〈1〉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―

一般社団法人 JPCERT コーディネーションセンター
早期警戒グループマネージャ　脅威アナリスト
佐々木　勇人 [1]

1. はじめに

2020 年の米大統領選挙での勝利の後、結果の確定に至る混乱などを経て、バイデン新政権が発足したのは年が明けた 2021 年 1 月 20 日であったが、新政権最初の 100 日間の「ハネムーン期間」前後で 2 つの大規模なサイバー攻撃へ対応することとなる。2020 年 12 月 13 日には Solarwinds 社のソフトウェア「Orion Platform」のアップデート経路を悪用した大規模なサイバー攻撃（いわゆる「サプライチェーン攻撃」）が発覚し、年明けにかけての調査により、標的の大半が米連邦政府や米国に拠点を置く IT／サイバー関連企業であったことが判明するに至った。

この事案では発覚直後から政府筋の情報として、ロシア情報機関傘下の攻撃グループによるものであるとの報道が流れ [2]、バイデン次期大統領（当時）も米メディアの取材に対して、ロシア側への経済制裁等の対抗措置を検討する旨を表明していた。最終的に、政権交代後の 2021 年 4 月 17 日、バイデン政権は SolarWinds 事案を含めた複数のサイバー攻撃についてロシア当局の関与と断定し、関係者への経済制裁措置 [3] を行うこととなった。

そして、今年 5 月 6 日にはアメリカ東海岸の主要なパイプライン企業であるコロニアルパイプライン社が標的型ランサムウェア攻撃の被害にあい、操業が 6 日間停止する事態となったが、この際も発覚 5 日後にはバイデン大統領がロシア政府の関与の証拠はないとしながらも、「ロシアに対処する責任がある」と非難した。

いずれの事案も本稿執筆時点では、米側の主張を裏付ける技術的な証拠は公表されておらず、本稿ではその真偽を検討することはしないが、この 2 事例のような社会的に大きな影響を及ぼすサイバー攻撃 [4] が発生した場合における、その発覚／発生直後に

[1] 本稿は筆者の所属元での活動知見を踏まえて執筆しているが、ここで述べる見解等は必ずしも組織を代表するものではない
[2] Reuters, “Suspected Russian hackers spied on U.S. Treasury emails - sources”, May 13 2021, <https://www.reuters.com/article/uk-usa-cyber-treasury-exclusive-idUKKBN28N0PI>
[3] 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/>
[4] 警察庁警備局の通達文書では「大規模サイバー攻撃」について「国民の生命、身体、財産若しくは国土に重大な被害が生じ、若しくは生じる恐れのあるサイバー攻撃事態若しくはその可能性のある事態又は社会的反響の大きなサイバー事象若しくはその発生につながるおそれのある事象」としている。（警察庁警備局通達丙備企発第 127 号等（令和 2 年 4 月 1 日）また、「重要インフラの情報セキュリティ対策に係る第 4 次行動計画」（サイバーセキュリティ戦略本部 (令和 2 年 1 月 30 日)）では「大規模重要インフラサービス障害」として「官邸対策室等が官邸危機管理センターに設置されるなどの政府として集中的な対応が必要となる規模の重要インフラサービス障害」と定義している。

攻撃者の特定とパブリックアトリビューション[5]に至るプロセスについて考察してみたい。

2.「誰が」攻撃を実行したのか

サイバー攻撃の実行者／組織の特定やその責任を特定国に求めることについて「アトリビューション（Attribution）」と呼ばれる。狭義にはサイバー攻撃者が所在していた国や発信元の所在国に対してその責任を求めるという国際法上の責任の帰属の文脈で用いられ、他方、広義にはサイバーセキュリティ業界を中心に「攻撃者グループの特定」といったより幅広い意味合いで用いられることが多く、必ずしも物理的な人物や所在地、特定国とのかかわりを特定するまで意味していない場合がある。

Solarwinds 事案に対して米当局では、今年 4 月 17 日の対ロ経済制裁措置発表において、SVR のサイバー攻撃アクターとする APT29（Cozy Bear, Dukes）を名指しし、攻撃の実行者であると指摘した。そして、ロシア当局を非難するとともに、対抗措置（Solarwinds 事案以外の活動も含め、SVR のサイバー活動を支援したとして複数の IT 企業を対ロ経済制裁指定対象に追加）を実施したのである。

この事案で使用された多数のマルウェアサンプルの解析が官民双方で行われ、各専門機関やセキュリティベンダからレポートが公表されているものの、少なくとも民間のサイバーセキュリティ業界側では、特定の既知の攻撃グループの特定には至っておらず、また、米当局が APT29 による攻撃であると特定した技術的な証拠も現時点で示されていない。

コロニアルパイプライン事案では DARKSIDE ランサムウェアが使われたことが早々に特定され公表されたが、実行した攻撃グループについては特定されておらず、ロシア当局／特定の人物の関与は（現時点で）示されていない。しかし、バイデン大統領は会見で攻撃者グループの所在地／発信元として、ロシア当局には同ランサムウェア攻撃に対処する「ある程度の責任がある」と非難した[6]。

この 2 事例でどのようなアトリビューションが行われたのか整理すると、SolarWinds 事案では実行者を名指しし、その所属組織／所在国に対して非難や対抗措置を実施したケースとなり、コロニアルパイプライン事案は攻撃者の特定やロシアの関与は不明ながら、攻撃者の活動がロシアを拠点していることを疑い、いわゆる「相当の注意義務」に違反しているとしてロシア政府を非難している[7]ものと解釈できる。

少し長くなるが、標的型ランサムウェア攻撃の実行者である攻撃グループの背景について解説をしておきたい。

標的型ランサムウェア攻撃は、首謀者と実行者が分担して攻撃を行う分業（「アフィリエイトスキーム」と呼ばれる）で実行されるものがあり、スキームのオーナー（首謀者）が「オペレータ（攻撃の実働部隊）」をアンダーグラウンドマーケット等を通じて多数“調達”し、これらのオペレータたちにランサムウェアを提供し実際の攻撃を実行させ、奪った身代金の“上前をはねる”仕組みになっている。各オペレータは自前でランサムウェアを開発しなくても、他のサイバー犯罪で使い慣れている得意な侵入方法で標的組織へ侵入することさえできればよい。この分業によってスキームのオーナーは効率よく、かつ大規模にランサムウェア攻撃キャンペーンを“運営”することが可能となっている。この Darkside もそうしたスキームで活動しているが、具体的にどこに所在する「オペレータ」＝攻撃グループが今回の攻撃を実行したのか特定には至っていない。

DARKSIDE ランサムウェアは侵害した先の端末の言語環境をチェックし、ロシアをはじめ CIS 諸国

[5] パブリックアトリビューションとはアトリビューションを判断し、その判断を対外的に公開するプロセスを意味する。必ずしも刑事訴追に係る公表だけではなく、外交上の何らかの声明の場で示したり、あるいは政府による相手国への責任言及まで至らずとも、専門機関やセキュリティ専門企業が分析レポートとして公表する、より“ソフトな”ケースも含まれる

[6] Bloomberg, “Biden Says Russia Has ‘Some Responsibility’ in Colonial Attack”, May 10 2021, <https://www.bloomberg.com/news/articles/2021-05-10/colonial-pipeline-is-undamaged-white-house-official-says>

[7] 高橋郁夫「パイプライン攻撃事件の法的論点 (国家責任・デューディリジェンス)-Colonial Pipeline 事件」（2021 年 5 月 14 日）<https://itresearchart.biz/?p=2827> ほか、タリンマニュアル 2.0 の規則 6（相当の注意）、規則 7（相当の注意原則の遵守）が参考となる。（中谷和弘、河野桂子、黒崎将広「サイバー攻撃の国際法　タリンマニュアル 2.0 の解説」(信山社 , 2018 年)、10-11 頁)

やアラビア語の言語環境が使われている場合は暗号化を行わないように設定されている。[8] また、攻撃者へのインタビューでロシア語話者である可能性が推測されていたり[9]、ロシア語のフォーラム上でオペレータ（アフィリエイト）が募集されていることなどといった状況証拠を考慮すると、ロシア語圏に所在するメンバーが運営している可能性は高いものの、少なくともセキュリティ専門企業などから公開されている情報においては、狭義のアトリビューションに十分な情報が揃っているとは言えない。また、第3章で解説する通り、各オペレータがどのようなグループなのかも明らかにはなっていない。

このようなアフィリエイトスキームで活動するランサムウェアは増加の一途をたどっているが、米司法当局は今年1月にNetwalkerランサムウェアのオペレータ（アフィリエイト）として標的型ランサムウェア攻撃を行っていたカナダ人を逮捕・訴追したことを公表した[10]。

このように、実際の実行役である「オペレータ」（アフィリエイト）が特定されるケースは稀であるが、司法当局による捜査としてだけではなく、サイバーセキュリティ業界による分析においても既知の攻撃グループとの結び付けに至れていないケースが大半を占める。その背景として、（広義の）アトリビューションに不可欠な「特徴的なマルウェア／TTP[11]の類似」が見られないことではないかと筆者は推測しているが、その理由については次章で述べる。

3. 攻撃者グループ特定に至るプロセス

一般的には、長期間に複数の被害組織から見つかった共通のマルウェアや攻撃インフラの特徴、TTPなどの共通点から「攻撃グループ」を分類する。セキュリティベンダが呼称する「APT ○～」や「～Panda」といった名称がこの「グループ」[12]を指す。この「攻撃グループ」はあくまでも分析／追跡の便宜上グルーピングしたものであり、必ずしも物理的に特定人物たちの集団を特定しているものではない。

同じ攻撃グループの活動を複数のセキュリティベンダや専門機関が分析し、それぞれ発表しあったり情報交換をすることで、「グルーピング」の精度は増し、これに加えて捜査当局による刑事捜査や攻撃者のオペレーション上のミスなどを捉える[13]ことで物理的な「実行犯」が特定される場合がある。

標的型サイバー攻撃の目的の大半は「情報窃取」にあるため、長期間わたるオペレーションが行われやすく、また、技術的に高度な人材が再利用される傾向があると推測されることから、同一グループの活動が長年にわたって各所で観測されやすいのではないかと思われる[14]。

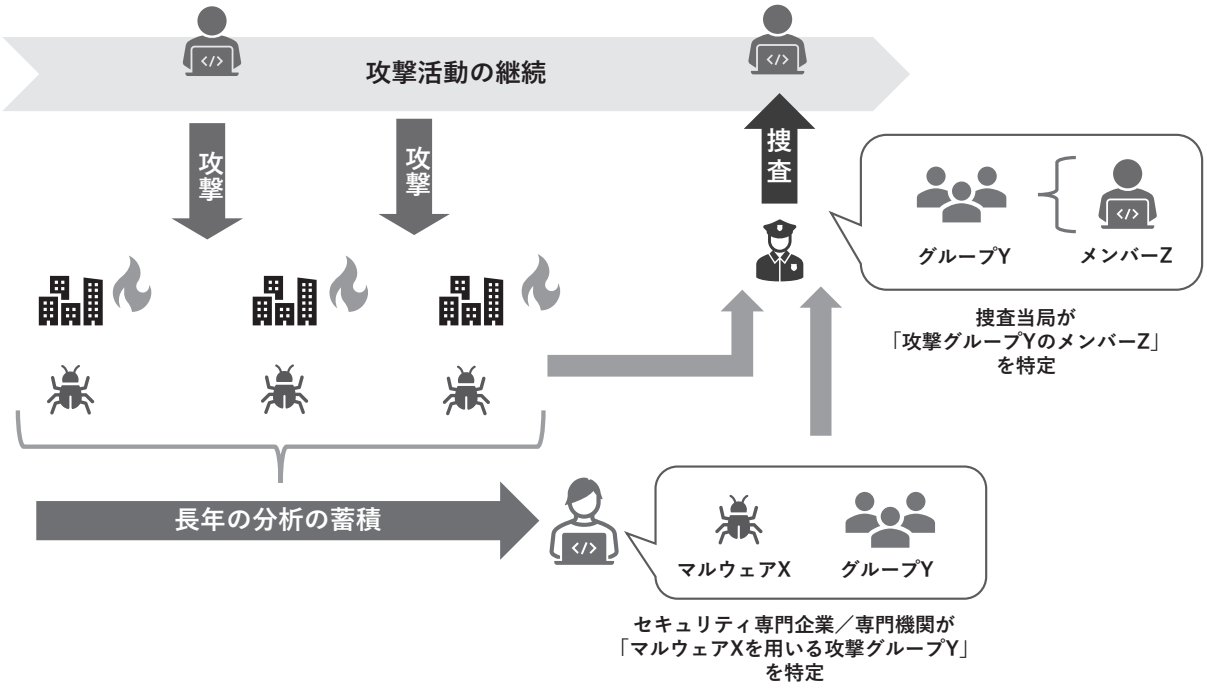
こうした長年にわたる活動のほか、攻撃グループ固有のマルウェアが使われることも攻撃者のグルーピングや追跡に重要なポイントである。例えば攻撃グループ固有のマルウェアは時間を重ねて改良されて使用され続けることが多く、被害現場に残されたマルウェアの詳細な解析により、特定の攻撃グルー

[8] Acronis, “DarkSide Ransomware Does Not Attack Hospitals, Schools and Governments”, <https://www.acronis.com/en-us/articles/darkside-ransomware/>
[9] DetaBreaches.net, “A chat with DarkSide”, April 12 2021, <https://www.databreaches.net/a-chat-with-darkside/>
[10] Department of Justice, “Department of Justice Launches Global Action Against NetWalker Ransomware”, January 27 2021, <https://www.justice.gov/opa/pr/department-justice-launches-global-action-against-netwalker-ransomware> この逮捕には仮想通貨のブロックチェーン分析を行う専門企業Chainalysis社が協力しており、同社のブログ記事では、押収された仮想通貨のブロックチェーン分析から、被告がNetwalkerのアフィリエイトスキームへの参加のほか、他のアフィリエイトスキームにも参加し、攻撃を行っていたとの推測がなされている。
Chainalysis, “Chainalysis in Action: U.S. Authorities Disrupt NetWalker Ransomware”, January 27 2021, <https://blog.chainalysis.com/reports/netwalker-ransomware-disruption-arrest>
[11] Tactics（戦術）, Techniques（技術）, Procedures（攻撃の流れ）の略
[12] グループ名に対して「Operation ～」のように一定期間／特定の攻撃手法／特定の評定分野に対する攻撃活動を一区切りの「攻撃キャンペーン」としてグルーピングすることがある。
[13] 攻撃グループのメンバーが攻撃用のサーバを契約する際などに登録したメールアドレスから、そのメンバーが攻撃グループとして活動する以前にネット上のフォーラムやSNS上に残した痕跡と紐づけされ、人物特定されるケースがある。
Crowdstrike, “Hat-tribution to PLA Unit 61486”, June 9 2014, <https://www.crowdstrike.com/blog/hat-tribution-pla-unit-61486/>
[14] また、攻撃対象とする国・地域となんらかの関係性を持つ国・地域に所在し、または当該国政府等の指示のもとで活動することから、活動地域の偏りがどうしても発生するため、攻撃者グループの特定がよりしやすくなっていると推測する

プによって過去の攻撃に使用されたマルウェアとの共通点などを見つけることで、攻撃グループの追跡が行えるのである。

これに比べて、標的型ランサムウェア攻撃の「オペレータ」たちは、特徴的なランサムウェア自体はスキームオーナーから提供されたものであり、被害現場では各オペレータが汎用的な攻撃ツールを用いることが多いため、各オペレータを特徴づける痕跡を見つけることが困難である[15]。

図１「攻撃グループ」の特定と「攻撃実行者」の特定



前述の通り、Solarwinds 事案では、米政府は攻撃者グループを APT29 であるとし、APT29 が SVR の傘下で活動していたと指摘しているが、これまでに各セキュリティベンダや米当局が公表したマルウェアや攻撃インフラの解析結果からは、過去の APT29 の活動との明確な共通点は見つかっておらず[16]、米当局は一般的な攻撃分析以外の情報により犯行を断定したと思われるが、その詳細は不明である。

同じく、コロニアルパイプライン社を攻撃したランサムオペレータも具体的にどの攻撃グループだったのか、技術的に特定できる情報は現時点で公開されていない[17]。

4. ケーススタディ

前章では SolarWinds 事案とコロニアルパイプライン事案という発覚直後に米政府がアトリビュー

[15] とはいえ、一部のオペレータをグルーピングし追跡する試みは行われており、例えばランサムウェア Ryuk の攻撃を行っているとされるオペレータのうち、比較的多くの事案を引き起こししている攻撃グループを Fireye 社は「UNC1878」として追跡している。（※ UNC は既知の攻撃グループとの紐づけを保留している「未分類 (uncategorized)」区分の意）
Fireeye, “Unhappy Hour Special: KEGTAP and SINGLEMALT With a Ransomware Chaser”, October 28 2020, <https://www.fireeye.com/blog/threat-research/2020/10/kegtap-and-singlemalt-with-a-ransomware-chaser.html>

[16] カスペルスキー社は Solarwinds 事案で使用されたマルウェア SUNBURST が過去に攻撃グループ「Turla」が使用してた Kazuar マルウェアに似ている点があるとする分析レポートを公表している。Turla についてもロシアとの関連が疑われる標的型攻撃グループであるが、米政府が指摘した APT29 とは別の攻撃グループとされている。
Kaspersky, “Sunburst backdoor – code overlaps with Kazuar”, January 11 2021, <https://securelist.com/sunburst-backdoor-kazuar/99981/>

[17] Fireye 社は DarkSide のオペレータとして 3 つのグループを追跡しているとしているが、過去のどのような攻撃に関わっていた攻撃グループなのかは不明として、UNC 分類をしている（未分類グループについては、脚注 15 を参照）Fireeye, “Shining a Light on DARKSIDE Ransomware Operations”, May 11 2021, <https://www.fireeye.com/blog/threat-research/2021/05/shining-a-light-on-darkside-ransomware-operations.html>

ション等を行った事案を取り上げたが、本章ではこの他過去の２つの事案のケーススタディから、アトリビューションの論点について検討してみたい。

4.1. SonyPicturesEntertainment 社へのサイバー攻撃事案（2014 年 11 月）

2014 年 11 月に発生した、ソニー・ピクチャーズエンタテインメント社へのサイバー攻撃（以下「SPE 事案」）では、発生が報じられた翌週にはトレンドマイクロ社、カスペルスキー社が、2013 年に韓国で発生した DarkSeoul 事案と同じ攻撃グループとの共通点を指摘する分析レポートを公表した[18]。これは被害現場から見つかったマルウェア「Destover」が 2000 年代後半から主に韓国向けの同グループの攻撃で用いられてきたマルウェアと同じベースを持っていることが判明したためである。

後に Lazarus と呼称されるこの攻撃グループは、2000 年代から韓国を狙った大規模な攻撃活動を度々行っており、韓国国内だけでなく欧米のセキュリティベンダも追跡を行い、知見が蓄積されてきていた。

Lazarus はこの攻撃グループ特有の特徴的なマルウェアを長年にわたり改良を重ねて使用してきた。そのためマルウェアから攻撃グループを比較的特定しやすく[19]、2014 年の SPE 事案においても早期の攻撃グループ特定に至ったと思われる。

4.2. 平昌冬期五輪開会式における OlympicDestroyer 感染事案

2018 年 2 月の平昌五輪開会式では Olympic Destroyer と呼ばれるマルウェアが使用され、攻撃グループの特定に大きな混乱を招いた[20]。当初、複数のセキュリティベンダは前述の攻撃グループ Lazarus の関与を指摘した。一方、APT3,APT10 が用いたマルウェアとの共通点を指摘する情報など他の攻撃グループによるものとする分析レポートが複数公表され、各セキュリティベンダの意見が割れることとなった。

4 か月後の Kaspersky 社の分析レポート[21]により、OlympicDestroyer は攻撃者（開発者）が Lazarus の過去のマルウェアの特徴を意図的に組み込ませていたことが判明し、いわゆる「偽旗作戦」が行われたことが指摘された。そのため、同年 3 月に APT28（Sofacy）の関与の可能性指摘していた同社はこの攻撃の実行者について、新たな未知の攻撃グループとして再区分を行うに至っている。

さらに 3 年後の 2020 年 10 月に米司法当局が同事案に関与したとして GRU 要員 6 名の刑事訴追を発表[22]し、被告らが関与した過去の攻撃事例から、長年にわたりセキュリティ業界から「Sandworm」と呼

---

[18] Kaspersy, “Sony/Destover: mystery North Korean actor’s destructive and past network activity”, December 4 2014, <https://securelist.com/destover/67985/>

Trendmicro, “Analysis of the Malware Behind FBI Warnings”, December 4 2014, <https://www.trendmicro.com/en_us/research/14/l/an-analysis-of-the-destructive-malware-behind-fbi-warnings.html>

[19] Lazarus については、実際には一つのグループではなく、ある時点から複数の「サブグループ」に分かれ、それぞれの目的に応じた攻撃活動を国際的に展開していると推測されているが、マルウェアの「系譜」などから、各サブグループの動向が追跡されている。 2018 年 9 月と 2021 年 2 月に米司法省が Lazarus の攻撃活動に関与していたとして、3 名の北朝鮮国籍の人物の刑事訴追を発表しているが、このうち、2018 年 9 月に訴追された被告は 2018 年 10 月の Fireeye 社のレポートによると、複数のサブグループにマルウェアを提供する役割を担っていたのではないかとされており、マルウェア開発作業が組織的に管理されている可能性がある。今後もセキュリティベンダや専門機関によるマルウェアや攻撃手法の分析と刑事捜査との組み合わせによって、その活動の全容が解明されることが期待される。

Fireeye「APT38 新たな攻撃グループの台頭」（2018 年 10 月）<https://www.fireeye.jp/content/dam/fireeye-www/regional/ja_JP/current-threats/apt/rpt-apt38.pdf>

[20] 各セキュリティベンダの分析は Virustotal 上になんらかの経緯でアップロードされた検体の解析がベースとなっており、実際の現場対応で得られる情報等が不足した状態で行われているため、ある程度、分析の精度が落ちてしまうことはやむを得なかったともいえる

[21] Kaspersky, “Hades, the actor behind Olympic Destroyer is still alive”, June 19 2018, <https://securelist.com/olympic-destroyer-is-still-alive/86169/>

[22] Department of Justice, “Six Russian GRU Officers Charged in Connection with Worldwide Deployment of Destructive Malware and Other Disruptive Actions in Cyberspace”, October 19 2020, <https://www.justice.gov/opa/pr/six-russian-gru-officers-charged-connection-worldwide-deployment-destructive-malware-and>

ばれた攻撃グループと紐づくことになった[23]。

このケースでは、SPE 事案とは対照的に、多数のセキュリティベンダがこれまで蓄積された知見を用いて攻撃グループの特定に取り組んだものの、偽旗作戦により混乱し、最終的な特定には 3 年近くの時間を要することになったのである。

5. 即応的なアトリビューションや対抗措置は可能か

Solarwinds 事案については、セキュリティベンダや専門機関が公開していない情報や政府独自の情報により、攻撃グループと SVR との関係を突き止めた可能性があるが、第 4 章で述べた過去の特定ケースを踏まえると、既知の活動との紐づけが困難な標的型サイバー攻撃の場合、即座に攻撃グループを特定したり、その背後に特定国の関与があるのか調査することは難しく、事案発生後ある程度の時間を要する可能性が高い。また、偽旗作戦のような工作や攪乱行為を行われた場合、特定は不可能になるか、長い時間を要することになる。

一方で、標的型ランサムウェア攻撃については少し事情が異なる。

標的型ランサムウェア攻撃のアフィリエイトスキームのオーナーやオペレータは情報窃取を目的とした標的型サイバー攻撃の攻撃グループとは異なり、従前は金銭目的のサイバー犯罪を行ってきたグループのメンバーが多いと思われる。

金銭目的のサイバー犯罪を行ってきたグループは、情報窃取目的の標的型サイバー攻撃の活動よりも活動が活発で、フォーラムや SNS 上の露出も多く、個人特定に至るような情報を残すミスも起こしがちなことから、セキュリティベンダの調査のみであっても人物特定されているケースが比較的多い。一方で複数国に分散して所在し、一つのサイバー犯罪スキームを運営することが多いため、人物や活動拠点の特定に多大なコストがかかることが想定される。

2021 年 6 月 17 日にランサムウェア CL0P のオペレータから入手した身代金のマネーロンダリングを行っていたと思われる[24] メンバーがウクライナ当局に逮捕された。ランサムスキームのオーナーはロシアに所在していると思われ、同グループの活動への影響は限定的とも思われる。

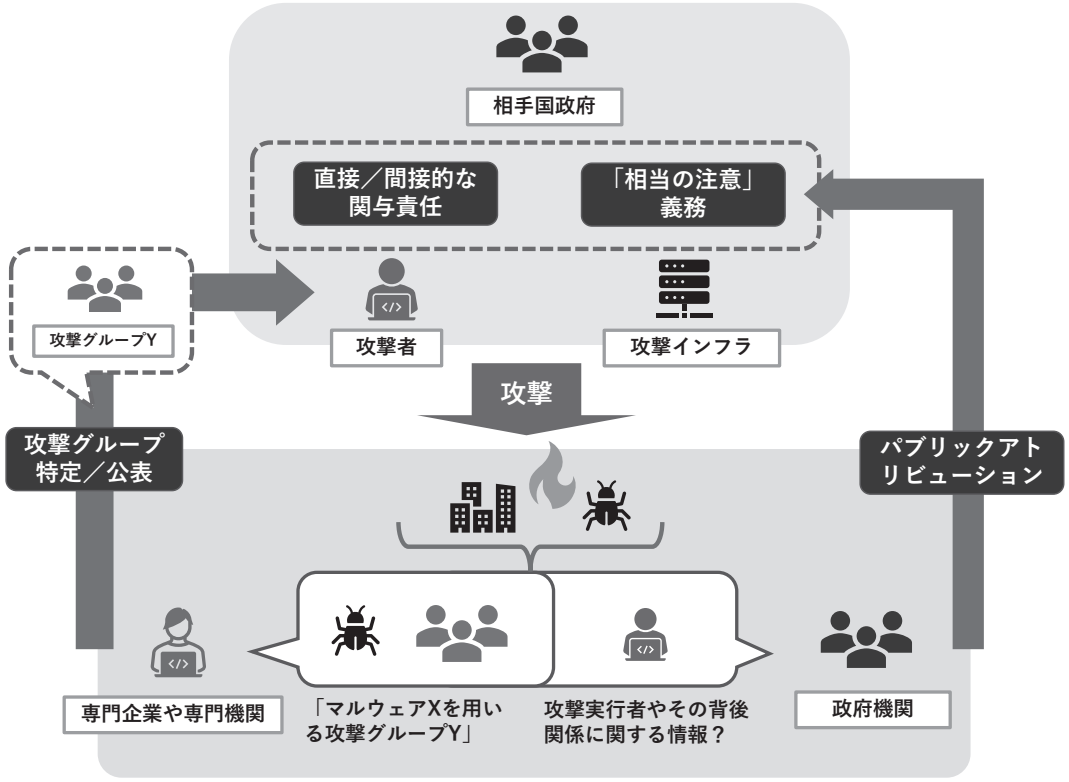
こうしたサイバー犯罪系のグループは所在する国内の企業等にも攻撃を行うことがあり、所在国捜査当局からの捜査の手がいつか及ぶ前提でグループメンバーやインフラを複数の地域に分散させている可能性があるのではないかと考えられる。

ここまでの事例考察から、何らかの対抗措置を打つための法的手続きに必要な個人の特定、所在地の特定には一程度の時間をかける必要があると想定され、事案発覚／発生直後のアトリビューションは困難であると考えられる。一方で、どのようなケースであれば、速やかなパブリックアトリビューションが可能なのか検討する。

[23] あくまでもこれまで複数のセキュリティベンダが追跡してきた「Sandworm」が行った攻撃事例と米当局が起訴した対象事件が一致しているだけで、同起訴状で公表された情報から Sandworm に関する技術的情報との結びつきは確認されていない。

[24] 本稿執筆当時は被告らの国籍や具体的な役割は不明である。
National Police of Ukraine, “Кіберполіція викрила хакерське угруповання у розповсюдженні вірусу-шифрувальника та нанесенні іноземним компаніям пів мільярда доларів збитків”, June 16 2021, <https://www.npu.gov.ua/news/kiberzlochini/kiberpolicziya-vikrila-xakerske-ugrupovannya-u-rozpovsyudzhenni-virusu-shifruvalnika-ta-nanesenni-inozemnim-kompaniyam-piv-milyarda-dolariv-zbitkiv/>

図２　サイバー攻撃の分析とパブリックアトリビューションの関係



即応的なパブリックアトリビューションが可能なケースと困難なケースを整理したのか表１である。

セキュリティベンダなどの過去の調査により「攻撃グループ」がグルーピングできており、発生した事案も「この攻撃グループが行った」というところまで技術的にかなりの確度で整理できていたとしても、実際にその実行者たちの所在地を特定するには情報が不足する（ケース１）。

他方で、長年にわたる追跡で攻撃者のミスや地理的特性から、ある程度所在地域が確度をもって推測できる場合や、攻撃活動の一部は（自国以外も含む）刑事訴追などによって実行した人物／組織やその所在地が明らかになっている場合、今回の攻撃を実行した人物／組織の特定まで至れなくても、これらの情報を組み合わせて、当該グループが所在する国、あるいは攻撃インフラが所在する国に対して、なんらかの意思表明をすることは可能であると思われる（ケース２、ケース３）。

現時点においては、コロニアルパイプライン事案がケース２またはケース３なのか不明であるが、ロシア当局の関与が不明であったとしても、ランサムウェアのアフィリエイトスキームのオーナーまたはオペレータ、あるいは攻撃インフラがロシア国内に所在していたという確度の高い情報があれば、少なくとも第２章で述べたような「相当の注意義務」違反として非難声明を出すことも、そこまで難しくはないように思えるが、同じく第２章で述べた、現時点における DarkSide のオペレータに関する情報においては、少なくとも今回の攻撃を実行したオペレータの所在地を具体的に示す情報は民間レベルでは得られておらず、ロシア国内のホスティングサービスを攻撃インフラとして悪用するオペレータがコロニアルパイプライン事案を行ったのかも不明である[25]。

[25] なお、米 US-CERT がコロニアルパイプライン事案を受けて発表した文書には同事案で悪用されたとみられる通信先の情報が公表されているが、キプロスのホスティング会社が管理する IP アドレスになっている。特に VPS（仮想専用サーバ）が攻撃に使われる場合、外部から見える IP アドレスと実際にサーバが所在する場所が異なることが多いため、IP アドレスのみからその所在地まで短期間で特定することは難しい。
US-CERT, “Alert (AA21-131A) DarkSide Ransomware: Best Practices for Preventing Business Disruption from Ransomware Attacks”, May 11 2021, <https://us-cert.cisa.gov/ncas/alerts/aa21-131a>

表１　即応的なパブリップアトリビューションが可能なケース

	技術的な分析で、既知の攻撃グループによる犯行と判明しているか	地理的特性を示す情報やオペレーションミスでおおよその所在地域が判明しているか	過去に関連する刑事訴追実績があり、攻撃者や活動の所在地が判明しているか	即応的にパブリックアトリビューションできるか
ケース１	判明している	不明	不明	×
ケース２	判明している	判明している	不明	△ ※左記分析結果の確度次第
ケース３	判明している	（判明している）	判明している ※対象となる攻撃グループと過去に所在が確認された人物／グループとの関連性が明確な場合	○

6. ケーススタディから見える課題

4 章と 5 章の分析から、アトリビューションについては様々な課題が浮かび上がってくる。ここでは代表的なものを 3 つとりあげる。

6.1. 事前の情報の蓄積

ここまで述べた通り、長年にわたるセキュリティ専門企業や専門機関による攻撃の分析による「コミュニティの知見の蓄積」というベースがあってこそ攻撃者の特定が可能であり、また、複数の専門組織が同じ攻撃活動／攻撃グループを対象に分析し、国を超えてレポート発表やカンファレンスでの講演などを経ることでその精度が向上することも重要な要素となっている。

例えば、ある一国でしか攻撃が確認されていない攻撃グループの場合、分析に関与する専門企業／専門機関の母数が少なくなるため、攻撃者特定のためのベースとなる情報や知見、さらには情報交換による分析精度の向上には限界があると考えられる。したがって、そのような“マイナーな”攻撃グループによる大規模なサイバー攻撃が行われた場合、基本的には「コミュニティの知見」の恩恵を得ることは難しく、１国内での対応知見での対処に迫られるのである。

6.2. 大規模サイバー攻撃におけるサボタージュ作戦の可能性

今後、重要インフラや国際イベントなどを狙ったサイバー攻撃が発生した場合、その手法としてはサボタージュ的な戦術が採られる可能性が高いと考えている。

その場合、攻撃によって混乱を引き起こすこと自体が目的である可能性が高いため、OlympicDestroyer 事案のように偽旗作戦が行われたり、全容解明までの時間を引き延ばすために攪乱工作を行う可能性がある。

前述の通り、こうしたケースでは現場から検体の解析等が必ずしも速やかな攻撃者特定につながるとは言えず、ある程度時間をかけた精査が必要になるため、社会的な影響を鑑みて即応的な対抗措置やパブリックアトリビューションを望む声に対して、望ましいタイミングで分析結果がもたらされない可能性が想定される。

6.3. 現場初動対応の課題

大規模なサイバー攻撃、特に今回取り上げたケースであれば、Solarwinds 事案のような長期にわたる標的型サイバー攻撃が発覚するようなケースではなく、コロニアルパイプライン事案のように攻撃被害の発生≒何らかのサービス影響を伴うような、即応的な対応が迫られる大規模サイバー攻撃の場合、攻撃者特定のための基本的な情報をインシデント対応現場から得られない可能性が高い。

社会的に大きな影響を与えるような攻撃の場合、重要インフラのサービス停止などが発生すると想定

されるが、この復旧作業が優先される中、通常のインシデント対応のように検体の回収・分析やログ分析などを悠長に行っている時間的余裕はないと考えられる。

本稿ではこの課題について検討する余裕はないため、また別の機会でご紹介できればと考えるが、大規模サイバー攻撃対処の根本的課題として示したい。

7. おわりに

社会的に大きな影響／反響のある大規模なサイバー攻撃が発生した場合、速やかに攻撃者を特定し、何らかの対抗措置へ結びつけていくことは非常に難しい。

特に OlympicDestroyer 事案のように、情報が多く流通していても、多くの分析組織が関与しても偽旗作戦により正しい分析が行えないケースがある。特に社会的混乱を目的とした大規模サイバー攻撃においては、今後より一層、分析回避行為や攪乱行為が行われるケースが増えることが想定される。

その場合、情報の量や解析リソースが多ければよい結果を出せるわけではなく、むしろ間違った分析結果などが入り乱れ、政策判断を混乱させる可能性すら出てくるのである。

悲観的なことばかり述べたが、一方でセキュリティ専門企業やアナリストたちは過去の失敗経験や対応困難な事象から学び、情報を発信・交換し続けることで改善を試み続けている。そして、試行錯誤を繰り返しているのは米国政府の各当局も同じであろう。紆余曲折がありながらも、アトリビューションに必要な捜査手法、手続きが徐々に確立してきていると言える。[26] また、アトリビューションに必要な技術的情報の整理やその解釈方法といった、現場側の分析手法も体系的な整理が進みつつある [27]。他方、米当局ならではの手腕が発揮されてきたアトリビューション事例もあるため、同じような方法を我が国はじめ他国でも直ちに実践することは困難である。

アトリビューションの目的は必ずしも経済制裁などの対抗措置や刑事訴追のためだけではない。パブリックアトリビューションが行われるようになった歴史は浅く、その効果は未知数である。また、民間レベルで攻撃グループの活動についてレポート公開するという「手の内を明かす」ことで、攻撃者がどのように活動を変化させるのか、また何らかの抑止になるのかについては実証的に検証されているわけではない。進化を続けるサイバー攻撃者に対する旧来の対抗措置以外のアプローチ方法について、アトリビューションのための捜査手法や分析手法の進化に遅れることなく、多様に検討されるべきではないかと考える。本稿で述べたような大規模なサイバー攻撃、特に重要インフラなど社会的影響の大きいサイバー攻撃には何らかの即応的な対応が求められるところ、ここまでに考察したように従前のアトリビューションのアプローチでは対応は難しく、既存の刑事捜査や国際法上の手続きだけにとどまらない、新たなコンセプトによる、攻撃者側へのアプローチが求められているのではないだろうか。

[26] 2014 年 5 月に初めて公表された標的型サイバー攻撃グループに対する刑事訴追の公表（APT1 の起訴）へ至る経緯、特に司法当局による判断などについては、David Sanger「The Perfect Weapon: war, sabotage, and fear in the cyber age」(2018) などで触れられている

[27] Timo Steffens 他「Attribution of Advanced Persistent Threats: How to Identify the Actors Behind Cyber-Espionage」（2020）