サイバースペースにおける安全保障

土屋大洋
慶應義塾大学教授

1. はじめに

サイバーセキュリティには大別して三つの分野があるといわれている。第一に、CND（Computer Network Defense）と呼ばれる防衛、第二に、CNA（Computer Network Attack）と呼ばれる攻撃、そして第三に、CNE（Computer Network Exploitation）と呼ばれる工作活動である。本来、CNE の「E」にあたる「エクスプロイテーション（exploitation）」とは「利己的な利用、搾取」という意味であり、サイバーセキュリティの文脈ではハードウェアやソフトウェアを本来の想定とは異なる使い方で使うことを意味し、工作活動と呼べる活動である。

マスメディアで言及される「サイバー攻撃」のほとんどは国際法上の「攻撃」には当たらない。ほとんどは嫌がらせ、サイバー犯罪、あるいはサイバーエスピオナージ（スパイ活動）の類いである。武力紛争法がいうような攻撃やそれに対応する防衛にあたる事例はほとんどなく、多くは CNE の領域に収まるグレーゾーンである。ある米国政府元高官は「CNE は全ての国家にとって必要なツール」と述べている[1]。

攻撃と防衛の境がはっきりせず、その間に大きなグレーゾーンが広がるという点で、サイバースペースの安全保障は、これまでの通常兵器による安全保障と異なる。本稿では、サイバーセキュリティが安全保障問題として強く意識される前の前史、そして 2010 年代以降の五つのタイプのサイバー攻撃について概観し、最後に、日本政府がまとめた防衛計画の大綱の目指すところについて見ていきたい。

2. サイバーセキュリティ前史

1981 年から 82 年にかけて、フランス政府にソビエト連邦（ソ連）の情報をもたらしたウラジミール・ベトロフ（Vladimir Vetrov：コードネーム「フェアウェル」）というスパイがいた。彼がもたらした情報をフランス政府が米国政府と共有したところ、ソ連が西側から求めているもののリストが見つかった。それを見た米国家安全保障会議（NSC）ガス・ワイス（Gus W. Weiss）は、ガス・パイプラインの制御ソフトウェアを、カナダ企業を通じて意図的にソ連に盗ませることに成功した。そのソフトウェアには細工がされており、それを使っ

[1] 発言者の意向により匿名。2018 年 12 月、筆者との私的な対話における発言。

たソ連のパイプ・ラインはシベリアで大爆発を起こした[2]。これがおそらく史上初めてのサイバー攻撃による物理的な破壊であろう。

そのすぐ後の 1983 年、米国では映画『ウォーゲーム（War Games)』が公開された。それを観賞したレーガン大統領が統合参謀本部議長に「こんなことが本当に起きるのか」と尋ねたところ、議長は「大統領、問題はお考えよりもいっそう深刻です」と伝えたという。その結果、レーガン政権は NSDD-145 と番号の振られた文書を作り、最初のサイバーセキュリティ対策を打ち出した[3]。

1990 年の湾岸危機に続いて 1991 年に湾岸戦争が起きると、制空権の掌握に続く地上軍の投入によって米軍は圧倒的な強さを見せる。そこでの英雄はノーマン・シュワルツコフ（Norman Schwarzkopf）中央軍司令官とコリン・パウエル（Colin Powell）統合参謀本部議長であった。しかし、陰の英雄は、国家安全保障局（National Security Agency）のウィリアム・ステュードゥマン（William Studeman）長官と彼が作った統合インテリジェンス・センター（Integrated Intelligence Center）を率いたマイク・マッコーネル（Mike McConnell）であった。マッコーネルの分析官たちはイラクのサダム・フセイン（Saddam Hussein）大統領の指揮命令ネットワークの中枢に潜入した。そして、イラクの首都バグダッドからクウェートに近い都市バスラまで光ファイバーのネットワークが敷設されており、それをイラク軍が指揮命令ネットワークとして使っていることを突き止めた。米軍はその光ファイバーの接続点を破壊した。イラク軍はすぐに指揮命令を無線システムに切り替えるが、無線信号は漏れ出してしまう。それを予期していた NSA は、漏れ出した微弱な信号を人工衛星その他で傍受し、イラク軍の動きを把握し、戦況を有利に進めた。イラク軍は無線の使用をやめ、バイクでの伝令に切り替えるが、当然、それでは戦争に勝てなかった。これはいわば制空権に対する制脳権であり、「対指揮制御戦争」の最初の戦役、ないし将来のサイバー戦争の前触れだと評価されている[4]。

1998 年 2 月、米国のアンドリューズ空軍基地で不正侵入が見つかった。同基地は大統領専用機エアフォースワンやマリーンワンが離発着する基地である。事件はソーラーサンライズと名付けられた。攻撃者を追跡したところ、アラブ首長国連邦までたどることができた。1991 年の湾岸戦争の記憶が生々しく残っていた時代でもあったので、イラクによる侵入かと思われた。しかし、犯人は、イスラエル人にそそのかされたカリフォルニア州のティ

---

[2] Thomas C. Reed, *At the Abyss: An Insider's History of the Cold War*, New York: Presidio Press, 2005.

[3] 正式には「電気通信と自動情報システムのセキュリティに関する国家政策（National Policy on Telecommunications and Automated Information Systems Security)」と題する文書である。

[4] Fred Kaplan, *Dark Territory: The Secret History of Cyber War*, New York: Simon & Schuster, 2016.

ーンエイジャー2 人だと分かった。

その翌月、ムーンライト・メイズと呼ばれる侵入事件がおき、米空軍のライトパターソン空軍基地が狙われた。こちらもいたずらかと思われたが、追跡するとロシア科学アカデミーにたどり着いた。当時はビル・クリントン（Bill Clinton）米大統領とボリス・エリツィン（Boris Yeltsin）露大統領との間で親密な関係が築かれているように表面的には見えていたが、裏ではロシアが情報窃取を狙っていることが明らかになり、関係者を驚かせた。

クリントン政権時代は、情報通信技術（IT）による好景気に沸き、景気循環のない「ニュー・エコノミー」の到来かとも呼ばれていた。しかし、その好景気も 2001 年 7 月にはじけ、9 月にはアル・カイダによる対米同時多発テロ（9.11）が起きることによって情勢は大きく転換していく。

アフガニスタンで戦争が行われ、まもなくイラクとの開戦が迫っていた 2003 年 1 月、米オハイオ州デイビス・ベッセ（Davis-Besse）原子力発電所でスラマー・ワームと呼ばれる悪質ソフトウェアが増殖し、原発の機能停止につながった。原子炉を止めている最中だったので深刻な被害はなかったが、出入り業者を通じてワームが侵入したことが分かった。重要インフラはインターネットにつながないから問題ないという認識が改められる契機になった。

2008 年頃、米軍の中東の基地において USB メモリが落ちていた。それを拾った基地関係者が基地内のコンピュータに挿入してしまったため、全世界の米軍のネットワークに侵入されるという事件が起きた。これに対処するために米軍は「バックショット・ヤンキー作戦」を展開し、不正アクセスを排除するとともに、サイバーセキュリティを強化することになった。その一環として、統合軍の一つの戦略軍（USSTRATCOM）の下にサイバー軍（USCYBERCOM）が準統合軍として設置された。司令官には NSA の局長であるキース・アレグザンダー（Keith Alexander）が兼務する形で就任した。

3. 五つのタイプのサイバー攻撃

（1）DDoS：分散型サイバー攻撃

2007 年、エストニアの首都タリンの中心部にある公園にあったブロンズ像を移設するニュースが流れた。ブロンズ像は第二次世界大戦のソ連兵を象徴するものであったため、郊外の戦没者墓地への移設は、ロシア系住民の反発を生み出した。そして、エストニアの金融機関などに向けて分散型サービス拒否（DDoS）攻撃が行われた。DDoS 攻撃は、コンピュータ・ウイルスに感染した多数のコンピュータからターゲットに向けてアクセスを殺到させる手法である。感染したコンピュータの所有者は利用されていることに気づいておらず、タ

ーゲットにされた側は通常のアクセスと不正なアクセスを区別できないため、機能不全に陥らざるを得ない。エストニアは当時からキャッシュレス経済を進めており、金融サービスの機能不全は社会的に大きな影響をもたらした。

この攻撃の首謀者は文脈からロシアだと考えられたが、ロシア政府は否定した。後にロシア系の非政府団体が関与を認めたものの、ロシア政府の意向があったのではないかと疑われている。いずれにせよ、エストニアという国全体が狙われたという点で、時代を画する事件として位置づけられることになった。

DDoS 攻撃は、その後も各国で金融機関や政府機関、その他の業務妨害のために多用されている。対策も進んでおり、致命的な事態に陥ることは考えにくいが、対策を全くとっていない組織は被害を避けることができない。また、金融取引のように高速取引を求めているところは DDoS 攻撃による遅延が業務損失につながることもある。

この頃からサイバーセキュリティが重要な安全保障問題の一つとして認識されるようになり、各国で対応が進むようになった。

（2）APT：高度で執拗な脅威

高度で執拗な脅威（Advanced Persistent Threat：APT）は、標的型電子メール攻撃と同義で用いられることもあるが、電子メールだけに頼るものではない。ソーシャル・エンジニアリングという言葉があるように、社会的な文脈を活用しながらさまざまな手法でターゲットとなる個人や組織のシステムに侵入し、システムを破壊したり、データを盗み出したり、密かに監視したりする行為全般を指す。

日本で APT が注目されるようになったきっかけは、2011 年 9 月に三菱重工業のコンピュータ 80 台がコンピュータ・ウイルスに感染し、情報が抜き取られたとする報道である。重要な機密情報は取られていないとされているが、日本最大の防衛企業が狙われたことは関係者に大きな衝撃を与えた。

APT の主要なプレーヤーは中国だとされている。中国の APT に関する報道は枚挙に暇がない。米国のサイバーセキュリティ企業ファイアアイは APT を実行しているグループに独自の番号を振っているが、例えば、APT1 は中国人民解放軍 61398 部隊とされる[5]。APT10 は米国、欧州、日本の土木建設企業、航空宇宙企業、通信企業、官公庁をターゲットにする中国のグループとされている。

2013 年 6 月、カリフォルニア州で米中首脳会談がなされ、バラク・オバマ（Barack Obama）

---

[5] Mandiant, ‘APT1: Exposing One of China’s Cyber Espionage Units’ http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf, March 2, 2013.

米大統領は中国の習近平国家主席にサイバースパイ活動をやめるよう求めるが、習主席は中国こそが被害者であると反論した。会談の数日前にエドワード・スノーデン（Edward Snowden）がメディアに現れ、NSA による通信監視を傍受し、中国もその対象になっていると報道されたためである。

2015 年には日本年金機構に不正侵入があり、124 万件の年金情報が盗まれたことが発覚した。しかし、日本年金機構だけではなく、同時に 1000 組織が狙われていたとする報道もある。日本年金機構はセキュリティに不備があったため、たまたま年金情報が取られたと見るべきだろう。

こうした APT は手法を変えながら各所で継続的に行われている。被害の程度はさまざまである。国家機密や軍事機密に関わるものから、個人情報まで多様であり、そもそも不正アクセスを受けたり、情報が盗まれていたりすることに気づかないことも多い。しかし、APT によって直接的に人命に危害が及ぶわけではない。無論、盗まれた軍事情報によって戦争の結果が左右される可能性はあり、潜在的には危険な行為である。

（3）CCC：サイバー・通常兵器の組み合わせ

1980 年代初めのシベリアにおけるパイプライン爆発に見られるように、サイバー攻撃によって物理的な破壊ができることは、一部には知られていた。2007 年、米国政府の国土安全保障省は「オーロラ発電機テスト」と名付けられた秘密実験を行った。船舶用発電機につながるコンピュータのプログラムに 21 行書き足し、発電機のベントが不正な動きをするよう細工すると何が起きるかを試した。すると、発電機は数分で機能不全を起こし、黒い煙を吐いて壊れた。実験後に分解してみると全ての部品に影響が出ていた。米国政府はサイバー攻撃によって物理的な破壊が可能であることを再確認していた。

2008 年、シリアの砂漠の中で北朝鮮系と見られる核施設の建設が進められていることにイスラエル政府が気づいた。イスラエルは米国に空爆を要請するが、アフガニスタンとイラクで戦争を進めていたジョージ・W・ブッシュ（George W. Bush）は要請を拒否する。しかし、後日、その施設は空爆を受けた。当初、シリア政府は何が起きたのか分からなかったが、事前にイスラエルがシリア軍のレーダー網にサイバー攻撃をかけて探知できないようにし、戦闘機をシリア上空に飛ばし悠々と空爆を実施した[6]。サイバー攻撃と通常兵器による攻撃を組み合わせるときわめて効果的に戦果が挙げられることを証明した事例である。

このように、サイバー兵器（cyber weapon）と通常兵器（conventional weapon）を組み

[6] リチャード・クラーク、ロバート・ネイク（北川知子、峯村利哉訳）『核を超える脅威 世界サイバー戦争　見えない軍拡が始まった』徳間書店、2011 年。

合わせる（combine）ことで成し遂げる攻撃を CCC とここでは呼ぶことにしよう。しかし、実際に通常兵器の使用までたどり着いた事例はほとんどない。以下の三つの事例は通常兵器の使用には至らなかったが、戦局を進めるに当たってサイバー攻撃が優位に使えることを示唆する事例である。

2020 年現在でも史上最も洗練されたサイバー攻撃だったされるイランの核施設をめぐる事件が 2010 年に起きた。イラン政府は平和利用のための核開発だとしていたが、各国政府は疑念を呈していた。イランとの武力衝突を回避しながら核開発を阻止したい勢力が、ナタンツでの核施設の遠心分離機を制御する装置にサイバー攻撃を仕掛け、1000 本程度の遠心分離機を不能にし、イランの核開発を遅らせたという。後にニューヨーク・タイムズ紙は、イスラエルと米国による共同作戦だったと報じた [7]。

第二に、2015 年 12 月 23 日、クリスマス直前のウクライナ西部で電力網に対するサイバー攻撃が行われ、23 万人が 1 時間から 6 時間、停電に直面した [8]。ウクライナの西部の街イヴァノ－フランキフシク（Ivano-Frankivsk）の 12 月の平均最高気温は摂氏 3 度、平均最低気温は摂氏マイナス 5 度である。死者が出るような事態にはならなかったが、大規模停電による社会機能喪失と混乱は、軍事作戦の初期段階としてはきわめて効果的であろう。

第三に、2014 年、米国のオバマ政権は、ミサイル発射実験を行う北朝鮮のミサイルを止めるべく、サイバー攻撃を命じ、それをドナルド・トランプ（Donald Trump）政権も引き継いだとニューヨーク・タイムズ紙が報じた [9]。本当に米国サイバー軍のサイバー攻撃が機能していたのかは不明だが、一時期、北朝鮮のミサイル発射実験の失敗率が高まったことがあった。報道が出た段階で、この作戦は中止になったか、効果がなくなったと見るべきだろう。しかし、実際の戦争が行われる場合には、そうした相手兵器システムへのサイバー攻撃は必須になるだろう。そのための準備は開戦前から行われていると見るべきである。

（4）SC：サプライチェーン

米国国防長官府は毎年、中国の軍事・安全保障上の展開に関する報告書を米国議会に提出

---

[7] David E. Sanger, "Obama Order Sped Up Wave of Cyberattacks Against Iran," *New York Times* <https://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html>, June 1, 2012.

[8] Kim Zetter, "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid," *Wired* <https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/> March 3, 2016.

[9] David E. Sanger and William J. Broad, "Trump Inherits a Secret Cyberwar Against North Korean Missiles," *New York Times* <https://www.nytimes.com/2017/03/04/world/asia/north-korea-missile-program-sabotage.html> March 4, 2017.

している。その 2009 年版では、「ファーウェイ、大唐（Datang）、中興通訊（Zhongxing[10]）を含む情報技術企業は人民解放軍と密接な関係を維持し、技術開発に関して協力している」と懸念を表明していた [11]。それ以来、10 年以上にわたってファーウェイに関する疑念は続いている。

2017 年 1 月にトランプ政権が成立すると、対中貿易赤字が問題となり、米中間の貿易摩擦、そして技術摩擦が顕在化した。特にその中でやり玉に挙がっていたのがファーウェイである。

2018 年 10 月、ブルームバーグ・ニューズウィークは、米国のエレメンタル・テクノロジーズ社が出荷しているサーバーの中で極小チップが見つかり、データが第三者に不正に送信されている疑いがあると報じた [12]。サーバーはアップルやアマゾン・ウェブ・サービス（AWS）に納入されていた。AWS はアマゾンのクラウド・サービスであり、利用者の中には米国中央情報局（CIA）、米国海軍、米国国防総省も含まれていたという。

こうした議論が行われる中、2019 年 12 月、ファーウェイ創業者・任正非の娘で、ファーウェイの最高財務責任者（CFO）を務める孟晩舟を、米国政府の要請を受けてカナダ政府が逮捕した。2020 年 2 月現在、孟はグローバル・ポジショニング・システム（GPS）の発信器を足首に付けられたまま、訴訟の進展を待っている。

ファーウェイはサプライチェーン・リスクを疑われている。サプライチェーン・リスクとは、ハードウェアやソフトウェアに仕込まれた不正である。意図しない場合にはバグ（不具合、欠陥）と呼ばれるが、何者かが意図的に仕込んでおくタイプをサプライチェーン・リスクと呼んでいる。

サプライチェーン・リスクには二つのタイプがある。第一に、製造段階で組み込まれる方法で、潜在的には製品の全ての利用者が影響を受ける。ファーウェイが疑われているのはこちらのタイプである。第二に、製造後、配送途中で抜き取られて不正が仕込まれるタイプである。これは政府機関の要請によって配送途中の製品がいったん引き抜かれ、ターゲットを絞った情報収集措置等が仕込まれ、配送に戻され、ターゲットに届けられる。

---

[10] 日本のメディアでは「ZTE」と呼ばれることが多い。

[11] Office of the Secretary of Defense, "Annual Report to Congress: Military Power of the People's Republic of China 2009," United States Department of Defense <https://archive.defense.gov/pubs/pdfs/China_Military_Power_Report_2009.pdf>, publish date unknown, accessed on February 16, 2020.

[12] Jordan Robertson and Michael Riley, "The Big Hack: How China Used a Tiny Chip to Infiltrate U.S. Companies," *Bloomberg Newsweek* <https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies>, October 4, 2018, accessed on February 16, 2020.

第二のタイプについて、米国政府高官は、「やれるチャンスがあれば 99%やるのが当たり前だ」と答えている[13]。ターゲットを特定した上で外交・安全保障目的で行うことは、国際法上のグレーゾーンにある。むしろ、戦争やテロを防ぐという意味ではそうしたインテリジェンス活動は必要悪でもある。

米国政府は、中国政府が外交・安全保障目的で米国に対するインテリジェンス活動を行うことについては異議を唱えていない。それは相互に行っていることだからである。しかし、第一のタイプのサプライチェーン・リスクは、民間人・民間企業が無差別に対象になっており、経済目的で行われたり、個人のプライバシーを侵害したりする可能性があるため、双方ともに行うべきではないとし、米中交渉の席でも持ち出している。2015 年 9 月にワシントン DC で行われた米中首脳会談ではそうしたサイバー攻撃は行わないと合意したが、記者会見での発言のみで、合意文書は作られなかった。

（5）IO：インフルエンス・オペレーション（影響工作）

2016 年の米国大統領選挙は、民主党のヒラリー・クリントン（Hillary Clinton）候補に共和党のトランプ候補が勝利した。しかし、選挙の過程でロシア政府による介入があったと、後に米国政府は断定した。ロシア政府に関連すると見られるグループが、米国民主党全国委員会やヒラリー・クリントン候補陣営幹部のメール・システムに不正侵入し、暴露したり、ソーシャル・メディアに偽ニュースを流したりした。

この選挙介入によってトランプ当選が可能になったのかどうかは検証も断定もきわめて困難であり、米国政府も判断していない。しかし、選挙に介入することによって、その結果に疑念を抱かせ、ひいては民主主義の正当性そのものに疑義を抱かせることが目的だったとされている。

2017 年 1 月のトランプ政権成立後も、この問題は米国政治を揺るがし続けており、2020 年 1 月にはトランプ大統領が米国政治史上 3 人目の弾劾裁判にかけられた。無罪評決は出たものの、米国政治の分裂を物語っている。

2018 年 11 月の米国中間選挙にもロシアは介入しようとした。米国政府は選挙システムを重要インフラ指定しており、外国からの介入阻止にサイバー軍を用いることができる。サイバー軍はロシアで偽ニュースを流しているとされるインターネット研究機構（IRA）のインターネット回線を遮断したり、介入活動を行う工作員の作業を妨害したりすることで中間選挙への介入を阻止した。

こうした介入阻止のための戦略を米国国防総省は前方防衛（defend forward）戦略と呼ん

[13] 注 1 と同じ人物。

でいる。またサイバー軍司令官のポール・ナカソネ（Paul Nakasone）大将は、「執拗な交戦（persistent engagement）」を行うことでロシアやその他の国々による介入を阻止しようとしている。

2020 年 1 月には台湾で総統選挙が実施された。選挙の 1 年前までは現職の蔡英文総統の再選の見込みはほとんどないとされていたが、香港情勢などが追い風になった。また、選挙前には蔡英文総統側が、中国による選挙介入を何度も警告したため、警戒心が高まった。結果的に中国はそれほど介入せず、蔡英文総統は、韓國瑜・国民党候補に圧勝した。しかし、中国はカンボジアなどで選挙介入を行っているとされ [14]、米国大統領選挙への介入の可能性も完全には否定できない。

4. 新しい防衛計画の大綱とサイバー

日本はこうした現状にどう対応しようとしているのか。

政府のサイバーセキュリティ政策の司令塔となるサイバーセキュリティ戦略本部（旧・情報セキュリティ政策会議）と内閣サイバーセキュリティセンター[15]（NISC）は、2013 年、2015 年、2018 年にサイバーセキュリティ戦略を出し、政府全体の方針を出している。

防衛省は 2014 年 3 月に防衛大臣直轄の指揮通信システム隊の隷下にサイバー防衛隊を設置した。サイバー防衛隊は、日常的には防衛省・自衛隊のシステムとネットワークの防衛に当たる。いったん防衛出動命令が下令されれば、日本全体のサイバー防衛に当たることになる [16]。

2018 年 12 月、政府は新しい防衛計画の大綱を閣議決定した。そこでは、多次元統合防衛力がキーワードとされた。これは実質的には、米軍が考慮していたクロスドメイン攻撃やマルチドメイン戦闘（MDB）を想定したものである（これらは後に平時も含めたマルチドメイン作戦とも呼ばれるようになった）。

新しい防衛大綱は、「有事において、我が国への攻撃に際して当該攻撃に用いられる相手方によるサイバー空間の利用を妨げる能力等、サイバー防衛能力の抜本的強化を図る」と述べ、日本に対して（サイバー攻撃に限らず）何らかの攻撃が行われた場合、攻撃者ないし攻

---

[14] 兼松雄一郎「中国、サイバー選挙介入か　カンボジアで『予行演習』」『日本経済新聞』2018 年 8 月 18 日電子版。

[15] 旧称は内閣官房情報セキュリティセンター（NISC）。もともと NISC は National Information Security Center の略だったが、現在では National center of Incident readiness and Strategy for Cybersecurity の略である。

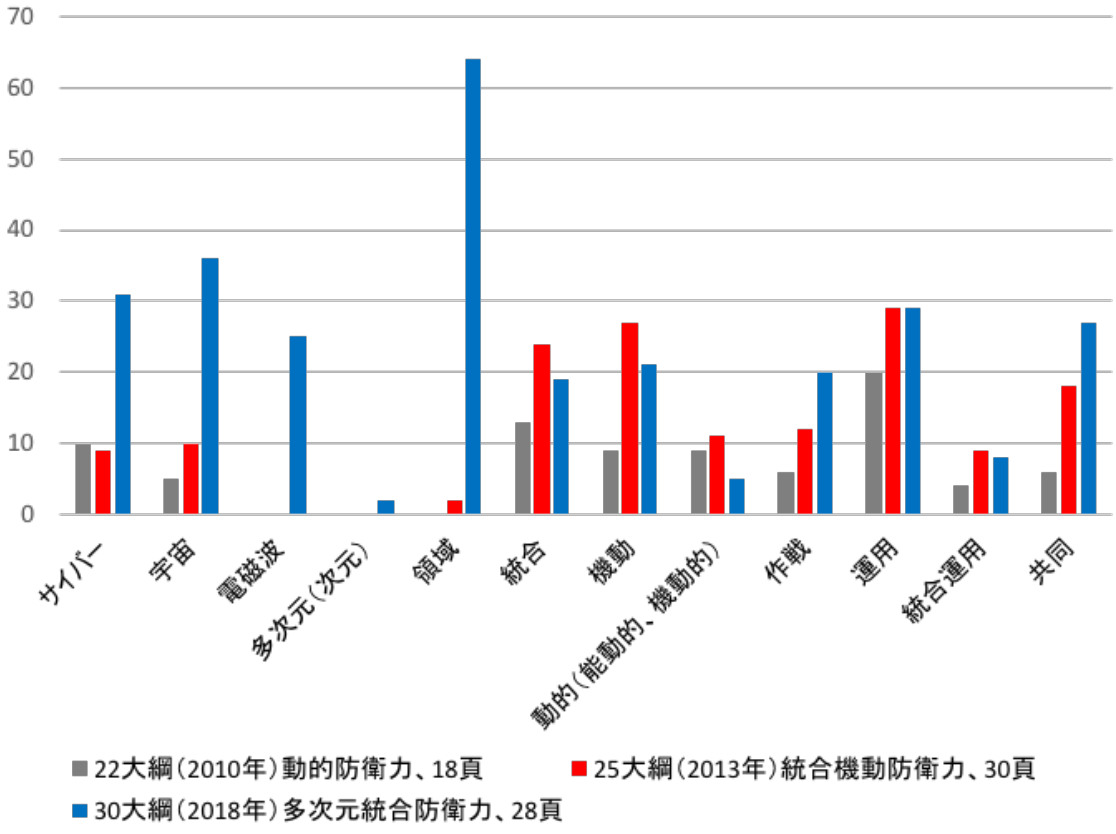
[16] ただし、物理的な被害のないサイバー攻撃において防衛出動命令が出る可能性は低い。逆に物理的な被害が出てしまえば、一般的な自衛権の発動となる可能性が高い。

撃国によるサイバースペースの利用を妨げる、つまり、反撃としてのサイバー攻撃ができるようになった。

さらには、「全ての領域における能力を活用して、我が国周辺において広域にわたり常時継続的な情報収集・警戒監視・偵察（ISR）活動（以下「常続監視」という。）を行うとともに、柔軟に選択される抑止措置等により事態の発生・深刻化を未然に防止する」とも書かれており、全ての「領域」にサイバースペースが含まれるとするなら、そこでの常続監視のための措置が検討されているだろう。

「多次元」とされているが、図表 1 を見れば分かるとおり、「多次元」ないし「次元」はあまり大綱の本文では使われておらず、それは実質的に「領域」を意味しており、サイバースペース、宇宙、そして電磁波という三つの新しい領域での取り組みを拡大することが、今回の防衛大綱の意義だといえるだろう。

図表 1：防衛大綱における用語使用頻度



5. おわりに

現代のサイバーセキュリティにつながるような事例は、すでに米ソ間の冷戦時代の 1980

年代から見ることができる。しかし、2010 年代になって、五つのタイプのサイバー攻撃と多様なアクターが交錯し、複雑化してきている。

日本は多次元統合防衛力の確立に向けた防衛計画の大綱を 2018 年に打ち出したが、その実現に向けた努力を進めるとともに、情勢は日々刻々と進化しているため、時代を先取りした対応も必要であろう。

米国の国家情報長官（DNI）を務めたジェームズ・クラッパー（James Clapper）は、「全ての国は直前の戦争をもう一度戦おうとしているのが軍事的な自明の理である、と国防総省でしばしば聞いた」と著書で述べている 。日本にとっては直前の戦争とは第二次世界大戦であろう。そこでは、暗号戦はあったものの、現代のサイバー戦のような状況は考えにくかった。宇宙、サイバー、電磁波の頭文字をとって「ウサデン」と呼ばれることがあるが、新しい領域での防衛能力の向上が至上命題である。