防衛研究所 National Institute for Defense Studies
NIDSコメンタリー
第 398 号　2025 年 9 月 26 日

能動的サイバー防御の実装に向けた残された論点（前編）

――攻撃者のポートフォリオ分析の必要性

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

はじめに

いわゆるサイバー対処能力強化法・整備法[1]が成立し、能動的サイバー防御のための整備が本格化していくところであるが、2022 年の国家安全保障戦略で示された能動サイバー防御の 3 本柱（ア）情報共有等の官民連携、（イ）通信情報分析、（ウ）アクセス・無害化、と体制整備について既に先行研究等で多くの論点が提示されている。まず法整備が先行したことから、法的論点としての関心が高い、（イ）通信情報分析、（ウ）アクセス・無害化にどうしても世間の注目が集まるところ、この 2 つ論点が別個に取り上げられがちであるが、（イ）と（ウ）を独立したものとして捉えるのではなく、（ア）官民連携の取組とどのように連携させていくかという視点が必要であり、国家安全保障戦略に記載の順番の通り、（ア）→（イ）→（ウ）という有機的な流れを捉えることで初めて、能動サイバー防御の具体的な「オペレーション」の姿も見えてくると考えている。

本年 7 月のサイバーセキュリティ戦略本部会合にて、サイバー対処能力強化法に基づく「重要電子計算機に対する特定不正行為による被害の防止のための基本的な方針」を検討するための有識者会議の設置方針や「基本的な方針」を令和 7 年中に策定していくスケジュールが示され[2]、具体的な関係省令等の整備が本格化するところである。本稿前編では、以下、（イ）通信情報分析、（ウ）アクセス・無害化に係る議論を整理しながら、その全体像を考察してみたい。

対抗オペレーションとポートフォリオへの“打撃”について

能動的サイバー防御におけるオペレーション（以下：対抗オペレーション）については前回のコメンタリー[3]のほか、拙稿[4]で解説の通りであるが、能動的サイバー防御による対抗オペレーションにおいては、その影響対象である「攻撃キャンペーン」と「ポートフォリオ」の概念が重要である。本稿では、特に「ポートフォリオ」の概念に焦点を絞るが、その説明の前提として、「攻撃キャンペーン」の概念についても簡単におさらいしておきたい。

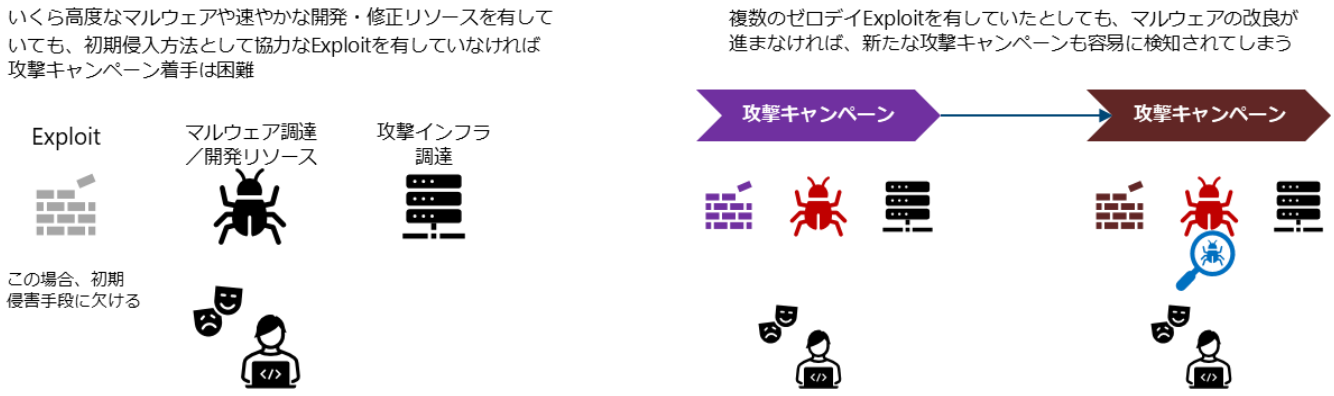
前回のコメンタリーにて解説の通り、従前、アメリカを中心の実施されてきた、「懲罰的抑止アプローチ」では、アクターやその背後にいる政府機関等に対して対抗措置を実施することが中核にあった。これに対して、2018 年以降米サイバー軍が採用した「持続的交戦（関与）（Persistent Engagement）」のような、「コスト賦課アプローチ」はその影響先として「攻撃キャンペーン」にフォーカスを当てている。今般の我が国における能動的サイバー防御の関連法整備においても、アクセス・無害化措置について、国家安全保障会議四大臣会合にて、「サイバー攻撃キャンペーンごとに議論」をして総論的な対処方針を定める旨が国会答弁で示されている[5]。

前回のコメンタリーでも整理の通り、安全保障上の影響があ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繰り返し」の中で行われる。特に多く観測されている、エスピオナージ目的の攻撃キャンペーンや情報工作としての攻撃キャンペーン（例：2015 年～2017 年におけるウクライナへのロシアからのサイバー攻撃活動）は、これまでの実績としても、10 年内において数か月から 1 年程度の攻撃キャンペーンが繰り返し観測されている。そもそもこうした攻撃活動は「強制（Coercion）」ではなく、累積的効果を狙う「Fait Accompli（既成事実化）」[6]であり、武力行使未満の閾値の活動にて行われるため、むしろ、1 回の活動で目的を達成できないがゆえに、長期間繰り返し実行されることになる。また、一見すると、突如発生したように見える大規模攻撃事案もその前段となる攻撃キャンペーンが繰り返されている[7]。こうした攻撃キャンペーンの繰り返しというものが逆に攻撃者側の弱点であり、分析の蓄積と早期検出の取り組みによって対抗オペレーションのチャンスが発生する点は前回のコメンタリーにて解説の通りである。

ここまでの拙稿で示しきれなかった観点として、攻撃者側への「累積ダメージの観点」がある。前回のコメンタリーでも、攻撃キャンペーンとこれに対する対抗オペレーションの繰り返しにより、攻撃者側の継戦能力や意思決定へ影響を与えられる可能性を示したが、これを具体化するものとして「ポートフ

ォリオ」[8]という概念がある。サイバー攻撃アクターにおけるポートフォリオは、主に脆弱性等の初期侵入方法（Exploit 等）、マルウェア、攻撃インフラから構成され、高度な攻撃キャンペーンを展開するためにはこれらが一定程度揃わなければならない。安全保障に影響を与えるような攻撃キャンペーンは基本的に繰り返し行われるが、前回の攻撃キャンペーンが発覚し、セキュリティ専門組織による注意喚起やレポート公表などの情報開示により、ポートフォリオの多くが無効化／効果が減衰することになり、次の攻撃キャンペーンまでにポートフォリオの回復（新たな脆弱性情報の開拓やマルウェア改良、攻撃インフラの再調達）が必要になる。

図：攻撃アクターの「ポートフォリオ」について



こうしたポートフォリオへの“打撃”は「決定的な一打」ではなく、累積的な効果を示すものである。例えば、アクター固有のマルウェアは攻撃キャンペーン毎に新たに開発・調達がなされるのではなく、ある程度、キャンペーンを跨いで改良が継続[9]されることが多い。攻撃キャンペーン毎に投入・改良されるマルウェアに対して、分析・レポートの開示が繰り返されるわけであるが、サイクルを繰り返すごとに、（開示された情報を元に）これを早期に検出するセキュリティ製品・サービスも徐々に増えていくことになり、マルウェアは当初のような優位性を徐々に失っていくのである。

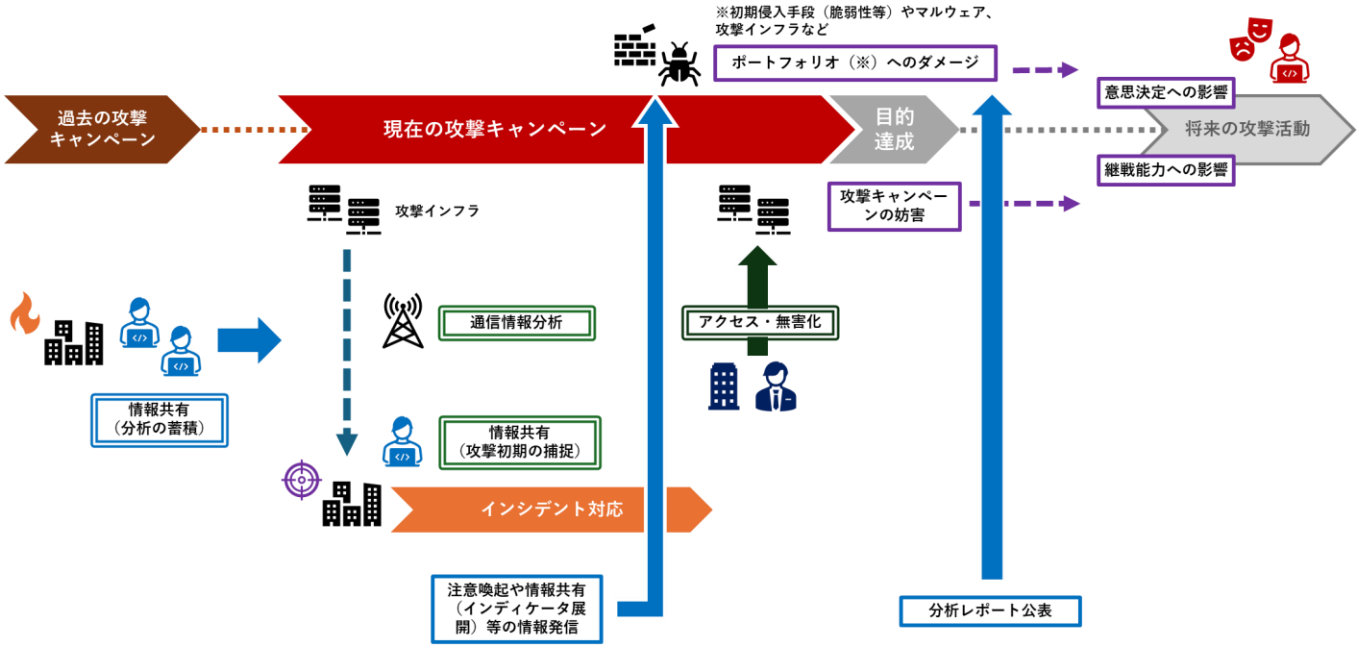
2020 年にイギリス政府が設立した National Cyber Force(NCF)は 2023 年 4 月に「Responsible Cyber Power in Practice」と題した文書を公表したが、そこにおいても、サイバー作戦における相手方への累積的なダメージ（下記太字箇所）と、累積的なダメージによって攻撃者のポートフォリオの有効性への信頼を揺るがせる点（下記下線部）について以下の通り言及[10]がなされている。

> A high degree of planning is required to achieve optimal impact and, in some cases, getting the precise timing right is essential. While the immediate effect of a particular cyber operation may be relatively short lived, <u>the cognitive impact – including a hostile actor’s loss of confidence in their</u>

data or technology – can often be longer term. Combining several operations, alongside other levers of power, into a campaign for **cumulative effect** also supports longer term outcomes.

以下、能動的サイバー防御の各論点の考察を進めていくにあたっては、上記の「攻撃キャンペーン」と「ポートフォリオ」（または「累積的ダメージ」）の観点からお読みいただきたい。

図：能動サイバー防御における対抗オペレーションの流れ



対抗オペレーションにおけるアクセス・無害化以外の対抗オプションの重要性

（イ）通信情報分析、（ウ）アクセス・無害化を巡る諸論点について考察していきたい。まず、アクセス・無害化における、その国際法上の違法性阻却事由[11]については、緊急避難として行われる可能性が政府から示されてきたところ、緊急避難として行うにあたって、危難を避ける「他の手段がなかったのか（当該措置が唯一の手段であったのか）」という論点が指摘[12]される。

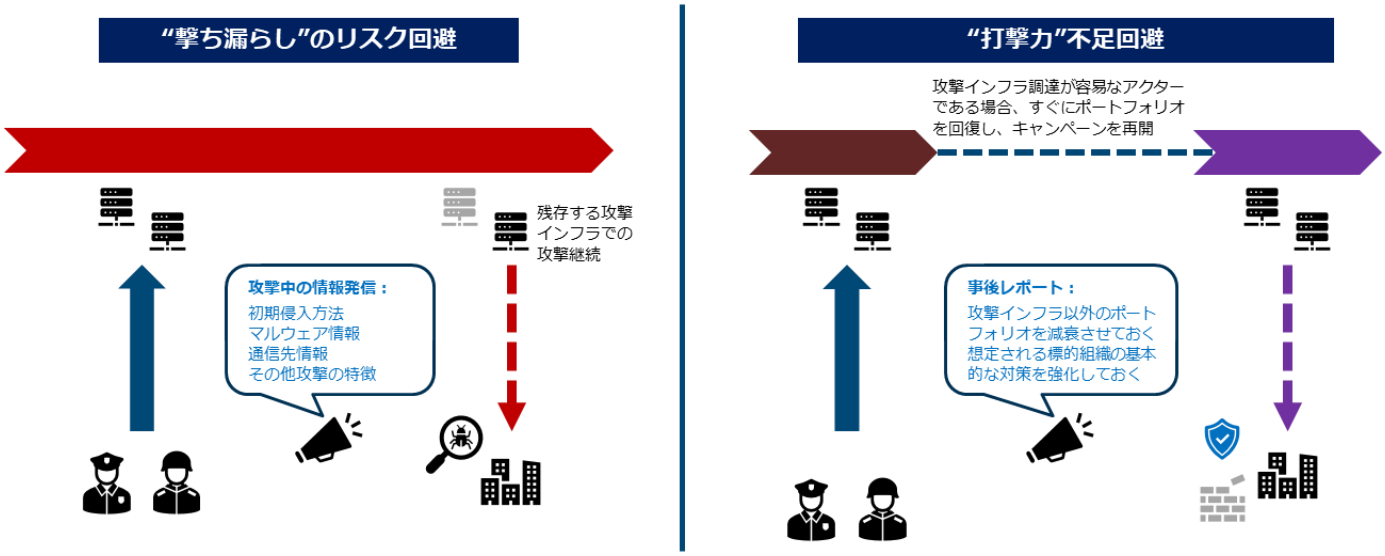
「攻撃サーバを無害化する」という手段ではなく、「攻撃者とマルウェア間の通信を遮断する」という効果に着目する場合、これを達成するための手段は必ずしもアクセス・無害化だけではなく、情報共有によって得たインディケータ情報による、標的組織側での不正通信の検知・ブロックや、通信経路上での遮

断／フィルタリング[13]も想定される。

さらに、「ポートフォリオ」の観点からもアクセス・無害化以外の対抗オプションの検討が重要である。アクセス・無害化だけでなく、インディケータ展開や遮断／フィルタリングでも同様の課題があるが、当該対抗オプションの実施時点で、攻撃インフラをどこまで捕捉できているのか、その網羅性が対抗オプションの効果に影響を及ぼすことになる。こうした、攻撃インフラの「撃ち漏らし」を避ける方法としては、攻撃インフラ以外の情報（初期侵入経路やマルウェアほか横展開手法等）をあわせて開示・共有し、侵入被害を各被害現場側で検出できるようにすることが現時点でも実施されている。

また、累積的なダメージという点でも課題がある。注意喚起や情報共有では、ポートフォリオのほぼすべて（初期侵入経路、マルウェア、攻撃インフラ）にダメージを与えうる可能性がある一方、アクセス・無害化はあくまで攻撃インフラにのみダメージを与えることになる。他方で、注意喚起や情報共有は、その効果を担保するのはオーディエンス（受信組織）側の実行力であり、対応や調査能力のばらつき次第で対抗オペレーション全体の効果が弱まってしまう。一方でアクセス・無害化は（網羅的に攻撃インフラを捕捉できた場合）、確実・強力な一撃を与えることが可能である。“打撃力”は弱いが広く「面」で防御する情報発信オプションと、“打撃力”が強く「縦深」で刺さるアクセス・無害化オプションにはそれぞれ長所短所があることから、ポートフォリオへの効果的なダメージを与えるためには、こうした複数の対抗オプションを組み合わせる必要が出てくるのである。

図：アクセス・無害化と他の対抗オプションを組み合わせる必要性について



こうした複数オプションの組み合わせが対抗オペレーションの有効性の担保として必要とされたケースとしては、例えば、2021 年 3 月の ProxyLogon（Microsoft Exchange Server の脆弱性（CVE-2021-26855 等））を悪用した攻撃キャンペーンへの対処が挙げられる。このケースでは、Hafnium など複数の APT アクター等がこの脆弱性を悪用した広範囲な攻撃を行ったが、この攻撃でサーバーに設置された Webshell に対して、連邦裁判所の令状をもとに FBI がアクセス・駆除するというオペレーションを実施[14]した。当初は、脆弱性の公表と注意喚起、攻撃に関するレポート公開が行われ、基本的に影響を受ける各ユーザー側で検出・駆除が進められたが、なおも未検出の Webshell が多く残留していることが観測されたため、攻撃キャンペーンの継続、あるいは新たな攻撃活動への悪用を阻止するために FBI によるオペレーションが実施されたものである。このケースで FBI が行った Webshell 駆除は令状に基づいて執行されたものであるが、よりソフトな、バックドア設置組織への「通知」レベルのオペレーションは筆者の本務先である JPCERT/CC でも実施[15]しており、注意喚起や情報共有と組み合わせ[16]て実施されている。

前述の緊急避難の成立条件の観点から言えば、アクセス・無害化による攻撃インフラへの越境オペレーションの前段として、注意喚起や情報共有といったソフトな対抗オプション実施、そして、国内における通信遮断／フィルタリングが実施可能かどうかというポイントがまずある。前段にあるソフトな対抗オプションや通信遮断が実施できない／実施しても効果が見込めない場合において、あるいは、これらソフトな対抗オプション実施に加えて、アクセス・無害化を組み合わせなければならないと判断されてはじめて、アクセス・無害化オプションが登場すると考えることができる。これはなにも「アクセス・無害化は“伝家の宝刀”である」ということを示すものではない。むしろ、侵入・無害化という最後の手段が控えているからこそ、その前段に控える、よりソフトな対抗オプションを速やかに実施できるよう、関係機関間の連携体制を整備しなければならないのである。

侵入・無害化のような越境的な措置は単に実施能力／可能性の観点だけで検討されるものではなく、エスカレーションに影響する可能性についても考慮が必要であるが、この際に、「アクセス・無害化を実施するか／しないか」という 2 択になってしまうと、「実施機会を失う前に早急に実施したい」という焦りが判断を曇らせる恐れがある。そうではなく、注意喚起や情報共有、通信遮断等の対抗オプションがグラデーションのように並んでいる必要がある。対抗オプションの選択・組み合わせという観点はエスカレーションコントロールの文脈においても重要である。

なお、情報共有や遮断／フィルタリングオプションについては、実行後に攻撃者がドメインを変更したり、未捕捉の C2 サーバに切り替える対抗手段に出ることが想定されるが、これはアクセス・無害化においても同じことが言え、いずれにせよ、長期的なアクター分析に基づくポートフォリオの捕捉により、

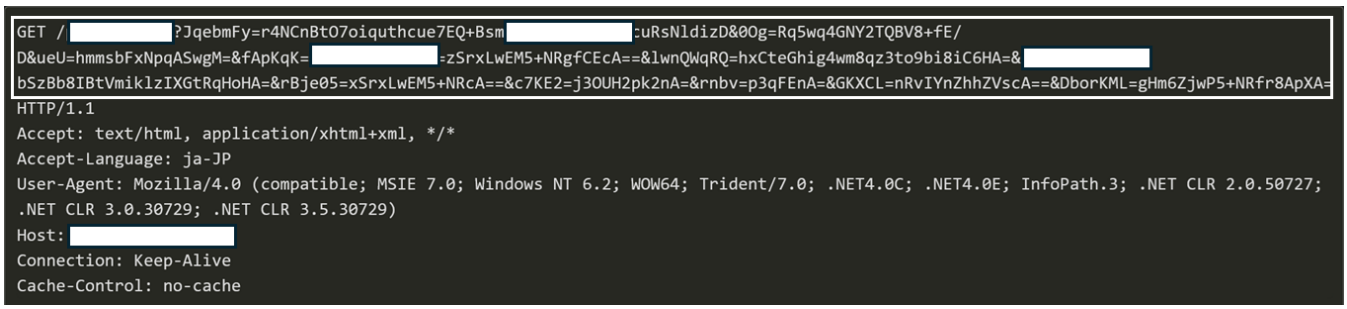
「攻撃者がどの程度の規模のインフラを用いているか／冗長性は有しているか」という想定が必要になる。この長期的なアクター分析の観点は後程解説する。

通信情報分析

次に通信情報分析の論点について考察する。通信情報分析については、その情報取得後の扱いが不明瞭な点[17]について指摘がなされている。これに対する筆者の考えとしては、①不正な通信を見つけるための「ヒント／端緒」情報（マルウェア解析情報に基づくもの）により不正通信をかなりの確度で特定できる、ことと②攻撃キャンペーンが終了した場合、取得データのほとんどは以後の攻撃対処に必要なくなる、ことの 2 点からある程度解消することが可能と考える。

まず、実際にどうやって通信情報を分析するのか考えてみたい。下記図は筆者の本務先である JPCERT/CC にて分析した、マルウェア「ANEL[18]」の通信情報[19]である。メッセージ本体ではなく、いわゆる「ヘッダ情報」と呼ばれるものであるが、このうち先頭行の「リクエスト」という箇所の文字列にこのマルウェア固有の文字列が含まれている。この通信自体は http であり、暗号化（https）されていないが、リクエスト内の文字列は暗号化されている箇所がある。こうした暗号化の仕組みはマルウェア自体の解析により解読することが可能であり、マルウェア解析情報を元に、同様の特徴的な文字列を通信情報から拾うことができれば、マルウェア－攻撃インフラ間の不正通信を見つけ出すことが理屈上は可能である。

図：マルウェア「ANEL」が行う通信の分析情報（JPCERT/CC による分析）



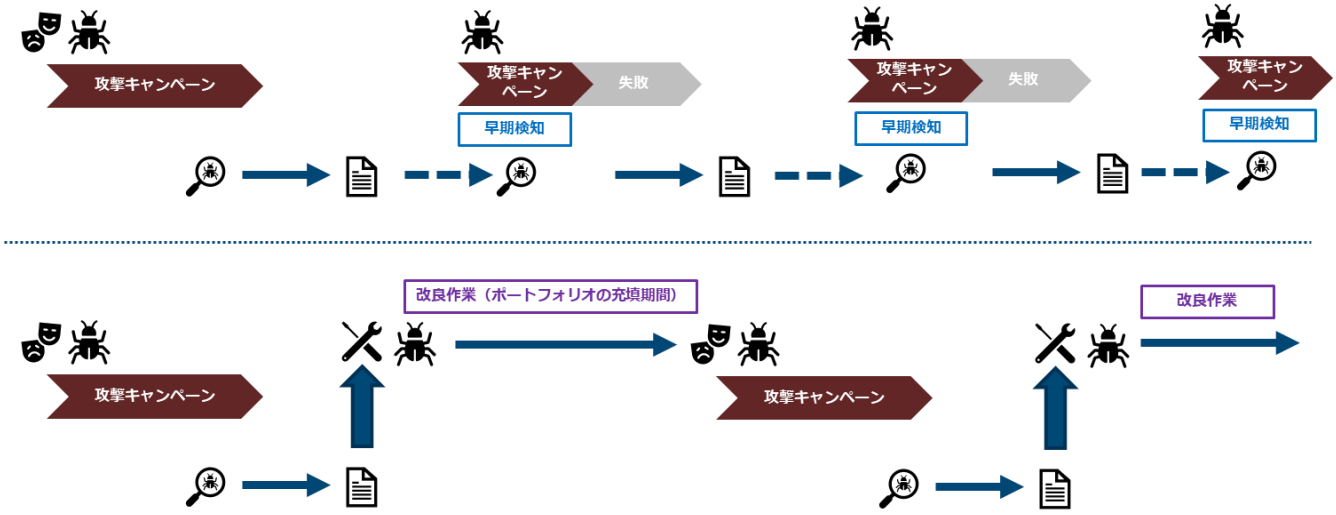
逆に言えば、こうした「ヒント／端緒」情報となる先行情報がなければ、膨大な通信データから不正な

通信だけを見つけ出すことは（現時点では）かなり困難である。大規模なボットネットのように「通信数自体が多いもの」や「ノード間で特徴的な通信を行うもの」[20]はこれまでも実際に通信データから特定された実績があるが、標的型サイバー攻撃のように比較的範囲が限定されるものは難しいと筆者は考える。

他方で、マルウェアは攻撃キャンペーン毎に改良されるため、前回の攻撃キャンペーンで使用された通信の特徴／暗号化方式が現在の攻撃キャンペーンにおけるマルウェアにも実装されているとは限らないわけであるが、マルウェアの改良は攻撃者側の能力やリソース次第であり、攻撃キャンペーン毎にまったく新しいマルウェアを毎回投入できるアクターはなかなか存在しない。基本的にマルウェアの部分改修に留まるものが多い。仮に、通信情報分析で多少の改良がなされたマルウェアの通信を早期に見つけることができるようになった場合、攻撃者側は改良の幅を大きくひろげ、我が方側の捕捉能力を超えようとしてくることが想定される。ただ、このための大幅な改良も攻撃者のポートフォリオ維持のためのコスト増加になるのであり、あるいは次の攻撃キャンペーン実施までのポートフォリオ充足期間を引き延ばす要因となる。

攻撃者が新たな攻撃キャンペーン着手までのタイムラグを短くするためには、マルウェアの使い回しをすることになり、通信情報分析による早期検知が可能になる。一方で、これを逃れるために大幅な改良をしようとすると、その分だけポートフォリオの充填期間が長くなり、攻撃キャンペーン実施回数が減るということになるのである[21]。なお、この効果については、攻撃インフラの使い回しに対しても同じことが言えるが本稿では紙幅の関係から省略する。

図：マルウェアの使い回しによる早期検知とマルウェア改良によって攻撃キャンペーンの実施回数が減る仕組み



法令に基づく詳細な運用が今後どのように決まっていくのかが現時点で不明ながら、理屈上は前項での解説の通り、過去の攻撃キャンペーン分析の蓄積により、専ら使われるマルウェアが発する通信の特徴（ヒント情報）や、C2 ハンティング[22]により得た、攻撃に使われる可能性が極めて高いと思わる不正サーバ情報（IP アドレス、ドメイン（FQDN））を元に、複製した通信情報から不正通信情報を選別することになると想定される。なお、昨今、不正通信のうち特にマルウェア－C2 サーバ間の通信は https 化（暗号化）されているものが多く、通信のヘッダ情報の解析だけでは不正通信の詳細を特定できないことが多いため、通信情報そのものの分析だけではやはりハードルが高く、ここまでに示したような、別の手段により見つけた不正通信の特徴や C2 サーバの情報から不正通信を特定することも必要なのである。

不正通信を特定した後のアクションについて解説されている文献等が見当たらないところ、一般的なインシデントハンドリング／コーディネーションの観点から言えば、以下のような流れが想定される。

1－A：同種の通信を行う他の C2 サーバの調査

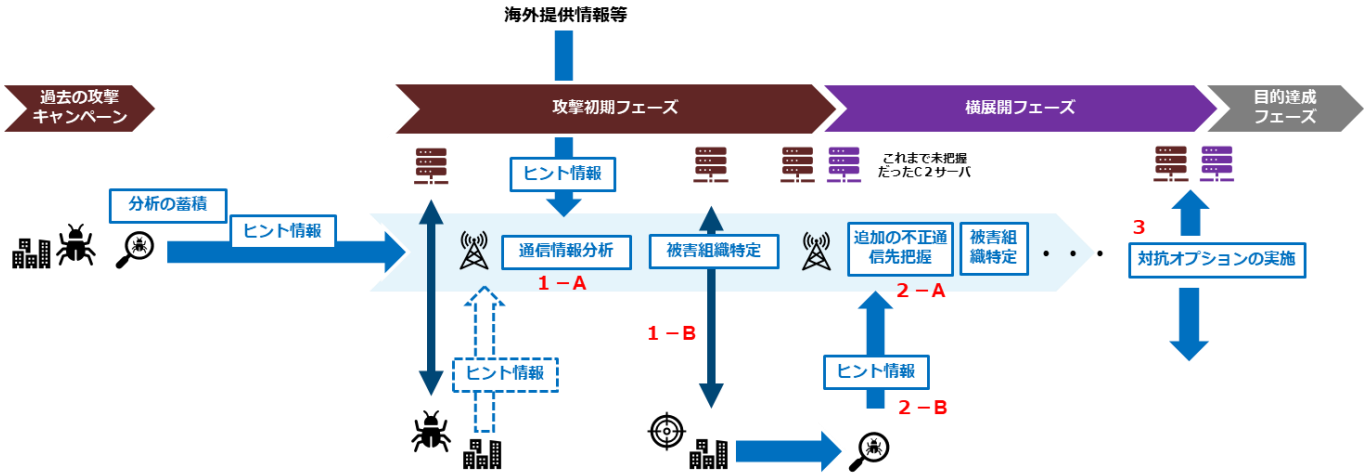
1－B：特定した不正通信を行っている被害組織側への通知とインシデント対応支援

2－B：上記 1－B のインシデント対応で現場から確保したマルウェア等の解析に基づく、不正通信の特徴等の正確な把握（未把握の通信特徴の把握）

2－A：上記 2－B 結果による、さらなる C2 サーバの把握

3：把握した C2 サーバ群に対するアクセス・無害化あるいは、それよりソフトな対抗オプション（注意喚起、情報共有）や通信遮断の実施

図：不正通信を早期に発見した場合のその後のオペレーション例



このとき、どの期間の通信情報をどの程度保管し続ける必要があるのだろうか。基本的には現時点で行われている攻撃キャンペーンの期間内の情報で十分であるはずである。他方で過去の攻撃キャンペーン当時の通信情報を保持し続けなければならない事態は想定されるだろうか。例えば、攻撃キャンペーン終了後しばらくして、海外 C2 サーバ（サーバ X とする）が差し押さえられるなどして、内部に保存されていたログデータから過去の国内被害組織の存在が判明する場合がある。この過去の被害組織を特定するために、過去の通信情報が必要になるかというとそうはならないと考える。まず、過去に取得された通信情報は、過去の対処時点で判明した C2 サーバ（サーバ Y）や特定できた特徴を持つ不正通信先情報にて選別した情報であり、当該時点で把握できていなかったサーバ X に関する通信情報は当該過去の取得情報にはそもそも含まれていないのである。（サーバ X は特定できていなくても、サーバ X と特徴的な通信をするマルウェア Z を被害現場から得るなどして解明できているなら、そもそも当該時点で通信情報分析からサーバ X が特定・対処できているはずである）

したがって、基本的には攻撃キャンペーン／対抗オペレーション毎に取得通信情報の「消費期限」が決まると考えるべきである。

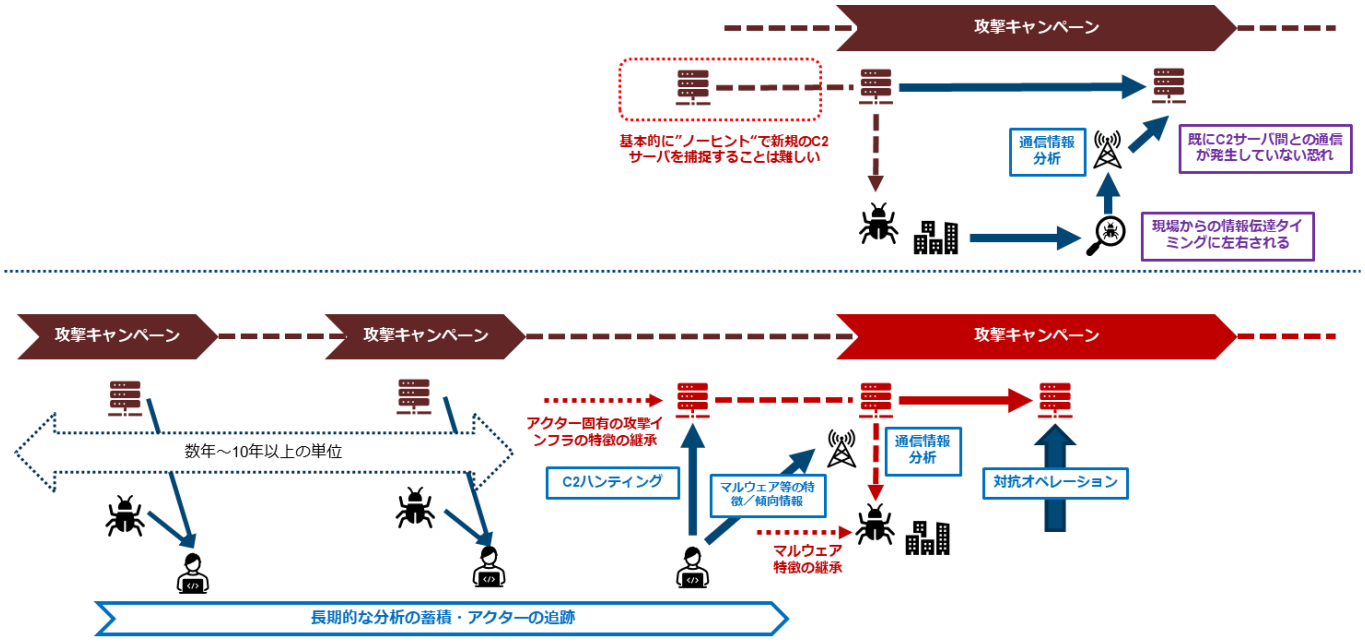
過去の攻撃キャンペーン分析の蓄積

ここまでに述べた通り、対抗オペレーションを成功させるためにも、また、通信情報分析を適切に運用

するためにも、長期間にわたる攻撃キャンペーンの追跡とアクター側のポートフォリオの分析が必須である。特に、この「長期にわたる追跡」という観点が極めて重要である。先述の通り、対抗オペレーションの目的・成果としては、攻撃インフラを無害化するといった“直接打撃”だけでは不足するため、ソフトな対抗オプションも組み合わせて、ポートフォリオの減衰を狙わなければならない。他方で、攻撃キャンペーン中においては攻撃の全容解明がいまだなされていないため、ポートフォリオを正確に・速やかに把握することは難しい。そこで、攻撃キャンペーンの連続性に着目し、過去の攻撃キャンペーンの傾向から、ある程度ポートフォリオを推定することが必要になるのである。

通信情報分析も同じであり、現在使われているマルウェアを確保・解析できてから通信情報を分析するだけでは、基本的に「後追い」になってしまう。直近までの攻撃傾向から、ある程度の不正通信の特徴を絞り込んでおくことも必要であり、また、C2 ハンティングのようなアプローチも併用しなければならない。いずれも長期的なポートフォリオ分析が必須である。

図：長期的なアクター／ポートフォリオ分析・追跡と対抗オペレーションの関係



セキュリティベンダや専門機関が公表するレポートを是非ご覧いただければと思うが、レポートは大きく 4 つの項目が記載される。

①：攻撃の流れの技術的解説。各マルウェアや攻撃手法、攻撃インフラの個別解説

②：アクターの推定や被害／標的範囲（業種、地域）

③：対策について

④：IoC 情報

このうち、ポートフォリオ分析に重要なのは、主に①となる。もちろん、それ以外の情報も有用であるが、それはポートフォリオ分析においてではない。例えば、②のうち、標的分野に関する情報について長年の追跡結果から、「アクター X は A 分野を狙う傾向がある」といった推測ができ、これをもとに現在の攻撃キャンペーンへの対処にあたって、「今回も A 分野が狙われている可能性があるから、A 分野にインディケータ展開をして攻撃を“あぶり出そう”」と考えることもできなくはない。ただそれは、情報発信という対抗オプションの有効性を高めるためのいち参考情報[23]であり、ポートフォリオの構成を推定できるものではないのである。

こうした長期間（数年～10 年程度）に渡るアクター／攻撃キャンペーンの追跡は基本的にはセキュリティ企業や専門機関のアナリストの仕事となり、定期的な異動が求められる行政機関ではなかなか取り組むことが難しい。他方で、基本的にポートフォリオを構成する情報は技術的情報であるから、これをデータベースに蓄積していれば、例え担当者が交代したとしても分析できるのではないかと考えることはできなくはない。ただ、実際の脅威分析は残念ながらそのように単純化できていないのが現状である。いくつか課題があるが、例えば、アクター／マルウェア等の命名規則問題を挙げることができる。同じアクターでもセキュリティベンダごとに名称が異なっていたり、さらにはグルーピングの精度が異なっていたりすることも多い[24]。アクターだけでなく、マルウェアの命名も揃っていないため、同種のマルウェアであるのに名称が異なっているために公開情報上の紐づけがなされていないケースも散見される。こうした差異は機械的処理だけでは紐づけが難しいことも多く、ある程度、アナリストの能力で補っているのが現状[25]である。

また、長期的なアクター／攻撃キャンペーン追跡においてアナリストという人的要因が重要な理由として、「アナリスト同士の情報共有」という点を挙げることができる。セキュリティ専門組織が公表する分析レポートには必ず執筆したアナリスト名が記載される。営利企業であるセキュリティベンダがレポートを公表するのは、ひとつには企業（が抱えるアナリスト）の能力を PR するためである一方、レポートそのものはアナリスト個人の成果として外部に示される。セキュリティベンダは営利企業であるから、基本的に脅威情報を囲い込む方が合理的である。他方で、その能力を支えるアナリストは自社サービスだけで捉えた脅威情報だけで活動し続けることには限界があり、ある程度、他社のアナリストと情報や知見の共有も行いながら、自らの能力を維持・向上させていくのである。他の安全保障、インテリジェンスの分野と比べると極めて異質なエコシステムであるが、攻撃に関する情報のほぼすべてが民間製品・

サービスを通じて提供・流通しているサイバーセキュリティ業界特有の背景由来のものであり、そして、活用することが必須の仕組みなのである。

仮に、命名規則の問題やデータベース化の課題をクリアできたとしても、単にマルウェアや通信先等の技術的情報を蓄積するだけではポートフォリオ分析は不十分である。ポートフォリオ分析から相手方の「弱点」を見つけるためには、当時の攻撃キャンペーンに対してどのような判断でどのような対処がなされたのか、どのような要因があり攻撃キャンペーンが失敗した可能性があるのか、という「対処側の知見」が必要なのである。こうした、長期にアクター／攻撃キャンペーンを追跡できる専門家リソースの活用なしに、攻撃者側のポートフォリオ分析は不可能であり、つまり、対抗オペレーションの実施は困難なのである。

（後編に続く）

[1] 2025 年 5 月　内閣官房サイバー安全保障体制整備準備室「サイバー対処能力強化法及び同整備法について」
https://www.cas.go.jp/jp/seisaku/cyber_anzen_hosyo_torikumi/pdf/setsumei.pdf

[2] サイバーセキュリティ戦略本部第 1 回会合（令和 7 年 7 月 1 日）事務局説明資料「資料 2　サイバー対処能力強化法に基づく基本方針の策定に向けて」https://www.nisc.go.jp/pdf/council/cs/n01/01document2.pdf

[3] NIDS コメンタリー　第 346 号　2024 年 8 月 6 日（特集：「新領域の安全保障」 vol.6）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」
https://www.nids.mod.go.jp/publication/commentary/commentary346.html

[4] 2025 年 7 月 10 日　佐々木勇人「「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」（東京海上ディーアール　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）」）https://www.tokio-dr.jp/thinktank/acd/acd-002.html

[5] 国会会議録　第 217 回国会参議院内閣委員会第 14（令和 7 年 5 月 15 日）https://kokkai.ndl.go.jp/txt/121714889X01420250515　政府参考人（飯島秀俊君）「アクセス・無害化措置については、国家安全保障会議四大臣会合で、いわゆるサイバー攻撃キャンペーンごとに議論をいたしまして総論的な対処方針を定めることとしております。その上で、その対処方針に基づき、内閣官房の総合調整により警察や自衛隊が個別の措置を実施することとなります。」　政府参考人（室田幸靖君）「サイバー攻撃キャンペーンについては、公式の定義があるわけではございませんけれども、サイバーセキュリティーをやっていらっしゃる皆様のイメージとしては、おおむね、ある特定のハッカー集団等が特定の目的の達成に向けて一定の時間的範囲の中で計画し、実施するサイバー攻撃のまとまりというふうな意味で使われているというふうに承知をしております。したがって、国家安全保障会議四大臣会合を開催する以前の段階として、こういったキャンペーンが行われる、あるいは行われるであろうという予兆を把握するということになり、それに対するアクセス・無害化が必要であるというふうな判断をサイバー新組織、あるいは関係省庁と連携して判断が出てきた場合には国家安全保障会議を速やかに開催をいたします。」

[6] こうした解釈については、Michael P. Fischerkeller, Emily O. Goldman, Richard J. Harknett「Cyber Persistence Theory: Redefining National Security in Cyberspace」（2022 年　Oxford University Press）など

[7] 2017 年 5 月の Wannacry2.0 事案、2017 年 6 月の Notpetya 事案のいずれも、マルウェアや侵害経路を試す、予備的／試験的な攻撃がこれ以前に行われており、また、マルウェアは関連するアクターが過去の攻撃キャンペーンで用いていたものの改良版等であった。

[8] 「攻撃キャンペーン」と同じく、業界として用語の定義が定まっているわけではないので、サイバーセキュリティのアナリストたちはこの概念を示すときに「アセット」「リソース」「プロファイル」「アーセナル」など、様々な用語で示すことがあるが、基本的に同じ概念や内容の重複を含んでいる。今回、筆者が用いたように、脆弱性／初期侵入方法・マルウェア・攻撃インフラのセットで示すこともあれば、「Exploit portfolio」のように、単独の要素について表現されることもある。ポートフォリオについて言及することが多い研究者としては、J.D.Work（”Offensive cyber capabilities”（収録：RESEARCH HANDBOOK ON Cyberwarfare” Edit by Tim Stevens, Joseph Devanny))、”Private Actors and the Intelligence Contest in Cyber Conflict”（収録：”DETER, DISRUPT, OR DECEIVE” Assessing cyber conflict as an intelligence contest“ Edit by Robert Chesney, Max Smeets, Forword by Amy Zegart） ほか類する概念についての言及は Max Smeets, Cyber Arms Transfer: Meaning, Limits, and Implications, Security Studies, 31:1. 5-91,

[9] 長期に渡すマルウェアの改良活動とその追跡事例としては、JPCERT/CC「マルウエア LODEINFO の進化」https://blogs.jpcert.or.jp/ja/2020/06/LODEINFO-2.html、伊藤忠サイバー＆インテリジェンス「分析官と攻撃者の解析回避を巡る終わりなき戦い: LODEINFO v0.6.6 - v0.7.3 の解析から」https://blog.itochuci.co.jp/entry/2024/01/24/134047

[10] 英 National Cyber Force(NCF)による言及のほか、同観点への言及は Paul Withers, “Do We need an effects-based approach for cyber operations?” (Edited by Tim Stevens, Joseph Devanny, “RESERCH HANDBOOK ON Cyberwarefare”205 ページ)など

[11] アクセス・無害化措置の実施においては、必ずしも国際法上禁止されていない合法的行為として行われる場合もある点にも留意が必要である。国会会議録　第 217 回国会参議院内閣委員会第 14（令和 7 年 5 月 15 日）https://kokkai.ndl.go.jp/txt/121714889X01420250515 国務大臣（平将明君）「そもそも国際法上禁止されていない合法的な行為に当たる場合やサーバー所在国の領域主権の侵害に当たり得るとしても、その違法性を阻却できる場合があります。」

[12] 西村弓「能動的サイバー防御に関する国際法上の論点」（ジュリスト 2025 年 8 月号（有斐閣））ほか、正当防衛や緊急避難の法的論点の考察については、西貝吉晃「アクティブ・サイバー・ディフェンスと刑事実体法」（講座情報法の未来をひらく 7　安全保障（山本龍彦監修、石井由梨佳編）収録）など。なお、アクセス・無害化を巡る国際法上のもう一つの論点として、「対抗措置」として越境アクセス・無害化が違法性阻却されるか、という議論がある（参照：米田雅宏「能動的サイバー防御としてのアクセス・無害化措置」（ジュリスト 2025 年 8 月号（有斐閣)))。この論点では、対抗措置として認められるために、先行する違法行為の存在があるのかどうかという問題が指摘されている。本項では紙幅の都合から、対抗措置としての越境アクセス・無害化の違法性阻却議論については本格的に触れないが、度々主張する通り、基本的に能動的サイバー防御における対抗オペレーションの対象は「攻撃キャンペーンを断続的に行うアクターの活動」であるのであり、先行する攻撃活動が既に存在している、という前提条件が存在する。また、これまでの累積被害の大きなアクターはすなわち、長年にわたり攻撃キャンペーンを繰り返してきたアクターであるから、そのいくつかは既にパブリックアトリビューションも実施され、先行する違法行為責任の帰属もなされていることが多い。攻撃キャンペーンを跨ぐ違法行為について、先行する違法行為として国際法上認められるのか、筆者の現時点での知見では考察が追い付かないところ、別の機会に取り上げることとしたい。

[13] 能動的サイバー防御をめぐる国の有識者会議での議論やそれ以外の議論においても、対応オプションとして不正通信の遮断／フィルタリングの話題がまったく見られない。通信遮断／フィルタリングをめぐってはこれまでサイバー攻撃対策以外の議論で様々な論争があったという経緯は承知しているが、能動的サイバー防御における対抗オペレーションにおいては、（実施可否は別として）検討自体も極めて重要な意味をもつ手段の一つであると筆者は考えている。特に論点の多い越境アクセス・無害化措置という「(もっとも）ハードな対抗手段」と、注意喚起・情報共有等の「ソフトな対抗手段」との間に手段の選択肢のグラデーションがないことが問題であると考えており、この間を埋める対抗手段として通信遮断／フィルタリングの検討がなされるべきと筆者は考えるが、これは単に対抗手段の選択というオペレーショナルな観点からでなく、本稿で述べた通り、法的議論の論点からも重要であると考えている。海外における様々なオプションを用いた対抗オペレーションのこれまでの実績については https://www.sipa.columbia.edu/global-research-impact/initiatives/cyber/research-and-projects/cyber-disruptions-dataset　にデータセットが公開されている。

[14] DOJ, “Justice Department Announces Court-Authorized Effort to Disrupt Exploitation of Microsoft Exchange Server Vulnerabilities” https://www.justice.gov/archives/opa/pr/justice-department-announces-court-authorized-effort-disrupt-exploitation-microsoft-

exchange

[15] 2025 年 9 月 19 日 JPCERT/CC Eyes 佐々木勇人「解説：脆弱性関連情報取扱制度の運用と今後の課題について（後編）～脆弱性悪用情報のハンドリングと今後の課題～https://blogs.jpcert.or.jp/ja/2025/09/handling_vul_info_2.html を参照。

[16] 2021 年の米国での事例においても、Webshell の駆除はできても、駆除前にすでに内部侵害が始まった被害においては、 Webshell 駆除だけでは対応として不足しており、Microsoft やセキュリティベンダが公表したレポートや情報共有されるインディケータ情報をもとに内部侵害の拡大（横展開）を検出・対応する必要があり、米当局もその旨を明示している。

[17] 小西葉子「通信情報の利用とサイバー通信情報管理委員会」（ジュリスト 2025 年 8 月号（有斐閣））

[18] ANEL は元々、APT10 が 2017 年から使っていたマルウェアで、APT10 の活動停止（分散）とともに観測されていなかったが、2024 年になり再び利用が観測されるようになったもの。2019 年頃まで分析例：JSAC2019：SecureWorks Japan 玉田 清貴「APT10 による ANEL を利用した攻撃手法とその詳細解析」https://jsac.jpcert.or.jp/archive/2019/pdf/JSAC2019_6_tamada_jp.pdf、2024 年の分析例：2024 年 10 月 トレンドマイクロ　原弘明「帰ってきた ANEL:「Earth Kasha (MirrorFace)」による日本での新たなスピアフィッシングキャンペーン」https://www.trendmicro.com/ja_jp/research/24/j/new-spearfishing-by-earth-kasha.html

[19] この「通信情報」というのは能動的サイバー防御で想定される、通信経路上の情報を取得したものではなく、解析環境側でマルウェアを実行し、マルウェアから外部に出て行こうとする通信を解析環境内でキャプチャしたものである。

[20] 以下の通信情報分析の先行事例では、ボットネットワーク固有の通信構成（C2 サーバーボット間の特徴的なネットワーク構成）からボットネットの全体像を把握することに成功しているが、この調査の初期段階では、既に発生しているインシデントから得られた既知の C2 情報をヒントとして調査を始めた旨が記されている。NTT セキュリティジャパン「海外 SOC の Trickbot に関するリサーチ結果の紹介」https://jp.security.ntt/tech_blog/102fvek

[21] こうした、サイバー攻撃における「逆説的論理（パラドキシカル・ロジック）」の考え方については、コリングレイが著書「現在の戦略（原題：Modern Strategy）」（日本語版 2015 年、原版 1999 年刊行）の中で既に指摘している（384 ページ）

[22] C2 サーバはインターネットに公開されており、その外形上の特徴（稼働しているソフトウェア／サービス、ポート番号、IP アドレス／ドメイン、ホスティング事業者等）は誰でも調査可能である。攻撃インフラには固有の特徴的な構成があり、マルウェアの解析など現場側で見つけた情報を元に、同様の特徴をもつサーバをインターネット上で探し出すことが可能である。C2 ハンティングの例としては、Paloalto Unit42「Cobalt Strike 解析&チュートリアル: 人気 Cobalt Strike Malleable C2 プロファイル技術の検出」https://unit42.paloaltonetworks.com/ja/cobalt-strike-malleable-c2/、Hunt io 「Into the Viper’s Nest: Observations from Hunt’s Scanning 」https://hunt.io/blog/into-the-vipers-nest-observations-from-hunts-scanning

[23] 巷に散見される、「APT〇〇（アクター名）は 202x 年に×××（被害組織名）への攻撃を行い、202x 年には△△△攻撃を行った」といったレポートは、あくまで「記録」であって、本稿で取り上げる、アクターのポートフォリオ分析やプロファイリングとしては不十分なものである。ポートフォリオ分析は個別の事案／公開レポートの TTP 情報の丹念な整理と追跡を伴う分析作業であり、単なる公開情報の整理ではない。

[24] JPCERT/CC　佐々木勇人「APT アクターの分類“中毒” ―Lazarus のサブグループ分類に見るアトリビューションの実務的課題―」https://blogs.jpcert.or.jp/ja/2025/01/grouping-lazarus-subgroups.html

[25] グループ間、マルウェア間の紐づけをアナリストの分析で補っている事例としては、上記のレポートのほか、JPCERT/CC　朝長秀誠「HUI Loader の分析」https://blogs.jpcert.or.jp/ja/2022/05/HUILoader.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　早期警戒グループマネージャー　兼　政策担当部長）

専門分野：サイバーセキュリティ

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