NIDS 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.3
第 319 号　2024 年 5 月 17 日

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

一般社団法人 JPCERT コーディネーションセンター[1]　脅威アナリスト
防衛研究所政策研究部サイバー安全保障研究室　サイバー特任研究員
佐々木　勇人

本コメンタリーは、2024 年 3 月 1 日に防衛研究所で実施した「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」研究会の内容を踏まえて、防衛研究所が執筆者に対して寄稿を依頼したものです。本稿における見解は、防衛研究所、および執筆者の所属組織を代表するものではありません。

はじめに

サイバー攻撃に対する防御を行ったり、脅威アクターそのものに対処したりするためには、「何から守るのか」「何に対抗するのか」識別するための、攻撃者の動向や攻撃手法等に関する「サイバー脅威インテリジェンス（Cyber Threat Intelligence）[2]」が必須である。サイバー脅威インテリジェンスは専ら、個別の攻撃被害現場で見つかるマルウェアや不正通信などの技術的情報の分析によって作出されるため、同様の攻撃の標的となっている他の標的組織／被害組織を含め、国全体で脅威に対処するためには、個別の被害現場間や官民間の「情報共有」活動が必要になる。

官民問わず、サイバー攻撃に関する「情報共有」の重要性が示され、さまざまな共有活動や法整備などの取り組みが国内外で行われているが、未公開情報や機微度の高い情報を非公開で共有するという情報共有活動の特性上、その活動実態が公にされることは少ないため、「本当に活動がうまくできているのか？」「効果は出ているのか？」今一つ判然としないことが多い。そうした中で国内においては、2023 年 3 月に「サイバー攻撃被害に係る情報の共有・公表ガイダンス」が公表[3]され、さらに、2024 年 3 月には「攻撃技術情報の取扱い・活用手引き」が公表[4]され、サイバー攻撃に関する情報の共有ルール作りが進んでいる。筆者が（JPCERT/CC として）この 2 つのガイダンスの検討会事務局と素案の作成に関わった

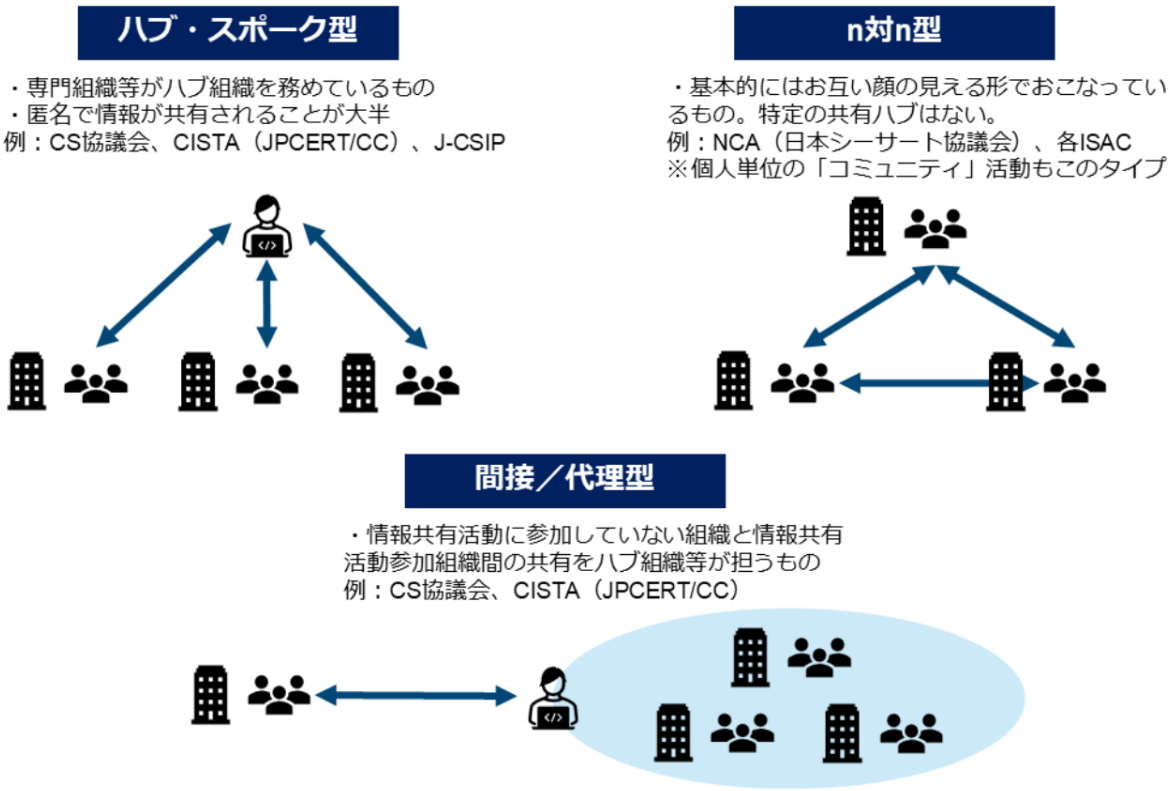
立場から、また、様々な情報共有活動の“ハブ”側として関わっている立場から、本稿では、現在のサイバー攻撃に関する情報共有をめぐる官民間の課題とその解消に向けた取り組み、そして、今後のあり方について考察してみたい。

情報共有活動における“摩擦”

2022 年 5 月から、サイバーセキュリティ基本法により設置された官民の協議体／情報共有活動体である、サイバーセキュリティ協議会に「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：サイバーセキュリティ協議会事務局（内閣サイバーセキュリティセンター、JPCERT/CC）、警察庁、総務省、経済産業省）が設置され、サイバー攻撃の被害組織などが情報共有や被害公表を行う際の「実務上の参考とすべきもの」として、ガイダンスの検討が行われることとなった。

サイバー攻撃が起きた際、被害組織はセキュリティ専門企業などに調査依頼を行うことが多いが、攻撃技術の高度化や事案の複雑化、攻撃者による証拠隠滅などによって、単独の組織だけで攻撃の全容を解明して被害範囲の特定や再発防止策を実施することが困難になっている。そのため、同じ攻撃を受けている他の被害組織やそのインシデント対応支援にあたっている他の専門組織との間で情報共有（交換）を行い、自組織の調査で不足している情報（攻撃手口など）を入手し、情報を補完する必要に迫られているのである。他方で、「サイバー攻撃を受けた」という事実を含む、攻撃に関する情報＝「攻撃被害情報」というのは、被害組織のレピュテーション等に影響する機微な情報であるため、その共有作業には多くの“摩擦”を伴うことになる。例えば、情報共有のさまざまな活動類型の中でも、被害組織同士が実際に「顔が見える」関係において情報共有をするパターン（n 対 n 型）の場合、情報共有のために「こういう攻撃を自社で受けたのだが、ほかに情報ありませんか？」と照会をかけることは、「未公表の自社の攻撃被害を第三者に明かす」行為そのものとなるため、被害組織にとってハードルが高い。他方で、こうしたハードルを緩和するために、JPCERT/CC のような専門機関が「ハブ」として情報の伝達を仲介することで、被害組織を匿名化する活動体も存在する（ハブ・スポーク型や間接／代理型）。しかし、被害組織にとって、このハブ組織／窓口組織に自社被害を明かすこと自体も抵抗を感じる場合が存在する。仮にこうした組織が行政機関だった場合、民間企業は自社のネガティブ情報を渡す行為自体に躊躇せざるを得ない。そのため、先述のサイバーセキュリティ協議会では、情報共有依頼の窓口／ハブ組織は内閣サイバーセキュリティセンターではなく、共同事務局を務める専門機関である JPCERT/CC が担当しているのである。

【図：サイバー攻撃に関する情報共有活動の構成類型】（サイバー攻撃被害に係る情報の共有・公表ガイダンスから抜粋）



情報共有活動の参加組織に展開（共有）される、主な対象情報は、マルウェア情報や不正通信先情報などの攻撃手法を示す情報（※ガイダンスでは「攻撃技術情報」と定義。「脅威インテリジェンス」の区分で言うところの「Operational Intelligence」や「Tactical Intelligence」に相当する[5]）であり、基本的に被害組織を特定するような情報は扱われないことがほとんどである。他方で、攻撃技術情報であっても、解析することで被害組織を特定できてしまうケースがある。例えば、2018 年 2 月に平昌オリンピックの開会式を襲ったとされる OlympicDestroyer マルウェアを用いた攻撃[6]では、攻撃に使われたマルウェア検体が公開解析サービス（VirusTotal）にアップロードされた。このマルウェアは実行されると感染先端末内に保存されたさまざまな認証情報（ID、パスワード、メールアドレスなど）を窃取して自らの内部に取り込み、ネットワーク内の他の端末への不正アクセスに悪用するという機能を有していた。そのため、公開解析サービスにアップロードされた検体の中身を解析すると、窃取された認証情報が丸見えになってしまうのであるが、認証情報の ID がメールアドレスだった場合、被害組織が容易に推測できてしまうのである。このケースでも大会組織委員会や関連する事業者のものと思われる認証方法を含んだマルウェア

が見つかったことで、被害公表前に大会関係先での被害事実が容易に推測されてしまったのである。必ずしも頻度が多いわけではないが、こうしたケースがあることも「被害組織が情報共有＝外部に未公開情報を開示する」ことへのハードルとなっており、ガイダンスではこうした留意点、情報の加工方法などを解説し、少しでも情報共有をめぐる“摩擦”を減らす取り組みを行っているのである。

情報共有の手段とタイミング

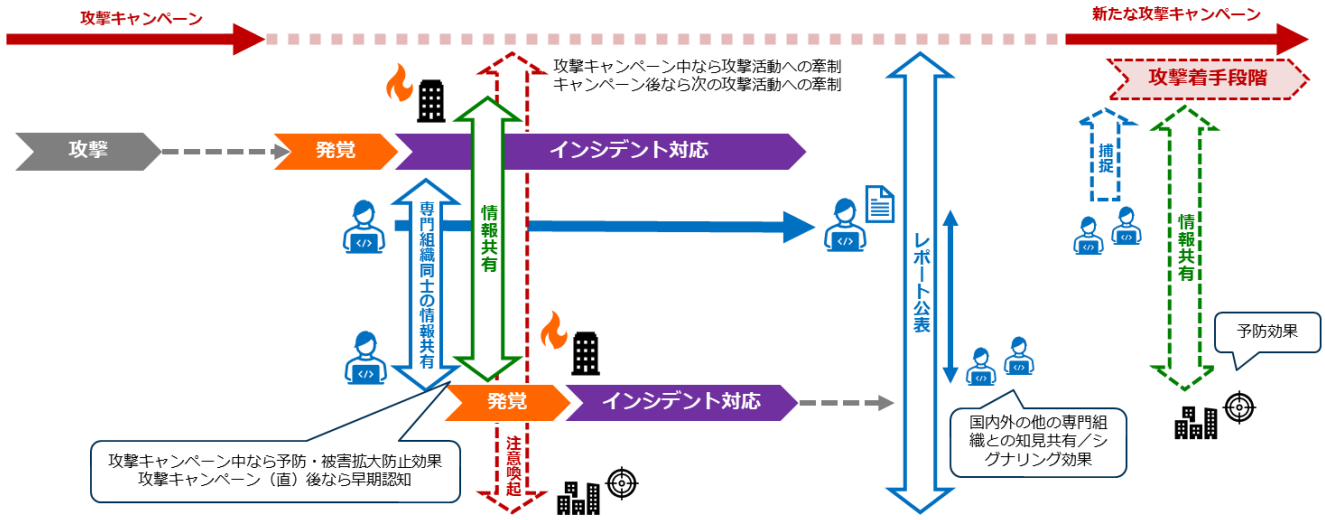
情報共有の効果を得るためには「タイミング」が重要である。攻撃活動の初期の段階、特に攻撃を本格的に開始する前やその直後の時点で「攻撃者がどのような方法で侵入を試みるか」という情報を標的組織間／分野内で共有できれば、被害の未然予防効果がある。一方で、被害がすべて出てしまってからこうした情報を共有しても、「侵害原因の特定」には活用できるかもしれないが、被害予防にはまったく間に合わない。とはいえ、サイバー攻撃の兆候を捉えることは難しく、また、検知の回避や証拠隠滅などのテクニックを攻撃者が多用するため、被害が発生するまえに攻撃を捕捉することは難しい。他方で、攻撃活動がすでに本格化し、複数の組織ですでに被害が発生してしまっている状況であっても、攻撃に関する情報を可能な限り早期に共有できれば、未認知の攻撃を早めに認知できることで、被害を最小限に抑えることができるかもしれない。特に被害公表時に「なぜそれほど長い間検知できなかったのか」と批判されるケースも散見される中においては、「可能な限り早期に認知できる」ことだけでもレピュテーションダメージの緩和にはなる。また、APT（Advanced Persistent Threat、標的型サイバー攻撃ともよばれる）のような、長期間潜伏して標的組織（被害組織）をモニタリング／情報窃取するような攻撃活動／攻撃グループにおいては、たとえ侵入されてしまったとしても、可能な限り早期に認知して攻撃者を追い出せた分だけ、被害を最小限に抑えることができるのである。

情報共有と同じく、「攻撃に関する情報を外部に開示する」活動として、注意喚起やレポート公表がある。情報共有は特定の関係者間において、基本的に非公開で行われる情報交換であるのに対して、注意喚起は主に専門機関が行う公開での情報開示であり、レポート公表は専門機関やセキュリティ専門企業が攻撃の分析結果を公表するものである。攻撃の範囲が広範囲である場合は、限定的な範囲での情報共有活動よりも公開による広範囲な注意喚起が必要になり、他方で、特定の組織／分野をピンポイントで狙う攻撃活動に対しては、「広く浅く拡散」してしまう注意喚起よりも、非公開での情報共有や個別の情報提供が有効であり、攻撃類型やその時の情勢に応じて使い分けや組み合わせが行われるのである。他方でレポート公表の多くは攻撃活動が終わり、各被害組織先でのインシデント対応がひと段落してから行われることが多い。その多くは民間のセキュリティ企業や専門家の「成果」を PR する目的で開示されることも多いが、他方で、攻撃手法や攻撃インフラの全容解明を行い、これを開示することで、同じ攻撃手

法が今後も悪用されないよう、攻撃手法の“陳腐化”がなされるという効果を有している。また、特定の攻撃グループに対する長期的な追跡のための、専門組織間／アナリスト間における長期的な情報共有としての側面もある。専門組織間における長期的な知見の蓄積により、攻撃者の新たな攻撃活動（攻撃キャンペーン）の着手初期の時点において早期の捕捉が可能になるのである。

米国を中心に、パブリックアトリビューションと呼ばれる、攻撃の実行者や外国政府との関係性などの背後関係を公にする取り組みが行われるようになって久しいが、同時に公開される技術情報については、そのタイミングの遅さを指摘する声[7]も少なくない。攻撃の実行者や背後関係の特定には、刑事捜査の手続きをはじめ、作業に相当の時間を要するものが多く、また、国の行政活動としての保秘のほか、インテリジェンス活動で得た情報の取り扱いも絡むケースがあるため、公式発表までの間、関連する情報の対外提供が厳しく制限されることとなる。これは、インテリジェンス情報の積極的な開示を巡る情報機関のジレンマ[8]の一つであるが、国の機関における情報の取り扱いの制約と、民間におけるサイバー脅威情報の取り扱いのルール／文化の間には大きなギャップがあり、これが官民間の脅威情報の流通と効率的な活用を阻害しているのである（後述）。

【図：攻撃からインデント対応の流れと、情報共有、注意喚起、レポート公表のタイミング】



専門組織同士の情報共有

サイバー攻撃情報の情報共有というと、もっぱら被害組織同士の直接の情報交換か、前述のとおり、ハブ組織を経由した被害組織同士によるものが想定されることが多い。他方で、JPCERT/CC のような専門

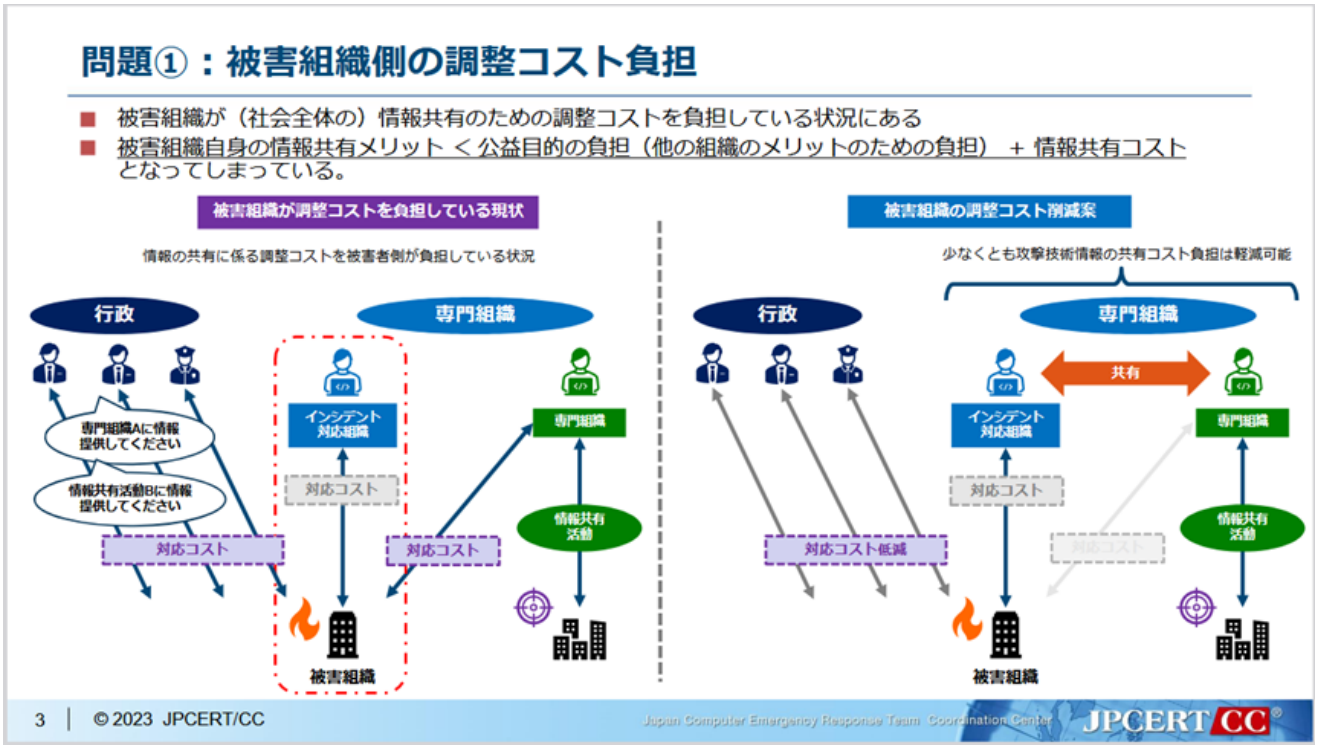
組織では、こうした被害組織を中心とした情報共有の支援だけでなく、専門組織同士で情報共有を行っている[9]。この相手方は各国の CERT 機関や当局のほか、国内外のセキュリティ専門企業や研究者なども含まれる。それぞれ支援する被害現場から得た情報やセンサーなどを使って観測した情報を共有しており、単独組織だけでは不足していた情報を補填するという、被害組織間の情報共有と同じ目的・効果を意図して行っているのである。

営利／非営利を問わず、専門組織にとって脅威情報は活動の源泉でもあり、また、競争優位性を生み出すものとして考えられることが多く、「競合他社との間で情報共有なんてできるのか？」と疑問視されることが多い。実際には公式／非公式な専門家／専門組織間の情報共有活動が行われているのであるが、表立って「専門組織による情報共有活動体である」と明示した活動がほとんどなく、また、機微度の高い情報を取り扱うことから、その活動実態や成果が外部に認知されにくいため、「専門組織同士の情報共有活動」に対する理解不足に繋がっているのではないかと思われる。

2023 年 5 月、経済産業省産業サイバーセキュリティ研究会に「サイバー攻撃による被害に関する情報共有の促進に向けた検討会」が新たに設置され[10]、被害組織を支援する専門組織同士の情報共有活動の活性化に向けた諸課題の検討が行われることとなり、JPCERT/CC も共同事務局として参加した。検討結果を踏まえ、2024 年 3 月には「攻撃技術情報の取扱い・活用手引き」と「秘密保持契約に盛り込むべき攻撃技術情報等の取扱いに関するモデル条文」が公開された。この検討会は先の「サイバー攻撃被害に係る情報の共有・公表ガイダンス」検討の“フェーズ 2 ”として行われ、専門組織同士が情報共有活動を積極的に行うことにより、被害組織の負担軽減や、インシデント初動対応支援にあたる「ファーストレスポンダー」（セキュリティベンダーのほか被害組織から委託を受けている運用保守ベンダーなど、インシデント対応の初動段階で被害組織からの相談を受ける者のこと）が知見不足でインシデント初動対応不備になることを避けることなどの目的が示された。

現状の情報共有活動の多くでは、被害組織自身が情報共有ハブ組織などの専門組織に情報提供して照会をかける、という作業を行っており、インシデント調査支援にあたるベンダーに加えて、こうした第三者とのやり取り自体が被害組織の対応コストを増やす要因となってしまっている。さらに、所管省庁からの問い合わせや警察への連絡など、対外応答に多くのリソースを割かれてしまう現状に対して、この検討会では「まずは民間側の情報のやり取りの整理と負担軽減」をすべく、初動対応支援にあたるファーストレスポンダーが専門組織同士の情報共有を行うことを目指すこととなったのである。

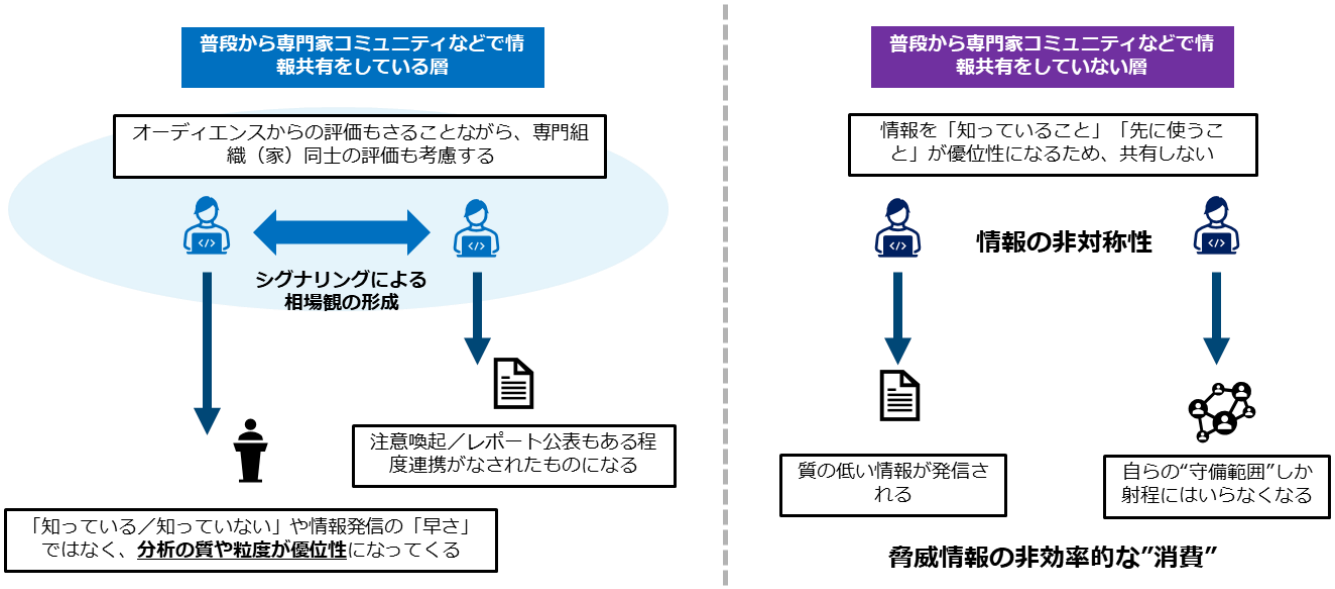
【図：サイバー攻撃による被害に関する情報共有の促進に向けた検討会事務局資料（JPCERT/CC からの問題提起資料）より抜粋】



「競合他社との間で情報共有なんてできるのか？」と疑問視されることが多いという点を先にふれたが、競争優位性の観点から脅威情報を競合他社と共有することのメリットが理解されづらいかと思う。限定的であるがすでに行われている専門家同士の情報共有においては、専門家同士の相互評価のメカニズムがベースとなっており、基本的に「どのような情報を（先に）持っているか」ではなく、「どのような分析をしているか」という観点で評価がなされており、情報は一つのコミュニケーション上の素材でしかない。専門組織同士が情報共有をする目的は、すでに自組織が対応・追跡している攻撃活動について情報が不足しているため、他の専門組織／専門家から不足している情報を得て、分析を高度化させたり、被害組織の支援に活用することである。「情報を得ること」だけが目的ではなく、「分析を高度化すること」「インシデント対応支援を確実に行う」ためである。したがって、共有活動で得た情報だけで分析レポートを公表することはなく、「共有していない独自の情報／知見」も含めて独自の成果としてレポート公表などが行われているのである。共有活動で得た情報だけでレポート公表するなど、共有情報を利己的に「消費」してしまえば、信頼関係が崩れ、以後の共有がなされなくなるため、共有活動の参加組織は利己的に「消費」しないよう振る舞うとともに、必要な時に情報が相手方から得られるよう、普段からの情報の提供（共有）行為によって信頼関係を維持しようとするのである。また、「この組織／専門家に照

会をかけたら情報／知見がもらえるのではないか」と他者から期待されることが必要になるため、普段から知見が十分にあることを示す行為、つまり、レポートやカンファレンスで分析を開示する行為が必要になってくる。この行為自体、専門家同士の相互評価メカニズムであると同時に、営利企業にとっては自社製品／サービスの PR にもなるため、企業の営利活動となんら齟齬はないのである。

【図：サイバー攻撃による被害に関する情報共有の促進に向けた検討会事務局資料（JPCERT/CC からの問題提起資料）より抜粋】

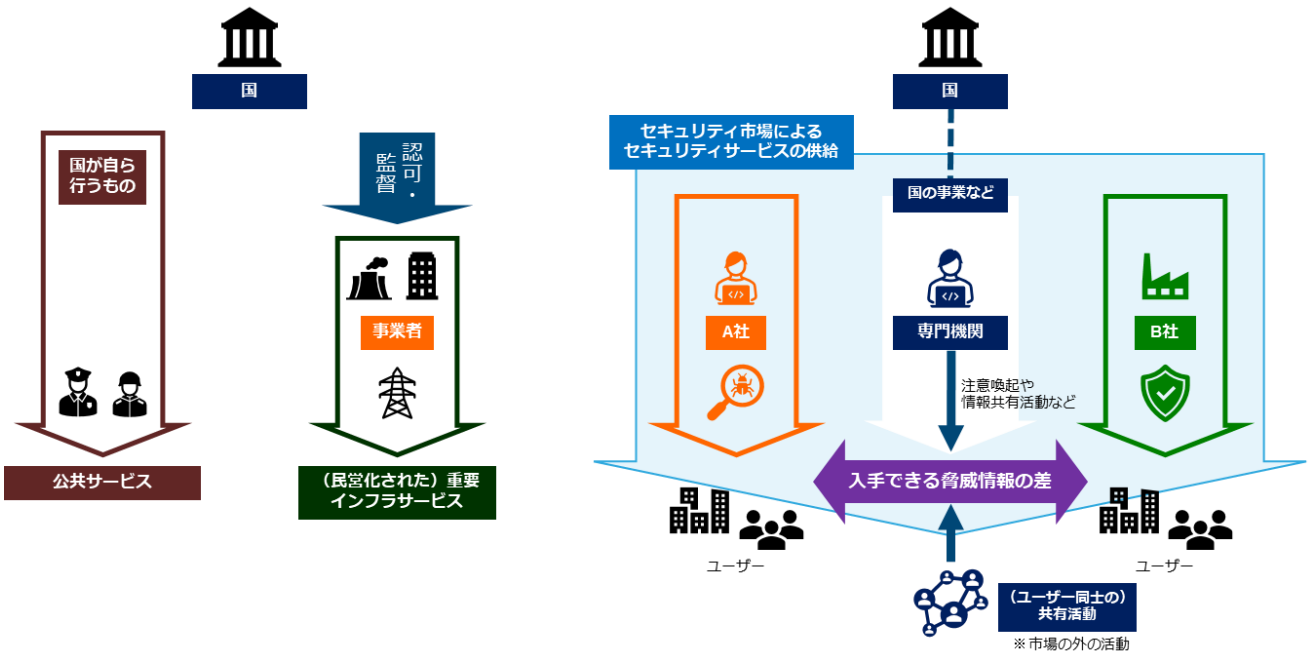


なぜ「共有しなければならない」のか―セキュリティサービスの「市場の失敗」―

情報共有の理由として、「他の被害現場から情報を得て補完しなければ適切な原因調査等が行えない」と冒頭で説明したが、情報共有を「しなければならない」理由は他にもある。アンチウイルス製品や監視サービスなどの「セキュリティサービス」というものは、公共サービスや重要インフラサービスのように、「従前国が提供していたものが民営化された」といった経緯と比べ、歴史的な経緯として「最初から完全に市場を通じて提供されている」サービスであるという特徴を持つ。サービスは市場を通じて提供されるため、ある攻撃について A 社の製品では検知できるが、B 社の製品では検知できないという差が一時的に発生する。これは「市場の失敗」[11]によるものと言えるが、これを補うために、情報共有活動がなされていると考えることができる。JPCERT/CC の活動の多くは経済産業省からの委託事業として行わ

れているが、国からの委託を受けた JPCERT/CC が注意喚起や情報共有を行うのは、この市場の失敗の是正措置（という経済政策）として捉えることができ、重要インフラ事業者同士が集まって行う ISAC（Information Sharing and Analysis Center）といった情報共有活動なども「市場外」の活動でこうした不足を補うものと理解することができるだろう。

【図：サイバー攻撃による被害に関する情報共有の促進に向けた検討会事務局資料（JPCERT/CC からの問題提起資料）より抜粋】



サイバー攻撃に関する情報の大半は民間企業のネットワークで見つかる。正確に言えば、被害組織の IT 資産（端末、サーバー、ネットワーク機器）やセキュリティベンダーの製品／サービス上でマルウェアや不正通信（先）を見つけることになる。公的機関が運用するセンサー網で無差別な攻撃を観測することもあるが、これは攻撃情報の一部でしかない。サイバーセキュリティの世界では脅威に関する情報の大半を公的機関ではなく、そのほとんどを民間サイドで発見し、情報として“生産”しているという、他の分野と比べて特異な環境にある[12]。したがって、国としての攻撃対処を検討する際には必ず、「民間サイドからいかに情報を入手するか」という壁にぶつかるのである。

なぜ国は情報集約の強化を求め続けるのか―情報集約の「政府の失敗」―

2022 年 12 月に公表された新たな国家安全保障戦略[13]におけるサイバー攻撃対処の文脈では、いわゆる「能動的サイバー防御」や通信の秘密を巡る論点が注目されたが、掲げられた項目の一番目に情報集約体制の強化が示されている。4 年ごとに策定されるサイバーセキュリティ戦略[14]には毎回、官民間の情報共有強化などが示されているが、これは海外でも同じであり、米国においても度々情報共有体制強化の法整備や活動体の発足が取り組まれている。では、この問題は延々と解消されていない／進捗がない問題なのだろうか？

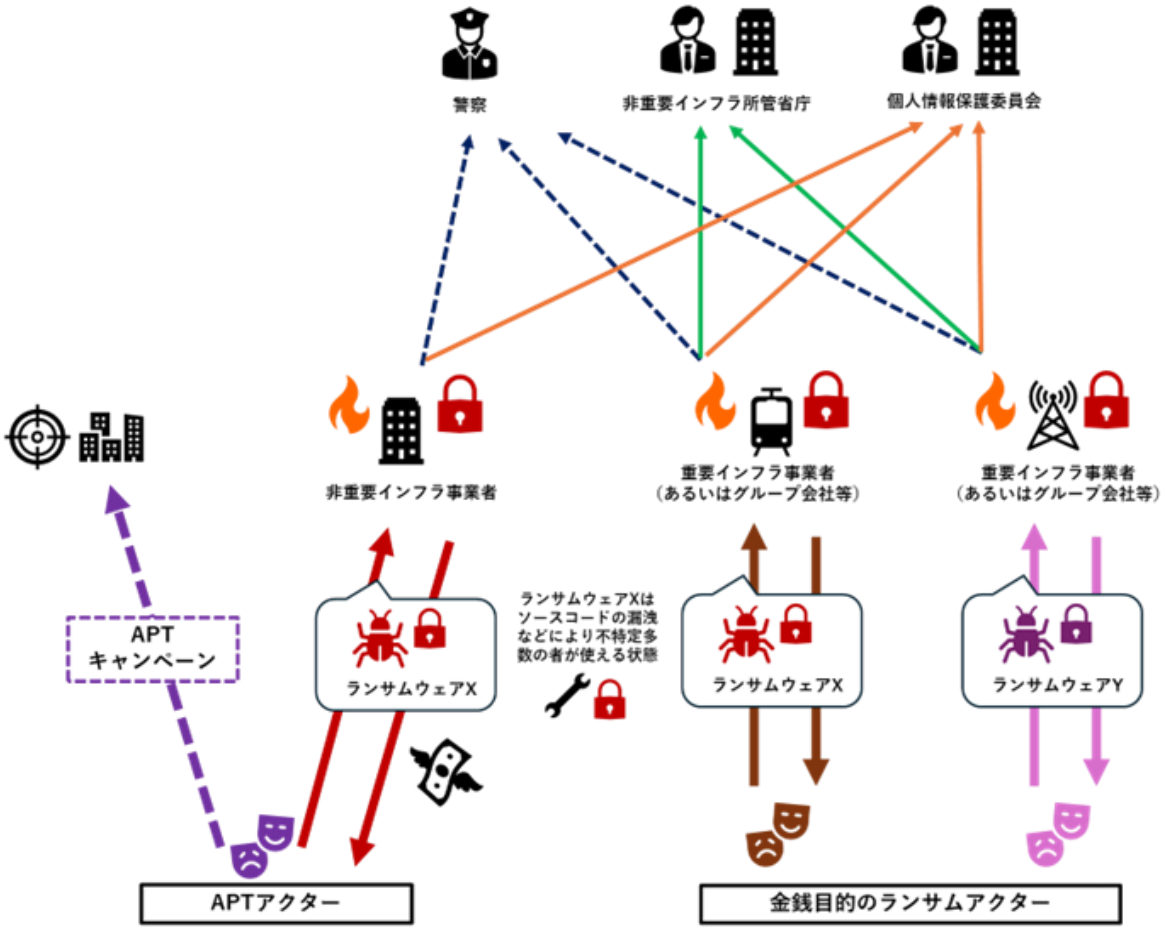
日本においては 2020 年に個人情報保護法が改正[15]され、事象を認知してから 3～5 日以内の速報が義務付けられ、また、ランサムウェア攻撃のように、情報を「棄損」したケース、さらには漏えい等の「可能性」のある段階での報告も求められるようになったため、これまで以上に広いサイバー攻撃のケースで報告が行われるようになった。基本的には、国内で発生したすべてのランサムウェア攻撃は国に報告されることになる。

ランサムウェア攻撃は基本的に金銭目的の攻撃者が実施するものであり、サイバーセキュリティの業界内では「（サイバー）クライム系」と分類される。他方で、APT をはじめ、国家が何らかの形で関与し、国の機微情報や企業の営業秘密などの情報窃取を目的とした攻撃者は「クライム系」とは別と区分されているが、こうした APT アクターがランサムウェア攻撃を実行しているケースが多数報告されている。筆者もこうした事例について国際カンファレンスの場で発表[16]するなどしているが、こうした活動の中には、北朝鮮の関与が指摘されている Lazarus と呼ばれる攻撃グループ群のサブグループが行ったと思われるものも含まれている。金銭目的ではない、国家が関与するサイバー活動の一部において、自組織の活動資金獲得のために別途、金銭目的のサイバー犯罪を行っているグループが存在することが海外専門組織から指摘[17]されているが、国内においては、数多ある「ランサムウェア攻撃被害」の中にこうした国家が関与する攻撃グループの活動・動向が埋もれてしまっているのではないかと懸念するのである。

ほぼすべてのランサムウェア攻撃事案が国に報告されているにもかかわらず、こうした APT アクターによる動向について、少なくとも現時点では分析した結果に関する情報発信や、それを背景とするような対抗措置はどの行政機関からもなされていない。日本においては、サイバー攻撃に関する情報が国に提供される場合、個人情報漏えい事案か否か、重要インフラ事業者に該当するか否か、といった、攻撃類型とは関係のない、被害組織の分類や被害情報の区分に基づくものであり、所管省庁間に情報が分散し、「特定のアクターの追跡」が極めて難しい構造にあると言える。国全体としては、すでに十分な量の被害情報が収集されているはずであるが、省庁間の連携がなされていないなどの理由により、これを適切に

分析することができてないのではないかと懸念している。これは本稿で触れたセキュリティ業界側の「市場の失敗」に対して「政府の失敗」であると言える。

【図：「ランサムウェア」攻撃の情報はそれぞれの行政機関に報告されるが、アクターの動向まで捕捉できていない事例】



なぜ国は情報集約の強化を求め続けるのか―情報を集める目的の不透明感―

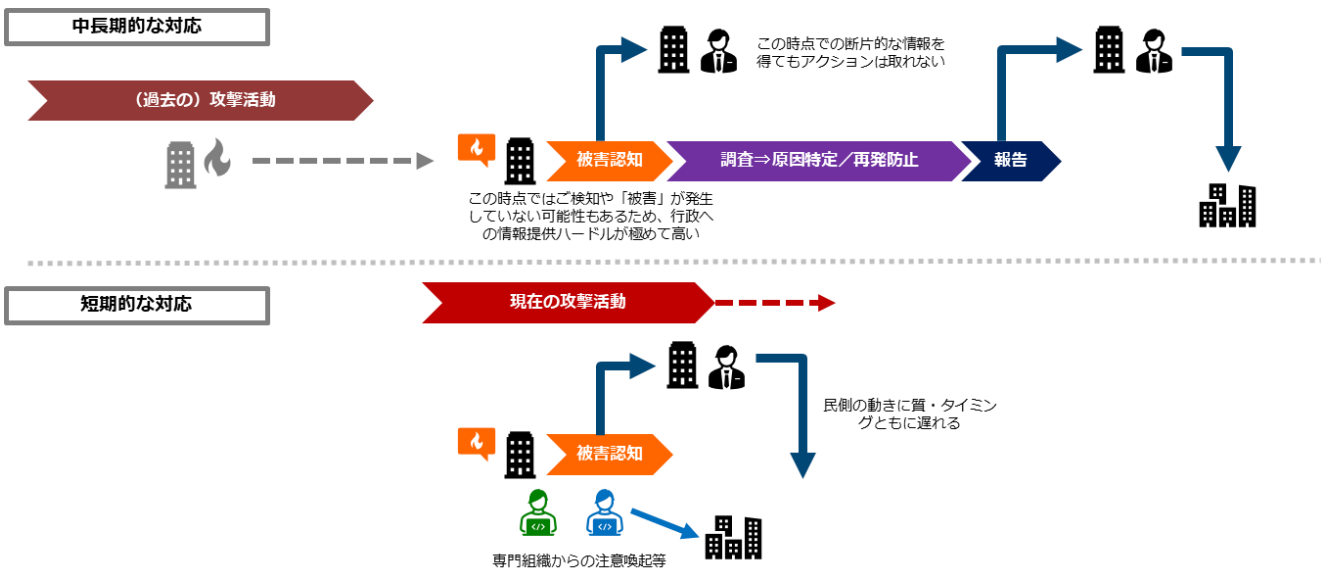
国が被害情報／脅威情報を必要とする理由として、「所管分野への注意喚起や分野を跨いだ情報共有のため」といった説明を聞くことが多い。重要インフラ事業者から所管省庁や内閣サイバーセキュリティセンターへの情報連絡を定めた、重要インフラのサイバーセキュリティに係る行動計画においても、情報連絡の目的として「分野横断の情報共有」が示されている[18]。先述のとおり、民間事業者から行政機関

に情報を出すこと自体に抵抗があることに加え、重要インフラにおいては、連絡先は業法を持つ規制官庁であるため、被害組織≒被規制事業者からの連絡は遅くなりやすい構造を有している。

被害組織から被害報告をする行為自体、被害組織にとっては極めて慎重にならざるを得なくなり、報告内容の精査や報告タイミングの検討など、被害組織内での調整コストもかかり、また、行政との間のコミュニケーションコストも高くなるため、したがって、情報提供が後ろ倒しにならざるを得ないのである。被害組織と専門組織間のやり取りの場合、「セキュリティ製品のアラートで検知した」といった、まだクロかシロか判然としないような状況でも速やかに相談（≒情報提供）されることが多いが、行政に対してそのような拙速な情報提供をする組織はまずいない。

他方で、国は「速やかに情報を得ること」を目指そうとする。被害公表や公表前の報道等により当該事案への社会的注目が高い場合、（業法の有無を問わず）所管省庁から被害組織に情報提供依頼がなされることが多いが、初動段階で「スピード」が必要になるのは、報道を踏まえた官房長官会見や大臣会見で国民・企業向けのメッセージを出すためである。所管省庁単位では、影響を受けそうな所管業界への注意喚起のためであったり、重要インフラのサイバーセキュリティに係る行動計画で示されているような、行政側がハブとなった情報共有活動のためであったりする。ただ、短期的な注意喚起であれば、専門機関や民間側での活動の方が動きは早く、また、技術的にも正確である。また、攻撃被害報告・公表のほとんどは「過去に起きた攻撃」に関するものであるところ、「長期的な所管分野の対策強化のため」ということであれば、「速報的な情報」よりも、時間のかかる原因調査等を終えてからの「正確な報告」が必要なはずである。様々な省庁から繰り返し「被害情報の集約強化」が示されているが、「所管分野への注意喚起や分野を跨いだ情報共有のため」という目的は、「帯に短し襷に長し」である。

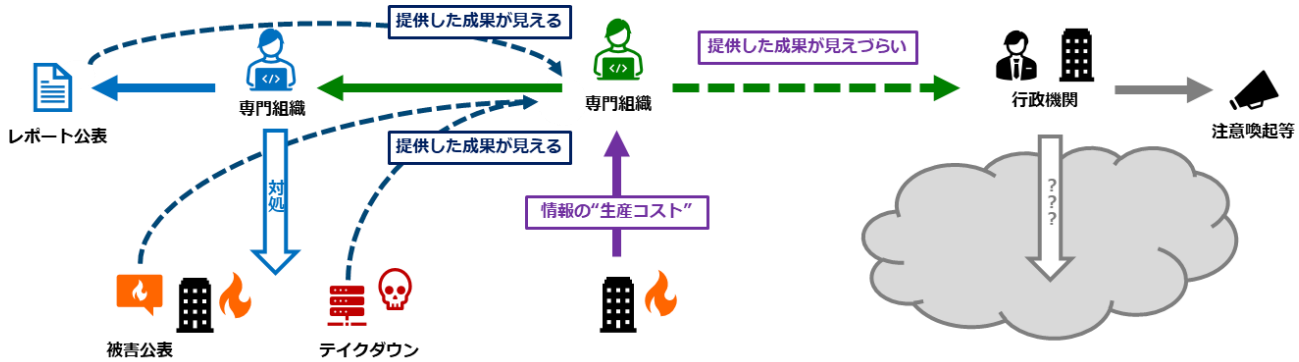
【図：攻撃活動に対する中長期的な国の対応（所管業界への指導等）と、短期的な活動】



筆者は官民間の情報共有活動に関わる中で、「被害組織はセキュリティベンダーや JPCERT/CC のような、民間の専門組織にはすぐに情報を提供するが、行政側への情報提供が遅い」という発言を聞く機会によく遭遇する。こうした声に対しては、「被害組織からすれば、インシデント対応を支援してくれる／知見があると考える専門組織にはすぐにコンタクトするインセンティブがあるが、行政側に対してはあくまで『報告』『届出』であるから、『相談』というインセンティブが働かないだけ」と解説しているが、被害組織からすれば、さらには専門組織から見ても、「行政側はその情報を入手して何に使うのか？」が判然としていないから、情報が渡されにくいのである。先述のとおり、攻撃被害情報というのは、被害組織にとってはネガティブな情報であり、「情報を第三者に出す必要性」がない限り、基本的に開示することはない。また、セキュリティベンダーなどの専門組織にとっては、攻撃に関する情報は自社の製品・サービスを通じて得た情報であり、情報の“生産コスト”があるわけで、これに見合ったリターンがなければ交換に応じるインセンティブが得られない。

JPCERT/CC に情報が提供される場合、必ずしも「インシデント対応に必要な情報が欲しい」からだけではなく、「この情報を情報共有や注意喚起など、他の被害防止に役立てて欲しい」「攻撃インフラの停止など攻撃活動の停止に向けて使って欲しい」といった理由で情報提供されるものも多い。これは、情報提供元に対して「JPCERT/CC は情報をどう使って、何をする（できる）のか」が事前に伝わっているからであり、実際に攻撃インフラが停止したり、情報共有活動や注意喚起、分析レポートを通じて、提供した情報が活用されていることが「見える」からである。他方で、行政側は提供された情報を何に使っているのか、極めて見えづらい。業法・規制法に基づく対応や、捜査、インテリジェンス活動など、活動の詳細をそもそも開示できない活動が多いため致し方ないとはいえ、こうした構造的問題を放置したまま、いくら「情報集約活動の強化」「インセンティブ策の検討」を行っても基本的に問題は解消されないと筆者は考える。報告（提供）した情報が何に使われるのかという予測可能性が官民間の情報共有活動に必須である。

【図：民間専門組織の活動の「見える化」と行政機関の活動の不透明感】



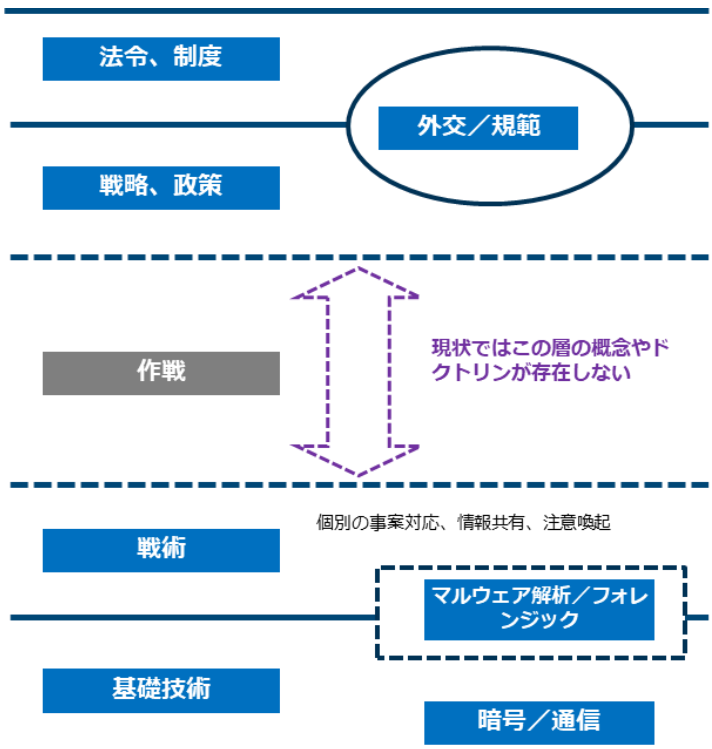
「能動的サイバー防御」に必要な「ドクトリン」

国家安全保障戦略で示されたとおり、「攻撃者のサーバー等への侵入・無害化」のような、脅威側への対抗オペレーションをもし国が行うようになるのであれば、情報集約はまた違った観点から整理しなければならない。こうした積極的な対抗手段の発動について、国家安全保障戦略では「国、重要インフラ等に対する安全保障上の懸念を生じさせる重大なサイバー攻撃について」と条件を付しているが、こうした重大なサイバー攻撃が発生しているケースでは、広範囲・同時多発的な攻撃発生（類似例：2016 年の Wannacry や Notpetya 事案）や、長期間にわたる重要インフラ／政府機関等への攻撃（類似例：2021 年以降の VoltTyphoon による攻撃キャンペーン）が想定されるところ、国による被害状況の把握という観点では、前者は個別の被害組織からの報告を刈り取るまでもなく報道や警察、専門機関からの情報により、行政側で情勢を把握することができ、また、後者については時間がかかるものの、既存の報告制度で被害に関する報告が十分なされるはずである。他方で、対抗手段を実施する対象である、攻撃インフラや攻撃アクターといった、攻撃技術情報の分析に基づく情報については、被害組織からその情報を得るよりも、当該事案対応とその分析を行っている専門組織から得る方が早く、正確である。仮に「攻撃者のサーバー等への侵入・無害化」を行うにしても、対抗手段を行う対象（攻撃インフラや攻撃アクター）が活動中でなければ意味がない。こうした現場側の情報がより早く行政側に提供されるためには、各現場における専門組織が認知した初動対応の段階で「この事案については国側に提供すべきだ」と判断されなければならない。

軍事における「ドクトリン」「作戦術」が、戦略次元と戦術次元をつなぐものとして生み出された[19]ように、サイバー攻撃対処においても、戦略／制度の次元と個別の現場対応などの技術的対応の次元との間をつなぐ「ドクトリン」「作戦術」が必要であると筆者は考える。インシデント対応の初動段階では基本的に被害組織と専門組織という「民間組織」が対応にあたる。初動段階で「この事案に関する情報は国に提供するべきだ」と判断を行うためには、平時から「国は何をするのか」ということが現場まで伝わっていなければならない。先述のとおり、サイバー脅威インテリジェンスは基本的に民間側の被害現場の調査・分析によって得ることができる情報である。国はあらかじめ「どういう情報が存在するのか」知ることができない[20]わけであるから、基本的には民間サイドからの情報提供を待つほかないのである。「国はどのタイミングでどういうことをするから（するため）、どういうタイミングでどのような情報が必要なのか」ということが官民間であらかじめ共有されていなければ、必要なタイミングで必要な情報が民間側から国側へ提供されないのである。そのために、国全体としてサイバー攻撃という脅威に対してどのような対抗オペレーションを行うのか、「ドクトリン」があらかじめ示されているべきと考える。

「ドクトリン」は現状における、官民間の役割分担を巡る混乱を解消する効果もあると考える。現状では、国は注意喚起や個別事案への介入のような「戦術」レベルの活動を行うことが多く、攻撃キャンペーンと呼ばれる特定期間の攻撃活動に対して対抗オペレーション[21]を実施することはほとんどない。「戦術」レベルの活動はもっぱらセキュリティサービスという民間の活動があるため、民間の専門組織と活動が重複したり、タイミング／内容的に劣ってしまったりすることも多い。国側も民間の専門組織と同じようなことをやろうとすれば、サイバー脅威インテリジェンス情報の元となる、攻撃被害情報を「取り合う」関係になる恐れもある。これは行政側が「専門組織の真似事をしている」ということではなく、目の前の問題に対して、法令や制度上では対応ができない／間に合わないため、戦術レベルの対応に“下りてきて”しまっているのである。国家安全保障戦略で掲げられたような「脅威側に向かっていく」行動を国が行っていくためには、攻撃者側の活動（攻撃キャンペーン）に対して対抗オペレーションを組み立て、実施する必要がある。対抗オペレーションは必ずしも行政機関だけで行うのではなく、専門機関からの注意喚起やセキュリティ専門企業からの情報発信など、ソフトな手段も適宜組み合わされ、中長期にわたって機動的に行われる[22]。官民間のさまざまな「現場」組織にどのように動いてもらい、全体として一つの対抗オペレーションを組み立てるのか、そのための術（Art）が現在は存在しないのである。「ドクトリン」があってはじめて、国はサイバー攻撃対処の「司令塔」になることができるのである。

【図：サイバー攻撃対処のためのドクトリン／作戦術の不在と位置付け】



サイバー脅威インテリジェンス“消費”の全体最適化に向けて

セキュリティベンダーや専門機関といった、サイバーセキュリティの専門組織は営利／非営利問わず、攻撃被害情報を「消費」して活動をしている。当然、被害組織の支援も行うが、そうした活動から得られた脅威情報やその分析結果を開示したり情報共有したりすることで同業他組織からの評価を得て、そのポジションを維持することを目指す。評価を得られれば、さらに他の専門組織などから情報を得られやすくなるためである。そして脅威情報は「将来標的になり得る組織」や世間一般に対して、Threat Awareness の素材としても「消費」される。「こういう攻撃があったからこういう対策をしましょう」「こんなに高度な攻撃が行われており現状の対策／体制では不備がある」といった形で情報発信が行われる。

こうした Threat Awareness は注意喚起としてだけでなく、普及啓発や社会全体の理解度向上のために必要なことであるが、ややもすると、行政機関や専門組織の自己拡大や組織維持のための言い訳として、極めて利己的に消費される恐れと紙一重である。例えば、「〇〇攻撃被害が年々増加している」という数字を見たときに、それが当該情報発信元組織の「認知件数」の増加なのか、実際に発生している件数なのか判別することは難しい。また、「増加している」という数字はよく見かけるが、他方で「〇〇攻撃がこのくらい減った／減らした」という数字を見る機会は極めて乏しい。

先述のとおり、サイバーセキュリティの各種サービスというのはその由来から現在までほぼすべて民間サービスから提供されているため、情報共有の必要性として解説したとおり、「市場の失敗」に陥りやすい。「〇〇攻撃がこれだけ減りました」という数字を見る機会が少ないのは、そうした数字を出すインセンティブがセキュリティ専門組織側に基本的にないからである。他方で、同じような現象は公的機関でも同じである。攻撃者の逮捕などによる活動停止やテイクダウンオペレーションによる攻撃インフラの解体などは頻繁に行えることではないため、また、何らかの施策によって、「何件の攻撃被害を未然に防げたのか」を証明することは困難であるため、「何件攻撃を減らすことができたのか」よりも、「どれだけの攻撃が現在存在しているから（自分たちが）活動を行う必要性があるのか」を示す方が合理的になってしまう。各行政機関も件数などの数字で評価され、予算確保に影響する以上、「何件減らせた」ではなく「どれだけの攻撃が発生しているか」という数字に引き寄せられやすいと言える。

また、依然として「他組織にはない情報を持っていること」が優位性であると考える組織は官民それぞれに多く、国内だけでなく、国際間の情報のやり取りにおいてもその弊害が出ている。「被害情報」を利己的・個別合理性だけに基づいて限定的に「消費」してしまうのではなく、全体合理的に効率よく「消費」することが脅威側に対抗する必要条件である。利己的・個別合理的に被害情報を「消費」してしまうのは、その行政機関や専門組織が非合理的な考えを持っているわけではない。先述のとおり、その組織として

個別最適な合理的な判断で情報を使ってしまっているに過ぎないのである。サイバーセキュリティの世界では、社会全体で攻撃被害を最小限にするためにも、個別の製品・サービスの質・機能を強化するためにも、国として脅威主体に対抗していくためにも、何をするにも、官民間のあらゆるプレーヤーに「情報」が必須である。民間だけで情報を共有していれば攻撃対処ができるわけでもなく、また、国だけがサイバー脅威インテリジェンス情報を保有していれば、民間企業を防護できるわけでもない。官民の個別のプレーヤーの個別合理性の殻を破り、全体合理的な情報の消費をするためには、先に述べたとおり、国全体としての攻撃対処の「ドクトリン」が必要であると筆者は考える。

（２０２４年４月２６日：脱稿）

[1] サイバー攻撃被害発生時のインシデント初動対応支援や攻撃停止・被害拡大防止に必要なコーディネーションを国内外の専門組織や通信事業者等と連携して行う中立の専門機関。各国・地域ごとに官／民さまざまなバックグラウンドを持つ CERT（Computer Emergency Response Team）が設立され、国内・国際連携を行っている。個別の民間企業等で社内／グループ内のセキュリティ統括を行う組織として設置される組織は CSIRT（Computer Security Incident Response Team）と呼ばれる。

[2] 脅威インテリジェンス（Cyber Threat Intelligence）の定義や理論的背景、歴史的経緯等については、石川朝久「脅威インテリジェンスの機能的・歴史的視座　民間セクターにおける共有エコシステム分析と政府の関与について」（2024 年 5 月 14 日　NIDS コメンタリー）を参照いただきたい。
https://www.nids.mod.go.jp/publication/commentary/pdf/commentary316.pdf

[3] サイバーセキュリティ協議会 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
https://www.nisc.go.jp/council/cs/kyogikai/guidancekentoukai.html　※サイバーセキュリティ協議会はサイバーセキュリティ基本法で定められた官民間の協議体／情報共有活動

[4] 経済産業省産業サイバーセキュリティ研究会 サイバー攻撃による被害に関する情報共有の促進に向けた検討会 報告書等
https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/cyber_attack/20231122_report.html

[5] 前掲注２図１を参照

[6] 2018 年 2 月 12 日 Cisco Talos, “Olympic Destroyer Takes Aim At Winter Olympics”,
https://blog.talosintelligence.com/olympic-destroyer/

[7] 瀬戸 崇志　防衛研究所 NIDS コメンタリー「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」https://www.nids.mod.go.jp/publication/commentary/pdf/commentary179.pdf；瀬戸 崇志　安全保障戦略研究 第 3 巻 2 号 「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―」 67 頁 https://www.nids.mod.go.jp/publication/security/pdf/2023/202303_04.pdf

[8] 瀬戸 崇志　防衛研究所 NIDS コメンタリー「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」」https://www.nids.mod.go.jp/publication/commentary/pdf/commentary224.pdf

[9] JPCERT/CC では専門組織／アナリスト同士の情報共有活動にも取り組んできており、インシデント対応支援にあたるファーストレスポンダー組織（セキュリティベンダーや運用保守ベンダー）からの相談にも対応している。実際の事案対応で専門組織同士の情報共有や分析を行っている事例として以下のレポートにて紹介を行っている。　JPCERT/CC Eyes「ランサムウェア攻撃事案から見る、ファーストレスポンダー同士の情報共有が必要な理由 」https://blogs.jpcert.or.jp/ja/2024/03/ransom_incident_and_infosharing.html

[10] 前掲注 3 を参照のこと

[11] 「市場の失敗」という民間によるセキュリティサービス提供の負の側面を強調しているが、攻撃手法の変化のスピードが速く、また国・地域・時間に関係なく発生するサイバー攻撃被害に対応するためには、民間市場を通じた製品・サービスの供給と競争による質の向上が必須であることは言うまでもない。

[12] JD Work, “Private Actors and Intelligence Contest in Cyber Conflict,” (Robert Chesney, Max Smeets, Amy Zegart, “Deter, Disrupt, or Deceive : Assessing Cyber Conflict As an Intelligence Contest by Robert Chesney” , 2023　収録)

[13] 内閣官房　2023 年 12 月 16 日閣議決定　国家安全保障戦略 https://www.cas.go.jp/jp/siryou/221216anzenhoshou/nss-j.pdf　この公表以前の「能動的サイバー防御」に関する議論における、筆者の見解としては、2022 年 9 月 21 日 JPCERT/CC Eyes「「積極的サイバー防御」（アクティブ・サイバー・ディフェンス）とは何か ―より具体的な議論に向けて必要な観点について―」https://blogs.jpcert.or.jp/ja/2022/09/active-cyber-defense.html

[14] 内閣サイバーセキュリティセンター　令和 3 年 9 月版　サイバーセキュリティ戦略 https://www.nisc.go.jp/pdf/policy/kihon-s/cs-senryaku2021.pdf

[15] 個人情報保護委員会　令和 2 年改正個人情報保護法の概要

https://www.ppc.go.jp/files/pdf/210324_seirei_kisoku_gaiyou.pdf

[16] 2024 年 1 月 JSAC2024 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」https://jsac.jpcert.or.jp/archive/2024/pdf/JSAC2024_2_6_hayato_sasaki_jp.pdf

[17] 北朝鮮の関与が指摘される、Lazarus の一部のサブグループは 2021 年頃からランサムウェア攻撃を多数行っており、米当局からも注意喚起が発出されている。https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-187a　このランサムウェア攻撃活動について、セキュリティ企業の Kaspersky 社は日本での被害も観測していると報告している。https://securelist.com/andariel-deploys-dtrack-and-maui-ransomware/107063/　また、この他の北朝鮮関連の攻撃グループについても金銭目的の活動が報告されており、セキュリティ企業の Mandinat 社は、グループ自体の活動資金の自己調達目的で暗号資産を狙う攻撃活動を行っている、APT43 についてレポートしている。https://services.google.com/fh/files/misc/apt43-report-jp.pdf

[18] 内閣サイバーセキュリティセンター　重要インフラのサイバーセキュリティに係る行動計画（2022 年 6 月）https://www.nisc.go.jp/pdf/policy/infra/cip_policy_2024.pdf

[19] 北川敬三「軍事組織の知的イノベーション　ドクトリンと作戦術の想像力」（勁草書房　2020 年）116 頁、齋藤大介「戦争を見る第三の視点　―「作戦術」と「戦争の作戦次元」―」（戦略研究学会「戦略研究 12」（2013 年）83 頁、堂下哲郎「作戦司令部の意思決定　米軍「統合ドクトリン」で勝利する」（並木書房 2018 年）17 頁、他

[20] 「能動的サイバー防御」に関する議論では、「通信を平時から監視・分析していれば、攻撃を早期に発見することができる」といった言及を散見するが、標的型サイバー攻撃をはじめとして高度な攻撃の大半では通信内容の暗号化・難読化や、正規のクラウドサービスを用いた通信が多用されているため、通信内容をいくら収集してもどの通信が攻撃なのかどうか判別することは極めて困難である。基本的には被害現場側でのマルウェア等の解析が必要である。ただし、ボットネットのようなサーバー／端末同士が大規模なネットワーク構造を構築して通信し合う攻撃インフラの場合、特徴的なネットワーク構造を見つけ出すことは可能である。参考：2019 年 12 月 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] 「能動的サイバー防御」について、攻撃キャンペーン単位での対抗オペレーションという観点からの考察については、JPCERT/CC のブログ記事で筆者が解説した以下の記事を参照。JPCERT/CC Eyes 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～」https://blogs.jpcert.or.jp/ja/2023/08/effectiveness-of-active-cyber-defense.html

[22] 前掲注 21 参照

PROFILE

佐々木　勇人

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

（防衛研究所政策研究部サイバー安全保障政策研究室　サイバー特任研究員）

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