防衛研究所 National Institute for Defense Studies
NIDSコメンタリー
特集：「新領域の安全保障」vol.6
第346号　2024年8月6日

サイバー攻撃対処における攻撃「キャンペーン」概念と「コスト賦課アプローチ」

――近年の米国政府当局によるサイバー攻撃活動への対処事例の考察から

政策研究部サイバー安全保障研究室　特任研究員　佐々木　勇人

政策研究部サイバー安全保障研究室　研究員　瀬戸　崇志

はじめに

本稿の主著者（佐々木）は、これまで日本国内でのインシデント対応等の実務に従事する過程[1]で、「日本国内のサイバーセキュリティは、『被害組織／将来の標的組織』側に過度に対応が集中し、『攻撃者』側に対応が向いていない」との思いを強く抱いてきた。

例えば、「サイバー攻撃は攻撃者側が圧倒的に有利」や「サイバー攻撃は匿名性が強いので実行者を捕まえることができない」といった声がよく聞かれる。確かに、攻撃が早期に認知できないケースは多く、実行者を特定し逮捕できないケースも多い。そのため国内のサイバーセキュリティ施策の多くは、被害組織／将来の標的組織の対策を強化し、いざ事が起きれば、再発防止策を徹底させ、また、ガイドライン等の対策基準をアップグレードするサイクルに重きを置いてきた。企業や個人に対策を求める行政側や、対策・サービスを提供するセキュリティ業界側も、サイバー攻撃側の優位性や匿名性といった脅威の点を強調することで、企業や個人に事前対策の導入・強化を迫ることが多い。

他方で、対策強化を求められる企業や個人からすると、次々に新たな攻撃手法／攻撃活動／攻撃グループが登場する状況や、これに対してセキュリティ対策の「どこまでやっても十分でない」点、そして、ひとたび攻撃被害を受けた後の膨大な事後対応コストなどに徒労感・閉塞感を感じざるを得ない。様々なプレイヤーのベクトルが被害組織／将来の標的組織側に過度に集中することの問題[2]は、こうした層の対策強化やそのためのインセンティブ設計に限界が出るだけでなく、国や専門組織が攻撃者側の動向把

握に必要とする脅威情報の流通にも大きな影響を及ぼしている。筆者の前回の考察[3]では、官民間で脅威情報の共有がうまく行われない理由、特に被害現場側から行政側に情報提供がされにくい構造的問題として、行政側が提供された情報を何に活用しているのか、提供側（被害組織側）から見えない点を指摘した。一方で、国側での「攻撃者側への対処」オプションは限定的であり、国として「攻撃者側にこういうことができるので、情報提供いただきたい」と真正面から示せないのが現状でもあろう。

以上の問題意識を踏まえて、本稿では、日本国内では前例の乏しい「攻撃者側への対処」について、その先例を積み重ねてきた米国政府の事例を振り返りながら、いかにサイバー攻撃側の優位性や攻撃者の匿名性を乗り越えて、攻撃者側に対処する選択肢を米国政府が増やそうとしているのか、そしてその効果がどの程度見込まれるのか考察しつつ、攻撃者への対処を考える上で重要な攻撃「キャンペーン」や「コスト賦課アプローチ」といった概念についても紹介したい。

なお本稿の着想や分析・執筆は、基本的に全て主著者（佐々木）個人の研究成果に基づく。ただし同僚の瀬戸崇志研究員からは、主に政府による「攻撃者への対処」の歴史的・理論的視座や近年の米国当局の取組の内在論理をめぐる知見を頂いたほか、特に第 2 節や第 5 節の執筆では、引用すべき先行研究や史料の提示、論理構成等への忌憚の無い意見や具体的な加筆修正を頂くなど、主著者のセキュリティ業界での実務経験の知見を、学術研究の蓄積にも裏打ちされた論考として磨き上げる上で必要な様々な支援を頂いた。以上の脱稿までの経緯も踏まえ、ご本人の了解の下で、共著者に連名させて頂く形とした。

1．セキュリティ業界における攻撃「キャンペーン」の捉え方

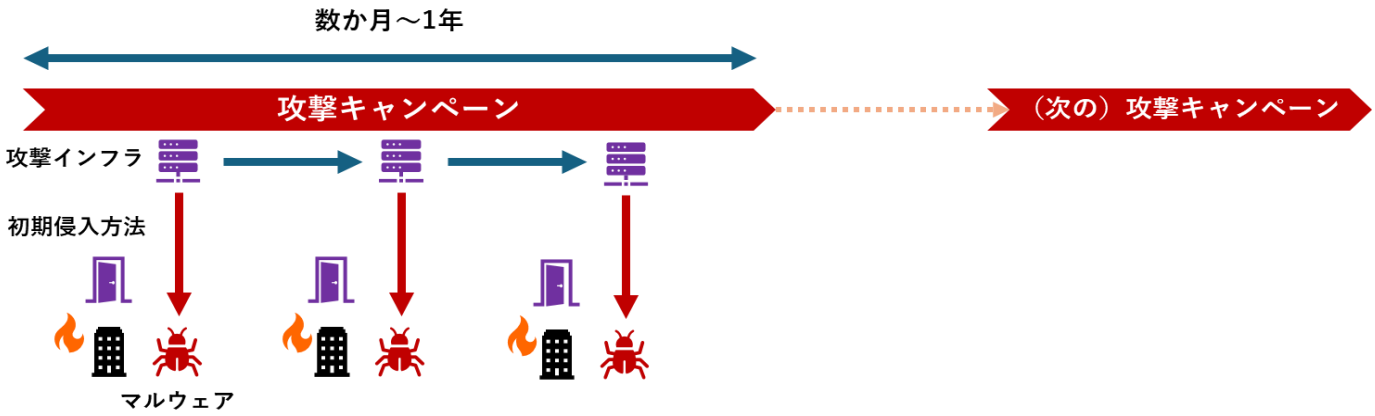
世界市場の中でも欧米圏の企業が業界標準の牽引力を握るセキュリティ業界では、米軍を始め、軍事の世界やインテリジェンスの用語・概念が民間側で借用される例が少なくない。例えば、主に国家的背景を持つ、高度な標的型サイバー攻撃を行う攻撃活動／攻撃グループについて「APT：Advanced Persistent Threat」と呼称されるが、この用語は 2006 年頃から米空軍内で用いられたものだとされている。他にも、主に APT アクターの攻撃プロセス／フェーズとその対策を整理したフレームワークである、「Cyber Kill Chain」フレームワークは、米航空大手、ロッキード・マーティン社のセキュリティ研究者が軍事用語としての「Kill Chain」の概念を使って編み出したものである[4]。

今日のセキュリティ業界では、特定の APT アクターにより、一定期間内に行われる複数の攻撃のまとまりを示すものとして、サイバー攻撃の「キャンペーン（または攻撃キャンペーン）」という表現を用いる[5]。セキュリティ専門組織の分析レポートなどにおいて、「〇〇〇（攻撃グループアクター名）による攻撃キャンペーン」と記述されたり、あるいは「Operation ×××（×××作戦）」と記述されたりするもので

ある。本稿が着目する、この「キャンペーン」という用語も、軍事用語たる「戦役（campaign）」に語源を持つとみられる。この意味での「戦役」とは、「ある戦略目標の達成に向けて、一定の時間的範囲と地理的範囲のなかで計画・実施される複数の軍事作戦のまとまり（a set of military operations[…] to achieve a strategic objective within a given time and geographical area）[6] 」を指す。

「政府機関」や「重要インフラ分野」、「先端技術」のように攻撃者が狙う特定の分野／情報の種類を 1 つの区分として、「攻撃キャンペーン」が整理・特定されることが多いが、必ずしも攻撃キャンペーンの向かう先が特定の分野／情報に限定されるわけではない。複数の業種が狙われてもひとつの攻撃キャンペーンとして区分されることもある。その場合、攻撃キャンペーンは同一の攻撃手法（初期侵入方法やマルウェア等）／同一の攻撃インフラ（C2 サーバ等）が用いられていることをもって整理・特定される。

図 1：タイムラインから見た「攻撃キャンペーン」の概要



出典：各種公開情報から主著者作成

他方、金銭目的のサイバー犯罪者の活動は、（国家を背景とした） APT アクターほど、攻撃キャンペーンの始期・終期を含めた活動区分は明白にはならないことが多い。各国で猛威を振るったマルウェア「Emotet」のように度々攻撃の「波」が発生したものもあるが[7]、サイバー犯罪者のフィッシングやランサムウェア攻撃は、多くは年中切れ目なく行われる。こうした違いが生ずる理由には、国家を背景とした APT アクターに比して、金銭目的の犯罪者が圧倒的に多数存在することが一因かもしれないが、必ずしも数の問題だけでなく、APT アクターの攻撃キャンペーンの特徴に起因すると考えうる 2 つの仮説が考えられる。

1 つ目の仮説は、攻撃の目的である。APT グループによる攻撃キャンペーンの多くは、特定分野の情報窃取を目的とするか、サボタージュ的なデータ破壊等を目的としている。特定組織がもつ特定の情報、ある期日までの組織の行動に関する情報、特定のシステムの停止・破壊といった「目的」を達成するタイミ

ングが必ず発生するため、その時点で攻撃キャンペーンが自然と終わる可能性がある。

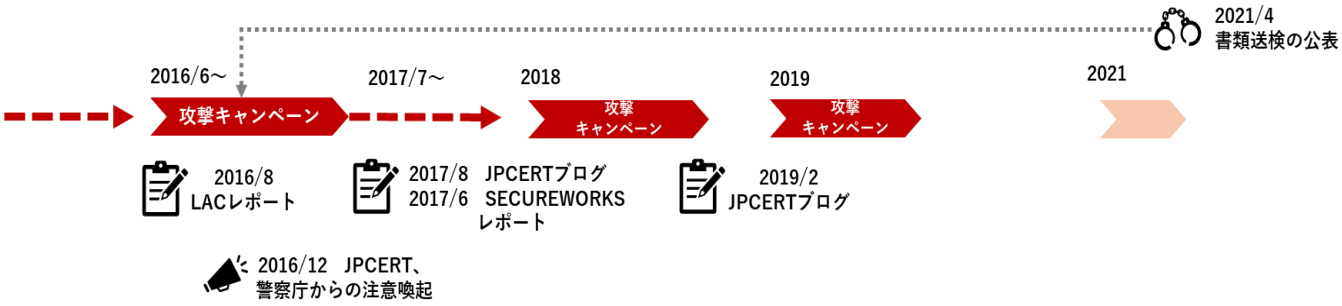
2 つ目は防御・対処側の動きによるものである。APT キャンペーンの多くでは、期間内において特定の攻撃手法や特定の攻撃インフラが用いられる。セキュリティ製品による検出を回避するために未知の脆弱性を初期侵入に使ったり、新たに開発された固有のマルウェアを使うことがあるが、なんらかのきっかけで攻撃キャンペーンの途中で被害組織側／防御側に検知され、セキュリティ専門組織が分析レポートを公表したり、専門機関からの注意喚起が行われることで、これらの攻撃手法が“陳腐化”してしまい、攻撃キャンペーンは終わりを迎えることがある。

かつては、攻撃キャンペーン毎の新たなマルウェア投入や、検出を回避・発覚を遅らせるために国内の正規サーバを踏み台とした攻撃などが度々行われてきたが、ここ数年では、固有のマルウェアではなく、被害組織で稼働する Windows OS の正規機能やオープンソースツールなどを使って検知を回避する、Living off the Land 戦術を採る APT アクターが増えてきている[8] 。ただし、こうした回避戦術も完全なものではなく、Living off the Land 戦術を使っていた APT アクターである Volt Typhoon は、攻撃インフラとして KV ボットネットという特定のボットネット[9]を使っており、このボットネットが特定され、対抗措置を打たれた[10]ことで一時的に活動を停止したと考えられる。他方で、攻撃インフラの特定・検出は困難だが、固有のマルウェアを改良して使い続けているアクターも存在する。いずれにせよ攻撃手法やインフラがセキュリティ専門組織側に捕捉されることにより攻撃キャンペーンは終結することがある。

このように、攻撃の事案を単発の「点」として捉えるのではなく、時間的広がりの中の「線」で捉える発想は、語源としての軍事用語の「戦役」とサイバーセキュリティにおける「キャンペーン」双方に共通する。また、上記仮説 1 のように、特定の目的単位でキャンペーンが形成される点や、仮説 2 のように、防御側の対処によってキャンペーンが目的達成前に終結を迎える点も共通した考えであろう。

最後に、攻撃キャンペーンの時間的な広がりについて付言したい。APT の攻撃キャンペーンは、多くの活動では数か月～1 年単位の攻撃キャンペーンが数年内に繰り返され、長ければ 10 年以上、断続的に繰り返されているケースもある。例えば Tick と呼ばれる APT グループは、2021 年に日本の警視庁により攻撃の支援者の書類送検が行われ、併せて警察庁から、同グループが中国人民解放軍戦略支援部隊の隷下にあったことが公表された[11]。ただし、この書類送検対象事案は、元を辿れば 2016 年の攻撃キャンペーンの一部であり、その公表までの約 5 年の間、Tick は複数回の攻撃キャンペーンを繰り返していた。

図 2：中国人民解放軍隷下の Tick による攻撃キャンペーンのタイムライン



出典：各種公開情報から主著者作成

2．米国政府の「攻撃者への対処」の思想史：懲罰的抑止から持続的交戦へ

近年、日本でも「能動的サイバー防御」をめぐる議論の中で、2018 年以降に米国サイバー軍（USCYBERCOM）が採用した「持続的交戦（Persistent Engagement）」－または「前方防衛（Defend Forward）」－と呼ばれる概念が参照される[12]。これらは、後述の 2010 年代に主に採られた「懲罰的抑止」アプローチの失敗が明白に認識され、これに代わって国家を背景とする攻撃キャンペーンの脅威に対処する新たなアプローチが必要とされたなか、米国の国防専門家コミュニティでの理論的検討を通じてボトムアップで受容されたものである[13]。言い換えれば、特に 2018 年以降の米国での「攻撃者への対処」のアプローチとは、米国政府によるサイバー攻撃対処の思想の歴史的系譜の上に成り立っている。

したがって、そのような歴史的系譜を理解するにあたり、まずは、2010 年代以降の米国のサイバー攻撃対処の思想の変遷を振り返ってみたい。2013 年 2 月に Mandiant 社が、APT1 の実行犯を特定した経緯についてレポート[14]を公表しサイバーセキュリティ業界に衝撃を与えたが、その翌年には米司法省が同じ実行犯を特定し、APT1 の背後に居た中国人民解放軍関係者の刑事訴追を発表[15]した。これ以降、数年にわたり、米国では政府機関による「アトリビューション（attribution）」が国による標的型サイバー攻撃対処の前提条件と認識され、いかに実行犯を特定して、その背後関係を同定し、特定国に帰属をさせるかという点に注目が集まった。

米司法省がその後も多数の APT アクターのアトリビューションと刑事訴追を公表してきたことからもわかるように、少なくとも 2010 年代前半において、米国には攻撃グループの背後に居る実行犯個人や国家機関の特定を行い、その公表（パブリック・アトリビューション[16]）を行うことで、相手国政府によるサイバー攻撃グループの支援の費用対効果計算を変容させ、攻撃キャンペーンを抑止しうるとの期待[17]が

存在してきた。その背景には、アトリビューションによる攻撃活動／攻撃グループの背後の国家の情報機関や軍の存在の特定（と公表）は、攻撃者側に耐え難いコストを伴う反撃等のリスクを認識させ、その攻撃の実行・関与を（永続的に）自制させる、いわゆる「懲罰的抑止（deterrence by punishment）」を機能させる前提条件と考えられていた[18]からといえる。

このように「アトリビューション」という用語が安全保障政策の専門家コミュニティとサイバーセキュリティ業界の双方で、「抑止」を考えるキーワードとして用いられるようになった。その一方で、国際法や法実務の世界では、その用語の定義の一貫性の無さに疑義が示されてきた[19]。サイバーセキュリティ業界では、攻撃キャンペーンの技術的特徴や被害セクターの傾向等の合理的推論として成り立つ「バーチャル」な攻撃グループの特定[20]までを示す用語として多用される一方で、国際法上では、より具体的な個人・国家機関の関与の立証と国家責任の帰属を問うところまでを示すものとして用いられてきたからである。ただし、この用語法のギャップ[21]はどちらかが間違っていることを意味する訳ではない。この差異は、各々の専門家コミュニティが、「アトリビューション」がどのようにサイバーセキュリティや国家安全保障に貢献するかについての捉え方の違いに起因する。すなわち、アトリビューションの目的を、あくまでインシデント対応に必要な情報としての攻撃グループの技術的な特性情報の特定を重視するセキュリティ業界側と、上記の通り伝統的な懲罰的抑止を想定し、背後組織（相手国）の特定による、反撃による「耐え難いコスト」を課す能力の信憑性のシグナリングを意識してきた政府側との間の認識のギャップが、用語法の相違にあらわれている[22]。

さて、懲罰的抑止の前提として想定された「耐え難いコスト」の源泉には、理論上は様々な措置があると考えられてきた[23]。いずれにせよ重要な点は、今日では「アトリビューション」を起点とした「懲罰的抑止」のアプローチは、実証的なデータ上は殆ど有効性が支持されない点にある。米司法省が刑事訴追を公表した中でも、中国政府機関の関与があると指摘とされた APT3 や APT10 についてはパブリックアトリビューション後にその活動が停止したように、観測されたものは僅かながら存在する。しかし、APT10 については、その後に分派か再編成したと思われる後継的な複数のグループ／攻撃キャンペーンが観測されてきた。またロシア関連の攻撃グループの APT28、Sandworm、APT29 や、北朝鮮関連の攻撃グループである Lazarus や関連性が見られる各サブグループなど、パブリックアトリビューションが行われた後も、活動の大幅な中断期間や再編成の兆候的な動きが殆ど観測されないアクターも多く存在[24]する。

そして、2010 年代後半に至る過程での「懲罰的抑止アプローチ」の限界への認識を経て登場したのが、米国サイバー軍（USCYBERCOM）が 2018 年に採用した「持続的交戦（Persistent Engagement）[25]」の概念である。同概念は、2018 年の『米国国家防衛戦略』の目標を実現するための USCYBERCOM の指針を示す『サイバー空間における優越性の達成と維持：USCYBERCOM のためのコマンド・ビジョン[26]』で示

され、2018 年以降の米国サイバー軍の運用ドクトリンに準ずる実質的な地位を占めてきた（以降、便宜的に「持続的交戦ドクトリン」と呼称）。関連する米国政府の公文書[27]や、概念の理論的支柱を提供した研究者達の先行研究[28]を紐解く限り、「持続的交戦ドクトリン」は次の 2 点の特徴を持つ。

第 1 には、「持続的交戦ドクトリン」は、国家の関与を背景とする攻撃グループの動向分析・対処の枠組を「キャンペーン」単位で捉えている[29]。APT アクターによる攻撃キャンペーンは単発の攻撃を超えて、中長期的な継続を通じた累積的(cumulative)な悪影響を各国の安全保障や経済社会に及ぼすことを認識し、防御側もこれに様々な手段で対処し、攻防双方の永続的な「競争」を前提に、相手に対する自身の優位を維持し続ける必要性を説く[30]。

第 2 には、この「持続的交戦ドクトリン」を体現する近年の USCYBERCOM による様々なオペレーションは、防御的なものから攻撃的なものまで含めて多様な様態[31]を取りつつも、いずれも、「攻撃者または攻撃キャンペーン」の脅威を減ずるための「対抗キャンペーン」の一部と位置付けることができる。具体的には、様々な措置により、一義的には攻撃側の攻撃キャンペーンの目標達成の（一時的な）妨害（disrupt）を企図し、同時に、妨害の継続による相手方の累積的なコスト賦課（impose costs）も含めて、相手方の攻撃キャンペーンの「（継戦）能力の摩耗（degrade the capabilities and network of adversaries）」を試みる[32]。こうしたプロセスを通じ、（サイバー攻撃をゼロに出来ずとも）国家として許容し得ないレベルの重大な事案の発生のリスクを引き下げていくことに眼目があるとされる[33]。

まとめれば、「持続的交戦」ドクトリンの根幹には、先述した「攻撃キャンペーン」の単位に着目し、「攻撃者への対処」のために「攻撃キャンペーン」単位への対抗オペレーション（あるいは、その累積としての「対抗キャンペーン」）を展開することが織り込まれている。この点を踏まえて、以下では米国による対抗オペレーションの事例を見てみたい。

3．「有事」を意識した米当局の対抗キャンペーン：台湾とウクライナでの事例

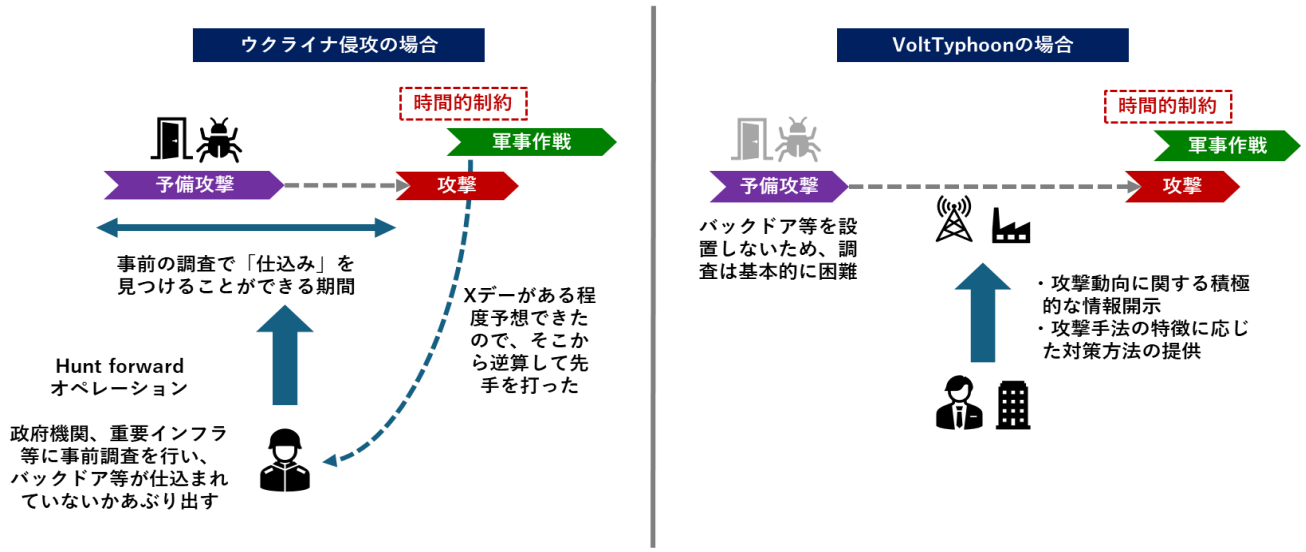
2023 年 5 月に米マイクロソフト社や米当局は、米国の重要インフラを狙う、Volt Typhoon による APT キャンペーンを公表し、注意を呼びかけた。この攻撃グループは将来想定される台湾有事など、有事（武力紛争）下での軍事作戦と連動した重要インフラシステムへの破壊活動を企図し、そのための侵入経路の開拓や有事にあわせた「再侵入」を行うものと分析されている。Volt Typhoon は少なくとも 2021 年頃から活動しているとされているが、その活動の最終目的はいまだ達成しておらず、これまでに確認された攻撃キャンペーンはある意味、長期的な攻撃キャンペーンの準備活動ともいえるのである。米当局側は 2023 年 5 月の注意喚起に加え、2023 年末には攻撃インフラである KV ボットネットの活動への妨害

を試み、2024 年 2 月には改めて重要インフラ事業者等への注意喚起やアドバイザリー公開を行っている。

2022 年のウクライナ侵攻では、その前後にて政府機関や重要インフラを狙った大規模なサイバー攻撃が度々行われたことがウクライナ政府を支援したマイクロソフト社[34]や、セキュリティ企業の ESET 社[35]などから報告されている。また、米サイバー軍は 2021 年 12 月の時点から現地に要員を派遣し、重要インフラシステムなどにおける侵害痕跡を探索する、Hunt Forward 作戦を行っており、ウクライナ当局者がメディアからの取材に語ったところ[36]では、事前に調査した対象についてはその後深刻な攻撃被害が出なかったとされる。

この 2 つの米当局の対処は基本的に同じコンセプトで整理することができる。有事に連動したサイバー作戦は、ある意味、キネティックな通常軍事作戦側の要請により活動タイミングを「制限」されており、有事の「X デー」がある程度予想される場合、そこから逆算して活動の存在を予想できてしまうのである。ウクライナでの対応では、米当局は 2021 年末の段階から翌 2022 年 1 月～2 月の軍事侵攻の可能性をすでに示しており、かなり正確に「逆算」ができていたと思われる。他方で Volt Typhoon のケースでは、具体的な「X デー」の日時はウクライナでのケースほど示されていないが、すでに活動が一部検出されたことで、注意喚起を発することが可能になったのである。Hunt Forward 作戦のように標的となる可能性の高い組織の調査を行う直接的な対応や、将来予想される攻撃活動やその準備活動に関する注意喚起を呼び掛ける間接的な対応により、相手方の攻撃キャンペーンを妨害したり、仮に攻撃が本格化しても予め標的組織側の対策を強化しておくことで、遅滞戦術を採ることが可能になるのである。

図 **3**：２つの攻撃キャンペーンの通常軍事作戦との連動による「制約」に着目した米側の対処



出典：各種公開情報から主著者作成

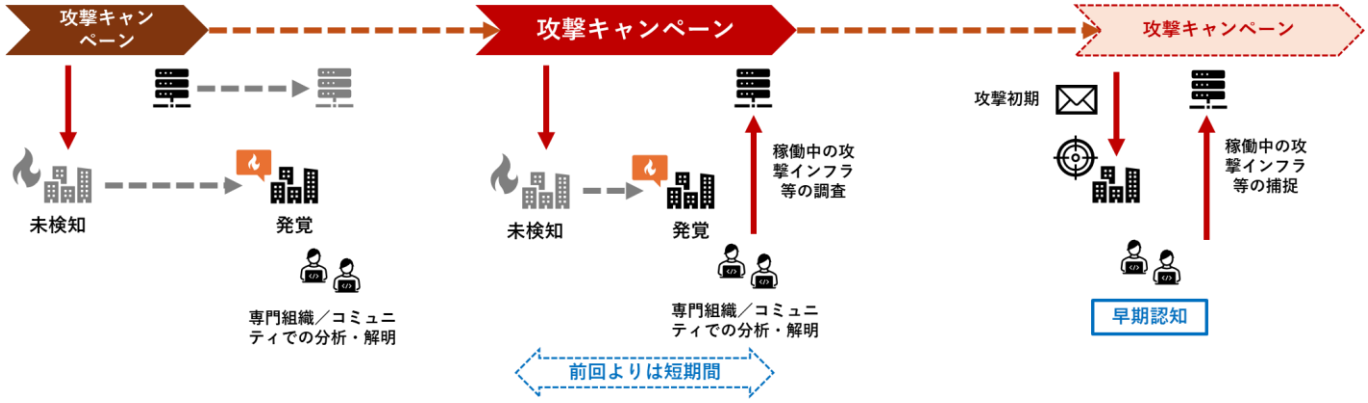
以上、米側の 2 つの対抗オペレーションを簡単に考察してみたが、他方で、有事と連動しない、平時からの情報窃取目的の APT キャンペーンにはどのような対抗オペレーションが考え得るのか、また違う観点から次節では考察してみたい。

4．攻撃インフラへの直接対処オペレーション：Trickbot と Volt Typhoon の事例

攻撃者側へのキャンペーン展開の能力を削ぐための直接的な「対処」としては、攻撃の実行者を逮捕することのほかに、攻撃インフラを使えなくさせること、攻撃者自身の操作環境をサイバー攻撃することが想定される。この中で現実的な解として、攻撃インフラへの対処が行われている。他方で、標的型サイバー攻撃は検知回避の戦術が多用され、また、ゼロデイ攻撃やサプライチェーン攻撃など、検知が困難な侵入経路を用いることもあるため、その攻撃を被害組織自身やセキュリティ専門組織が認知するまで相当の時間がかかってしまい、多くのケースでは、認知時点ではすでに攻撃キャンペーンは終了しており、攻撃インフラはすでに稼働しておらず、対処しようがないケースが大半である。

それでは、まったく対処のしようがないのかというとそういう単純な話ではない。先に述べた通り、攻撃キャンペーンは数か月～1 年以上の単位で行われ、また、これが数年～１０年あまりの間に何度も繰り返し行われるが、しかしながら、仮に最初の攻撃キャンペーンは完全に「見逃して」しまったとしても、この攻撃キャンペーンの分析を行うことで、次の攻撃キャンペーンはより速い段階で補足することができるかもしれない。そうなれば、稼働中の攻撃インフラを捕捉することができるようになり、攻撃インフラへの対処という直接的なオペレーションが実行可能となる。個別の事案、個別の攻撃キャンペーンだけに注目すれば、「早期に対処できた／できなかった」という議論にしかならないが、長期間にわたり断続的に行われる攻撃キャンペーンの束で捉えるならば、稼働中の攻撃インフラを捕捉し、対抗オペレーションを行える機会が得られるのである。

図 4：攻撃キャンペーンの繰り返しと被害認知・分析速度の改善



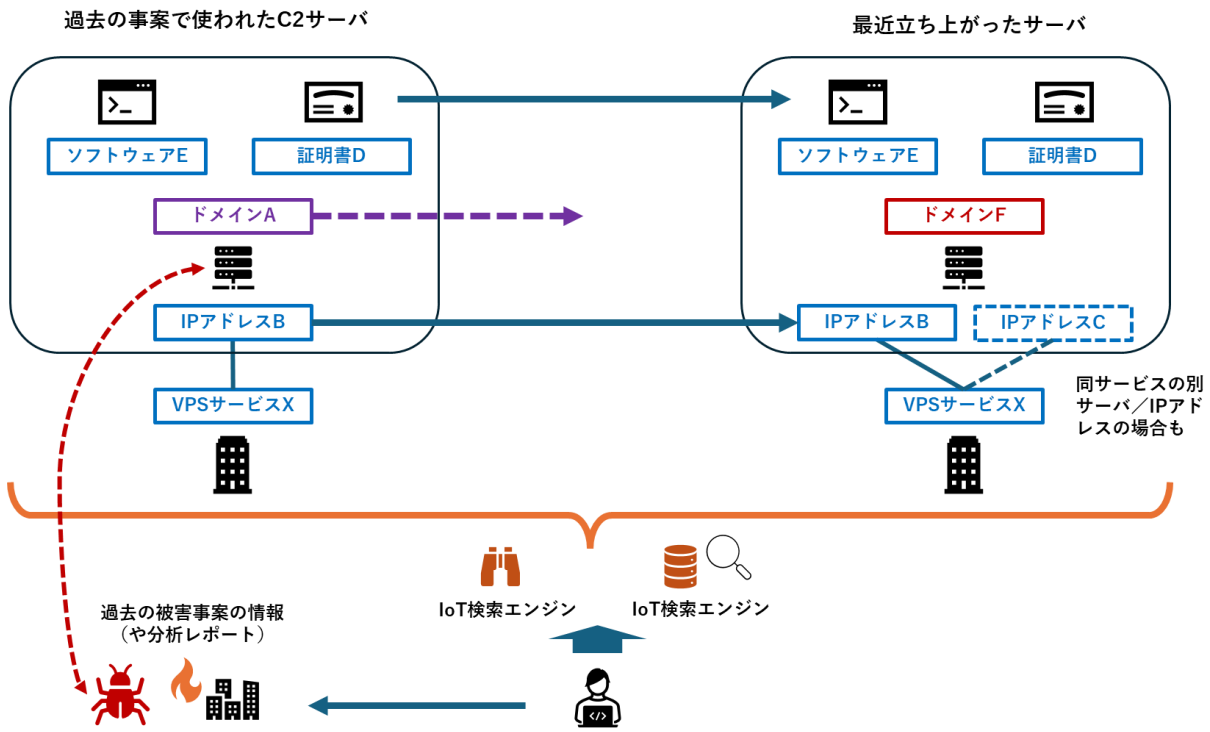
出典：各種公開情報から主著者作成

2020 年の米大統領選挙にあわせて、Trickbot のテイクダウンオペレーション[37]が行われたが、USCYBERCOM による作戦も行われたのではないかと指摘されている。Trickbot の攻撃インフラに対して何者かが攻撃を行い、一時的に攻撃インフラの一部が麻痺する事象が観測されているが、これが USCYBERCOM による作戦によるものではないかと指摘されたのである。米側から公式見解は出ていないものの、米大統領選挙期間中にランサムウェア攻撃や APT アクターの活動に Trickbot を使わせない、という目的を達成した作戦と評価することも可能である。Trickbot は 2016 年から稼働しており、攻撃活動を長期間追跡し攻撃インフラの構造を解明することができたために、こうした作戦が可能だったと考えることもできる。これに比べて、長くても数か月程度しか稼働しない APT キャンペーンの攻撃インフラを捕捉することは困難にも思える。

そこで、あらためて APT キャンペーン固有の攻撃インフラの特徴について整理してみたい。2010 年代には APT アクターの C2 インフラを事前に探す調査が頻繁に行われていた。攻撃者側はドメイン／FQDN は標的毎、攻撃キャンペーン毎に変更するものの、サーバ自体や IP アドレスは使い回したり、あるいは、ドメイン／FQDN は使い回すが、IP アドレスだけは変更したり、また、サーバ上で稼働させるソフトウェアや SSL 証明書を使い回すというように、攻撃インフラの構成要素について何かしらの「使い回し」を行う傾向が多かった。こうした外形上の特徴や変遷を長期間追跡することで、攻撃者の攻撃インフラ構築の傾向を把握することができ、同じ特徴を持つサーバが立ち上がった、攻撃キャンペーンの準備段階で攻撃インフラを捕捉することが可能だったのである。他方で、こうした手法を含め、攻撃者のアトリビューションが進むにつれて、攻撃者側も分析側のアトリビューション対策を取るようになり、最近で

はこうした使い回し等を避けるようになっている。

図 5：APT の攻撃キャンペーンにおける C2 サーバインフラ等の使い回し



出典：各種公開情報から主著者作成

ところで、攻撃者は C2 サーバなどの攻撃インフラを使い回すほど、攻撃活動を早期に捕捉されたり、被害拡大防止のための情報共有活動を有効にしてしまうのであるが、なぜ「使い回し」をするのであろうか。攻撃者側の動機／事情を正確に把握することは難しいが、ひとつには、攻撃インフラを大量に整備・運用するコストの問題があるのではないかと筆者は考えている。攻撃インフラは立ち上げて終わりということではなく、攻撃キャンペーン中にメンテナンスなどが必要であり、マルウェアの開発・改良、標的組織への侵入、潜伏、情報窃取などの様々な準備／オペレーションと並行して攻撃インフラを運用するには、割り当てられるリソースにも限りが出てくる。また、検出を回避するために、初期侵入に使う不正アクセス元、マルウェアの DL 元、遠隔操作するためのサーバと 1 つの攻撃で複数の C2 を用いることが一般的であるため、仮に使い回しを回避しようとすると、10 の組織を狙うために 10 の C2 サーバを用意すればいいのではなく、その数倍の C2 サーバを用意しなければならないのである。こうした事情から、C2 サーバをある程度使い回す運用が一般化したと推測されるのである 。

上記の通り、C2 使い回しによる捕捉・情報共有による無効化をさけるために、サイバー犯罪グループなどはボットネットを運用することが多い。本稿では紙幅の都合で詳細な解説は省略するが、ボットネットは数百台以上の感染端末やサーバを多層構造のネットワークで構築することによって、捕捉性を下

げたり、いくつかの C2 サーバがテイクダウンされても、全体として稼働可能にする冗長性が高められている。こうした複雑・巨大なネットワーク／システムを構築・運用するためには膨大なリソースが必要になるため、サイバー犯罪グループにはこうした巨大ボットネットの構築・運用だけを行うグループが存在しており、ボットネットを攻撃インフラとして他の犯罪グループに「貸し出す」ことで収益を上げている。犯罪グループも自前で構築できないため、運用グループから借りることで、ボットネットタイプの攻撃インフラの恩恵に預かっているのである。

一方で、APT アクターもボットネットを利用する場合がある。直近では Volt Typhoon が KV ボットネットというボットネットを攻撃インフラとして使っていることが判明している。このボットネットは正規の企業が使っている SOHO 向けルーターを数百台以上乗っ取って構成されており、使い回しを避けるためだけでなく、検知回避も狙っていたと思われる。KV ボットネットを追跡していた、アメリカの ISP 企業、Lumen 社のセキュリティチームによると、KV ボットネットは Volt Typhoon 以外の別のアクターも利用していたと思われ、運用・構築グループが別にいた可能性[38]をうかがわせる。

以上まで、使い回しの回避のために APT でもボットネットが使われる可能性／事例について解説したが、だからといって、2010 年代のような C 2 サーバの早期捕捉が困難になったということではない。Volt Typhoon が使っていた KV ボットネットも活動当初は把握できていなかったが、2023 年になり捕捉・解明され、2023 年 12 月には米当局が一部のテイクダウンを実施している。攻撃キャンペーン単独でみれば捕捉が難しい攻撃インフラも、複数の攻撃キャンペーンを経た、数年単位のスパンで見ると捕捉・対抗措置が可能なのである。特にボットインフラのような巨大な攻撃インフラを攻撃者が使う場合、この構築・運用にも相当のコストがかかっていることから、１つの攻撃キャンペーンだけで使い捨てしない可能性が想定される。よって、長い眼でみれば、結局、ボットネットいう攻撃インフラを「使い回して」しまっていると考えることができるのである。

5．コスト賦課アプローチ：攻撃キャンペーンの妨害と継戦能力の摩耗

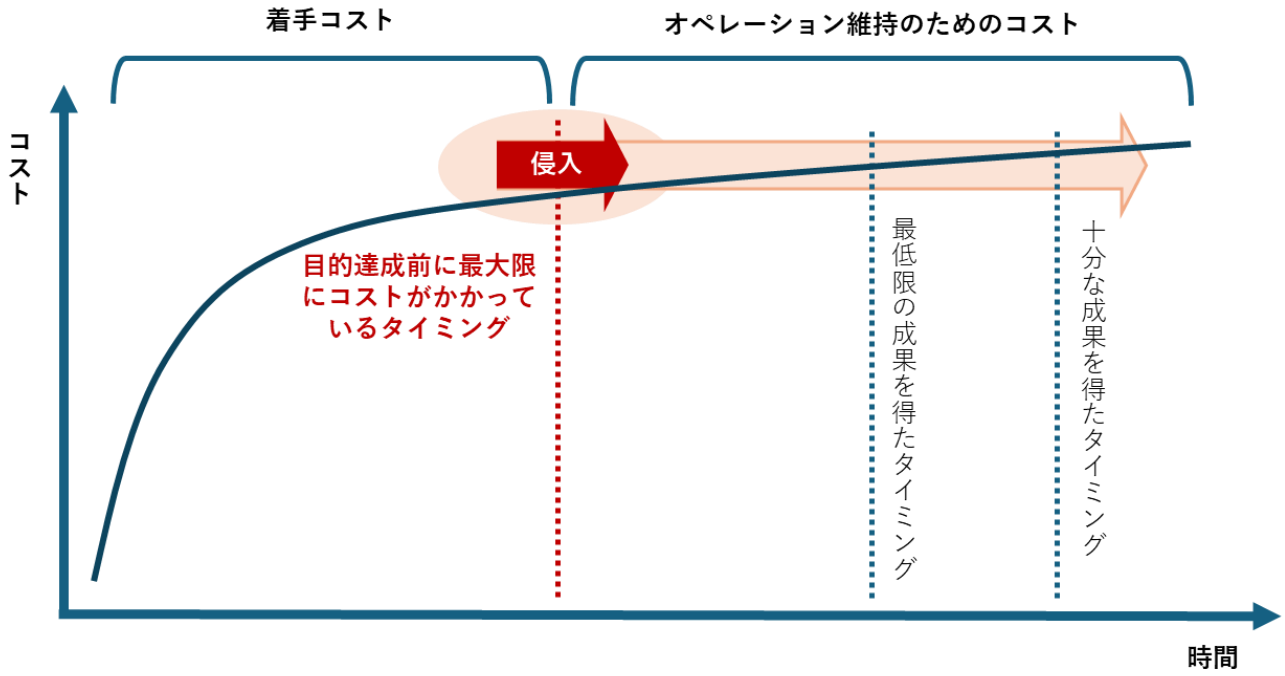
近年の米当局の対抗オペレーションの事例を踏まえつつ、改めて「持続的交戦ドクトリン」に象徴される、近年の米当局の「攻撃者への対処」の取組のキーワードの１つである「コスト賦課（cost-imposing）」（以下：「コスト賦課アプローチ[39]」）の含意を考察したい。

技術的な大前提として、サイバー攻撃の準備段階や侵害後の潜伏活動を捕捉することが難しい一方で、攻撃の初期段階、例えばスピアフィッシングメールの送付や特定製品の脆弱性を突くアクセスなどを認知できるケースがある。こうした攻撃初期の段階で情報共有や注意喚起が行われることで、攻撃の個別

の成功率がある程度下がることが想定される。

下記図は、以上の前提を踏まえて、攻撃者側のひとつの攻撃キャンペーン単位の「コスト」を図示[40]したものである。マルウェア開発、サーバの調達、運用人員の稼働など、時間の経過とともに、準備コストや運用コストが蓄積されていくわけだが、基本的には攻撃着手までの準備段階のコストがもっともかかると筆者は考える。この攻撃初期の段階、つまりまだ攻撃目標を達成していない時点で、上記のような注意喚起等で攻撃活動が露見し、攻撃キャンペーンが失敗した場合、ここまでに準備したコストがサンクコスト（埋没費用：sunk costs）となってしまうのである。

図 **6**：１つの攻撃キャンペーンにおける攻撃者側のコストと時間の経過のイメージ



出典：主著者作成

ここで強調しておくべきは、こうした「攻撃キャンペーン単位のコスト」に着目し、「攻撃者への対処」をめぐる理論を精緻化していく流れは、近年の学術研究でも見られ始めている点にある。代表的なものとして、近年のワーク（JD Work）[41]らによる「持続的交戦ドクトリン」の下での「（敵対者の）サイバー活動を妨げる対抗オペレーション（[Disruptive] Counter-Cyber Operations）」の機能をめぐる先行研究群がある[42]。これらの先行研究を敷衍すると、攻撃キャンペーンの妨害やサンクコストの累積が、攻撃者の活動に対して作用するプロセス（作用機序）については、主には次の 2 つのパターンが想定されている。

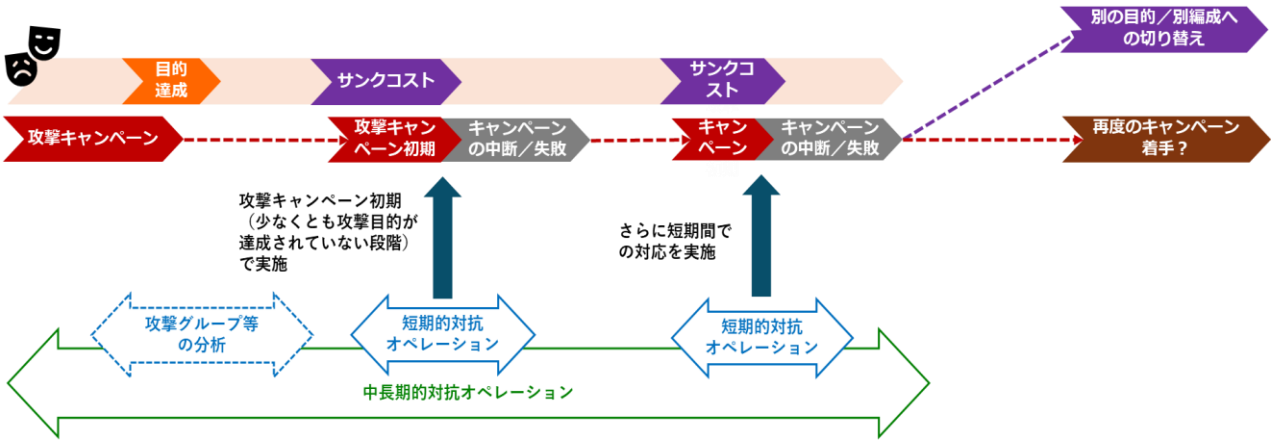
1 つは前述の通り、攻撃グループに対してキャンペーンに必要なツール・インフラの再調達等に必要な人員、資金、時間といった有形無形の資源の浪費を強いることで、攻撃キャンペーンの継戦能力を摩耗さ

せる機能を持つ。様々な形での継戦能力の摩耗は、攻撃グループによる将来的な攻撃キャンペーンでの OPSEC ミス等を誘発するリスク[43]を高める、あるいは資源制約下での攻撃キャンペーンの展開規模の制約を強いる効果を持ちうることになる。具体的には、例えば攻撃キャンペーン初期のフェーズで C2 サーバがテイクダウンされたり、妨害が行われたとしても攻撃キャンペーン全体が維持されるような冗長な攻撃インフラを用意したり、そもそも C2 サーバに逆侵入されないように様々なセキュリティ対策や運用強化を行うようになれば、攻撃キャンペーンを準備するためのコストと時間がかかるようになり、高頻度で攻撃キャンペーンを繰り返すことができなくなるかもしれない。

もう 1 つは、（組織/要員間の）「摩擦(friction)の創出」と呼称される機序である。一般的には国家の情報機関や軍事組織の隷下にあるとされる APT アクターは、実際にサイバー攻撃に携わる要員やキャンペーンの管理・統制を担う要員のほか、こうした APT アクターの攻撃キャンペーンの成果の利用者となる、様々な政策決定者や軍事作戦の立案に携わる幕僚が存在する。このとき度重なるキャンペーンの目標達成の失敗は、組織の指揮系統上に連なる上位者の視点からの能力への不信感を醸成する効果を持つ[44]。こうした組織の指揮系統の中での APT アクターの能力の確実性に対する疑義は、中長期的な攻撃キャンペーンの持続的運営や、その成果の利活用を妨げる作用をもたらし易い。

例えば一口に APT アクターといっても、政府当局側の攻撃者への指揮統制構造や民間企業への委託/指示などの程度は多様となる。政府当局と委託された攻撃者の関係性の如何では、ある程度の目的達成をできないアクターは指示主体／背景主体との関係で攻撃活動を停止させる可能性も想定されよう。特に政府当局から民間企業が委託／指示を受けて攻撃キャンペーンを展開しており、この実行者（民間企業）には「競合相手」がいる場合[45]、攻撃キャンペーンの成功率が低ければ、いずれは競合相手に仕事を「奪われる」可能性が考えられるのである。

図 **7**：対抗オペレーションによるサンクコストの累積と攻撃者側の行動変容の可能性



出典：主著者作成

前述の「懲罰的抑止アプローチ」と「コスト賦課アプローチ」は、外形上は共に相手方への「コスト」を賦課する要請の面では共通するが、両者の間では「コスト」の捉え方と作用機序の想定が異なる。従前の「懲罰的抑止アプローチ」では、アトリビューションによる実行犯の特定とは、自衛権行使を始めとした追加的なコストの源泉たる政策対応のための事態認定の要件であり、かつコストの賦課対象は、実行犯の背景にいる特定国の政府機関やその意思決定者を想定する。言い換えれば「懲罰的抑止アプローチ」は、ある攻撃の実行国の特定と反撃を念頭に置く耐え難いコストの行使の脅しを通じて、相手国の政治指導者等の費用対効果計算という「意思」を左右し、行動変容を目指すアプローチといえる[46]。

これとは対照的に、「持続的交戦ドクトリン」に象徴される「コスト賦課アプローチ」における「コスト」は、一義的には攻撃者のキャンペーンを支える継戦能力や攻撃グループに連なる指揮系統の中での円滑な意思決定のプロセスにダメージを与えることが含意されている。これは相手方の攻撃キャンペーンの単位に着目し、その最終的な戦略目標の達成を妨げる中長期的な対抗オペレーションの累積による「(継戦) 能力」の摩耗の継続・累積を重視する。つまり「能力」への対処を通じ、相手国の政治指導者等の「意思」の如何を問わず[47]、攻撃キャンペーンの目標達成を阻み続けることを目指す。

こうした「コスト賦課アプローチ」のもたらす中長期的含意については様々な論争が存在するが、これまでの学術研究の蓄積も踏まえた幾つかの演繹的な仮説としては、次のような点は指摘することができよう。第 1 に当然ながら、防御側の対応に適応し、攻撃者が攻撃キャンペーンを展開するためのツール・インフラの抗堪性を向上させることや、前述のように攻撃者が「交代」する例もある。この点、戦略目標を達成する断固たる決意と豊富な資源を有し、状況の変化に適応しうる余力を備えた国家やその支援を受けた APT アクターが、その攻撃キャンペーンを「永続的に停止」することは考え難いことは、今日までの米国の状況を見ても明らかであろう。

第 2 に、一方で「攻撃者への対処」と「被害者へのアプローチ」の両面を含みうる中長期的な対抗キャンペーンは、攻撃者側の継戦能力を削ぎつつ、同時に攻撃キャンペーンの展開のハードルを従前より引き上げる。現時点では仮説に留まるが、ここで攻撃者側の人材や時間といった「資源の有限性」と、攻撃国の意思決定者の「主観」からなる (サイバー攻撃の)「政策・軍事的手段としての信頼性」の問題を加味すると、次の機序を想定しうる。

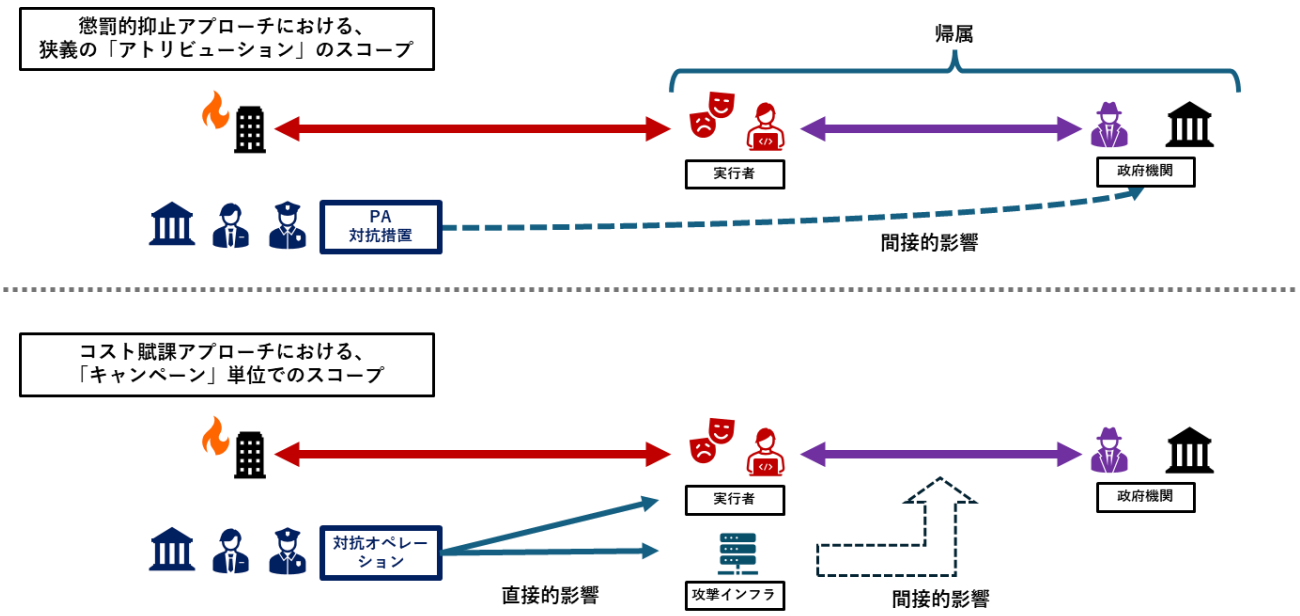
例えば、防御側による検知回避と継戦能力の維持に必要な攻撃ツール・インフラの抗堪化の工夫は、その要請に適応する追加的な時間・労力・費用を攻撃者側に強いるほか、特に Volt Typhoon のような「有事」への準備を念頭に置く攻撃キャンペーンの場合、有事のまさに「X デー」まで能力を温存する OPSEC 上の所要から、達成可能な目標や標的をある程度絞り込む必要も生ずる。こうした蓄積により特定国・地域での戦略目標達成のための攻撃キャンペーンの展開の障壁を高くし続けることで、それを乗り越えら

れる練度を備えた攻撃グループの母数や攻撃可能な標的の範囲を、特定国・地域全体で絞り込む（制限する）効果が期待できる[48]。

また前述の「（組織/要員間の）摩擦の創出」の観点からは、攻撃キャンペーンによる目標達成までの費用・所要時間の増大や目に見える失敗率の上昇は、敵対国の意思決定者の「主観」としてのサイバー攻撃（能力）の政策手段/軍事的手段としての価値への疑念も創出しうる[49]。（実態の有無を問わず）意思決定者の「主観」として、有形無形の投資の割に成果が伴わない、あるいは「有事」の軍事的手段としては機能の不確実性が高過ぎる場合、各国の安保政策・軍事作戦の全体の中での「サイバー攻撃」の比重を限定し、（意思決定者の主観上）より確実性の高い、例えば通常戦力での軍事的オプションに依拠[50]するように促す[51]。この作用は、サイバー攻撃による非対称かつ低コストでの目標達成を許さず、より捕捉・対策され易く攻撃側が反撃されるコスト/リスクも高い物理的な軍事的行動を攻撃者に強いる[52]。また能力の摩耗と不確実性の増大は、武力紛争の初期段階で有用性の高い「サイバー攻撃」と、「通常戦力での軍事作戦」の連動を狂わせ、攻撃者側の事前の作戦計画の円滑な遂行を妨害/遅滞する効果も持ちうる[53]。

最後に、一連の機序の（サイバー攻撃への）「抑止（戦略）」への含意に触れたい。一連の想定機序は、冷戦期の抑止理論での敵対者への対兵力打撃やミサイル防衛等からなる「損害限定(damage-limitation)[54]」あるいは（相手方の能力への）「拒否戦略（denial strategy）[55]」に近い。一連の取組が結果的に「拒否的抑止（deterrence by denial)」に貢献するかの検討は本稿の紙幅を超えるが、このように「コスト賦課アプローチ」を捉えれば、従来各国が掲げてきた「抑止（戦略)」のナラティブとも矛盾しないといえる[56]。

図８：「懲罰的抑止アプローチ」と「コスト賦課アプローチ」のターゲットの違い



出典：主著者作成

6．結論：「国家の総力によるコスト賦課」を糾合する「ドクトリン」の必要性

本稿は「（攻撃）キャンペーン」の概念を整理した後、これまでの米国当局による「（サイバー）攻撃者への対処」の思想の変遷や具体的なオペレーションの事例を紐解きつつ、2018 年以降の USCYBERCOM の「持続的交戦ドクトリン」に象徴される、攻撃者を中心としたキャンペーンの展開能力に働きかける「コスト賦課アプローチ」の理論的整理を行った。

攻撃者も被害者も、双方が「キャンペーン」を継続するとの世界観に立脚する「コスト賦課アプローチ」は、伝統的な軍事の世界での「消耗戦(a war of attrition)[57]」に近い。より平たくいえば、「懲罰的抑止アプローチ」が「短距離走」とすれば、「コスト賦課アプローチ」は「マラソン」といえる[58]。2010 年代後半に米国で生じた、いわば競争のルールをめぐる解釈の転換を、「サイバー攻撃側に決定的な打撃を与えられない妥協策であり、結果的に消耗戦という現実を強いられた」と否定的に捉えることもできるが、他方で「競争のルールの理解により、初めて攻撃者側との対等な競争を行いうる」とも考えられる。

例えば、2014 年に公的機関としては初めてパブリックアトリビューションを行った米司法省/米国連邦捜査局（FBI）の高官は、2010 年代後半に入ると刑事訴追の公表が所謂「名指しによる非難」が目的であるとの俗説を否定したうえで、財務省による経済制裁指定や、同盟国・同志国と連携した攻撃グループのインフラ等への共同対処を含め、米国政府全体としての様々な攻撃者への対処によるコスト賦課アプローチを誘発する選択肢の 1 つであるとの説明を行っている[59]。この説明が象徴するのは、米司法省/FBI が、パブリックアトリビューションの効果を攻撃者への非難がコストになるとの想定に矮小化せず、むしろキャンペーンの公表に続く米国全体としてのサイバー攻撃者への対処でのコスト賦課アプローチを前提に、その触媒として司法省／FBI が持つオプションとしての刑事訴追の公表を位置付けている点にある[60]。

本稿で触れた USCYBERCOM の「持続的交戦ドクトリン」は、2018 年のトランプ（Donald J. Trump）政権下の国防省で成立したものだが、「攻撃者への対処」による「コスト賦課アプローチ」の思想は、前段で触れた近年の司法省/FBI のサイバーセキュリティ関連施策[61]はもとより、例えば今般のバイデン（Joseph R. Biden Jr.）政権下での『国家サイバーセキュリティ戦略』や『国防省サイバー戦略（要約版）』にも継承され、政権の党派性を超えた米当局全体の「ドクトリン」となりつつあるし、そこでは米当局の能力を触媒とした官民連携によるコスト賦課の取組の強化も強調されている[62]。これは見方を変えると、財務省の経済制裁指定や USCYBERCOM による攻撃者のインフラのテイクダウンから選挙干渉対策のための脅威情報共有の拡充まで、官民連携も含めて国家の総力を挙げて「攻撃者への対処」の取組の拡充を行う要請があり、多様なステークホルダーを糾合する理論的支柱として、本稿が解説した攻撃「キャンペーン」に着目した「コスト賦課アプローチ」が機能したということであろう。

2022 年 12 月の『国家安全保障戦略』を筆頭とする戦略 3 文書の刊行以降、今日まで続く日本政府でのサイバー安全保障体制の強化の検討を経て、今後我が国でも「攻撃者への対処」のための様々なオプションの具体化に向けた政策的議論の加速が見込まれる。それらの検討に対して本稿の議論が持つ含意とは、個々の対処措置に注視するのではなく、官民の様々な組織が持つオプションを有機的に組み合わせ、中長期的に攻撃者側と競争可能な、理論的な支柱を備えた「ドクトリン」が必要となることにあろう。

補論：「攻撃者のプロファイリング」と「防御側のコスト軽減」の問題

本稿では攻撃「キャンペーン」に注目し、主に「攻撃者への対処」をめぐる米国当局の思想をめぐる先行研究や具体的な事例を基に、「コスト賦課アプローチ」の考察を行った。こうした本稿の分析の射程からは外れるため、以上 6 節の「本論」では含み得なかったが、「コスト賦課アプローチ」を議論する上で欠かせない 2 つの関連論点について、以下では「補論」という形で触れて行きたい。

第 1 に、「コスト賦課アプローチ」の時代における「アトリビューション」の意義の再検討である。「本論」の第 5 節でも若干触れたように、攻撃者の「コスト」は、攻撃キャンペーンの背景に、様々な人間と組織が関与する重層的なネットワークが存在することが前提にある。同時に、こうした攻撃キャンペーンのための人的・組織的なネットワークや攻撃のパターンの特徴は、特に国家を背景とした APT アクターであれば、各国の固有の戦略目標や地政学的な文脈・国内の政治経済社会要因に応じても異なる。それゆえに、様々な攻撃グループの抱える固有の特徴や弱点のプロファイリングが、対抗オペレーションでも必須となる[63]。本稿では、2010 年代の（パブリック）アトリビューションに重きを置いた抑止アプローチの限界を取り上げたが、その一方で 10 年近い官民間でのアトリビューションの蓄積が、APT アクターの活動原理を徐々に明らかにし、プロファイリングの基本となる分析方法／証拠の収集方法を編み出すことに貢献してきたことは間違いない。今後は、そうしたアトリビューションの方法論を「攻撃者側のコストの算定」のための手段としてどのように用いるかという視点も求められよう。

第 2 の、より本質的な論点は、「消耗戦」ないし「マラソン」を勝ち抜く上で、「防御側のコスト」をどのように軽減していくのかという問題である。先述の通り、「サイバー攻撃側に決定的な打撃を与えられないから、妥協策として、かつ、消耗戦的に戦うことになっただけなのでは」と否定的に考えるのか、「このようなパラダイムの採用によって初めて、攻撃者側との競争が可能になる」と考えるか、見方が大きく異なるだろう。しかし、いずれの見方にしても、我々防御側も累積的なコストを負う現実からは逃れられない。攻撃者との長きにわたる「消耗戦」を前提としても、そこで我々は相手方への優位を維持する必要があり、相手方に不利な消耗を強いつつも自身の消耗を減らす「持久戦」の思想が求められる。

現行の国内体制・制度では、攻撃被害の事後対応に重きを置いた、リスク行政的な体制・制度が組まれている。サイバー攻撃を起因とする個人情報漏えいや重要インフラサービス障害が発生した事案について国への報告を行わせ、再発防止を行政機関側が直接／間接的に監督していく仕組みである。こうした現状の国内体制／制度は基本的に被害のインパクトに応じた行政機関の対応基準／法令として整備されている。インパクトが大きいということは自ずと、大量の個人情報の保有、重要インフラサービスの運用というように、企業規模が大きな組織が対象となることが確率的に多くなるわけであり、社会的な関心の高さもあいまって、報道で取り上げられやすくもなれば、報道をトリガーとして国側も官房長官／大臣会見対応を行ったり、国会でも取り上げられやすい、というように「個別事案へのフォーカス」が再生産されやすい構造になっている。

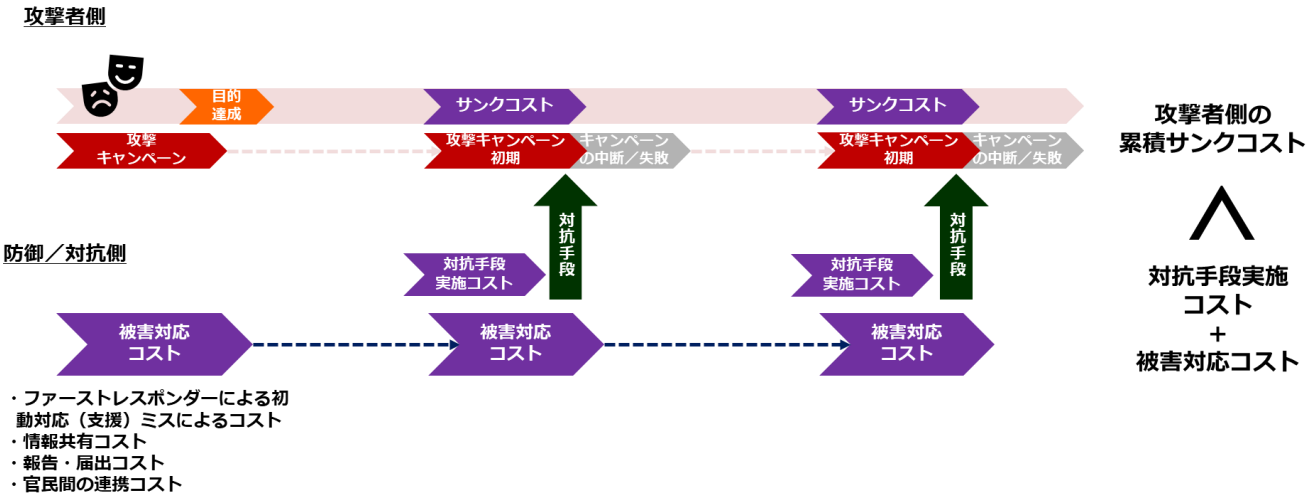
サイバー攻撃被害組織は「叩かれやすい」と言われる。その背景として、上記の通り、国内の報告制度・行政として事案をキャッチアップするベースが、「被害により社会的に与えたインパクトの大きさ」基準であるため、必然的に、「被害公表・報告を行う組織≒顧客や社会に影響を与えて“しまった”組織」となってしまうからである。また、繰り返しの説明になるが、国内の行政機関の体制も、リスク行政として、「事故を起こした企業への指導」がベースとなっており、攻撃者側に向かわず、被害組織にその活動・関心のベクトルが極めて向きやすくなってしまっているのである。被害組織にとっては、原因の技術的調査だけでなく、被害公表、顧客・ステークホルダーへの通知・連絡、報道対応、複数の行政機関への報告等の対応と、膨大な対応コストと出費を負担することとなる。

個別事案へのフォーカスが強く、また、個別企業の責任を問う事後対応が強い以上、被害組織は組織外に（いかなる情報であれ）情報を出すことに強い抵抗感を感じざるを得ない。上記の通り、技術的情報の情報共有以外の対外対応に多くのリソースを割かなければならない現状ではなおさらである。現状の国内の攻撃対応体制下では、被害現場で見つかる脅威情報（攻撃痕跡、攻撃手法、攻撃動向に関する情報など）の流通にあまりにも摩擦とコストがかかりすぎている [64] が、その背景は以上のような問題点があるからである。また、ひとたび特定の業界／業種にスポットライトがあたれば、「対策の強化」ということで、所管省庁や警察などの行政機関のアプローチが集中し、情報の流通が極めて悪くなってしまうのである。

現状の「個別被害にフォーカス」してしまう対応体制／構造がそのままであれば、「次の攻撃キャンペーン」のための分析・追跡に必要な脅威情報が流通しづらいままとなり、いつまでも攻撃活動の「後追い」のままとなってしまうのである。確かに、1 件 1 件の攻撃被害の影響を軽んじることはできないが、他方で、現状の制度に基づいた個別最適を行い、個々の案件をミクロな視点で取り上げれば取り上げるほど、

防御側の内部調整コストがかかりすぎ、キャンペーン観点での対抗オペレーションという全体最適は成立しない。法制度上も、そして概念上も「被害」のあり方を根本的に変え、被害組織だけでなく、行政機関、専門機関、専門企業間の情報流通コストを大幅に下げなければ、攻撃キャンペーンに注目したコスト賦課アプローチを用いて、攻撃者と競争をしていくことは到底不可能なのである。

図９：攻撃者側のサンクコストの累積と防御／対抗側の対応コストの累積



出典：主著者作成

（本文以上）

（２０２４年８月５日脱稿）

[1] 2024 年 5 月より防衛研究所特任研究員（非常勤）。本務先はサイバー攻撃対処の専門機関である、（一社）JPCERT コーディネーションセンターにて脅威アナリストをしており、注意喚起等の情報発信やインシデント対応支援、脅威情報の共有活動に従事している。

[2] 本稿の主題ではないが、ここ数年で被害が拡大しているランサムウェア攻撃においては、暗号化による直接的なダメージのほか、個人情報漏えいに伴う行政指導・課徴金や被害公表や攻撃者側のリーク・報道等によるレピュテーションダメージを攻撃者側が被害組織を脅迫する「材料」として用いている現状もある。

[3] 佐々木 勇人「サイバー 脅威インテリジェンス活用のための「ドクトリン」の必要性について―情報共有を巡る「市場の失敗」と「政府の失敗」を乗り越えるために」『NIDS コメンタリー』 第 319 号、2024 年 5 月、https://www.nids.mod.go.jp/publication/commentary/pdf/commentary319.pdf、13 頁。

[4] 石川 朝久『脅威インテリジェンスの教科書』（技術評論社、2022 年）52 頁。

[5] サイバーセキュリティ業界での「キャンペーン」の捉え方は、特に APT を中心とした攻撃グループのアトリビューションの実務の要請からも生じてきた。このような文脈でのキャンペーンの含意については、次も参照。Timo Steffens, *Attribution of Advanced Persistent Threats - How to Identify the Actors Behind Cyber-Espionage*（Wiesbaden: Springer Vieweg, 2020), pp. 26-32.

[6] 本定義は北大西洋条約機構（NATO）のドクトリンを反映した英国の統合ドクトリンを参照。Ministry of Defence, *Joint Doctrine Publication 0-01 UK Defence Doctrine*, Six edition, November 2022, https://assets.publishing.service.gov.uk/media/63776f4de90e0728553b568b/UK_Defence_Doctrine_Ed6.pdf.

[7] Emotet は 2019 年から特に活動を活発化・大規模化させ、2023 年まで断続的に広範囲な感染拡大活動を繰り返した。Emotet のオペレータは、多くの端末を感染させ、これを他の犯罪者に転売することで収益を上げているため、より多くの端末／組織に感染させるために、ある程度攻撃の有効性が下がり感染拡大が収束すると、Emotet や感染方法を修正し、再び、感染拡大の攻撃活動を再開する、というサイクルを繰り返した。

[8] 直近では、Volt Typhoon の攻撃キャンペーンが注視されている。一般社団法人 JPCERT コーディネーションセンター（JPCERT/CC） 「Operation Blotless 攻撃キャンペーンに関する注意喚起」 2024 年 6 月 25 日、https://www.jpcert.or.jp/at/2024/at240013.html.

[9] Lumen’s Black Lotus Labs, “Routers Roasting on an Open Firewall: the KV-botnet Investigation,” December 13, 2023, https://blog.lumen.com/routers-roasting-on-an-open-firewall-the-kv-botnet-investigation/.

[10] U.S. Department of Justice, “U.S. Government Disrupts Botnet People’s Republic of China Used to Conceal Hacking of Critical Infrastructure,” January 31, 2024, https://www.justice.gov/opa/pr/us-government-disrupts-botnet-peoples-republic-china-used-conceal-hacking-critical.

[11] 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/pressconf_2021/04_22.htm.

[12] こうした議論は例えば以下の資料を参照。郡 義弘「『能動的サイバー防御』を考える、この言葉の指すところは何なのか？」NEC セキュリティブログ、2023 年 2 月 10 日、https://jpn.nec.com/cybersecurity/blog/230210/index.html.

[13] 「持続的交戦」および「前方防衛」の概念の米国の国防専門家コミュニティにおける歴史的な形成過程は、例えば以下の文献を参照。Joe Devanny, "'Madman Theory' or 'Persistent Engagement'? The Coherence of US Cyber Strategy under Trump," *Journal of Applied Security Research*, vol.17, no.3. (February 2021), pp. 282–309, https://doi.org/10.1080/19361610.2021.1872359.

[14] Mandiant, APT1: Exposing One of China's Cyber Espionage Units, February 19, 2013, https://www.mandiant.com/sites/default/files/2021-09/mandiant-apt1-report.pdf.

[15] The U.S. Department of Justice, "U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage," May 19, 2014, https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor.

[16] ただし近年の学術研究によれば、米国政府をはじめとした各国政府主導の（パブリック）アトリビューションの政策は、2010 年代におけるサイバーセキュリティ政策のパラダイムの変容と軌を一にしながら目的と形態の変遷（多様化）を続けてきた。こうした政府によるアトリビューションの取組の変遷史は、次を参照。瀬戸 崇志「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 ―」『安全保障戦略研究』第 3 巻 2 号（2023 年 3 月），https://www.nids.mod.go.jp/publication/security/pdf/2023/202303_04.pdf.

[17] 特に 2010 年代後半に入るまでは、パブリックアトリビューションは「名指しによる非難（name and shame)」とも呼ばれる結果の公表と非難の過程を通じて、相手方の費用対効果計算を変化させるものと捉えられてきた。こうした内在論理と、これに対する批判は次を参照。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. 971–977.

[18] 特に 2010 年代前半までのサイバー抑止の議論での「懲罰的抑止」モデルの中心性と、その中での「アトリビューション」の機能の位置付けは、同時代の専門家により執筆された以下の文献群に詳しい。栗田 真広「サイバー攻撃に対する「抑止」の現状―米国の安全保障政策の事例から―」『情報通信をめぐる諸課題（科学技術に関する調査プロジェクト 調査報告書)』（国立国会図書館調査及び立法考査局、2015 年）157-180 頁、https://ndlsearch.ndl.go.jp/books/R100000039-I9104304.；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、https://koara.lib.keio.ac.jp/xoonips/modules/xoonips/detail.php?koara_id=0402-1502-0078.

[19] 例えば、次の記事を参照。 「専門家風の用語の落とし穴『アトリビューション』」株式会社 IT リサーチ・アート、2018 年 7 月 8 日、https://itresearchart.biz/?p=1273.

[20] 具体的には、物理的な実行者の特定や実世界での背後関係の特定まで行わず、「APT〇〇」「×××PANDA」といったような、グループ区分・グループ定義や、他組織がすでに区分している既知のグループとの関連性／同一性を特定するところまでが専ら行われる。ただし、この過程においては、必ずしもバーチャルな攻撃グループ間の照合だけでなく、米司法省等が公表した、具体的な個人・国家機関の関与まで行われたアトリビューション結果との照合も行われることもあり、また、その逆（捜査当局が、民間専門機関が行ったバーチャルな攻撃グループ特定結果の参照を行うこと）も行われている。

[21] こうした「アトリビューション」が示す範囲／粒度のギャップの整理は次を参照。佐々木勇人「脅威情報共有・活用を巡る現場の課題」防衛研究所 サイバー脅威インテリジェンス（CTI）をめぐる内外動向と産官学連携研究会発表資料、19-20 頁、https://www.nids.mod.go.jp/about_us/topic/pdf/240301_1_02.pdf.; Steffens, Attribution, pp.39-40, pp. 165-166.

[22] この点については、次を参照。瀬戸「パブリックアトリビューション」65-68 頁。

[23] 例えば①国際社会からの非難声明による外交的孤立を狙った「名指しによる非難（name and shame）」と捉えるか、または②実行犯の刑事訴追や関連法人への制裁措置、究極的には自衛権行使等を含めた、非難を超える烈度の高いオプションが必要かといった点の意見は分かれる。この点は次を参照。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、5 頁、https://www.nids.mod.go.jp/publication/commentary/pdf/commentary179.pdf.

[24] こうしたデータは元より、少なくとも 2018 年以降の時間軸では、当の米国の司法省/連邦捜査局（FBI）も、刑事訴追の公表の目的が「名指しによる非難」にあることを明確に否認している点を付言する必要があろう。この点は次を参照。瀬戸「パブリックアトリビューション」　75 頁

[25] なお本稿は「持続的交戦」概念と、後に米国防省の用語法として登場する「前方防衛（Defend Forward）」概念を、実質的に互換可能なものと捉えたうえで、前者の語感が、2018 年以降の米国による「攻撃者への対処」の哲学をより忠実に体現するものとして、あえて前者の用語を用いる。両者の関係性は次を参照。USCYBERCOM PAO, “CYBER 101 - Defend Forward and Persistent Engagement,” USCYBERCOM, October 2022, https://www.cybercom.mil/Media/News/Article/3198878/cyber-101-defend-forward-and-persistent-engagement/.

[26] 次を参照。United States Cyber Command（USCYBERCOM）, *Achieve and Maintain Cyberspace Superiority : Command Vision for US Cyber Command* (hereafter *Command Vision*), March 2018, https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf?ver=2018-06-14-152556-010.

[27] 代表的なものとして、2018 年に刊行された『米国防省サイバー戦略（要約版）』がこれにあたる。次を参照。 Department of Defense (DOD), *Summary: Department of Defense Cyber Strategy 2018* (hereafter *DOD Cyber Strategy 2018*), September 2018, https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF.

[28] 代表的なものとして、次を参照。Michael P. Fischerkeller, Emily O. Goldman, Richard J. Harknett, *Cyber Persistence Theory: Redefining National Security in Cyberspace*, （New York: Oxford University Press）May 2022.

[29] USCYBERCOM, *Command Vision*, pp.2-3.; DOD, DOD Cyber Strategy 2018, pp.2-4.

[30] 武力紛争の敷居以下で続く攻撃キャンペーンの累積的な戦略的含意の問題と対処の必要性の議論は、次を参照。Robert Chesney and Max Smeets eds, Deter, Disrupt, or Deceive Assessing Cyber Conflict as an Intelligence Contest, pp.109-133; DOD, *DOD Cyber Strategy 2018*, pp. 2-4,; Michael P. Fischerkeller, Emily O. Goldman, and Richard J. Harknett, *Cyber Persistence Theory*, pp. 58-85.; Richard J. Harknett and Max Smeets, “Cyber Campaigns and Strategic Outcomes,” Journal of Strategic Studies, vol. 45, no.4 (March 2020), pp. 534–567, https://doi.org/10.1080/01402390.2020.1732354.

[31] 例えば次項で紹介する Hunt Forward 作戦（Hunt Forward Operations）のような、USCYBERCOM と同盟・同志国当局との共同でのスレッド・ハンティングや脅威インテリジェンスの共有活動は防御的な性質である一方、2020 年米大統領選の際に行ったとされる Trickbot の攻撃インフラへの対抗オペレーションは攻撃的なものである

[32] この運用思想は、例えば近年の USCYBERCOM 司令官の戦力態勢概況説明（posture statement）や後述する Hunt Forward 作戦の公式説明のなかに色濃く表れている。次を参照。USCYBERCOM, "2023 Posture Statement of General Paul M. Nakasone," March 7, 2023, https://www.cybercom.mil/Media/News/Article/3320195/2023-posture-statement-of-general-paul-m-nakasone/. ; USCYBERCOM PAO, "Cyber 101: Hunt Forward Operations," USCYBERCOM, November 2022, archived at the National Security Archive, https://nsarchive.gwu.edu/sites/default/files/documents/semon9-giki0/2022-11-15-USCYBERCOM-Cyber-101-Hunt-Forward-Operations-960th-Cyberspace-Wing.pdf.

[33] 平素からの国家間競争とキャンペーンの永続を前提に、敵対国の戦略目標達成の妨害/遅滞(disrupt[ion])とコスト賦課（cost-imposition）を通じ、自国のリスクを管理可能なものとする発想は、近年では米軍によるサイバー作戦の役割のほか、特殊作戦部隊（SOF）の戦略的機能をめぐる議論のなかでも観測される。例えば SOF による「戦略的妨害（strategic disruption)」のコンセプトは、次を参照。Eric Robinson et al, *Strategic Disruption by Special Operations Forces: A Concept for Proactive Campaigning Short of Traditional War* （Santa Monica: RAND Corporation）, December 2023, https://www.rand.org/pubs/research_reports/RRA1794-1.html.

[34] Microsoft, *Defending Ukraine: Early Lessons from the Cyber War*, June 2022, https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE50KOK.

[35] ESET Research, "A Year of Wiper Attacks in Ukraine," ESET, https://www.welivesecurity.com/2023/02/24/year-wiper-attacks-ukraine/.

[36] Dina Temple-Raston and Sean Powers, "Exclusive: How a Defend-forward Operation gave Ukraine's SBU an Edge over Russia," *Recorded Future*, October 20, 2023, https://therecord.media/illia-vitiuk-interview-ukraine-sbu-defend-forward.

[37] Krebs on Security, "Report: U.S. Cyber Command Behind Trickbot Tricks", October 10, 2020, https://krebsonsecurity.com/2020/10/report-u-s-cyber-command-behind-trickbot-tricks/.

[38] Lumen's Black Lotus Labs, "Routers Roasting on an Open Firewall: the KV-botnet Investigation", December 13, 2023, https://blog.lumen.com/routers-roasting-on-an-open-firewall-the-kv-botnet-investigation/.

[39] 米国の防衛・安全保障当局者や専門家が用いる"cost-imposing"との標語は、その語源を辿れば米国による冷戦期来の有事に至らないレベルでの国家間競争の指針である「コスト強要戦略（またはコスト賦課戦略：Cost-imposing strategies)」に辿り着くと見られる。ただし同概念は必ずしも明文化された文書の形式を取らず、米国政府当局の様々な文書・施策に内面化された指針・理念の総称であるため、本稿では読者の混乱を避ける観点で、「コスト賦課アプローチ」との表現を用いる。米国における「コスト強要戦略」の概念については、次を参照。葛西 浩司『コスト強要戦略』の現代的意義―平時の戦いを考える視座」『海幹校戦略研究』 第 10 巻第 1 号（通巻第 20 号） （2020 年 7 月)、20-39 頁、https://www.mod.go.jp/msdf/navcol/assets/pdf/ssg2020_07_03.pdf.

[40] 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～」JSAC2023 発表資料、JPCERT/CC、https://jsac.jpcert.or.jp/archive/2023/pdf/JSAC2023_2_2_sasaki_jp.pdf.

[41] ワークは、米国防大学情報・サイバースペースカレッジ（CIC）教授。脅威インテリジェンス、サイバー作戦等に関する研究を行う。セキュリティ企業や米政府などで 20 年以上のキャリアを経て、米国防大学のほか、コロンビア大、海兵隊大学、シンクタンク等での研究活動も行っている。

[42] 以下の議論は、特に断りなき場合は次の文献群を参照して構成されている。JD Work, “Cumulative Outcomes of Counter-Cyber Operations Campaigns: Contributions to Integrated Deterrence,” in *Integrated Deterrence and Cyberspace: Selected Essays of Exploring the Role of Cyber Operations in the Pursuit of National Interest*, Joseph L. Bilingsley eds (Washington D.C.: National Defense University Press), pp. 55-112, https://ndupress.ndu.edu/Portals/68/Documents/strat-monograph/Integrated-Deterrence-and-Cyberspace.pdf. ; 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, https://ccdcoe.org/uploads/2020/05/CyCon_2020_14_Healey_Jenkins_Work.pdf.

[43] 本稿の主題ではないので省略するが、これまでに APT グループが特定されたケース（セキュリティベンダによるものから刑事訴追まで）の多くでは、攻撃者側の OPSEC ミスを端緒として、様々な証拠が明らかになったものが多い。攻撃者キャンペーンの継戦能力の摩耗というアプローチはアトリビューションを更に容易とする付随効果が期待できるかもしれない。

[44] こうした機序は、伝統的な防諜(counterintelligence）の論理に近い。次の文献群も参照。JD Work, “Successful Counter-cyber Operations Secure US Election,” *Janes Intelligence Review,* January 28, 2021, p. 6; https://www.janes.com/osint-insights/defence-news/successful-counter-cyber-operations-secure-us-election；瀬戸 崇志 「ロシアのウクライナ侵攻と米英両国のインテリジェンス公表政策―情報機関の『ジレンマ』と 2014 年以降の安全保障協力の『系譜』」『NIDS コメンタリー』第 224 号 2022 年 5 月、7 頁、http://www.nids.mod.go.jp/publication/commentary/pdf/commentary224.pdf.

[45] 本稿では触れられないが、特に中国当局の関与が指摘される APT アクターのいくつかについては、実行者自体は民間企業であり、情報機関等から指示を受けて攻撃活動を行っていたことが指摘されている。（2018 年 APT10 刑事訴追、2020 年 APT41 刑事訴追ほか）また、直近では中国のセキュリティ企業（I-soon 社）から漏洩したとされる内部情報が GitHub 上にリークされ、当該情報からは、同社が APT キャンペーンに関与している可能性が明らかになっている。

[46] このような論理構造は、前掲注 18 の栗田・川口の論文を参照。

[47] 「持続的交戦ドクトリン」の理論的基礎を提供した研究者達が、その論理構成においてサイバー空間でのキャンペーンによる「既成事実化戦略(fait accompli)」のアナロジーを強調する背景の 1 つは、上述の懲罰的抑止を含む「強制（coercion)」の理論体系が、（脅し等による相手方の「意思」を介した（自発的な）行動変容が前提であるのに対し、（抑止の失敗の一類型たる）「既成事実化戦略」は、相手方の意思を介せず、行動者が目標を達成する機序を念頭に置いているからである。この点については次を参照。Fischerkeller, Goldman, and Harknett, Cyber Persistence Theory, May 2022, pp. 10-36.

[48] また、仮にある国家が、そのハードルを越えるために、知見・経験豊富な人材を結集した攻撃グループを再編して運用する場合、ある時点の攻撃者の人材プールが有限とすれば、グループの編制に伴う人材の再配分を通じて、他の攻撃グループの活動に影響を与える可能性もある。

[49] この点は次を参照。Work, “Cumulative Outcomes of Counter-Cyber Operations,” pp. 69-70.

[50] 例えばスミーツ（Max Smeets）による、米国主導の軍事作戦のなかで「サイバー攻撃の選択肢が（検討されたにもかかわらず）選択されなかった」事例の意思決定過程に光を当てた先行研究では、1990 年代の湾岸戦争、2000 年代のイラク戦争、2010 年代のリビアへの多国籍軍の介入といった事例で、サイバー攻撃による軍事的目標の達成の成功率や付随的損害のリスクをめぐる意思決定者や作戦の立案者達の主観的な不確実性が高い状況下で、同様の軍事的効果（effects）を達成するためにより確実な通常戦力の行使が選好されたパターンが示唆されている。次を参照。Max Smeets, “A US History of not Conducting Cyber Attacks,” *Bulletin of the Atomic Scientists*, vol. 78, no. 4, pp. 208-213, https://doi.org/10.1080/00963402.2022.2087380.

[51] Work, “Cumulative Outcomes of Counter-Cyber Operations,” pp. 69-70.

[52] Ibid., pp. 74-75.

[53] Ibid., p. 88, pp.92-93.

[54] この用語は、元来は核抑止/核戦略における 1 つのアプローチの潮流を示す概念であり、その詳細は次を参照。本山 功「コラム①：核戦略の論理をめぐる二潮流」 一政 祐行 編『核時代の新たな地平』（防衛研究所、2024 年 3 月）、60-74 頁、https://www.nids.mod.go.jp/publication/perspective/pdf/j2024/jColumn1.pdf. ただし、核抑止/核戦略の文脈での「損害限定」（能力・戦略）とは、ある種の立場からは核抑止の戦略的安定性を損ね得るリスクを内包するものとして捉えられてきたのに対して、本文における「損害限定」は、専ら通常戦力の敷居以下のオプションとしてのサイバー攻撃能力の策源地への打撃または被害の軽減策を念頭に置いたものとして、価値中立的なものとして用いている。

[55] 当該概念については、次の論文を参照。Samuel Zilincik and Tim Sweijs, “Beyond Deterrence: Reconceptualizing Denial Strategies and Rethinking their Emotional Effects. *Contemporary Security Policy*, vol. 44, no. 2, pp. 248–275. https://doi.org/10.1080/13523260.2023.2185970.

[56] 例えば USCYBERCOM の「持続的交戦ドクトリン」や近年の米国政府の「コスト賦課アプローチ」における「攻勢的（offensive）」な取組について、攻撃の策源地に対する拒否能力として整理したうえで、拒否的抑止のフレームワークのなかに位置付けたものとしては、次の研究を参照。Erica D. Borghard and Shawn W. Lonergan, “Deterrence by Denial in Cyberspace,” *Journal of Strategic Studies*, vol. 46, no. 3, pp.534–569, https://doi.org/10.1080/01402390.2021.1944856.

[57] 佐々木 勇人「『能動的サイバー防御』は効果があるのか？ ～注目が集まる offensive なオペレーションの考察～」JPCERT/CC Eyes, 2023 年 8 月 29 日、https://blogs.jpcert.or.jp/ja/2023/08/effectiveness-of-active-cyber-defense.html.

[58] 必ずしも「コスト賦課戦略」の議論の文脈ではないが、国家によるサイバー安全保障態勢の構築における理念として、「短距離走ではなく、マラソン（a marathon, not sprint）」との表現を用いた例としては、以下を参照。Dan Black, *Russia's War in Ukraine: Examining the Success of Ukrainian Cyber Defences*, The International Institute for Strategic Studies, March

2023, p.16, https://www.iiss.org/globalassets/media-library---content--migration/files/research-papers/2023/03/russias-war-in-ukraine-examining-the-success-of-ukrainian-cyber-defences.pdf.

[59] 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/.

[60] この点については、次も参照。瀬戸「パブリックアトリビューション」75-77 頁。

[61] 近年の米司法省/FBI による「コスト賦課アプローチ」に基づく取組の強化は、例えば次を参照。 U.S. Department of Justice, *Comprehensive Cyber Review,* July 2022, p.2, pp. 9–15, pp. 24–39, https://www.justice.gov/dag/page/file/1520341/download.；瀬戸「パブリックアトリビューション」76-77 頁（注 48-50 を参照）。

[62] バイデン政権下での「攻撃者/キャンペーンへの対処」による「コスト賦課戦略」の思想は、例えば『国家サイバーセキュリティ戦略』の第 2 の柱である「脅威アクターの妨害と解体（Disrupt and Dismantle Threat Actors）」の項や、『国防省サイバー戦略』における「米国全体の防衛（Defend the Nation）」ならびに「同盟国・パートナーとの共同でのサイバー空間の防護」の柱の内容に、色濃く反映されている。それぞれ次を参照。The White House, *National Cybersecurity Strategy*, March 2023, pp.15-18 https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf.；DOD, *Summary: 2023 Cyber Strategy of the Department of Defense*, pp.6-8, pp. 11-12, https://media.defense.gov/2023/Sep/12/2003299076/-1/-1/1/2023_DOD_Cyber_Strategy_Summary.PDF.

[63] この点については、前掲注 40 を参照。

[64] 脅威情報流通のコストを可能な限り減らし、被害組織自身も調査に必要な情報を得られるよう、情報共有活動のレファレンスとなる、「サイバー攻撃被害に係る情報の共有・公表ガイダンス」（検討会事務局：内閣サイバーセキュリティセンター、警察庁、総務省、経済産業省、JPCERT/CC）が 2023 年 3 月に策定され、筆者も本務先（JPCERT/CC）の立場で検討・作成に関わった。https://www.nisc.go.jp/council/cs/kyogikai/guidancekentoukai.html.

PROFILE

佐々木　勇人

政策研究部サイバー安全保障研究室　特任研究員

（本務先：一般社団法人 JPCERT コーディネーションセンター　脅威アナリスト）

専門分野：サイバーセキュリティ

瀬戸　崇志

政策研究部サイバー安全保障研究室　研究員

専門分野：インテリジェンス、サイバー・情報領域と安全保障、欧州の安全保障政策

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 29177）
防衛研究所 Web サイト：www.nids.mod.go.jp