【研究ノート】
ドイツのサイバー・スペースのガバナンス
──国防省及び連邦軍のサイバー部門の機能強化を中心に──

小橋　史行

〈要旨〉

地球規模で随所随時に頻発するサイバー攻撃に直面したドイツ国防省及び連邦軍は危機感を抱き、抜本的な組織改編を行い、新たな任務に取り組むことになった。

ドイツは 2015 年以降、サイバー・スペースのガバナンスの改革を進めており、特に国防省・連邦軍のサイバー関連防衛力を整備する体制・態勢へと移行している。国防省及び CIR において抜本的なサイバー IT 改革が継続中のサイバー中枢都市のボン、CODE を中心としたサイバー・クラスターが充実しつつあるミュンヘン、そして産・官・学の一体化を目指し、動き始めたサイバー・イノベーション・ハブが存在するベルリンの 3 大都市を中心として、今後、ドイツ独自のアプリケーション、プログラム、システム、器材そして装備品が開発され、整備されていく可能性は高い。他方、サイバー技術の進展速度は速く、課題も多い。ドイツが諸課題を克服し、どのように進歩・発展していくのか、サイバー・スペースのガバナンスへの取り組みについて、引き続き、注視していくことが必要である。

はじめに

現代社会は洋の東西を問わず、デジタル化されたネットワーク社会に移行しており、身近な例を挙げれば、インターネットの活用なくしては日々の生活にも支障をきたす時代となっている。また、インターネットに接続されていなくても、防衛省・自衛隊の各種業務、指揮統制通信関連システム、装備・兵站関連システム、医療・衛生関連システム、人事管理システム、会計システムなどは、常にデジタル化の影響を強く受けている。現在、サイバー攻撃は世界規模で頻発している。サイバー攻撃を行う犯行者はテロリスト、政府機関、ハッカー、スパイ、密告者、犯罪者など多岐に亘り、その特定、すなわち、アトリビューション（attribution: 特定）は極めて困難である。他方、サイバー攻撃は軍事組織のデジタル化されたシステムのあらゆる側面に深刻な影響をもたらす。

我が国では 2000 年、内閣官房における情報セキュリティ対策推進室の創設を始め、

2014 年にサイバー・セキュリティ基本法が公布、翌年の 2015 年にはサイバー・セキュリティ戦略が閣議決定された。サイバーの急速な拡張・発展を踏まえ、2018 年 7 月、このサイバー・セキュリティ戦略が改訂された。防衛省においても、2018 年、多次元統合防衛力の整備を謳った防衛計画の大綱が策定され、宇宙、サイバー、電磁波といった新たな領域の能力を獲得・強化し、サイバーについては大綱別表に示すようにサイバー防衛隊 1 個防衛隊の創設する旨が規定された。

サイバー攻撃は世界中で頻発するが、欧州にあっても、その例外ではない。ドイツはサイバー・セキュリティ[1]に関しては欧州諸国の中でも、サイバー先進国と言われているエストニアと並ぶ、高い評価を得ている[2]。そもそも、ドイツは 19 世紀後半から 20 世紀前半にかけて我が国が近代化を進める中、諸制度を参考にしてきた、代表的な欧州諸国であり、第 2 次世界大戦での敗戦国という共通項に加え、戦後は、我が国と似通った経済発展を遂げた点において、現在も日本の各分野において制度等の比較・参考の対象となっている。特に、軍事組織である国防省・連邦軍は、その歩みから防衛省・自衛隊と多くの面において比較の対象となってきた。ドイツ国防省では重要な結節を踏まえ、国防白書を刊行しているが、サイバーに関しては、2006 年に発刊された『国防白書 2006 ～ドイツの安全保障政策と連邦軍の将来のために（Weißbuch 2006 zur Sicherheitspolitik Deutschlands und zur Zukunft der Bundeswehr[3]、以下、国防白書 2006）』ではサイバーに言及したのは 1 か所のみであったが、2016 年の『国防白書～安全保障政策と連邦軍の将来のために～ 2016（Weißbuch zur Sicherheitspolitik und Zukunft der Bundeswehr）[4]。以下、国防白書 2016』では 63 か所へと激増・拡大した[5]。

サイバー・セキュリティに関する先行研究については、グローバル規模でサイバー攻撃が生起し、洋の東西を問わず、サイバー、とりわけサイバー・セキュリティに関する研究は質量

1　ドイツにおけるサイバー・セキュリティ（Cyber Sicherheit）とは、データ及びシステムを含むサイバー空間における情報技術の保全という意味で使用される教育訓練、技術開発、整備、調達などにおいて使用される行政用語である。（Bundesministerium für inneres《BMI》, *Cyber-Sicherheitsstrategie für Deutschland,* 2016, S. 46）なお、ドイツではサイバー・情報技術・セキュリティ（Cyber IT Sicherheit）として使用されることが多い。（平成 30 年 9 月 7 日、ドイツ国際政治・安全保障問題研究所《Stiftung Wissenschaft und Politik：SWP、英語名：German Institute for International and Security Affairs》における意見交換時の先方研究員の発言）

2　BSA (The Software Alliance), *EU Cybersecurity Dashboard: A Path to a Secure European Cyberspace*, pp.8-9, pp.11-16. , https://www.bsa.org/~/media/Files/Policy/Security/EU/study_eucybersecurity_en.pdf, accessed on Feb.21, 2019.

3　Die Bundesregierung, *Weißbuch 2006 zur Sicherheitspolitik Deutschlands und zur Zukunft der Bundeswehr,* Okt.2006.

4　Die Bundesregierung, *Weißbuch zur Sicherheitspolitik und Zukunft der Bundeswehr 2016*, 13 Juli 2016.

5　ドイツにおいて『国防白書 2016』の 10 年前に発刊された『国防白書 2006』では「サイバー空間に対する、またはサイバー空間からの軍事攻撃を受けるリスクがある」旨記述されているのみである。Die Bundesregierung, *Weißbuch zur Sicherheitspolitik und Zukunft der Bundeswehr 2006*, S. 19.

ともに増加傾向にある。我が国はもとより、欧米諸国、イスラエルなどにおいてはサイバー・スペースにおけるガバナンス[6]強化に関する研究[7]、学説としての本編及び続編からなるタリン・マニュアル[8]（Talinn manual）を始めとした、サイバー・スペースにおける法制・規範に関する研究[9]、サイバー・レジリエンス（resilience）に関する研究[10]などは政府機関、産業界などを問わず、多数、実施されている。ドイツの政府機関によるサイバー・セキュリティに関しては、我が国においても幾つかの研究が行われている[11]。これらの研究はドイツの政府機関に関する研究であるが、国防省・連邦軍に関する先行研究は皆無である。ドイツ国内では、サイバー・セキュリティについて国防省・連邦軍関連の先行研究は僅かに存在される[12]。アネグレット・ベンデイェク（Annegret Bendiek）はサイバー・スペースに対し注意責任を有する5つの所管官庁として第5に連邦軍を挙げている[13]。しかしながら、この論文は 2016 年以前に書かれた

6　サイバースペースのガバナンスを巡る論争については、以下に詳述。原田有「サイバー空間のガバナンスを巡る論争」『NIDS コメンタリー』第 43 号（2015 年 3 月 20 日）。

7　例えば、次の文献を参照されたい。土屋大洋「サイバースペースのガバナンス」公益財団法人 日本国際問題研究所（外務省外交・安全保障調査研究事業）平成 25 年度研究プロジェクト『グローバル・コモンズにおける日米同盟の新しい課題』分析レポート、Samantha A. Adams, Marlou Brokx, Lorenzo Dalla Corte, Maša Galič, Kaspar Kala, Bert-Jaap Koops, Ronald Leenes, Maurice Schellekens, Karine e Silva, Ivan Škorvánek, *The Governance of Cybersecurity, A comparative quick scan of approaches in Canada, Estonia, Germany, the Netherlands and the UK,* Tilburg University, November 2015., Daniel Benoliel, “Towards A Cybersecurity Policy Model: Israel National Cyber Bureau Case Study,” *North Carolina Journal of Law & Technology*, vol. 16, no. 3: (March 2015).

8　河野桂子「武力攻撃未満のサイバー攻撃に関する国際法―『タリン・マニュアル 2』を題材に–」『ブリーフィングメモ 2017 年 10 月号』防衛研究所、1 頁。

9　例えば、橋本 靖明「サイバー攻撃と関連法制度」『防衛研究所紀要』第 5 巻第 1 号（2002 年）。

10　例えば、Reza Arghandeh1, Alexandra von Meier, Laura Mehrmanesh, Lamine Mili, “On the Definition of Cyber—Physical Resilience in Power Systems,” California Institute for Energy and Environment Electrical Engineering and Computer Science Department University of California—Berkeley and Eletrical and Computer Engineering Department Virginia Polytechnic Institute and State University Falls Church, April.23, 2015.

11　例えば、公益財団法人　笹川平和財団『政策提言 “日本にサイバー・セキュリティ庁の創設を!” 2018』（2018 年 10 月）にドイツのサイバー・セキュリティ政策が記述されている。また、情報通信総合研究所『平成 26 年度内閣サイバー・セキュリティセンター委託調査～サイバー空間に対する諸外国の施策動向調査報告書』（平成 27 年 3 月）にはドイツのサイバー・セキュリティ戦略から規制が記述されている。田川義博・林紘一郎「サイバー・セキュリティのための情報共有と中核機関のあり方―3 つのモデルの相互比較とわが国への教訓」『情報セキュリティ総合科学(第 9 号)』（2017 年 11 月）はドイツのサイバー・セキュリティ戦略及び政策に言及している。土屋大洋「サイバー攻撃で、ドイツの製鋼所が甚大な被害を被っていた」ニューズウィーク日本版（2015 年 9 月 1 日）はドイツが受けたサイバー攻撃事案について紹介している。

12　Annegret Bendiek, “Sorgfaltsverantwortung im Cyberraum Leitlinien für eine deutsche Cyber-Außen- und Sicherheitspolitik,” *SWP Studie*, März 2016.; Thomas Reinhold/Matthias Schulze, “Digitale Gegenangriffe Eine Analyse der technischen und politischen Implikationen von „hack backs“,” Arbeitspapier von Forschungsgruppe SWP und Deutsches Institut für Internationale Politik und Sicherheit Interdisziplinäre Forschungsgruppe Abrüstung, Rüstungskontrolle und Risikotechnologien (IFAR) Institut für Friedensforschung und Sicherheitspolitik, Universität Hamburg, August 2017.

13　Bendiek, Ebenda, S. 11-14.

ものであり、既述した『国防白書 2016』を反映した、ドイツの国防省・連邦軍におけるサイバー・スペースのガバナンスの最新状況に関する先行研究については、日独双方に皆無である。

本論においては、グローバルに頻発するサイバー攻撃に直面したドイツ国防省及び連邦軍がサイバー・スペースのガバナンスをどのように強化していったのか、その機能強化の軌跡と展開について明らかにすることを主眼としている。具体的には、国家としてのサイバー・スペースのガバナンスの中で、軍事部門、すなわち国防省・連邦軍におけるサイバー・レジリエンスの強化のための組織及び編成から、施策といった制度に関わる状況、そして将来に開発されるシステムなどの趨勢について明らかにすることを主眼とするものである。なお、本論文作成にあたり、公刊資料の活用とともに、ドイツ政府関係者及び研究者への聞き取りを行った。

1. ドイツを巡るサイバー攻撃の状況

ドイツは NATO 加盟国であり、NATO がサイバー分野を強化する契機となったのが、2007 年に生起した NATO 加盟国エストニアに対するロシアのサイバー攻撃である。これを受けて、2008 年、エストニア・タリンに NATO 協同サイバー防衛センター（NATO Cooperative Cyber Defence Centre of Excellence[14]、以下 CCDCOE）が創設された。同年、Win32/Conficker というコンピュータワームが Windows OS に感染するという事態が世界的に発生し、ドイツ連邦軍の 100 台以上のコンピュータにも感染した[15]。翌々年の 2010 年には、Windows OS に感染する Win32/STUXNET というコンピュータワームがイランの原子炉においてサイバー攻撃に使用された。2013 年には Yahoo が標的型攻撃メールによるハッカー攻撃を受け、30 億人のアカウント情報が流出した。2014 年にはドイツ製鉄業界に対し、フィッシング攻撃が行われた[16]。2015 年には米中央軍（United States Central Command、以下、USCENTCOM）がハッカー攻撃を受け、フランスの放送メディア TV5　MONDE がイラク・レバントのイスラム国（Islamic State in Iraq and the Levant、以下、ISIL）と名乗る組織のサイバー攻撃を受けた[17]。同年初頭、ドイツ連邦議会がロシアによるハッカー攻撃

14　Cyber Defense は英語であるが、NATO、EU その他、外国におけるサイバー防衛関連全般を指すことが多い。（SWP 研究員、筆者によるインタビュー、於ベルリン、2018 年 9 月 7 日。）

15　Heisse Security Website, “Hunderte Bundeswehr-Rechner von Conficker befallen,” 14.02.2009.

16　Bundesamt für Sicherheit in der Informationstechnik (BSI), *Die Lage der IT-Sicherheit in Deutschland 2014*, S. 31. なお、土屋大洋は前掲記事で本件を詳細に分析している。

17　BBC News, “How France’s TV5 was almost destroyed by Russian hackers,” Gordon Corera Security correspondent, 10 October 2016. なお、TV5 モンド社長イブ・ビゴット氏（Yves Bigot）はイスラム国を装ったロシア関係者による犯行と述べている。

を受けた[18]。

ドイツでは2006年から2011年にかけて、サイバー・セキュリティに関する戦略文書が経済技術省（Bundesministerium für Wirtschaft und Technologie:BMWi[19]）及び内務省（Bundesministerium für inneres: BMI）から相次いで発刊されているように[20]、国家としてサイバー・セキュリティには諸対策を講じていた。しかしながら、産業界から市井の市民・個人に至るまで度重なるサイバー攻撃を受けるとともに、既述したように2015年には、政治の中枢である連邦議会へのサイバー攻撃が現実に生起したのであった。

2. ドイツにおけるサイバー・セキュリティに関する所掌

サイバー・セキュリティに関する独政府内の所掌は平成30年9月7日の時点では次のとおりである[21]。国防省は防衛・緊迫事態におけるサイバー防衛（Cyber Verteidigung）[22]を所掌し、それ以外の民間のサイバー・セキュリティ、サイバー反撃（Cyber Abwehr）[23]についてはBMIが所掌する。首相府（Bundeskanzleramt、以下、BKAmt）は首相が各省庁の政策指針を所掌するため、サイバー・セキュリティについては外国の秘密情報活動を行う連邦情報局（Bundesnachrichtendienst、以下、BND）を隷下に置き、主として内務省と国

18　Deutscher Bundestag, *Kleine Anfrage der Abgeordneten Stephan Thomae, Jimmy Schulz, Manuel Höferlin, Grigorios Aggelidis, Renata Alt, Christine Aschenberg-Dugnus, Jens Beeck, Nicola Beer, Dr. Jens Brandenburg (Rhein-Neckar), Mario Brandenburg, Hartmut Ebbing, Dr. Marcus Faber, Otto Fricke, Thomas Hacker, Katrin Helling-Plahr, Markus Herbrand, Katja Hessel, Reinhard Houben, Ulla Ihnen, Olaf in der Beek, Gyde Jensen, Thomas L. Kemmerich, Katharina Kloke, Daniela Kluckert, Pascal Kober, Dr. Lukas Köhler, Wolfgang Kubicki, Konstantin Kuhle, Alexander Kulitz, Ulrich Lechte, Michael Georg Link, Till Mansmann, Alexander Müller, Roman Müller-Böhm, Dr. Martin Neumann, Christian Sauter, Frank Schäffler, Matthias Seestern-Pauly, Frank Sitta, Judith Skudelny, Bettina Stark-Watzinger, Dr. Marie-Agnes Strack-Zimmermann, Benjamin Strasser, Katja Suding, Linda Teuteberg, Michael Theurer, Manfred Todtenhausen, Dr. Andrew Ullmann, Gerald Ullrich, Johannes Vogel (Olpe) und der Fraktion der FDP*, 19. Wahlperiode 04.05.2018.

19　連邦経済技術省は2013年に連邦経済エネルギー省（Bundesministerium für Wirtschaft und Energie）に改称された。但し、略称はBMWiで変更はされていない。

20　2006年にはBMWi『情報社会　ドイツ（iD2010 - Informationsgesellschaft Deutschland 2010）』、2009年にはBMI『重要インフラ防護―リスクと危機管理（官民への手引き）Schutz Kritischer Infrastrukturen – Risiko- und Krisenmanagement (Leitfaden für Unternehmen und Behörden)』、2010年にはBMWi『ドイツ連邦政府の情報通信技術戦略―ドイツのデジタル化2015（„IKT-Strategie der Bundesregierung“ Deutschland Digital 2015）』、2011年にはBMI『独サイバー・セキュリティ戦略2011（Cyber-Sicherheitsstrategie 2011）』が刊行された。

21　平成30年9月7日、独連邦首相府における意見交換時における担当の発言。

22　サイバー防衛（Cyber Verteidigung）は国防省（Bundesministerium der Verteidigung：BMVg）・連邦軍（Bundeswehr）で使用される言葉であり、軍事的なサイバー攻撃に対する反撃に必要な攻撃力及び防御力を総括したものであり、防御的な概念である。（BMI, *Cyber-Sicherheitsstrategie*）

23　サイバー反撃（Cyber Abwehr）はサイバー・セキュリティを保持し、向上するためのあらゆる手段であり、独連邦軍の作戦・運用面における防御的行動を示す。（SWPにおける先方研究員の発言。）

防省の総合調整部署となっている。内務省隷下には、連邦情報技術安全庁（Bundesamt für Sicherheit in der Informationstechnik、以下、BSI）、連邦憲法擁護庁（Bundesamt für Verfassungsschutz、以下、BfV）、連邦警察（Bundespolizei、以下、BPOL）、連邦刑事庁（Bundeskriminalamt、以下、BKA）などのサイバー・セキュリティ関連部署がある。BSI は連邦内の通信網におけるサイバー脅威の阻止を任務とし、BfV は国内での秘密情報活動を所掌する。また、BPOL は国境を越えて進行するサイバー脅威を阻止する他、BKA はサイバー犯罪行為の追跡を所掌している。また外務省（Auswärtige Amt、以下、AA）はサイバー外交政策、とりわけ、国連におけるサイバー政策を所掌している。また、2011 年に発足し、2016 年に改編された国家サイバー反撃センター（Nationales Cyber-Abwehrzentrum、以下、NCA）は 24 時間体制、年中無休で、各省庁の一段階下のレベルの代表者から構成され、サイバー攻撃を予防し、攻撃受け後、分析・評価を行い、対処法を勧告する任務を有する[24]。また、BSI の隷下には 24 時間体制、年中無休態勢の IT 危機対応センター（IT-Krisenreaktionszentrum）がある[25]。

さらに、国家レベルにおける官民横断の調整組織として国家サイバー・セキュリティ評議会（Nationalen Cyber-Sicherheitsrat）がある[26]。ここでは、首相府を始め、外務省、内務省、国防省、経済エネルギー省、司法・消費者保護省、財務省、教育・研究省の事務次官級、各州の代表そして、ドイツ産業連盟（Bundesverband der Deutschen Industrie）、ドイツ商工会議所連合会（Deutschen Industrie- und Handelskammertag）などの産業界代表が年に 3 回、戦略的・政策的な総合調整をし、ドイツのサイバー・セキュリティ戦略策定のため、重要な位置づけにある。

総括すれば、ドイツのサイバー・コミュニティは首相府を筆頭に平時においては内務省が主管であるが、防衛・緊迫事態ではサイバー防衛は国防省の所掌であり、サイバーに関する外交政策は外務省の所掌である。

24　Bundersministerium der Verteidigung Homepage, “Nationales Cyber-Abwehrzentrum,” https://www.bmvg.de/de/themen/cybersicherheit/partnerschaften-zur-cybersicherheit/nationales-cyber-abwehrzentrum.

25　Bundesamt für Sicherheit in der Informationstechnik Homepage, “IT-Krisenreaktionszentrum,” https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/Aktivitaeten/IT-Krisenreaktionszentrum/itkrisenreaktionszentrum_node.html.

26　BMVg, “Cyber-Sicherheitsrat,” https://www.bmvg.de/de/themen/cybersicherheit/partnerschaften-zur-cybersicherheit/cyber-sicherheitsrat.

3. 独国防省・連邦軍のサイバー・レジリエンス強化への取り組み

（1）国防省の改編

2015年初頭にドイツ連邦議会がサイバー攻撃を受けると、同年9月17日、ウアズラ・フォン・デア・ライエン（Ursula von der Leyen）国防大臣は次の4点の骨子からなる日々命令を発出した。世界中で生起するサイバー攻撃は最早、他人事ではないと、従来の認識を改める契機となったのである。「第1は、今やサイバーは陸・海・空と並ぶドメイン（領域）である。第2に連邦軍は高度にネット化、デジタル化され、サイバー空間を最大限活用するとともに、サイバー攻撃から守る必要がある。第3に既存のサイバー能力を強化し、サイバー・情報空間（Cyber-Inforamtionsraum）を所掌する、あるべき新組織（ein neues Zielbild）を国防省内及び国防省隷下に創設する。第4は、第3の目的のため、民間から登用したカトリン・ズダー（Katrin Suder）事務次官を長とする幕僚作業グループ（Aufbaustab）を立ち上げ、新体制を検討させる。[27]」

このように、連邦議会がサイバー攻撃を受けたことは、ドイツにとって、現状を変更すべき、大きな情勢変化であったと考えられ、サイバー攻撃に対する危機感から、2012年に行われた国防省の大改革以降、大きな改革に着手することになったのである。翌年の2016年には内務省は『独サイバー・セキュリティ戦略2011』の改訂版である『独サイバー・セキュリティ戦略2016[28]』を刊行した。この中で、国防省・連邦軍関連個所は次のとおりである。まず、政府全体でのサイバー・セキュリティを強化しなければならないが、その中で連邦軍の役割が増大している[29]と言及している。また、防衛という観点において、重要インフラの防護については政府全体の責任となり、国家全体で対応することが明記された[30]。さらに、ミュンヘン連邦軍大学のサイバー防衛研究所（Forschungsinstitut Cyber Defence、以下、CODE）を中心にドイツにおけるサイバー防衛関連の教育・研究基盤としてのサイバー・クラスター（Cyber Cluster）を導入し、発展させるとした[31]。さらに連邦軍と緊密に連携した国家サイバー防衛センター（NCA）を更に発展させる旨、記述された[32]。さらに、連邦軍事案対応チーム（Bundeswehr Incident Response Team）は政府全体でのセキュリティ強化策の一つと記述された[33]。そして国主体のコンピュータ緊急対応チーム（Computer Emergency

27 Die Bundesministerin, *Tagesbefehl*, 17. Sep. 2015.
28 BMI, *Cyber-Sicherheitsstrategie*, 2016.
29 Ebenda., S. 33.
30 Ebenda., S. 32.
31 Ebenda., S. 18.
32 Ebenda., S. 28.
33 Ebenda., S. 29.

Reaction Team、以下、CERT）との協力強化が記された[34]。また、連邦軍におけるサイバー関連の専門家確保の観点から、サイバー予備の導入が示された[35]。NATOと同様、サイバー情報空間は陸・海・空と同様、ドメイン一部との認識が示された[36]。内務省の『独サイバー・セキュリティ戦略』の発刊と同じ 2016 年、国防省は『国防白書 2016』を発刊した。記述した国防大臣の日々命令を受け、サイバー・情報空間を所掌する組織の在り方について次のとおり、記述されている[37]。連邦軍サイバー・情報空間関連部署は、政府全体での取り組みは勿論、研究機関、産業界そして国内外の関係機関とも連携を促進する必要がある。また、サイバー・情報空間ドメインについて、連邦軍のサイバー能力の向上、特に IT システムのセキュリティを強化し、被害から回復力を確保しなければならない。また、連邦軍サイバー・情報関連部署は保有すべき装備システム、指揮所、装備補給システムをさらに強靭なものにすべきである。また、連邦軍サイバー・情報空間部署で勤務する専門家の育成に関して、魅力溢れるキャリアパスを創造し、革新的な募集戦略を策定して、関係機関との新たなパートナーシップ及び協力プログラムを通じて、優秀な後継者を確保する必要がある。さらに、連邦軍のサイバー・情報空間に関する能力を強化することにより、様々な組織を抱え、多くの責任を担うことになる。また、連邦軍のデジタル化のための IT 能力を維持しつつ、他国及び他省庁の担当部署と連携する部署を創設すべきである。

このように、『国防白書 2016』ではサイバー・情報空間関連部署創設への布石となる文言が増え、既述したように、10 年前の『国防白書 2006』に比べて、サイバー攻撃に関する記述が大幅に増加した。

また、同じ 2016 年の 4 月には、既述した国防大臣日々命令でサイバー・情報空間関連部署の新態勢を検討していた幕僚作業グループが最終報告書『サイバー情報空間部署の幕僚作業グループによる最終報告～サイバー情報空間の責任、能力そして任務を有する新組織への勧告及びサイバー防衛の戦略的指針の改正のための補足的対策（Abschlussbericht Aufbaustab Cyber und Infomationsraum, Empfehlungen zur Neuorganisation von Verantwortlichenkeiten, Kompetenzen und Aufgaben im Cyber- und Informationsraum sowie ergänzende Maßnahmen zur Umsetzung der Strategischen

34　Ebenda., S. 34.
35　Ebenda., S. 37.
36　Ebenda., S. 40.
37　Ebenda., S. 93.

Leitlinie Cyber-Verteidigung[38]、以下、CIR 創設最終報告）』を国防大臣に提出した。同年同月、フォン・デア・ライアン国防大臣は日々命令を発出し、ここで最終的にボンを本拠地とする国防省内にサイバー IT 局を新設し、国防省隷下に陸・海・空・衛生・統合支援の各軍種に次ぐ第 6 の軍種となるサイバー情報空間コマンドをボンにおいて創設する決定を下したのであった[39]。

2016 年 10 月、フォン・デア・ライアン国防大臣は新設された国防省サイバー IT 局（Bundesminiterium der Verteidigung, Abteilung Cyber Informationstechnik、以下、BMVg, Abt.CIT）の初代局長として Thyssenkrupp AG、Volkswagen AG、Daimler AG などドイツを代表する大手民間企業で情報統括役員（Chief Information Officer）を歴任したクラウス・ミューラク（Klaus Mühleck）を抜擢し、国防省において国防省情報統括官（Chief Information Officer）も兼務させた。なお、2018 年 8 月、国防省サイバー・IT 局の新編後、サイバー・情報空間関連部署の新態勢を検討した幕僚作業グループの長の装備・IT 担当のズダー事務次官が辞任し、後任の事務次官（装備・IT 担当）には国防省装備局長であったベネディクト・チマー（Benedikt Zimmer）陸軍中将が抜擢され、文官に転換して事務方のトップとしてサイバー・情報空間部署の立ち上げに関わる大任を所掌することになった。事務方のトップの事務次官（Staatssecretär）に軍人出身者が就任するのは極めて異例[40]のことであり、フォン・デア・ライアン国防大臣のサイバー IT 分野への改革の執念を具現化し、諸準備を加速していく布陣となった。

（2）連邦軍の第 6 の軍種たるサイバー情報空間コマンドの創設

既述したように 2016 年 4 月の『CIR 創設最終報告』を受けて、フォン・デア・ライアン国防大臣は同月、日々命令を発出したが、この日々命令で初代司令官を指名し、2017 年

38　Bundersministerium der Verteidigung, *Abschlussbericht Aufbaustab Cyber und Infomationsraum, Empfehlungen zur Neuorganisation von Verantwortlichenkeiten, Kompetenzen und Aufgaben im Cyber- und Informationsraum sowie ergänzende Maßnahmen zur Umsetzung der Strategischen Leitlinie Cyber-Verteidigung*, April 2016.

39　Die Bundesministerin, *Tagesbefehl*, 26 April. 2016.

40　事務方トップの事務次官に軍人出身者が就任するのは実際は今回が初めてではない。1977 年 1 月、ギョーグ・レバー（Georg Leber）国防大臣は NATO 中欧軍司令官（Commander in Chief, Allied Forces, Central Europe: CINCENT）であったカール・シュネル（Karl Schnell）陸軍中将を装備担当の事務次官に任命した。1992 年 1 月には元陸軍総監のヨーグ・シェーンボーム（Jörg Schönbohm）陸軍中将は安全保障政策・連邦軍計画・装備担当の事務次官に就任した。現役の将官が事務次官に昇格した事例としてはチマー陸軍中将（当時）は、3 例目となる。

の 2 四半期まで第 6 の軍種[41]となるサイバー情報空間コマンド（Kommand Cyber-und Informationsraum、以下、CIR）を創設するよう指示した[42]。国防大臣は初代の CIR の司令官としてルドヴィッヒ・ラインホス（Ludwig Leinhos）空軍少将を指名した[43]。さらに大臣は既存の連邦軍指揮支援コマンド[44]（Führungsunterstützungskommando der Bundeswehr、以下、FüUstgKdoBw)、戦略偵察コマンド[45]（Kommando Strategische Aufklärung、以下、KdoStratAufkl）、連邦軍作戦コマンドセンター（Zentrum Operative Kommunikation der Bundeswehr、以下、ZOpKomBw）、連邦軍地理情報センター（Zentrum für Geoinformationswesen der Bundeswehr、以下、ZGeoBw）及び連邦軍情報技術センター[46]（Zentrum für Informationstechnik der Bundeswehr、以下、IT-ZentrumBw）を CIR の隷下に置くことを命じた[47]。この結果、SIGINT、軍事情報、電子戦、コンピュータ・ネットワーク作戦、地球宇宙での支援、IT 業務、サイバー情報セキュリティ支援及び作戦上の通信といった機能が集約・統合され、最適化されることになった[48]。特筆すべきは、新設された、戦略偵察コマンド（KdoStratAufkl）内のサイバー作戦センター（ZCO）が攻撃的対処行動を遂行し、連邦軍 IT コマンド（KdoITBw）内の連邦軍サイバー・セキュリティセンター（ZCSBw）が防御的対処行動を遂行することにある[49]。

2017 年に非公表の『連邦軍デジタル化戦略指針（Strategische Leitlinie Digitalisierung im Geschäftsbereich BMVg）』が部内に配布されたが、その骨子は次のとおりである。「情報技術の革新速度は著しく、連邦軍の必要性を如何に調和させるかが課題であり、情報技

41　ドイツ連邦軍では「軍種（Teilstreitkraft）」は「機能別の軍隊」（Streitkräften nach funktionalen Gesichtspunkten）であり、「陸軍（Heer）、空軍（Luftwaffe）、海軍（Marine）の他、衛生軍（Zentrale Sanitaetsdienst）及び統合支援軍（Streitkräftbasis）」である。Ernst-Christoph Meier, Andreas Hannemann, Rainer Meyer zum Felde, *Wörterbuch zur Sicherheitspolitik - Deutschland in einem veränderten internationalen Umfeld*, 16. Januar. 2012, Mittler, S. 440.

42　Die Bundesministerin, *Tagesbefehl*, 26 April. 2016.

43　Ebenda. なお、司令官（Inspector CIR）は中将職、副司令官兼ねて連邦軍情報保全官（Chief Information Security Officer）は少将職、参謀長も少将職、隷下の指揮統制部、運用部、計画部の各部長は准将職と定められている。BMVg, *Abschlussbericht Aufbaustab Cyber- und Informationsraum*.

44　2017 年 4 月に CIR が創設されたが、連邦軍指揮支援コマンド（FüUstgKdoBw）は連邦軍 IT コマンド（Kommando Informationstechnik der Bundeswehr: KdoITBw）へと新編され、同時に新設された連邦軍ソフトウェア能力センター（Zentrum Softwarekompetenz der Bundeswehr: ZSwKBw）とともに現在に至っている。BMVg, *Abschlussbericht Aufbaustab Cyber- und Informationsraum*.

45　2018 年に戦略偵察コマンド（KdoStratAufkl）の隷下にはサイバー作戦センター（Zentrum Cyber-Operationen: ZCO）が新設され、現在に至っている。Ebenda.

46　連邦軍情報技術センター（IT-ZentrumBw）は廃止され、現在、新編連邦軍 IT コマンド（Kommando Informationstechnik der Bundeswehr: KdoITBw）の隷下に連邦軍サイバー・セキュリティセンター（Zentrum für Cyber-Sicherheit der Bundeswehr: ZCSBw）が新設されている。Ebenda.

47　Die Bundesministerin, *Tagesbefehl*, 26 April. 2016.

48　CIR 担当、筆者によるインタビュー、於ボン、2018 年 9 月 5 日。

49　同上。

術は、業務プロセスを支援するための手段ではなく、業務要領を見直す推進基盤である。デジタル化は単に技術という問題ではない。考え方を抜本的に変える必要がある[50]。」

また、CIR の司令部に状況センター（Situation Center）を創設し、サイバー状況図により、共通認識を図り、政府内での協力を促進することになった[51]。2018 年 4 月に CIR 本部が創設され、暫定運用が開始された。CIR は各省の隷下の 6 機関（連邦軍、連邦情報技術安全庁、連邦災害救援市民防護庁、連邦憲法擁護庁、連邦犯罪庁、連邦情報庁）とも連携しつつ、次の任務を遂行する[52]。ドイツ防衛のための憲法上の任務、連邦軍への浸透への防衛任務、連邦軍の指揮通信の要となる IT 業務を確実に運用する任務、敵対勢力によるサイバー情報空間の使用を混乱もしくは拒否する任務、そして、災害統制あるいは市民防護のため、連邦軍による行政支援に関する任務である。具体的な CIR の業務は、連邦軍の IT システムの運用、電磁、サイバー空間、情報環境に関する情報業務、地理情報、政府間のサイバー・セキュリティの 4 本柱から構成される[53]。今後、2019 年 4 月には連邦軍ソフトウェア能力センター（Zentrum Softwarekompetenz der Bundeswehr: ZSwKBw）が連邦軍 IT コマンド（KdoITBw）内に新設され、2021 年には CIR は完全運用を開始する予定である[54]。

（3）ミュンヘン連邦軍大学サイバー防衛研究所の創設

日本の防衛大学校、そして米国の陸海空の各士官学校に相当する、将来の将校（幹部）を育成する機関として、ドイツには連邦軍大学が2つ存在し、それぞれ南のミュンヘンと北のハンブルクに所在することから、ミュンヘン連邦軍大学（Universität der Bundeswehr München）及びハンブルク連邦軍大学（Universität der Bundeswehr Hamburg）と呼称される。ミュンヘン連邦軍大学には宇宙センター、リスク・インフラ・安全・紛争研究所、現代操縦システム研究所、ミュンヘン宇宙統合研究所がある[55]。これらに加えて、2013 年、高まるサイバー脅威を踏まえ、サイバーを研究する、ドイツ唯一の研究機関としてサイバー防衛研究所（Forschungsinstitut Cyber Defence、以下、CODE）が創設された。既述したよ

50　CIR 高官、筆者によるインタビュー、於ベルリン、2018 年 9 月 5 日。

51　同上。

52　BMVg, *Abschlussbericht Aufbaustab Cyber- und Informationsraum*.

53　Homepage BMVg, “Aufstellung Kommando CIRCyber- und Informationsraum: Ein Meilenstein deutscher Sicherheits- und Verteidigungspolitik,” 5 April 2017, https://www.bmvg.de/de/aktuelles/aufstellung-kommando-cir-11120.

54　BMVg homepage, “Entwicklung des Organisationsbereichs bei der Bundeswehr,” https://www.bmvg.de/de/themen/cybersicherheit/cyber-verteidigung/entwicklung-des-org-bereich-bei-der-bw.

55　Homepage Universität der Bundeswehr München, “Forschungseinrichtungen,” https://www.unibw.de/forschung/forschungseinrichtungen.

うに 2016 年に刊行された『独サイバー・セキュリティ戦略』において CODE は単に国防省・連邦軍に留まらず、ドイツ国内におけるサイバー研究機関となると示されており、軍事面でのサイバー IT の安全保障については、ミュンヘン連邦軍大学に新設される CODE がサイバークラスター（群）として、研究機関、民間企業、非軍事組織のサイバー保全と連携しつつ、中心的な役割を担うことになった[56]。

CODE が付与されている任務としては次の諸点である[57]。まず、新技術の利用への助言、新技術及び手段の分析・試験・評価、脆弱性分析及び、物理的サイバーシステムに関する基礎研究、保全基準に基づく IT 保全構想の更なる発展、サイバー・IT 関連の講義・訓練における IT 専門家の提供、サイバーに関する実際的訓練の実施、リスク分析の準備、試作品の製造・建設、並びに、連邦軍関係機関への支援と多岐に亘っている。教育分野においては、2018 年に CODE はサイバー・セキュリティに関する修士課程を発足させたが、留学生の受け入れを視野に入れており、今後は教授の増員、実験場の増加など研究の重要な基盤の拡大が不可欠となっている[58]。CODE における研究分野はサイバー防衛、スマート・データ、移動上の安全（Mobile Security）、e-Health、重要インフラの5つの分野を網羅している[59]。特筆すべきは e-Health である。この研究は、医療・健康分野のデジタル化、医療分野の取り込みを図るものであり、具体的には外科手術の演練をコンピュータで実施したり、バイオ技術を駆使した監視を行ったり、連邦軍衛生庁と連携し、グローバル健康安全センターの導入に寄与することを狙いとしている。但し、遺伝子操作の影響など倫理上危険な分野までには踏み込んでいない[60]。なお、CODE は 2019 年には更に秘密情報機関要員養成の修士課程を創設する予定であり、参加者としては想定されているのは国防省、連邦軍の文官、軍人の他、内務省、連邦情報庁、外務省、憲法擁護庁など公務員である[61]。

（4）国防省を中心としたサイバー・セキュリティ・イノベーション庁の創設

ドイツ連邦共和国の旧首都ボンには国防省の第 1 拠点、いわば本拠地が所在し、ベルリンは第 2 拠点が所在する。既述したように、国防省サイバー・IT 局及び連邦軍サイバー情報空間コマンド（CIR）はボンに所在し、他省庁間の要員で構成される国家サイバー反撃センター（NCA）もボン所在機関であることから、ボンはドイツにおけるサイバー中枢都市と言

56　ミュンヘン連邦軍大学高官、筆者によるインタビュー、於ミュンヘン、2018 年 9 月 3 日。
57　CODE 高官、筆者によるインタビュー、於ミュンヘン、2018 年 9 月 3 日。
58　同上。
59　Homepage Universität der Bundeswehr München, “Ziel von CODE,” https://beta.rz.unibw-muenchen.de/unibw/code/im-profil/ziele.
60　CODE 高官、筆者によるインタビュー、於ミュンヘン、2018 年 9 月 3 日。
61　ミュンヘン連邦軍大学高官、筆者によるインタビュー、於ミュンヘン、2018 年 9 月 3 日。

える。他方、ミュンヘンに所在するCODEはサイバー・クラスターとして呼称されている。『CIR創設最終報告』を纏めた作業幕僚グループ長であった、ズダー事務次官は、サイバー関連技術の進展が極めて速いことを踏まえ、サイバーに関するイノベーションを促進するため、軍人・企業からの成るチームを構成し、産業界と当初から技術協力を行うという「サイバー・イノベーション・ハブ（Cyber Innovation Hub、以下、CIH）」を首都ベルリンに立ち上げることを提唱した[62]。このCIHは例えば、新規に研究開発する軍事関連の装備品は、戦闘を想定して頑丈さ、あるいは耐久性などを考慮し、軍事能力に特化していくが、サイバー関連の技術の進展速度の速さと重厚長大な装備品よりも、システムなどの開発が主体となることから、装備品等もスリムな構造にしていくという戦略的な発想に基づくものである。このCIHで想定されているのは、人工知能（AI）、サイバー作戦、サイバー情報、自動化システムなどである。また、軍人と企業から構成されるチームを形成することによって、不足する人材をサイバー予備として確保できる利点も有するのが特色である。2018年8月、CIHをさら発展すべく、国防省と内務省の間でサイバー・セキュリティ・イノベーション庁（Agentur für Disruptive Innovationen der Cybersicherheit）の創設が公表された[63]。同庁の創設目的は国内外のサイバー・セキュリティを確保するため、各種プロジェクトの中で、優先順位を定め、特に可能性が高い計画・プロジェクトを促進していくことを調整することにある[64]。すなわち、現在の研究及び技術を発展させ、産業界、官側、そして研究者から柔軟な構想を受け、短期間に計画を進捗させることが可能となる。同庁の規模は100名の職員に2018年は1,500万ユーロ（約20億円）、2019年から2022年までは2億ユーロ（約260億円）の予算が見込まれており、年間平均すると4,000万ユーロ（約50億円）から5,000万ユーロ（約65億円）の規模であるが、80%は研究及びイノベーションそのものに活用される[65]。

4. ドイツ国防省・連邦軍におけるサイバー関連システム整備の方向性

ドイツ国防省・連邦軍は既述した組織改編を踏まえ、サイバー・レジリエンス強化のためのシステム等の研究・開発を進めている。拙稿では、既述した国防省内のミュンヘン連邦軍大学CODE及び、国防省が研究を委託しているフラウンホーファー研究所

62 BMVg Homepage, “Cyber Innovation Hub,” https://www.bmvg.de/de/themen/cybersicherheit/partnerschaften-zur-cybersicherheit/cyber-innovation-hub.

63 Homepage BMVg, “Bundeskabinett beschließt Cyberagentur,” 29.08.2018, https://www.bmvg.de/de/aktuelles/bundeskabinett-beschliesst-cyberagentur-27392.

64 Ebenda.

65 Ebenda.

（Fraunhofer-Institut、以下、FH）におけるサイバー関連の研究プロジェクトの一端について紹介したい。

（1）CODE における、将来のサイバー関連システム等の萌芽

第 1 は CODE である。CODE は各企業と研究プロジェクトに係る覚書（Memorandum of Understanding：MoU) を交わし、プロジェクトを進めている。Hensoldt 社とは覚書を締結後、プロジェクトに基づく協力、高度に保全が徹底された運用システム及び、IT システムの強化に関する研究成果について、既に Schaeffler AG、BMW、T-System あるいは Deloitte 社との協力に関する契約を締結した[66]。また、ESG 社との間では覚書締結後、サイバー・レンジ訓練、ネット・シュミレーション、サイバー訓練、公開情報などの軍事・技術システムの強化に関する研究成果について、上述企業との協力に関する契約が進められている[67]。その他、CODE と共同研究について覚書を交わしたのは、次の 7 社である[68]。連邦軍保有の BWI 社とはセキュリティ・オペレーション・センターの充実、学生と研究者を統合に関する研究を実施する。また、Infodas 社とはネットワーク・セキュリティ、情報流出の発見、サイバー・セキュリティにおける広報について研究を行う。さらに、Uni Twente 社とは共通の研究分野での協力及び、研究インフラの共通使用について合意した。Secunet 社とはソフトウェアでネットワークを運用（Software Defined Network、以下、SDN）する技術の検証、人工知能と認識手法への革新的な攻撃に対する共通の研究について署名した。Atos 社とはサイバー・セキュリティ、スーパーコンピュータ・量子コンピュータ（HPC/QC）、ビッグデータと分析（BDA）、モノのインターネット（IoT）に関する研究を進めていくことになった。ENISA 社とはネットワーク・セキュリティにおける革新的なサイバー・セキュリティ技術に関する研究開発を実施する。CGI 社とはフェイク・ニュース、SNS に関する事項について研究を行う予定である。また、Rheinmetall 社と SANS 研究所とも近い将来、共同研究の覚書を締結する予定である[69]。これらに加えて、CODE では最先端量子コンピュータ研究拠点として IBM Q Network Hub を開設する予定である[70]。IBM Q は、IBM（米国）で開発されている最先端の汎用量子コンピュータであり、世界では米国の国家安全保障局（National Security Agency、以下、NSA）、中央情報局（Central Intelligence Agency、以下、

66　CODE 高官、筆者によるインタビュー、於ミュンヘン、2018 年 9 月 3 日。
67　同上。
68　同上。
69　Rheinmetall 社とは国内ユーザーのためのサイバー情報・移動目標からの防衛について、SANS 研究所とは専門家の交換、IT 保全コミュニティの創設などについて共同研究が検討されている。
70　Universität der Bundeswehr München Homepage, “Forschungsinstitut CODE baut Cybercluster weiter aus,” 13 Juli 2018, https://www.unibw.de/home/news/forschungsinstitut-code-baut-cybercluster-weiter-aus.

CIA）、英国のオックスフォード大学、豪州の大学、日本の慶応大学に次ぎ6番目のものである[71]。サイバー・セキュリティ関連の解析・分析に、この量子コンピュータは大きな役割を果たすものと思われる。

（2）国防省委託研究に見られる、将来の連邦軍システム等の萌芽

第 2 はフラウンホーファー研究所 (FH) である。FH は独国内に 72 の研究所を保有するが[72]、その中で、ネット化されたシステムの統制、ネット化システムの運用指揮などの研究分野を所掌し、国防省及び連邦軍の研究に特化した研究所はボンに所在するフラウンホーファー通信・情報処理・人間工学研究所 (Fraunhofer-Institut für Kommunikation, Informationsverarbeitung und Ergonomie[73]、以下、FKIE) である。FKIE の予算については 80% が国防省から拠出されており、予算別プロジェクトの内訳は、半分が研究所独自でテーマを決めて研究する自主研究、残りの半分が国防省・連邦軍指定研究である[74]。

FKIE は世界的に大被害をもたらしたオンライン犯罪 Avalanche（アヴァランチ）への対応を踏まえ、権限を持たないユーザーがカーネル（kernel）・コード[75] を修正することなく独自のファイルシステムを作成できる機能を提供するソフトウェアである pcapFS を開発した[76]。また、FKIE ではマルウェアの発見、確定のソフトウェアである MALPEDIA も開発している[77]。

おわりに

ドイツ国防省は、いわゆるサイバー分野における軍事力、あるいは防衛力を整備していく

71　IBM Homepage, “IBM und die Universität der Bundeswehr München starten IBM Q Hub,” 12 Jul 2018., https://www-03.ibm.com/press/de/de/pressrelease/54152.wss.

72　フラウンホーファー研究所は欧州最大の応用研究機関であり、民間企業や公共機関向け、また社会全体の利益を目的として、実用的な応用研究を実施している。全体の予算額は 23 億ユーロ（3,000 億円）であり、研究員・職員等併せて 25,500 名。この過半数が研究者・職員であるが、30% は大学生、大学院生、専門学校生となっている。Fraunhofer-Institut, *Annual Report 2017*, S. 1. & S. 35.

73　FKIE は 1963 年に創設された研究所が 2009 年に FH に編入されて、現在に至っている。総職員数は 400 名であり、総予算は 3,000 万ユーロ（4 億円）である。部署ごと研究分野を所掌しており、細部はセンサー・データ融合、通信システム、人的要素、人間ロボット・システム、人間工学システム、指揮システムのための情報技術、認知移動システム、サイバー分析及び防衛、サイバー・セキュリティ及び、利用可能なセキュリティとプライバシーである。FKIE Homepage, https://www.fkie.fraunhofer.de/.

74　FKIE 研究者、筆者によるインタビュー、於ボン、2018 年 9 月 4 日。

75　OS の核となる部分。コンピュータを動作させるための基幹となるサービスを提供する。ホームページ、『ASCII.jp デジタル用語辞典』, http://yougo.ascii.jp/caltar/%E3%82%AB%E3%83%BC%E3%83%8D%E3%83%AB.

76　Martin Lambertz and Jan-Niclas Hilgert, “pcapFS,” FKIE.

77　Daniel Plohmann and Sascha Alexander Jopen, “MALPEDIA,” FKIE.

サイクルを次のように規定している[78]。第1段階は基礎研究、特別研究、部署での研究など研究・開発である。第 2 段階は、この研究・開発の成果を踏まえ、民間企業、他省庁との連携しつつ、各種プロダクトの構想化を図る。第 3 段階は各種試験、試作品生産、保全に留意した作業を通じて、各種システムを生産する。第 4 段階は製品として各種システムを生産し、製品についての教育・訓練を行い、整備を実施して、市場化及び汎用化を図る。このように、第 1 段階から第 4 段階まで夥しい時間が必要である。

ドイツ国防省では、装備品等の国際協力・共同開発を進めているが、ドイツ連邦共和国として国防技術上、極めて重要な技術と位置付けている分野においては、単独にて国産装備品を整備している。この極めて重要な技術分野（Schlüsseltechnologiefelder）としては、陸軍においては防護力関連及び装軌・装輪車両関連、海軍においては潜水艦関連であり、陸・海・空・宇宙のドメインで共通しているのがセンサー関連、そして、陸・海・空・宇宙・サイバーの全ドメインで共通するのが、ネットワーク化された作戦指揮能力及び秘匿・暗号関連の技術である[79]。従って、国防省・CIR における抜本的なサイバー IT 改革が継続中のサイバー中枢都市のボン、CODE を中心としたサイバー・クラスターが充実しつつミュンヘン、そして産・官・学の一体化を目指し、動き始めたサイバー・イノベーション・ハブが存在するベルリンの 3 大都市を中心として、今後、ドイツ独自のアプリケーション、プログラム、システム、器材そして装備品が開発され、整備されていく可能性は高い。

しかしながら、サイバー技術の進展速度は速い。現在、独ではサイバー攻撃事態を如何にアンティシペーション（anticipation: 予測）し、アトリビューションはいつ、どのように判断するのか、これらの所掌は誰になるのか、などの議論が活発に行われているが、未だ結論に到達していない[80]。加えて、ドイツ国防省・連邦軍はサイバー IT 関連部署の改革を断行しているが、今後の課題について申し述べたい。ドイツ連邦軍は、陸軍、海軍、空軍、衛生軍、統合支援軍にサイバー情報空間コマンド（CIR）が加わり、いわば 6 個の軍種から構成されることになった。これまで 5 個の軍種により、人事管理を行ってきた国防省・連邦軍は、今後、サイバー IT において、どのようなキャリアパスと経歴、教育・訓練体系を発展させていくのかは大きな課題である。ドイツ連邦軍の軍人は入隊当初、陸・海・空のいずれかの制服を着用するが、CIR で勤務している陸軍歩兵大尉が陸軍歩兵中隊長を 2 年から 3 年経験すれば、その間にサイバー・IT 関連技術は著しく進展し、陸軍歩兵大尉が再び、サイバー部署に復帰しても、部下を指導することは勿論、戦力発揮することは極めて厳しいとの見方が趨

78　Prof. Dr. Gabi Dreo Rodosek, “Cyber-Cluster an der UniBw M,” https://www.afcea.de/fileadmin/user_upload/Sonderveranstaltungen/FA_mit_FueUstgKdoBw/14-UniBw-CyberDefence1.pdf.

79　独国防省装備局第 2 部担当、筆者によるインタビュー、於ベルリン、2018 年 9 月 6 日。

80　独首相府連邦軍高官、筆者によるインタビュー、於ベルリン、2018 年 9 月 7 日。

勢である[81]。さらに、ドイツ連邦軍も、我が国と同様、少子高齢化、産業界の景気拡大基調などにより、サイバー・IT 関連の人材を確保するのは至難の業である。国防省では、サイバー関連の学位を取得する学生で将来、連邦軍のサイバー部署で勤務を希望する者にはサイバー奨学金の給付、あるいは、国防省サイバー・IT 局、CIR で勤務する職員には毎月支給されるサイバー給付手当を更に充実させることを検討している。サイバー・イノベーション・ハブの構築の目的は、産業界で活躍するサイバー関連の転職者を獲得し、一部はサイバー予備として、民間でも連邦軍でも勤務できる体制を企図している。ドイツは、2015 年以降、サイバー・スペースのガバナンスを強化しており、特に国防省・連邦軍のサイバー関連防衛力を急速に強化する体制・態勢へと移行している。この意味で、ドイツが既述した課題を克服し、どのように進歩・発展していくのか、サイバー・スペースのガバナンスへの取り組みについて、引き続き、注視していくことが必要である。

最後に、日独間の防衛協力への含意を指摘したい。日独の装備協力については、協定の文書化が必要との認識から、関係部署での調整が重ねられてきたところ、2017 年 7 月 17 日には、ベルリンにおいて八木毅駐ドイツ大使とズーダー事務次官との間で「防衛装備品及び技術の移転に関する日本国政府とドイツ連邦共和国政府との間の協定[82]」が締結された。この協定により、日独間で移転される防衛装備品及び技術の第三国移転や目的外使用に係る適正な管理が確保されることになった[83]。さらに、2019 年 2 月に日本を訪問したアンゲラ・メルケル（Dr. Angela Merkel）首相と安倍首相は、情報保護協定の締結交渉が大筋合意に至ったことを歓迎し、これを機に安全保障・防衛分野での協力を推進していくことを確認した[84]。日独情報保護協定の締結については、現状は大筋合意であるが、近い将来、正式に締結されることになれば、サイバー分野を含めた日独の装備協力が進展することが予測される。

（こばしふみゆき　1 等陸佐　第 2 地対艦ミサイル連隊長兼ねて美唄駐屯地司令（前軍事戦略研究室主任研究官））

81　CIR 高官、筆者によるインタビュー、於ベルリン、2018 年 9 月 5 日。

82　外務省ホームページ「日・独防衛装備品・技術移転協定の署名」https://www.mofa.go.jp/mofaj/erp/c_see/de/page22_002828.html.

83　同上。

84　外務省ホームページ「日独首脳会談」（平成 31 年 2 月 4 日）https://www.mofa.go.jp/mofaj/erp/c_see/de/page6_000255.html.