第９章　デジタル時代の経済安全保障

包括的なサイバー防衛戦略の構築を急げ

Guest Speaker

大澤 淳（おおさわ・じゅん）
公益財団法人 中曽根康弘世界平和研究所　主任研究員

1971 年生。慶應義塾大学法学部 1994 年卒、同大学大学院法学研究科修士課程 1996 年修了（法学修士）。1995 年世界平和研究所研究員、2009 年同主任研究員、2014 年～2016 年内閣官房国家安全保障局参事官補佐(サイバー安全保障担当)、2017 年中曽根康弘世界平和研究所主任研究員。現在、鹿島平和研究所理事、独立行政法人情報処理推進機構(IPA)情勢研究室長・統括情報分析官、笹川平和財団上席フェローを併任。2004 年～2006 年外務省国際情報統括官組織専門分析員、2007 年～2009 年外務省総合外交政策局外交政策調査員、2013 年米国ブルッキングス研究所招聘客員研究員、2012 年～2016 年政策研究大学院大学（GRIPS）客員研究員、2017 年～2019 年内閣官房国家安全保障局シニアフェローを併任している。専門は国際政治学（戦略評価、サイバー安全保障）、公共政策（政策分析）。最近の著作に、『ウクライナ戦争はなぜ終わらないのか』（共著、文春新書、2023 年 6 月）、『新領域安全保障』（共著、Wedge、2024 年 1 月）、「ハイブリッド戦争と認知領域の戦い」戦略研究学会『戦略研究』Vol. 34 （2024 年 3 月）。

■　この章の問題意識　■

2000 年代に入って、サイバー空間は陸、海、空、宇宙に続く「第五の作戦領域だ」と言われるようになり、サイバー空間における安全保障問題が注目されるようになった。それから 20 年が経過。サイバー攻撃の巧妙化・高度化が続き、最近ではロシアによるウクライナ侵攻、さらに中東における紛争においてもサイバー攻撃が最重要のツールの一つとして使われるなど、ハイブリッド戦争（有事と平時の境目の曖昧化）やグレーゾーン事態（軍事と非軍事の境目の曖昧化）が現実化し、リアル空間とサイバー空間が一体化する中でサイバー空間における安全保障のあり方が検討課題となっている。

サイバー空間を巡る安全保障関連の事態が複雑化する中、デジタル時代の安全保障戦略を考える上では、技術、外交、軍事など、様々な領域の知見を総動員しつつ、各領域の知恵を縦軸に、戦略的思考を横軸としながら、立体的に検討することが求められている。こうした問題意識の下、デジタル時代の経済安全保障が抱える課題や今後の検討の方向性について展望する。

聞き手＝**谷脇 康彦**　デジタル政策フォーラム 代表幹事

世論戦、心理戦、法律戦に勝ち抜けるか

谷脇　国家安全保障会議（NSC：National Security Council）[1]とその事務局である国家安全保障局（NSS：National Security Secretariat）[2]が内閣に設置されたのが 2014 年。私自身は、内閣サイバーセキュリティセンター（NISC：National center of Incident readiness and Strategy for Cybersecurity）[3]の前身である内閣官房情報セキュリティセンター（NISC：National Information Security Center）の副センター長として、サイバーセキュリティ基本法の策定に携わったりしていました。2013 年 12 月に閣議決定された国家安全保障戦略[4]の中では宇宙空間やサイバー空間といった国際公共財（グローバルコモンズ）のセキュリティ防御が初めて取り上げられました。当時から大澤さんとはいろいろと意見交換させてもらってきましたが、あれから約 10 年。サイバー空間の環境は大きく変化し、脅威も複雑化・多様化しています。この間の環境変化について、どのようにとらえていますか。

大澤　一番大きな事件は、2022 年に始まった**ロシアのウクライナ侵攻**です。それまで日本では、サイバー攻撃で重要インフラが破壊されたり、政府機関のネットワークが攻撃を受けたりということは、遠い国の話であり、頭の体操ぐらいの受け止め方にとどまっていました。ところが、ロシア・ウクライナ戦争によって、多くの人たちが現実を目の当たりにしました。

ウクライナの地方都市へのミサイル攻撃の直前には地方政府へのサイバー攻撃によって対応力を奪うというように、サイバー攻撃が軍事作戦にがっちり組み込まれているのです。いわゆる「情報戦」も激しさを増しています。例えば「ゼレンスキー大統領が逃亡した」とか「ゼレンスキー大統領が降伏を宣言した」といった、ウクライナ国民の士気を砕くような偽情報が流布されたりしています。現代戦では、サイバー空間における情報戦が明確な意図をもって用意周到に行われているということが明らかになり、現実的な有事の脅威になりました。

そして、ロシアのウクライナ侵攻の前後から、**台湾有事への危機感**が急速に高まったことも見逃せません。台湾有事でもサイバー攻撃が多用されることは間違いありません。中国の人民解放軍は、「**情報化戦争**」や「**三戦：世論戦、心理戦、法律戦**」というコンセプトで、サイバー攻撃や情報戦を戦争と一体的に行うハイブリッド戦略を持っています。ロシアがウクライナでやっているように、ミサイルや砲弾で攻撃する前に情報戦やサイバー攻撃を仕掛け、自軍に優位な状況を作る戦略です。日本が中国からのサイバー攻撃を受ける蓋然性は非常に高まっています。有事となれば、重要インフラを止め、不可逆的な破壊を行うといった烈度の高いものになる。厳しい現実を見ることにならざるを得ません。

もう一つの特徴的変化は、**平時と有事の境の「グレーゾーン」**の事案が急増していることです。ロシアの国家主体が関与していると見られる武力行使の一歩手前のランサムウェア（身代金ウイルス）

攻撃が観測されています。米国で地方自治体の機能が止まったり、緊急通報用電話「911」がかからなくなったりということが頻発しています。2021 年には、米国最大の石油パイプライン会社「コロニアルパイプライン」がランサムウェア攻撃を受け 5 日間にわたって操業を停止し、首都ワシントン周辺のガソリンスタンドが営業を停止、航空機の燃料供給が滞る安全保障上の緊急事態となりました。日本でも、犯人は特定されていませんが、2021 年に徳島県つるぎ町立半田病院がランサムウェア攻撃を受け、電子カルテシステムや請求システムが停止、2022 年には大阪急性期・総合医療センターが同様の被害に遭ったことが大きく報じられました。市民生活に直接的に悪影響が出るサイバー攻撃が増えているのです。

これらが、金欲しさの犯罪行為なのか、偵察行為のようなグレーゾーン事案なのか、ロシアや中国がやっているのか、明確に特定できないのですが、この 10 年間で件数が非常に増えてきているということは感じております。

大澤 淳　中曽根康弘世界平和研究所 主任研究員

「2027 年台湾有事」が変革ドライバーに

谷脇　台湾有事の話が出ました。日本の国家安全保障戦略[5]でも台湾有事への対処、準備というものをしっかりしないといけないという意識が強く現れている。軍事攻撃の前にサイバー攻撃が事

前に仕掛けられるということを考えると、既に臨戦態勢に入っているという見方もできると思います。他方、大澤さんのような専門家が抱く危機感と一般国民の認識の間に、大きなズレがあるように感じます。

大澤　2020 年頃でしょうか、米国ワシントン D.C.界隈の軍関係者やシンクタンク関係者の間では危機感がかなり高まっていました。日本では政府、自衛隊も含めてまだのんびりしていたのですが、アメリカに刺激されるかたちで、自衛隊 OB などが集まって台湾シミュレーションを始めたり、メディアでも台湾有事が取り上げられたりするようになっていきました。台湾に近い先島諸島（宮古列島、八重山列島）では有事における避難計画の具体的な検討も始まっています[6]。2024 年 1 月に石垣島の自衛隊駐屯地を訪問したのですが、地元の危機感は高く、住民から首長さんに「退避計画を早く整備してくれ」というようなプレッシャーがかかっているようです。そうした意味で、一般国民の中でも安全保障に多少なりとも興味関心がある人にはある程度浸透してきたとは思います。

ただし、実際にどういうことが起きるのかという点までは周知が進んでいません。例えば、報道機関のニュース配信が止まってしまうかもしれないとか、政府からの情報発信が届かなくなってしまうかもしれないとか、電力や港湾システムがダウンしてエネルギーや食料の供給が滞るとか・・・。漠然と南西諸島が紛争に巻き込まれるかもしれないという危機感はあるのですが、ハイブリッド戦争によって一般国民が受ける深刻な影響を具体的にイメージできるところまでは至っていないように思います[7]。

谷脇　霞が関（官庁）や永田町（政治）の認識はいかがでしょうか。

大澤　現在の**国家安全保障戦略**を作り始めたのが 2021 年の冬です。その頃には米国から「**2027 年までに台湾有事が起こる恐れがある**」という見方が発信されていましたから、2027 年に照準を当てて戦略検討が進められました。反撃能力の点では射程 1000km 超の中距離巡航ミサイルの配備など、敵の攻撃に耐える抗堪力（こうたんりょく）の点では基地や格納庫の地下化や弾薬の備蓄など、有事が勃発しても最前線を保持できるような対応策が戦略に入りました。

能動的サイバー防御（アクティブサイバーディフェンス）の考え方も盛り込まれています。先制攻撃ではなく、あくまで重大な攻撃のおそれがある場合にこれを未然に排除するという位置付けですが、有事の際に敵のネットワークを止める技術を獲得するという宣言も盛り込まれており、2027 年を念頭に線表が引かれています。

谷脇　10 年くらい前から、国家の関与が疑われるサイバー攻撃が急増しているということが言われ始めていました。そして最近ではサイバー攻撃の攻撃者を特定する「**アトリビューション**」が注目されていて、攻撃を仕掛けてきた国を突き止めて日本政府が直接非難するということも行われるようになっ

てきました。国家の関与が疑われるサイバー攻撃は、どのような状況になっていますか。

大澤　日本にとって懸念すべきは、**ロシア、中国、北朝鮮、イラン**の 4 カ国です。それぞれのサイバー攻撃には特徴があります。

北朝鮮は、核・ミサイル開発、経済制裁への対抗、体制維持のために外貨獲得が必要です。1990 年代までは朝鮮総連を介した日本からの送金がありました。そのルートが閉ざされると、偽ドル札、偽タバコ、麻薬生産など非合法活動で外貨を稼ぎました。2006 年に米国当局が偽造米ドル紙幣への対策を打ってからは、中国からの直接投資などで凌いでいました。そして、ビットコインなどの暗号通貨が流通するようになると、サイバー攻撃で暗号資産を盗む仮想通貨ハッキングに手を染めるようになりました。暗号通貨の取引所が主な標的でしたが、最近では一般の銀行取引や個人のオンラインバンキングなども狙われているようです。**北朝鮮のサイバー攻撃は「金銭目的型」**と言ってよいでしょう。

サイバー攻撃の類型別攻撃主体

金銭目的型：標的型攻撃、脆弱性利用などにより、特定の政府機関、銀行、企業、個人のネットワークに侵入し、不正な送金を行い、またはPC内のデータを暗号化し、解読に身代金を要求する攻撃。

情報窃取型：標的型攻撃（ウィルス付きメール、水飲み場攻撃、ゼロデイの脆弱性利用）などにより、特定の政府機関、企業、団体、個人のネットワーク、PCに侵入し、機密情報、営業情報、特許などを窃取する攻撃。

機能妨害型：DDoS攻撃等の手法により、ネットワークの許容量を超える飽和通信要求によって、サーバー、ネットワークを麻痺させる攻撃。

機能破壊型：標的型攻撃などにより、特定の政府機関、企業、団体、個人のネットワークに侵入し、システム破壊・改ざんを行う攻撃。ネットワーク内のデータ消去・改ざんを目的とするものと、制御系システムを標的として物理的破壊を目的とするものがある。

情報操作型：代理主体(Proxy)等を用いて真の発信者を隠匿たうえで、SNS等に偽ニュースを流布させることにより、対象国（主に民主主義国）における世論操作を目的とした攻撃。選挙結果に影響を与えることを企図していることも。

軍事的サイバー攻撃：軍事攻撃と一体的に行われる機能妨害・機能破壊を目的とした攻撃。電子戦の一環としてC4Iを標的とするものと、軍事行動に影響を与える死活的インフラを標的としたものがある。

ロシアは、ハッカー集団が身代金目的のランサムウェア攻撃をかけていますが、それらの一部には犯罪をカモフラージュにして国家関与の偵察行為を行っているものがあると思います。

中国は「情報窃取型」に特化しています。一つは、知的財産や特許といった機密情報です。最近では半導体のチョークポイント技術（性能やコストを左右する最重要技術）や宇宙関連技術が狙われています。2021 年には、宇宙航空研究開発機構（JAXA）などへのサイバー攻撃に関与した疑いで中国共産党員の男が書類送検されました 。中小企業も攻撃を受けているようです。もう一つは、政府の政策情報です。特に安全保障関係の政策情報を狙ったアクセスが非常に多く観測されています。日本でも、政府の重要ポストを経験した OB の個人用パソコンを集中的に狙った事案が見えてきています。

「**機能妨害型**」というのは、複数のシステムから標的に対して一斉にアクセスをかける DDoS（Distributed Denial of Service）攻撃が主な手法です。ロシアは、ウクライナ侵攻後のこの 2 年間、日米欧の政府ウェブサイト、オンラインバンキング、鉄道予約システムなどに、たびたび攻撃を仕掛けています。

「**機能破壊型**」は、ロシアがウクライナ侵攻で多用しています。重要インフラにマルウェアを連続的に送り込み、機能を停止させることが目的です。北朝鮮も一時期、韓国や米国を標的として行っていましたが最近はほとんど見られず、金銭目的中心になっています。一方、パレスチナのガザ地区におけるイスラム組織ハマスとイスラエルの戦闘が勃発して以降、イラン系のハッカー集団がイスラエル製の機械制御コンピュータ（PLC : Programmable Logic Controller）を狙ってサイバー攻撃を仕掛けています。これによって水道の制御装置が止まるなど、小規模ですが重要インフラでトラブルが起きています。

「**情報操作型**」というのはいわゆる情報戦と呼ばれるものです。サイバー攻撃とは別に考える人も多いのですが、私はこれをあえてサイバー攻撃の範疇に入れています。偽情報、フェイクニュースの流布が情報戦だというイメージがあるのですが、その裏側では政府機関への DDoS 攻撃やメディアのウェブサイト改ざんなどが並行して実行されているのです。合わせて、情報空間を錯乱、攪乱させるサイバー攻撃であると私は考えています。情報操作型はロシアが得意とする手法でしたが、最近中国の動きも目立つようになってきました。台湾、韓国、東南アジア諸国、2023 年からは米国をターゲットにしています。日本に対しては、福島第一原発の処理水放出に関してこのタイプの攻撃を始めています。

ハイブリッド戦、グレーゾーン事態にどう対処するか

谷脇　国家の関与が強く疑われるサイバー攻撃が出てくると、国際法上の扱いが気になります。武力紛争の場合は平時と有事を明確に切り分けた上で有事の国際ルールというものが明確化されていますが、そもそも平時と有事の境目が曖昧なグレーゾーン事態において、しかもキネティックな武力の行使とは異なるサイバー攻撃を国際法上でどう位置付けるのかという点はまだ整理されていないし、非常に難しい問題だと思います。

大澤　武力行使、武力攻撃、国際法上の対抗措置について、平時と有事のサイバー攻撃をどのように整理するのかを笹川平和財団の研究会で議論した時、国際法の先生からは「かなり烈度の高いものでない限り、サイバー攻撃は武力行使の範疇に至らない」という見解が出されました。武力行使ないしはその上の武力攻撃の範疇でないと自衛権の行使ができませんので、すなわちサイバー攻撃を受けても反撃ができないということになってしまいます。ウクライナでロシアがやっているようなことは別として、西側諸国に対して平時に行われているグレーゾーンのサイバー攻撃は、まず武力行使の閾値を超えないので、国際法上は「緊急避難」か「対抗措置」で対応することになるという結論をまとめて、研究会の成果を書籍[8]で発表しています。

戦争状態なら相手は武力攻撃クラスの烈度のサイバー攻撃を繰り出してくるので、武力攻撃事態であると認定し、有事法制に則って自衛権を行使するということになります。しかし、グレーゾーン事態では電気が止まるとか、病院の機能が止まるといった被害は出るかもしれませんが、人命が多数失われるといったところまではいかない。そうした状況では、そう易々と自衛権の行使はできないわけです。こちらのネットワークが破壊されたから敵のネットワークを破壊するというような措置も難しい。平時の対抗措置の範囲内でやるしかないのです。

谷脇　交戦状態とまでは言えないグレーな状態が続き、自衛権の行使に至らない時こそ、外交を含めた他の手段の重要性が高まると思います。憲法論としても緊急事態をどう捉えるべきかという議論とも関連してくると思います。

大澤　残念ながら、日本の国家安全保障法制における"認定"の対象は武力攻撃しか想定していません。サイバーに関しては「**大規模サイバー攻撃事態**」というクライテリアが設けられていますが、これは安全保障法制の範疇外で、テロを超えたグレーゾーン事態に対してどう対処するのか、国際法上の対抗措置でどこまでできるのか、ということについては、まだ議論されていません。本来は、グレーゾーンにおける事態認定をして、通信を傍受して対処したり、攻撃を受けた国内サーバーを止めたりといった対抗措置を可能にすべきだと思います。先ほど触れた米コロニアルパイプラインがサイバー攻撃を受けたケースでは、暗号化されて盗まれたデータは米国内のサーバーにあったので、司法省はこれを差し押さえるかたちで、サーバーそのものを物理的に止める措置をとりました。

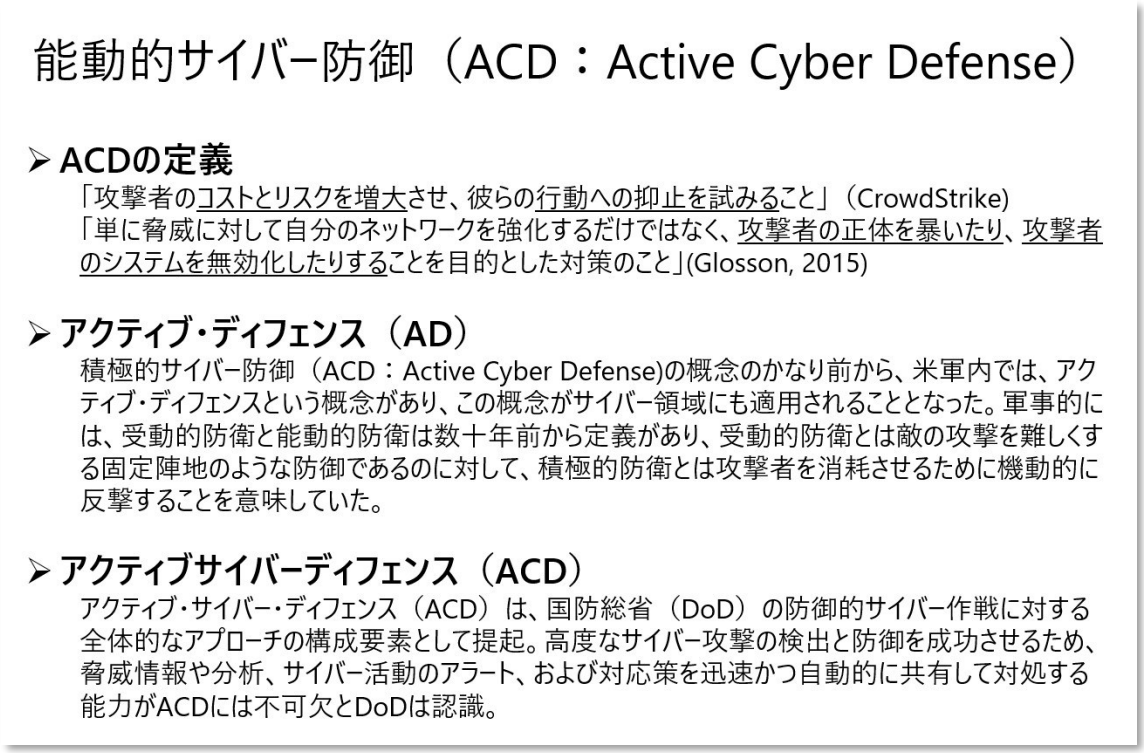
日本でもグレーゾーン事態において、国民の権利制限を伴うような措置をとるためにきちんと事態認定し、公共の福祉のためであるということを明確にした上で対処する必要があると思います。不正アクセス禁止法とか電気通信事業法の改正で留まるのではなく、もう一段進めて、**安全保障法制のサイバー・グレーゾーン版**を作るべきだと思います。

アメリカの**ACD**（**Active Cyber Defense**）の発動状況を見ると、NSC（国家安全保障会議、National Security Council）をきっちり開き対処しています。コロニアルパイプラインのケースではかな

り激しい対応をしましたが、NSC の大統領安全保障問題担当副補佐官（サイバー担当）が記者会見で背景や措置、国家安全保障上の重大性について説明するというステップを踏んでいます。そうした一連の基準や方法、手順を決めておかないとグレーゾーンには対処できないと思います。

能動的サイバー防御の本質

谷脇　今、アクティブサイバーディフェンスの話が出てきました。安全保障戦略では ACD そのものを定義していません。具体的に何かという例示も行われていません。そうした中、能動的サイバー防御、積極的サイバー防御というように翻訳され、本来はサイバー攻撃を未然に防ぐための措置という意味なのに、一般国民の中には「反撃」「攻撃」というイメージで捉える人も少なくありません。そもそも ACD とは何なのでしょうか。



大澤　「パッシブディフェンス」というのが塹壕戦で敵を迎え撃つという固定防御であるのに対して、「アクティブディフェンス」という用語は米軍で積極的防御という現代的ニュアンスで使われます。戦車や装甲車を停めて敵を待ち受けるのではなく、積極的に相手の弱点を見つけ、機動的に動き、叩き

に行くというイメージです。その考え方をサイバーに適用したのが「アクティブサイバーディフェンス」です。敵からのサイバー攻撃の兆候をリアルタイムで検知、分析し、その攻撃様態に応じて、防御の手段や技術を選択し、先んじて動くことによって、被害を軽減する考え方です[9]。

脚光を浴びるようになったきっかけは、2016 年にデニス・ブレア元国家情報長官、マイケル・チェルトフ元国土安全保障省（DHS）長官が参画した**ジョージ・ワシントン大学のプロジェクト**でした。

Active Cyber Defense （2016 GW プロジェクト）

デニス・ブレア元国家情報長官、マイケル・チェルトフ元DHS長官が参加したジョージ・ワシントン大学のプロジェクトでは、下記のように定義されている。

「アクティブディフェンスとは、従来の受動的な防御と攻撃の間に位置するプロアクティブなサイバーセキュリティ対策の領域」

自己のネットワーク内における対策を「**受動的防御**」、攻撃者のネットワーク内での妨害・破壊を「**サイバー攻撃**」と位置付け、その間の自己のネットワーク外において行われる様々な対策を「**積極的防御**」と位置付けている。

受動的防御	積極的防御	サイバー攻撃
・基本的なセキュリティ管理（リスク低減対策） ・ファイアウォール ・アンチウイルス ・パッチ管理 ・スキャン ・監視 など	低リスク／効果小 ・情報共有 ・タービット（遅延技術） ・サンドボックス ・拒否と欺瞞 ・脅威ハンティング ・ビーコン：情報窃取先から情報所有者に位置通知 ・ビーコン：相手側ネットワークに関する情報の提供 ・ディープウェブ、ダークネットにおける情報収集 ・ボットネットの停止措置 ・制裁、起訴、貿易救済（相殺関税や輸入制限など）の政策調整 ・防衛目的のランサムウェアによる反撃 ・情報資産回収のための侵入救出行為 高リスク／効果大	・ハックバック ・アクセス権限なしに相手側のネットワークや情報の破壊・混乱を目的として行われるサイバー行為

このプロジェクトでは、自己のネットワーク内における対策を「**受動的サイバー防御**（Passive Cyber Defense）」、攻撃者のネットワーク内での妨害・破壊を「**サイバー攻撃**（Cyber Attack）」、その間の自己のネットワーク外において行われる様々な対策を「**能動的サイバー防御**（Active Cyber Defense）」と位置付けました。ちなみに、日本のサイバーセキュリティは最初の受動的サイバー防御に当たります。

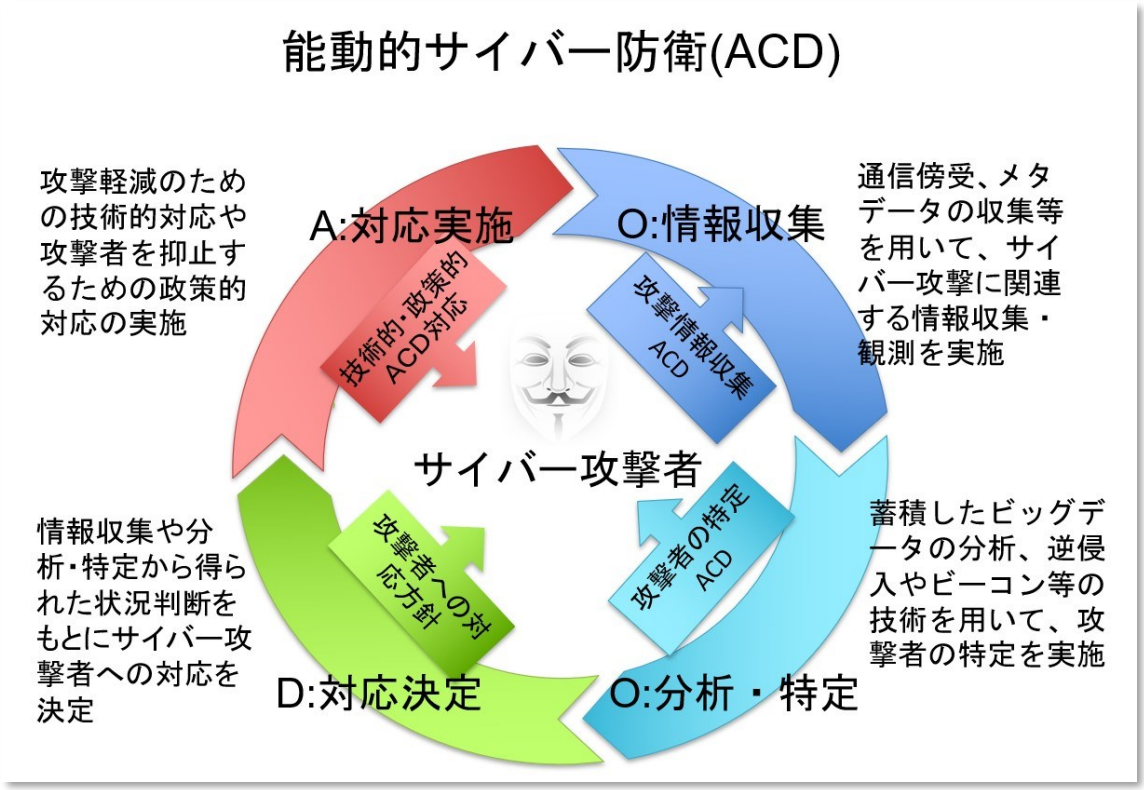
ACD にも、低リスク／効果小なものから高リスク／効果大なものまでレベルの幅があります。**情報共有**（サイバー攻撃痕跡情報（IOC）をリアルタイム共有して対処に利用）、**サンドボックス**（ソフトウェアによってコンピュータ環境を模した疑似環境）、**ハニーポット**（サイバー攻撃者をおびき寄せる

罠）のようなパッシブに近いやり方もあります。**ビーコン**（サイバー攻撃で奪われたファイルから信号を発して、攻撃元を知らせるプログラム）など、日本では刑法上の不正指令電磁的記録に関する罪や不正アクセス禁止法などに抵触するようなものもあります。ボットネットの停止措置、制裁・起訴・金融制裁、防衛目的のランサムウェアによる反撃、敵ネットワークに逆侵入して窃取された情報を消去する救出活動といった、政府と緊密な協力が必要なものも含まれています。

ACD とは OODA ループを回すこと

谷脇　かなり強弱がありますね。

大澤　はい。ただ、一貫して言えるのは、あくまで攻撃者に対するカウンターアクションであるということです。軍事用語の「**OODA ループ**」というプロセスを回していきます。「**Observe（情報収集）**」「**Orient（分析・特定）**」「**Decide（対応決定）**」「**Act（対応実施）**」の順番です。元々は米空軍を発祥とする理論です。



戦闘機の空戦で敵機がどこから飛んでくるかをレーダーあるいは目視でキャッチするのが Observe（情報収集）。その上で、どこの国の戦闘機か、何時の方向からどれくらいの速度で向かってくるのかなどを精査するのが Orient（分析・特定）。それに対して、ミサイルを打つのか機関銃を打つのかというアクションを決めるのが Decide（対応決定）。それを実行に移すのが Act（対応実施）という具合です。

ACD でも、まずは攻撃者の情報を収集するところから始まります。次にビーコンのような技術を使ったり、メタデータを活用したり、逆侵入（ハックバック）の手法を駆使したりして攻撃者を特定。テイクダウンのような技術で対応するのか、訴追や制裁、外交的な手段を含めた政策で対応するのか、方針を決める。ACD は、あくまでも攻撃者を抑止するための手法なのです。単にファイアウォールで守りを固めたり、ネットワーク内の監視を強化したりする待ち受けではなくて、攻撃の様態に合わせて直接的なアクションを攻撃者に対して行っていくことなのです。

谷脇　アメリカ政府の「**サイバースペース・ソラリウム委員会（CSC：Cyberspace Solarium Commission）**」[10]が 2020 年に公表したレポートでは、（1）Shape behavior（同盟国、友好国とのサイバー空間における責任ある行動規範の促進）、（2）Deny benefits（敵にメリットを与えない官民連携による強固な守り）、（3）Impose costs（敵に対する懲罰的対応）――の 3 層構造のサイバー抑止戦略を提案しました。日本の安全保障戦略には、この抑止戦略の考え方が組み込まれていないのではないでしょうか。

大澤　これは公表されている資料ですが、2018 年にサイバーセキュリティ戦略を検討した際、「**サイバーセキュリティ戦略案の作成に際しての国家安全保障会議意見**」[11]というタイトルの意見書を、内閣サイバーセキュリティ戦略本部の会議資料として提出しました。その中で、「悪意のある者の行動を抑止する」という表現で、攻撃者を知り、特定し、対応するという抑止概念に基づいてサイバーセキュリティ戦略を構築すべきという意見を国家安全保障会議から提出しました。その文脈で「積極的サイバー防御」という形で言葉も入れ込みました。

結果的に、**2018 年のサイバーセキュリティ戦略**では、欧米と同じようにサイバー攻撃への抑止の概念が導入されました。サイバー攻撃から安全保障上の利益を守るため、「国家を防御する力（防御力）」「サイバー攻撃を抑止する力（抑止力）」「サーバー空間の状況を把握する力（状況把握力）」のそれぞれを高めることが重要であるとの指摘がなされました。

ただし、攻撃者に対してアクションするというところまでは議論されていなかったので、あくまで攻撃を受けたときに攻撃者の情報をいち早く集め、それを後方に共有して、防御策をとるという意味での積極的サイバー防御ですが・・・。

サイバーセキュリティ戦略に足らない「抑止論」

谷脇　抑止戦略をきちんと作り、しっかり実施するためには様々な政府機関や組織との連携が必要になってくるはずです。それに対応するため、現行の **NISC（内閣サイバーセキュリティセンター）**を発展的に改組してサイバー安全保障の政策を一元的に総合調整すべきという方向が国家安全保障戦略にも持ち込まれています。組織の人員の増強はもちろんですが、司令塔と実働部隊の体制をどのように組み立てるのか、その二つの機能をどのように連携させていくのかが重要な課題になると思います。

例えば元内閣安全保障局次長の兼原信克さんは、近著『日本人のための安全保障入門』[12]で、官邸に**内閣サイバーセキュリティ局**を新設し、その下に実働部隊としての自衛隊サイバー防衛隊と発展改組したサイバーセキュリティセンターを配置するという提案をされています。大澤さんは、日本国としてのサイバーセキュリティ組織体制のあり方について、どのようにお考えですか。

大澤　アメリカを例にとりますと、担務内容によって実施主体が分かれています。

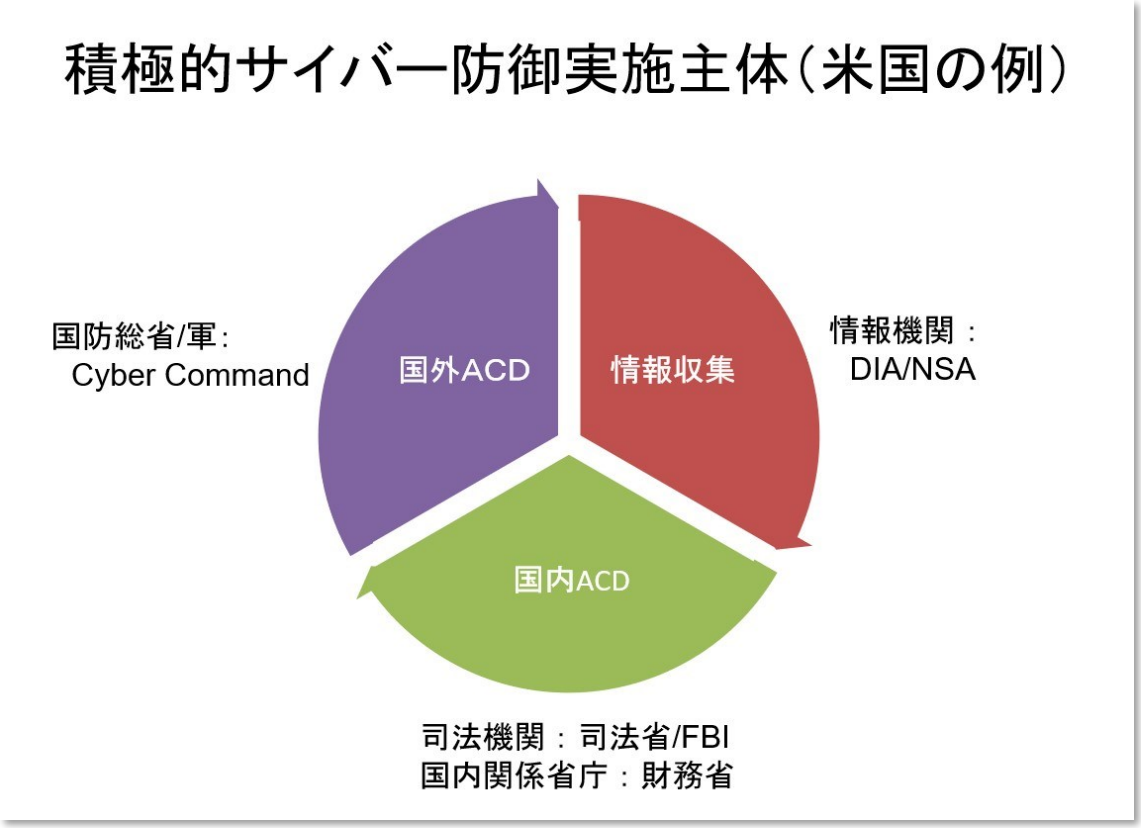
サイバーセキュリティの基準作りや監査といった業務は、**国土安全保障省（DHS：Department of Homeland Security）**が担当しています。ACD オペレーションのうち、情報収集は**国防情報局（DIA：Defense Intelligence Agency）**や**国家安全保障局（NSA：National Security Agency）**などの国防総省のインテリジェンス機関が担当。サーバー差し押さえや通信切断といった技術的対処については、**国内を司法省や連邦捜査局（FBI：Federal Bureau of Investigation）**が、国外を**国防総省／サイバー軍（United States Cyber Command）**が担当しています。

この建付けは国際法に合わせたものです。警察が国外で ACD 活動を行うことは、国際法上の司法管轄権の規定によって禁じられています。相手国の同意がない限り警察権を国外で行使することはできないのです。国外における ACD 活動は、あくまで安全保障目的で軍が担務するというように区分けされています。

日本では、これまで NISC が担務してきたサイバーセキュリティの基準作りや監査、戦略策定の部分は残しつつ、実際にオペレーションをやる部分を新たに創らなければなりません。米国の例を見て分かるように、オペレーションは警察と防衛省の混合でやらざるを得ません。内閣官房の中に司令塔を置き、警察のユニットと防衛省のユニットに対して指示を出せるような建付けは必要になってくると思います。

同じような建付けになっているのが、内閣情報調査室の**内閣衛星情報センター**です。防衛省、警察、外務省それぞれの分析官が出向し、同じ衛星を使って情報の収集と分析を行っています。日本の場合、CIA に当たる組織はありませんし、DIA に当たる部分も弱いので、少なくとも国内における技術的なアクションは警察が警察権を行使する形でやらざるを得ません。国外については自衛隊がや

ることになります。そうしたオペレーションの機能を"内閣サイバーセキュリティ局"に備えて、判断していくことになります。情報機関、国内の ACD 執行、国外の ACD 執行の 3 機能が一つになった組織が必要だと思います。



ただし、日本でも ACD のオペレーションは国際法に則って行う必要があります。重大なサイバー攻撃に対して、国外で ACD を行う場合、国際法上の緊急避難か対抗措置に基づく実施を明確にする必要がありますし、国内で ACD を行う場合には、安全保障の確保という公共の福祉に基づいて、国民の権利制限を伴うテイクダウンなどの措置を行うこととなります。その判断は、国家としての事態の認定と安全保障上の意思決定が必要であり、ACD のオペレーションの決定は国家安全保障会議で行う必要があります。

その観点からは、新しいサイバーの司令塔を、「**事態室**」（内閣官房副長官補 事態対処・危機管理担当）と**安全保障局**の横並びにするか、事態室と安全保障局の両属にして、サイバー攻撃の烈度に応じて、事態対処のテロのほうで対処するか、それとも安全保障上の ACD オペレーションにするのか――という判断をする形になるでしょう。いずれにしても、内閣官房の組織になると思いますし、

事態室、内閣情報室、安全保障局の次に来るようにしておいたほうがオペレーションはやりやすいだろうと思います。

谷脇　課題が三つあると感じました。

第一に、自衛隊のサイバー防衛隊は今のところ自衛隊の情報システムを守るという役割しか担っていません。今のサイバー防衛隊のミッションを大幅に拡充することを検討していく必要があります。

第二に、事態認定のあり方について整理する必要があります。「大規模サイバー攻撃事態」から安全保障に直結する事態認定へとエスカレーションするプロセスと、このプロセスに合わせた各組織の動き方についてどう整理するかということ。

第三に、現行 NISC がどう絡むのかという点。現行 NISC の中にも政策の企画立案部門とセキュリティ対策のオペレーションを担う部門があります。このオペレーション部門を平時と有事でどう切り分け、他の組織と連携させていくのが最も適当なのか、制度的な壁を超えなければならないという問題があります。

防衛省設置法の見直しが必要

大澤　はい。おそらく、**防衛省設置法**を見直さなければならないでしょう。2022 年 12 月に閣議決定された防衛 3 文書[13]のうち「国家防衛戦略」で「サイバー要員を大幅増強する」方針が明記され、防衛省は自衛隊サイバー防衛隊を 2022 年度末の約 890 人から 2027 年度末には約 4000 人に拡充する方針を示しました[14]。また、一歩引けた書きぶりではありますが「重要インフラに対する攻撃に際しては実効的な対処」を行うとの文言が入り、サイバー防衛隊の守備範囲拡大に含みを持たせました。防衛省設置法の改正が想定されていると思っています。

谷脇　自衛隊の「中」を守るから「外」も守るとなると、今のサイバー防衛隊にそのためのスキルセットを持った隊員がどのくらいいるのかが気になります。絶対的に不足しており、人材育成が非常に重要になってくると思います。官民が連携したサイバー人材育成の仕組みづくりが必要ですし、特に ACD にかかわる部分については専門性の高い特別のトレーニングコースを用意するといったことも考えるべきだと思います。こうした人材育成プログラムの強化は民間のセキュリティ人材の育成にも裨益（ひえき）することが期待されます。しかし、その点がまだ十分議論されていないように感じます。

大澤　要員の育成は始まっています。例えば通信職種の人たち向けの育成プログラムにサイバーセキュリティやサイバー安全保障の講座を追加するなどの取り組みです。採用を増やせば、高度セキュリティ人材も徐々に育っていくと思います。

ただし、採用増と教育だけで全て良しというわけではありません。ゆくゆくは、自衛隊で訓練してある程度のキャリアを積んだ人を民間企業に出すというキャリアパスを作るべきだと考えています。昇進、給与ということを考えると、現時点ではサイバー職種一筋で自衛隊に留まるよりも民間のセキュリティ企業などに移った方がチャンスは広がるのではないかと思います。予備自衛官として任用し、いざという時には応召してもらう。1000 人から 2000 人くらいまで増やすイメージを描いています。

逆に、民間セキュリティ会社の高度人材にどのようにして国家安全保障の仕事に携わってもらうか、「**セキュリティクリアランス**」をどうするのか、ということも課題です。

また、訓練の仕方もより実戦形式に近いものしていかなければなりません。**サイバーレンジ**（攻撃・防御演習用の仮想サイバー空間）での訓練だけでは有事には使い物になりません。米軍では、錬成度 7 割くらいで実戦に出しているようです。敵の情報ネットワークへの侵入口の探索力、脆弱性を見極めてどこをどのように突けばよいかの分析力・判断力といったテクニックを、ケースバイケースで学んでいかなければなりません。そういう経験値を持ったサイバー人材の層を厚くしていくこと、民間人も含めて拡大していくことは大きな課題です。

なにしろ、今までは攻撃することを前提としていなかったので、まずは能動的サイバー防御、つまり、こちら側から攻撃を仕掛けることもあることを前提とした経験とノウハウの蓄積を急がなければなりません。国家が関与する攻撃を受けた時には 10 年単位の過去のデータと照らし合わせて手口や意図の分析を行うのですが、そうした経験値は一朝一夕には高まりません。あるサイバー攻撃が、国家戦略とどのように関連しているのか、軍の部隊改編とどのようにつながっているのか、といったサイバーに限定されない広い視野と知識、分析力が必要になります。それができないと、次の手口を読むことができません。また、民間企業がランサムウェア攻撃などを受けた時、担当者がパニックを起こさないよう心理的ケアをしつつ、情報を提供してもらうというところにもノウハウがあります。そうしたことができる人材を育てていかなければなりません。

谷脇　認知戦などの領域に対応できる人材の育成もすごく大事ですよね。特に認知戦の領域では、**オープンソースインテリジェンス**（**OSINT : Open-Source Intelligence**）に長けた人材が求められます。OSINT（オシント）の先駆者として、オランダに本拠を置く調査報道（ファクトチェック）機関ベリングキャット[15]は偽情報の判定を行う際に OSINT（オシント）を駆使していることで知られていますが、日本では OSINT のスキルを磨く場が、私が知る限りほとんどありません。攻撃者のアトリビューション問題に対応する観点からも貴重なツールになっていくでしょうから、そうした人材も求められると思います。

大澤　OSINT 人材というのは、結果・成果を出せるようになるまでに 5 年、10 年かかる“オタク”的な領域なので、長い目で投資できるかというところが一つのポイントになります。そして、長い期間にわたって部署異動せずに取り組む仕事なので、日本的な年功序列システムの中では扱い方が非常に

難しい。「育てる」ことはもちろんなのですが、超専門人材をいかに「遇する」かも課題になってきます。同じ部署にずっといながらにして、きちんと昇給し、ランクも上がるような人事システムをどう作るか、そういった人材マネジメントの議論が必要だと思います。これは特に 2 年、3 年で異動することが当たり前の官僚組織においては本質的な問題です。梁山泊とは言いませんが、高度人材をプールするための機関を作ることを真剣に考えるべきだと思います。

AI は人類の救いか脅威か？

谷脇　最後に AI（人工知能）についてお伺いします。生成 AI などが進化して広く活用される一方で、ダークウェブの世界では、サイバー犯罪向け生成 AI ツール「WormGPT」のように、マルウェアを自動生成したり、システムの脆弱性を自動検出したりするものも出てきています。米国政府は 2023 年 2 月、「**AI と自律性の責任ある軍事利用に関する政治宣言（Political Declaration on Responsible Military Use of Artificial Intelligence and Autonomy）**」を発表し、この中で「AI の軍事利用は、国際人道法上の国家の義務に合致した形で、責任ある人間の指揮命令系統の下で運用し、責任の所在を明らかにする必要がある」としました。日本を含めた約 50 カ国が支持を表明しています[16]。

AI の開発・利用が推進される一方で、リスクへの対応が必要だという意見もある。この状況を、どうお考えですか。

大澤　10 年くらい前から、**自律型致死兵器システム（LAWS：Lethal Autonomous Weapons Systems）**[17]に関する議論が重ねられてきました。まだ明確な定義もされておらず、ルールに関する議論が先行している状況です。完全自動のロボット兵器を創り出さないためには、攻撃に際して人間の判断、意思決定を入れるという最低限の合意が必要ですが、必ずしも世界各国が合意しているわけではありません。

汎用 AI のセキュリティを考える場合にも、最初はルール作りだと思います。中国やロシアのように国際ルールなど関係ないよという国々もあるのでルールの有効性は疑わしいのですが、少なくとも一般の AI ツールに、サイバー攻撃プログラムの自動生成とか、標的システムの脆弱性の自動発見とかができないようにすることをルール化しておくのは非常に重要です。

ただし、アメリカには他国の AI 開発をできるだけ遅らせたいという意図が見え隠れしています。特に GAFAM は先行優位性を維持したいがために、ルール化で縛りをきつくし、世界の新興企業が追い付いてこないようにしたいわけですね。ある GAFAM 企業は国連の AI 関連会議に多額の資金を供与しています。そうした思惑には注意が必要です。先行者にとって都合の良いルールを作られてしまったら、日本の「K-Pro」（経済安全保障重要技術育成プログラム、K-Program）[18]でやっている

AI 開発プロジェクトが突然止められてしまうなどということが起こるかもしれないと懸念しています。

汎用 AI のサーバーをどこに置くかも重要な問題です。国民が生成したデータを学習させていくわけですから、データサーバーは日本国内に置くべきです。AI エンジンも国産を使いたいところです。そうしないと、日本のデータがどんどん海外に蓄積され、どういう情報を打ち込むと日本国民はどう動くかといった行動予測、ひいては行動操作にさえつながりかねない危険性を放置することになります。

谷脇　大変興味深いお話をありがとうございました。

◇　　◇　　◇

【対談を終えて】

この対談では、サイバー空間における安全保障問題がクローズアップされる中、もはや他国からのサイバー攻撃を拒否的に抑止する従来の手法だけでは不十分であり、より能動的な防御が必要になっていることが明確になった。しかし、能動的サイバー防御を実際に展開するに際しては、その狙いや運用体制など、共通認識をしっかり持ちながら議論を進める必要があるだろう。法制度に関する丁寧な議論も求められる。

また、サイバー空間における安全保障問題を考える場合、もはやデジタルコミュニティだけの話ではなく、技術、外交、軍事を含む総合的な抑止戦略の策定とこれを実効たらしめるための体制の実現などが求められている。さらに、長年の課題ではあるものの、サイバー人材の育成を官民連携で総合的に進めることの必要性も改めて浮き彫りになった。

大澤氏の広範囲にわたるご発言からは、「今そこにある危機」に対し、デジタル時代の経済安全保障問題について、冷静かつ迅速、かつ最優先で議論を進めていかなければならないとひしひし感じた。（谷脇）

＜参考情報＞

[1] https://www.kantei.go.jp/jp/singi/anzenhosyoukaigi/index.html
[2] https://www.cas.go.jp/jp/gaiyou/jimu/anzenhosyou.html
[3] https://www.nisc.go.jp/
[4] https://www.cas.go.jp/jp/siryou/131217anzenhoshou/nss-j.pdf
[5] https://www.cas.go.jp/jp/siryou/221216anzenhoshou/nss-j.pdf、2022 年 12 月 16 日、国家安全保障会議決定・閣議決定
[6]「先島諸島の避難計画 検討チーム設置へ 台湾有事が念頭 政府」、https://www3.nhk.or.jp/news/html/20240113/k10014319531000.html
[7]「台湾有事とハイブリッド戦争」、大澤淳、2022 年 8 月 24 日、https://www.spf.org/iina/articles/osawa_02.html

[8] 笹川平和財団新領域研究会編『新領域安全保障』（2024 年 1 月、Wedge）
[9]「日本も導入目指す「ACD」とは？ サイバー安全保障の最先端の姿」、大澤 淳、2023 年 12 月 25 日、https://wedge.ismedia.jp/articles/-/32480
[10] The Cyberspace Solarium Commission (CSC)、https://www.solarium.gov/home
[11]「資料１ － 5 サイバーセキュリティ戦略案の作成に際しての国家安全保障会議意見」、https://www.nisc.go.jp/pdf/council/cs/dai18/18shiryou01.pdf
[12]『日本人のための安全保障入門』（2023 年 11 月、日経 BP・日本経済新聞出版刊）、https://amzn.asia/d/c2DZfy5
[13] 防衛三文書（安保三文書とも言う）とは、「国家安全保障戦略」「国家防衛戦略」「防衛力整備計画」で構成される防衛政策の要。2022 年 12 月に閣議決定された。
https://www.mod.go.jp/j/policy/agenda/guideline/index.html
[14]「サイバー人材の確保及び 育成について」2023 年 5 月、防 衛 省
https://www.mod.go.jp/j//policy/agenda/meeting/kiban/pdf/20230531_01.pdf
[15] https://www.bellingcat.com/
[16]「AI と自律性の責任ある軍事利用に関する政治宣言」、外務省、2023 年 11 月
https://www.mofa.go.jp/mofaj/gaiko/arms/page23_004519.html
「Political Declaration on Responsible Military Use of Artificial Intelligence and Autonomy」、U.S. Department of State、2023 年 11 月 https://www.state.gov/political-declaration-on-responsible-military-use-of-artificial-intelligence-and-autonomy/
[17]「自律型致死兵器システム（LAWS）について」、外務省、2023 年 5 月
https://www.mofa.go.jp/mofaj/dns/ca/page24_001191.html
[18] 経済安全保障重要技術育成プログラム、内閣府
https://www8.cao.go.jp/cstp/anzen_anshin/kprogram.html