サイバー研究所の分析

井手　達夫

はじめに

想像力がなく、夢を見ない人間に未来はない。

シモン・ペレス　元イスラエル大統領[1]

20世紀末、サイバー空間が広く一般に開放されたことにより、時空は瞬く間に圧縮された。空間を隔てた2者間において、かつて郵便を用い、数日から数週間かけて送られていた文字や画像は、今や電子メールで即時かつ安価に届けられるようになった。音声や動画についても、国家間、企業間でしか採算の合わなかったテレビ電話等は、すでに庶民のものである。それらを通じ組織を超え、国境を超え、今日人々は緊密に結びつくことができるようになった。

同時に時間の流れも急速となった。異質のものが交じり合う中にイノベーションは随所で起こり、世界は著しい変貌を遂げている。電話が5000万人のユーザーを獲得するまでに要した時間は75年であったが、インターネットでは4年である[2]。新たな技術が生まれ、それが商品化され、社会に出てくるまでの期間は、20世紀であれば年単位の時間が必要であったが、21世紀であれば、月単位、日単位、あるいは時間単位になるのかもしれない。

このように目まぐるしく物事が移り変わる中、諸外国においては既にサイバー領域専門の研究所を創設し、その動向を見極め、その成果を施策や装備、また教育訓練に反映させている。我が国でも、昨年（2018年）末発簡された30大綱の中に、国内外の先端技術動向について調査・分析等を行うシンクタンクの活用や創設等が謳われており、今後その早期具現化

---

[1] 『WIRED』2016年9月28日、https://wired.jp/2016/09/28/shimon-peres-interview/、2019年3月20日参照。この語の後を継いで「世の中にはたくさんの専門家がいるが、彼らは過去に起きたことの専門家に過ぎない。これから起こる何かについては、誰も確かなことは言えないのだ。だからわれわれは、子どもたち、そして自分自身に夢を見ることを教えなければならない。これまでに起こったことがない出来事を想像できる力こそが、未来を生き抜くためには必要なのだから。」としている。

[2] Carl Benedikt Frey, Michael Osborne, “TECHNOLOGY AT WORK -The Future of Innovation and Employment,” *CITI Grobal Perspective & Solutions,* February 2015, p. 13.

が望まれる。

本論は、それに先立ち各国のサイバー研究所の現況を分析するものである。第 1 節　研究背景では、30 大綱の言及を吟味した上で、研究所の必要性を説明する。第 2 節　研究手法では、研究所を定義した上で、研究対象と方法を明示する。第 3 節　実例検証では、各国のサイバー研究所の事例を概観する。第 4 節　分析・考察ではそれらの事例を分類、吟味し、検討を加える順で論を進める事とする。

1　研究背景

世の中には 2 通りの企業がある。サイバー攻撃を受けた企業と、攻撃されたことにまだ気付いていない企業だ。

ケレン・エラザリ　サイバーセキュリティ研究者[3]

（1）30 大綱の中でのサイバーに関する言及

今日、サイバーセキュリティ問題は、社会の喫緊の課題となっている。30 大綱の中でもサイバー領域は、宇宙、電磁波と並んで我が国にとり、優位性を獲得することが死活的に重要な領域とされ、抜本的に強化し得るようサイバー防衛部隊を保持することが謳われている。

ア　「サイバー」の言及頻度

30 大綱の文中におけるサイバー領域の重要性の認識を、改めてその出現頻度から明らかにしてみた。

使用したのは KH Coder というテキストマイニングツールで、対象を文書全文とし、複合語については形態素解析（品詞分解）「Chasen」を用いて抽出、1 語とカウントするようにした。

その結果「サイバー」の語は、総語数約 5775 語中、34 回と 9 番目に高い頻度で登場している[4]。同じく重要とされている「電磁波(19 回)」は 22 位、「宇宙(16 回)」は 32 位であり、これをみても、その重視の姿勢を読み取ることができる。

---

[3] 『IT メディア』2016 年 1 月 22 日。サイバーセキュリティ業界の格言としてケレン・エラザリ氏が国際会議「CODE　BLUE」で紹介した。

[4] 8 位までの語は「強化（118 回）」「我が国（97 回）」「能力（54 回）」「推進（49 回）」「行う（48 回）」「安全保障（45 回）」「領域（41 回）」「防衛力（39 回）」であった。

イ　「サイバー」の位置付け

次にどのような文脈で用いられているかを明らかにするために、同じく KH Coder を用いて「サイバー」の現れる段落中、同時に現れた（共起した）語との関連を共起ネットワーク図（語の関係性（共起の度合）を図示したもの）を用いて調べてみた。

その結果は図 1 のとおりである。関連性（共起度）の強いものほど太い線で描画され、バブルが大きいほど出現数が多い。

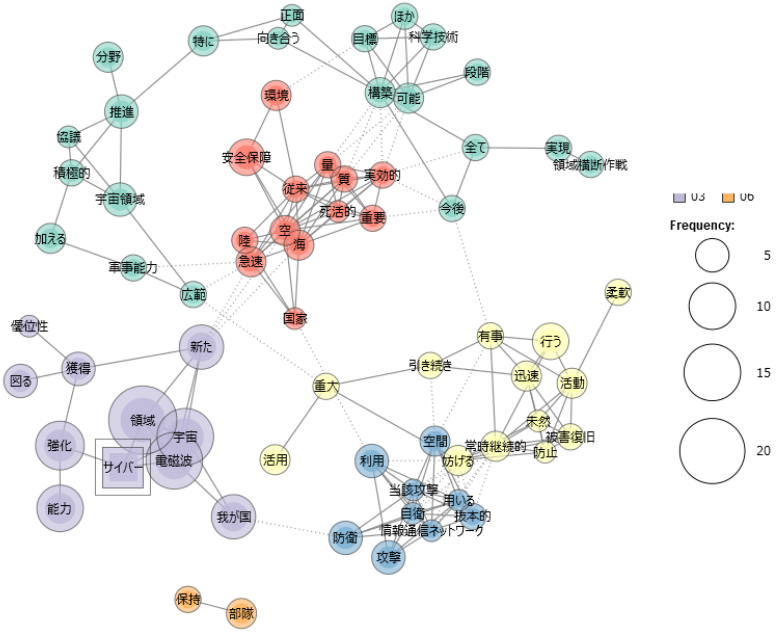

図 1　サイバーの語を中心とした共起ネットワーク図
（筆者作成）

これを見ると、「サイバー」の語は「宇宙」「電磁波」「領域」「強化」という語と強い結びつきを持っていることがわかる。すなわちサイバー領域は宇宙、電磁波と並んで新たな領域として認識され、強化していく対象ということが強調されているのを改めて読み取ることができる。抜本的な強化のためにサイバー防衛部隊の保持が謳われたのも、その所以である。

（2）サイバー研究所（シンクタンク）の必要性

しかしながら主として実務を担当するサイバー防衛部隊のみならず、今後専門的な研究を行うサイバー研究所（シンクタンク）も必要になってくるのではないだろうか。

30 大綱の中でも「シンクタンク」の語は 2 度出てきている。初出は「技術基盤の強化」の項の中に「革新的・萌芽的な技術の早期発掘やその育成を狙う」とあり、2 度目は及び「知的基盤」の項の中に「防衛研究所の活動の充実と大学、シンクタンク等との教育・研究に係る組織的な連携を図る」とある。

ここではサイバー研究所（シンクタンク）が必要とされる理由を、この領域における知見の拡大、変化の加速、情報共有の必要性の観点から明らかにする。

ア　知見の拡大

拡大するサイバー領域の中で、サイバーセキュリティに関する知見は、増加の一途を辿っている。

今日、インターネットに接続される機器の数が増大している。情報を交換する機材のみならず、機械を制御する装置の接続数も増える一方である。そのような IoT（Internet of Things）ディバイスは 2014 年には約 170 億台であったものが、2020 年には約 403 億台、約 2.4 倍になると言われている[5]。

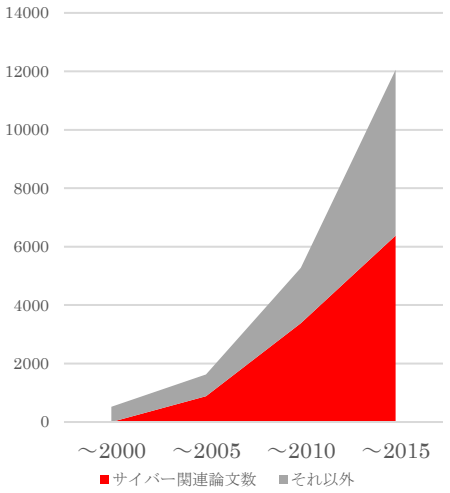

図 2　サイバー関連論文の割合
（出典：井手ほか「セキュリティ分野の学術俯瞰」を基に筆者作成）

それに伴い人のみならず、機械もそのステータス等の膨大な量のデータを生み出すようになった。そのため人類の扱うことのできる情報は情報爆発ともいわれるほど幾何級数的に増大している。その量は 2000 年代には 6.2EB だったものが

[5] 総務省『情報通信白書』平成 30 年度版、http://www.soumu.go.jp/johotsusintokei/whitepaper/ja/h30/html/nd111200.html 、2019 年 3 月 20 日参照。

2020 年には 35ZB にもなると言われている[6]。

同時にサイバー領域に関する知見も増える一方である。図 2 は 1900 年からこれまでの論文を収録している学術論文データベース Web of Science Core Collection に対し、収録されているものに対して“security”をタイトル・キーワード・アブストラクトに含むものを抽出し、引用関係にあるものの中でサイバー関連論文とそれ以外に分類したものである。その結果、2000 年以降、論文総数は急速に増加し、2010 年以降過半数を占めるに至ったことが分かる[7]。

このように、インターネットの覆域の拡大とともに、生み出される情報は増加し、サイバーセキュリティ分野に関する知見も大幅に増大しつつある。

イ　変化の加速

知見の急速な拡大に伴う爆発的なイノベーションにより、サイバー領域をめぐる環境も大きく変化している。

イノベーションの進展とともに、新たなハード・ソフトの拡大の速度は早まる一方である。5000 万人のユーザーを獲得するまでの時間について、20 世紀広く一般に普及したラジオは 38 年かかったが、テレビでは 13 年であった。21 世紀に入り広まっているフェイスブックは 3.5 年、アングリーバード(ゲーム)は 35 日でしかない[8]。

同様にマルウエアも次々に開発され広まっている。図 3 は総務省の発刊した情報通信白書による脅威の変遷であるが、これを見ると 90 年代の Happy99、Melissa に始まり、新たな種類のものが続々と開発され、その手法も、次第に高度化しつつあることが分かる[9]。

その対象も個人から組織、重要インフラから国家までに広がっている。その目的も個人の快楽から経済的な利益、政治的な主張にまでに至っている。

このように、内容、手法、対象、目的ともに目まぐるしく変化し、その

---

[6] 喜連川優「情報爆発のこれまでとこれから」『電子情報通信学会誌』Vol. 94, No. 8, 2011、662-663 頁。原典は Horizon Information Strategies, cited from Strange New Game New rules, p. 34.

[7] 井手達夫、高野泰朋、橋本正弘「セキュリティ分野の学術俯瞰」『情報システム学会誌』Vol. 12、No.　2、2017 年、37 頁。

[8] Frey, Osborne, “TECHNOLOGY AT WORK,” p. 13.

[9] AVTEST-The Independent IT-Security Institute ホームページ（https://www.av-test.org/en/statistics/malware/）によると、毎日 35 万件以上登録されている。

パラダイムも大きくシフトしている[10]。

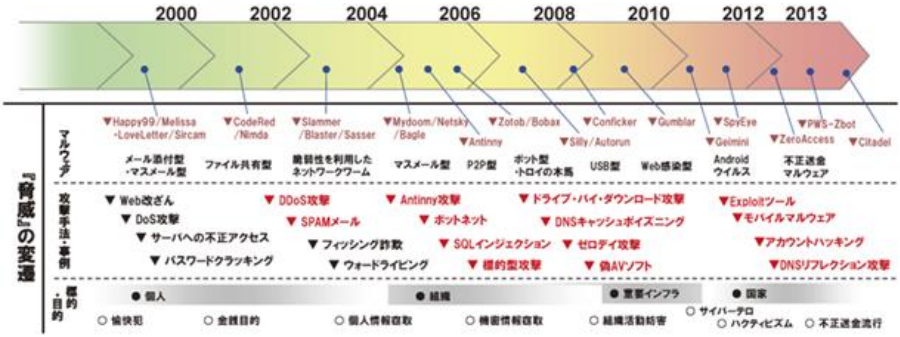

図 3　脅威の変遷（出典：総務省　平成 26 年度情報白書）

ウ　情報共有の必要性

このようなサイバー領域では、その防護のために関連組織間の情報共有が必要となる。

これまでの陸海空や宇宙とは異なり、この領域は人工領域であり、それを構成するソフトウエア、ハードウエア、ネットワーク等を提供、運営するのは、主として民間事業者である。加えて金融、電力、鉄道といった国家の重要インフラもネットワーク化される趨勢にあり、そのセキュア化にはそれらの事業者の協力が求められる[11]。

また種々の攻撃により、サイバー犯罪が世界経済全般に与える経済損失は、約 6000 億ドル（約 67 兆円）と推定されている[12]。そのような中にあって、被害を受けても企業価値等を損なわぬよう公表は憚られる傾向にあるものの、その局限には組織間における被害情報等の共有が必要となる[13]。

---

10 総務省『情報通信白書』平成 26 年度版、http://www.soumu.go.jp/johotsusintokei/whitepaper/ja/h26/html/nc143210.html、2019 年 3 月 20 日参照。

11 山口嘉大「サイバー防衛における官民連携の強化について－エストニア共和国との比較を通じて」『防衛研究所紀要』第 21 巻第 1 号、2018 年 12 月、164-165 頁。

12 CSIS, “Economic Impact of Cybercrime,” February 2018, p. 4, https://www.csis.org/analysis/economic-impact-cybercrime.

13 平成 28 年度内閣サイバーセキュリティセンター委託調査「平成 28 年度企業のサイバーセキュリティ対策に関する調査報告書」2017 年 3 月、27 頁。ここでは、企業によるサイバーセキュリティに関する情報発信の姿勢として、「同業種や同規模の企業と同じレベルでできていればよい」という回答が 74.1%で、「他企業よりも積極的に情報発信する」という企業は 18.1%にとどまる。

実際 2014 年に欧州ネットワーク・情報セキュリティ機関 ENISA（European Network and Information Security Agency）は「国家サイバーセキュリティ戦略の評価枠組」を発刊し、その評価対象として官民協力と役割の確立というものが評価項目となっている[14]。

また 2018 年に国際電気通信連合（ITU）は、「国家サイバーセキュリティ戦略開発ガイド」を発刊した。その中にも「政府組織内の協力」「(国内の）分野横断的な協力」の最良慣行として取り上げられている[15]。

我が国でも、昨年（2018 年）内閣サイバーセキュリティセンターが発簡した「サイバーセキュリティ戦略」の中に、「従来の枠を超えた情報共有・連携体制構築」として 1 項が設けられている[16]。

このように、国際機関でも我が国でもサイバー領域の防衛には、社会の連携による情報の共有が重要であると認識されている。

研究所とは、新たな知見を求める場、それを社会と共有する場である。今日知見は拡大し、変化は加速し、その情報共有が求められている。目まぐるしく状況が移り変わる中にあって、30 大綱により自衛隊が保持しようとしているサイバー部隊がその連続的な変化に順応できたとしても、パラダイムシフトのような非線形的な変化には研究所でなければ対応が難しい。このような事情から、各国でサイバー研究所が設けられているものと考えられる。

---

[14] ENISA, *An evaluation Framework for National Cyber Security Strategies*, 2014, p. 13. https://www.enisa.europa.eu/publications/an-evaluation-framework-for-cyber-security-strategies.

[15] ITU, *Guide to Developing a National Cybersecurity Strategy* ," 2017, p. 37, https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-CYB_GUIDE.01-2018-PDF-E.pdf.

[16] 内閣サイバーセキュリティセンター「サイバーセキュリティ戦略」2018 年、https://www.nisc.go.jp/active/kihon/pdf/cs-senryaku2018.pdf、2019 年 3 月 20 日参照。

2　研究手法

「政策の是非を議論するスパーリングパートナーがほしい」

高見澤將林　防衛庁防衛局調査課長[17]

（1）サイバー研究所（シンクタンク）の定義

もとより研究所、シンクタンクの語の意味するものは限定的ではない[18]。一橋大学名誉教授　野口悠紀雄は「研究という商品を売る独立の組織体」と定義した[19]。またペンシルバニア大学シニアフェローのジェームス・マクガン氏は「公共政策とそれに関与する組織であり、政策に関して政策立案者と一般市民がより良い意思決定を行うために、国内外の政策指向の調査･研究及び助言を行うための機関であり、永続的な形をとるもの」とし、コルゲート大学理事のジェームス・スミス氏は「アメリカの正式な政治過程の周辺で活動する民間・非営利の研究グループ」としている[20]。

その機能として、マクガン氏は、

1　調査研究
2　提言
3　政策参画

の 3 点を挙げた[21]。

また日本再建イニシアティブ理事長　船橋洋一氏は

---

17 船橋洋一『シンクタンクとは何か』中央公論新社、2019 年、245 頁。そこには船橋氏と高見澤氏の議論についての当時のメモとして以下のように記されている。「政府は民間から有識者を招いて数多の審議会を作っているが、役に立たない。というより、政府がそれらを役に立たなくしているといったほうが的確かもしれない。ここではほとんどが結論先にありきで、そこで丁々発止の議論をすることはまずない。しかし、日米防衛ガイドラインの改定のように安全保障政策は、益々現実のリスクと脅威に正面から対応していく時代に入った。世界の専門家と共同研究できる民間の政策プロの力も借りなければならない。安全保障政策を真剣勝負で議論できるスパークリングパートナーが欲しい。そういう政策プロが活躍できる本格的なシンクタンクが必要だ。」

18 野口悠紀雄『シンク・タンク』東洋経済出版社、1970 年、288 頁。；　船橋『シンクタンクとは何か』8 頁。

19 野口『シンク・タンク』289 頁。

20 James G. McGann “2018 Global Go To Think Tank Index Report” *Think Tank and Civil Society Program University Pennsylvania* , p. 12, https://repository.upenn.edu/think_tanks/16/, accessed March 20, 2019. ; 船橋『シンクタンクとは何か』9 頁。原典は James A. Smith, *The idea brokers: Think Tank and the Rise of the New Policy Elite,* The Free Press, 1991.

21 船橋『シンクタンクとは何か』9 頁。

1　長期的ないしは短期的な調査・研究を行う。
2　本を出版し、また、具体的な行動思考のペーパーを出す。
3　世論、政策当局者、そしてメディアに訴える。
4　政府に継続的に人材を提供する。

の 4 点を挙げている[22]。

これらを元にサイバー研究所（シンクタンク）を定義するならば、サイバー問題は､必ずしも政策的なものばかりではなく技術的なものも包含し、営利活動を伴わないものも存在することを勘案し、ここでは「サイバー空間における、よりよい社会活動のために研究を中心として活動する恒常的組織」とする。

その組織的機能として、以下の 3 点を挙げる。

まずマクガン第 1 項、船橋第 1 項に共通した調査・研究を技術的側面も考慮して、ここでは「研究・開発」とする。

次にマクガン第 2 項、第 3 項にある提言や政策参画、船橋の第 2 項、第 3 項にある、出版、世論に対する働きかけは、外部との接点を通じて得られた知見を社会に還元する活動であり、「協力・交流」とする。

最後にマクガン第 3 項、船橋第 4 項にある政策参画、人材提供は、社会的な、外部からの視座によるものであり、組織として内部から見た場合、人を育て、世に送り出す活動を意味することから「教育・訓練」とする。

（2）分析の方法

研究の対象として、前述の定義に適合する、調査可能かつ十分な情報が得られた表 1 の 6 つの軍のサイバー関連研究所とした[23]。

調査の方法は、現地調査及び関係者への聞取調査である。

分析の方法は、調査により得られた結果を、先に定義等を基に分類の上俯瞰し、その特質を抽出する形で行うこととする。

---

[22] 船橋『シンクタンクとは何か』10 頁。

[23] このほか、米海軍大学校、米空軍士官学校、米沿岸警備隊学校、韓国陸軍士官学校にもサイバー研究所があり、日本では民間の総務省の元、情報通信研究機構（NICT)、経済産業省の元、産業総合研究所　サイバーフィジカル研究センター、慶応大学にサイバーセキュリティ研究センター、東京電機大学サイバーセキュリティ研究所に調査を行ったが、海外事例に絞り、情報が十分集まったところのみ研究対象とするため、6 つの研究所に絞った。

表 1　研究の対象

項番	所在	名称	現地調査時期
1	エストニア	NATO サイバー防衛研究所（CCDCOE: Cooperative Cyber Defence Centre of Excellence）	2017 年 3 月
2	アメリカ	陸軍サイバー研究所（Army Cyber Institute）	2017 年 8 月
3	アメリカ	陸軍士官学校サイバー研究所（Cyber Research Center）	2017 年 8 月
4	アメリカ	海軍兵学校サイバーセキュリティ研究所	2017 年 8 月・2018 年 11 月
5	ドイツ	連邦軍大学サイバー研究所 CODE	2018 年 12 月
6	フランス	陸軍士官学校研究センター（CREC: Centrede recherche　des ecoles de Saint-Cyr Coetquidan）	2013 年 9 月・2014 年 6 月・2014 年 10 月・2016 年 3 月・2017 年 3 月

（筆者作成）

3　事例検討

この（ランド研究所の）成果は、空軍にとってこの上もなく貴重なものとなった。それは陸・海軍に対する空軍の発言力を著しく高めたのである。（中略）予算配分の比率が陸軍 23%、海軍 28%に対し、空軍は 46%と他の 2 倍近い規模になったことがそれをよく示している。　野口悠紀雄　一橋大学名誉教授[24]

先述のように攻撃も変化も烈度を増す中にあって、その情勢、趨勢の把握のためにも研究は欠かせない。ここでは先に挙げた 6 つの研究所がどのような活動を行っているのか、その状況を概観する。

(1) エストニア：NATO サイバー防衛研究所（CCDCOE: Cooperative Cyber Defence Centre of Excellence）

NATOサイバー防衛研究所は、2007年の国家に対する大規模なサイバー攻撃事案の生起したことなどが契機となり、2008年にエストニアの首都タリンに設立されたNATOのサイバー防衛研究中枢である。現在(2019年)米英仏独伊はじめ25か国が参加している。

そのビジョンは、NATO加盟国及びそのパートナー国の協力を促進する

[24] 野口『シンク・タンク』289 頁。

ことで、その任務は、サイバーディフェンスにおけるアカデミックな専門的知識をもって、加盟国とNATOを支援することである。

組織は運営委員会の元、管理部の下に、以下の6つの部門がある。

1　技術部門
2　戦略部門
3　作戦部門
4　法律部門
5　教育訓練部門
6　支援部門

活動は、3 つの領域がある。

1　研究
2　教育
3　演習

その主要な活動に、以下の3つがある。

1　LOCKED SHIELDS－サイバー演習
2　CYCON－サイバーカンファレンス
3　TALLINN MANUAL－サイバー国際法

サイバー演習に関しては、毎年行われるもので、昨年(2018 年)は 30 か国から約 1000 名が参加した。

サイバーカンファレンスに関しては、世界中から有識者を募り、参加者は昨年(2018 年)で 600 名を超え、同時に多くの有識者の論文から選ばれた、品質の高い予稿集も発刊される。

サイバー国際法に関しては、サイバーの文脈における国際法の適用の在り方を検討したもので、2013 年に第 1 版、2017 年に第 2 版が出された。

研究者数は約 60 名であり、日本も今年（2019 年）3 月から研究者を送り、共同して研究を行っている[25]。

予算は参加国（CCDCOE の活動に加盟している国）から支出され、総額は 1 億 6 千万円（130 万ユーロ）である[26]。

（2）アメリカ：陸軍サイバー研究所（Army Cyber Institute）

米陸軍サイバー研究所（Army Cyber Institute）は、2014年、米国ニ

[25] 防衛省「防衛省職員のＮＡＴＯサイバー防衛協力センターへの派遣について」2019 年 3 月 8 日。防衛研究所の研究者 1 名を派遣した。
[26] NATO サイバー防衛研究所　法務部長　ラウリ・アースマン氏、筆者によるインタビュー及びその後のメールによる回答、於東京、2019 年 2 月 13 日。

ューヨーク州ウエストポイント陸軍士官学校の敷地に設立されたサイバー研究所である。

そのビジョンは、国家がサイバースペースで敵対者を圧倒することを可能にする、知的リソースと影響力のあるパートナーシップを発展させることである。

任務として、サイバー領域における学際的な研究、提言および教育、国防総省、陸軍、政府、学術および産業のサイバーコミュニティの知見を育むことが挙げられる。

組織は将官を長として以下の 3 つの研究室がある。

1　インテリジェントサイバーシステム分析
2　IoT
3　バーチャルリアリティと仮想現実

現在の主要研究分野は、以下の5分野である。

1　重要インフラのサイバーレジリエンス
2　技術の将来と高密度コンピューティング
3　サイバーオートノミー
4　制御システムにおけるサイバーの影響
5　将来のサイバーワークフォースにおける人材管理

ACI は米軍の中で最も大きなサイバー研究所であり、年に 1 回後述の NATO サイバー防衛研究所（CCDCOE）と共催で、サイバーカンファレンス CYCON US を開催している。併せてその知見等をジャーナル“Cyber Defense Review”の形で発刊している。

また同じ敷地内にある陸軍士官学校のサイバー関連教務の講義等を支援している。

研究者数は約 60 名であり、予算は約 9 億円（800 万ドル：実質研究費は約 3 億 8000 万円（350 万ドル））である[27]。

（3）アメリカ：陸軍士官学校サイバー研究所（Cyber Research Center）

米陸軍士官学校サイバー研究所（Cyber Research Center)はニューヨーク州の米陸軍士官学校の敷地内にある。その前身は 1985 年に設立された、人工知能分析評価室（Office of Artificial Intelligence Analysis & Evaluation）で、同室は 1997 年情報技術運用研究所（Information

[27] アメリカ陸軍サイバー研究所　ポール・マックスウェル博士、筆者によるインタビュー及びその後のメールによる回答、於東京、2018 年 4 月 4 日。

Technology Operation Center）に改編され、2012 年サイバー研究所（Cyber Research Center）に改められたものである。

その任務は以下の 4 つである。

1　士官候補生教育の充実
2　教官の専門性の強化
3　陸軍と国家の直面する課題解決
4　陸軍士官学校の名誉の獲得

研究計画は以下の 6 つである。

1　候補生の教育訓練
2　スマートグリッドと産業用制御システムのセキュリティ
3　並立省電力コンピューティング
4　制御システム、IoT、シングルボードコンピュータ
5　ヒューマン コンピュータインタラクション
6　サイバーセキュリティ

その活動は教育の支援が主眼であり、その一環としてサイバーに関する部外に対する発表・紹介等も行っている。

研究所員数は12名である[28]。

（4）アメリカ：海軍兵学校サイバーセキュリティ研究所

米海軍兵学校サイバーセキュリティ研究所は、2011年、米国メリーランド州アナポリスにある米海軍兵学校内に設立されたサイバー研究所である。

その任務は、士官候補生に対するあらゆる分野のサイバー戦争に関する教育を強化し、その専門知識や見解の共有を促進し、優先順位を認識するための合理化された手段を提供することであり、またサイバー戦争における学術研究、および情報共有、取組の調整、並びに米海軍兵学校でのサイバー戦争関連の活動の共通の枠組みを形成することである。

活動として、海軍兵学校で行われるサイバー戦争に関するカリキュラムおよび職業訓練を改善し、教育の質を向上させるために必要な支援を提供している。その中には海軍士官学校におけるサイバー戦争の知識、研究および研究に貢献するすべてのプログラムの支援が含まれる。

[28]アメリカ陸軍士官学校マイケル・ラーハム中佐及び同校サイバー研究所レイモンド・ブライン中佐、筆者によるインタビュー及びその後のメールによる回答、於ウエストポイント、2017 年 8 月 29 日。

研究内容として以下のようなものがある[29]。

1　重要インフラの防護
2　3Dプリンタの脆弱性
3　Amazon Alexaに対する攻撃
4　電子投票法

また毎年サイバーに関するカンファレンスや出版活動も行っている。

研究所員数は12名である[30]。

（5）ドイツ：連邦軍大学サイバー研究所 CODE

CODE は2013年ドイツ南部の街ミュンヘンにある連邦軍大学に設立された研究機関である。

その目的は革新的な技術を実現し、総合的かつ学際的、法的および経営環境に適応したデータ、ソフトウェアおよびシステムの防護を行うことである。

その活動領域は、以下のとおりである。

1　連携－サイバーエコシステムを形作るミュンヘンサイバーイノベーションハブの中
　枢としての機能
2　研究－後述する分野・範囲の研究
3　教育－修士課程学生教育等

主要研究分野は以下の5分野で、これらを横断した3範囲の研究も併せて行われている。

(5分野)

1　サイバーディフェンス
2　スマートデータ
3　モバイルセキュリティ
4　e -Health
5　重要インフラ防護

(3範囲)

1　リスクマネジメント

---

[29] 今年(2019年)実施している教官と学生の研究にある14テーマの一例としてリスト上の4テーマを挙げた。

[30] アメリカ海軍兵学校サイバーセキュリティ研究所ポール・トルトラ所長、筆者によるインタビュー及びその後の質問に対する回答、於アナポリス、2017年8月28日及び2018年11月13日。

2　サイバーセキュリティにおけるナレッジマネジメント
3　ネットワーク、セキュリティと技術革新のためのビッグデータ

CODEはサイバーセキュリティ専門家のネットワーク、軍事、ビジネス、産業等の組織、起業の中核であり、2018年、連邦軍大学の敷地から離れてビジネス街に移動した。そこで安全保障のための軍事・民間部門間の交流を促進し、産業界、研究機関および公的機関間の相互作用を強化し、イノベーションのためのエコシステムを構築している。また連邦内のサイバー教育を先導するため、世界各国のサイバー教育を研究し、その修士課程に反映させている[31]。

（6）フランス：陸軍士官学校研究センター（CREC:Centrede recherché des ecoles de Saint-Cyr Coetquidan）

フランス陸軍士官学校研究センターは、1998年フランスブルターニュ半島の中枢都市レンヌ郊外にあるサンシール陸軍士官学校に設立された研究機関である。

その目的は、研究者の活動を統合し、フランスとヨーロッパにおける優れた研究成果を得ることである。

サイバー防衛研究部門の主要研究分野は以下の分野である。

1　国際関係
2　地政学
3　社会科学
4　管理
5　人類学
6　コンピュータサイエンス
7　暗号学

その主要な活動領域は、研究と教育であり、フランスの軍隊が直面している防衛と安全保障の問題を研究し、士官候補生教育とその修士課程教育(含：サイバー教育カリキュラム)、そして幹部に対する継続的な教育を通じて、新しい知識の創造、ドクトリンに関する論議を活性化し、知識の普及に貢献している。またサイバーに関するカンファレンスや出版活動も行っている。

更にCRECは2013年より産官学連携して構築の始まったブルターニュ

[31]ドイツ連邦軍大学サイバー研究所 Klaus Buchenrider 副所長、筆者によるインタビュー及びその後のメールによる回答、於ミュンヘン、2018 年 12 月 12 日。

サイバークラスタの中核研究所として機能し、研究開発、人材育成において貢献している。サイバー防衛研究グループの研究者数は13名で、その予算は年間約1億3千万円（100万ユーロ）である[32]。

4　分析・考察

研究のない教育は考えられない。

ポール・トルトラ　アメリカ海軍兵学校サイバーセキュリティ研究所長[33]

事例検討を、それぞれ先述の定義等に基づき「位置付・任務」「研究・開発」「協力・交流」「教育・訓練」「その他」にまとめると、表 2 のようになる。それに基づき以下の考察を行った。

（1）位置付／任務

位置付けに関して、調査した中でエストニアの NATO サイバー防衛研究所以外はすべて軍の高等教育機関（初級～上級幹部教育機関）の中に設置されている。サイバー防衛研究所はエストニアが中心となる活動ではあるが国際機関であり、自国の学校組織とは別になっている。

他の国々で高等教育機関を中心に設置されていることの理由として、すでに専門的な研究者がそこに勤務しており、軍として校内の人的資産の再配分で研究所が設置できることが考えられる。

任務に関しては、NATO サイバー防衛研究所、アメリカ陸軍サイバー研究所のように、組織として主に研究活動に力点を置くところと、他の 4 研究所のように学生教育に責任を持つところがあった。後者に関しては、研究成果等を、直接学生に教えることができ、知見を効率よく組織に還元できることと考える[34]。

---

[32] フランス陸軍士官学校研究センター　ディダー・ダネ博士、筆者によるインタビュー及びその後のメールによる回答、於サンシール、2016 年 3 月 27 日。

[33] アメリカ海軍兵学校サイバーセキュリティ研究所ポール・トルトラ所長、筆者によるインタビュー、於ワシントン D.C.、2018 年 11 月 13 日。更に、「教官も学生も軍事作戦と市民生活におけるその重要性に鑑み、ダイナミックでチャレンジングなサイバー領域で研究を継続することは重要だ。」とも語っている。

[34] 2014 年 1 月　EU サイバー政策調整担当課長ヘリ・ティルマ・クララ氏も防衛大学校における特別講義の中で「大学はサイバー教育に最適なところである。」と指摘している。

表 2　各研究所の要目

研究所名（設立年）	位置付・任務	研究・開発	協力・交流	教育・訓練	その他
NATO サイバー防衛研究所（2008 年）	サイバーディフェンスにおけるアカデミックな専門的知識をもって加盟国と NATO を支援すること NATO 加盟国及びそのパートナー国の協力を促進すること	研究室 ・技術部門 ・戦略部門 ・作戦部門 ・法律部門 ・教育訓練部門 ・支援部門	サイバーカンファレンス　CYCON 同上プロシーディング発刊	サイバー演習 Locked Shield	研究者数約 60 名 予算は：1 億6千万円（130万ユーロ）
アメリカ：陸軍サイバー研究所（2014 年）	サイバー領域における学際的な研究、提言及び教育、国防総省、陸軍、政府、学術及び産業のサイバーコミュニティの知見を育むこと	研究室 ・インテリジェントサイバーシステム分析 ・IoT ・バーチャルリアリティと仮想現実	サイバーカンファレンス CYCON US 開催 ジャーナル“Cyber Defense Review”発刊	陸軍士官学校の教育を支援	研究者数約 60 名 予算：約 9 億円（800 万ドル）
アメリカ：陸軍士官学校サイバー研究所（1985 年）	・士官候補生教育の充実 ・教官の専門性の強化 ・陸軍と国家の直面する課題解決 ・陸軍士官学校の名誉の獲得	研究テーマ ・候補生の教育訓練 ・スマートグリッドと産業用制御システムのセキュリティ ・並立省電力コンピューティング ・制御システム ・IoT ・シングルボードコンピュータ ・ヒューマン コンピュータインタラクション ・サイバーセキュリティ	サイバーに関する研究成果の発表	教育の支援が主眼	研究所員数：12 名

研究所名（設立年）	位置付・任務	研究・開発	協力・交流	教育・訓練	その他
アメリカ：米海軍兵学校サイバー研究所（2012 年）	士官候補生に対しあらゆる分野のサイバー戦争に関する教育を強化し、その専門知識や見解の共有を促進し、優先順位を認識するための合理化された手段を提供すること	研究テーマ ・重要インフラの防 ・3Dプリンタの脆弱性 ・Amazon Alexaへの攻撃 ・電子投票法　等	サイバーに関するカンファレンス・出版活動	海軍兵学校で行われるサイバー戦争に関するカリキュラムおよび職業訓練を改善し、教育の質を向上させるために必要な支援を提供	研究所員数 12 名
ドイツ：連邦軍大学サイバー研究所（2013 年）	革新的な技術を実現し、総合的かつ学際的、法的および経営環境に適応したデータ、ソフトウェアおよびシステムの防護を行うこと	研究テーマ (5分野) ・サイバーディフェンス ・スマートデータ ・モバイルセキュリティ ・e -Health ・重要インフラ防護	サイバーセキュリティ専門家のネットワーク、軍事、ビジネス、産業等の組織、起業の中核となるべく大学の敷地から離れてビジネス街に移動	連邦内のサイバー教育を先導するため、世界各国のサイバー教育を研究し、その修士課程に反映	ミュンヘンサイバーイノベーションハブの中核
フランス；仏陸軍士官学校研究センター（1998 年）	研究者の活動を統合し、フランスとヨーロッパにおける優れた研究成果を得ること	研究領域 ・国際関係 ・地政学 ・社会科学 ・管理学 ・人類学 ・ｺﾝﾋﾟｭｰﾀサイエンス ・暗号学	サイバーに関するカンファレンス・出版活動	士官候補生に対するサイバー防衛教育	研究者数（サイバー防衛研究グループ）：13 名 予算：年間約 1 億 3 千万円（100 万ユーロ） ブルターニュサイバークラスタの中核

（筆者作成）

(2)　研究・開発

NATO サイバー防衛研究所には、「戦略」「作戦」等の軍事色の強い部門があるが、個々の研究内容を見れば、「バーチャルリアリティと仮想現実」「並立省電力コンピューティング」「e-health」等民間の研究テーマと同様のものが多い。サイバー領域で用いられる技術は、その多くがデュアルユーステクノロジーであり、その知見の多くが民間にあることとも考えあわせ、広く官民交流の可能性と必要性を示すものと考える。

またその研究には、技術的テーマのみならず、NATO サイバー防衛研究所では法務等、フランス陸軍士官学校では人類学等からのアプローチがある。日本に比して、欧米では社会科学的アプローチも多く、その表れであると考える[35]。

(3)協力・交流

NATO サイバー防衛研究所とアメリカ陸軍サイバー研究所では、同じ「CYCON」の名を冠した年次のサイバーカンファレンスを実施していることから分かるように、密接な提携関係にある。またフランス陸軍士官学校研究センターも各国の研究機関と積極的に MOU を結び交流を深めている[36]。これらは研究所が国内外のサイバー関連情報流通のためのハブとして機能していることを示すものであると考える。

また CYCON は広く知見を集めると同時に、論文を募りプロシーディングスを発行している。米陸軍士官学校、米海軍兵学校、フランス陸軍士官学校研究センターでも研究成果の発表・紹介、カンファレンス、出版等を通じて部外との協力、交流を図っている[37]。

(4)教育・訓練

NATO サイバー防衛研究所では毎年 Locked　Shield という演習が行われている。NATO 加盟国、友好国の関係者が一堂に会し、演習を行うもの

---

[35] 2019 年 5 月に参加したアメリカ海軍大学サイバー紛争研究所主催のサイバーカンファレンスでは、ジョセフ・ナイハーバード大学特別功労教授はじめ、多くの著名な経済学者、社会学者達がサイバーディフェンスを語っていた。日本では他の分野の第一人者がサイバーセキュリティカンファレンスに参加して、サイバーセキュリティを語ることは寡聞にして聞いたことはない。

[36] フランス陸軍士官学校研究センターは、韓国高麗大学をはじめ、多くの機関と MoU を結んでいる。

[37] ドイツの CODE の情報は得られなかったが、2018 年 12 月訪問時の説明では、その講堂の構造は、部外者のカンファレンス参加と保全を考慮し、区画の変更ができるようになっており、部外との交流を前提にした設計となっていた。

で、一国のみならず多国間協力を図る上での良い訓練機会となっている。各研究所とも、すべて教育・訓練の機能を有している。特にアメリカ陸海の士官学校では教育研究を重視した研究所がある[38]。移り変わりの早いこの分野においては、教育に研究は必要不可欠であるとアメリカ軍では認識されている[39]。

米軍では士官学校間の連絡会議があり、年に一度各士官学校が会合を開き、教授法等の検討を行っている[40]。各士官学校ではどの学校も学生の関心を引くようにドイツの暗号機 ENIGMA が展示され、サイバー競技を競う学生チームとそれに親しむ学生クラブが設置されるなど、その教育体制が標準化されるとともに、継続してより良い教育・訓練の在り方が模索されている[41]。フランス陸軍士官学校でもサイバー関連教育について、近傍にある陸軍通信学校や、民間大学との教授、学生交流がある[42]。そのような学校を超えた教育・訓練の在り方の検討は、最良慣行の一つであるものと考えられる[43]。

(5)その他

予算規模はわかった範囲で 1～8 億円の間であった。また組織の規模は 10～60 名の間であった。予算の中には人件費、管理費等も含まれるため、実質研究費の明示された米陸軍サイバー研究所のデータでみると、研究者

---

[38] 注 23 に記したように、アメリカ空軍士官学校、準軍隊である沿岸警備隊学校にも研究所がある。

[39] エストニアで開催されるサイバーカンファレンス CYCON には毎年アメリカ海軍士官学校の候補生が参加し、昨年(2018 年)からは陸軍士官学校からの参加も見られた。アメリカで行われる CYCON　US にも毎回陸海軍士官学校の候補生の参加がみられる。最先端のものがすぐに陳腐化していく中にあって、直接その内容に触れさせようとする配慮があるものと考えられる。； 2017 年 3 月フランス陸軍士官学校調査時、ディダー・ダネ博士も同様の発言を行っており、2017 年 11 月ローマで行われた NATO サイバー教育訓練会議では、2019 年秋リスボンに開校予定の NATO サイバー学校（現在ローマにある NATO 通信システム学校の後身）にナレッジセンターという研究所を創設する構想が発表された。これらのことを勘案して一般に移り変わりの激しいサイバー分野においては教育には研究が必要なのだと考える。

[40] アメリカ陸軍サイバー研究所ベガス大佐、筆者によるインタビュー、於韓国陸軍士官学校主催国際サイバーカンファレンス、2015 年 11 月 4 日。

[41] 2017 年 8 月米陸海空軍士官学校及び沿岸警備隊学校の調査で明らかになった。

[42] 2016 年 3 月フランス陸軍士官学校の調査で明らかになった。

[43] 韓国軍でも 2017 年 2 月の調査では、同様に国防部の委託を受けてサイバーコマンドの中核要員を養成する高麗大学と各士官学校で定期的な会合がもたれている。

一人当たりに換算してその研究費は約 600 万円となる[44]。

またドイツ連邦軍大学サイバー研究所とフランス陸軍士官学校研究センターは地域のサイバークラスタの中心にある。NATO サイバー防衛研究所の所在するタリンはサイバークラスタの呼称は用いていないものの、大学やベンチャー企業が数多くある。サイバー産業は知識集約的な業種であり、各国とも知見が集まり、人材を輩出する研究所の周辺に、そこで育まれた技術を核として産業を振興させようとしているものと考えられる。

おわりに

壁の一つ一つが扉である。　　ラルフ・ワルド・エマーソン　米国　哲学者[45]

本論では第 1 節　研究背景で、30 大綱の中で「サイバー」の語が高い頻度で出現しており、宇宙、電磁波と並んで新たな領域として認識され、強化すべきされていることを明らかにした上で、そこでは知見の拡大、変化の加速、また情報共有の必要性からサイバー研究所が必要とされることを説明した。第 2 節　研究手法では、研究所・シンクタンクの持つ機能からサイバー研究所を定義した上で、研究対象となるサイバー研究所を定め、現地調査、聞取調査を用いて定義等を基に分類し、特質を抽出する形で分析することを明示した。第 3 節　実例検証では、研究対象とした 6 つのサイバー研究所の事例を概観した。第 4 節　分析・考察では調査した範囲内において、多くのサイバー研究所は軍の高等教育機関に併設される傾向があり、研究に力点を置くものと教育に力点を置くものがあること、研究・開発では、その研究内容が民間とほぼ同様であり、社会学的アプローチの取組もみられること、協力・交流のために、研究所間の知見の交換も広く行われ、会議・出版も行われていること、教育・訓練のために、研究所で多国間演習等も行われ、研究は教育に必要不可欠であるとみなされ、組織を超えて教授法等の意見交換、標準化、また教官・学生の交換も行われていること、その他調査した範囲で予算規模は 1 ～8 億円、研究所員数は 10 ～60 名であり、研究所はサイバークラスタの中心とされる場合があること

[44] NATO サイバー防衛研究所　ラウリ・アースマン博士、アメリカ陸軍サイバー研究所　ポール　マックスウェル博士、フランス陸軍士官学校研究センター　ディダー・ダネ博士、筆者によるメールでの聞取、2019 年 3 月。

[45] Blago Kirov, *Ralph Waldo Emerson Quotes & Facts*, CerateSpace Independint Publishing Platform, 2016, p. 5.

等を明らかにした。これらの知見は、今後日本においてサイバー研究所創設の際の資となることと考える。今回調査対象とした研究所は 6 か所と少なく、一般性の担保と包含される恣意性に関する問題については、爾後調査範囲を拡大していく中で解消していきたい。

今後研究所は益々重要性が高まることが予想される。以前、自衛隊の活動領域が拡大する中にあって「訓練」の自衛隊から「実働」の自衛隊への変容と言われた時期があったが、人口減少による経済、社会の縮小、また AI 化・IoT 化等の趨勢とも考え併せ、その効率的運用のために「思索」の自衛隊を目指すべき時期が来ているのではないだろうか。

歴史を振り返るとき、かつて戦いに敗れベルサイユ体制で兵力に大きな制限を科されたドイツでは、多くの研究組織を立ち上げ、敗戦の原因を究明するとともに、その 10 万の兵力のみで戦うのではないとして、現実の兵力に拘泥することなく自由な発想の元新たな戦いのあり方を検討した[46]。一方で戦いに勝利したはずの日本は、第 1 次大戦を決した圧倒的な物量を生産する工業力に欠け、列強との差を埋めるため、無形戦力として精神力の鍛錬を強調し、その合理を超越した思考法は、戦中の玉砕、特攻につながっていった[47]。それを評して無形戦力とは知恵であり、理論とすべきではなかったかとの指摘がある[48]。

思考は自ら縛ることがなければ、誰もそれをとどめることができない。現実の社会には制約が多くても、想像の世界では無限に想いを広げることができる。そして時空が圧縮し、変化の激しい中では、抗い得ないと思われていたような制約もまた、いかようにも変わっていくのである。

パラダイムシフトの時代にあっては、与えられた中でベストを尽くすのではなく、ベストを尽くすにはいかにあるべきかから考えられなければならない。そのためにも知見を集め、議論を深め、意見を広め、現場とは切り離し、真理の探究の場、知見の交流の場として、我が国においてもまたサイバー研究所を創設する必要がある。それはともすれば社会から孤立しがちな防衛省・自衛隊に、新鮮な空気をもたらすものとなるだろう。この

---

46 ドイツ国防軍陸軍統帥部／陸軍総司令部編纂、旧日本陸軍／陸軍大学校訳、大木毅監修・解説『軍隊指揮』作品社、2018 年、13 頁。

47 片岡徹也『軍事の事典』東京堂出版、2009 年、258-288 頁。；　寺崎英成、マリコ・テラサキ・ミラー『昭和天皇独白録　寺崎英成御用掛日記』文藝春秋社、1991 年、84 頁。昭和天皇は敗戦の原因の一つに「余りに精神に重きを置き過ぎて科学の力を軽視した事」を指摘している。

48 葛原和三「陸軍の戦術競技について－「戦闘綱要」を中心にして」2009 年 2 月 19 日、軍事史学会例会資料、95 頁。

領域は新たな領域であり、その第 1 歩としてふさわしいものである。

最後に本研究の中で、今後創設すべき研究所の在り方に言及しようとも考えたが、そのためには更に多くの検討が必要なことから断念した。また次回研究できればと思料する。