パブリックアトリビューションの「拡散」と「多様化」
――政策当局間の「多様化」の国際比較研究――

瀬戸　崇志

＜要旨＞

本稿では、2010 年代後半のサイバー攻撃のアトリビューションに関する学術研究の新たな発展を検討し、その研究関心であるパブリックアトリビューションの「拡散」と「多様化」という現象のうち、政策当局間での「多様化」の要因とモデルの把握を試みた。本稿が比較対象とした米国司法省の刑事手続と欧州連合の制裁手続に付随したパブリックアトリビューションは、いずれも本来的には国家ではなく自然人・法人を対象とし、対象の権利保護のために制度が要求する手続的な制約も類似する。しかし、両者は「司法手続の政策化」と「政治対立の司法化」と表現しうる異なる要請に導かれ、近年の運用の様式や実績を異にしてきた。この結果は、政策当局間でのパブリックアトリビューションの「多様化」が、その（ⅰ）目的とオーディエンスの変化と、分析に要する機微な情報の収集・共有・公表の制約などの（ⅱ）施策の自由度を縛る政策過程の構造の双方の要因によって規定されうることを示した。

はじめに

2021 年 4 月 22 日、日本の警察庁は、2016 年以降に日本の宇宙航空研究開発機構（JAXA）や約 200 以上の国内企業などを標的にした一連のサイバー攻撃事案について「Tick と呼ばれるサイバー攻撃集団によって実行され、当該 Tick の背景組織として（中略）中国人民解放軍戦略支援部隊ネットワークシステム部第 61419 部隊が関与した可能性が高い」との分析を公表した[1]。当該対応は、日本政府が、上述の 2016 年以降の一連のサイバー攻撃[2]事案への組織的関与について中国政府機関に対するアトリビュ―ション（attribution）に至り、そのうえでパブリックアトリビューション（public

1　警察庁「国家公安委員会委員長記者会見要旨」2021 年 4 月 22 日、https://www.npsc.go.jp/presscon f_2021/04_22.htm.　なお警察庁の会見に先立つ 2021 年 4 月 20 日に、警視庁公安部が東京地方検察庁に対して、当該事案の攻撃インフラとして悪用された日本のレンタルサーバーの契約を行った中国籍の男を書類送致している。

2　本稿が特に断り無く「サイバー攻撃」の用語を用いる場合は、法的には、その目的や技術的類型を問わない再広義の総称概念を指す「サイバー活動（サイバー作戦：cyber operations）」と同義で用いる。次を参照。黒崎将広他 編『防衛実務国際法』（弘文堂、2021 年）240–248 頁。

attribution）（以下：PA）と呼ばれる、その成果の戦略的な公表に踏みきった例としても知られる。

こうした各国の政策当局による PA は、2017 年以降の欧米諸国の安全保障研究を中心に大きな関心を集めてきたが、この時期のアトリビューションをめぐる学術研究は、2010 年代後半に顕在化した PA の「拡散」と「多様化」と表現できる現象と呼応して発展を遂げてきた。これは第 1 節で詳述するが、2010 年代後半にかけて、主に欧米諸国の政府機関や民間セキュリティ企業が、サイバー攻撃のアトリビューションの成果の公表を政策手段や商慣行の一部として受容しつつも、その対象事案、公表される情報の質量、公表の媒体、実施時期などにばらつきが見られることを指す。アトリビューションが国際法上の自衛権行使や懲罰的抑止の前提条件と捉える 2010 年代前半の先行研究の立場を仮に「第 1 世代」の議論[3]とすれば、これと比較して近年の先行研究の議論の射程は PA の「拡散」と「多様化」に呼応して変化を遂げており、「第 2 世代」の先行研究と呼ぶに値する。

しかし日本国内の安全保障研究では、この PA の「拡散」と「多様化」の問題と車の両輪の関係である「第 2 世代」の先行研究の発展は、体系的な分析の対象とはされてこなかった。また欧米諸国の先行研究でも、PA の「多様化」という現象が、なぜ、どのようなプロセスにより生じるかについて国際比較に基づく実証研究を試みたものは、依然乏しい状況にある。

以上より本稿は、その発展の経緯も含めて「第 2 世代」の先行研究を検討しつつ、政策当局間の PA をめぐる取組の国際比較を通じて、PA の「多様化」の要因とモデルを明らかにすることを試みる。特に本稿では、米国司法省（DOJ）（以下：米司法省）の刑事手続と欧州連合（EU）とその加盟国によるサイバー攻撃関連制裁レジームの運用を通じたパブリックアトリビューションの追求に着目した比較事例研究を試みる。

本稿が比較対象とした米司法省と EU の取組は、いずれも本来的には国家機関ではなく自然人・法人を対象とし、この点に由来した制度が要求する手続的な制約も類似する。ここで事例研究の結論を先取りすれば、両者の取組はそれにもかかわらず、「司法手続の政策化」と「政治対立の司法化」とも表現しうる異なる要請に導かれ、2010 年代後半にその運用の様式・実績を異にしてきた。この結果は、各国の政策当局間での PA の「多様化」は、PA の目的の相違や変化のみならず、アトリビューションに必要な機微情報の共有・公表をめぐる多様な利害関係者間の政治的対立をはじめとして、

3　2015 年頃までのアトリビューションの議論の射程の参考としては次を参照。川口貴久「米国におけるサイバー抑止政策の刷新 ── アトリビューションとレジリエンス」『KEIO SFC Journal』第 15 巻 2 号（2015 年 2 月）84–87 頁、89–90 頁。

政策当局の施策の自由度を縛る政策過程の構造にも規定されうる点を裏付ける。

本稿は次の構成をとる。第1節では、2010年代後半のPAの「拡散」と「多様化」に伴う「第2世代」の先行研究の発展の経緯を念頭に、本稿の（パブリック）アトリビューションの概念を定義し、一連の先行研究の検討と課題をふまえて事例研究の分析枠組を構築する。第2節と第3節では、米司法省とEUの施策と制度を概観し、各種の公文書や先行研究から、2010年代後半での双方の施策の運用をめぐる異なる発展の経緯と要因を分析する。「おわりに」では本稿の事例研究の結論を要約し、その含意と将来の研究課題を示す。

1．問題の所在と分析枠組

（1）サイバー攻撃のアトリビューションの概念と実践をめぐる多義性

サイバー攻撃のアトリビューションは、攻撃に対する政策対応や法的責任の立証を念頭に、これを実行した人物や組織、更にはその指揮統制の責任を負う国家（機関）の特定を目指す取組として、サイバー攻撃を「誰がやったのか（who did it）」の問題とも形容されてきた[4]。例えばハーバート・リン（Herbert Lin）の論文が掲げる（ⅰ）使用機器、（ⅱ）実行者、（ⅲ）責任を負う敵対者の3段階での分析の到達過程を想定した定義[5]にせよ、実務家が用いる「MICTICフレームワーク」や「ダイアモンドモデル（Diamond model）」などの方法論[6]にせよ、この取組が、究極的には攻撃の背後に存在する主体を把握する「情報収集・分析」の営為である点には一致をみてきた。

一方で、トマス・リッド（Thomas Rid）らも指摘してきたように、アトリビューションは、情報収集・分析の段階を超えて、実施主体の目的達成のために、分析の成果物を第三者に提示する「コミュニケーション」の段階を必ず含む[7]。フロリアン・エグロフ（Florian J. Egloff）によれば、PAとは、この成果物のコミュニケーションの段階で、機密指定などで成果物の提示対象の第三者を限定せずに、一般に広く公表する行為を

4　この点は、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；Thomas Rid and Ben Buchanan, “Attributing Cyber Attacks,” *Journal of Strategic Studies*, vol. 38, no. 1–2（January 2015), p. 8.

5　リンの定義は、次を参照。Herbert Lin, “Attribution of Malicious Cyber Incidents：From Soup to Nuts,” *Journal of International Affairs*, vol. 70, no. 1（Winter 2016), pp. 75–137.

6　各国政府機関や民間セキュリティ産業の実務の要請のなかで体系化されてきたアトリビューションのための情報収集･分析の方法論の動向は、次を参照。石川朝久『脅威インテリジェンスの教科書』（技術評論社、2021年）280–349頁。

7　Rid and Buchanan, “Attributing Cyber Attacks,” pp. 26–30.

指す[8]。

そのうえで、近年の学術研究の議論や実務上の（パブリック）アトリビューションの実践は、「誰がやったのか」との比喩に還元しきれない 2 つの論点を含んでいる。

第 1 の論点は、把握を目指す「誰」の想定の拡大であり、この点を象徴するのは近年の民間セキュリティ産業を中心とする脅威アクター（攻撃グループ：threat actor）の水準のアトリビューションの慣行である。これは民間のセキュリティ企業や専門機関が、攻撃キャンペーンと呼ばれる特定国・地域や業種などを標的として反復・継続するサイバー攻撃の観測データをふまえ、その痕跡（Indicator of Compromise：IoC）[9]や攻撃手法（Tactics Techniques Procedures：TTPs）[10]からなる侵入セット（Intrusion-sets）と呼ばれるパターンを見出し、それに「APT ○○」や「○○ Bear」などの情報共有用の識別名を付した「脅威アクター」を特定する作業となる[11]。留意すべきは、この「脅威アクター」とは、攻撃キャンペーンのツール・インフラなどの「手口（how）」の特徴や、被害の地理的分布や標的業者の傾向などから推論される「動機（why）」を、いわば「擬人化」した存在であり[12]、例外的条件がある場合を除けば、必ずしも個人の刑事責任や国家責任の国際法上の帰属を立証しうる具体的な実行犯や国家機関までをも特定するものではない[13]。

8　Florian J. Egloff, “Public Attribution of Cyber Intrusions,” *Journal of Cybersecurity* , vol. 6, no. 1（September 2020), pp. 6–7.

9　正式には「侵害指標」と訳され、「実際に発生した攻撃情報を特定するための技術的特性情報」を意味する。ファイルのハッシュ値、接続先の IP アドレス・ドメイン名、マルウェアが被害 PC 上に残すレジストリや一時ファイルなどが含まれる。IoC の定義・概念は次を参照。石川『脅威インテリジェンス』28–33 頁。

10 攻撃者の利用する攻撃手法のパターンを指す。厳密には「戦術（Tactics）」が、標的への侵入の過程で攻撃者が達成する中間目標（例：認証情報へのアクセス）、「技術（Techniques）」が、「戦術」を達成する具体的な技術・ツール、そして「手順（Procedures）」が、この「戦術」と「技術」の組み合わせを通じた、攻撃者の一連の行動様式を指すとされる。次を参照。石川『脅威インテリジェンス』50–51 頁。

11 IoC/TTPs や侵入セットの概念を含む一連のプロセスは、次の文献を参照。Timo Steffens, *Attribution of Advanced Persistent Threats - How to Identify the Actors Behind Cyber-Espionage*（Wiesbaden: Springer Vieweg, 2020), pp. 26–41, pp. 197–199; 石川『脅威インテリジェンス』280–289 頁。

12 そのため、例えば汎用の攻撃ツールの利活用を通じて複数の脅威アクター間で TTPs の重複が見られるときなどは、当該 TTPs がいずれの「脅威アクター」と結びくつくのか否かの絞り込み自体が困難を極め、アトリビューションは一層困難となる。次を参照。 佐々木 勇人「パブリックアトリビューションの課題－大規模なサイバー攻撃や国際的イベントへのサイバー攻撃事例から」『CISTEC journal』第 194 号（2021 年 7 月）130–138 頁；John Sakellariadis, “The SolarWinds Hack and the Perils of Attribution,” *Recorded Future*, January 6, 2021, https://therecord.media/the-solarwinds-hack-and-the-perils-of-attribution/.

13 侵入セットの擬人化としての「脅威アクター」と、その背後に居る「実行犯」や「国家機関」の関係性を立証する粒度でのアトリビューションは、その目的や必要な情報源の性質に鑑みると、短期的な時間軸では政府の法執行機関やインテリジェンス機関の領分となりやすい。ただし（1）攻撃者の運用保全上の過失により、その個人情報などが容易に特定可能な場合や、(2) 中長期的な時間軸では、過去に政府機関などが公表した「実行犯」や「国家機関」の侵入セットの特徴と、民間企業・専門機関が観測していた既知の「脅威アクター」のものが強く符合する場合などには、政府機関でなくとも特定の「脅威アクター」と「実行犯」や「国家機関」の関係を見出すことが可能な場合もある。以上の点は例えば次を参照。佐々木「パブリックアトリビューション」131–133 頁；Steffens, Attribution, pp.39–40, pp.165–166; Milton Mueller et al., “Cyber Attribution: Can a New Institution Achieve Transnational Credibility?” *The Cyber Defense Review*, vol. 4, no.1 (Spring 2019), pp. 108–110.

第 2 に、水面下の「情報収集・分析」と「(PA を含む) コミュニケーション」の成果物に生じうるギャップである。例えば上記の脅威アクターの水準のアトリビューションは、刑事責任や国際法上の帰属の立証には足りずとも、ネットワーク防衛担当者への注意喚起文書 (security alerts) (以下:注意喚起)[14] の発出と対策情報共有のためには、この成果物の時宜を得た流通が実行犯や国家機関の名称よりも重要となる[15]。こうした目的に応じた成果物の要請の差に加え、情報収集・分析に利用しうる情報源の機微度の差に応じて、事案対応の関係者のみで進む水面下の「情報収集・分析」の段階でのアトリビューションの成果物と、PA の段階で「一般公表」されうる成果物は一致しないケースが存在する[16]。

こうした実践のなかで、ティモ・ステフェンス (Timo Steffens) らを筆頭とする近年の主要な先行研究は、安全保障研究や法学研究の文脈で意識される具体的な実行犯 (自然人) や国家機関の水準に留まらない、より多様な粒度 (granularity)[17] を持つアトリビューションの成果物の利活用や、情報収集・分析段階とコミュニケーションの段階のギャップも念頭に、(パブリック) アトリビューションのプロセスを包括的に概念化してきた[18]。

以上を踏まえ、本稿も「アトリビューション」を、ある主体による「攻撃キャンペーンの背後の実行主体 (以下:攻撃者) と、その手口・動機などの攻撃者の属性の把握を目的とした情報収集・分析に始まり、その分析の成果物の第三者に対するコミュニケーションの段階までを含むプロセス」と定義する。この定義における「攻撃者」に

14 脆弱性情報をはじめとする各種のセキュリティ対策に資する技術的情報の通知で、一般的に機械判読ではなく対策担当者が読むことを想定したものの総称。この概念の定義については次を参照。Christopher S. Johnson et al., *Guide to Cyber Threat Information Sharing*, NIST-SP 800-150 (Gaithersburg, MD: National Institute of Standards and Technology, 2016), p. 2, http://dx.doi.org/10.6028/NIST.SP.800-150.

15 Brian Bartholomew and Juan Andrés Guerrero-Saade, "Wave Your False Flags! Deception Tactics Muddying Attribution in Targeted Attacks," (conference paper presented at Virus Bulletin Conference 2016, Denver, CO, USA: Virus Bulletin, October 2016), p. 9, https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2017/10/20114955/Bartholomew-GuerreroSaade-VB2016.pdf.

16 その典型例は、各国政府が他国の政府機関への PA に際して、機微な情報源の保護のために一切の技術的な証拠を示さずに分析の結論のみを公表する場合である。こうした対応の背景と論点は、以下の文献を参照。William Hoverd, "Cyber Threat Attribution, Trust and Confidence, and the Contestability of National Security Policy," in *Emerging Technologies and International Security*, ed. Reuben Steff, Joe Burton, and Simona R.Soare, (London: Routledge, 2020), pp. 221–239; 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.

17 ここでの「粒度」とは、アトリビューションの「分析の絞り込みの度合い」や、PA として「公表する分析の成果物の情報量」と言い換えることもできる。具体的には分析の成果物には、サイバー攻撃に関与した実行犯の個人名や国家機関の特定には至らない多様な到達水準が存在し、特定の攻撃で用いられたマルウェアと既知の脅威アクターの TTPs の関係性や、攻撃者が所在する領域国などの水準でのアトリビューションもありうる。また、政府や民間企業が PA として公表する内容も、あえて具体的な実行犯や国家機関の責任を名指しせず、攻撃者の所在国や「脅威アクター」の名指しに留まる場合なども存在する。

18 前掲注 17 を含め、この点は次の文献を参照。Steffens, *Attribution*, pp. 33–41, pp.173–180; 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 2020), pp. 974–998.

は、具体的な実行犯や国家機関の特定には至らない「脅威アクター」の粒度も含まれる。また PA とは、この定義の「コミュニケーション」の段階での「特定の攻撃者にまつわる分析の成果物」の「一般公表」と整理したうえで、具体的な成果物の粒度を都度明記する。

（2）2010 年代後半の PA の「拡散」と「多様化」

前項の概念と実践の多様性の議論も含め、特に 2010 年代後半におけるアトリビューションをめぐる学術研究の議論の射程は、2010 年代前半の想定よりも大幅に拡大してきた。その背景には、PA の「拡散」と「多様化」と表現しうる近年の現象の影響が見受けられる。

PA の「拡散」とは、ここでは次の 2 つの現象を指す。第 1 に、（米国を超えた）自由民主主義諸国の外交・安全保障当局間における PA の政策伝播である。特に 2017 年の「WannaCry」の世界的な感染拡大を筆頭とする相次ぐ国際的な重大事案と、これらに対する米英両国主導の同盟・同志国連携での対応などを経て、PA は欧米諸国の外交・安全保障当局の間で、他国政府機関が関与しつつも国際法上の武力攻撃には至らない烈度のサイバー攻撃事案に対処する政策手段として受容されてきた[19]。第2に、民間セキュリティ産業を起点としたアトリビューションをめぐる市場の形成である。特に北米圏を起点とするサイバー脅威インテリジェンス（cyber threat intelligence：CTI）の概念や産業の成熟に伴い、先述の脅威アクターの PA は欧米諸国の民間セキュリティ企業の商慣行として受容され、この動向は政府の PA への姿勢にも影響を与えてきた[20]。

PA の「多様化」とは、この「拡散」の傾向のなかで、各国政府機関や民間企業による PA が、その対象とする事案、分析の粒度、公表する媒体、分析の根拠証拠として付される情報の質量、そして公表時期などの面でのバリエーションを見せてきた現象を指す[21]。例えば 2017 年以降の米英両国主導の PA をめぐる同盟・同志国連携への

19 次を参照。Keir Giles and Kim Hartmann, “ ‘Silent Battle’ Goes Loud: Entering a New Era of State-Avowed Cyber Conflict,” in *11th International Conference on Cyber Conflict: Silent Battle. Proceedings 2019*, ed. T. Minárik et al.（Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, May 2019), pp. 23–35; 瀬戸崇志「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」『NIDS コメンタリー』第 179 号（2021 年 7 月）3–5 頁、http://www.nids.mod.go.jp/publication/commentary/pdf/commentary179.pdf.

20 特に、米国の CTI 産業の成熟が政府の PA の慣行に与えてきた影響は、次を参照。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 (July 2021), pp. 463–93; J. D. Work, “Evaluating Commercial Cyber Intelligence Activity,” *International Journal of Intelligence and CounterIntelligence*, vol. 33, no. 2（April 2020), pp. 278–308.

21 その全般的な傾向は次を参照。Garrett Derian-Toth et al., *Opportunities for Public and Private Attribution of Cyber Operations*, NATO CCDCOE Tallinn Paper, no.12 (Tallin: NATO Cooperative Cyber Defence Centre of Excellence, 2021), pp. 7–11, https://ccdcoe.org/uploads/2021/08/Tallinn_Papers_Attribution_18082021.pdf.

EU 加盟国の対応を例にとれば、エストニア政府のように米英両国と連動して外交当局声明での攻撃国の非難に踏み込み、後述の PA による規範設定機能の意義を強調する国[22]もあれば、フランス政府のように攻撃国への公然な非難は回避しつつ、攻撃国への 2 国間の外交ルートでの警告や、民間企業になぞらえた「脅威アクター」の粒度の技術的な分析の公表に留める国もある[23]。

（3）「第 2 世代」の先行研究が提示する「多様化」の分析のための 2 つの視角

この PA の「拡散」と「多様化」という現象を横目に発展してきた 2017 年以降の先行研究を仮に「第 2 世代」の先行研究と呼称すれば、その要請とは、理論上の可能性の議論を超えて、現実に観測可能となった世界各国の官民によるアトリビューションの動態を解明することにある。その論点は多岐にわたるが、本稿が着目する PA の「多様化」の要因を捉えるうえでは、近年の先行研究が提示する次の 2 点の分析の視角をおさえる必要がある。

第 1 の視角は、欧米諸国の学術研究での戦略的コミュニケーション（strategic communication）の議論[24]に近しい発想から、PA に伴う情報や言説の発信を触媒とした、多種多様なオーディエンス（audience）の行動変容による政策的機能を見出す立場である。先のエグロフやステフェンスに加え、マーサ・フィネモア（Martha Finnemore）らの先行研究に代表されるこの立場は、各国政府や民間企業の PA には、その目的と、そのために成果物の公表を梃に行動変容を促すオーディエンスが複数想定されると捉え、その組み合わせに応じて、PA の対象事案、成果物の公表の是非、要求される特定の粒度、分析に付すべき証拠の質量、適切な公表媒体や時期などが変化しうることを指摘してきた[25]。

第 1 の視角の例示として、表 1 がある。これはエグロフとマックス・スミーツ（Max Smeets）の共同研究が提唱した「パブリック・アトリビューション・フレームワーク（Public Attribution Framework）」が示す、政府の PA の主要な政策目的の 6 類型を土

22 エストニアの近年の姿勢は次を参照。Piret Pernik, *Cyber Deterrence: A Case Study on Estonia's Policies and Practice*, Hybrid CoE Papers no. 8 (Helsinki: The European Centre of Excellence for Countering Hybrid Threats, October 2021), pp. 16–18.

23 フランスの近年の姿勢は次を参照。Alix Desforges and Aude Géry, "France Doesn't Do Public Attribution of Cyberattacks. But It Gets Close," *Lawfare*, September 3, 2021, https://www.lawfareblog.com/france-doesnt-do-public-attribution-cyberattacks-it-gets-close.

24 この「オーディエンス」の概念を含めた、近年の学術研究における戦略的コミュニケーションの概念と機能の議論については、次を参照。青井千由紀『戦略的コミュニケーションと国際政治－新しい国際政治の理論』（日本経済新聞出版、2022 年）23–47 頁。

25 Florian J. Egloff and Max Smeets, "Publicly Attributing Cyber Attacks: A Framework," *Journal of Strategic Studies*, Published online (March 2021), pp. 5–8, https://doi.org/10.1080/01402390.2021.1895117; Steffens, *Attribution*, pp. 173–180.

台にしつつ、本稿の筆者が近年の学術研究の指摘を踏まえ、その目的の達成に至る機序や、その過程で念頭にあるオーディエンスについて補足する情報を追加・整理したものである。この表 1 の内容が象徴するのは、近年の先行研究が、PA の機能をネーム・アンド・シェイム（name and shame）と呼ばれる概念に基づく「相手国を非難して辱めることがコストとなり将来の攻撃を抑止する」と捉える単純化された想定を採用していないことにある [26]

表 1　政策当局のパブリックアトリビューションの主要な政策目標と作用の機序

①　強制 Coercion	主に現在の敵対国などの意思決定者をオーディエンスに、その「意図（intentions）」（費用対効果計算）に作用して将来の行動変容を促す作用。抑止（deterrence）もその一類型。後続の報復措置の脅しによる懲罰的抑止を超え、②の脅威対抗や④の予防・防御の継続を通じた、能力の再調達や目標達成コストの上昇（累積）による拒否的抑止の機序も含む。
②　脅威対抗 Counter-threat	主に現在の敵対国を念頭に置くが、相手方の（継戦）「能力（capabilities）」に作用し、攻撃キャンペーンの一時的な妨害（disruption）を狙う防諜政策の論理（①と異なり、攻撃者の意図・判断での行動変容を前提としない）。オーディエンスと作用の機序は複数あり、IoC/TTPs などの暴露とネットワーク防衛強化による相手方の攻撃手法の無力化（burn）や、攻撃者とキャンペーンの暴露を触媒とした官民・国際連携を通じ、相手方の要員・資金・攻撃ツール / インフラの調達と維持を妨げる措置を導く機序も含む。
③　規範設定 Norm-setting	主に将来的に規範を共有する余地のある第三国をオーディエンスとする作用。敵対国が関与した一定の性質を備える攻撃を公然と非難し、その違法性または合法でも許容しえないとのメッセージを国際社会に示すことで、国際法やソフトローの形成と適用を促す。規範を共有しえない敵対国よりも、将来のサイバー攻撃能力の拡散を念頭に、同盟国や潜在的競争国の能力の運用政策を規範に沿った穏健なものに誘導することが主な狙いとなる。
④　予防・防御 Prevention & defense	主に自国や同盟国を含む第三国の公的機関・民間セクターのネットワーク防衛担当者や意思決定者をオーディエンスとし、注意喚起を通じた官民のネットワーク防衛の強化を促す。この目的は、原理上はアトリビューションが無くとも達成可能だが、IoC/TTPs などの技術情報と紐づけた脅威アクターや他国政府機関などの名指しは、注意喚起対象の事案の重大性・喫緊性の強調と攻撃者の意図や標的業種などの脅威の文脈（context）の情報の付与を通じ、注意喚起の接受者側の優先的な対策導入を促す。

26 PA の機能をネーム・アンド・シェイムの概念と互換的に捉える傾向への批判は、次を参照。Finnemore and Hollis, “Beyond Naming and Shaming,” pp. 971–977.

⑤ 共同体形成 Community -building	国内外の政策当局者や、脅威情報の分析にかかわる（官民の）セキュリティ専門家などをオーディエンスとする作用。事案発生からアトリビューションの公表に至る前後での情報共有や政策調整の過程の累積を通じて、事案対処に携わる当局者・専門家の相互の信頼構築や実務協力の深化を促す。
⑥ 正統性・評価獲得 Legitimacy& reputation building	自国民・同盟国の世論などをオーディエンスとする作用。アトリビューションの公表を通じて、自国の情勢認識や対外政策をめぐる国内外からの政治的支持の形成や各省庁の施策強化や予算獲得の正統性を強化する。

（出所）Egloff and Smeets, “Publicly Attributing,” pp. 1–32 の政策目的の類型を基に、その作用の機序などにつき各種先行研究[27]を参照して執筆者が補足する形で作成。

この第1の視角からは、PA の「多様化」現象は、主に PA の実施主体の戦略目標やオーディエンスへの認識（の変化）に基づく能動的な選択の帰結と説明しうる。例えば予防・防御の作用を狙う場合、PA の成果物には脅威アクターの IoC/TTPs などの技術的な脅威情報や、その対策手法を含むことが重要であり、実行犯の個人名や他国の政府機関の名指しは従たる要素に過ぎない。しかし、仮に規範設定の作用を重視するならば、技術的な情報よりも、むしろ規範的な言説を付して攻撃国を糾弾する必要性が高くなる[28]。各国政府は、このように個々の認識する目的に応じた合理的選択として、PA の実施の是非や様式を調整しているとの捉え方が可能となる。

第2の視角は、アトリビューションをめぐる政治（politics of attribution）に着目した捉え方である。これはアトリビューションを、官民・国内外の多様な利害関係者（以下：アクター）の目的と依拠する制度の異なる複数の経路が並走する政策過程と捉え、そのなかでの取組の技術的・法的・政治的要請が競合する現象に着目する[29]。この立場は政策過程での異なるアクターと制度の相互作用が、情報収集・分析からコミュニケー

27 表1の6つの主要な政策目標に対応したオーディエンスと作用の機序の記述には、出所内に明記したエグロフとスミーツの共同研究のほか、特に以下の先行研究を参照している。Egloff, “Public Attribution,” pp. 7–10; Steffens, *Attribution*, pp.23–26, pp.173–182; Romanosky and Boudreaux, “Private-Sector Attribution,” pp. 478–479; Jon Bateman, “The Purposes of U.S. Government Public Cyber Attribution,” in *Managing U.S.-China Tensions Over Public Cyber Attribution*, ed. Ariel E. Levite et al.（Washington, D.C: Carnegie Endowment for International Peace, 2022), pp. 14–24; Jason Healey, Neil Jenkins, and J. D. Work, “Defenders Disrupting Adversaries: Framework, Dataset, and Case Studies of Disruptive Counter-Cyber Operations.” in *12th International Conference on Cyber Conflict. 20/20 Vision: The Next Decade. Proceedings 2020*, ed T. Jančárková et al. (Tallinn: Estonia: NATO Cooperative Cyber Defence Centre of Excellence), pp. 251–274; Erica D. Borghard and Shawn W. Lonergan, “Deterrence by Denial in Cyberspace,” *Journal of Strategic Studies*, Published Online (August 2021), pp. 1–36, https://doi.org/10.1080/01402390.2021.1944856.

28 Steffens, *Attribution*, p. 180; Finnemore and Hollis, “Beyond Naming and Shaming,” pp. 974–998.

29 この「アトリビューションをめぐる政治」の発想は、例えば次を参照。Kristen Eichensehr, “The Law & Politics of Cyberattack Attribution,” *UCLA Law Review*, vol. 67, no. 3 (July 2020), pp. 520–599; Annegret Bendiek and Matthias Schulze, *Attribution: A Major Challenge for EU Cyber Sanctions*：*An Analysis of WannaCry, NotPetya, Cloud Hopper, Bundestag Hack and the Attack on the OPCW*, SWP Research Paper, no. 11（Berlin: The German Institute for International and Security Affairs, 2021), pp. 10–19, https://www.swp-berlin.org/publications/products/research_papers/2021RP11_EU_CyberSanctions.pdf.

ションに至るアトリビューションの全段階に影響すると捉え、特に次の 2 点の政策過程の構造が PA の様式に影響を与える点を示唆する。

1 点目は、官民の双方のアクターが直面する機微な情報の共有・公表リスクである。例えば政府の法執行機関やインテリジェンス機関と民間セキュリティ企業では、アトリビューションに利活用しうる情報源の種類・質量や比較優位が異なる [30]。そのため、総論ではアクター間の情報共有は分析の精度向上の観点で望ましい一方、その内容・相手方・時期によっては、将来の情報収集・分析に不可欠な機微な情報源の喪失から、被害組織への風評被害や法令・秘密保持契約違反に至るまで様々なリスクを内包する [31]。特に成果物を「一般公表」する PA は、一定の法的資格や当事者間の信頼に根差したクローズドな情報共有枠組と比べても一連のリスク管理が難しい。一連のリスクの多寡はアトリビューションの前提となるアクター間の情報収集・分析の段階での協力への関与の誘因から、官民による PA の対象事案、実施時期、公表する証拠量に至るまで、多岐に渡る影響を及ぼす [32]。

2 点目には、アトリビューションが依拠する制度の手続的な要求水準と、複数の制度・手続の選択可能性である。一口にアトリビューションといっても、実行犯個人の刑事手続や国際法上の帰属立証などの法的行為の一部としての対応と、法廷外での事実行為としての政策対応では、情報の収集・分析の段階での手続的な要求水準の厳格さが異なる [33]。例えば実行犯への刑事責任の立証の文脈でのアトリビューションには、基本的に各国法令に則った法執行機関の捜査権限で収集した証拠の裁判所への提出が必要となる。よってインテリジェンス機関が、その能力を駆使して収集しえても、情報源

30 欧米諸国を念頭に置くと、民間セキュリティ企業は顧客に提供する製品・サービスなどに由来した情報量（観測範囲）の優位があり、ある攻撃キャンペーンの IoC/TTPs や脅威アクターの分析の精度と発出速度では政府を凌駕する。他方で政府機関は、法執行機関の捜査証拠やインテリジェンス機関の機微な HUMINT・SIGINT を通じ、具体的な実行犯個人や国家機関の組織的関与を割り出すことに長ずる傾向がある。次を参照。 Steffens, *Attribution*, pp. 165–170; Adam Janofsky, “Cyber Attribution Is More Art Than Science. This Researcher Has a Plan to Change That,” Recorded Future, February 19, 2021, https://therecord.media/cyber-attribution-is-more-art-than-science-this-researcher-has-a-plan-to-change-that/; Bendiek and Schulze, *Attribution: A Major Challenge for EU*, p.10.

31 脅威情報の共有と公表に付随する種々のリスクは、特に次を参照。Johnson et al., *Guide to Cyber Threat Information Sharing*, pp. 4–5; Thomas D. Wagner et al., “Cyber Threat Intelligence Sharing: Survey and Research Directions,” *Computers & Security*, vol. 87 (November 2019), p. 10.

32 特に PA による機微な情報源の喪失のリスクと、政府機関の PA の判断への影響は次を参照。Egloff, “Public Attribution,” p. 5; 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 2019 (Hague: Leiden University, September 2019), p. 4, https://www.thehagueprogram.nl/research-and-publication-posts/foreign-intelligence-in-the-digital-age-navigating-a-state-of-unpeace.

33 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 2020 (Hague: Leiden University, April 2020), pp. 12–13, https://www.thehagueprogram.nl/research-and-publication-posts/three-tales-of-attribution-in-cyberspace-criminal-law-international-law-and-policy-debates.

の保護などの観点から裁判所への提出と公判での開示が困難な証拠などの利用は困難となる[34]。

ここで確認すべきは、既に触れたアクター間の情報の共有・公表のリスクと、この制度上の要求水準の相互作用である。一例として、法廷でのアトリビューションに要求される証拠水準や証拠の開示義務を含む証拠法理の厳格さや、証拠の提出先機関の機密保全の能力などは、各国政策当局が抱く機微な情報源の共有・公表リスクの認識を左右し、結果的に（パブリック）アトリビューションの追求の能力・意思に影響する[35]。この点で各国の政策当局による PA の経路の選択の可能性や、司法府との関係での証拠の扱いをめぐる制度設計などは、政策当局の PA の追求の様式や頻度にも影響を与える[36]。

（4）各国の政策当局間の「多様化」をめぐる実証研究の不足

こうした「第 2 世代」の先行研究でも、各国の政策当局間での「多様化」の要因とモデルは、厳密にいえば体系的な実証研究の対象となってきたとは言い難い。前項の先行研究群も、近年の各国政府の PA の一般的傾向を敷衍した分析枠組の提示の側面が強く、具体的な事例研究を通じて「多様化」の要因の実証を試みたものは、米国政府の関係省庁間の取組の比較が大宗を占めてきた[37]。また、その例外に挙げうるステファン・ソエサント（Stefan Soesanto）による米英主導の同盟・同志国間連携での各国間比較も、外交当局の非難声明を通じた、実施様式の行政裁量が大きい PA を比較単位としてきた[38]。よって各国の法制度や、政策過程におけるアクター間の協調・対立構造などが、政策当局による PA の様式に与える影響を必ずしも捉え切れていない。

---

34 Ibid, pp. 4-5; Bendiek and Schulze, *Attribution: A Major Challenge for EU*, p. 10.

35 歴史的に、国際法廷の事務局組織の機密保全制度の不十分さや、国際裁判における厳格な証拠開示の要求が課されることが、訴訟当時国が抱く証拠提出に伴う機微な情報源の喪失のリスク認識を増幅し、結果として裁判に必要な証拠の提供が停滞する事例が存在してきた。以下の文献を参照。Allison Carnegie and Austin Carson, *Secrets in Global Governance: Disclosure Dilemmas and the Challenge of International Cooperation in Worlds Politics*, (Cambridge: Cambridge University Press, 2020), pp. 193–239；清水 翔「国家間サイバー攻撃の法的アトリビューション──国際司法裁判所における ‘ 証拠偏在 ’ 論の再構成──」『情報ネットワーク・ローレビュー』第 19 巻（2020 年）121–131 頁。

36 次を参照。Broeders, Busser, and Pawlak, *Three Tales of Attribution*, pp. 12-13; Eichensehr, “The Law & Politics,” pp. 544–545.

37 米国の国内政策過程での関係省庁の PA の目的と様式の多様化をめぐる研究は、例えば次を参照。Heajune Lee, “Strategic Publicity?: Understanding US Government Cyber Attribution,” (Ph.D. thesis, Stanford University, May 2021), https://purl.stanford.edu/py070wt8487.

38 Stefan Soesanto, *The 19th of July: Divided or United in Cyberspace? From the EU and NATO to Five Eyes and Japan*, Working Paper, vol. 11, (Madrid: Elcano Royal Institute, October 2021), https://media.realinstitutoelcano.org/wp-content/uploads/2021/10/wp11-2021-soesanto-the-19th-july-divided-or-united-in-cyberspace-from-eu-nato-five-eyes-japan.pdf.

（5）事例研究の目的と分析枠組

以上の先行研究の課題を踏まえ、本稿では米司法省の起訴（状）によるアトリビューション（attribution by indictment）と呼ばれる施策と、EU のサイバー攻撃関連制裁レジームによる制裁指定を通じた PA という、本来要求されるアトリビューションの粒度や手続的な要求水準に類似性を備える制度に付随した PA の比較を通じて、政策当局間の PA の「多様化」の要因とモデルを明らかにすることを試みる。

米司法省と EU の施策は、刑事手続と行政法上の不利益措置の差はあれども、いずれも他国の政府機関を名宛人とはせずに、攻撃に関与した自然人・法人の粒度のアトリビューションを要求する。それゆえに被疑者や制裁対象の基本的人権の保護と適正手続の要請から、その追求には一定の証拠水準の充足が求められるほか、事前または事後に裁判所による司法審査が介在するといった手続的な要求水準に由来する制約条件も近しい。

しかし、後述するように双方の取組は、EU の制裁レジームの運用が開始された 2019 年以降の時間軸でのみ絞って比較しても、その運用実績には顕著な差が生じている。また米司法省の施策は、刑事手続が本来想定する実行犯の検挙と被疑者の有罪判決の確定という点からは、一見して非合理的な側面も有するにもかかわらず継続してきた。この点から両事例の比較は、政策当局が念頭に置く PA の（ⅰ）目的[39]・オーディエンス（の変化）と、（ⅱ）施策の追求の自由度を縛る政策過程の構造という、前項で検討した近年の先行研究の 2 つの分析の視角に対応して導かれる 2 種類の潜在的要因が、各々の PA の運用面の差異に影響を及ぼしてきたか否かを過程追跡するうえで適した事例選択といえる。

2．米司法省の起訴によるアトリビューションの事例研究

（1）施策の概要と論争

起訴によるアトリビューションとは、米司法省が他国政府の組織的関与が疑われるサイバー攻撃キャンペーンについて捜査し、裁判所に送達した起訴状の機密指定解除（unseal）を行う取組を指す。本来の起訴状の送達は、検察当局である米司法省が、裁判所に訴因と公訴事実を提出し、被疑者の刑事手続を進める過程の一部に過ぎない。

39「目的」とは、各国の政策当局の公式見解などから読み取れる PA の追求の動機を指す。よって、この動機に沿って PA が実際に所期の効果を挙げたか否かという施策の「効果」の検証は、本稿の分析の射程には含まれていない。

ただし、攻撃に関与した他国の軍・インテリジェンス機関要員や関連法人の名称などを公訴事実に含む起訴状の公表は、実質的に他国政府への法廷外での政策的な PA といえる[40]。

この起訴状の機密指定解除による一般公表は、法執行機関の捜査活動の情報を相手方に晒すため、実行犯の身柄を確保していない段階では、その逃亡や証拠隠匿も促し、特に国外犯の場合、短期的にはその検挙と有罪判決の確定を断念することになる[41]。こうした刑事手続の本来の目的からは奇妙な運用と、米司法省も取組の真意を明示しない状況が重なり、当該施策は、その端緒となる 2014 年の中国人民解放軍の要員の起訴状の公表以来、米国内でも目的と効果をめぐる様々な論争を巻き起こしてきた[42]。

（2）2010 年代後半の米司法省による「妨害」と「コスト強要」戦略との一体化

それでも米司法省の起訴によるアトリビューションは、2014 年来継続し、特に 2018 年をピークに起訴状の公表件数や起訴状毎の被疑者数の増加傾向を見せてきた[43]。また近年では、米司法省や、その一部である米国連邦捜査局（FBI）（以下：米司法省・FBI）の公刊資料や担当者の証言などを通じ、米司法省自身が施策の目的への認識や運用の過程を徐々に明らかにしてきた。米司法省・FBI が提供する公刊資料と、近年の先行研究を踏まえると、2018 年以降の米司法省・FBI の取組は、次の 3 つのポイントを指摘できる。

まず、この施策は、政権のトップダウンの決定よりも、むしろ米司法省や関係省庁の実務当局レベルで主導する政策手段として発展してきた。米司法省の掲げる施策の目的は後述するが、この時点で確認すべきは、アダム・ヒッキー（Adam Hickey）司法次官補代理（国家安全保障部担当）を含む複数の米司法省幹部経験者が、起訴状の公表は、他国へのいわゆるネーム・アンド・シェイムを狙った施策ではない旨を言明している点である[44]。

40 起訴によるアトリビューションの関連制度や運用のプロセスの概要は、例えば次を参照。Chimène I. Keitner, “Attribution by Indictment,” *AJIL Unbound*, vol. 113 (June 2019), pp. 207–212.

41 Garrett Hinck and Tim Maurer, “Persistent Enforcement: Criminal Charges as a Response to Nation-State Malicious Cyber Activity,” *Journal of National Security Law and Policy*, vol. 10, no. 3（January 2020), pp. 529–530.

42 次を参照。Jack Goldsmith, “Why Did DOJ Indict the Chinese Military Officers?” *Lawfare*, May 20, 2014, https://www.lawfareblog.com/why-did-doj-indict-chinese-military-officers.

43 Keitner, “Attribution by Indictment,” p. 207; Garrett Hinck and Tim Maurer, “What’s the Point of Charging Foreign State-Linked Hackers,” *Lawfare*, May 24, 2019, https://www.lawfareblog.com/whats-point-charging-foreign-state-linked-hackers.

44 John Sakellariadis, “How the Justice Department Is Stepping up Its Efforts To Indict State-Sponsored Hackers,” *Recorded Future*, February 3, 2021, https://therecord.media/how-the-justice-department-is-stepping-up-its-efforts-to-indict-state-sponsored-hackers/

次に、起訴状の公表の判断は、実施による機微な情報源の喪失のリスク判断を含めたインテリジェンス・コミュニティ内部の調整プロセスを経て実施されるが、こうしたプロセスの合理化が徐々に図られてきたとされる[45]。また、このプロセスで起訴状が公表対象となる事案とは、被疑者の身柄が競争国内にある場合など、被疑者の検挙または司法共助での同盟国からの引渡の見通しが低いとの評価されたものを中心としている[46]。この指摘に鑑みると、起訴によるアトリビューションは、被疑者の検挙と法廷での有罪判決の確定という目標が達成困難なことを前提にした取組といえる。

以上の 2 点を踏まえ、米司法省の認識する起訴状の公表の目的は、次の 2 点に整理できる。1 つには、起訴状の公表による事実上の注意喚起政策である。起訴状内の公訴事実で過去に米司法省が捜査活動の過程で収集した攻撃者の身元や TTPs をめぐる追加情報を公表し、また起訴状の公表で国際的な注目が喚起されたタイミングで、関連する攻撃者により進行中の別個の攻撃キャンペーンの注意喚起なども併せて公表することで、民間での「脅威アクター」の分析の精度向上や追加の脅威情報の流通を促し、ネットワーク防衛の強化の向上を促す[47]。

もう 1 つは、表 1 の「脅威対抗」機能の想定に近く、公訴事実内の情報や起訴状の公表自体を触媒として、省庁間連携・官民連携・国際連携に基づき相手方の攻撃キャンペーンを妨害（disruption）する各種の政策対応に繋げることにある[48]。前提として近年の米司法省・FBI は、犯人の検挙と刑事手続のための自身の捜査能力を、法廷外での攻撃キャンペーンの妨害に積極的に転用し、その継続と拡大を通じた敵対者への

45 John Sakellariadis, “How the Justice Department.”
46 Ibid.
47 米司法省の起訴状の公表や他省庁と連携した注意喚起の運用の理念は次を参照。Federal Bureau of Investigation, “Four Russian Government Employees Charged in Two Separate Hacking Campaigns Targeting Worldwide Critical Infrastructure,” March 24, 2022, https://www.fbi.gov/news/stories/russian-government-employees-charged-in-hacking-campaigns-032421; Arielle Waldman, “ Nation-state Hacker Indictments: Do They Help or Hinder?” *TechTarget*, April 15, 2021, https://www.techtarget.com/searchsecurity/feature/Nation-state-hacker-indictments-Do-they-help-or-hinder?amp=1.; Federal Bureau of Investigation, “NSA and FBI Expose Russian Previously Undisclosed Malware Drovorub in Cybersecurity Advisory,” August 13, 2020, https://www.fbi.gov/news/press-releases/nsa-and-fbi-expose-russian-previously-undisclosed-malware-drovorub-in-cybersecurity-advisory.
48 次を参照。U.S. Department of Justice, *Comprehensive Cyber Review* (Washington, DC: July 2022）pp. 9–15, pp. 24–39, https://www.justice.gov/dag/page/file/1520341/download; Hinck and Maurer, “Persistent Enforcement,” pp. 532–533, pp. 551–553. これらは基本的に攻撃キャンペーンの要員（攻撃キャンペーンの管理者や実行者に加え、これらを支援する人物や団体も含む）・資金源・攻撃ツールやインフラなどの運用基盤の調達と維持を困難とすることを目指す。具体的には、攻撃キャンペーンのハンドラーとなる外交官身分のインテリジェンス機関要員の国外追放、逮捕状発給による司法共助・国際共同捜査による関係者の一斉摘発のほか、資産凍結・犯罪収益の没収、市場での攻撃ツール・インフラの調達を阻むための輸出管理・取引禁止指定、攻撃者が管理する C & C サーバー・ドメインや、犯罪集団の情報交換フォーラムのテイクダウンなど多岐にわたる。

コスト強要（imposing costs）による行動変容を目指す指針を表明してきた[49]。2022年3月のFBIの捜査幹部の公聴会証言も踏まえれば、今日の起訴状の公表によるPAも、この米司法省・FBIの指針の一部であり、具体的には妨害とコスト強要の選択肢とスケールメリットの拡大のため、米国政府の関係省庁、同盟国などの政府機関、国内外の民間セクターとの連携や共同対処を促すものと認識されている[50]。

（3）「司法手続の政策化」による妨害・コスト強要戦略の追求

近年の米司法省の起訴によるアトリビューションは、「司法手続の政策化」とも表現できるPAの多様化のモデルを示唆している。その本質は、元来は犯人の検挙と刑事手続で司法府（裁判官）を説得するための法執行機関の捜査権限と能力を、PAを触媒とした「法廷外」での防諜・安全保障政策上の目的に転用する取組と理解できる。これは先に見た、米司法省・FBIが標榜する近年の指針と軌を一にした、アトリビューションの目的・オーディエンスへの認識の変化を反映している。

政策過程の構造の影響としては先述の関係省庁間での調整の合理化のほか、恐らくは提出・開示証拠の実質的裁量が、機微な情報源の喪失の懸念を緩和させ、米司法省の施策に許容的環境を創出した可能性も指摘できる。後者につき、従来の起訴状内の証拠は、公判段階での有罪の立証には質量共に不足しうる点が指摘されてきた[51]。それは逆にいえば、米司法省は公判に至らない前提での提出・開示証拠の裁量を維持したともいえるからである。

3．EUのサイバー攻撃関連制裁レジームの事例研究

（1）施策の概要と論争

EUのサイバー攻撃関連制裁レジームとは、2017年6月に欧州連合理事会（Council

49 刑事手続のための捜査能力の法廷外での「妨害」と「コスト強要」のための利用を積極化する当該指針については、特に次を参照。Ibid., p.2, pp. 9–10; *Oversight of the FBI Cyber Division, Hearing Before Committee on Judiciary, United States House of Representatives*, 117th Congress (2022), pp. 2–5（Statement of Bryan A Vorndran, Assistant Director Cyber Division, Federal Bureau of Investigation-U.S. Department of Justice), https://docs.house.gov/meetings/JU/JU00/20220329/114533/HHRG-117-JU00-Wstate-VorndranB-20220329.pdf.

50 *Oversight of the FBI Cyber Division*, pp. 2-3; U.S. Department of Justice, *Comprehensive Cyber*, pp. 9–15, 24–39.

51 例えば複数の専門家から、過去に米司法省の公表した幾つかの起訴状には、被告人の関与の立証に本来ならば必要なはずの証拠が除外されている形跡があり、実際の公判段階で、裁判官に対して被告の有罪を証明するための証拠力としては不十分な点が指摘されてきた。この点は、次を参照。Steffens, *Attribution*, pp. 174–175; Goldsmith, “Why Did DOJ Indict.”

of the European Union）（以下：EU 理事会）が採択した「サイバー外交ツールボックス（Cyber Diplomacy Toolbox：EU-CDT）[52]」の一部として、EU が一定のサイバー攻撃事案に関与する人物（person）または団体（entity）の資産凍結や渡航禁止などを課しうる制裁制度を指す（以下：CDT 制裁）。EU-CDT の採択は、国際法上の武力攻撃に至らない烈度での悪意あるサイバー活動の常態化に伴う安全保障環境の悪化を背景に、特に他国が関与する脅威の抑止と対処には、EU と加盟国の共同での対外政策上の措置の強化が必要との認識を背景に持つ[53]。このなかで CDT 制裁は、2016 年以降、オランダとエストニアを筆頭とする EU 加盟国内の同志国グループの働きかけを通じて、EU-CDT の共同対処の選択肢の 1 つに組み込まれた[54]。

CDT 制裁は、関連規則の整備に伴い 2019 年 5 月に正式運用が開始されたが、本稿脱稿時点（2023 年 1 月）までの過去数年間の運用面での特徴として次の 2 点を挙げられる。

第 1 に、制裁の指定対象の面では、先の米司法省の取組を含めた米英両国などの PA を通じ、ロシア・中国・北朝鮮の政府機関の関与が暴露された攻撃キャンペーンに関与した人物・団体を対象とし、その中にはイゴール・コスチュコフ（Igor Kostyukov）ロシア軍参謀本部情報総局（GRU）長官などの現役の政府高官も含まれる。この標的選定の傾向から、CDT 制裁は、他国の政府機関が関与する悪意あるサイバー活動の牽制のためのシグナリングや、規範形成の機能を念頭に置くものとして理解されてきた[55]。

第 2 に、その一方で、制裁指定の件数や対象となる人物・団体数で見た運用実績は、同期間内の米司法省の取組[56]と比較して極めて限定的である。具体的には、2020 年 7 月と同年 10 月の 2 段階に分け、2018 年までに発覚してきた中国・ロシア・北朝鮮関

52　正式名称は Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities だが、一般的に Cyber Diplomacy Toolbox の通称で議論されるため、本稿の表記もこれに従う。

53　この点は、2016 年上半期の EU 議長国であるオランダが提出したノン・ペーパーを参照。Council of the European Union, *Non-Paper: Developing a Joint EU Diplomatic Response Against Coercive Cyber Operations*, 5797/4/16 REV 4, April 16, 2016, pp.4–5, https://data.consilium.europa.eu/doc/document/ST-5797-2016-REV-3/en/pdf.

54　2016 年以降の EU-CDT と CDT 制裁の策定までの経緯は、次を参照。Siim Alatalu,“Alliance Attribution of Global Cyber Attacks : The European Union,” in *National Cyber Emergencies: The Return to Civil Defence*, ed. Greg Austin (London: Routledge, 2020), pp. 179–180.

55　Jamie Collier, “Europe’s New Sanction Regime Suggests a Growing Cyber Diplomacy Presence,” *FireEye Industry Perspectives*, August 6, 2020, https://www.fireeye.com/blog/executive-perspective/2020/08/europe-new-sanction-regime-suggest-a-growing-cyber-diplomacy-presence.html.

56　例えば起訴状の公表数と制裁指定の発動の件数を基準に比較した場合、米司法省の公表数は 2020 年には 7 件を数えるが、この 1 年の件数のみで 2019 年から 2023 年 1 月現在までの EU の制裁指定件数の 5 件を上回っている。

連の計 5 事案[57]に関与した計 8 名・4 団体の制裁対象指定が行われて以降、2023 年 1 月までに新たな制裁指定は一切行われず、運用の一貫性の欠如や硬直化が指摘されてきた[58]。以下では、こうした CDT 制裁の運用の背景について、EU 当局の公文書や近時の CDT 制裁をめぐる先行研究を駆使して分析する。

（2）アトリビューションをめぐる政治のなかでの CDT 制裁の制度設計

CDT 制裁の 1 つの特徴は、上述の他国政府機関の要員を含めた制裁指定の標的選定の傾向にもかかわらず、EU は制裁指定が「アトリビューションにはあたらない」との公式見解を示してきたことにある。注意を要するのは、ここでの「アトリビューション」とは「第三国（third state）」に対するものを指しており、そうした行為への判断を EU 加盟国の固有の権利として留保しつつ、あくまで EU としての CDT 制裁は「人物・団体」が名宛人であるため、加盟国の権利とは抵触せず実施しうるとの法的解釈を明示したものである[59]。

ユリヤ・ミアジェツカヤ（Yuliya Miadzvetskaya）らの分析も踏まえれば、以上の EU の立場は、EU-CDT の策定過程での EU 当局と加盟国間のアトリビューションをめぐる政治に由来する。元来、欧米諸国の間でもアトリビューションの概念と国際法上の国家責任の帰属の概念の相互の関係性が論争的であったことに加え、外交的にも、「国家」を名宛人とする PA は、対象国との対決姿勢の表明も不可避とする。よって EU-CDT の策定過程では、EU-CDT の措置と「国家」に対する「アトリビューション」との関係性や、情報収集・分析から PA の実施判断までの EU 当局と各加盟国間での

57 具体的には、（1）2017 年 5 月の WannaCry 事案（北朝鮮）ならびに（2）同年 6 月の NotPetya 事案（ロシア）に加えて、（3）2010 年代を通じた脅威アクター「APT10」による知財窃取キャンペーン（Operation Clowd Hopper）（中国）、（4）2015 年に発生したドイツ連邦議会からの情報窃取事案（Bundestag Hack）（ロシア）、そして（5）2018 年の化学兵器禁止機関（OPCW）への近接ハッキング未遂事案（ロシア）の計 5 つの事案を指す。各事案の概要は次を参照。Bendiek and Schulze, *Attribution: A Major Challenge for EU*, pp. 20–33.

58 Ibid, pp. 34–36; Stefan Soesanto, “After a Year of Silence, Are EU Cyber Sanctions Dead?” *Lawfare*, October 26, 2021, https://www.lawfareblog.com/after-year-silence-are-eu-cyber-sanctions-dead.

59 次を参照。Council of the European Union, *Council Decision Concerning Restrictive Measures Against Cyber-attacks Threatening the Union or its Member States*, 7299/19, May 14, 2019, p.5, https://data.consilium.europa.eu/doc/document/ST-7299-2019-INIT/en/pdf.

権能・能力の配分[60]が、EU の加盟国間の対立の争点として燻り続けてきた[61]。

そのため、「国家」ではなくあくまで「人物・団体」を対象とする CDT 制裁の制度設計は、それ自体がアトリビューションをめぐる加盟国間の政治対立を「棚上げ」し、CDT 制裁の制度化を達成するための政治的な考慮を背景としたものであった[62]。

（3）制度の要求水準と、EU 当局・各加盟国の運用能力・意思の乖離

以上の経緯を踏まえて制度化された EU による CDT 制裁は、国・地域別の包括的な制裁ではなく、2000 年代前半の国際テロ対策などのためのスマートサンクションの制度の前例を踏襲したものとなる。この点で CDT 制裁は、「他国（の政府機関）」に対するアトリビューションは求めないにもかかわらず、実務上は「人物・団体」の粒度のアトリビューションにつき、EU 理事会における全会一致での合意を必要とする。同時に前例となる EU の制裁レジームと同水準の基本的人権の保障と適正手続の要求を課され、制裁指定の根拠となる証拠の不十分性など、手続面の瑕疵が認められた場合には、欧州司法裁判所（ECJ）の事後審査により制裁指定自体が取消の対象となる[63]。

他方で、この CDT 制裁の制度設計は、EU 加盟国側の機微情報共有の消極性と結びつき、制裁運用の制約条件となりうる点が懸念されてきた。そもそも EU 当局は、CDT 制裁の運用に足る独自の情報収集能力を備えておらず、制裁指定根拠となる「人物・団体」の粒度のアトリビューションを、加盟国政府の提供する機微情報に依存せざるをえない。しかし各加盟国は、理事会での合意までの調整過程や ECJ の司法審査の段階での情報源の喪失リスクから、制裁運用に必要な機微情報の出し渋りの誘因を有するからである[64]。

60 例えば 2019 年の段階で、EU 加盟国間のアトリビューションの共通基準の策定や欧州対外行動庁（EEAS）の EU 情報活動分析センター（EU INTCEN）を中心とした EU 当局の情報収集・分析能力強化を内容に含む指針の採択は、加盟国の反対で立ち消えとなった。次を参照。Council of the European Union, *Implementation of the Framework for a Joint EU Diplomatic Response Malicious Cyber Activities: Attribution of Malicious Cyber Activities: Discussion of a Revised Text*, 6852/1/19 REV 1, March 18, 2019, https://www.statewatch.org/media/documents/news/2019/mar/eu-council-cyber-6852-REV-1-19.pdf.

61 EU-CDT と CDT 制裁の制度設計過程でのアトリビューションをめぐる加盟国間の亀裂は、次を参照。Yuliya Miadzvetskaya, “Challenges of the Cyber Sanctions Regime under the Common Foreign and Security Policy (CFSP),” in *Security and Law: Legal and Ethical Aspects of Public Security, Cyber Security and Critical Infrastructure Security*, ed. Anton Vedder et al., vol. 4, KU Leuven Centre for IT & IP Law Series (Cambridge: Intersentia, 2019), pp. 283–291; Yuliya Miadzvetskaya and Ramses A. Wessel, “The Externalisation of the EU’s Cybersecurity Regime: The Cyber Diplomacy Toolbox,” European Papers, vol. 7, no. 1 (July 2021), pp. 434–437.

62 Miadzvetskaya and Wessel, “The Externalisation,” p. 435.

63 Ibid., pp.434–438.; Miadzvetskaya, “Challenges of the Cyber Sanctions Regime,” pp. 282-290.

64 Ibid., pp. 290–292.; Yuliya Miadzvetskaya, *Cyber Sanctions: Towards a European Union Cyber Intelligence Service*? The College of Europe Policy Brief, no. 1.21 (Brugge, Belgium: The College of Europe, February 2021), pp.2–4.

この懸念は、2020 年の 2 度に渡る EU の CDT 制裁の運用の標的選定や、その後の運用の停滞に影響を与える形で顕在化してきたと見受けられる。アンネグレート・ベンディエク（Annegret Bendiek）らの分析によると、制裁指定が制度上要求する攻撃者の意図の立証は、IoC/TTPs などの技術的証拠を超えた、インテリジェンス機関や法執行機関由来の機微情報が必要となるが、現行の制度運用では、EU 当局はこの部分の取組を米英両国政府や米国の民間セキュリティ企業に依存[65]し、また、それでもなお、EU 理事会での加盟国の全会一致に至るまでの EU 当局の関係機関の調整にも滞りがみられたとされる[66]。

こうした分析を踏まえれば、現行の CDT 制裁の運用の硬直化とは、EU 加盟国の政治的妥協の産物として定まった制度の要求事項と、EU 当局・加盟国の運用能力や意思の乖離によるものといえよう。

（4）「政治対立の司法化」の帰結としての制度運用の硬直化

米司法省の施策が「司法手続の政策化」とすれば、EU の CDT 制裁の特徴は「政治対立の司法化」というモデルとして表現できる。一面では EU は「人物・団体」を標的とするスマートサンクションの前例を踏襲し、EU 理事会での全会一致や ECJ の司法審査も介在させうる透明性の高い制度・手続を選択することで、アトリビューションをめぐる EU 加盟国間の政治対立の問題を棚上げした。その一方で、制度が要求する厳格な手続面の要求水準と、EU 当局の制度の運用能力の乖離は、結果的に CDT 制裁を通じた EU の政策目標の追求の自由度を制約してきた。以上の点からすれば EU の事例は、政策過程の構造が、制度・手続の設計から運用に至るまで（パブリック）アトリビューションの様式を型にはめていく作用を示すものといえる。

65 具体的には、EU が制裁指定の対象とした事案は、過去に米司法省の起訴状の公表などを通じて実行犯の具体名を特定する証拠が既に公表されたものか、または英国政府からの機微情報の事前提供に基づき、オランダの軍情報保安局（MIVD）がハーグ市内で GRU 要員の身柄を拘束し証拠を直接押収した化学兵器禁止機関（OPCW）へのハッキング未遂事案に限られる。いずれも EU 加盟国のインテリジェンス機関の独自の機微情報の提供が無くとも、特定の人物・団体の事案への関与が立証しえた事案といえる。

66 前掲注の内容を含め、以上の点は主に次を参照。Bendiek and Schulze, *Attribution: A Major Challenge for EU*, pp. 5–6, pp. 20–36; Miadzvetskaya and Wessel, “The Externalisation,” pp. 436–437.

おわりに

本稿の比較事例研究が扱った米司法省と EU の施策は、その依拠する制度が本来要求するアトリビューションの粒度や手続的な制約条件の類似性にもかかわらず、2010 年代後半に「司法手続の政策化」と「政治対立の司法化」と表現しうる異なる要請に導かれ、PA の追求の様式や実績も異なる形に収斂してきた。この事例研究の結果は、各国政策当局の PA の「多様化」は、その（ⅰ）目的とオーディエンスに加え、（ⅱ）施策の運用の自由度を制約する政策過程の構造にも規定されてきたとの結論を実証的に支持する。

上記の結論は、アトリビューションを懲罰的抑止の前提条件に還元する、または PA の機能を、他国を糾弾することで相手方の行動変容をもたらすと捉えるネーム・アンド・シェイムの概念と互換的に用いる先行研究の立場からは見落とされてきた、今日の各国の政策当局が直面するアトリビューションをめぐる課題の諸相を示す。すなわち、PA の「拡散」と「多様化」という現象と軌を一として、いわゆる「アトリビューション問題」のなかで「何が問題とされているのか」の軸足の変化を実証的に明示した点が、本稿の既存のサイバー安全保障研究に対する学術的貢献となる。

最後に、今後の研究課題として次の 3 点を提示してむすびとかえる。第 1 に、PA の「多様化」の要因をめぐる理論の一般化を目指すにあたっては、国・機関別単位でのアトリビューションを取り巻く政策過程の構造について、より観察対象を増やすことが求められる。本稿の事例が見てきた米司法省と EU 当局の事例は、アトリビューションに要する情報収集・分析の能力基盤の有無や制度運用の裁量性の面で両極端な事例であり、この両極の間に、第 1 節で触れたエストニアとフランスのような EU 加盟国間での PA に対する姿勢の差異なども存在する。こうした事例でも、本稿が着目した「多様化」の要因が妥当するかは、国別の詳細な事例研究を通じた検証を必要とする。

第 2 に、サイバー攻撃以外の、実行者の特定が困難な脅威への PA に類する政策との比較研究の要請である。2016 年以降の欧米諸国は、ソーシャル・メディア上での悪意ある影響工作や、伝統的な物理空間での諜報活動（espionage）や非公然工作活動（covert action）に対しても、国家機関の組織的関与を特定して暴露する施策を活発化させてきた[67]。こうした事例でも、アクター間の情報源の断片化と機微な情報源の共

67 この潮流は例えば次を参照。Rory Cormac, *How To Stage A Coup : And Ten Other Lessons from the World of Secret Statecraft* (London: Atlantic Books, 2022), pp. 275–295; Justin Sherman, “Changing the Kremlin’s Election Interference Calculus,” *The Washington Quarterly*, vol. 45, no. 1 (January 2, 2022), pp. 118–121.

有・公表の課題[68]から、国内法に基づくインテリジェンス機関や法執行機関の証拠収集能力や刑事手続の柔軟性が施策に与える影響[69]まで、本稿が触れたアトリビューションの政策過程の諸論点が見え隠れする。そのため、こうした隣接事例との比較研究は、本稿が展開したPAの「拡散」と「多様化」の要因が、サイバー攻撃のアトリビューションに固有のものか否かを捉える点でも重要となる。

第3に、本稿が研究の射程外とした、PAの実際の「効果」の検証である。近年のセキュリティ専門家による脅威アクターの追跡調査は、仮にIoCやTTPsの暴露を触媒とした連鎖的な政策対応がその一時的な妨害を達成した場合でも、その永続的な停止にまで至った例は殆ど見られない点や、PAの効果が攻撃キャンペーンの目的や運用面の特徴などにより異なる可能性を指摘してきた[70]。

その意味で、例えば米司法省・FBIが念頭に置くPAを触媒とした妨害・コスト強要という方針も、想定された効果を挙げてきたか否かは今日まで自明ではない。この点に鑑みれば、攻撃キャンペーンの観測データの分析による個々の攻撃者の特徴のプロファイリング[71]や、PAの前後での脅威アクターの行動変容をめぐる事例研究の蓄積は、実務上の要請は勿論、PAの効果と作用機序の検証という学術研究の発展にも重要な課題となる。

（防衛研究所）

68 例えばソーシャル・メディア上の影響工作に対するアトリビューションをめぐる当該課題は、次を参照。James Pamment and Victoria Smith, *Attributing Information Influence Operations: Identifying Those Responsible for Malicious Behaviour Online* (Riga, Latvia: NATO Strategic Communications Centre of Excellence, 2022), pp.11–24, https://stratcomcoe.org/pdfjs/?file=/publications/download/Nato-Attributing-Information-Influence-Operations-DIGITAL-v4.pdf?zoom=page-fit.

69 例えば近年のエストニア政府は、ロシアのインテリジェンス機関の諜報活動を、刑事裁判を通じて暴露する施策を追求してきたが、同国の法制度改革や刑事手続の柔軟な運用が当該施策に与えた影響は次を参照。Michael Jonsson and Jakob Gustafsson, *Espionage by Europeans 2010-2021: A Preliminary Review of Court Cases*, FOI-R-5312-SE, (Stockholm: Swedish Defence Research Agency[FOI], May 2022), pp. 17–18, 56–57, p. 62, https://www.foi.se/rest-api/report/FOI-R--5312--SE; Ivo Juurvee and Lavly Perling, *Russia's Espionage in Estonia: A Quantitative Analysis of Convictions*, Analysis (Tallinn: International Centre for Defence and Security, November 2019), pp.1–2, p.8, https://icds.ee/wp-content/uploads/2019/11/ICDS_Analysis_Russias_Espionage_in_Estonia_Juurvee_Perling_November_2019.pdf.

70 例えば次を参照。Matthew Armelli et al., *Named but Hardly Shamed: The Impact of Information Disclosures on APT Operations*, SIPA Capstone Project 2020 (Washington, DC: Columbia University's School of International and Public Affairs[SIPA], Spring 2020), p. iii, pp. 92–97, https://www.sipa.columbia.edu/sites/default/files/migrated/downloads/SCB%2520Capstone%2520Final%2520Report%2520-%252013May2020%2520%25281%2529.pdf.

71 攻撃者のプロファイリングに基づく、攻撃者や事案の性質に応じたケース・バイ・ケースでのPAの有効性をめぐる議論の要請については、特に次を参照。佐々木勇人「'アクティブ・サイバー・ディフェンス'事始め――攻撃者プロファイリングの意義について」一般社団法人JPCERTコーディネーションセンター（2023年1月）22頁、28–30頁、https://jsac.jpcert.or.jp/archive/2023/pdf/JSAC2023_2_2_sasaki_jp.pdf.

［付記］本稿の完成にあたり、査読者の先生方から貴重な修正のご提案とご指導を頂いた。また本稿は、執筆者が2021年から2022年にかけて参加したいくつかの研究会での発表や参加者の方々との議論からも示唆を頂いている。個別にお名前を挙げることは差し控えるが、ここに記して感謝申し上げたい。