001343414.pdf.
[14]本稿の定義は、本文内の 2 つの定義に加え、次の文献を参照のうえで設定した。Clement Guitton, *Inside the Enemy’s Computer: Identifying Cyber Attackers,* Hurst Publishers, 2017, pp. 10-11, pp. 65-83; Martha Finnemore and Duncan B Hollis, “Beyond Naming and Shaming: Accusations and International Law in Cybersecurity,” *European Journal of International Law,* Vol. 31, No. 3, December 15, 2020, pp. 974-977, pp. 985-993; Gil Baram and Udi Sommer, “Covert or Not Covert: National Strategies During Cyber Conflict,” T. Minárik et al, eds., *11th International Conference on Cyber Conflict: Silent Battle*, NATO Cooperative Cyber Defence Centre of Excellence (hereafter NATO CCDCOE), 2019, pp. 198-203; Broeders, Busser, and Pawlak, “Three Tales of Attribution,” p. 2. 以上の文献の内容を整理すると、現在「パブリック・アトリビューション」として議論されている各国政府の対応は、より厳密には[a]攻撃者や攻撃国の特定(attribution)、[b][a]にまつわる状況証拠や関連情報（被害規模や攻撃手法など）の第三者への暴露（exposure）、[c]攻撃の実行犯や国家に対する非難（condemnation）、の 3 段階の行為に分解できる。このうち、例えば同志国連携の事例で、自国が証拠を保持していないが、同志国の[a]の結果に依拠して[c]を行うケースを、（パブリック・）アトリビューションと異なる外交的非難（accusation）とみる立場もある。他方で、攻撃の被害や手法の情報公開にとどめ、攻撃者や攻撃国を名指しで非難しない対応（[c]を伴わない[b]）も存在する。本稿では、こうした論争を踏まえつつも、自国が攻撃者や攻撃国を名指しする判断（judgement）の公表を概念の中核的な要素とし、それが伴う場合は当該対応をパブリック・アトリビューションに含む立場をとる。その理由は、次の 3 点による。第 1 に、国家の関与が疑われるサイバー攻撃への（パブリック・）アトリビューションは、犯罪者への刑事司法手続とは異なる国家安全保障政策の営為であり、事実関係を 100%立証しうる証拠は入手不可能な中で、最後は限られたインテリジェンスと政治的判断で行われる。そのため、攻撃国を名指しする際に公開を要求される証拠の質や量に客観的な基準は無く、同志国のインテリジェンス（評価）に依拠したうえでの対応が否定される訳ではない。第 2 に、各国がインテリジェンス機関の非公開の機微情報をアトリビューションで用いることがあるなかで、各国が攻撃者や攻撃国を特定する証拠を有しないか否かは、例外的な場合を除けば公開情報からは判別できない。第 3 に、パブリック・アトリビューションの目的は多様だが、政策目的により公表すべき情報やメッセージが異なる。そのため、厳密にはパブリック・アトリビューションに含みうるか論争のある[a]を伴わない[c]や、[c]を伴わない[b]といった行為も議論の射程に含めることは、各国の近年の政策対応の機能と限界を把握するうえでも有益となる。
[15]Kristen Eichensehr, “The Law & Politics of Cyberattack Attribution,” *UCLA Law Review,* Vol. 67, No. 3, July 2020, pp. 531-536.
[16]攻撃者や攻撃国の特定に至るプロセスの全体像と、用いられ得る証拠や手法は次を参照。Timo Steffens, *Attribution of Advanced Persistent Threats: How to Identify the Actors Behind Cyber-Espionage,* Springer, 2020, pp. 23-50; John Davis et al., *Stateless Attribution: Toward International Accountability in Cyberspace: Toward International Accountability in Cyberspace,* RAND Corporation, 2017, pp. 9-16.
[17]アトリビューション問題を扱った日本語での主な先行研究や論考としては、例えば次を参照。土屋大洋「サイバーセキュリティとインテリジェンス機関―米英における技術変化のインパクト」『国際政治』第 179 号、2015 年 2 月、45-48 頁；土屋大洋『サイバーグレートゲーム―政治・経済・技術とデータを巡る地政学』千倉書房、2020 年、3-22 頁；川口貴久「【コラム】サイバー攻撃は誰がやった？」安全保障用語―絶対に知っておくべき平和と安全のための基礎知識、2018 年 10 月 12 日、http://dictionary.channelj.co.jp/2018/c18101201/.
[18]Thomas Rid and Ben Buchanan, “Attributing Cyber Attacks,” *Journal of Strategic Studies,* Vol. 38, No. 1-2, January, 2015, pp. 26-30; Guitton, *Inside the Enemy’s Computer,* pp. 79-83.
[19]Keir Giles and Kim Hartmann, “‘Silent Battle’ Goes Loud: Entering a New Era of State-Avowed Cyber Conflict,” T. Minárik et al, eds., *11th International Conference on Cyber Conflict: Silent Battle*, NATO CCDCOE, 2019, pp. 23-27.

[20]White House, *National Cyber Strategy of the United States of America*, September 2018, p. 21, https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf. 米国は同戦略の 21 頁で「サイバー抑止イニシアティブ（Cyber Deterrence Initiative）」と呼ばれる、悪意あるサイバー活動（malicious cyber activities）の抑止に向けた同志国連携を強化する枠組みを提唱し、具体的な連携内容としてインテリジェンスの共有、（公開した）アトリビューションの主張を相互に補うこと、同志国が取った政策対応を公的に支持すること、悪意あるサイバー活動の実施主体に（制裁などで）結果（consequence）を伴わせると述べている。
[21]Netherlands Ministry of Defense, *Defence Cyber Strategy 2018: Investing in Cyber Striking Power for the Netherlands*, November 2018, p. 7, https://english.defensie.nl/binaries/defence/documents/publications/2018/11/12/defence-cyber-strategy-2018/NLD+MoD+cyber+strategy+2018_web.pdf. 同戦略の 7 頁では、積極的な政治的アトリビューション政策（active political attribution policy）は抑止能力（deterrent abilities）に寄与するとの認識を示す。国家主体は、自身の行動が公開の場などで非難され、攻撃が完全な匿名では行えないと認識すれば、行動を変え得るとの見方を示す。なお同戦略は蘭語版が正文だが、正文の記述は次の論文内の英訳を参照。Egloff and Smeets, “Publicly Attributing Cyber Attacks,” p. 2.
[22]Department of Foreign Affairs and Trade, *Australia’s International Cyber and Critical Tech Engagement Strategy*, April 2021, pp. 41-42, https://www.internationalcybertech.gov.au/sites/default/files/2021-04/21045%20DFAT%20Cyber%20Affairs%20Strategy%20Internals_Acc_update_1_0.pdf. 同戦略の 42 頁では、特に 2017 年から、パブリック・アトリビューションが豪州のサイバー攻撃の対応措置の 1 つ（a toolkit of responses)となったと明示的に述べている。対応措置(response)は抑止態勢を支える 4 本の柱に含まれ、その目的はサイバー空間における責任ある国家の行動（responsible state behavior)の促進による、平和かつ安定的な国際環境の護持とされる。なお対応措置は公表されない場合があるとも言及している。
[23]ジョージア工科大学の研究プロジェクトで作成されたデータセットによれば、2016 年から 2018 年(第 1 四半期)において国家の関与が疑われた重大サイバー攻撃事案 (n=82)につき、少なくとも 70%以上が民間企業または政府により、攻撃国に対する（パブリック・）アトリビューションの対象となった。当該データセットの詳細は次を参照。Milton Mueller et al., “Cyber Attribution: Can a New Institution Achieve Transnational Credibility?” *The Cyber Defense Review*, Vol. 4, No. 1, Spring 2019, pp. 111-112.
[24]典型例として 2018 年に発覚したシンガポール最大手医療機関 SingHealth へのサイバー攻撃に対するシンガポール政府の対応が挙げられる。次を参照。Baram and Sommer, “Covert or Not Covert,” pp. 207-208.
[25]2017 年に発生した NotPetya 事案をはじめ、ロシアの関与が疑われる欧州での重大なサイバー攻撃事案で、ドイツとフランスがロシア政府に対する非難を回避する傾向が指摘されてきた。次を参照。Jamie Collier, “Europe’s New Sanction Regime Suggests a Growing Cyber Diplomacy Presence,” *Fire Eye Industry Perspectives*, August 06, 2020, https://www.fireeye.com/blog/executive-perspective/2020/08/europe-new-sanction-regime-suggest-a-growing-cyber-diplomacy-presence.html/.
[26]例えばチェコ外務省は 2020 年 2 月 20 日、前年 10 月に発生した（ロシアの関与が疑われた）ジョージア（旧グルジア）への大規模サイバー攻撃を非難したが、その際に「本件で直接のフォレンジック証拠（primary forensic evidence）を有しないものの、同盟国によるアトリビューションの評価に疑う余地はない」と明言し、米国と英国による公式非難声明を引用している。また日本経済新聞の報道によれば、日本政府による、2017 年 12 月の WannaCry 事案対応での北朝鮮政府に対する非難も、自国ではなく同盟国の情報に依拠したものであった。チェコ政府と日本政府の対応はそれぞれ次を参照。Czech MFA(@CzechMFA) “@CzechMFA condemns cyberattacks on #Georgia from October 28, 2019. While we do not have the primary forensic evidence in this case, we have no reason to doubt the attribution assessment made by our allies,” *Twitter*, February 20, 2020, https://twitter.com/CzechMFA/status/1230491060150964230; 「JAXA サイバー攻撃に反撃　日本初『特定』の狙い」『日本経済新聞』2021 年 5 月 12 日。
[27]以上のような視座を有する近年の主要先行研究として例えば次を参照。Egloff, “Public Attribution of Cyber Intrusions,” pp. 1-12. Baram and Sommer, “Covert or Not Covert,” pp. 197-212; Finnemore and Hollis, “Beyond Naming and Shaming,” pp. 969-1003; Sasha Romanosky and Benjamin Boudreaux, “Private-Sector Attribution of Cyber Incidents: Benefits and Risks to the U.S. Government,” *International Journal of Intelligence and Counterintelligence*, Vol 34, No. 3, pp. 463-493; Michael Poznansky and Evan Perkoski, “Rethinking Secrecy in Cyberspace: The Politics of Voluntary Attribution,” *Journal of Global Security Studies*, Vol. 3, No. 4, October 2018, pp. 402–416; Austin Carson, *Secret Wars: Covert Conflict in International Politics*, *Secret Wars*, Princeton University Press, 2018, pp. 295-297.
[28]Broeders, Busser, and Pawlak, “Three Tales of Attribution,” p. 9, pp. 17-18; Egloff and Smeets, “Publicly Attributing Cyber Attacks,” p. 21. NotPetya 事案、OPCW 事案、ジョージア事案は、以上の 2 次資料も参照し、2021 年 7 月の時点で 1 次情報にアクセス可能なものもふまえて、適宜記載内容を修正している。WannaCry 事案、APT10 事案、SolarWinds 事案は、各々の連合形成の日付における各国の政府発表および外交当局の公式 Twitter などの検索結果に基づく。
[29]Egloff and Smeets, “Publicly Attributing Cyber Attacks,” p. 16; Broeders, Busser, and Pawlak, “Three Tales of Attribution,” p. 10.
[30]具体的には、証拠の開示により相手方に対するシギントなどのテクニックが推論されてしまうほか、インテリジェンス機関が存在を認知しつつ、自身の諜報活動での利用のために意図的に秘匿していたゼロデイ脆弱性（zero-day vulnerability）などが公表されることで、当該脆弱性へのパッチの適用で情報収集手段が無力化されるケースなどもある。パブリック・アトリビューションとインテリジェンス機関の能力基盤の維持はこの点でトレードオフになることがあるが、自国に優れたセキュリティ産業が存在する国では、官民連携と情報共有でこの問題が克服し得る可能性も指摘されている。以上の点は次を参照。Dennis Broeders, Sergei Boeke, and Ilina Georgieva, “Foreign Intelligence in the Digital Age: Navigating a State of ‘Unpeace’,” *The Hague Program for Cyber Norms Policy Brief*, Institute of Security and Global Affairs at Leiden University, September 2019, p. 4, https://www.universiteitleiden.nl/en/research/research-output/governance-and-global-affairs/foreign-intelligence-in-the-digital-age.-navigating-a-state-of-unpeace; Egloff and Smeets, “Publicly Attributing Cyber Attacks,” pp. 8-11; Guitton, *Inside the Enemy’s Computer*, p. 7; Dave Aitel and Matt Tait, “Everything You Know About the Vulnerability Equities Process Is Wrong,” *Lawfare*, August 18, 2016, https://www.lawfareblog.com/everything-you-know-about-vulnerability-equities-process-wrong.
[31]Florian J. Egloff and Andreas Wenger, “Public Attribution of Cyber Incidents,” *CSS Analyses in Security Policy*, No. 244, Center for Security Studies of ETH Zurich, May 2019, p. 2; Broeders, Boeke, and Georgieva, “Foreign Intelligence in the Digital Age,” p. 4. パブリック・アトリビューションの主張の信頼性維持のための国際連携の必要性は、次に詳しい。Guitton, *Inside the Enemy’s Computer*, pp. 76-82.
[32]国際法上も攻撃国に対する非難に際し、客観的な証拠水準や証拠開示の義務といった、いわゆる証拠法理と呼ばれるものを厳密に定めるべきとの論争は存在する。ただし証拠法理の厳格化は、インテリジェンス機関の機密情報や政治判断に依拠した各国のパブリック・アトリビューションを事実上困難とする。そのため米・英・蘭・仏などはパブリック・アトリビューションをめぐる国際法上の厳密な証拠法理の設定には消極的立場を取ってきた経緯がある。次を参照。Eichensehr, “The Law & Politics of Cyberattack,” pp. 545-546; Broeders, Busser, and Pawlak, “Three Tales of Attribution,” pp. 6-8, p. 9.

[33]ただし機密情報への依存度が高く証拠が開示されないパブリック・アトリビューションは、国内外の政治的な分極化が進むなかではその信頼性が敵対国の偽情報などで毀損されやすく、パブリック・アトリビューションの政策目的を達する観点からも、中立的なセキュリティ専門家の関与と検証メカニズムによる判断の透明性の担保を求める声もある。次を参照。Egloff, "Contested Public Attributions," pp. 70-73; Davis et al., *Stateless Attribution*, pp. 20-21.
[34] Broeders, Busser, and Pawlak, "Three Tales of Attribution," pp. 4-6; Guitton, *Inside the Enemy's Computer*, pp. 65-109; Broeders, Boeke, and Georgieva, "Foreign Intelligence in the Digital Age," p. 5.
[35]厳密にいえば、刑事司法手続における証拠水準が問題となるのは、基本的には実際の審理（actual trial）係属時となる。たとえば実行犯が国外逃亡し引き渡される見込みが無いケースでの書類送検などは、刑事司法手続の外形をとった単なる政治的対応であり、証拠水準が問題とならないとみる立場もある。次を参照。Broeders, Busser, and Pawlak, "Three Tales of Attribution," pp. 5-6, p. 11.
[36]次を参照。Yuliya Miadzvetskaya, "Challenges of the Cyber Sanctions Regime under the Common Foreign and Security Policy (CFSP)," Anton Vedder et al., eds., *Security and Law: Legal and Ethical Aspects of Public Security, Cyber Security and Critical Infrastructure Security*, Intersentia, 2019, pp. 279-292.
[37]Ibid., p. 282, pp. 290-292.
[38]Egloff and Smeets, "Publicly Attributing Cyber Attacks," pp. 8-11.
[39]次を参照。Ibid., pp. 13-15; Guitton, *Inside the Enemy's Computer*, pp. 42; Baram and Sommer, "Covert or Not Covert," p. 9.
[40]Miadzvetskaya, "Challenges of the Cyber Sanctions," pp. 283-287.
[41]エグロフとスミートは、政府によるパブリック・アトリビューションの目的を（1）規範設定（norm-setting）、（2）（抑止も含む）強制（coercion）、（3）脅威対抗（counter-threats）、（4）予防・防御（prevention and defense）、（5）（国内外のアトリビューションに携わるステークホルダー間の）コミュニティ構築（community building）、（6）国内ないし国際的な正統性・信頼性の獲得、という 6 類型で整理する。本稿では主に（2）を第 1 の機能、（3）と（4）を第 2 の機能、（1）を第 3 の機能に対応させ整理する。また、同志国との関係強化は主に(5)に該当する。以上の 6 類型は次を参照。Egloff and Smeets, "Publicly Attributing Cyber Attacks," pp. 5-8.
[42]例えば次を参照。外務省「第 10 回記念サイバーセキュリティ国際シンポジウムにおける赤堀毅サイバー政策担当大使講演」2020 年 10 月 13 日、3 頁、https://www.mofa.go.jp/mofaj/files/100102541.pdf；内閣サイバーセキュリティセンター「資料 6-2 『国際社会の平和・安定及び我が国の安全保障への寄与』に係る取組状況（詳細資料）」2019 年 1 月 24 日、7 頁、https://www.nisc.go.jp/conference/cs/dai21/pdf/21shiryou06.pdf.
[43]この点は次を参照。Mathew Schwarz, "Turla Teardown: Why Attribute Nation-State Attacks?" *BankInfoSecurity*, October 30, 2019, https://www.bankinfosecurity.com/blogs/turla-teardown-attribute-nation-state-attacks-p-2813; Erica D. Borghard, "U.S. Cyber Command's Malware Inoculation: Linking Offense and Defense in Cyberspace," *Net Politics*, April 22, 2020, https://www.cfr.org/blog/us-cyber-commands-malware-inoculation-linking-offense-and-defense-cyberspace.
[44]2016 年から 2017 年の UNGGE の第 5 期会合での報告書の採択失敗を指す。当時の経緯は次を参照。Arun M. Sukumar, "The UN GGE Failed. Is International Law in Cyberspace Doomed As Well?" *Lawfare*, July 4, 2017, https://www.lawfareblog.com/un-gge-failed-international-law-cyberspace-doomed-well. 特にこの時期から、米国は、国連と並行して G7 などの同志国の枠組みを活用し、サイバー空間における既存の国際法や責任ある国家の行動規範の適用可能性を確認し、その一環として武力攻撃に至らない事案に対する国際法上の対抗措置の権利を国際合意などで明示していく。この点は次を参照。Andres Heriksen, "The End of the Road for the UN GGE Process: The Future Regulation of Cyberspace," *Journal of Cyber Security* Vol. 5, No. 1, January 2019, pp. 6-7; 外務省「サイバー空間における責任ある国家の行動に関する G7（ルッカ）宣言」2017 年 4 月 11 日、2 頁、https://www.mofa.go.jp/mofaj/files/000246366.pdf.
[45]この発想が最も端的に表現されているのが、2018 年における米国の「国家サイバー戦略」の情勢認識と、「サイバー抑止イニシアティブ」（前掲注 20）にかかる記述である。次を参照。White House, *National Cyber Strategy*, pp. 1-3, p. 21. また、同戦略の内容を含め、ファイブ・アイズ諸国によるアトリビューション連合の運用思想や背景は、次の研究も参照。Josh Gold, "The Five Eyes and Offensive Cyber Capabilities: Building a 'Cyber Deterrence Initiative'," *NATO CCDCOE Research Paper*, NATO CCDCOE, October 2020, pp. 9-11; Broeders, Busser, and Pawlak, "Three Tales of Attribution," p. 9.
[46]Finnemore and Hollis, "Beyond Naming and Shaming," p. 971, p. 975.
[47]Egloff, "Public Attribution of Cyber Intrusions," p. 9; Giles and Hartmann, "'Silent Battle' Goes Loud," p. 10.
[48]Broeders, Busser, and Pawlak, "Three Tales of Attribution," p. 11, p. 14; Giles and Hartmann, "'Silent Battle' Goes Loud," p. 10; Chris Painter, "Deterrence in Cyberspace: Spare the Costs, Spoil the Bad State Actor: Deterrence in Cyberspace Requires Consequences," *ASPI Policy Brief*, No. 4, ASPI International Cyber Policy Centre, July 1, 2018, p. 6, https://s3-ap-southeast-2.amazonaws.com/ad-aspi/2018-05/Deterrence%20in%20cyberspace_0.pdf?VersionId=JtY9WhXLd53pCnni2U5PiHr8ikcPMC5I.
[49]対処・防御は、抑止のように相手方のコスト認識や費用対効果計算による行動変容を前提とせず、仮に抑止が失敗したとしても脅威を提起する能力それ自体を削ぐ点で独自の意義を持つ。そのため、本稿では両者は別個の機能として整理する。ただし拒否的抑止(deterrence by denial)の発想に立つ場合は、この機能は抑止と一体的に論じられうる。次を参照。Romanosky and Boudreaux, "Private-Sector Attribution," p. 478; Eichensehr, "The Law & Politics of Cyberattack," pp. 555-556.
[50]APT グループの定義や特徴などは次を参照。川口貴久「国家が関与するサイバー攻撃と戦略的脅威インテリジェンスの活用」東京海上日動リスクコンサルティング株式会社、2021 年 5 月 18 日、1-3 頁、https://www.tokiorisk.co.jp/publication/report/riskmanagement/pdf/pdf-riskmanagement-353.pdf.
[51]TTPs の概要は次を参照。石川朝久「C12：脅威インテリジェンスの実践的活用法」Internet Week 2020 - Day4 Session 講演資料、2020 年 11 月 24 日、17-21 頁、https://www.nic.ad.jp/ja/materials/iw/2020/proceedings/c12/c12-ishikawa.pdf.
[52]Schwarz, "Turla Teardown: Why Attribute?"; Egloff and Smeets, "Publicly Attributing Cyber Attacks," pp. 7; Rid and Buchanan, "Attributing Cyber Attacks," p. 28; Finnemore and Hollis, "Beyond Naming and Shaming," p. 980; Davis et al., *Stateless Attribution*, p. 17. もっとも TTPs の公表は各国の CSIRT（Computer Security Incident Response Team）や民間セキュリティ企業も日頃から行っており、政府の脅威情報アラートの内容も多くは公開情報に基づく。国家による取り組みの効果は、新たに公表される情報の量、質、タイミングにも依存し、情報セキュリティ専門家からは部分的公表では十分な効果を有さないとの指摘もある。次を参照。Catalin Cimpanu, "US Cyber Command Starts Uploading Foreign APT Malware to VirusTotal," *ZDNet*, November 8, 2018, https://www.zdnet.com/article/us-cyber-command-starts-uploading-foreign-apt-malware-to-virustotal/.
[53]TTPs 公表のカウンターインテリジェンスとしての側面は次を参照。Egloff and Smeets, "Publicly Attributing Cyber Attacks," p. 7. また、刑事訴追や外交官追放については次を参照。Michael Warner, "Intelligence in Cyber-and Cyber in Intelligence," George Perkovich and Ariel E. Levite, eds., *Understanding Cyber Conflict: 14 Analogies*, Georgetown University Press, 2017, pp. 19-20; Gustav Gressel, "Protecting Europe Against Hybrid Threats," *ECFR Policy Brief*, European Council on Foreign Relations, June 15, 2019, pp. 8-9, https://ecfr.eu/wp-content/uploads/6_Protecting_Europe_against_hybrid_threats.pdf.

なお、刑事訴追や外交官追放がサイバー空間をめぐるカウンターインテリジェンスに資するのとの議論は、高度なサイバー攻撃に従事できる能力を持つ人員が限られていることのほか、2018 年 4 月の化学兵器禁止機関（OPCW）事案における近接ハッキングのように、ある種のサイバー攻撃が被害国内から直接行われる場合があり、その場合はオペレーションを統括する外交官身分を有したインテリジェンス・オフィサーや、被害国内における有形無形のインフラ（拠点、使用機材、協力者のネットワークなど）を潰していくことが対処手段の 1 つになりうるからである。

[54]Egloff and Smeets, “Publicly Attributing Cyber Attacks,” p. 5; Broeders, Busser, and Pawlak, “Three Tales of Attribution,” p. 11; Eichensehr, “The Law & Politics of Cyberattack,” pp. 557-558.

[55]Finnemore and Hollis, “Beyond Naming and Shaming,” p. 974, pp. 981-984.

[56]Ibid., pp. 975-976; Henrik Beckvard et al., "Recent Cyber Events: Considerations for Military and National Security Decision Makers," *NATO CCDCOE Recent Cyber Events Series*, No. 10, NATO CCDCOE, May 2021, p. 10, https://ccdcoe.org/uploads/2021/05/Recent-Cyber-Events-10_May-2021.pdf.

[57]Beckvard et al., “Recent Cyber Events,” p. 10; Gold, “The Five Eyes and Offensive Cyber,” pp. 10-11, p. 22.

[58]Anushka Kaushik, "Public Attribution and Its Scope and Efficacy as a Policy Tool in Cyberspace," *ORF Digital Debate 2019*, Observer Research Foundation, October 19, 2019, pp. 38-42; Painter, “Deterrence in Cyberspace,” pp. 6-11.

[59]Michael P. Fischerkeller, “Persistent Engagement and Tacit Bargaining: A Strategic Framework for Norms Development in Cyberspace’s Agreed Competition,” *IDA Document*, Institute for Defense Analysis, November 2018, pp. 1-11, https://www.ida.org/-/media/feature/publications/p/pe/persistent-engagement-and-tacit-bargaining-a-strategic-framework-for-norms-development-in-cyberspaces-agreed-competition/d-9282.ashx. 米国の国防分析研究所（IDA）のフィッシャーケラー（Michael P. Fischerkeller）をはじめとするこの立場は、トマス・シェリング（Thomas C. Schelling）やハーマン・カーン（Harman Kahn）らによる冷戦期の戦略理論の体系を継承し、サイバー空間における規範（cyber norm）を限定戦争遂行時のエスカレーション管理の前提となるフォーカル・ポイント（focal point）に相当するとみる。この立場は武力攻撃の閾値以下のサイバー攻撃事案に、懲罰的抑止とエスカレーションのリスクを梃とした伝統的な抑止の機序は機能しないとし、相手方への攻勢作戦も含むサイバー空間における低強度紛争の積極的な遂行による攻撃者（攻撃国）の能力の破壊や消耗の必要性を説く。この発想を体現したのが、2018 年に米国トランプ政権下で公式化された「執拗な関与（persistent engagement）」と呼ばれるドクトリンである。この点は次を参照。Jason Healey, “The Implications of Persistent (and Permanent) Engagement in Cyberspace,” *Journal of Cyber Security*, Vol. 5, No. 1, August 2019, pp. 2-5.

[60]Joseph S. Nye, Jr., “Deterrence and Dissuasion in Cyberspace,” *International Security*, Vol. 41, No. 3, January 2017, pp. 60–62; Broeders, Boeke, and Georgieva, “Foreign Intelligence in the Digital Age,” pp. 8-9.

[61]Egloff, “Public Attribution of Cyber Intrusions,” pp. 8-9; Florian J. Egloff, “Why Do States Publicly Attribute Cyber Intrusions?” *Net Politic*s, October 14, 2020, https://www.cfr.org/blog/why-do-states-publicly-attribute-cyber-intrusions.

[62]SolarWinds 事案をめぐる概要は、主に次の資料を参照した。山添博史「ロシアをめぐるサイバー問題―ロシアの情報セキュリティ概念と SolarWinds 社事案」日本国際問題研究所編『大国間競争時代のロシア』（令和 2 年度外務省外交・安全保障調査研究事業）2021 年 3 月、104-107 頁; Robert K. Knake, “Why the SolarWinds Hack Is a Wake-Up Call,” *CFR Article*, Council on Foreign Relations, March 9, 2021, https://www.cfr.org/article/why-solarwinds-hack-wake-call; Marcus Willett, “Lessons of the SolarWinds Hack,” *Survival*, Vol. 63, No. 2, March 2021, pp.7-26; Pierluigi Paganini, “6 out of 11 EU Agencies Running Solarwinds Orion Software were Hacked,” *Security Affairs*, April 17, 2021, https://securityaffairs.co/wordpress/116914/hacking/solarwinds-eu-agencies-hacked.html.

[63]Mathew J. Schwartz, “Target Selection: SolarWinds' Orion 'Big Fish' Most at Risk,” *BankInfoSecurity*, December 15, 2020, https://www.bankinfosecurity.com/blogs/target-selection-solarwinds-orion-big-fish-most-at-risk-p-2979.

[64]例えば次を参照。Erica D. Borghard,“Was SolarWinds a Different Type of Cyber Espionage?” *Lawfare*, March 9, 2021, https://www.lawfareblog.com/was-solarwinds-different-type-cyber-espionage; Andy Greenberg, “‘Retaliation’ for Russia’s SolarWinds Spying Isn’t the Answer,” *Wired*, March 8, 2021, https://www.wired.com/story/us-solarwinds-russia-retaliation-cyber-policy/.

[65]SUNBURST は標的のネットワークに侵入後、本格的な情報窃取の開始以前に攻撃に用いる C2 サーバーと接続する段階で、感染した標的のネットワークを識別し得る情報を特殊な形式で暗号化し、防御側に検知されずに攻撃者と共有する機能を備えていた。この情報を通じ攻撃者は、任意に選択した標的に対してのみ追加的なマルウェアを SUNBURST のバックドアを通じて注入し情報窃取を行い得る。その際に、攻撃者は自らの標的ではないターゲットに対して、セキュリティ用語で「キルスイッチ（kill switch）」ともよばれる特定条件下でマルウェアの挙動を停止する機能を駆使し、意図的に SUNBURST が開いたバックドアを使用不可能することで標的の限定を試みていたとされる。SUNBURST の機能による攻撃者の標的限定の手法は、次を参照。Dave Buster, “What You Should Learn from the SolarWinds Attack,” *Global Knowledge*, March 25, 2021, https://www.globalknowledge.com/us-en/resources/resource-library/articles/what-you-should-learn-from-the-solarwinds-attack/; Dmitri Alperovitch and Ian Ward, “How Should the U.S. Respond to the SolarWinds and Microsoft Exchange Hacks?” *Lawfare*, March 12, 2021, https://www.lawfareblog.com/how-should-us-respond-solarwinds-and-microsoft-exchange-hacks.

[66]Brad D. Williams, “SolarWinds Hack: ‘The Truth Is Much More Complicated’,” *Breaking Defense*, March 29, 2021, https://breakingdefense.com/2021/03/solarwinds-hack-the-truth-is-much-more-complicated/.

[67]White House, "FACT SHEET: Imposing Costs for Harmful Foreign Activities by the Russian Government," April 15, 2021, https://www.whitehouse.gov/briefing-room/statements-releases/2021/04/15/fact-sheet-imposing-costs-for-harmful-foreign-activities-by-the-russian-government/. 2021 年 1 月 5 日の段階で、米国政府は「(攻撃に携わった APT グループが）ロシア起源の可能性が高い（likely Russian in origin)」との暫定見解は示したが、ロシア政府に対する公式のパブリック・アトリビューションは本大統領令による。

[68]Dominic Raab, “CYBERUK Conference 2021: Foreign Secretary's Speech,” Foreign, Commonwealth & Development Office (hereafter FCDO) and UK National Cyber Security Centre (hereafter NCSC), May 12, 2021, https://www.gov.uk/government/speeches/cyberuk-conference-2021-foreign-secretarys-speech.

[69]攻撃者の TTPs の公表がもたらす対処・防御機能向上と、攻撃者に対するコスト強要機能について、英国やファイブ・アイズ諸国のインテリジェンス機関が有する認識は次も参照。Schwarz, “Turla Teardown: Why Attribute?”; Danny Palmer, “Naming and Shaming Nations that Launch Cyberattacks Does Work, Say Intel Chiefs,” *ZDNet*, April 26, 2019, https://www.zdnet.com/article/naming-and-shaming-nations-that-launch-cyberattacks-does-work-say-intel-chiefs/.

[70]2021 年 4 月 15 日に公表された米国政府による脅威情報アラートは次を参照。National Security Agency, “Russian Foreign Intelligence Service Exploiting Five Publicly Known Vulnerabilities to Compromise U.S. and Allied Networks,” April 15, 2021, https://www.nsa.gov/News-Features/Feature-Stories/Article-View/Article/2573391/russian-foreign-intelligence-service-exploiting-five-publicly-known-vulnerabili/; US Cyber Command, “US Cyber Command, DHS-CISA Release Russian Malware Samples Tied to SolarWinds Compromise,” April 15, 2021, https://www.cybercom.mil/Media/News/Article/2574011/us-cyber-command-dhs-cisa-release-russian-malware-samples-tied-to-solarwinds-co.

[71]NCSC, “Joint Advisory: Further TTPs Associated with SVR Cyber Actors,” May 7, 2021, https://www.ncsc.gov.uk/news/joint-advisory-further-ttps-associated-with-svr-cyber-actors.
[72]サイバー諜報をめぐる米国やファイブ・アイズ諸国のスタンスは次を参照。Erica D. Borghard, “Punitive Response to SolarWinds Would Be Misplaced, But Cyber Deterrence Still Matters,” *Russia Matters*, March 31, 2021, https://russiamatters.org/analysis/punitive-response-solarwinds-would-be-misplaced-cyber-deterrence-still-matters; Sergei Boeke and Dennis Broeders, “The Demilitarisation of Cyber Conflict,” *Survival* , Vol. 60, No. 6, November 2018, pp. 74-77, p. 85; Asaf Lubin, “SolarWinds as a Constitutive Moment: A New Agenda for International Law of Intelligence,” *Just Security*, December 23, 2020, https://www.justsecurity.org/73989/solarwinds-as-a-constitutive-moment-a-new-agenda-for-the-international-law-of-intelligence/.
[73]Egloff, “Public Attribution of Cyber Intrusions,” p. 9; Eichensehr, “The Law & Politics of Cyberattack,” p. 548; Kristen Eichensher, “‘Strategic Silence’ and State-Sponsored Hacking: The US Gov’t and SolarWinds,” *Just Security*, December 18, 2018, https://www.justsecurity.org/73921/strategic-silence-and-state-sponsored-hacking-the-us-govt-and-solarwinds/.
[74]Alperovitch and Ward, “How Should the U.S. Respond,”; Borghard, “Punitive Response to SolarWinds,”.
[75]例えば 2015 年に発覚した米国人事管理局（OPM）からの情報窃取は、中国政府の関与の可能性が広く報じられ、後に実行犯個人への刑事訴追もなされたが、同事案について米国政府は中国政府の関与を公式に断定したうえでの外交的非難や対中制裁にまでは至らなかった。ジェームズ・クラッパー（James Clapper）元米国家情報長官が回顧するところによれば、当時、米国政府もまた同様の行為に手を染めうる中国の情報窃取に、公式の非難や制裁を行うことへの躊躇があったことが明らかになっている。次を参照。Egloff, “Public Attribution of Cyber Intrusions,” p. 9; Davis et al., *Stateless Attribution*, p. 7. なお APT29 についても、米国などがロシア政府との関係を断定し、サイバー諜報との咎で公式に非難したのは今回が初となる。次を参照。Emily Taylor, “Biden’s Sanctions Targeting Russian Cyber Behavior Could Backfire,” *World Politics Review*, April 20, 2021, https://www.worldpoliticsreview.com/articles/29585/the-danger-of-treating-solarwinds-as-a-russia-cyber-attack.
[76]標的のネットワークやシステムへの侵入を伴うサイバー諜報と破壊活動（狭義のサイバー攻撃）の手順と識別困難性の問題は次を参照。Max Smeets, “Integrating Offensive Cyber Capabilities: Meaning, Dilemmas, and Assessment,” *Defence Studies* Vol. 18, No. 4, October 2018, pp. 397-400, pp. 402-403; Max Smeets and Herbert Lin, “Offensive Cyber Capabilities: To What Ends?” T. Minárik, R. Jakschis, and L. Lindström., eds., *10th International Conference on Cyber Conflict CyCon X: Maximising Effects*, NATO CCDCOE, 2018, pp. 59-60.
[77]別途注が無い限り、本段落の記述は次の文献の内容を参照。Martin Libicki, “The Coming of Cyber Espionage Norms,” H. Rõigas et al., eds., *9th International Conference on Cyber Conflict: Defending the Core*, NATO CCDCOE, 2017, pp. 7-23; Broeders, Boeke, and Georgieva, “Foreign Intelligence in the Digital Age,” p. 4; Lubin, “SolarWinds as a Constitutive Moment.”; Michael Warner, “A Matter of Trust: Covert Action Reconsidered,” *Studies in Intelligence* Vol. 63, No. 4, December 2019, pp. 33–41; Borghard, “Punitive Response to SolarWinds,”
[78]Libicki, “The Coming of Cyber Espionage Norms,” pp. 7-23; Broeders, Boeke, and Georgieva, “Foreign Intelligence in the Digital Age,” p. 1-3, pp. 8-9; Ilina Georgieva, “The Unexpected Norm-Setters: Intelligence Agencies in Cyberspace,” *Contemporary Security Policy*, Vol.41, No. 1, January 2, 2020, pp. 33-54. 特に、サイバー諜報の標的、手法、窃取した情報の利用法（リークによる選挙干渉や組織犯罪への転用）などに着目した、許容し得る原則と許容し得ない例外の線引きの可能性や、サイバー諜報で各国が享受する利益や、インテリジェンス機関の活動の秘匿性にも照らし、規範の相互遵守や履行検証のメカニズムが設計可能か否かにつき議論が重ねられてきた。
[79]“Biden Chief of Staff Says Hack Response Will Go Beyond 'Just Sanctions'," *Reuters*, December 21, 2020, https://www.reuters.com/article/usa-cyber-breach-idUSKBN28U0IK.
[80]White House, “Press Briefing by Press Secretary Jen Psaki and Deputy National Security Advisor for Cyber and Emerging Technology Anne Neuberger, February 17, 2021,” February 17, 2021, https://www.whitehouse.gov/briefing-room/press-briefings/2021/02/17/press-briefing-by-press-secretary-jen-psaki-and-deputy-national-security-advisor-for-cyber-and-emerging-technology-anne-neuberger-february-17-2021/.
[81]Kristen Eichensehr, “SolarWinds: Accountability, Attribution, and Advancing the Ball,” *Just Security*, April 16, 2021, https://www.justsecurity.org/75779/solarwinds-accountability-attribution-and-advancing-the-ball/; Andy Greenberg, “US Sanctions on Russia Rewrite Cyberespionage’s Rules,” *Wired*, April 15, 2021, https://www.wired.com/story/us-russia-sanctions-solarwinds-svr/.
[82]Robert Chesney, “Sanctioning Russia for SolarWinds: What Normative Line Did Russia Cross?” *Lawfare*, April 15, 2021, https://www.lawfareblog.com/sanctioning-russia-solarwinds-what-normative-line-did-russia-cross; Jamie MacColl, “The UK’s Approach to Russian Cyber Operations Shows No Signs of Changing,” *RUSI Commentary*, Royal United Services Institute, May 21, 2021, https://rusi.org/commentary/uk-approach-russian-cyber-operations-shows-no-signs-changing.
[83]FCDO, “Russia: UK Exposes Russian Involvement in SolarWinds Cyber Compromise,” April 15, 2021, https://www.gov.uk/government/news/russia-uk-exposes-russian-involvement-in-solarwinds-cyber-compromise.
[84]元々英国は、詳細な規範の内容には言及せずに曖昧にとどめる公式非難声明を好むが、それでもなおジョージア事案と APT10 事案では、国際法や G20 でのサイバー知財窃取の停止をめぐる合意などに照らし、規範の侵害や許容し得ない性質に言及している。次を参照。Foreign & Commonwealth Office (hereafter FCO) and NCSC, “UK Condemns Russia's GRU over Georgia Cyber-attacks,” February 20, 2020, https://www.gov.uk/government/news/uk-condemns-russias-gru-over-georgia-cyber-attacks; FCO and NCSC, “UK and Allies Reveal Global Scale of Chinese Cyber Campaign,” December 20, 2018, https://www.gov.uk/government/news/uk-and-allies-reveal-global-scale-of-chinese-cyber-campaign.
[85]民間企業のサプライチェーンを駆使した各国のサイバー諜報や、産業競争力強化を目的とした知財窃取との線引きは次を参照。Libicki, “The Coming of Cyber Espionage Norms,” pp. 1-4; Alperovitch and Ward, “How Should the U.S. Respond,”; Greenberg, “ ‘Retaliation’ for Russia’s,”.
[86]The Hague Program for Cyber Norms, “Rethinking Cyber Espionage After the Solarwinds Hack,” *Youtube Video*, 22:00-23:00, https://www.youtube.com/watch?V=fqjg1aochbc.
[87]内閣サイバーセキュリティセンター「資料 1－2『次期サイバー』」、22-23 頁。
[88]エグロフとスミートは、各国政府によるパブリック・アトリビューションは、各国がこの取り組みのもとで達成したい一貫した戦略目標（consistent goal）をもって実施されることが重要だと言及し、事案の性質によっては各国がパブリック・アトリビューションを実施しないことが好ましい場合もあると指摘する。Egloff and Smeets, “Publicly Attributing Cyber Attacks,” p. 1, pp. 21–23.