

ロシアのサイバー軍事力の現状と展望

佐々木 孝 博*

Current Russia's Cyber Military Power and the Future

Takahiro SASAKI

Abstract

Russia states security issues in cyberspace as an important area of national security. In particular, the space is not regarded as a mere communication / information infrastructure, but as a domain where conflicts such as information warfare occur, as the fifth domain after land, sea, air, and space. The “national security strategy,” “military doctrine,” and “information security doctrine” clearly define what the threat to Russia is in that domain and how to counter it. In order to embody that strategy, Russia established an “Information Operation Troops (Cyber Warfare Troops)” in the Armed Forces of Russian Federation. This troops is believed to be a working troops aimed at ensuring information superiority in cyberspace through cyber-attacks and offensive propaganda activities.

In addition, Russia is trying to win by incorporating AI into cyber warfare, which it recognizes as the key of modern and near-future warfare. Russia sees AI as a technology as a game changer to gain hegemony, and by 2030, it is trying to break into the US-China hegemony battle using AI. In the future, it is necessary to carefully look at how Russia intends to utilize AI in the field of cyber warfare, and it is important for Japan to take measures that do not allow Russia to run alone in this field.

* 東海大学客員教授 (Visiting Professor, Tokai University)

要旨

ロシアは、サイバー空間における安全保障問題を国家安全保障の重要な1つの分野と位置付けている。特に、同空間を単なる通信・情報インフラとして捉えるのではなく、情報戦をはじめとする紛争が生起する領域として、陸上、海上、空中、宇宙に次ぐ第5の領域と捉えている。

その領域におけるロシアにとっての脅威はいかなるものなのか、その脅威にどのように対抗していくのかを、「国家安全保障戦略」「軍事ドクトリン」および「情報安全保障ドクトリン」などで明確に規定している。そして、ロシアはその戦略を具現化するために、ロシア連邦軍に「情報作戦部隊（サイバー軍）」を創設した。同部隊はサイバー攻撃や攻勢的なプロパガンダ活動の実施などを通じ、サイバー空間における情報優越を確保することを目的とした実働部隊とみられる。

また、ロシアは、現代戦・近未来戦の雌雄を決するための鍵になると認識しているサイバー戦に、AIを取り入れ、勝ち抜こうとしている。ロシアはAIを、覇権を得るためのゲームチェンジャーとしての技術と捉えており、2030年までに、AIを使って米中の覇権争いに割って入ろうとしている。

今後、ロシアがAIをサイバー戦分野においていかに活用しようとするのかを注意深くみていく必要があり、我が国としては、この分野におけるロシアの独走を許さないような施策をとっていくことが重要となってくるだろう。

キーワード：サイバーセキュリティ、ロシア、影響工作、AI、軍事ドクトリン

1. はじめに

ロシアは近年、物理的な軍事力の行使のみならず、非軍事手段の重要性に目を向け、特に、サイバー空間での活動を活発化させている。同空間においては、2007年の「エストニアの重要インフラへのサイバー攻撃事例」に端を発し、2008年の「グルジア（ジョージア）紛争時のサイバー攻撃事例」、2014年の「クリミア併合時に行われた情報操作・サイバー攻撃事例」、2016年の「米大統領選時のSNS（ソーシャル・ネットワーキング・サービス）による介入事例」および「2020年の史上最大の損害を与えた米政府機関へのサイバー攻撃事例」など、ロシアの関与が疑われている事例が多数生起している。その各々は、「国家機能を麻痺させた初の事例（エストニア事例）」、「軍事行動とサイバー攻撃とを同時に行った初の事例（グルジア事例）」、「初めて大規模に行われたハイブリッド戦（クリミア事例）」「SNSプロパガンダを利用した初の対外的な選挙介入による情報操作事例（米大統領選事例）」など「〇〇初」ともいえるべき事例であった。これだけ複数の事例が積み重なると、ロシアはサイバー空間において、何を狙おうとしているのかの疑問が生じて

くる。また、ロシアは同空間を単なるインフラ・公共財と位置付けているのか、新たな戦争・紛争の領域と位置付けているのかなどの疑問も生じてくる。

そこで本稿においては、ロシアのサイバー軍事力の現状を検証し、サイバー空間でのロシアの狙いを明らかにすることを目的として、まず、サイバー戦略を具体的に定めている「軍事ドクトリン」の内容を読み込み、その行間に隠れる真意を見出していくこととする。

次に、その戦略を具現化するためにどのような体制を構築しているのかを明らかにするために、国防省・ロシア軍に創設された「サイバー軍（情報作戦部隊）」および「国家との関係が深いとみられるサイバー組織」に焦点を当て考察していく。

そして、近未来にロシアがサイバー空間においてAIをいかに軍事適用していこうとしているのかを考察することにより、ロシアのサイバー軍事力の将来を展望していく¹⁾。

2. ロシアのサイバー戦を司る「軍事ドクトリン」

ロシアは2014年12月に、国際的な安全保障環境の変化を受けて、「軍事ドクトリン」を改訂した。本ドクトリンの改訂において、多数のロシア研究者が注目したのが、同年に生じたウクライナ危機（クリミア併合）などを念頭に、米国やNATO（北大西洋条約機構）を脅威として明確に定義したことや、「非核抑止力」という新しい概念を取り入れたことであった。後者の「非核抑止力」については「核兵器以外の手段によって、ロシア連邦に対する侵略を防止するための、対外政策上の手段、軍事的手段および軍事技術的手段の複合体」と定義している。この中の「軍事技術的手段」には情報空間で行われるサイバー攻撃などの非動的な（ノン・キネティックな）戦いが含まれているものと考えられる。これを視点に「軍事ドクトリン」を「軍事戦略の一部としてのサイバー戦略」が記載されている公文書として読み解いていきたい²⁾。

（1）情報空間における紛争の抑止・防止施策

「軍事ドクトリン」の紛争の抑止・防止策の項目において、物理的な軍事施策が複数定義されている中で、情報空間に関わる施策を2点指摘したい。

第1に、軍事紛争を抑止または防止する施策として「政治的・外交的その他の非軍事的手段を用いた、考えうる軍事的危険および軍事的脅威の中立化」を掲げている点である。「その他の非軍事手段」とは、隠密裏にも使用できるサイバー兵器、電子戦兵器および情報戦兵器が念頭におかれたものと考えられ、これらの手段により、情報空間における優越を獲得することが、脅威の中立化に資すると定義しているということである。

第2に、「国際法に違反して国家の主権、政治的独立性、領土の一体性に敵対し、国際

社会、グローバルおよび局地的規模の安定性に脅威を与える活動を行うための軍事・政治目的で情報通信技術（ICT）が利用されるリスクを低減させること」としている点である。「軍事・政治目的で ICT が利用されるリスク」との表現で、サイバー脅威を低減させることが紛争抑止・防止の手段であると規定しているということである。換言すると、相手方の脅威を低減させるということは、攻勢的な活動も含まれると捉えるのが軍事の常識であるので、相手方の効果的な情報空間での活動を阻害するような攻勢的なサイバー攻撃活動も実施すると公言したものと捉えていいだろう。

（2）サイバー空間における軍の活動

「軍事ドクトリン」第3章32項において、ロシア連邦軍を国外で使用する要件について、「ロシア連邦およびその市民の利益を防護し、国際的な平和および安全保障を担保するため、国際慣習法、国際法規範、ロシア連邦が締結した国際条約および連邦法に基づきロシア連邦の国境外において軍の部隊を機動的に使用することができる」と規定している。これは、グルジア紛争（2008年）やウクライナ危機（2014年）において国外でロシア軍を使用した時の根拠として政府が示した内容と同じであり、一義的には物理的に国外で軍事力を使用する要件を定めたものと考えられる。

しかしながら、情報空間においては、物理的な領土、領海、領空の概念が当てはまらない。物理的には国外に所在する情報空間を構成するシステム・ネットワークおよびそのなかを行き交うコンテンツ（中身の情報）に対しても、ロシアの国益擁護のためには軍事力を行使する（サイバー攻撃や世論誘導などを含む情報戦の実施）ことも念頭に置いていると考えていいだろう。

（3）情報戦・サイバー戦実施のための装備

「軍事ドクトリン」第4章46項において、サイバー戦関連で今後発展させるべき軍事装備について、「情報敵対活動を行うための戦力および装備を発展させること」が規定されている。情報敵対活動とは一義的には、相手方の行っている情報作戦に対抗するためのカウンター・インテリジェンス活動を念頭に置いたものと考えられる。

しかし、軍事の常識からすれば、防勢的に対処するより、能動的に対処するほうが効果的であるため、この表現は、サイバー攻撃などの能動的な情報活動を行うための戦力および装備（サイバー攻撃装備、電子戦装備、影響工作のための情報活動の装備など）を充実させることも念頭に入れているものと捉えることができる。

近年、情報戦・サイバー戦に関し、ロシアが最も注力しているのが、SNS プロパガンダによる影響工作である。その代表例が冒頭に述べた「米大統領選への介入事例」だろ

う。SNS プロパガンダには2つの方法が確認されている。1つは「ボット」と呼ばれている方法で、プログラムを使ってコンピュータが自動的にSNSにおいて発言したり、リツイートしたりするものである。今1つは「トロール」と呼ばれているもので、いわゆる人海戦術で大量の発言やリツイートさせることにより、世論を誘導する方法である。さらに、それらを組み合わせた「サイボーク」という方法も確認されている（一田2018：45）。「軍事ドクトリン」により、具体的にこれらの装備の充実に注力すべきと定めたとと言えるだろう。

（4）「軍事ドクトリン」の規定と具体的なサイバー施策

「軍事ドクトリン」ではその他にも、情報空間における脅威認識、およびその脅威へいかに対応するかの指針を明確に定めている。ここでは、「軍事ドクトリン」で記載されている具体的な軍事行動が、どのような指針に基づいているのか、それが情報空間（サイバー空間）ではどのような活動を見積もっているのかなどを、米国のコンサルティング会社のブーズ・アレン・ハミルトンが取りまとめたレポートを基に総括してみたい（Hamilton 2020）。その概要を図表1に示す。

図表.1 サイバー空間における具体的な軍事活動

「軍事ドクトリン」で規定する軍事活動の特性	具体的な指針	サイバー空間における活動
先進兵器・技術の幅広い活用	コンピュータ化、指向性エネルギー、ロボット工学、無人飛行などの先端技術を用いた幅広い兵器の使用	サイバー作戦のツールは、防衛のための技術的・財政的能力を欠く他の国家よりも優位に立つ高度な軍事技術である可能性がある
同時に敵の領土の全縦深に影響を及ぼす戦争・紛争	物理的またはデジタル的な戦場で敵に広範な被害をもたらす能力の使用	サイバー作戦は、標的国のコンピュータ化された機器に広範な被害をもたらす可能性がある
精密破壊攻撃	無差別に被害を与えるのではなく、標的を選択的に破壊する能力の使用	サイバー作戦は、正確な結果を伴って、高度に標的を絞った破壊を引き起こすことができる
先制行動による軍事行動の開始時間の短縮	行動の原因が現れてから行動に移るまでの時間は最小限にしなければならない	正確で破壊的なサイバー攻撃は、通常、時間的に長引いている。したがって、価値の高いデジタルおよびコンピュータ化された目標への永続的なアクセスを事前に確立することが必要である

グローバルなコンピュータ化された指揮統制	コンピュータ・システムにより統一された作戦状況認識を提供し、分散した軍隊の間で統一された決定を可能にする。隷下の下位部隊は、意外性、決断力、積極性をもって主導権を握ることができる	サイバーオペレーターは、迅速かつ決定的な行動をとる権限を与えられている
恒久的な戦争地帯の創設	現代の戦争は常に対立している状態を作り出し、敵に再編成や再評価の機会を与えず、敵のストレスや混乱を増大させる	サイバー作戦は、エスカレーションのリスクを最小限に抑えながら、継続的な競合状態を維持できる
非正規・民営化戦	非正規の戦闘員、民兵、テロリスト、民間軍事会社が戦争に関与すること	サイバー作戦は、軍事的成果を達成するために、雇用契約者、傭兵、その他の非国家主体を利用することができる。この特徴には、正規の軍事オペレーターが軍事目的を達成するために偽の非国家人物を使用することも含まれる
間接戦・非対称戦	同等の戦力を展開することなく脅威を無力化する能力	サイバー作戦は通常、動的戦闘よりも少ない兵力と少ない資材で済む
社会的・政治的環境の操作	相手を社会的に弱体化させるか、より友好的な政治家を設置することを目的として、政治的および社会的運動に影響を与え、支配し、または扇動しようとする試み	サイバー作戦は、政治的・社会的標的の評判を傷つけるような、政治的・社会的操作の取り組みを強化する可能性がある

(出典：Booz Allen Hamilton “*Bearing Witness: Uncovering the Logic Behind Russian Military Cyber Operations*” を基に筆者作成)

3. ロシアの「サイバー軍（情報作戦部隊）」³⁾

(1) 「サイバー軍（情報作戦部隊）」の概要

2014年以降、ロシアのサイバー施策が次々と明らかになってくる過程において、2017年2月22日、セルゲイ・ショイグ（Сергей Кужугетович Шойгу）国防大臣は、国家院（下院）議会に対し「ロシア軍隷下に『情報作戦部隊（Войска информационных операций = Information Operations Troops）』が存在すること」を報告した⁴⁾。この報告と同時期に、ロシアの情報セキュリティ・コンサルティング会社のゼクリオン・アナリティクス（Аналитический центр Zecurion = Zecurion Analytics）が、世界各国の軍事組織が保有する「サイバー軍（Кибервойска = Cyber Troops）」についての分析レポートを発表した⁵⁾。この分析レポートにおいて「サイバー軍」と呼称された組織が、ロシアではショイグ国防大臣が保有すると明言した「情報作戦部隊」に該当するものと考えら

れる。ここで、同分析レポートおよびそれを引用し、独自の評価を行った『コメルサント』紙の分析（Коломыченко 2017）⁶⁾も加味して、ロシア軍が保有する「サイバー軍（情報作戦部隊）」の概要を考察していきたい⁷⁾。

ゼクリオン・アナリティックスの分析レポートでは、ロシアを除く世界各国の「サイバー軍」を独自の基準により評価し、その総合力を順位化している。それを元に、『コメルサント』紙はロシアの評価を加えた⁸⁾。同分析のなかで「サイバーセキュリティへ最も多くの予算を充当している国家は米国であり、米国防総省からは毎年約70億ドルの予算が割り当てられ、当該任務に従事するサイバー兵士の数は9000人以上である。米国に続くのが中国および英国であり、両国の予算は、それぞれ15億ドルおよび4億5000万ドル、サイバー軍兵士の数は、それぞれ2万人と2000人である」と評価した⁹⁾。

一方、同分析レポートでは対象外であったロシアについて、『コメルサント』紙は独自の情報源に基づいて分析を加えており、「ロシアのサイバー軍の構成員数は、約1000人であり、年間予算は、3億ドルが充当されている」と評価した¹⁰⁾。さらに、ゼクリオン・アナリティックスの分析では、予算および兵員数のほかにも、独自の評価基準に基づいてサイバー軍の総合力を順位付けした。その評価項目について、同社のウラジーミル・ウリヤノフ（Владимир Ульянов）分析センター長は、「本ランキングは、年間予算およびサイバー軍兵士数のほかに、潜在的な成長力、法令・規則類、サイバー戦略（情報安全保障戦略）、参考となる国際機関の情報、高官の公式見解や内部情報などにに基づき総合的に評価した」と述べている¹¹⁾。ロシアの能力評価については、独自の分析を行った『コメルサント』紙においても、予算および兵力のランキングを評価したのみであり、これら2つの指標から総合力を判断することは難しい。

しかしながら、ゼクリオン・アナリティックスの掲げたその他の評価項目をロシアに適用し評価を試みると、『軍事ドクトリン』や『情報安全保障ドクトリン』などのサイバー戦略を詳細に規定していること「それを運用するための法令・規則類も適切に整備していること」などは高く評価できる¹²⁾。また、米セキュリティ会社ファイア・アイ、クラウド・ストライク等の分析によれば、「APT28（FANCY BEAR）」「APT29（COZY BEAR）」「VOODOO BEAR」「VENOMOUS BEAR」などと呼称される国家と密接な関係があると見積もられる高度なサイバー攻撃能力を有する組織がロシア国内に複数存在することが確認されている¹³⁾。ロシアの国家としての潜在的なサイバー戦能力は相当程度高いものと見積もっていいだろう。したがって、総合力としては、米国、中国および英国に続くレベルと評価するのが妥当であると考えられる。ゼクリオン・アナリティックスによる各国サイバー軍の総合力（予算・兵力・評価ポイント）の評価に加え、『コメルサント』紙のデータを考察した上での筆者による総合評価（上位10ヶ国及び日本）を図表2に掲げる。

図表.2 各国サイバー軍の総合力（上位10ヶ国及び日本）

	サイバー軍の予算 (100万ドル／年)	サイバー軍の兵士数 (人)	評価ポイント (点)
1位：米国	7000	9000	6.1
2位：中国	1500	20000	5.4
3位：英国	450	2000	4.6
4位：(ロシア)	(300)	(1000)	—
5位：ドイツ	250	1000	3.9
6位：北朝鮮	200	4000	3.8
7位：フランス	220	800	3.4
8位：韓国	400	700	3.4
9位：イスラエル	150	1000	3.4
10位：ポーランド	50	400	3.1
(参考) 11位：日本	250	500	3.0

（出典：Аналитический центр Zecurion, “КИБЕР ВОЙНЫ 2017: БАЛАНС СИЛ В МИРЕ”、ロシアについては『コメルサント』紙のデータに基づく筆者の評価）

ただし、総合力ランキングは、予算やサイバー兵士数など定量的に比較できる分野とは異なり、評価項目の選定や評価方法、さらにはポイントの重みづけ基準などによって、分析組織の主観が入る可能性もあることから、ひとつの参考指標として扱いたい。いずれにしても、ロシアの「サイバー軍（情報作戦部隊）」が高いサイバー戦能力を保有していることは疑う余地はないだろう。

（2）サイバー軍の任務・能力

ショイグ国防相がロシア軍に「サイバー軍（情報作戦部隊）」が存在していることを明言した際に、その任務・能力等は明らかにしなかった¹⁴⁾。したがって、その詳細を明示することは難しい。しかしながら、ゼクリオン・アナリティクスの分析報告を注意深くみていくと、その内容を推察することができる。

ゼクリオン・アナリティクスでは、世界各国が保有する「サイバー軍」は、異なる目標・目的で設立されているとしながらも、根本的には当然実施すべき活動分野があり、次の3つを掲げている¹⁵⁾。

① 秘密情報を得る目的の「エスピオナージ活動（Шпионаж = Espionage）」

- ② 情報システム、テレコミュニケーション網および技術・輸送インフラなどへの物理的な損害をもたらす「サイバー攻撃（Кибератаки = Cyber Attack）」
- ③ メディアおよび SNS を使った「情報戦（Информационные войны = Information Warfare）」

しかし、そのような軍事組織の活動は、一義的には国外からのサイバー攻撃に対する防護を想定しているとしている。前出のウリヤノフ分析センター長もロシアについて「ロシアの『情報安全保障ドクトリン』も、攻撃ではなくまずは防護を念頭においている」という点を指摘している。一義的にはサイバー防護を念頭においていたとしても、サイバー空間というものは、攻撃法が分からなければ防護策を採ることはできない攻防一体の領域である。また、効果的な防護を実施するには、サイバー脅威情報（サイバーインテリジェンス）というものが必要となってくる。したがって、防護能力を高めるために、高い攻撃能力や情報収集能力をロシア軍の「サイバー軍（情報作戦部隊）」が保有していたとしても不思議はない。そのような能力を保有しているのであれば、軍事組織としてそれを活用しないということは考え難いということである。

4. 国家との関係が深いサイバー組織

ここまで、ロシアのサイバー戦に関わる軍の組織について考察してきたが、広くサイバー一軍勢力を捉えた場合、インテリジェンス組織の負う職責は大きいものと見積もられる。そこで国家によるサイバー戦における役割分担を考察してみたい。サイバー空間における活動の全般統括・調整は「国家安全保障会議（情報安全保障に関する省庁間委員会）」が所掌しているとみて間違いないただろう。そして、同空間での戦い（紛争・戦争などに関連する対外工作を含む）については国防省・ロシア軍が、国内の情報安全保障（国内所掌事項と一部関連する対外工作を含む）については連邦保安庁（FSB）が、対外的な国外への情報活動については対外情報庁（SVR）が所掌しているの見積もられる。しかし対外的な活動において、これら3つの組織の隷下で、具体的にどのような組織がその任を担っているのかについては、ロシア側発の一次情報では判別し難い。したがって、本項では、各セキュリティ会社が被攻撃側から入手できるサイバー攻撃の証跡等から分析した調査結果を多数報告しているので、それを基に考察していくこととする。

ロシアによるとみられるサイバー攻撃の証跡（攻撃に使われた IP アドレス¹⁶⁾などの帰属、プログラムに使われた言語、攻撃の行われた時刻帯、過去の同種の攻撃行動との比較など）から分析すると、ロシア軍参謀本部情報総局（GRU）、FSB、SVR と関係が深い

(あるいは命令・指示を受けて行動している)とみられる組織が対外的な任務を担っているという事実を確認することができる。その代表例が、「APT28 (FANCY BEAR)」「APT29 (COZY BEAR)」「VENOMOUS BEAR」および「VOODOO BEAR」といった組織である¹⁷⁾。これらの組織の概要を図表3に示す。

図表.3 サイバー組織概要と国家機関との関連性

組織名称等	関係が疑われる国家機関	行動の概要
APT28 FANCY BEAR 第26165部隊 第74455部隊	ロシア軍参謀本部情報総局 (GRU)	APT28の活動は、米国、NATO、ウクライナを特に標的とし、2004年以降、世界中の政府、外交、軍事、航空宇宙、防衛、エネルギー、メディア、政治組織、反体制派を標的にしている。2018年10月、米国司法省は、APT28が行った作戦に関し GRU 将校数人を起訴。英国の国家サイバーセキュリティセンター (NCSC) は、APT28という名称は GRU の活動そのものを指すと明言
APT29 COZY BEAR Office Monkeys CozyCar The Dukes CozyDuke	連邦保安庁 (FSB)、 対外情報庁 (SVR)	伝統的に APT29は、知的財産を搾取するのではなく、国家の安全保障政策に向けての諜報活動に注力。2016年の米大統領選時、民主党全国委員会の情報に不正アクセス。2020年7月には新型コロナウイルスワクチンの開発に取り組む世界の研究機関にサイバー攻撃を実施。2020年の米政府機関への史上最大の被害を及ぼしたサイバー攻撃に関与。米英加の情報当局は「APT29をロシアの情報機関の一部であることがほぼ確実」と断定
VENOMOUS BEAR Turla Snake Krypton	FSB	主な標的は、政府、航空宇宙、NGO、防衛、暗号学、教育の各セクター。これまでに標的となった組織は、米中央軍 (2008年)、CIS 諸国首相官邸 (2012年)、スイスのテクノロジー企業 RUAG (2014年)、G20の参加者 (2017年)、独政府のコンピュータネットワーク (2018年) など
VOODOO BEAR	GRU	2011年以降、諜報活動や破壊目的で SCADA、政府、メディアを標的。特にウクライナの企業に焦点を当てており、2015年のウクライナのエネルギーグリッド停電も対象とした。使用するツールから GRU との関係が深いとみられる

(出典：Booz Allen Hamilton “*Bearing Witness: Uncovering the Logic Behind Russian Military Cyber Operations*” および小泉悠「プーチン・ロシアの『サイバー攻撃』を暴く」を基に筆者作成)

これらの組織は国家機関直属の組織ではないとみられているが、国家機関と関係が深い(または、関係を曖昧な状態にしている)組織である。国家機関が直属の組織をサイバー攻撃に直接関与させずに、ここで掲げた組織に実行を委ねている理由は、攻撃源を特定された場合、国家の責任ということの追及を逃れるために、その関与を不明確にするといった狙いがあるものと推察される。

5. ロシアのサイバー軍事力の展望¹⁸⁾

プーチン大統領は2019年10月10日、「2030年までの人工知能発展に関する国家戦略¹⁹⁾」を承認した。2017年9月には、「AIの分野でリーダーになれる者（国）こそが世界のリーダーになれる」とも発言している²⁰⁾。ロシアはAI技術を強化することによって、米中の覇権争いに割って入ろうとしている。特に、AI技術は経済・産業分野だけでなく軍事分野でも応用が可能であり、今後の軍事戦略においてもAIを活用した兵器とシステムは重要になると見られることから、AI技術の発展は国家安全保障の強化と国際関係におけるバランスの維持にも直結していると考えている。

そこで本項では、ロシアが近い将来、サイバー空間においてAIをいかに軍事適用していかようしているのかを考察し、ロシアのサイバー軍事力の将来を展望していきたい。

（1）サイバー防衛におけるAIの活用²¹⁾

従来の情報セキュリティ技術では既知の脅威にしか対応できなかった。しかし近年、マシーンラーニング（機械学習）²²⁾を活用することで、未知のマルウェアを検知する技術が生まれてきた。例えば、インターネット上で行き交っているマルウェアに関する情報を収集し、マシーンラーニングを使って分析することで、今後生じる攻撃手法を事前に把握するということである。サイバー防衛に関して現在では、AIはディープラーニング（深層学習）²³⁾を使ってリアルタイムに大量の通信を監視し、サイバー攻撃に共通する事項や攻撃源に関する情報などを解析、その中で異常を検知して新たな脅威の予測と迅速な対策を行っている。ディープラーニングを用いたAIによる分析とは、収集した情報のなかで注目すべき特徴的な点を数多く検出しそれを分析、マルウェアに関する脅威情報（サイバーインテリジェンス）を見出していくというものである。

またAIを活用することで、マルウェアが初めて検出されてから、脆弱性の修正やウイルス対策ソフトの脅威ファイルの作成などの有効な対策を作成するまでの時間を短縮することによって、ゼロデイ攻撃を防止することにも使われている。今後、AIを活用したサイバー防衛分野では、高度なサイバー攻撃を検知し、自動的に監視を行い、自動的に防衛策をとることができるというようなシステムを開発することも期待されている。また、AIは人間の代わりに24時間稼働することができ、マシーンラーニングで判定可能なものは自動化し、管理者の負担を軽減することができる。

ロシアのサイバー防衛システムに関する情報はほとんどオープンになっていないため、具体的にロシアがサイバー防衛にAIをどのように活用しているかは明確ではない。しか

しながら、AIをどのような分野においてサイバー防衛に活用していくかは、各国でも検討されており、各国にロシアが遅れをとるようなことは考え難い。したがって、ロシアが当然推し進めている項目を推定するために、各国が進めているサイバー防衛にAIを活用しようとしている分野を取り上げる。

まずは、「マルウェアの自動検出」である。前述のように既知のマルウェアを大量に学習させれば、その特徴を見出すことができ、人を介することなしにマルウェアを検出できる。「セキュリティシステムにおけるログの監視・解析」「継続的な認証」「通信トラフィックの監視・解析」などにもAIを活用し自動で防護ができる。「情報流出の防止」などにも適用できるだろう。情報流出防止に関しては、国内のインターネット空間の監視・管理を強めたいロシアにとって鍵となる事項と考えられ、今後注力していく分野と推測される。これらは単機能の「弱いAI²⁴⁾」ともいえ、一部はすでに実現している。ロシアも当然、既に導入しているか、今後の活用を考えている分野と見積もられる。

(2) サイバー攻撃におけるAIの活用²⁵⁾

サイバー攻撃の分野においては、AIやマシンラーニングが進展することで、これまでよりも多くの攻撃が自動化するものと見積もられる。例えば、人間が作成するよりも人を騙すことができる巧妙なフィッシング・メール²⁶⁾を作成し、より騙されやすいターゲットに送り付けることができるようになることが見積もられる。

AIを活用した攻撃システムは、サイバー攻撃に使用するターゲットに関する大量の情報を収集し、それをデータベース化し、詳細な情報を攻撃者に与え、攻撃をより迅速かつ的確に実行させることができるようになるだろう。特に、AIを活用すると迅速化できることに注目したい。現状でもクラウド・ストライク社の解析によると、不正侵入の全体的な平均時間は4時間37分とされている。その中で国家が関与しているとみられる攻撃では、ロシアは18分49秒、北朝鮮は2時間20分、中国は4時間、イランが5時間9分、組織犯罪グループは9時間42分と分析されている²⁷⁾。つまり、ロシアが最も短時間で侵入できるということである。この不正侵入に、さらにマシンラーニングやディープラーニングなどのAI技術を活用すると、不正侵入に要する時間も各段に向上してしまい、対処が難しくなるということだ。

また、マシンラーニングを活用して、サイバー防衛側のシステムが使用するスパムメールフィルタ²⁸⁾を混乱させることも可能となるだろう。ネットワーク内でのユーザーの動作を模倣して異常動作の検出を回避することも可能となるであろう。

さらに、AIを活用すれば情報の搾取、DDoS攻撃、パスワードクラッキング²⁹⁾などサイバー攻撃で主用される現在の各種手法を、より巧妙化することができ、人間のハッカー

に代わって、複雑な攻撃を迅速かつ効果的に実施することができるようになるだろう。AIを活用したサイバー攻撃事例は、すでに複数出現している。それらの代表例について、図表4に示す³⁰⁾。

図表.4 「弱いAI」を活用したサイバー攻撃例

攻撃の名称	AIの活用方法	詳細の内容
DeepExploit	最適な攻撃手法の判断	ディープラーニングを侵入テストに利用した例。侵入対象のシステムから収集した情報（OSのバージョンなど）を基に、システム侵入に成功する確率が最も高い攻撃手法を判断して侵入行為を実行。侵入に成功後、侵入したシステムを踏み台にし、内部のシステムに侵入を繰り返す
DeepLocker	・標的の識別 ・マルウェアの秘匿	ディープラーニングを標的型攻撃に利用した例。暗号化したマルウェアを内蔵し、平時は顔認証アプリやビデオアプリとして振舞いながらWebカメラ／マイク経由で標的人物の情報を収集
tAIchi	マルウェアの自動生成	強化学習 ⁽¹⁾ をマルウェア生成に利用した例。既知のマルウェアを強化学習により変形させ、アンチウイルスソフトによる検知を回避するマルウェアを自動生成
Deepfake	・顔の入れ替え ・表現の再現	オートエンコーダー ⁽²⁾ ソフトをフェイク動画の作成に利用した例。オリジナル動画の顔部分を標的人物の顔に入れ替えることでフェイク動画を作成

(出典：日本ネットワークセキュリティ協会「AI x Security」)

- (1) 「強化学習」とは、ある環境内において現在の状態を観測し、取るべき行動を決定する問題を扱う機械学習の一種。
- (2) 「オートエンコーダー」とは、ニューラル・ネットワークのひとつ。入力されたデータを一度圧縮し、重要な特徴量だけを残したあと、再度もとの次元に復元処理をするアルゴリズムを意味する。

攻撃分野でもロシアの公開情報は明確ではないが、サイバー強国が一般的に考えている手法は当然ロシアも考えているだろうということは容易に推察できる。具体的には、第1は「脆弱性情報の悪用」が挙げられる。脆弱性情報を収集し、それをデータベース化し、その情報を学習して攻撃行動を自動化することが考えられる。第2は「行動予測による標的型攻撃」も想定される。人間の行動やシステム内部の脆弱性を予測し、最適な標的型攻撃を自動で実行することである。第3は「チャットボット³¹⁾による詐欺」の可能性も考えられる。悪意に基づきユーザーを誘導するチャットボットにより、ソーシャルエンジニアリング³²⁾を自動化することである。第4は「認証情報の偽造」にもAIを利用する可能性がある。これらも単機能の「弱いAI」であり、今後容易に導入されることが見積もら

れる。

またAIを活用すれば、攻撃源を秘匿し相手方からのアトリビューション調査からも逃れることができ、反撃を防ぐこともできる。これらは、サイバー攻撃と防護に関する大量のデータとマシンラーニング、強力なマシンパワーをもったコンピュータがあれば近い将来可能になると見積もられる。さらに攻撃側・防御側がともにAI技術を発展させると、多機能で「強いAI³³⁾」へと進展し、サイバー空間における戦いは、人間が関与しない「AI対AI」の戦いに移行していくものと考えられる。

元在日米軍サイバーセキュリティ責任者のスコット・ジャーコフ氏（Scott Jarkoff：筆者が防衛省統合幕僚監部サイバー企画調整官として勤務していた時の在日米軍のカウンターパートであり、在日米軍退役後、米セキュリティ会社のマカフィーおよびクラウド・ストライクの日本法人で引き続きサイバー問題の専門家として勤務）が、これらのサイバー攻撃におけるAIの適用に関するロシアや中国の情報を入手し、産経新聞に発表した。ジャーコフ氏によれば中露がAIの使用で攻撃を強化できる最大の利点は「睡眠を取る必要がないので攻撃の効率が大幅に上がる」ということである。

また「AIが大量のデータを基に自ら学習するディープラーニングを行うことで攻撃の技術や手口のレベルが自動的に上がり、特に人材育成しなくても優秀なハッカー（攻撃者）を創出することができる」とのことである。「人間のハッカーであれば手法の特性・傾向や攻撃を実施する時間帯などの証跡から攻撃源を特定されやすいが、AIを活用した攻撃ではアトリビューション調査が難しく、攻撃側は追跡から逃れやすい」ということで、反撃を受けにくいということも指摘している。

（3）影響工作におけるAIの活用

EUが設定した「欧州ハイブリッド脅威対策センター」の分析によれば、ロシアによるサイバー空間におけるAI適用形態の見積もりでは、情報操作や世論誘導を主とした影響工作におけるAIの活用が大きな割合を占めるとしている³⁴⁾。現在でも、情報操作などの作戦は人海戦術で行う트롤作戦のほかにも、プログラムが自動で「偽情報（ディスインフォメーション）」を拡散するボットも多数使用されている。これにAIを活用すれば、人間の関与がより少なく自律的に情報操作を行うことが可能となる。

現代戦・近未来戦における情報作戦は、最前線の戦地の兵士をターゲットに行われるのは勿論、相手国内の一般民衆、兵士の家族などに行われることも想定されている。最新のディープ・フェイク³⁵⁾技術を利用すれば、真偽の判別が困難な動画を作成することも可能となる。例えば、残虐行為を行っている米軍を描いたディープ・フェイク動画が拡散されると、活動地域において残虐行為が実際に行われるのではないかと不安を引き起こさ

せることもできる。米軍に対する国際的な非難を起こすことも想定される。米本国では政府に対する非難も生起し、政権自体も不安定な混乱状況にすることも可能となる。

ロシアは敵対する国家機関を弱体化させることに焦点をあてて、情報操作により一般国民の心理的側面をつく行動に出ている。これは米大統領選への関与の事例などからも明らかである。そして、AIの技術的進歩はロシアの「偽情報（ディスインフォメーション）」と「戦略的な情報リーク（正しい情報が悪意をもって拡散される手法）」を利用した影響工作を各段に進化させる可能性を秘めている。選挙干渉などの影響力の行使にはマシンラーニングが利用され、人種、民族、イデオロギー、人口統計や地理的条件など、利用し得るあらゆるデータを収集し、分析し、マイクロ・ターゲッティング³⁶⁾に利用することが可能となる。それも、人が関与することなく自律的に実施できるようになると見積もられる。

2016年の米大統領選挙では、人海戦術によりマイクロ・ターゲッティングに必要なデータを収集していたが、今後はそれもAIを活用し実施していくことになるだろう。また情報を拡散するには、AIが創造した偽りの合成アカウント³⁷⁾やサイバー攻撃によって盗み出したアカウントなどが利用され、加速度的に偽りの情報が拡散することも想定される。すでに言語領域のAIは革新的に発達しており、人が作成するテキストとAIが作成するテキストを識別することは困難になりつつある。ロシアには、伝統的に情報戦を繰り返してきた歴史がある。現在ロシアは、その手段として従来のやり方に加え、サイバー空間を利用し、AI技術を活用し、人間の「認知領域」をも支配し、革新的に情報戦を勝ち抜こうとしているともいえる。

（4）サイバー空間におけるAI活用の課題³⁸⁾

このように、サイバー攻撃および防衛などの分野において有効な活用が期待できるAIにも脆弱性がある。それは、AI自身が騙されやすいということである。特に「教師ありAI³⁹⁾」でそれは顕著である。誤ったデータを、悪意を持つ攻撃者によって学習させられた場合、そのAIアルゴリズムは期待される結果とはまったく異なる答えを出力してしまうということだ。

この代表例は、「パンダの画像にノイズを加えたという試験」である。AIでは57.7%の信頼度でパンダと認識する画像に、8.2%の信頼度で線形動物（回虫など）と認識するわずかなデータをノイズとして加えると、その出力画像は人間の目では引き続きパンダと認識できる画像ではあるが、AIは99.3%の信頼度でテナガザルと認識してしまったという試験結果である。

また、マイクロソフトが2016年3月に行った試験も特徴的である。マイクロソフトでは

「テイ」という設定上は「19歳の米国の女性を模擬した」という AI にツイッターの対話から自己学習する試験を行った。しかし、ツイッターの発言から差別的な言葉を大量に教え込まれ、一日で差別的な発言を繰り返すようになり試験を終了せざるを得なかった事例である。AI を騙すことが可能な一定の入力パターンが分かれば、AI の行う動作や判断を混乱させることができるということである。このような AI を誤作動させるようなサイバー攻撃が、AI の効果的で安全な利用を行う上での課題であるが、これに関する研究はまだまだ進んでいないのが実情である。AI を活用し、サイバー攻撃を企図するロシアの課題はここにあるとみられる。AI に対する攻撃手法はすでに複数の種別が出現しており、その代表例を図表 5 に示す⁴⁰⁾。

図表 5 AI に対する攻撃例

攻撃種別	分類	詳細の内容
回避攻撃	・透明化攻撃 ・なりすまし攻撃	人間には認識できないノイズの内容を含んだデータ入力により、人間と機械学習の推論エンジンとで異なる認識を起こす攻撃（本文中のパンダ事例などが該当）
中毒攻撃	・可用性攻撃 ・バックドア攻撃	学習データへの「不正データ入力」により、学習モデルの境界を何らかの方法によりシフトする攻撃（本文中のマイクロソフト事例が該当）。
移転攻撃	・プライバシー攻撃 ・メンバーシップ推論攻撃	機械学習の「推論エンジン」へのデータの入出力または反応」によって元データなどの機密情報を抽出する攻撃

（出典：日本ネットワークセキュリティ協会「AI x Security」）

また、サイバー空間における LAWS（自律型致死兵器）の問題もある。2019年11月、プーチン大統領は AI 関連のイベントに出席し、「AI 技術の発展には『倫理面でのルール』『モラルのルール』を整備していくことが必要だ。AI を搭載したロボットが発展するにつれて、人間の関与が安全確保のために必要である。社会での AI 技術の活用に向けた倫理面、モラルの観点からの議論は行われており、今後もそのような議論を行っていくことが非常に重要である」と発言していた⁴¹⁾。このことから、ロシアはサイバー空間においても、AI の発展が国家の管理下におけない情勢になることを危惧しているとみられる。

一方で、ロシアはサイバー空間の安全保障分野において他国がロシアに先んじて意思決定機能をもつ自律型兵器の開発に成功し、同空間での優越を確保してしまうことも危惧しているものとみられる。一義的には、サイバー空間における LAWS の危険性が具体的に

判明するまでは、ロシアとしても意思決定機能をもつ自律型兵器の開発を最優先するものと考えられる。しかしながら、LAWS の危険性が具体的に判明し、国家によるコントロールが及ばないと判断した場合には、国際枠組みなどにより、その危険性を低減する施策を進めるものと見積もられる。

6. おわりに

ロシアはサイバー空間における安全保障問題を国家安全保障の重要な1つの分野と位置付け、特に、同空間を単なる通信・情報インフラとして捉えるのではなく、情報戦をはじめとする紛争が生起する領域（ドメイン）として、陸上、海上、空中、宇宙に次ぐ第5の領域と捉えている。そしてその領域において、優越を確保することが国益を担保するためには必須であると考えている。そのために、同領域におけるロシアにとっての脅威はいかなるものなのか、その脅威にどのように対抗していくのかを、「国家安全保障戦略」「軍事ドクトリン」および「情報安全保障ドクトリン」などで明確に規定している。

そして、ロシアはその戦略を具現化するために、必要な組織が不十分であるならば、即座に新しい組織を立ち上げるということも実行している。それが、サイバー空間において戦うための組織としてロシア軍に創設された「情報作戦部隊（サイバー軍）」である。

同部隊はサイバー攻撃や攻勢的なプロパガンダ活動の実施などを通じ、情報空間における情報優越を確保し、脅威対象の国家と「物理的に戦わずして勝つ」「物理的に戦う前に雌雄を決する」ことを目的とした非動的な（ノン・キネティックな）戦いを実行するために創設された実働部隊とみられる。

これらの考察に加えて、ロシアが近い将来、サイバー空間においてAIを活用し、それをいかに軍事適用していこうとしているかを検証した。

ロシアは、現代戦・近未来戦において情報戦を中心に位置づけていることは間違いない。その中でも、特にサイバー戦に焦点を当てているとみられる。

ユーリー・ボリソフ副首相によれば「AIの力を活用することで、ロシアはより効果的に情報作戦に対抗することができ、サイバー戦争で勝利することができる」とのことである。このことから、ロシアが現代戦・近未来戦の雌雄を決するための鍵になると認識しているサイバー戦に、AIを取り入れ、勝ち抜こうとしている姿勢を伺うことができる。

ロシアはAIを、覇権を得るためのゲームチェンジャーとしての技術と捉えており、2030年までに、AIを使って米中の覇権争いに割って入ろうとしている。今後、ロシアがAIを軍事分野、とりわけサイバー戦分野においていかに活用しようとするのかを注意深くみていく必要があり、我が国としては、この分野におけるロシアの独走を許さないよう

な施策をとっていくことが重要となってくるだろう。このような、サイバー空間におけるロシアの現状を正確に把握したうえで、今後の我が国の政策を的確に制定し、体制を整備し、国家が確実に統制する形でサイバー空間での安全を確保していくことが重要となってくるだろう。

参考文献

- 一田和樹 (2018) 『フェイクニュース——新しい戦略的戦争兵器』 角川新書
- 佐々木孝博 (2021) 『近未来戦の核心サイバー戦－情報大国ロシアの全貌』 育鵬社
- 佐々木孝博 (2015) 「サイバー戦の必要性からみたロシアの軍事ドクトリン改訂」『ディフェンス第53号』 隊友会、2015年10月30日
- 佐藤仁「ロシア、プーチン大統領：AI 技術発展に伴う『倫理面でのルール』作りの必要性強調」Yahoo News、2019年12月8日、
<https://news.yahoo.co.jp/byline/satohitoshi/20191208-00154111/> (2021年4月12日取得)
- Hamilton, Booz Allen (2020) “*Bearing Witness: Uncovering the Logic Behind Russian Military Cyber Operations*”, April 4, 2020, https://library.cyentia.com/report/report_003459.html (last visited, April 12, 2021).
- Аналитический центр Zecurion (Zecurion Analytics), “*КИБЕР ВОЙНЫ 2017: БАЛАНС СИЛ В МИРЕ*”, январь 2017
〈http://www.zecurion.ru/upload/iblock/cb8/cyberarmy_research_2017_fin.pdf〉 (last visited, April 12, 2021)

註

- 1) 本稿は、拙著「近未来戦の核心サイバー戦－情報大国ロシアの全貌」(育鵬社、2021年10月22日)を基にしている。
- 2) この項、拙稿「サイバー戦の必要性からみたロシアの軍事ドクトリン改訂」『ディフェンス第53号』(隊友会、2015年10月30日)を基に加筆・修正した。
- 3) この項、拙稿「情報大国ロシアのサイバー戦(2)」『治安フォーラム令和3年7月号』(立花書房、2021年6月)を基に加筆・修正した。
- 4) BBC, “*Russian military admits significant cyber-war effort*”, 23 Feb.2017
〈<http://www.bbc.com/news/world-europe-39062663>〉(2020.4.12).
- 5) (2021.4.12).
- 6) なお、「Коммерсантъ」(『コメルサント』紙)は、政治・経済記事を中心とするロシアの日刊全国紙である。
- 7) これら分析評価を取り上げる理由については、以下のことが考えられるためである。ロシアではソ連時代から引き続き言論統制や世論誘導等の施策が行われている状況が見受けられている。国家機関が何らかの情報発信をした際は、国家と関係の深いメディアなどがそれを補う形で情報発信することが多い。2017年初頭のロシア軍のサイバー関連部隊の創設に関する情報発信と当該分析評価が非常に近い時期に行われたことから、両者が密接に関係しており、ロシアが国家として公的に対外発表できない事項について、メディアを活

- 用して公表したのではないかと判断したためである。
- 8) Коломыченко, “*В интернет ввели кибервойска, Аналитики оценили количество хакеров на госслужбе*”.
 - 9) Аналитический центр Zecurion (Zecurion Analytics), “*КИБЕР ВОЙНЫ 2017: БАЛАНС СИЛ В МИРЕ*”.
 - 10) Коломыченко, “*В интернет ввели кибервойска, Аналитики оценили количество хакеров на госслужбе*”.
 - 11) Аналитический центр Zecurion (Zecurion Analytics), “*КИБЕР ВОЙНЫ 2017: БАЛАНС СИЛ В МИРЕ*”.
 - 12) ポイントの算定方法、各評価項目の重みづけなどの詳細については、分析報告に記述されていないので不明である。
 - 13) ファイア・アイ「APT28：ロシア当局から支援を受けたサイバー・スパイ活動の可能性について」『ファイア・アイ HP』2014年10月27日〈<https://www.fireeye.jp/company/press-releases/2014/apt28-a-window-into-russias-cyber-espionage-operations.html>〉(2021年4月21日アクセス)。
 - 14) BBC, “*Russian military admits significant cyber-war effort*”.
 - 15) Аналитический центр Zecurion (Zecurion Analytics), “*КИБЕР ВОЙНЫ 2017: БАЛАНС СИЛ В МИРЕ*”.
 - 16) 「IP アドレス (Internet Protocol Address)」とは、インターネット・プロトコールにおいて、パケットを送受信する機器を判別するための固有の識別番号のこと。サイバー攻撃の攻撃源を判別する際に必須の情報である。
 - 17) 「APT (Advanced Persistent Threat) ○○」との呼称は、ファイア・アイが付与した名称であり、「○○ Bear」との呼称は、クラウド・ストライクが付与した名称である。
 - 18) この項、拙稿「情報大国ロシアのサイバー戦(6)」『治安フォーラム令和3年11月号』(立花書房、2021年10月)を基に加筆・修正した。
 - 19) Администрация Президента Российской Федерации, “*Национальная стратегия развития искусственного интеллекта на период до 2030 года*”.
 - 20) CNN「AIを制する国が『世界を支配』、プーチン大統領が持論展開」『CNN HP』2017年9月4日〈<https://www.cnn.co.jp/tech/35106734.html>〉(2021年4月12日アクセス)。
 - 21) この項、原田泉「サイバー強国中国といかに向き合うか」『危機管理研究第27号』2019年3月〈https://crmsj.org/journal/27/crmsj_journal_27_1.pdf〉(2021年4月12日アクセス)を参考としている
 - 22) 「マシンラーニング (Machine Learning)：機械学習」とは、経験からの学習により自動で改善するコンピュータアルゴリズムもしくはその研究領域で、人工知能の一種である。「訓練データ」もしくは「学習データ」と呼ばれるデータを使って学習し、学習結果を使って何らかのタスクをこなす。例えば過去のスパムメールを訓練データとして用いて学習し、スパムフィルタリングというタスクをこなす、といったことが可能となる。
 - 23) 「ディープラーニング (Deep learning)：深層学習」とは、対象の全体像から細部までの各々の粒度の概念を階層構造として関連させて学習する手法のことである。深層学習として最も普及した手法は、多層の人工ニューラル・ネットワーク (ディープ・ニューラル・ネットワーク：Deep Neural Network) による機械学習手法である。

- 24) 「弱い AI」とは高度に専門化された問題のみを解決できる AI のこと。
- 25) この項、原田「サイバー強国中国といかに向き合うか」を参考にしている。
- 26) 「フィッシング詐欺」とは、ネットバンキングやクレジットカード会社、有名企業になりすまして個人情報をだましとる詐欺の手口のこと。手法としては、企業からのお知らせメールを装い、本物そっくりに偽装したホームページへ誘導し、ログイン ID、パスワード、クレジットカード番号などの個人情報を入力させる。その際に利用されるメールを「フィッシング・メール」という。
- 27) シャーロット・ジー『『北朝鮮の 8 倍速い』ロシアのハッカー集団、驚きのスピードで圧倒』『MIT Technology Review』2019年 2 月21日 〈<https://www.technologyreview.jp/nl/russian-hackers-are-eight-times-faster-than-north-korean-groups/>〉(2021年 4 月12日アクセス)。
- 28) 「スパムメールフィルタ」とは、迷惑メールの疑いがあるメールを受信したときに、自動的に専用フォルダー（[迷惑メール] フォルダー等）へ移動するなどの機能のことをいう。
- 29) 「パスワードクラッキング (Password Cracking)」とは、コンピュータシステムで保存あるいは伝達されるデータからパスワードを割り出すクラッキング手法をいう。
- 30) 日本ネットワークセキュリティ協会「AI x Security」2020年 3 月 4 日 〈https://www.soumu.go.jp/main_content/000696633.pdf〉(2021年 4 月12日アクセス)。
- 31) 「チャットボット (Chatbot)」とは、「チャット」と「ボット」を組み合わせた言葉で、人工知能を活用した「自動会話プログラム」のこと。
- 32) 「ソーシャルエンジニアリング (Social Engineering)」とは、人間の心理的な隙や、行動のミスにつけ込んで個人が持つ秘密情報を入手する方法を指す。
- 33) 「強い AI」とは、様々な問題を解決し考え相互に作用し変化に対応できる AI のこと。人間に近づく AI とも言える。
- 34) European Centre of Excellence for countering Hybrid Threat, “Addressing Hybrid Threat”, 〈<https://www.hybridcoe.fi/wp-content/uploads/2018/05/Trevertton-Addressing-HybridThreats.pdf#search=%27Addressing+Russian+Hybrid+Threats%27>〉(2021.4.12)。
- 35) 「ディープ・フェイク (Deep Fake)」は本来、機械学習アルゴリズムのひとつである深層学習（ディープラーニング）を使用して、ふたつの画像や動画の一部を結合させ元とは異なる動画を作成する技術である。現在、世間で言われているディープ・フェイクはフェイク動画、偽動画を指すことが多い。現実の映像や音声、画像の一部を加工して偽の情報を組み込み、あたかも本物のように見せかけて相手をだます方法として認識されつつある。
- 36) 「マイクロ・ターゲッティング」とは、選挙運動やマーケティングなどで、対象とする個人に関する情報を詳細に分析し、嗜好や行動パターンを把握することによって選挙に役立てるといったようなビッグデータシステムおよびその戦略の総称のこと。
- 37) 偽りの情報でユーザーを惑わせる偽のアカウントのなかには、AI で合成したプロフィール写真を使っているアカウントもあることが判明している。
- 38) この項、原田「サイバー強国中国といかに向き合うか」を参考にしている。
- 39) 「教師あり AI」とは、「正しいデータ」という名の教師がいて、そこに不明なデータを持ち寄った際には正解を教えてくれるというイメージで機能する AI のこと。正解となる膨大なデータを学習することで、新しいデータに対しても対応が可能となる。
- 40) 日本ネットワークセキュリティ協会「AI x Security」。