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.2
第 316 号　2024 年 5 月 14 日

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公共セクターの関与について

東京海上ホールディングス株式会社　IT 企画部　Lead Cyber Security Architect

石川　朝久

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

脅威インテリジェンス（Cyber Threat Intelligence）は、脅威に対する情報を収集し、サイバー防御に活用する技術で、民間セクター（民間企業）を中心に積極的に活用されている。一方、脅威インテリジェンスのエコシステムにおいて、公共セクター（政府機関）の関与は限定的である場合が多い。

本論考では、脅威インテリジェンスの利活用と公共セクターの関与について、３つの側面から分析を行う。第一に、脅威インテリジェンスの役割や位置づけについて、理論的整理を確認する。第二に、機能的視座として、脅威インテリジェンスのステークホルダーを洗い出し、目的・役割を提示することで、利活用のエコシステムを分析する。そして、どのようなインセンティブに基づいて活動しているか、なぜ公共セクターの関与が少ないのか、考察する。第三に、脅威インテリジェンスの歴史的変遷に焦点を当てる。脅威インテリジェンスは、伝統的なインテリジェンス技法を拝借しつつ独自の進化を遂げており、歴史を紐解き、現在の立ち位置を分析する。

脅威インテリジェンスの基礎理論

最初に、脅威インテリジェンスの基礎理論の概略[1]を示し、議論の共通知識を整理する。

脅威インテリジェンスとは？

定義を紐解くため、「脅威」と「インテリジェンス」という 2 種類の用語に分解して解説する。

脅威（Threat）とは、様々な意味・文脈で利用されるが、米国のセキュリティ研究教育機関 SANS Institute の定義[2]によれば、①意図、②能力、③機会の 3 要素が備わった状態を脅威と定義しており、当該脅威となる個人・組織・グループを攻撃グループ（Threat Actor）と呼ぶ。第一に、意図（Intent）とは、攻撃グループが攻撃対象組織を狙う目的・動機を意味する。Microsoft[3]は、イランの支援を受けた Mint Sandstorm が、大学や研究機関で中東問題に取り組む研究者を標的として、情報収集していると報告した。第二に、能力（Capability）とは、目的を達成するために必要な攻撃者の能力・攻撃手法を意味する。前述の例によれば、評判の高い報道機関のジャーナリストを装うソーシャルエンジニアリング、レジストリキーを利用した持続性確保、カスタムバックドア MediaPI の利用などが該当する。また、Open AI と Microsoft 社の共同調査[4]によれば、昨今の攻撃グループは大規模言語モデル（LLM）を活用していることも知られている。第三に、機会（Opportunity）とは、攻撃を可能とする環境・条件を意味する。前述の例でいえば、攻撃者は、なりすましたジャーナリストの個人メールに類似したメールアドレスを使用し、イスラエルとハマス戦争に関する記事について意見を求める無害な電子メールを送り、信頼関係を事前に構築した。これにより、標的型フィッシング攻撃が成立しやすかったことが挙げられる。

一方インテリジェンス（Intelligence）とは、シャーマン・ケントが著書[5]で「インテリジェンスとは知識であり、組織であり、活動でもある」と表現した通り、インテリジェンスの定義[6]には①成果物、②プロセス、③組織の 3 種類がある。具体的には、インテリジェンスサイクル（方針策定→収集→加工→分析→配布）に従い、収集したデータからインテリジェンスを生成する。上記の定義から、脅威インテリジェンスとは、「（サイバーセキュリティの）脅威に関する情報について、収集・加工・統合・評価・分析・解釈を行った成果物。あるいは、当該成果物を作成するためのプロセス・組織を指す」と定義される。

脅威インテリジェンスの目的

脅威インテリジェンスの目的は一般に、より高度な「セキュリティリスク管理」のためとされている。前述の SANS Institute の記事によれば、サイバーセキュリティリスクは、以下の方程式で成立する。

リスク ＝ 脅威 × 脆弱性 × 資産

一般に「脅威」は、様々なセキュリティ対策に保護された「資産」を狙う。そして、セキュリティ対策に「脆弱性」がある場合、資産を破壊したり、盗み出したりすることが可能となり、リスクが発生する。

重要な観点として、防御側としてコントロールできる要素は「脆弱性」と「資産」に限定される。そのため、伝統的なリスク管理手法では、できる限り「脆弱性」をつぶし、安全な場所で「資産」を保有することが重要であるとされてきた。しかし、その伝統的なリスク管理手法も成立しなくなっている。その理由は様々であるが、データの増加、攻撃対象領域の拡大、技術的負債やサーバの増加、利用製品の多様化、クラウド活用やリモートワークの普及、サプライチェーンリスクの台頭など、管理負荷・難易度が増加していることが挙げられる。一方、サイバーセキュリティへのリソース（ヒト・モノ・金・時間）は限られており、全方位的な対策を行うことは現実的ではない。そのため、リスクの優先度をつけるために「脅威」に着目する脅威インテリジェンスが注目されている。「敵を知る」ことで、具体的な脅威へ対応することを優先する脅威ベース型リスク管理手法が主流となりつつある。

脅威インテリジェンスの分類と良いインテリジェンスの要件

脅威インテリジェンスは、ステークホルダーに利用され、初めて価値を持つ。そのため、種類とその目的を理解することが重要となる。図 1 に、その分類を示す。

Long Term

Short Term

カテゴリー	想定する利用者	概要
Strategic Intelligence	経営層	リスク変化に対するハイレベルな情報を提供することで、セキュリティに関する適切な意思決定・投資判断のインプットとする。
Operational Intelligence	セキュリティアーキテクト 管理者 SOC担当者	攻撃者のプロファイル、攻撃手法（TTPs）など攻撃者の手法を理解し、短期～中期的なセキュリティ改善活動に活用する。
Tactical Intelligence	SOC担当者	日々のセキュリティ運用において、攻撃シグニチャ（IOC）を取得・設定することでインシデントを未然に防ぐ。

図 **1** 脅威インテリジェンスの分類

また、脅威インテリジェンスが有効活用されるためには、①正確性（Accurate）、②利用者目線である（Audience Focused）、③アクショナブル（Actionable）、④適切なタイミング（Adequate Timing）の 4A 条件を満たす必要がある。図 2 にその概要を示す。

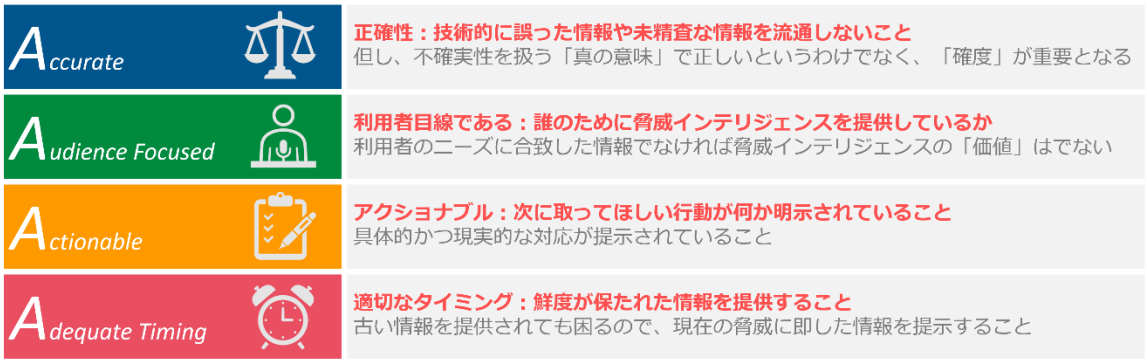

図 **2** 脅威インテリジェンスを有効活用するための **4A** 条件

脅威インテリジェンスの機能的視座：民間セクターにおける独自の進化

民間セクターでは「脅威」への分析技術を高度化するため、国のインテリジェンス機関が持つ技術・思考方法を借りつつ、サイバー領域へ応用してきた経緯がある。その具体例として、インテリジェンスサイクル、あるいは『The Red Team Handbook - The Army's Guide to Making Better Decisions』[7]で紹介されている競合仮説分析、批判的思考などが挙げられる。また、元米国空軍士官である Kevin Mandia 氏が創業した Mandiant 社は、2013 年に中国人民解放軍が米国のサイバー攻撃に関与していることを示したレポート『APT1 - Exposing One of China's Cyber Espionage Units』[8]を発表したが、伝統的なインテリジェンス技法がサイバー領域にも有効に活用できることを実証した事例と言える。加えて、脅威に最も携わるであろう DFIR（Digital Forensics & Incident Response）の専門家に、米軍・警察経験者が多数いたことも、伝統的なインテリジェンス技法を受け入れる上で下地になってきたと推察される。一方、国のインテリジェンス機関の技術・思考法を利用してきた民間セクターにおいて、脅威インテリジェンスは独自の進化・活用を遂げてきた。その理由を 3 種類の観点から紐解いていく。

理由１：目的の相違

第一に、インテリジェンスを必要とする目的の相違である。伝統的なインテリジェンスは国防を目的に収集され、国家の専権事項である。一方、サイバー攻撃において、民間セクターが「脅威」を分析する理由はあくまで「リスク管理」であり、漏洩・攻撃・侵害を防ぐことが主眼である。国防の文脈でも、脅威インテリジェンスの文脈でも「脅威の排除」という用語は登場するが、民間セクターにとっては予防活動、被害を最小化・極小化する検知・対応活動を意味する。一方、国防を担う公共セクターにとって、「脅威の排除」とはより広い意味で利用されている。そのため、サイバー攻撃を受けた場合、公共セクターと民間セクターにおいて脅威インテリジェンスに対する関わり方は異なる。

その一例として、アトリビューション分析[9]を取り上げてみたい。アトリビューション分析とは「攻撃グループを特定する技術」であり、図 3 で示した C4 モデル[10]はアトリビューション分析プロセスと実施レベルを示した図である。

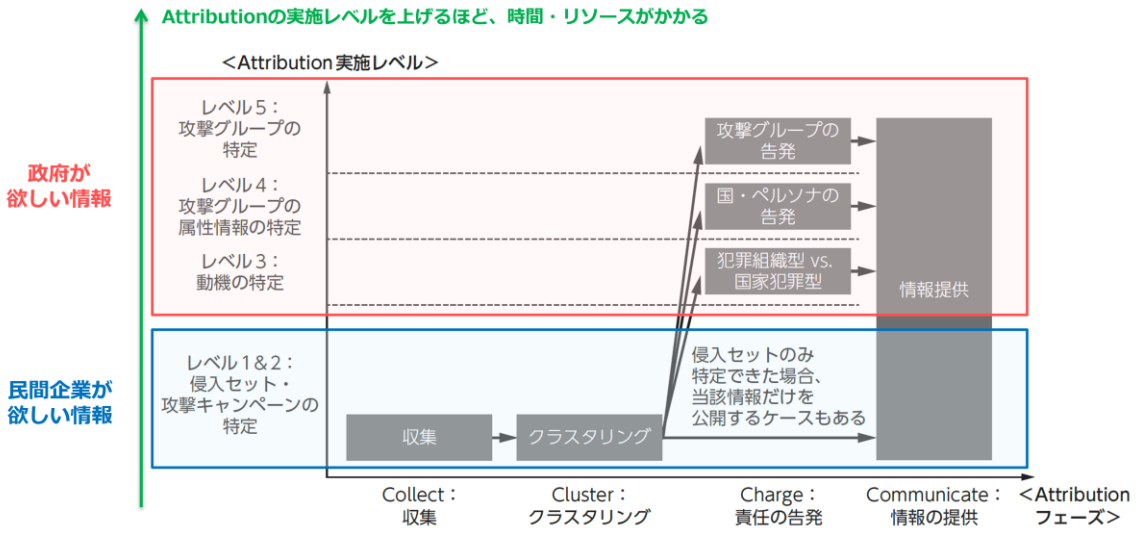

図 3 アトリビューションプロセスモデル（C4 モデル）と実施レベル

横軸がアトリビューションの実施プロセスを意味し、収集→ クラスタリング→ 告発→ 情報の提供の流れで実施していく。一方、縦軸は実施レベルを意味する。実施レベルは、「攻撃キャンペーン」と呼ばれる攻撃パターンを特定するレベルから、攻撃グループの動機、攻撃者の特定に至るレベルまである。民間セクターと公共セクターが必要とするインテリジェンスに注目した場合、民間セクターの多くは「侵入セット・攻撃キャンペーンの特定」を必要とする。攻撃パターンがわかれば、自社環境への影響を分析し、予防・検知に役立てられるため、「リスク管理」に役立つアクショナブルな情報である。一方、動機・攻撃グループの属性情報は、民間セクターにとってはアクショナブルな情報ではないが、国防を担う公共セクターの観点では脅威動向や政策を反映させる上でアクショナブルな情報であると推察される。言い換えれば、アトリビューション一つに着目しても、公共セクター・民間セクターで必要とする情報には差異があり、利活用の差に表れている。

理由２：調査主体・調査対象の相違

第二に、調査主体と調査対象の違いである。例えば、エスピオナージの場合、調査主体は警察・防諜機関であり、民間セクターの事案でも、捜査、取り調べ権限、鑑識技術などは法的・技術的制約から国家の専権事項である。あるいは、重要インフラでの攻撃が発生した場合、自衛隊が衛星写真・レーダーを活用して対応する点で同様である。一方、民間セクターがサイバー攻撃を受けた場合、民間セクターがセキュリティベンダーと協力しながら調査を行うことが一般的である。例えば、情報漏洩事案の場合、被害者や関係省庁への報告など民間セクターとして説明責任を果たす必要があること、予防・検知・対応に対する再発防止策を実装し、事業継続を行うといった目的があるため、デジタルフォレンジック技術を活用し

て、端末・サーバに残された痕跡・ログの分析を行う。言い換えれば、調査主体・調査対象が民間セクターに閉じる傾向にあったため、得られる脅威インテリジェンスも民間セクター内で流通し、独自に進化を遂げた傾向がある。

理由３：共有インセンティブの相違

民間セクターが脅威インテリジェンスを共有する際、インセンティブが大きく影響する。図 4 は、横軸に共有、公表、報告・連絡[11]を取り、ステークホルダーをマッピングした。そして、民間セクターが作成した脅威インテリジェンスを共有する際のエコシステムと課題を表現した図である。

以後、図 4 で整理した 3 種類の論点について議論していく。

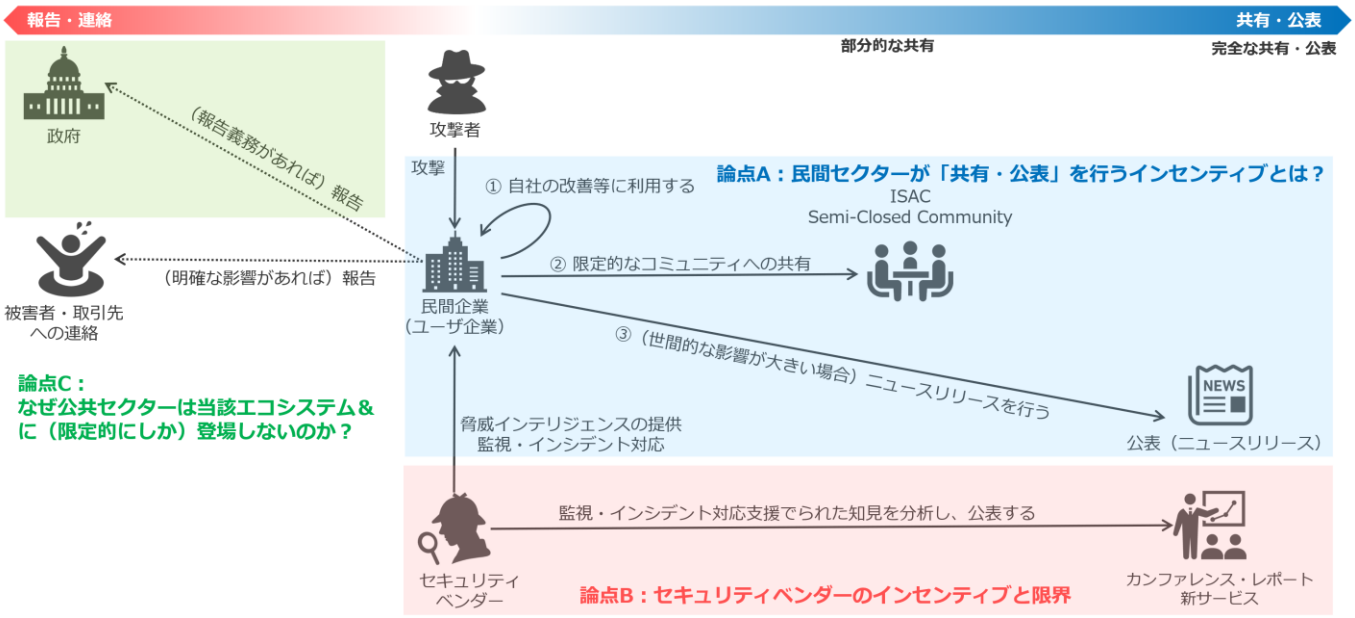

図 **4** 民間セクターを中心とした脅威インテリジェンス共有のエコシステムと課題

論点 **A**：民間セクターが「共有・公表」を行うインセンティブとは？

民間セクターは、「自助・共助・公助」のために共有を行うが、インセンティブをコストとして分析するため、以下の式を利用しながら検討していく。

①予防コスト+②検知・対応コスト+③共有コスト+④（共有に伴う）追加コスト ＜ 共有するメリット

一般に、インシデント発生時において、（セキュリティ製品の導入・運用などの）①予防コストに加え、（分析・対策など）②検知・対応コストを支払う必要がある。また、「共有」を行う際には、既に示した

4A 条件を満たした上で、「誰にどこまで何を開示するのか？」を考えなければならず、③共有コストは大きい。また、共有後、意図しない形で情報が伝播してしまうリスクがある、更問が行われるなど様々な④追加コストが発生する。一方、各組織が共有を行う際には、当該コストの総量よりも「共有するメリット」が大きい必要がある。しかし、共有を実施しても「フリーランチ」の提供となる可能性、そもそもネガティブな情報を出したくないなど、「共有するメリット」が上回るケースは少ないと推察される。

一方、筆者の在籍する金融業界では金融 ISAC などのコミュニティが成立し、「共助」を実践している。その背景には、インセンティブ設計にも様々な施策が取り入れられていることが挙げられる。まず、左辺に注目すると、共有範囲・共有内容が定式化されており、③共有コストが低減されている。また、コミュニティによる秘密保持、TLP プロトコル、善意での活動であることが徹底されており、④（共有に伴う）追加コストが増加しない工夫がされている。次に右辺に注目すると、「共有するメリット」についてコンセンサスが取られている。同じ業界であれば、直面する脅威や攻撃グループ、悪用される攻撃手口も同様である一方、（異なるテレメトリ、リソース、キャパシティ、偶然性など）脅威情報を網羅的に収集できる組織はないというコンセンサスがある。そのため、「共助」として情報を共有することで、自社では把握できない脅威の全体像を把握できる長期的なメリットがあり、潜在的な脅威を排除することが可能となる。また、この「共助」により、②検知・対応コストを低減することにもつながっている。

また、内在的な論理としてマタイ効果（Matthew Effect）を指摘しておきたい。マタイ効果とは、1968 年に科学社会学者ロバート・キング・マートンによって提唱された考え方で、「条件に恵まれた研究者は優れた業績を挙げることでさらに条件に恵まれる」という現象を説明した概念であるが、情報共有コミュニティにおいても、「情報共有した組織に、より多くの情報が集まる」効果は実務でも多く観察される。

論点 **B**：セキュリティベンダーのインセンティブと限界

セキュリティベンダーは、自社技術力のアピール、サービス開発への活用、製品に対するニーズ構築のため、共有には積極的である。一方、ベンダーが提供するインテリジェンスの課題を列挙する。

第一に、情報粒度である。被害企業から見れば、サービス利用に必要な情報を提供しているだけであり、ベンダーが取得できる情報は技術的情報に限られる。それゆえ、能力については分析できるが、意図・機会に関する十分な分析は難しいと推察される。また、詳細情報を開示できないケースも多く、情報粒度も汎化された内容となる。

第二に、ベンダーが取得するデータのカバレッジである。ベンダー間での情報連携はほとんど行われず、自社のサービス・製品で取得できるデータに基づいて分析される。言い換えれば、当該ベンダーの観測範囲で分析・解釈された結果であるため、偏り等を踏まえて取り扱う必要がある。

第三に、ベンダーの脅威インテリジェンスが、本当に「正確な」情報なのか、検証する術がないという問題である。ここでいう「正確性」は、データセットが公開されないため、情報の受け手として、自組織との関連性・影響度を自身で検証することが難しいという意味である。

論点 **C**：なぜ公共セクターは当該エコシステムに（限定的にしか）登場しないのか？

公共セクターがエコシステムに限定的にしか登場しない理由は、インセンティブの不一致と考えられる。まず、公共セクターへの報告に対し、一定のハードルがある。また、公共セクターが脅威インテリジェンスを必要とする理由は国防のためであるが、アトリビューション分析を含め、「第 5 の戦場」と呼ばれるサイバー空間において、公共セクターが観測可能な「レーダー」は限定的である。言い換えれば、公共セクターだけで情報収集を完結することは難しく、民間セクターで受けた攻撃等をメタ分析することが現実的である。一方、民間セクターからすると、情報提供のハードルが高いこと、当該情報を公共セクターに提供しても 4A 条件を満たすインテリジェンスが作成されるまでには時間がかかる可能性があるなど、提供へのメリットが見えづらく、インセンティブの不一致が発生していると推察される。

脅威インテリジェンスの歴史的視座

最後に、脅威インテリジェンスの米国産業界における歴史に焦点を当て、その変遷を分析する。（所説あるが）世界で初めて行われたサイバー脅威インテリジェンス活動とは、『カッコウはコンピュータに卵を産む』[12]という小説という形で描かれた、1980 年代半ばの実話だとされているが、米国産業界の変遷を理解することで、日本の脅威インテリジェンス動向がどの段階にいるか分析する。北米における脅威インテリジェンスの歴史的変遷は図 5 で示す通り、 4 種類の段階で説明できると考えている。

段階	期間	概要
第一段階：黎明期	~2010年頃	・ゼロデイ脆弱性など、Tactical Intelligenceを中心に提供されていた段階
第二段階：「理論」構築	~2013年頃	・脅威インテリジェンスに必要な概念が登場してきた段階
第三段階：普及と「共助」の開始	~2017年頃	・脅威インテリジェンスの普及・流行と、コミュニティによる「共助」が開始してきた段階
第四段階：「公助」の開始	2018年頃~	・政府主導で様々な施策が開始してきた段階

図 **5** 脅威インテリジェンスの歴史的変遷

第一段階： 黎明期

2010 年頃までを黎明期とする。この時期には、「脅威インテリジェンス」というキーワードは登場しているが、その多くがゼロデイ脆弱性などの脆弱性情報、攻撃元 IP アドレスなどを中心とした脅威インテリジェンス、現在でいえば Tactical Intelligence が主に利活用されていた。

第二段階：「理論」構築

2013 年頃までは「理論」構築の時代であり、脅威インテリジェンスに必要な概念が登場している。例えば、脅威インテリジェンスでは重要なキーワードである IOC（Indicator of Compromise）[13]、MITRE ATT&CK フレームワーク[14]、Pyramid of Pain[15]（痛みのピラミッド）といった概念が整理され、実践するツール[16]が登場したのもこの時期である。また、前述で紹介した Mandiant 社の APT-1 レポートが登場したのも 2013 年度であり、理論の提唱とその実践が行われた時代である。

第三段階：普及と「共助」の開始

第三段階は、2017 年度頃までを指す。この頃から、第二段階で登場してきた概念を利用し、脅威インテリジェンスの作成・活用方法が定式化され、脅威インテリジェンスが流行・普及した時期である。実際、各種書籍やトレーニングなどが多数登場したのもこの時期である。

また、同時にコミュニティによる「共助」が開始した時期でもある。2015 年度に米国にて Cybersecurity Information Sharing Act[17]が議会で承認され、官民で情報共有する枠組みが定められたこともあり、ISAC を含む脅威インテリジェンスコミュニティ[18]が形成され、脅威インテリジェンスを利用・交換する組織がより活発に活動し始めた時期である。一方、当時筆者は米国に滞在していたが、脅威インテリジェンスの活用ブームの裏で、脅威インテリジェンス「疲れ」などの声も出始めてきた時期でもある。

また、アトリビューション分析に関する議論が活発に行われた時期でもある。2016 年は、ドナルド・トランプ氏が第 45 代米大統領に就任した歴史的な大統領選挙であったこともあり、当時はサイバー攻撃による選挙介入も話題になっていた。その一例として、DNC（Democratic National Committee）に対する攻撃が APT28 と APT29 による攻撃[19]だと発表され、各社が競うようにアトリビューションを行っていた。その一方、サイバーセキュリティのカンファレンスでは、こうしたアトリビューション分析に関して、False Flag（偽旗）である可能性を考慮すべきと示唆する発表[20]や、民間セクターは「アトリビューションをする必要がないのではないか？」といった指摘[21]が行われている。言い換えれば、脅威インテリジェンスに対する各ステークホルダーの役割・線引きが行われ、アトリビューションの有効性なども指摘

されていた時代である。

第四段階：「公助」の開始

第四段階として、2018 年から現在までを意味する。この段階は、「公助」の開始と位置付けられる。2018 年には、CISA（Cybersecurity and Infrastructure Security Agency）[22]が設立され、KEV（Known Exploited Vulnerability）[23]や Cybersecurity Alerts & Advisory[24]を発表にするなど、政府主導で様々な活動が行われている。また、各種政府機関も様々なガイドライン・ツールの公開[25]を開始している。その代表例として、NSA が開発したマルウェア解析フレームワーク Ghidra[26]があるが、他にも様々なツール[27]を公開している。また、2018 年度以降、FBI でも積極的に APT グループを"Cyber's Most Wanted"[28]で名指ししている。

歴史的変遷からの考察

歴史的変遷からわかる通り、脅威インテリジェンス分野で進んでいる北米産業界でも、公共セクターがステークホルダーとして活動し始めたのは 2018 年前後である。米国でも CISA が設立されて以降、様々なレポート・ツールを公開するなど積極的な情報発信・共有を行っており、その存在感を示している。なお、「公助」においても、CISA のようなトップダウン型アプローチ以外にも、ボトムアップ型アプローチも存在する。その一例として、InfraGard[29]と呼ばれる組織が挙げられる。1996 年に FBI（連邦捜査局）のクリーブランド支局におけるローカルな取り組みとして始まり、その後全米の支局に拡大された組織である。FBI、地方の法執行機関、民間企業や学術機関との連携、情報共有を目的としたプログラムであり、テロ、インテリジェンス、犯罪、サイバーセキュリティについて情報交換が行われている。サイバー犯罪やテロ対策などは、「官のみの対応で重要インフラを防護することは困難である」ことから生まれた組織であり、接点を増やすことにより公共セクターで取得可能な情報を増やす狙いがあると推察される。

一方、日本の状況を鑑みると、執筆時点で民間セクターでの脅威インテリジェンス活用が普及し、「共助」のコミュニティ形成が進んでいる。そのため、北米産業界の歴史に習うのであれば、第四段階である「公助」の支援に移行する時期であると推察される。

最後に

本稿では、脅威インテリジェンスの利活用、および公共セクターの関与が限定的である構造について、機能軸と歴史軸で紐解いてきた。機能軸から見てわかる通り、脅威情報を収集し、サイバー防御に活用する脅威インテリジェンスは、民間セクターで積極的に活用されている。一方、エコシステムからみると、目的・インセンティブの観点から、公共セクターの関与は限定的であることを指摘した。また、歴史軸からすると、日本は「共助」が進んできており、今後「公助」へと移行する可能性を指摘した。

様々な分析からみてわかる通り、公共セクターと民間セクターがそれぞれ脅威インテリジェンスに求める目的は異なる。そのため、情報の流通を活性化したり、情報に一定の品質を担保したりする目的で、公共セクターがエコシステムに関与することは重要だが、民間セクターと同じことをする必要はないと考えられる。むしろ、公共セクターが脅威インテリジェンスを必要とする理由は、政策・国防の側面が強く、当該目的に必要な情報を収集できる仕組み・態勢を構築することが重要であると考えられる。

ハイブリット戦など、国防の観点でサイバー攻撃が果たす役割は増えており、アトリビューション技術を中心に、脅威インテリジェンスはより重要な技術となる。本稿が、その一助になれば幸いである。

（２０２４年４月２６日：脱稿）

[1] 脅威インテリジェンスのより詳細な理論・応用については、拙書『脅威インテリジェンスの教科書』（石川朝久 著）を参照のこと。

[2] “Security Intelligence: Introduction (pt 2)”：https://www.sans.org/blog/security-intelligence-introduction-pt-2-/

[3] “New TTPs observed in Mint Sandstorm campaign targeting high-profile individuals at universities and research orgs”：https://www.microsoft.com/en-us/security/blog/2024/01/17/new-ttps-observed-in-mint-sandstorm-campaign-targeting-high-profile-individuals-at-universities-and-research-orgs/

[4] “Staying ahead of threat actors in the age of AI”：https://www.microsoft.com/en-us/security/blog/2024/02/14/staying-ahead-of-threat-actors-in-the-age-of-ai/

[5] 『シャーマン・ケント　戦略インテリジェンス論』（シャーマン・ケント著／並木均 監訳／熊谷直樹 訳）

[6] “DOD Dictionary of Military and Associated Terms”：https://www.supremecourt.gov/opinions/URLs_Cited/OT2021/21A477/21A477-1.pdf

[7] “The Red Team Handbook: The Army's Guide to Making Better Decisions”：https://usacac.army.mil/sites/default/files/documents/ufmcs/The_Red_Team_Handbook.pdf

[8] “Mandiant Exposes APT1 – One of China's Cyber Espionage Units & Releases 3,000 Indicators”：https://www.mandiant.com/resources/blog/mandiant-exposes-apt1-chinas-cyber-espionage-units

[9] アトリビューション分析は、「攻撃グループを特定する技術」であり、その技術的手法については、拙書『脅威インテリジェンスの教科書』（石川朝久 著）を参照のこと。国家によるアトリビューションの動向・変遷は、安全保障戦略研究（第 3 巻 2 号）に掲載された『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』や NIDS コメンタリー（第 179 号）に掲載された『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・諸国のアトリビューション連合と SolarWinds 事案対応』を参照のこと。

[10] C4 モデルは、Timo Steffens 氏の著書“Attribution of Advanced Persistent Threats: How to Identify the Actors Behind Cyber-Espionage”で提唱されたモデルである。本図は、当該書籍を参考に筆者が作成した。

[11] 共有、公表、報告、連絡と類似した概念があるが、「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）で公開された『サイバー攻撃被害に係る情報の共有・公表ガイダンス』を参照のこと。

[12] 『カッコウはコンピュータに卵を産む』（クリフォード・ストール著／池央耿 訳）は、実話をもとにした小説である。1980 年代半ば、勤務先のローレンス・バークレー研究所のコンピュータシステムへの侵入に気付いた著者 Clifford Stoll 氏が、警察当局と共同で捜査を進め、ハニーポットを設置して、KGB に雇われたドイツ人ハッカーを謙虚に追い込む実話である。

[13] IOC（Indicator of Compromise）とは「侵害指標」と訳され、「実際に発生した攻撃情報を特定するための技術的特性情報」を意味する。ファイルのハッシュ値、接続先の IP アドレスやドメイン名、マルウェアが被害端末上に残すレジストリ、一時ファイルなどの痕跡などが含まれる。なお、IOC の概念が登場したのを本稿では第二段階（~2013 年頃）としているが、IOC という用語の歴史を紐解けば、筆者が文献を確認できる限り、2003 年に発売された『Incident Response & Computer Forensics, 2nd Ed.』（Kevin Mandia, Chris Prosise, Matt Pepe）に登場しており、当該書籍は APT1 レポートで有名な Mandiant 社の創業者である Kevin Mandia 氏によって書かれている。その後、筆者が確認できる限り Black Hat DC 2007、M-Trends 2010 などでも記載されている。一方、Mandiant 社は OpenIOC と呼ばれる IOC を取り扱う XML スキーマを提唱し、Open IOC 1.0 Editor、IOC Finder などのツールを発表しており、実用化が進んだと考えられる。より詳細を知りたい方は、Richard Bejtlich 氏の記事（https://taosecurity.blogspot.com/2018/11/the-origin-of-term-indicators-of.html）と Lenny Zeltser 氏の記事（https://zeltser.com/indicators-of-compromise-entering-the-mainstream/）を参照のこと。

[14] MITRE ATT&CK（Adversarial Tactics, Techniques & Common Knowledge）とは、攻撃者が利用する攻撃手法、専門用語では TTPs（Tactics、Techniques、Procedures）を整理したフレームワークである。2013 年（https://attack.mitre.org/resources/faq/）より開発が開始し、現在も更新が続いている。本フレームワークを利用することで、攻撃手法を共通言語として取り扱うことが可能となる。

[15] Pyramid of Pain（痛みのピラミッド）は、David Bianco 氏が提唱した概念で、IOC の種類を分類・階層化し、攻撃グループの活動を検出するために使用できる指標の種類と、当該指標を利用して攻撃者を予防・検知できた場合に攻撃グループに与える影響の関係性を示した概念である。詳細は、ブログ（https://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html）を参照のこと。

[16] その代表例として、IOC Finder（https://fireeye.market/apps/211408）や OpenIOC Editor（https://fireeye.market/apps/211404）などが挙げられる。

[17] “Cybersecurity Information Sharing Act”：https://www.cisa.gov/sites/default/files/publications/Cybersecurity%20Information%20Sharing%20Act%20of%202015.pdf

[18] 厳密には、FS-ISAC などの ISAC（Financial Sector Information Sharing and Analysis Center）は、1998 年 5 月に署名された大統領令（PDD-63）により重要インフラ業界に対し、業界別に組織を設立し、脅威情報や脆弱性情報を共有することを要請されたことに始まっている（https://www.nationalisacs.org/about-isacs）。一方、2015 年には、オバマ大統領（当時）による大統領命令 13691 により、安全保障省（DHS）の監督のもとに、ISAO（Information Sharing and Analysis Organization）と呼ばれる情報共有組織を構築することを推奨され、重要インフラ・業界という範囲以外にも情報共有コミュニティの設置を推進する方針が打ち出された（https://obamawhitehouse.archives.gov/the-press-office/2015/02/13/executive-order-promoting-private-sector-cybersecurity-information-shari）。この手の情報共有コミュニティの変遷の詳細は、拙書『脅威インテリジェンスの教科書』（石川朝久 著）の 6 章を参照のこと。

[19] 一例として、ThreatConnect 社の発表“Does a BEAR Leak in the Woods?”（https://threatconnect.com/blog/does-a-bear-leak-in-the-woods/）が挙げられる。カンファレンスでの発表は、Youtube（https://www.youtube.com/watch?v=9qi5T8B4-nU）を参照のこと。

[20] NSA や DISA などに勤務経験がある Dr. Mark Kuhr の講演“Leveraging Threat Intel Disinformation Campaigns”（https://archive.org/details/shmoocon2017_Leveraging_Threat_Intel_Disinformation_Campaigns）を参照のこと。架空のシナリオとして、偽情報などを利用しながらアトリビューションを別の攻撃グループに仕向けるテクニックを紹介している。

[21] Kaspersky Lab の講演 “Wave Your False Flags! Deception Tactics Muddying Attribution in Targeted Attacks”（https://www.youtube.com/watch?v=BpmxYIKvRRs）を参照のこと。

[22] https://www.cisa.gov/news-events/alerts/2018/11/19/cybersecurity-and-infrastructure-security-agency

[23] KEV（Known Exploited Vulnerability）とは、CISA が管理している実際に悪用された脆弱性のカタログ（https://www.cisa.gov/known-exploited-vulnerabilities-catalog）である。

[24] CISA は、攻撃グループの攻撃手法や検知方法などをまとめたレポートを、”Cybersecurity Alerts &

Advisories”（https://www.cisa.gov/news-events/cybersecurity-advisories）として公開されている。

[25] 一例として、NSA（National Security Agency）が発表している”NSA Cybersecurity Advisories & Guidance”（https://www.nsa.gov/Press-Room/Cybersecurity-Advisories-Guidance/）や、2023 年には、アメリカ航空宇宙局（NASA）が”New Space Security Best Practices Guide”（https://www.nasa.gov/general/nasa-issues-new-space-security-best-practices-guide/）を発表している。

[26] Ghidra（https://ghidra-sre.org/）は RSA Conference 2019（https://www.rsaconference.com/Library/presentation/USA/2019/come-get-your-free-nsa-reverse-engineering-tool-3）で発表され、ソースコードも公開されている。

[27] その他公開ツールは、GitHub（https://github.com/orgs/NationalSecurityAgency/repositories）を参照のこと。NSA 以外にもアメリカ陸軍研究所（The U.S. Army Research Laboratory）は、DShell と呼ばれるフレームワーク（https://github.com/USArmyResearchLab/Dshell）を公開している。

[28] “Cyber’s Most Wanted”：https://www.fbi.gov/wanted/cyber/

[29] 『第２１４号コラム：官民連携モデル、InfraGard』：https://digitalforensic.jp/2012/06/28/column214/

PROFILE

石川　朝久

東京海上ホールディングス株式会社 IT 企画部　Lead Cyber Security Architect

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