国家が関与するサイバー攻撃と戦略的脅威インテリジェンスの活用[1]

昨今、外国政府や国家が関与するとみられるサイバー攻撃が多く報じられている。もちろんサイバー攻撃の多くは犯罪者や愉快犯によるものだが、大規模または洗練されたサイバー攻撃の背景には、国家の関与や国家間の地政学的対立があることが多い。軍や情報機関等がサイバー攻撃のために投入するリソース（資金、要員、技術資産等）は単なる犯罪集団や個人のそれを凌駕する。国家が関与するサイバー攻撃グループは「高度で持続的な脅威（Advanced Persistent Threat: APT）」とも呼ばれ[2]、APT は一般的なサイバー攻撃者とは異なる狙い・特徴・背景がある。そのため、一定のリスクマネジメント態勢・サイバーセキュリティ態勢を構築済の一部の企業・組織は、APT に関する脅威情報を収集し、経営・事業戦略、サイバーセキュリティ戦略、マネジメントに反映する「戦略的脅威インテリジェンス（strategic threat intelligence）」を導入・活用していく必要がある。企業・組織の脅威インテリジェンスの生成と活用には、サイバーセキュリティ、自組織や事業戦略に関する理解、外交・防衛・安全保障や経済・産業政策、特定国の政治・経済・社会に関する知見が不可欠である。

1. 国家が関与するサイバー攻撃

（1）国家が関与するサイバー攻撃グループ： 高度で持続的な脅威（APT）

国家が関与するサイバー攻撃といっても、その様態は様々である。①最高指導者による承認と政府機関による直接指揮がある場合、②国家が偽造民間団体、ペーパー企業、金銭的動機に基づく犯罪者等の「代理人」に財政的・技術的・戦術的支援を行い、攻撃を奨励する場合、③国家が「代理人」による攻撃を看過する場合（消極的関与）等様々である。

では、どの国家がサイバー攻撃を行っているのか。極論すれば、ある程度のサイバー能力を持つほぼ全ての国家がサイバー攻撃を行っている可能性がある。米国も同様であり、軍事活動もしくは秘密工作活動の一環として、イランの原子力関連施設の遠心分離機を破壊したマルウェア「スタックスネット（Stuxnet）」（2010 年）は米国とイスラエルによる共同開発と報じられた。

しかし、国家が関与して**外国の民間企業**を攻撃するケースはそれほど多くない。米国のインテリジェンスコミュニティが毎年公開する「世界脅威評価（Worldwide Threat Assessment）」2021 年版は、米国に対するサイバー攻撃を積極的に行う国家として、ロシア、中国、イラン、北朝鮮を名指しで非難している。実際、米司法当局はこれら国家の軍・情報組織や関連する企業・個人を、民間企業へのサイバー攻撃を理由に度々刑事訴追し、米財務省は経済制裁対象に指定している。

2021 年秋に閣議決定予定の次期「サイバーセキュリティ戦略」も「中国・ロシア・北朝鮮は、サイバー能力の構築・増強を行い、その関与が疑われるサイバー攻撃を行っているとみられている」との認識を示す[3]。また、これまで日本政府は、中国および北朝鮮による個別のサイバー攻撃を非難してき

[1] 本稿の「3.戦略的脅威インテリジェンスの活用」は、外部研究プロジェクト（公益財団法人笹川平和財団主催「サイバーインテリジェンス研究会」）における専門家ら（青木眞夫氏、大澤淳氏、梶浦敏範氏、武智洋氏、田中達浩氏、長迫智子氏、政本憲蔵氏）との議論を反映したものである。
[2] APT は必ずしも国家関与のサイバー攻撃グループに限定されないが、APT の多くは国家の関与が疑われ、本稿では APT＝国家関与のサイバー攻撃グループとする。
[3] サイバーセキュリティ戦略本部「次期サイバーセキュリティ戦略の骨子」2021 年 5 月 13 日、4 頁。

た。松本光弘警察庁長官は 2021 年 4 月 22 日の記者会見で、宇宙航空研究開発機構（JAXA）を始めとする約 200 の国内企業・組織に対するサイバー攻撃は「Tick と呼ばれるサイバー攻撃集団によって実行」され、その背景に「山東省青島市を拠点とする中国人民解放軍戦略支援部隊ネットワークシステム部第 61419 部隊が関与している可能性が高い」と結論付けた[4]。これは日本独自の捜査として、初めて外国政府によるサイバー攻撃を特定したものであった（こうした攻撃元の特定は「アトリビューション」と呼ばれる）。また、2017 年 5 月に世界中で拡散した身代金要求型ウイルス（ランサムウェア）「WannaCry」については「事案の背後に、北朝鮮の関与があったことを非難」した[5]。

国家が関与するサイバー攻撃グループは「高度で持続的な脅威（Advanced Persistent Threat: APT）」とも呼ばれ、サイバーセキュリティ各社・各国の関心度は高い。そのため各社・各国は詳細な調査を行い、特定した攻撃者グループに独自の APT 名称を与えている。表 1 は、国家組織の関与が強く疑われるサイバー攻撃グループである。これらは少なくとも被害を受けたと主張する国家政府が名指しで批判している攻撃グループである（なお関与が疑われた国は、サイバー攻撃や攻撃グループへの関与を否定している）。

■表 1：国家組織の関与が強く疑われるサイバー攻撃グループ（一部抜粋）

関与が疑われる国家組織	サイバーセキュリティ企業等が命名した APT 名称 注 1	概要・関与が疑われる事案
中国人民解放軍（PLA）戦略支援部隊ネットワークシステム部第 61419 部隊	• Tick（Symantec） • Bronze Bulter（Secureworks） • RedBaldkNight（Trend Micro）	山東省青島市を拠点とし、日本・韓国を標的としているグループ（2015 年 12 月以前は総参謀部第三局第四局と位置付けれていた）。 JAXA、慶應義塾大学、一橋大学、大手電機メーカー等が被害にあったとされる。
中国国家安全部（MSS）天津市国家安全局	• APT10（Mandiant/FireEye） • Stone Panda（CrowdStrike） • Red Apollo（PwC） • Potassium（Microsoft）	フィッシングメール攻撃、標的企業が契約する IT サービスの保守・運用委託先経由での各国民間企業への攻撃に関与。2018 年 12 月、米陪審が APT10 関係者を訴追。日米英加独豪 NZ 政府も中国を非難。
ロシア連邦軍参謀本部情報総局（GRU）特殊技術総センター（74455 部隊）	• Sandworm • Voodoo Bear（CrowdStrike） • BlackEnergy Actors	情報収集（諜報）、破壊・妨害活動、影響力行使活動等の多岐に渡る任務に従事し、米大統領選に関する機密情報暴露（2016 年）、ウクライナ停電（2014、15 年）、マルウェア「NotPetya」（2017 年）等に関与。
北朝鮮偵察総局（RGB）121 局	• Lazrus Group（Kaspersky 他）注 2 • HiddenCobra（米政府） • Labyrinth Chollima（CrowdStrike） • ZINC（Microsoft） • Appleworm（Symantec） • Black Artemis（PwC） 等	米エンターテイメント企業への攻撃・脅迫（2014 年）やランサムウェア「WannaCry」（2017 年）に関与。ラザルスは、北朝鮮によるサイバー攻撃全般を行う組織の総称として用いられることもある。

（注 1）（）内は命名した企業名を指す。上記表では、セキュリティ各社・各機関が特定した APT を便宜的に同じカテゴリーに分類しているが、完全に一致するとは限らない。また現時点では公開されていない APT アクターも数多く存在する。
（注 2）北朝鮮 RGB およびラザルスの範囲が各セキュリティ会社によって幅がある。詳細は脚注 20 を参照。
出典：米・英政府、EU 理事会、エストニア対外情報庁、公安調査庁、各セキュリティ会社の公表資料から作成。

[4] 国家公安委員会「国家公安委員会委員長記者会見要旨」（2021 年 4 月 22 日）。
[5] 外務省「米国による北朝鮮のサイバー攻撃に関する発表について（外務報道官談話）」2017 年 12 月 20 日。この他、日本政府は「中国を拠点とする APT10 といわれるサイバー攻撃グループ」を非難している。この指摘は厳密にいえば、中国政府の関与を直接明示していないが、米英政府の公式声明に言及していることから、中国政府との関連を示唆していると考えてよいだろう。外務省「中国を拠点とする APT10 といわれるグループによるサイバー攻撃について（外務報道官談話）」2018 年 12 月 21 日。

（2）APT の特徴

APT も一般的なサイバー攻撃と同様の戦術・技術・手順を採用することもある。しかし、APT は、一般的なサイバー攻撃や攻撃者とは異なる特徴がいくつかある。

□APT のサイバー攻撃・活動は、国家の政策や国家間関係の影響を受ける

APT によるサイバー攻撃・活動は、その国の政策を強く反映する。APT は国家にとって優先順位の高い政策課題・領域に焦点を絞って諜報活動・情報収集活動、産業振興、外貨獲得等のためのサイバー攻撃・活動を行うことが多い。

ただし、同一国内の複数の APT は必ずしも協力している訳ではなく、複数の APT が競争しながら、同一の標的にアクセスすることもある。米民主党全国委員会（DNC）や日本の大手総合電機メーカーでは、それぞれロシアと中国の複数の APT が侵入していると報じられた[6]。

□APT にとって、サイバー攻撃は唯一の手段ではない

APT は、犯罪者等による一般的なサイバー攻撃とは異なる戦術・技術・手順を採用するだけではなく、場合によってはサイバー攻撃以外の手段を用いることがある。なぜなら、APT にとってサイバー攻撃は主要な手段かもしれないが、目標達成のための唯一の手段ではない。例えば、以下は APT による攻撃や活動として確認された手法である。

- 国外の協力者を通じて標的の近くに攻撃用のサーバを契約する [7]
- 国外の標的に物理的に近づき（工作員を派遣し）、不正に無線を傍受する [8]
- 国内の標的（外資企業の事業拠点）の IT マネージャを協力者（内部犯）に仕立て、機密情報を不正に入手する [9]
- 標的（外国企業）のエンジニアを学術講演の名目で国内に招聘し、金銭を贈与し、見返りに営業秘密の提供を求める [10]

□APT は、当該国内で（合法的だが不当に）民間企業のデータにアクセスできる場合がある

一般論として、多くの政府・法執行機関は、当該国に設置されたデータセンターや情報資産に合法的にアクセスする権限を有している（中国インターネット安全法（網絡安全法）等）。APT は、こうした権限を不当に行使することで、当該国に設置されたデータにアクセスする恐れがある。近年、各国では、個人情報保護や治安維持を目的に、個人データ・通信データ・その他機密情報を第三国に移転することを禁止・制限する法律が制定されている。こうした「データローカライゼーション」の動きは、APT にとってプラスとなり、企業は不当な「ガバメントアクセス」の可能性を常に考慮する必要がある[11]。

---

[6] Dmitri Alperovitch, “Bears in the Midst: Intrusion into the Democratic National Committee,” CrowdStrike, June 15, 2016; 須藤龍也「標的の分野・時期は多様：三菱電気 4 集団がサイバー攻撃」朝日新聞、2020 年 1 月 21 日。

[7] 「JAXA などに大規模なサイバー攻撃 中国人民解放軍の指示か」NHK ニュース、2021 年 4 月 20 日。

[8] Genmaj. O. Eichelsheim, Defence Intelligence & Security Serivise, Ministy of Defense, the Netherlands, “GRU close access cyber operation against OPCW,” October 4, 2018.

[9] U.S. District Court for the Southern District of California, *Indictment*, Case No.13CR3132-H, October 25, 2018.

[10] U.S. District Court for the Southern District of Ohio, *Indictment*, Case No.1:18CR-00043, April 4, 2018.

[11] また、当該国にデータセンターが物理的に設置されていなくとも（日本にデータセンターが設置されていても）、特定国では当該国を本拠地とする法人が所有する国外のデータやサーバへのアクセスを要求することができる（米国 CLOUD 法等）。つまり、日本国内に設置された米企業のデータセンターは米政府によるアクセスの恐れがあるが、これ（民主主義国家のガバメントアクセス）を日本企業がリスクと捉えるかどうかは別の問題である。

2. 民間企業が懸念すべき国家関与のサイバー攻撃

具体的にどのような産業・民間企業が APT の標的となっているのか。表 2 は過去の実際の攻撃事例から、民間企業が懸念すべき国家関与のサイバー攻撃の様態（例）と標的となりやすい産業をまとめたものである。

■表 2：民間企業が懸念すべき国家関与のサイバー攻撃の様態（例）

分類	概要	標的となりやすい産業
① 産業スパイ	自国の産業振興・商業的優位性獲得のため、外国企業の営業秘密や知的財産を窃取するもの。	全ての企業（競争力のある営業秘密や知的財産を持つ全ての企業）
② 大量の個人データの窃取	自国の産業振興もしくは諜報活動（対象国全国民の情報収集）のため、大量の個人データを窃取するもの。	大量の個人データを保有する事業者（特に国民全体の包括的なデータを保有する医療、社会保障、金融（銀行、保険）、通信、航空等）
③ 金銭の窃取	金融機関や仮想通貨取引所等の金融資産を窃取するもの。	金融機関、仮想通貨取引所 等
④ サービス妨害・破壊活動	重要インフラ事業者によるサービス提供を妨害したり、企業の経済活動全般を停止せしめるもの。	重要インフラ事業者（特に、電力、通信、運輸、金融）等

出典：筆者作成。

（1）産業スパイ

民間企業が第一に懸念すべき APT 攻撃の様態は産業スパイ、すなわち外国政府機関が自国の産業振興・商業的優位性獲得のために、サイバー攻撃を通じて営業秘密（trade secret）や知的財産を窃取するものである。

産業スパイ目的のサイバー攻撃は 2010 年以降の米中間の外交上の最優先事項の一つである。米司法当局は、これらの攻撃者（中国人民解放軍、国家安全部、民間企業関係者等）を刑事訴追している。米国の説明によれば、2015 年 9 月 25 日、米中首脳会談でバラク・オバマ（Barack H. Obama）大統領と習近平（Xi Jinping）主席は、米中両国が「（自国の）企業・商業セクターに商業的優位性を提供することを意図して」、サイバー活動を通じて営業秘密や知的財産を窃取しないこと等に合意した[12]。しかし、この合意は破綻しているとの見方が支配的である。このことが、ドナルド・トランプ（Donald J. Trump）政権下で表面化した米中対立の要因の一つとなっている[13]。

この類で有名な攻撃グループは、2015 年米中合意以前から指摘されていた「APT1」である。この攻撃グループは 2013 年 2 月、米セキュリティ会社「マンディアント（Mandiant）」（後にファイア・アイ社が買収）が明らかにしたもので、同社は APT1 が中国人民解放軍総参謀部第 3 部第 2 局（61398 部隊）と密接な関連があると結論づけた。同社の報告書によれば、2006 年以降少なくとも 141 の組織

[12] The White House, Office of the Press Secretary, “FACT SHEET: President Xi Jinping’s State Visit to the United States,” September 25, 2015.
[13] 米通商法 301 条調査によれば、米国の認識では、中国政府による不公正な政策・方法を通じた技術獲得・競争優位性獲得を問題視し、その手段の一つが「商業的優位性の獲得のため、サイバー攻撃を通じた知的財産や営業秘密の窃取」である。Office of the United States Trade Representative (USTR), Executive Office of the President, *Findings of the Investigation into China’s Acts, Policies, and Practices Related to Technology Transfer, Intellectual Property, and Innovation under Section 301 of the Trade Act of 1974*, March 22, 2018, p.3, 5.

や機関が被害に遭い、2011 年 1 月から 2013 年 1 月に活動が活性化した[14]。2014 年に公開された米起訴状では、原子力、太陽光、鉄鋼、非鉄金属等の企業が被害にあったことが明らかになった。

中国人民解放軍内では、米国産業界へのサイバー攻撃は「61398 部隊」が、日本産業界へのサイバー攻撃は「61419 部隊」が担ってきたと考えられている。前述のとおり、警察庁長官は人民解放軍 61419 部隊がハッカー集団「Tick」に関与し、約 200 の日本企業・組織を標的にしてきた可能性が高いと結論付けた。ある脅威分析の専門チームは、61419 部隊が各国のアンチウイルスソフトを購入したことを確認し、同部隊がアンチウイルスソフトによる検出を回避しようとしているか、リバースエンジニアリングによってこうしたソフトウェアの（未知の）脆弱性を探している可能性が高いと分析する[15]。

これらに加えて、多くの日本企業が被害にあったとされるのが「APT10」である。米司法当局は 2018 年 12 月 21 日、民間企業等を標的とするサイバー攻撃グループ「APT10」のメンバーで、中国国家安全部の下部組織である天津市国家安全局と協力してきた 2 名を刑事訴追すると発表した。日本も初めて中国発のサイバー攻撃を公式に非難し、外務省報道官は「かかる攻撃を断固非難」という極めて強い表現の声明を発表した。日米だけではなく、英独加豪 NZ が同様の声明を発表している。

こうしたサイバー攻撃の標的は、中国の産業振興政策と関係があると考えられている。専門家らは、APT1 と APT10 が標的とした産業は、それぞれ中国の「戦略的新興産業（第 12 次 5 カ年計画（2011-15 年））（2010 年 10 月発表）と中国製造 2025「10 大重点産業分野」（2015 年 5 月）と親和的であると分析している[16]。

また最近では、米英政府のサイバーセキュリティ機関が、新型コロナウイルス感染症（COVID-19）のワクチンの開発情報等が、APT によるサイバー攻撃の標的となっていると警鐘を鳴らした[17]。さらに、米司法当局は 2020 年 9 月、全世界 100 以上の組織を標的としたサイバー攻撃に関与したとして、中国国内を発信源とするとみられる「APT41（FireEye）」（または「BARIUM（Microsoft）」「Winnti（Kaspersky 等）」「Wicked Panda（CrowdStrike）」）関連のハッカー4 名を起訴した。

企業価値やビジネスの影響が懸念されるためか、企業はサイバー攻撃により営業秘密が漏洩しても、必ずしもその事実を公開していない。そのため、報道される以上のサイバー攻撃被害があると考えてよいだろう。競争力のある営業秘密や知的財産を持つ全ての企業が潜在的標的である。

（2）大量の個人データの窃取

サイバー攻撃による個人情報漏洩は毎日のように発生している。その多くは、クレジットカード等の情報を盗んだり、フィッシングメールを送付するためのメールアドレスを入手することが狙いだ。だが、APT による個人データ窃取は、（(1)と同様の）産業振興や諜報活動があると考えられている。最近では、米国の政府機関・民間企業に対するサイバー攻撃と個人データ搾取が確認された。

- 2015 年 2 月　米医療保険大手アンセム（Anthem）：約 8,000 万人の顧客情報の漏洩
- 2015 年 6 月　米国人事管理局（Office of Personal Management: OPM）：約 2,200 万人の現役および元連邦政府職員のデータの漏洩（セキュリティクリアランス取得者の情報を含む）
- 2017 年 9 月　米信用調査会社大手エクイファックス（Equifax）：米国人口の半数近くに相当

[14] Mandiant, *APT1: Exposing One of China's Cyber Espionage Units*, February 2013.
[15] Insikt Group, "China's PLA Unit 61419 Purchasing Foreign Antivirus Products, Likely for Exploitation," *Recorded Future*, May 5, 2021.
[16] Mandiant, *Op. Cit.*; PwC & BAE Systems, O*peration Cloud Hopper: Exposing a Systematic Hacking Operation with an Unprecedented Web of Global Victims*, April 2017.
[17] National Cyber Security Centre, "UK and US security agencies issue COVID-19 cyber threat update," April 8, 2020.

する約 1 億 4,300 万人分の顧客情報の漏洩

- 2018 年 11 月　米大手ホテルチェーン・マリオットグループ傘下のスターウッド（Starwood）：約 3 億 2,700 万人の旅券番号を含む約 5 億人の顧客情報の漏洩

上記 4 事案について、ウィリアム・バー（William P. Barr）米司法長官は中国の APT によるものと明言している。バー長官によれば、その狙いは個人データを機械学習・深層学習に利用することに加え、諜報活動である[18]。諜報活動という点で、異なる個人データベースを相互に参照することで、政治家・政府高官・軍や諜報機関関係者・経営者等のハイバリューターゲットを含む米国人とその重要な動きを把握することができるとの評価もある[19]。国民全体の包括的なデータを保有する医療・社会保障、金融（特に銀行、保険）、通信、航空等はこの類の潜在的標的と考えて良い。

（3）金銭の窃取

APT によるサイバー攻撃のうち、明らかな金銭的動機に基づくものは多くない。しかし、国際機関や諸外国から厳しい経済制裁下にある場合、外貨獲得のためにサイバー攻撃を行う国もある。国連の専門家パネル報告書によれば、北朝鮮は、核・ミサイル開発のため、仮想通貨取引所等にサイバー攻撃を仕掛け、2019 年から 2020 年 11 月までの期間に約 3 億 1640 万米ドルを稼いだ[20]。この他、国際銀行間通信協会（SWIFT）、各国の中央銀行・金融機関、オンラインカジノ等を主な標的とし、継続的なサイバー攻撃を行っている。

（4）サービス妨害・破壊活動

最後は、重要インフラ事業者によるサービス提供を妨害したり、企業の経済活動全般を停止せしめたりする類のサイバー攻撃である。各国により、サイバーセキュリティ上の重要インフラ産業は異なるものの、日本では 14 分野が重要インフラに指定されている（表 3）。幅広いセクターが重要インフラ指定されているが、電力、通信、金融、運輸は特に国家関与のサイバー攻撃のリスクが高いと考えられている。実際に重要インフラのサービス停止に至らないまでも、攻撃の準備活動や侵入活動も報告されている。具体的には、2013 年 3 月の韓国の金融・放送事業者の一部におけるサービス中断、2015 年 12 月および 2016 年 12 月のウクライナでの広域停電、2016 年 3 月以降の米電力網への侵入活動等である[21]。2013 年 3 月の韓国のケースは企業内のパッチ管理システム経由でマルウェアが配付されたものであり、ソフトウェアの更新機能を悪用したものであった。これは、近年まれにみる深刻な被害をもたらした米ソーラーウィンズ（SolarWinds）社製の監視ソフトウェア経由でのサイバー攻撃（2020 年 12 月）と同様の手法といえる[22]。

重要インフラ以外の民間企業もこの類の攻撃の被害に遭っている。2017 年 6 月に、ウクライナを中心に全世界で被害が発生した「NotPetya」は外形的には身代金を要求する「ランサムウェア」に見える。しかし、攻撃者（ロシア GRU74455 部隊[23]）が担っているであろう役割、ウクライナに焦点を当

---

[18] Department of Justice, “Attorney General William P. Barr Announces Indictment of Four Members of China’s Military for Hacking into Equifax,” February 10, 2021.
[19] Richard J. Harknett & Max Smeets, “Cyber Campaigns and Strategic Outcomes,” *Journal of Strategic Studies*, March 2020, pp.1-34.
[20] *Final report of the Panel of Experts submitted pursuant to resolution 2515 (2020)*, UN doc.: S/2021/211, March 4, 2021, p.56. なお、北朝鮮国家偵察局と関係するサイバー攻撃集団は「ラザルス（Lazarus）」と呼ばれることがあるが、ラザルスの範囲は注意する必要がある。詳細は、「国家が支援するランムウェア：2017 年の WannaCry と NotPetya の意図に関する分析　後編」国際情報ネットワーク分析 IINA、笹川平和財団（2021 年 4 月 8 日）。<https://www.spf.org/iina/articles/kawaguchi_03.html>
[21] 電力インフラへのサイバー攻撃は「ブラックアウトがもたらす社会的影響と企業の対策」リスクマネジメント最前線、2020-No.17（2020 年 9 月）、4-5 頁。<https://www.tokiorisk.co.jp/publication/report/riskmanagement/pdf/pdf-riskmanagement-344.pdf>
[22] ただし、ソーラーウィンズ社製品を介したサイバー攻撃の狙いは破壊活動ではなく、諜報・情報収集活動と考えられている。
[23] 米英政府は 2018 年 2 月、NotPetya をロシア軍によるものと発表した。勿論、ロシア政府はこれを否定している。さらに米大陪審の起訴状（2020 年 10 月 15 日付）は、攻撃者をロシア連邦軍参謀本部情報総局（GRU）の「74455 部隊」と断定した。United States District Court for the Western District of Pennsylvania, *Indictment*, Criminal No.20-316, October 15, 2020, p.1.

てた感染経路、金銭的動機とは考えられないマルウェア設計、ウクライナとロシアの政治状況を踏まえると、NotPetya はウクライナに対する破壊活動（の実験）か威力偵察の類と考えるべきである[24]。

■表 3：日本・米国・英国・EU におけるサイバーセキュリティ分野の重要インフラ指定産業

日本 14 分野	米国 16 分野	英国 13 分野	EU7 分野[注]
情報通信	Information Technology Communication	Communications	Digital Infrastructure
金融	Financial Services	Finance	Banking
クレジット			Financial market infrastructures
航空	Transportation Systems	Transport	Transport
空港			
鉄道			
物流			
	Nuclear Reactors, Materials, and Waste	Civil nuclear	
ガス	Energy	Energy	Energy
石油			
電力			
	Dams		
水道	Water and Wastewater Systems	Water	Drinking water supply and distribution
政府・行政サービス（地方公共団体を含む）	Government Facilities	Government	
	Emergency Services	Emergency services	
医療	Healthcare and Public Health	Health	Health sector
化学	Chemicals	Chemicals	
	Critical Manufacturing		
	Commercial Facilities		
	Defense Industrial Base	Defence	
		Space	
	Food and Agriculture	Food	

[注] 欧州連合「ネットワークおよび情報システム指令（Network and Information Systems Directive）」第 4 条 4 および付属書Ⅱにいう「基幹サービス運営者（operator of essential services）」を指す。なお、同指令では OES の他、第 4 条 5 および付属書Ⅲにいうオンラインストア、検索エンジン、クラウドコンピューティング等の「デジタルサービス運営者（digital service）」にも一定の責務を示している。

※1 各セクターの下位単位として指定されたサブセクターは割愛している。各国の重要インフラは必ずしも一致しないが、並び順を変更して、便宜上の対応関係を示している。

※2 重要インフラ指定の経緯は各国により異なる。例えば、日本の重要インフラは情報セキュリティ・サイバーセキュリティの観点から指定されたものであるが、米国は 9.11 テロ直後、より広範な国土安全保障の文脈で重要インフラを再検討し、これらの重要インフラを大統領政策指令（Presidential Policy Directive: PPD）21 該号（2013 年 2 月 12 日）でサイバーセキュリティの観点で確認した結果である。

出典：以下の公開資料から作成。

（日本）サイバーセキュリティ戦略本部「重要インフラの情報セキュリティ対策に係る第 4 次行動計画（第 4 次行動計画）」2020 年 1 月 30 日改定　<https://www.nisc.go.jp/active/infra/outline.html>

（米国）Cybersecurity and Infrastructure Security Agency, Department of Homeland Security, “Critical Infrastructure Sectors,” Last Updated at October 21, 2020.　<https://www.cisa.gov/critical-infrastructure-sectors>

（英国）Centre of the Protection of National Infrastructure, “Critical National Infrastructure,” Last Updated at April 20, 2021.<https://www.cpni.gov.uk/critical-national-infrastructure-0>

（EU）European Commission, The Directive on Security of Network and Information Systems, July 2016, Annex II. < https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016L1148>

[24] 詳細は、「国家が支援するランムウェア：2017 年の WannaCry と NotPetya の意図に関する分析　前編」国際情報ネットワーク分析 IINA、笹川平和財団（2021 年 3 月 30 日）。<https://www.spf.org/iina/articles/kawaguchi_02.html>

3. 戦略的脅威インテリジェンスの活用

APT は一般的なサイバー攻撃とは異なる狙い・特徴・背景がある。そのため企業は、APT に関する脅威情報を収集・分析し、経営・事業戦略、サイバーセキュリティ戦略、マネジメントに反映する「戦略的脅威インテリジェンス（strategic threat intelligence）」を導入・活用していく必要がある。

戦略的脅威インテリジェンスとは、自社の経営・事業戦略、サイバーセキュリティ戦略、マネジメントに関する判断・意思決定に活用できるよう加工された情報である。具体的には、サイバー攻撃の実行者の属性、攻撃の目的や動機、脅威や攻撃の動向・トレンド、地政学的背景等である。懸念すべき国家の戦略的関心や安全保障・産業振興政策も重要な戦略的脅威インテリジェンスである。

ここでは、（1）戦略的脅威インテリジェンス活用の前提条件、（2）戦略的脅威インテリジェンスの特徴（詳細）、（3）自組織にとっての戦略的脅威インテリジェンスの生成・活用プロセスの例を紹介する。

（1）戦略的脅威インテリジェンス活用の前提条件

戦略的脅威インテリジェンスを活用するにあたっての前提条件は、既にサイバーセキュリティ態勢が一定程度整備されている（一定程度成熟している）ことである。サイバーセキュリティ態勢が十分ではない企業・組織は、戦略的脅威インテリジェンスを活用する前にやるべきことが多数ある。具体的には、サイバーセキュリティ確保のための十分な投資、セキュリティを考慮した物理的・論理的なデータ資産配置・アクセス制御、24 時間 365 日の監視体制を含む平時および有事の態勢整備、定期的かつ多様な脆弱性診断、役員や従業員への教育・演習、内部犯対策等である。

組織のサイバーセキュリティ成熟度[25]をどこまで高めれば、戦略的脅威インテリジェンスを活用できるかは、一概には判断できない。しかし一例を示すのであれば、(a) 情報システム部門から独立し、機能しているサイバーセキュリティ部門が存在、(b) これを所掌するトップマネジメント（最高情報セキュリティ責任者（Chief Information Security Officer: CISO）等）が存在する場合、戦略的脅威インテリジェンスの活用を検討してもよいだろう。

（2）戦略的脅威インテリジェンスの特徴（詳細）

「脅威インテリジェンス（threat intelligence）」とは、特定の目的のためのコンテクストに関連付けられ、分析・解釈が加えられたもので、意思決定・行動に活用できるものである。これらの点で、脅威インテリジェンスは、完全なローデータで議論・解釈の余地が一切ない「脅威データ（threat data）」や脅威データを整理・抽出・構造化した「脅威インフォメーション（threat information）」とは区別される[26]。

インテリジェンスは、目的に応じていくつかの階層がある。脅威インテリジェンスは表 4 のとおり、戦略的脅威インテリジェンス（strategic threat intelligence）、作戦的脅威インテリジェンス（operational threat intelligence）、戦術的脅威インテリジェンス（tactical threat intelligence）に大別されうる（これ以外の分類・整理方法もある）。

戦略的脅威インテリジェンスは、経営者が能動的な意思決定を行うための、中長期で個別性の高

25　一例として、米エネルギー省「サイバーセキュリティ能力成熟度モデル（Cybersecurity Capability Maturity Model:C2M2）」や米国防総省の「サイバーセキュリティ成熟度モデル認証（Cybersecurity Maturity Model Certification: CMMC）」があげられる。電力や金融など、特定産業に特化した成熟度モデルも存在する。

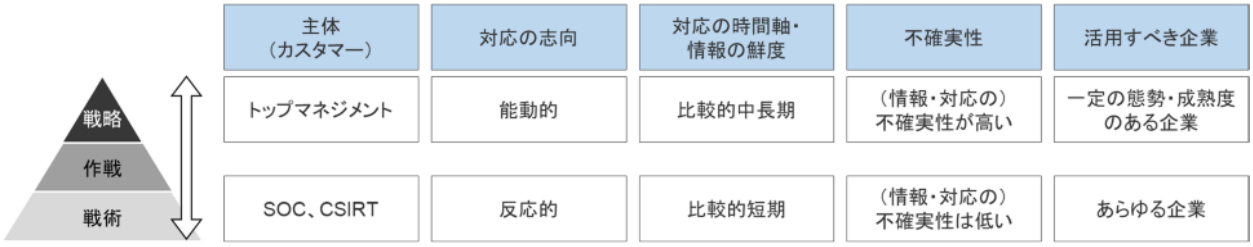
26 “Threat Intelligence, Information, and Data: What Is the Difference?” *Recorded Future*, March 8, 2017.

い、しかし一定の不確実性があるインテリジェンスである。また戦略的脅威インテリジェンスは、各業界・各組織の文脈に依存するため、それを記述し、組織間で交換する際の形式・標準が広く普及していない[27]。前述のとおり、こうした脅威インテリジェンスを活用する場合、当該組織に一定程度のサイバーセキュリティ態勢が確保されていることが前提となるが、作戦的・戦術的脅威インテリジェンスはどのような組織でも活用すべきだろう（図 1）。

■表 4：戦略的・作戦的・戦術的脅威インテリジェンスの概要

分類	概要	例
戦略的脅威インテリジェンス strategic threat intelligence	経営戦略・事業戦略、サイバーセキュリティ戦略に活用できるもの。 サイバー攻撃の Who や Why に焦点。	攻撃者の属性・組織構成、攻撃の狙い・動機、政策との関連性・地政学的背景等。
作戦的脅威インテリジェンス operational threat intelligence	リスク評価、リスク低減計画の立案・実行、インシデント対応等に活用できるもの。サイバー攻撃の How や Where に焦点。	攻撃手法、攻撃対象、攻撃ベクター、脆弱性情報、戦術・技術・手順（TTP）等。
戦術的脅威インテリジェンス tactical　threat intelligence	脅威の検知・検出・対処に活用できる機械可読性（machine-readable）のあるもの。サイバー攻撃の What に焦点。	マルウェアのハッシュ値、攻撃元の IP アドレス等の侵害指標（Indicator of Compromise: IoC）等。

■図 1：戦略的・作戦的・戦術的脅威インテリジェンスの特徴



出典：表 4 および図 1 ともに、“Threat Intelligence, Information, and Data: What Is the Difference?,” *Recorded Future*, March 8, 2017; Home Office Digital, Data and Technology, The UK Government, *Cyber Threat Intelligence in Government: A Guide for Decision Makers & Analysts*, Version 2.0, March 2019, p.16.および研究プロジェクト「サイバーインテリジェンス研究会」の議論（注 1 を参照）から筆者作成。

（3）自組織にとっての戦略的脅威インテリジェンスの生成・活用

多くの組織にとって、戦略的脅威インテリジェンスを生成・活用するためには、外部機関による脅威レポートを活用することが現実的である。ただし、自組織にとっての戦略的脅威インテリジェンスと広く公開される戦略的脅威インテリジェンスは区別する必要がある。

民間セキュリティベンダやアンチウイルスソフトベンダ（具体的な企業名は表 1 を参照）は継続的に詳細な戦略的脅威インテリジェンスに関するレポートを公開している。また米国土安全保障省サイバーセキュリティ・インフラセキュリティ庁（Cybersecurity and Infrastructure Security Agency:

[27] 他方、作戦・戦術レベルの脅威インテリジェンスは交換・記述方法が一定程度、標準化されている。例えば、共通脆弱性評価システム（Common Vulnerability Scoring System: CVSS）、脅威情報構造化記述形式（Structured Threat Information eXpression: STIX）、検知指標情報自動交換手順（Trusted Automated eXchange of Indicator Information: TAXII）、サイバー攻撃観測記述形式（Cyber Observable eXpression: CybOX）は脅威インテリジェンスの交換・記述の標準形式である。サイバー脅威インテリジェンスの交換については、英連邦内部向けガイダンスに概略が記載されている。Foreign, Commonwealth & Development Office (FCDO), Guidance: Cyber-threat intelligence information sharing guide, March 8, 2021. <https://www.gov.uk/government/publications/cyber-threat-intelligence-information-sharing/cyber-threat-intelligence-information-sharing-guide>

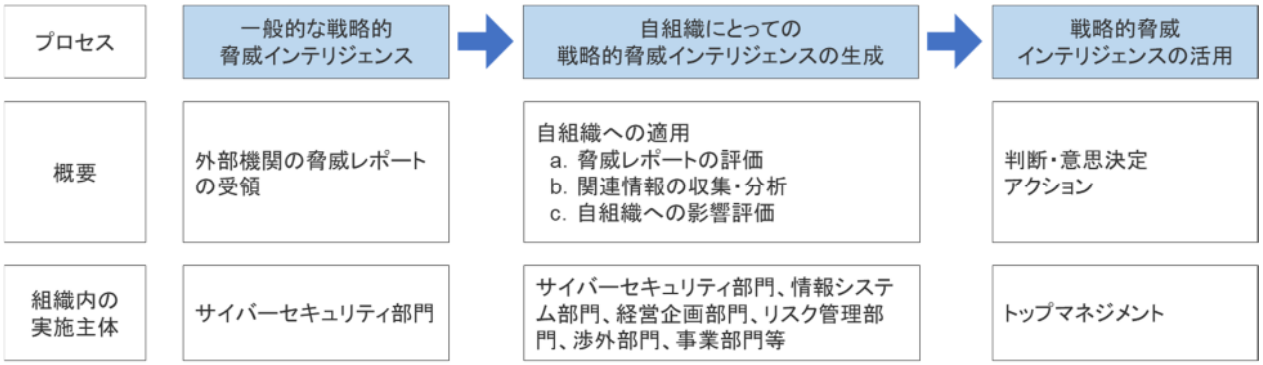
CISA）や英国家サイバーセキュリティセンター（National Cyber Security Centre: NCSC）等の政府機関も戦略的脅威インテリジェンスを公開することがある。

外部機関による脅威レポートは一般的な意味での「戦略的脅威インテリジェンス」と呼べるが、個別組織の「戦略的脅威インテリジェンス」とは呼べない場合がある。なぜなら、外部機関の脅威レポートは「政府組織・民間企業全般」や「特定業界」をカスタマーとするが、個別組織の戦略的脅威インテリジェンスはその組織の置かれた事業環境や課題が加味される必要があるからである（もちろん、個別組織や事業ベースのインテリジェンスを提供するサービスはある）。

つまり、外部機関の脅威レポートを受領しても、直ちに自組織の「戦略的」判断・対策に使えるものとは限らない。戦略的脅威インテリジェンスの活用は「作戦的」「戦術的」脅威インテリジェンスほど自動化されたプロセスではなく、外部の脅威レポートを自組織に必要な「戦略的脅威インテリジェンス」に昇華させるためには、組織内での一定のプロセスが必要である。こうした意味では、外部機関からもたらされる脅威レポートは、自組織内で戦略的脅威インテリジェンスを生成するトリガーといえる。

「戦略的脅威インテリジェンス」の生成・活用のためには、少なくとも、組織内での（a）外部機関の脅威レポートの評価、（b）関連情報の収集、（c）自組織への影響評価が必要である（図 2）。

■図 2：自社にとっての戦略的脅威インテリジェンスの生成・活用



出典：筆者作成。

a. 脅威レポートの評価

各組織のサイバーセキュリティ部門は、外部機関の脅威レポートの内容の確からしさ・妥当性を精査し、スクリーニングする必要がある。優れた外部機関の脅威レポートは、判断結果の蓋然性や判断根拠となる情報源の信頼性について確度を評価した上で、記述方法やその基準（例えば、「ほぼ確実」という表現は何を意味するのか等）を明らかにしている。

サイバーセキュリティ部門は、別の外部機関による脅威レポートを相互参照したり、外部のサイバーセキュリティ専門家や専門機関の見解を求め、脅威レポートの妥当性を評価することが重要である。実際、著名な脅威レポートであっても、別の専門家からすれば、「レポートのこの箇所は妥当ではない」と評価されるケースもある。なおセキュリティ各社・各機関の脅威レポートは、一見、同じサイバー攻撃グループについて言及していたとしても、各社・各組織が呼んでいる攻撃グループは完全に一致しているわけではなく、若干の差異もあるため、注意が必要である[28]。

[28] John S. Davis II, et al., *Stateless Attribution: Toward International Accountability in Cyberspace*, Santa Monica, CA: RAND Corporation, 2017, pp.20-21.

b. 関連情報の収集

次いで、外部機関の脅威レポートが指摘するサイバー攻撃グループや攻撃キャンペーンについて、APT そのものは勿論、APT に課せられた任務・役割、APT の目的・動機、標的となっている国・産業・企業、サイバー攻撃以外の手法等の周辺情報を収集する必要がある。

その際、サイバーセキュリティ部門や情報システム部門等のＩＴ部門に加えて、経営企画部門、リスク管理部門、渉外部門等の非ＩＴのコーポレート部門、関係する事業部門の関与が必要となる。この時点で、脅威インテリジェンスは必ずしもサイバーセキュリティに限定されない場合がある。

APT の場合、当該国の中長期関心・利益、当該国と日本の地政学的対立や背景、当該国の安全保障・産業振興政策等を把握することが不可欠である。これにはサイバーセキュリティの専門家ではなく、外交・防衛・安全保障や経済・産業政策、特定国の政治・経済・社会に関する専門家が必要となり、自組織で完結できない場合もある。

c. 自組織への影響評価

最後に、特定のサイバー攻撃キャンペーンが自組織の経営・事業やサイバーセキュリティにどのような影響を与えるかを評価・検討する。財務、広報、研究、開発、生産・製造、調達、営業、保守、サービス等の機能やバリューチェーン、複数事業を行う組織であれば各事業ドメイン、事業展開国・地域への影響を検討する必要があるだろう。その結果、例えば、特定国で特定事業を行うことは（許容できない程）リスクが高いと評価されたり、短期的に特定事業や情報インフラ・資産のサイバーリスクが高まっていると評価されたりするかもしれない。

現時点で、APT によるサイバー攻撃は減少していく見込みは極めて低く、一部の国家や政府機関は国家目標を達成するため、ますますサイバー攻撃やサイバー活動に依存していくだろう。サイバーセキュリティ分野で「相手が APT ならば仕方ない」という考え方は全く通用しない。またサイバー攻撃に限定せずとも、リスクマネジメントは経済安全保障や地政学リスクを考慮しなければならない状況となっている。一定のリスクマネジメント態勢・サイバーセキュリティ態勢を構築している企業・組織は、APT に関する脅威情報を収集し、経営・事業戦略、サイバーセキュリティ戦略、マネジメントに関する意思決定・判断に活用するため、戦略的脅威インテリジェンスを積極的に導入・活用していく必要がある

以上

2021 年 5 月 15 日脱稿　［2021 年 5 月 18 日発行］

東京海上日動リスクコンサルティング株式会社
TOKIO MARINE NICHIDO
To Be a Good Company
ビジネスリスク本部 兼 戦略・政治リスク研究所 プリンシパルリサーチャ 川口貴久 https://www.tokiorisk.co.jp/consultant/tkawaguchi.html
〒100-0004 東京都千代田区大手町 1-5-1 大手町ファーストスクエア ウエストタワー23 階
Tel. 03-5288-6594　Fax. 03-5288-6626
https://www.tokiorisk.co.jp/

