2026 年 3 月 30 日

サイバー攻撃と複合的脅威
―日本の対応課題―

山本マクシミリアン拓馬

1 はじめに

日本の公的機関および民間企業を狙ったサイバー攻撃は後を絶たない。例えば、2024 年 10 月には親露ハッカー集団「Noname057(16)」による大規模な DDoS 攻撃が行われた[1]。同グループによる攻撃が疑われるものの中には、選挙妨害を狙った可能性がある事例も含まれている。さらに 2024 年末から 2025 年年始にかけては、金融機関をはじめとした重要インフラに対する DDoS 攻撃が再度発生した。しかし、攻撃主体は声明を出しておらず、公開情報からではその正体を特定できていない。2025 年のアサヒビールやアスクルを狙ったランサムウェア攻撃は、業務停止だけでなく、情報流出の可能性も指摘されている[2]。

こうしたサイバー攻撃の事例は一例に過ぎず、攻撃主体の目的や意図によって手法は多様である。また、技術的な脆弱性だけでなく、不注意や心理的な弱点といった人間の脆弱性を利用する手法も存在する。「サイバー攻撃」という言葉は便利で報道でも広く使われているが、その一方で必要以上の不安を生み、実態とは異なるイメージを与えてしまう可能性がある。

本稿では、「サイバー攻撃」とは何を指すのかを、手段と目的の関係に着目して整理する。また、偽情報工作や政治工作など他領域の偽情報工作や政治工作といった他領域の手法との複合によって日本に及び得る影響と、その際に検討すべき課題について論点を提示する。

2 筆者の立場

ここで、サイバー攻撃や情報工作を中心とした話題に触れるが、筆者の立場を明らかにしたい。本稿では、サイバー攻撃と情報工作は近い領域で展開されるものではあるものの、同一の領域で行われるものとしては見なしていない。

例えば、マーティン・リビッキ（Martin Libicki）は情報戦(Information Warfare)を Command-and-control warfare(C2W), Intelligence-based warfare (IBW), Electronic warfare (EW), Psychological warfare (PSYWAR), Hacker warfare, Economic information warfare (EIW), そして Cyberwarfare の 7 種類に分類している[3]。なお、リビッキの枠組みにおいて、現代のサイバー攻撃に最も近い概念は第 5 類の「Hacker warfare」であり、第 7 類の「Cyberwarfare」は より広範で他 6 類には収まらない、（当時における）将来の情報空間における脅威全般を指す概念として位置づけられている。 アメリカの国防総省も当初、情報戦争（Information Warfare）の概念のもとでサイバー戦や心理戦を包括的に扱っていたが、情報作戦（Information Operations）

論を経て、サイバー空間作戦は独自のドクトリン（JP 3-12）として分離された。すなわち、かつては同一の枠組みに包含されていたサイバー戦と心理戦が、制度的にも別個の領域として位置づけられるに至ったのである。サイバー攻撃が機械情報の窃取・改ざん・機能停止を目的とするのに対し、情報工作は人間の行動や認知に直接影響を及ぼす点で大きく異なる。したがって、本稿ではこの考えに基づき、サイバー攻撃と情報工作は別の領域で行われているものとして扱う。

3 サイバー攻撃はいかにして行われるか

サイバー攻撃は、何を目的とし、何を意図しているかによって攻撃方法が異なる。米国のロッキード・マーティン社がまとめた「サイバー・キルチェーン」モデルにおいては、偵察（Reconnaissance）、武器化（Weaponization）、運搬（(Delivery）、運用（Exploitation）、インストール（Installation）、C2（Command and Control）、目的の実行（Actions on Objectives）の 7 段階にまとめている[4]。米国の MITRE 社がまとめた MITRE ATT&CK においては、より概念的にまとめたサイバー・キルチェーンとは対照的に、より詳細な戦術や攻撃技術が記されている[5]。

中でも、「偵察」段階では、機械的・組織的な脆弱箇所を把握することが主眼となる。対象のサーバーへパケットを送信してシステムの構成を把握する技術的偵察に加え、対象人物に直接コンタクトして情報を引き出すソーシャル・エンジニアリングも用いられる。後者は米国の大手企業や政府機関への侵入を数々行ったハッカーであるケビン・ミトニック（Kevin Mitnick）が多用した古典的手法であり、MITRE ATT&CK の偵察フェーズにおいてもフィッシングによる情報収集として体系化されている。攻撃者はこうして得た情報をもとに攻撃ツールや方法を検討し、サイバー攻撃を実行するのである。

「サイバー攻撃」といっても、その内容は多岐にわたる。サーバーの処理能力を一時的に低下させる DDoS 攻撃、盗聴・情報の窃取をする中間者攻撃など、様々である。これらの攻撃は金銭、政治的主張、情報の窃取・破壊、社会的混乱といった目的によって、使用する手段が異なる。例えば、金銭目的であれば、不正なリンクや添付ファイルをクリックさせることでマルウェアを侵入させ、身代金を要求するランサムウェア攻撃、あるいはクレジットカード情報を窃取するフィッシング攻撃が一般的である。政治的主張を発信する目的であれば、DDoS 攻撃を特定の組織や政府の Web サイトに仕掛け、攻撃グループが事前または事後に政治的メッセージを伴った声明を出す手法が用いられる。社会的混乱をもたらすことを目的とする場合には、選挙をはじめとした国家的イベントに合わせてサイバー攻撃を行い、あるいは虚偽の情報とサイバー攻撃を連動させることで、社会の不安や混乱を効果的に拡大する手法がとられることがある。無論、目的は単一ではなく複数存在する場合がある。サイバー攻撃の目的と対応する主要な種類（手段）を整理したものは表 1 のとおり。

なお、サイバー対処能力強化法において頻繁に使用されている「能動的サイバー防御（Active Cyber Defence：ACD）」は、国や地域によって定義が異なるものの、基本的にはこの攻撃の準備段階において何らかの無害化措置を行い、未然に防ぐものである。

では、社会的混乱をもたらすような攻撃においては、どのようなものがあるのか、次節で検討する。

表１　主要なサイバー攻撃の目的と種類（手段）

目的	種類（手段）
妨害	DDoS 攻撃（分散型アクセス拒否型攻撃）など
盗聴	中間者攻撃
窃取	標的型攻撃、フィッシング、ディレクトリトラバーサルなど
改ざん	SQL インジェクションなど
破壊	ワイパー攻撃など

筆者作成

4 社会的混乱をもたらすサイバー攻撃

前節では、サイバー攻撃の手段と目的の関係を整理した。本節では、とりわけ「社会的混乱」をもたらすことを企図した、あるいは結果的にそれを引き起こしたサイバー攻撃の事例を、国外・国内の双方から検討する。

なお、ここでいう「社会的混乱」とは、サイバー攻撃によるシステムの停止や情報の窃取といった直接的・技術的な被害にとどまらず、国民の間に不安・不信・恐怖が拡散し、社会機能や政治過程に対する信頼が毀損される状態を指す。重要なのは、技術的被害そのものが甚大でなくとも、情報工作や社会的文脈との連動によって、その影響が認知領域において増幅されうるという点である。

例えば、2007 年 4 月から 5 月にかけて、エストニアはソ連時代の記念碑「ブロンズの兵士」の移設を契機として、22 日間にわたる大規模な DDoS 攻撃を受けた。攻撃対象は、政府機関、議会、主要銀行、報道機関、インターネットサービスプロバイダなど広範に及んだ。特に銀行のオンラインサービスが数週間にわたり利用不能となり、国民生活に直接的な影響を与えた。この事例が注目されるのは、サイバー攻撃が単体で行われたのではなく、ロシア政府高官による敵対的な政治的発言、経済的圧力措置、そしてエストニア国内のロシア系住民による街頭抗議活動と同時並行的に展開された点にある。技術的には DDoS 攻撃というサービス妨害に過ぎないが、政治的・社会的文脈と組み合わさることで、エストニア社会全体に不安と混乱が広がった。ロシア政府は関与を否定し、攻撃主体の帰属は法的に確定されていないが、NATO 加盟国を含む多数の国が、組織的な関与を示唆する見解を示している。この事件を契機として、NATO はタリンにサイバー防衛協力センター（CCDCOE）を設立し、サイバー攻撃に対する国際的な法的枠組みの議論が本格化した。エストニアの事例は、国家的な文脈における「サイバー攻撃＋政治的圧力＋社会的動揺」の複合的脅威の原型として、今日においても広く参照されている[6]。

ウクライナやジョージアにおいても、サイバー攻撃と認知領域の撹乱などを利用した事例が報告されており、本研究委員会が扱っている台湾においても、2024 年 1 月 13 日の台湾総統選挙に際し、中国に紐づくとされる APT グループおよび影響工作（IO）アクターによる大規模な複合的活動が観測された。米国のサイバーセキュリティ企業 Trellix の報告によると、選挙前日の 24 時間で台湾

の組織に対する悪意のあるサイバー活動が倍増し、1 月 11 日の 1,758 件から 1 月 12 日には 4,300 件以上に急増した。攻撃対象は主に政府機関、警察、金融機関であった[7]。

情報工作の側面では、Microsoft の調査により、中国に関連するグループが生成 AI 技術を用いて偽のニュースキャスターによるニュース映像を作成し、選挙に影響を与えようとしたことが確認された。これは国家アクターが AI 生成コンテンツを外国の選挙への介入に使用した、Microsoft が確認した初めての事例であった。さらに、与党 DPP（民主進歩党）の候補者・頼清徳氏を標的とした AI 生成のミーム、ディープフェイク動画、捏造された「ハック・アンド・リーク」型の情報流出も展開された[8]。

注目すべきは、台湾がこれらの複合的脅威に対して「社会全体での対応（whole-of-society response）」で臨んだ点である。政府機関、独立系ファクトチェック組織、メディアリテラシー教育の三層構造により、選挙は大きな混乱なく実施された。この台湾の経験は、サイバー攻撃と情報工作の複合的脅威に対する防御の成功例として、日本にとっても示唆に富むものである。

我が国においても、2024 年 10 月 14 日から 16 日にかけて、親露ハクティビスト集団 NoName057(16) および Russian Cyber Army Team が、日本の組織に対して DDoS 攻撃を実施した。この攻撃は、10 月 11 日にロシア外務省が日本の防衛費増大や米国主導の軍事演習への参加について懸念を表明したことに呼応するものであった。攻撃対象のうち、半数は港湾・造船を中心とする物流・製造業であったが、残る主要な標的は政府機関や政治組織であり、与党である自由民主党のウェブサイトも含まれていた[9]。与党への攻撃に関しては、衆議院議員総選挙の公示日に行われ、事実上の海外勢力からの選挙妨害の試みがあったと言える。大勢に影響はなかったものの、官房副長官の青木一彦氏は記者会見で「公正な選挙は民主主義の根幹をなすものだ。公正な選挙を害する行為はいかなる組織、団体、個人であれ断じて容認できない」とコメントしている[10]。

こうした一連の攻撃からは、サイバー攻撃に情報操作や心理的影響を伴わせ、社会的混乱を誘発する手法がうかがえる。今回の日本での事例では、与党サイトへの攻撃が衆議院議員総選挙の公示日に重なったものの、投票操作や選挙手続きの中断といった深刻な事態には至らなかった。一方で、ここでは詳細には触れないが、AI を用いた影響工作も確認されており、今後はサイバー攻撃と組み合わさる形でより大規模な干渉が行われる可能性もある。では、こうした混乱の抑止や被害の最小化に向けて、日本はどのような対応を検討すべきなのだろうか。

5 日本の今後の対応

このような脅威に立ち向かうための提言や枠組みにおいては、国内外で熟議されたものが複数存在し、本研究委員会が使用した「ハイブリッド脅威コンセプトモデル」もその 1 つだと言える[11]。

一方で、現行制度にも依然として多くの課題が残されている。サイバーセキュリティに関しては、2022 年 12 月に閣議決定された安全保障関連 3 文書（国家安全保障戦略、国家防衛戦略、防衛力整備計画）に基づく『サイバー対処能力強化法』において、能動的サイバー防御（ACD）が国家全体の戦略として拡大され、自衛隊および警察などの対処能力は確かに強化されている一方、同法で官民連携を行う上での人間の脆弱性をいかにカバーするのか。経済安全保障推進法や特定機密保護法、重要経済安保情報保護活用法などで強化されているが、かえって組織の内部脅威が高まるリスクや、民間にどこまでの情報を迅速に共有できるかといった課題も残されている。

情報工作への対処に関しては、防衛省情報本部（DIH）が情報戦への対応を強化しつつあり、偽情報の収集・分析体制や専門部署の新設、AI を活用した公開情報の自動収集・分析機能の整備が 2027 年度までに進められている[12]。しかし、これらはあくまで収集・分析および戦略的コミュニケーション（カウンターナラティブの発信）に重点を置くものであり、偽情報そのものを直接排除・無害化するための法的権限や専門組織は、公開情報の限りでは整備されていない。国内のプラットフォーム上で流通する偽情報に対しては、被害を受けた個人や組織がプロバイダに対して発信者情報開示請求等を行うなど、個別の法的手段に依拠せざるを得ず、国家レベルの情報工作に対する迅速な対処は依然として課題である。

この様に、日本全体として最新の枠組みや考え方に基づき、脅威による被害抑止、あるいは脅威そのものを排除するためのプランや、実務的な職務にあたる組織の存在および能力に乏しい。とはいえ、国家サイバー統括室（NCO）は NISC から改組されたばかりであり、高市政権においては内閣情報調査室を国家情報局として改組する動きが出ている。今そこにある危機に日本政府として取り組む姿勢は見え始めている。しかし、組織改編はあくまで器の整備であり、その実効性は、運用の具体化と、領域を横断した統合的な対処能力の構築にかかっている。

冒頭で述べたように、「サイバー攻撃」という包括的な用語は便利である一方、手段・目的・主体の違いを覆い隠し、対処の優先順位を曖昧にするリスクを孕んでいる。本稿で示したとおり、現実の脅威はサイバー攻撃単体で完結するものではなく、情報工作や政治的圧力と複合的に組み合わさることで、その影響は認知領域において増幅される。こうした脅威の構造を正確に理解することこそが、適切な対処の前提条件である。制度の整備と並行して、脅威の実態に対する国民的な理解の深化が求められている。

---

[1] NETSCOUT ASERT, "DDoS Attacks against Japan," NETSCOUT Blog, October 17, 2024, www.netscout.com/blog/asert/ddos-attacks-against-japan.

[2] アサヒグループホールディングス株式会社「サイバー攻撃被害の再発防止策とガバナンス体制の強化について」2026 年 2 月 18 日、www.asahigroup-holdings.com/newsroom/detail/20260218-0101.html；アスクル株式会社「ランサムウェア感染によるシステム障害発生によるご注文受付停止のお知らせとお詫び（第 1 報）」2025 年 10 月 19、https://pdf.irpocket.com/C0032/w4ok/STuh/ai44.pdf；アスクル株式会社「情報流出に関するお知らせとお詫び （ランサムウェア攻撃によるシステム障害関連・第 7 報）」2025 年 11 月 11 日、https://pdf.irpocket.com/C0032/lAG8/UMnd/Mnlw.pdf。

[3] Martin C. Libicki, "What Is Information Warfare? (ACIS Paper No. 3)," National Defense University, Institute for National Strategic Studies, May 1995, permanent.fdlp.gov/lps14211/www.ndu.edu/inss/strforum/sf_28/forum28.html.

[4] Lockheed Martin, "The Cyber Kill Chain," www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html, accessed March 10, 2026.

[5] MITRE Corporation, “MITRE ATT&CK®," https://attack.mitre.org, accessed March 10, 2026.

[6] Rain Ottis, "Analysis of the 2007 Cyber Attacks against Estonia from the Information Warfare Perspective," *Proceedings of the 7th European Conference on Information Warfare and Security*, Academic Publishing Limited, 2008, pp. 163-168, https://ccdcoe.org/uploads/2018/10/Ottis2008_AnalysisOf2007FromTheInformationWarfarePerspective.pdf.

[7] Aria An, "Cyberattack on Democracy: Escalating Cyber Threats Immediately ahead of Taiwan’s 2024 Presidential Election," Trellix Advanced Research Center, February 13, 2024, www.trellix.com/blogs/research/cyberattack-on-democracy-escalating-cyber-threats-immediately-ahead-of-taiwan-2024-presidential-election/.

[8] Clint Watts, "Same Targets, New Playbooks: East Asia Threat Actors Employ Unique Methods," Microsoft Threat Analysis Center (MTAC), April 4, 2024, blogs.microsoft.com/on-the-issues/2024/04/04/china-ai-influence-elections-mtac-cybersecurity/.

[9] NETSCOUT ASERT, "DDoS Attacks against Japan”.

[10] 「自民党 HP にサイバー攻撃の可能性　官房副長官が言及」日本経済新聞、2024 年 10 月 17 日、

https://www.nikkei.com/article/DGXZQOUA1730V0X11C24A0000000/。
[11] The European Centre of Excellence for Countering Hybrid Threats, “The landscape of Hybrid Threats: A conceptual model,” 2021, pp. 9-14, https://www.hybridcoe.fi/wp-content/uploads/2021/02/conceptual_framework-reference-version-shortened-good_cover_-_publication_office.pdf; 中曽根平和研究所海洋安全保障研究委員会『最終報告 台湾有事抑止のための対応要領及び多国間抑止態勢の構築―不可欠なハイブリッド戦対処』中曽根平和研究所、2026 年 3 月 2 日、14-18 頁、https://www.npi.or.jp/research/data/npi_policy_maritime_security_20260302.pdf.
[12] 防衛省『令和 7 年版 防衛白書』2025 年、258 頁