「能動的サイバー防御（ACD）」における対抗オペレーションとその「勝利」について

一般社団法人 JPCERT コーディネーションセンター
佐々木 勇人*

2022 年 12 月に「国家安全保障戦略」が示され、関連法令等の整備が進む「能動的サイバー防御（active cyber defense: ACD）」態勢のうち脅威側に対して行われる対抗オペレーションの可能性とその課題について、これまでに実施されてきた対抗オペレーションの経験を踏まえて、解説・考察する。

1．対抗オペレーションについて[1]

安全保障上の影響を与え得るようなサイバー攻撃活動は、基本的に「攻撃キャンペーン」の形態をとる。攻撃キャンペーンは一定期間内において特定の目的のために特定の攻撃手法／攻撃インフラを用いて行われるサイバー攻撃活動であり、数年単位で繰り返し行われる傾向がある。例えば、2023 年に発覚した Volt Typhoon による攻撃キャンペーンは、有事における通信等の重要インフラに対する破壊・妨害のための準備攻撃としてのサイバー攻撃活動を断続的に繰り返していた。また、2022 年のウクライナ侵攻前後の攻撃キャンペーンについては、その準備活動的な攻撃も数カ月前から行われ、また、2015 年以降、同じアクター等による同様の戦術を用いた攻撃活動が繰り返しウクライナ国内に対して行われてきた。こうした攻撃活動の繰り返しは必ず攻撃者側の「弱点」をさらすこととなり、我々が「対抗オペレーション」を実施できる余地が生まれる。

攻撃者にダメージを与える方法は、アクセス・無害化や通信遮断のような強力な対抗オプションだけでなく、従前から行われている、注意喚起や情報共有活動におけるインディケータ情報の展開、詳細な解析結果を踏まえた分析レポートの公表等の比較的ソフトな対抗オプションも存在する[2]。いずれの対抗オプションも、攻撃者側のポートフォリオ（脆弱性等の初期侵入方法やマルウェア、攻撃インフラ等）の有効性を低下させることで攻撃キャンペーンを失敗に終わらせるとともに、将来の攻撃活動にも影響を与えようとするものである。

従前から注意喚起や情報共有、レポート公表、通知オペレーション（※脆弱な機器の利用者に早期に連絡し、侵入可能な経路を塞いだり、攻撃初期に仕掛けられたバックドアを駆除したりすること）等の対抗オプションが実施されている。しかしながら、実施する各組織間の連携が不足していたり、情報共有が速やかに行われていなかったりといった、様々な「摩擦」によって、対抗オプションの実施タイミングが遅くなる、あるいは実施が不十分でポートフォリオに十分

---

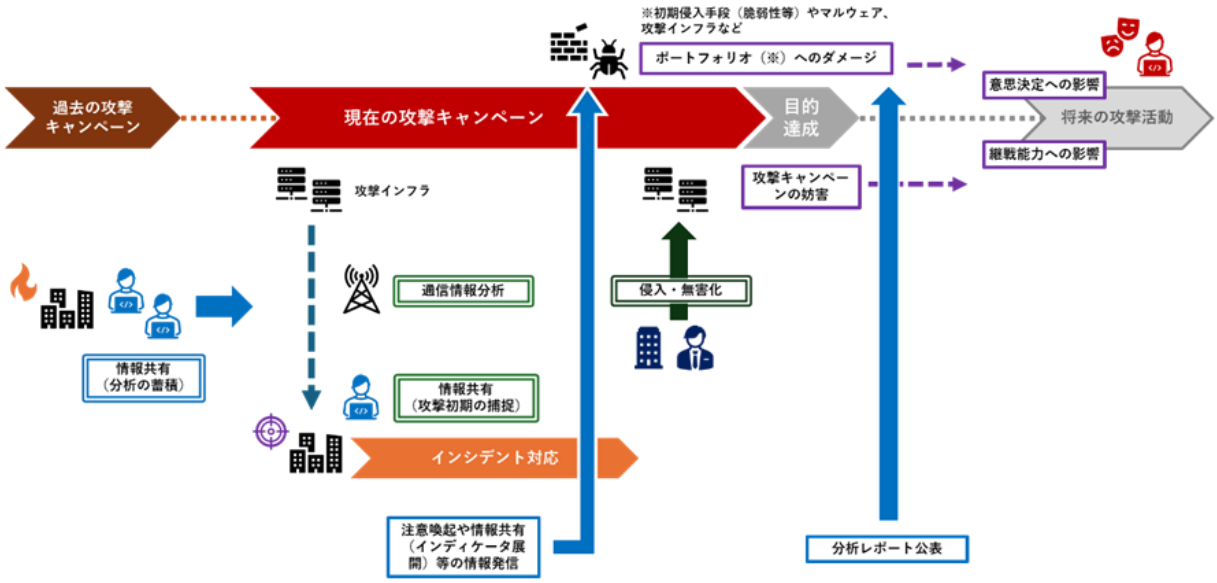
* 一般社団法人 JPCERT コーディネーションセンター　脅威アナリスト（政策担当部長　兼　早期警戒グループマネージャ）
（兼務　防衛研究所　サイバー安全保障研究室　特任研究員）

[1] 本稿でいうところの「対抗オペレーション」については、国際法上の「対抗措置」とは異なるものである。攻撃キャンペーンの概念と対抗オペレーションの理論については、次の拙稿を参照いただきたい。佐々木勇人、瀬戸崇志「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」『NIDS コメンタリー』第 346 号（2024 年 8 月）。

[2] 川口貴久「新たな段階に進む『能動的サイバー防御（ACD）』」サイバー安全保障と能動的サイバー防御（ACD）、Vol.1（2025 年 5 月 21 日）を参照。

なダメージを与え切れていないケースがあり、攻撃キャンペーンの完全な中断・停止には至っていない。そこで、能動的サイバー防御の態勢整備では、情報共有の見直し・強化や通信情報の分析といった新たな手段・環境整備が行うことで、こうした対抗オペレーションのサイクルをより早く回せるようになり、効果的なダメージを攻撃者に与えられるようになることが期待される。

図：能動的サイバー防御の態勢整備後に想定される対抗オペレーションの流れ



出典：筆者作成。

2．対抗オペレーションの「勝利」とは

一方で、こうした取り組みはややもすると「消耗戦」の様相を呈する。

「能動的サイバー防御」では民間にも相当の負担を求めた上で、アクセス・無害化措置等の対抗オプションを使って攻撃者側への対抗オペレーションを実施することになる。対抗オペレーションの成果が見えないまま、あたかも「終わりのない戦い」が続いてしまうと、この協力関係は続かないだろう。

何をもって対抗オペレーションの成果を出したのか、つまり攻撃者に「勝利」[3]したのか、軍事戦略における「勝利」の定義の観点から考察してみたい。

軍事戦略において「勝利」の定義は明確に定まっていないが、スウェーデン国防大学のヤン・オングストロームと J・J・ワイデンの著書『軍事理論の教科書 戦争のダイナミクスを学ぶ（原題：Contemporary Military Theory: The Dynamics of War）』[4]で紹介されている 4 つの観点／考え方から考察してみたい（なお、各小見出しは便宜上筆者が付けたものである）。

①目標ベースの「勝利」の評価

目標達成状態に達すると勝利を宣言し、達成できなければ敗北であると考えるもの。

先述の、Volt Typhoon への対処や、2022 年ウクライナ侵攻前後の攻撃キャンペーンに対する米・ウクライナの Hunt Forward オペレーションがこれに当たる。しかし、関連損失を考慮しないまま戦争が進行することで目的達成状態が修正・変更され、「終わりの見えない展開」になるという問題点がある。

[3] 本調査研究プロジェクトでは、「そもそも『勝利』を必ずしも定義する必要はないのでは」という指摘もあったが、筆者としては、対抗オペレーションの「効果」を常に評価し、対抗オペレーションを実行すること自体が自己目的化しないためにも、「勝利」の概念の整理が必要と考える。

[4] ヤン・オングストローム、J・J・ワイデン（北川敬三監訳）『軍事理論の教科書：戦争のダイナミクスを学ぶ』（勁草書房、2021 年）

②費用対効果ベースの「勝利」の評価

政治的目標達成状態に達することを、そのためにかかった費用と比較して評価すること。費用便益計算の観点から勝利と敗北を理解する場合、価値観の対立に直面するという問題点がある（サイバー攻撃対処における固有の「被害」「コスト」の論点については後述することとしたい）。

③観念ベースの「勝利」の評価

軍事作戦を評価する「得点表」があるのではなく、勝利の概念は社会的に構築・「創造」されるものであり、戦争とは何かという一連の先入観、価値観、軍事行動への期待値、そしていかに情報が処理され拡散するかに影響を受けるとするもの。

2025 年 4 月に WSJ 紙が報じたところによると、前年 12 月にジュネーブで開かれた米中当局者間の会合の場で、中国側から Volt Typhoon の攻撃活動を認めるような発言があり、米側参加者は台湾問題に絡んで米国に対して警告しているものと解釈したとされる。当初の攻撃目的が達成されなくても、脅迫効果／接近拒否的な使い方ができるというケースであるが、同時に、攻撃キャンペーンの解釈によって、勝利／敗北が定められないケースであるともいえる。

④規範ベースの「勝利」の評価

紛争当事者それぞれが、いかに軍事力を理解し、正当な軍事行動であると考えているのか、戦いながら「規範」がさらけ出され、二者間でおのおのの規範構造を知り、暴力を通じて規範構造を「共有」することにより、共同規範構造が形成され、勝利が理解される／相手に理解させるというもの。

2016 年米国大統領選挙に対するロシアの介入事案で米国が刑事訴追の公表を行った際、ロシア法務省はわざわざ「米国の指摘のとおり軍事作戦として行われたのであれば、それは主権免除行為である」と当てこすり的な声明[5]を出したが、仮にロシアが軍事作戦としてサイバー活動を実行しているのであれば、ロシア側の攻撃実行分担等のデマケ／行動ルール（軍事作戦）と、米側の対抗オペレーションのためのルール（刑事手続き）が異なり、食い違っていたことなる。

３．対抗オペレーションと戦略的オーディエンスとの間の課題

残念ながら、今後も安全保障上の影響を与えるような高度なサイバー活動が（成功するかどうかは別として）減ることはないだろう。他方で、そうした活動に対して攻撃キャンペーン単位で失敗させるなど、被害を最小限に抑え、また、攻撃者へのコスト賦課により行動を変容させることは可能である。サイバー攻撃という一つ一つの技術的な事象を予防できたか、あるいは侵害されてしまったか、ということではなく、攻撃キャンペーンやアクターという活動全体に対して、国全体がどのような情勢にあるのかという点で評価されなければならない。たとえサイバー攻撃が行われたとしても、安全保障に著しい影響がなく、社会経済活動を安心して行うことができるかどうか、政治レベルでの評価・情報発信が必要なのであり、国民をはじめとするさまざまな戦略的オーディエンス[6]がいかに納得できるかが重要になってくる。

戦略的オーディエンスに対して、どのように対抗オペレーション、能動的サイバー防御の「勝利」を説明するかについては、先に挙げたように 4 つの観点から説明することが可能である。しかしながら、そのためには

[5] "RE: Democratic National Committee v. The Russian Federation et al.," Ministry of Justice of the Russian Federation, November 6, 2018 (filed on November 9, 2018).

[6] サイバー対抗オペレーションにおける戦略的オーディエンスは、相手方（攻撃者ほか）、潜在的な標的組織やそのステークホルダーのほか、セキュリティ専門コミュニティー、対抗オペレーションに協力する通信事業者や IT ベンダー、マスメディア、同盟国が想定される。対抗オペレーションと戦略的オーディエンスの関係性については、軍事戦略における対反乱作戦と戦略的オーディエンスとの関係論を説いた、エミール・シンプソン（吉田朋正訳、菊池茂雄監修）『21 世紀の戦争と政治　戦場から理論へ』（みすず書房、2024 年）［Emile Simpson, *War From the Ground Up: Twenty-First-Century Combat as Politics* (Oxford, UK: Oxford University Press, 2012)］を参考とした。

乗り越えなければならない、４つの課題も同時に存在する。

①「目標ベース」で勝利を評価するための課題

脅威分析が適切に行われておらず、攻撃キャンペーンやアクターの目的を捕捉できていないケースが散見されている。例えば、2022 年 2 月に大手自動車メーカーのサプライチェーン企業がランサムウェア攻撃を受けた際には、直前のウクライナ侵攻と関連づけるような「分析」が拡散していた。しかし、この時期に同様の攻撃を行っていたアクターはウクライナ情勢とはまったく関係なく活動していたことが判明[7]している。「能動的サイバー防御」で想定されるのは攻撃活動が本格化する前か、攻撃キャンペーンの目的達成前での対抗オペレーションであり、いかに「攻撃活動中」に速やかに捕捉・目的を推定して実施するかが重要である。いかに短時間で適切な脅威分析を行い、攻撃キャンペーンの目的を推定できるかが課題である。

②「費用対効果ベース」で勝利を評価するための課題

サイバー攻撃「被害」は情報漏えいによる中長期的被害やシステム停止による機会損失、復旧費用、専門企業による調査費用だけではなく、対外応答等の「目に見えない対応コスト」や「レピュテーションダメージ」も重くのしかかる。

被害組織にとっては、対抗オペレーション等により攻撃キャンペーンが目的達成前に終わったとしても、そうでないケースとほぼ同様の対応コストが発生する。どちらにせよ、侵害されてしまった以上、個人情報保護法やその他法令等に基づき、また、行政やステークホルダーからの問い合わせに対応するために、漏えいの「可能性」を調査する作業に変わりはない。さらに、調査費用という目に見えるコストだけでなく、各省庁対応、ステークホルダー対応、メディア対応等の目に見えない「対応コスト」も膨大に発生する。

アクターや攻撃キャンペーンの実態に応じた妥当な対応ラインが制度上定められない限り、被害組織側の「被害」はいつまでも減らない。

③「観念ベース」で勝利を評価するための課題

「目標ベース」での評価における課題と重複するが、適切な脅威分析ができていないもう一つの問題として、脅威を過大に評価してしまっている問題[8]を挙げることができる。従前のサイバーセキュリティ政策やサイバーセキュリティ産業は、標的となる可能性のある組織にいかに対策を強化／製品を導入してもらうかという「自己責任による防御」に重点を置いてきたため、オーディエンスを「怖がらせる」アプローチを採ってきた。また、分析や事案対応にあたる行政機関や専門企業も「いかに新しい攻撃手法／攻撃活動を見つけたか」ということにインセンティブを有してきたため、企業としての PR であれ、行政機関としての活動の対外説明であれ、脅威を強調する情報発信にならざるを得ない構造上の課題を有している。

たとえ、マルウェアの仕組み自体が「洗練された（sophisticated）」ものであったとしても、攻撃キャンペーン全体がそうであるとは限らない。攻撃者は強力なゼロデイ攻撃をしているわけでもなく、攻撃インフラも使いまわしているが、標的組織側での管理不備が侵害原因だったり、あるいは情報共有活動で IoC 情報が流通しておらず、攻撃の早期検知に失敗したりすることで、対処に失敗するケースがある。脅威を過度に評価してしまうことで、適切な対抗オプションが選択されず、検討外れの対応がなされてしまうだけでなく、場合によってはさらなるコスト負担を標的／被害組織に強いることになりかねない。

---

[7] 佐々木勇人「ランサムウェア攻撃のアクター 特定をすべきこれだけの理由」セキュリティアナリストカンファレンス JSAC2024（2024 年 1 月）

[8] 脅威の過大評価の問題に対する指摘については、Lennart Maschmeyer, *Subversion: From Covert Operations to Cyber Conflict* (Oxford, UK: Oxford University Press, 2024) や Robert Chesney and Max Smeets, eds., *Deter, Disrupt, or Deceive: Assessing Cyber Conflict As an Intelligence Contest* (Washington, D.C.: Georgetown University Press, 2023)を参照。

④「規範ベース」で勝利を評価するための課題

攻撃者は企業の先端技術情報や政府機関の外交・安全保障上の機微な情報を狙った攻撃キャンペーンを展開したにもかかわらず、被害組織は「（攻撃目的と関係のない）個人情報が漏えいしたかどうか」の観点で調査や対外応答に追われるケースが少なくない。攻撃者も何らかの所在国あるいはスポンサーとなっている政府の制度や組織間の力関係等に制約され、攻撃者側の「ルール」の中で活動してくるわけであるが、我々はこれとは何の関係もない制度やルール、対応コストに制限されて被害対応を行っている。対抗オペレーションや脅威に沿ったインシデント対応ができる制度が作られなければ、いつまでも「攻撃者と同じルールで戦う」ことはできないだろう。

ここまで述べたとおり、安全保障に影響を与えるサイバー攻撃活動との長い戦いのためには、国は戦略的オーディエンスに対して「勝利」の説明ができなければならないが、現行のサイバーインシデントに係る各種制度は残念ながらこれに即したものになってはいない。

「能動的サイバー防御」については、どうしても「アクセス・無害化」や「通信情報分析」といった「目立つ」施策に注目・議論が集中してしまいがちであるが、本稿で述べた各課題の焦点はいずれも「脅威分析」と「インシデント対応」という旧来から存在していた現場の取り組みにある。これまでの長年の知見の蓄積がすでにある「脅威分析」と「インシデント対応」を改めて見直すことで、対抗オペレーションの「勝利」はおのずと見えてくるだろう。

本稿は、東京海上ディーアール株式会社が運営する調査研究プロジェクト「サイバー安全保障と能動的サイバー防御（ACD）」の成果の一部です。
https://www.tokio-dr.jp/thinktank/acd/