警察政策学会資料　第134号
令和６（２０２４）年６月

国家安全保障に関する諸論考

警察政策学会

テロ・安保問題研究部会

国家安全保障に関する諸論考

Ⅰ　中国共産党員である留学生の受入管理の日米比較 …… 1

Ⅱ　ガザ戦争～シギント、AI、そして多数の民間人死傷者 …… 15

Ⅲ　米国 ACD・Defend Forward とシギント機関の役割 …… 31
～日本「能動的サイバー防御」と対比して～

Ⅳ　Hunt Forward 作戦とは何か …… 45

Ⅴ　米国サイバー任務部隊（通称、サイバー軍）の惨状と教訓 …… 51

中国共産党員である留学生の受入管理の日米比較

茂田　忠良

＜目次＞

1　はじめに …… 1
2　米国における中国共産党員の入国管理 …… 2
3　米国における中国共産党員留学生のセキュリティ管理 …… 5
4　我が国における中国共産党員の入国管理 …… 6
5　我が国における中国共産党員留学生のセキュリティ管理 …… 9
6　外国為替及び外国貿易法 25 条（経産省所管部分）による規制 …… 10
7　まとめ …… 12

1　はじめに[1]

（1）「中国共産党に選ばれる国」

元内閣官房参与の谷口智彦氏が、2024 年 3 月 3 日付け産経新聞に、「中国共産党に選ばれる国」というコラム[2]を執筆している。それによれば、

○　2023 年 6 月末現在、在留資格を得て日本に住む中国人は 78 万 9495 人。中国では労働人口の 9 人に 1 人は中国共産党員であり、「勤勉で忠実、頭脳明晰という者ほど、党員である確率が高い。入党の勧誘を、党は当然にも優秀な人材に向け集中させるからだ。してみると、日本の一流大学院、有名企業の研究開発部門に属す中国人には、平均を上回る比率で党員がいるとみておくべきだろう。」

○　中国共産党の党規約（「章程」）第 30 条は、「正式党員が 3 人以上いる場合、必ず「基層組織」（細胞）を作らなければならないと定めている。」

（2）中国共産党員のセキュリティ・リスク

谷口氏の言に従えば、在留中国人の内 10%以上は中国共産党員であり、日本の大学院や企業の研究開発部門で働いている中国人研究者には中国共産党員が多数存在するということになる。ところで、もともと共産党組織は、マルクス・レーニン主義に基づき暴力革命遂行のための組織原理に従って構築されており（19 世紀ロシアのテロ組織をモデルにしたと言われている）、中国共産党は民主主義国家における議会政党とは全く性格が異なる。中国共産党員は、党「章程」第 3 条にあるように「党の決定を実行し、組織の任務に服従し、党の

---

[1] 本論考の執筆に当たっては、警察政策学会テロ・安保問題研究部会の宇生航氏から貴重な御助言をいただいた。ここに謝意を表します。

[2] 谷口智彦、「中国共産党に選ばれる国」、2024 年 3 月 3 日付け産経新聞「日曜コラム」

任務を積極的に完遂する」義務を負っている。正に中国共産党のエージェントであり、潜在的なスパイである。

一般に中国インテリジェンスによる先端技術収集の手法は、人海戦術的な側面がある。先ず、多数の学生・研究者を送り出し、その中で情報価値のある地位に就いた者を通じて情報を収集する。従って、中国人学生や研究者が中国共産党員でないからといって、リスクがないとは言えない。一方、共産党員は、既述の如く共産党に特別の義務を負っているのであるから、スパイ活動をする可能性はより大きくなる。

従って、経済安全保障や技術流出防止の観点からは、当然、大学院や研究所の中国人研究員が中国共産党員であるか否かを把握し、違法なスパイ活動をしていないか調査をして防止する必要性が高いと言えよう。また、この中国共産党員に対する受入管理の在り方は、我が国の経済安全保障や技術流出防止に対する取組を見る上で、一つのバロメーターと言えるであろう。

そこで本稿では、中国共産党員である留学生の入国管理と在留中のセキュリティ管理（国家安全保障上の脅威の調査）について、米日両国の現状を対比する。但し、本論点に関する公開資料はそれほど多くないので、公開資料を基礎に合理的推定を加えて記述する。

2　米国における中国共産党員の入国管理

（1）米国留学のためのビザ申請手続

米国への留学目的の入国ビザ申請においては、共産党員であるかどうか情報開示が要求されていると推定できる。先ず、米国務省のオンライン申請書の解説書[3]によれば、（留学を含む）非移民ビザ申請のための質問票 DS-160 には、「今までに所属、貢献、又は勤務した、職業的、社会的、又は慈善的な団体」を全て記入する項目がある[4]。この表現だけでは、共産党が「社会的団体等」に該当するのか明白ではないが、これには共産党が含まれると考えられる。その理由は、米国ビザ専門弁護士によれば、元々この質問項目は、ビザ申請者が所属する普通の団体名を収集しようという質問ではなく、（潜在的に危険な）政治的傾向や政治団体との関係の把握を意図したものされているからである[5・6]。また、後述するように、

---

[3] US Department of State, Bureau of Consular Affairs, *Online Nonimmigrant Visa Application DS-160 EXEMPER,* undated, accessed 3 March 2024.

[4] 2024 年 3 月 3 日にアクセスしたオンライン査証申請の質問文は、“Have you worked for any organizations, such as professional, social, or charitable ones?”　となっている。

[5] Giacomo Jacques Behar’s Answer, "Have you belonged to, contributed to, or worked for any professional, social, or charitable organization?" *Avvo Questions & Answers*, 10 September 2023, accessed 3 March 2024, https://www.avvo.com/legal-answers/-have-you-belonged-to-contributed-to-or-worked-for-5838238.html

[6] 米国務省のオンライン申請書の解説書を見ると、申請書提出前の確認コーナーの「安全保障及び背景情報」の欄に、「貴方は共産党や全体主義政党の党員であるか又は関係を持っていますか」の質問項目があるが、この質問は必ずしも非移民ビザ申請書全体に付されてはいない様である。筆者が 2024 年 3 月 3 日にウェブ上で米留学生用のビザ申請書の内容を閲覧した際には、この質問項目は見つからなかった。
--US Department of State, Bureau of Consular Affairs, *Online Nonimmigrant Visa Application DS-160 EXEMPER,* undated, accessed 3 March 2024.

共産党員であることを理由に、ビザの有効期間を短縮したり、移民ビザの発給拒否事由とするなどの実務が行われている事実からもその意図が伺われる。

さて、意図はそうであるとしても、文章上からは明白ではないので、この質問で把握できるのかと疑問が生じるが、そこで領事担当職員によるインタビューが登場する。即ち、留学生ビザ発給の前提として、申請書の提出に加えて、大使館や領事館の領事担当職員のインタビューがあるので、その際に共産党員であるか否かの質問が行われていると考えられる。米中蜜月時代であれば別として、次節（2）（イ）でも述べるように[7]、現在の米国は中国共産党員を強く警戒しているので、先ず、インタビューの際に質問しないとは考えられない。

なお、このビザ申請の際の申告の真実性を確保するため、虚偽申告は、合衆国法典 18 篇 1546 条（a）によって可罰的であり、その違反には 10 年以下の拘禁刑が規定されている[8]。

また 2019 年以来、ビザ申請時には、（申告の真実性を確保するための情報収集手段として）本人の E メールアドレスに加えてソーシャルメディアのアカウントとハンドル名の申告が義務付けられている[9]。サイバー空間における活動履歴の調査によって相当程度、本人の申告の真実性が担保できるが、特に留学先が機微な部署である場合には詳細な調査が行われるであろう。

以上を要約すると、①ビザ申請時の申請書の記載内容（虚偽記載には刑事罰）、②領事担当者によるインタビュー（虚偽供述には刑事罰）、そして、③ソーシャルメディアの活動調査による裏付け調査の三者を組み合わせることによって、留学生が中国共産党員であるかどうかを含めて国家安全保障上の脅威を評価する態勢が構築されている。更に、疑念がある場合には、FBI などを通じて、④米国内のデータセンターにある当人関連の情報（ウェブメール、ウェブ検索履歴等）から当該者のセキュリティ・リスクを更に調査することが可能であろう。

なお現在、米国は中国共産党員の留学自体を禁止している訳ではない。但し、ビザ審査の過程で、機微な研究部署への留学についてはビザを拒否できる態勢が整っているということである。

（２）中国共産党員の米国入国の規制

近年、中国共産党員の米国入国に対する規制は厳しさを増しているが、その状況を概観する。

ア　移民ビザでの規制

先ず、米国における長期居住を目的とする移民ビザは、移民国籍法 212 条（a）(3)(D)の規定により、共産党員に対しては昔から基本的に認められていない。即ち、共産党その他全体主義的政党の党員である者又は関係を持っている（affiliated）者は、基本的に米国への移

---

[7] 共産党員やその直近家族にだけ、査証有効期間を短縮し且つ 1 回限りにするなど、共産党員であることを把握できることを前提に、査証制度が運用されている。

[8] 例えば、ボストン大学の留学生であった Ye Yanqing は、ビザ取得時に経歴について虚偽の申告（人民解放軍での勤務歴を不申告）をしたとして、2020 年 1 月に指名手配されている。茂田忠良「インテリジェンスこぼれ話４　FBI 国家安全保障部門によるスパイ摘発（下）」警察公論 78 巻第 5 号（立花書房、2023 年 5 月）参照。

[9] Maggio Kattar, “Nonimmigrant VISA Application DS-160 Now Collecting Social Media Information,” *Maggio Kattar (blog),* 7 June 2019, accessed 3 March 2024, https://maggio-kattar.com/blog/nonimmigrant-visa-application-ds-160-now-collecting-social-media-information/

民は認められないのである。但し、除外規定があり、①5 年以上前に離党している場合、②強制的に入党させられたなど、非自発的な場合、③党員や活動歴が全て 16 才未満の過去のことである場合、④入党することが、多くの国民に提供されている食糧など生活必需品・仕事や教育を得るなど生活の必要上已むを得ない場合などは、個別審査によって移民が認められる余地がある[10・11]。

なお、K－1 ビザ（婚約者ビザ）は、形式的には非移民ビザであるが、移民ビザの実質をもっているため、申請書の質問項目に、「あなたは、共産党その他全体主義的政党の党員である者又は関係している者ですか」がある[12]。移民ビザの発給拒否事由であるからである。

イ　非移民ビザの規制強化

移住のためでない滞在ビザ（非移民ビザ）についても、中国共産党員に対する制限が厳しくなりつつある。2020 年 12 月、中国共産党員と直近の家族の米国旅行のためのビザは、有効期間を発行から 1 ヵ月間、且つ 1 回限りに制限する旨国務省報道官が公表した[13]。それまでは、中国共産党員も中国一般国民と同様に、ビザの有効期間は 10 年間で複数回の入国が可能であった。

また、2020 年秋には、中国の航空会社の搭乗員や船舶会社の乗組員に対する入国審査が強化された。入国審査官が、中国共産党員か否か、入党の動機は何かなどを執拗に質問し、場合によっては審査が数時間に及ぶこともあったという。これに対しては、中国外務省報道官が中国の搭乗員・乗組員に対する嫌がらせであると非難している[14]。しかし、ソ連時代の慣行を見ても分かるように、共産主義国家は、しばしば搭乗員や乗組員を諜報工作やインテリジェンスのエージェントとして使っているので、搭乗員や乗組員に対する入国審査を厳しくするのは、国家安全保障の観点から自然である。

なお、中国共産党員自体に対する規制ではないが、米国政府は、中国公営報道機関の在米中国人職員に対する規制も強めている。即ち 2020 年 2 月 28 日に、中国共産党及び中国政府が経営する報道機関 5 社の在米中国人職員数の上限を 100 人に制限する（実質約 60 人の削減）と公表し、同年 3 月 13 日に発効させた。5 社とは新華社（国営）、中国環球電子網

---

10 米国国籍移民局の政策マニュアル第 8 部第 3 章：USCIS, *Chapter 3-Immigrant Membership in Totalitarian Party,* undated, accessed 3 March 2024. https://www.uscis.gov/policy-manual/volume-8-part-f-chapter-3

-- US Department of State, Bureau of Consular Affairs, *Ineligibilities and Waivers: Laws,* undated, accessed 3 March 2024.

11 中国の場合は④が適用される可能性は低いと見られている。Gary Chodorow, "Communist Party Membership Makes Some Ineligible for U.S. Green Card and Citizenship," *Chodorow Immigration Law,* 24 April 2023, accessed 3 March 2024.

12 US Department of State, Bureau of Consular Affairs, *Online Nonimmigrant Visa Application DS-160 EXEMPER,* undated, accessed 3 March 2024.

13 Paul Mozur and Reymond Zhong, "U.S. Tightens Visa Rules for Chinese Communist Party Members," The New York Times, 3 December 2020, updated 19 April 2021.

14 Chun Han Wong, "China Complains of U.S. Harassment of Chinese Airline and Ship Crews," *The Wall Street Journal,* updated 30 November 2020.　本記事によれば、航空機搭乗員や船舶乗組員を含む旅行用のビザの申請書でも、申請者が「共産党その他全体主義的政党の党員である者又は関係を持っている者」か否かの申告を求められるとしているが、筆者が 2024 年 3 月 3 日にビザ申請書の内容を閲覧した際には、その質問項目は見つからなかった。

--Abby Lemert and Eleanor Runde, "New U.S. visa Rules Prompt Scrutiny of CCP Members," *Lawfare*, 11 December 2020.

（国営）、中国国際放送局（国営）、中国日報（党営）、人民日報（党営）である。また、米国国務省は、同年 2 月に上記 5 社を今後は（民間企業ではなく）中国政府機関として扱い、その職員には外交官と同様の制限を課すると宣言している[15]。共産党は公営報道機関を「共産党の口舌」であると位置付けて重視しており、また諜報機関員のカバーとして使用するのは常套手段である。1970 年代のソ連の在日公営報道職員の約半数は諜報機関員であったと推定されている[16]。公営報道機関の海外派遣職員は、インテリジェンス機関員である可能性が高く、また党員である可能性も高いのであるから、それら職員の数を規制し監視するのは、国家安全保障の観点から当然であろう。

3　米国における中国共産党員留学生のセキュリティ管理

これまで述べたように、中国共産党員は一定の機微な研究部署への留学は、ビザ審査の段階で排除されていると考えられるが、中国共産党員であることを隠して留学して来る者もいるであろう。また、留学を認められた中国共産党員も、留学後に機微な研究部署にアクセスする可能性は考えられる。

このようなリスクに対して、米国政府はどのように対処しているのであろうか。対処の主たる責任部署は、米国のセキュリティ・サービスたる FBI 国家安全保障部門である。FBI 国家安全保障部門がどう対応しているか、従来の検挙事例などから得られる情報から、推定してみよう。

先ず、前提として、米国政府においては治安関係諸機関やインテリジェンス諸機関は情報共有や相互協力に積極的であり、FBI が中国人のビザ申請に関する調査を行う際には行政各部門が保有する各種情報に対しては任務遂行上必要があれば自由にアクセスできると考えられる。

そこで、仮に筆者が FBI の担当官であった場合にどう調査するかを例として考えてみる。先ず、機微な部門で研究する中国人留学生の一覧表を国務省領事局から入手する。この一覧表には当然、電話番号、E メールアドレス、使用するソーシャルメディアのアカウント情報が付随している。その中から、相対的にリスクが高いと判断される者のソーシャルメディアでの情報を分析（メタデータ分析と内容分析）してみる。そこで不審点を感じれば、対外諜報監視法に基づく行政調査へ移行する。つまり、米国 IT 企業のデータセンター内にあるウェブメール、ネット検索履歴、ネット地図検索履歴やソーシャルメディアの資料などを分析する。これらの調査によってその人物の行動や活動、人物像は把握可能である。更に必要と認めれば、同人を標的として継続的に通信傍受も行うこととなる[17]。メールで暗号通信を多

---

[15] Lara Jakes and Marc Tracy, "U.S. Limits Chinese Staff at News Agencies Controlled by Beijing," *The New York Times*, 2 March 2020, accessed 3 March 2024.

[16] レフチェンコ『レフチェンコ議会証言』（1982 年）『KGB の見た日本』（1984 年）他

[17] 中国のエージェントとして情報収集を行う者は、中国担当者との連絡や情報報告は、インターネット通信や一時帰国時に行われることが通常である。そこで、米国 FBI の検挙事例を見ると、容疑性の高まった留学生や研究者については、①インターネット通信などウェブ活動を監視する。②一時帰国のための飛行機搭乗時に、預入手荷物の秘密捜索をする、持込手荷物の開披検査をするなどによって、容疑性を解明している例が多い。これらの情報収集は、通常、国家安全保障調査として行われ

用していたり、TOR などの匿名化通信などを使用していれば、要注意人物である。

このように、FBI 国家安全保障部門は、調査するために十分な手段を持っている。

例えば、2020 年にはボストン大学への留学生が、中国の国防科学技術大学のために情報収集活動をしたため、起訴された。罪名は、合衆国法典 18 篇 1001 条（a）（2）（虚偽供述）、同 951 条（外国代理人登録義務違反）、同 1546 条（a）（ビザの偽造等）で、犯罪行為としては、ビザ取得時に軍歴を隠し虚偽の申告をしたことが含まれている[18]。また、本行政調査・司法捜査では、通信傍受が行われたことは、同人の起訴資料から明白である。

このように、FBI 国家安全保障部門には、調査・捜査・検挙能力はあるが、課題は必要なマンパワーである。FBI 国家安全保障部門の人員は限られており、取り組むべき課題も多いので、このような調査に十分な人員を投入できるとは思えない。

ではどう対処するか。やはり、AI の活用であろう。上記のような分析作業を AI を活用して自動化し、容疑性の高い留学生を絞り込むことが出来れば[19]、その後は FBI 担当官が個別に調査し摘発することが出来るのであるから、留学生や研究者のセキュリティ管理は格段に容易となるであろう。

4　我が国における中国共産党員の入国管理

以上、米国の現状を見てきたが、さて、我が国の現状ではどうであろうか。外国人留学生・研究者の在留資格は「留学」の他にも「研究」「教授」「高度専門職 1 号イ」などがあるが、基本的な制度枠組は同一であるので、本論考では「留学」を代表例として記述対象とする。

（1）査証申請書

在中国の日本大使館のウェブサイトによれば、日本留学に必要な査証は、就労・長期滞在査証である。この申請手続で提出が求められる「査証申請書」[20]を見ると、質問事項には、有罪判決歴、国外退去処分歴、売春従事歴、人身売買従事歴など、一般治安に影響する項目についての質問はある。しかし、ここには共産党員であるかどうかを問う項目はない。それどころか、国家安全保障に関する質問事項が全く存在しない。

国家安全保障に関する質問項目とは、米国に対するビザ申請では定型的な質問項目として次のような質問項目がある[21]。これらに該当する場合は、申請却下となる。即ち、

○　あなたは、スパイ行為、諜報行為、妨害・破壊行為、輸出管理規制違反行為、その他の違法行為に関わる積りですか。

ており、秘密通信傍受や秘密捜索は、対外諜報監視法（FISA）の規定に基づくなどして、司法捜査よりも緩い要件で実施されている。

[18] 茂田忠良「インテリジェンスこぼれ話４」前掲（脚注 8）

[19] 2023 年 10 月以来のイスラエル・ガザ戦争において、イスラエル軍は、シギント・システムを使用してガザ地区から膨大な通信データを収集しているが、AI を使用したデータ分析によって、自動的にハマスやイスラミック・ジハードの戦闘員容疑者を抽出している。

[20] 在中国日本国大使館ウェブサイト、ビザ申請関連情報「就労・長期滞在」、2024 年 3 月 8 日最終閲覧、https://www.cn.emb-japan.go.jp/itpr_ja/visa_shikaku.html

[21] US Department of State, Bureau of Consular Affairs, *Online Nonimmigrant Visa Application DS-160 EXEMPER,* undated, accessed 3 March 2024.

○　あなたは、テロ活動に関わる積りですか。今までテロ活動に関わったことがありますか。
○　あなたは、テロリストやテロ組織に対して資金援助その他の支援を行ったことが、今までにありますか。或いは今後行う積りですか。
○　あなたは、テロリストの一員又は代表者ですか。
○　あなたの配偶者又は子が、過去 5 年間に、テロリストやテロ組織に対する資金援助その他の支援を含む、テロ活動に関与したことがありますか。

これらの質問は国家安全保障（National Security）に関連する項目であり、軍事活動以外の国家安全保障上の脅威である主要４項目が包含されている。即ち、Espionage（スパイ行為、諜報行為）、Subversion（破壊活動を含む国家転覆活動）、Terrorism（テロ）そして Proliferation（大量破壊兵器拡散）である。

これらの４項目は、第二次世界大戦後の民主主義国家において、国家安全保障に対する主要脅威であると認識され、これらへの対処がセキュリティ・サービス[22]の主要任務とされてきたのである。即ち、その基本的任務は、C-E、C-S、C-T、C-P などと呼称されているが、それぞれ Counter-Espionage（スパイ対策、諜報対策）、Counter-Subversion（破壊活動を含む国家転覆活動対策）、Counter-Terrorism（テロ対策）そして Counter-Proliferation（大量破壊兵器拡散対策）を意味している[23]。

実際の米国へのビザ申請において、申請者が、これらの質問項目に該当する場合、正直に回答することはそれほど期待できないであろう。しかし、虚偽申告は、合衆国法典 18 篇 1546 条（a）（ビザの偽造等）に違反する犯罪となり可罰的であり、且つ、質問項目の存在自体が、国家安全保障に脅威となる虞のある者を排除しようという国家の意思を示している。

これに対して、我が国の査証申請書には、国家安全保障上の脅威となる者の入国を制限しようという意思の表明自体さえ存在しない。

（２）在留資格認定証明書[24]

次に、「在留資格認定証明書」を見てみよう。日本留学の際は、査証申請書に添付する必要があるからである。「在留資格認定証明書」とは、日本で行おうとする活動（留学）に対

---

[22] 国家の安全保障のために主として国内で活動するインテリジェンス機関。主な組織は、英国 Security Service、仏国 DGSI、独国 BfV、米国 FBI 国家安全保障部門など。

[23] これらの情報は、公開情報では必ずしも明解に示されていないが、諸機関との渉外活動を通じて得た筆者個人の体験に基づいている。

[24] 高宅茂著『入管法解説』（有斐閣、2020 年）121 - 125 頁によれば、中長期在留者として新規入国をする者については、長時間にわたる複雑な審査が必要である。しかし、海空港での上陸審査においてこれを行うことは事実上困難であるので、従来から査証制度を利用して査証発給時に実質的な事前審査が行われてきた。一方、在外公館の審査能力には限界があるので、外務本省経伺・法務省協議を経て査証を発給していた。ところが、法務省協議にも時間を要するので、法務省協議を簡略化して、査証を申請する外国人が、直接、地方出入国在留管理局から在留資格認定証明書の交付を受け、在外公館はこの提出を受けて査証を発給する手続が取られている。この在留資格認定証明書は代理申請が可能である。

在留資格認定証明書は、出入国管理及び難民認定法 7 条 1 項 2 号の要件（在留資格）の充足を証明するものではあるが、同法 7 条 1 項 4 号の要件（5 条 1 項の上陸拒否事由のないこと）とは直接関係しない。つまり、現在の手続では、法律 5 条 1 項の上陸拒否事由の審査は弱体である。

なお、高宅茂氏は元法務省入国管理局長（2010 年 12 月～2013 年 3 月）であり、本書は本法についての有権解釈に近いものと考えられる。

応する在留資格に該当することを証明する文書であり、出入国在留管理庁が交付する。

「在留資格認定証明書」の交付申請[25]は本人が行うこともあるが、通常は留学受入れ先の大学が行政書士（法制度上は、当該行政書士は申請者本人の申請取次者の位置付け）を通じて行っており、要するに文書審査である。そこでその交付申請書を見ると、ここでも査証申請書と同様であり、犯罪を理由とする処分歴と強制退去や出国命令の処分歴を問う質問項目しか存在しない。国家安全保障への脅威の観点からの質問項目は存在しないのである。

（３）我が国の査証発給のまとめ

以上をまとめると、留学目的の査証申請においては、先ず第１に、申請書類には、中国共産党員であるか否かを問う質問項目は存在せず、更に、国家安全保障上の脅威除去の観点からの質問項目も存在しない。第２に、申請は基本的に文書審査であり、米国のような領事担当者によるインタビューは予定されていない。第３に、ソーシャルメディアのアカウントとハンドル名の申告も義務付けられていない（因みに、査証申請書にも在留資格認定証明書交付申請書にもＥメールの記載項目自体が存在しない）。

即ち、我が国の査証発給手続においては、国家安全保障に脅威となる者を排除するための米国における３要素、即ち①査証申請時の申請書の記載内容、②領事担当者によるインタビュー、そして、③ソーシャルメディアの活動調査による裏付け調査、の何れも存在しないのである。

（４）出入国管理及び難民認定法上の国家安全保障に関連する規定

以上から、現実の査証発給手続においては、国家安全保障上の脅威に対処するという制度的枠組が欠落していることが明らかになったが、法制度上はどうであろうか。そもそも法制度上、国家安全保障の視点が存在しないのであろうか。

これに関しては、出入国管理・難民認定法第５条（上陸の拒否）があり、上陸拒否の事由が列挙されているが、国家安全保障上の脅威に関する事由には、同条１項11号、12号、13号、14号[26]がある。

11号は、「日本国憲法又はその下に成立した政府を暴力で破壊することを企て、若しくは主張し、又はこれを企て若しくは主張する政党その他の団体を結成し、若しくはこれに加入している者」。要するに国家転覆活動を行う団体の構成員を指している。12号、13号は11号の政党団体のフロント組織或いは類似団体（公務員に対する暴行・殺傷を勧奨する団体、公共施設の損傷・破壊を勧奨する団体など）の構成員や支援活動を行う者を規定しており、結局、C-S、国家転覆活動の脅威の排除を規定している。

また、14号は、「法務大臣において日本国の利益又は公安を害する行為を行うおそれがあ

---

[25] 出入国在留管理庁ウェブサイト、「在留資格認定証明書申請」、2024年３月８日最終閲覧。https://www.moj.go.jp/isa/applications/procedures/16-1.html
出入国管理及び難民認定法施行規則第６条の２の規定によれば、本人が地方入国管理局に出頭して申請するのが原則であるが、代理人を通した申請を認めている。代理人申請では、本人面接を実質的に行うこともできない。

[26] 高宅茂、前掲書105頁によれば、これら４つの項目は「利益公安関係の上陸拒否事由」と呼ばれている。

ると認めるに足りる相当の理由がある者」と規定しているので、これには、欧米民主主義国家が国家安全保障上の脅威と定義する、Espionage（スパイ行為、諜報行為）、Subversion（破壊活動を含む国家転覆活動）、Terrorism（テロ）そして Proliferation（大量破壊兵器拡散）の 4 つが含まれるのであるから、国家安全保障上の脅威となる者の入国を排除する根拠規定は存在しているのである。

つまり、法制度上は、国家安全保障上の脅威を理由に査証発給拒否をすることは可能であるが、それを実行するための具体的な手続的枠組が存在しないのである。即ち、査証発給手続を見る限り、「査証申請書」の質問事項には、有罪判決歴、売春従事歴など一般治安に係わる質問項目はあるが、国家安全保障上の脅威に係わる質問項目は存在しない。また、上陸審査では、これら拒否事由の有無を含めて審査していることになっているものの、そのための面接調査や質問などの実質的な手続は定められていないのである[27]。

出入国管理・難民認定法についての代表的解説書『入管法解説』[28]を見ても、これら国家安全保障上の脅威に対する「上陸審査」における具体的取組の記載はない。

5　我が国における中国共産党員留学生のセキュリティ管理

前章で見たところから、先ず、我が国では入国審査段階で、共産党員かどうかを把握する枠組が存在しないことが明らかとなった。それは、共産党員であるかどうかが申告事項になっていないだけでなく、共産党員かどうかを調査するために必要な手立がないからである。米国とは異なり、査証発給審査のための領事担当者によるインタビューもなければ、ソーシャルメディアのアカウント情報など本人の脅威性を掘り下げるための基礎情報の収集もしていないのである。

このようにして、中国共産党員を含めて中国人は、査証発給手続において国家安全保障上の脅威という視点からのチェックを実質的に受けずに、入国してくると見て間違いないであろう。

---

[27] 過去の国会答弁（1962 年 3 月 15 日衆議院内閣委員会における高瀬侍郎入国管理局長答弁）を見る限り、国交樹立国に対しては、国家安全保障上の観点からの入国審査の手順は整備されていなかったようであり、現在でも、国家安全保障上の脅威を排除する実質的な枠組は、殆ど整備されていないとみられる。https://kokkai.ndl.go.jp/simple/detail?minId=104004889X01719620315

出入国管理・難民認定法 6 条によれば、入国の際は「上陸審査」をすることとなっており、同法 7 条によれば、①査証の有効性、②在留資格要件、③欠格事由の非該当性などの要件の審査することとなっている。在留資格要件については、本文でも記述のように「在留資格認定証明書」は文書審査で入手可能である。そして、本文でも述べた法５条の１１号から１４号までの（国家安全保障の観点からの）欠格事項の有無については、その判断のための手続、本人面接或いは口頭審理などについて、政令省令の何れにも規定がない。法 10 条は口頭審理を規定しているが、これは上陸を拒否する場合の手続であって、そもそも欠格事項に該当するか否かを調査するための面接調査の制度は存在しないようである。

他方、戦前の我が国の外国人の入国在留管理は、内務省の所管であり、昭和 14 年内務省令第 6 号「外国人ノ入国、滞在及退去ニ関スル件」が内務大臣と外務大臣連名で発出されている。同省令 5 条は、「警察官吏ノ査閲ヲ経タル後ニ非ザレバ入国又は通過スルコトヲ得ズ。前項ノ査閲ニ際シ外国人ハ（中略）必要ナル事項ノ質問ニ対シ真実ナル陳述ヲ為スベシ。」と定めており、その運用実態は良く分からないものの、入国に際して警察官吏（特別高等警察）による面接を規定している。興味深いものがある。https://dl.ndl.go.jp/pid/2960137/1/2

[28] 高宅茂、前掲書。

それでは、警備警察部門は、中国人留学生による機微技術の流出阻止という課題にどのような対策を採っていくのであろうか。具体的な手法については情報開示されていないので、推測してみる。先ず、警察の担当者とすれば、基礎資料として、機微技術を扱っている部署で研究している中国人留学生の一覧表を入手したいところであろうが、それは極めて困難であろう。大学や研究所が自発的に一覧表を警察に提供するとは、我が国の大学・研究所の現状からは考え難い。また、出入国在留管理庁との関係では、捜査照会書などによる個別の照会に対する回答は別として、我が国の「個人情報保護」の風潮から判断して全国に及ぶ一覧表の提供は望み薄であろう。

また仮に、機微技術を取り扱う部署で研究する中国人留学生の全国一覧表を手にしたところで、その先の脅威度を評価するための有効な情報収集手段を我が国警察は持っていない。第 3 章で述べた FBI 国家安全保障部門による基本的な情報収集手法、その中心は通信傍受であるが、その権限を我が国警備警察は保持していないからである。従って、尾行張込、協力者からの情報収集など任意の手段によって調査するしか方法がないが、全国的に行うには膨大なマンパワーが必要で、容疑性も明確でない留学生の情報収集をすることは、基本的に現在の警察の現場にはできないであろう。

たまたま、他の個別の事件捜査などから浮上した不審者、或いは協力者からの通報などを端緒に捜査を進めることはあったとしても、個別具体的な情報もなしに、中国人留学生に関して国家安全保障上の脅威情報を収集するような調査活動は、現在の警備警察では困難であろう。

つまり、我が国の中国人留学生の国家安全保障上の脅威の調査、セキュリティ管理は極めて弱体であると言わざるを得ない。

６　外国為替及び外国貿易法 25 条（経産省所管部分）による規制

さて、出入国在留管理以外で、中国共産党員の留学生受入れに関わる規制がある。それは、外国為替及び外国貿易法 25 条と外国為替令 17 条に基づく規制である。これによって、共産党員であるか否かなど、国家安全保障上の脅威の把握が可能か、検討してみよう。

同規定は、特定技術（機微技術）の輸出を規制（経産大臣の許可事項）するものであるが、2021 年に「みなし輸出管理の明確化」に関する通達[29]が発出されて、特定類型の国内居住者（留学生など）への機微技術の提供も「輸出」と見做され、規制対象となった。

これに伴い、経済産業省からの行政指導[30]に基づき、大学・研究機関の自主管理の一環とし

---

[29] 経済産業省貿易経済協力局長通達「『外国為替及び外国貿易法第２５条第１項及び外国為替令第１７条第２項の規定に基づき許可を要する技術を提供する取引又は行為について』」等の一部改正（2021 年 11 月 18 日）。
https://www.meti.go.jp/policy/anpo/law_document/tutatu/211118tsutatsu2.pdf
　経済産業省貿易管理部、「経産省からのご協力のお願い　『みなし輸出』管理の明確化について」2021 年 11 月。https://www.meti.go.jp/policy/anpo/law_document/minashi/jp_daigaku.pdf

[30] 経済産業省貿易管理部、「安全保障貿易に関する機微技術管理ガイダンス第 4 版」2022 年 2 月。71 頁、110-113 頁、
https://www.meti.go.jp/policy/anpo/law_document/tutatu/t07sonota/t07sonota_jishukanri03.pdf

て、機微技術を担当する組織が留学生の受入に当たっては、「外国人受入れの事前確認シート」で特定類型に該当する人物かどうかなど安全保障上の懸念の有無を確認し、必要に応じて経産省と連携を行うこととされた。

そこで、「外国人受入れの事前確認シート」の内容であるが、シートには留学生の出身組織と特定類型該当性を記述することとされている。先ず、出身組織については、受入予定者（留学生）がこれまで所属した組織名全てを記入するとしているが、記入すべき組織の定義がなく、且つ、記入欄も狭く、共産党員であることを記入するべきかどうか不明である。

次に、特定類型とは、受入予定者（留学生）が外国勢力の支配下にあるかどうかを検討する 3 類型である。類型①は「契約に基づき、外国政府等・外国法人等の支配下にある者」である。但し、ここでいう「支配」とは労働基準法上の労働者性が基本であって、「外国政府等」への忠誠義務があっても、「時間的・場所的に拘束されるなど雇用者と被用者の関係に類する場合」でなければ、該当しないとされている[31]。従って、この解釈では単なる共産党員は含まれない。また、類型②は「経済的利益に基づき、外国政府等の実質的な支配下にある者」であり、「多額の金銭その他の重大な利益（年間所得の 25%以上相当）」を得ることが要件である[32]。これも、通常の共産党員は含まれないであろう。類型③は、「その他、国内において外国政府等の指示の下で行動する者」であるが、「外国の国家情報活動について、法律上義務が課されているだけでは該当せず、外国政府等から本邦における行動に関し指示又は依頼を受けている場合」であるとする[33]。これは中国の国家情報法によって、一般中国国民は国家情報活動への協力義務を課されているが、それだけでは本類型には該当せず、具体的な情報活動の指示依頼が必要であるという趣旨である。この論理によれば、中国共産党員であっても、具体的な情報活動の指示依頼を受けていなければ、これに該当しないということになる[34]。

このように、経産省の作成した「外国人受入れの事前確認シート」では、そもそも「出身組織」記載欄において中国共産党員であることが記載事項であるかどうかが不明瞭である上、「特定類型性」では、単に中国共産党員というだけでは該当しないと解釈できる。更に、「外国人受入れの事前確認シート」の作成者は、留学生本人ではなく、受入元の組織・担当者であり、実効性は担保されない。

また大学において、指導教授が、みなし輸出規制に違反していないことを担保するため、当該留学生から、「外国為替及び外国貿易法第 25 条第 1 項及び第 2 項の遵守のための特定類型該当性に関する申告書」を徴収して、当該留学生から「特定類型」の該当性有無についての申告を求めることとされているが、ウェブ上で容易に調査できる大学・研究機関の様式 9 個を調べてみると[35]、7 つ、つまり大多数、そして大学の全てで特定類型①②の該当性のみが

---

31 前掲。34-35 頁。
32 前掲。35 頁。
33 前掲。36 頁。
34 つまり、共産党員が「特定類型」に当たる場合とは、当該党員が最初から諜報機関員であって諜報機関員として報酬を受け、又は諜報機関の指揮命令下に諜報活動に従事する目的で、留学生をカバーとして来日する場合位しか、該当しないであろう。
35 ウェブ上で容易に閲覧できるものを調査した結果、特定類型①②該当性のみを問う組織 7 つ：明治大学、埼玉大学、弘前大学（研究・イノベーション機構）、東京都立産業技術大学院大学、総合研究大学院大学、土木研究所、防災科学技術研究所、特定類型③該当性も問う組織 2 つ：産業技術総合研究所、光イノベーションセンター。

記述対象となっている。特定類型③の記載項目がなければ、単なる中国共産党員がスパイ活動の密命を受けただけの場合は、そもそも記載する必要がないことになる。

このように、外国為替及び外国貿易法 25 条（経産省所管部分）による規制も、中国共産党員かどうかを把握するための質問とはなっていない。更に、そもそも「外国政府等の指示の下で行動する者」であるか否かを把握する責任は、留学生の指導教授等の教育する側にあって、留学生本人に申告義務、虚偽申告に対する罰則も何も存在しないのである。諜報活動について知識のない教授などの研究者にこのような義務付けをしても実効性は、期待できない。

つまり、本規制は、実効性に期待を持てない規制に留まるであろう。

7　まとめ

本稿では、中国共産党員の留学生を念頭に、国家安全保障の観点から、その入国管理及び入国後の情報収集や監視の態勢（セキュリティ管理）について概観した。

米国では、ビザ申請時に、①申請書の記載内容（虚偽記載には刑事罰）、②領事担当者によるインタビュー（虚偽供述には刑事罰）、そして、③ソーシャルメディアの活動調査による裏付け調査の三者を組み合わせることによって、留学生が中国共産党員であるかどうかを含めて国家安全保障上の脅威を評価し必要に応じて排除できる態勢が構築されている。また、入国後も、FBI 国家安全保障部門による情報収集態勢が整備されており、必要に応じて、対外諜報監視法に基づく国家安全保障調査（national security investigation）が可能である。具体的には、米国 IT 企業データセンター内にあるウェブメール、ネット検索履歴、ネット地図検索履歴やソーシャルメディアのデータ分析、更に当該人物を標的とする継続的通信傍受など、十分な調査手段が与えられている。

これに対して、日本では、留学目的の査証申請においては、先ず①申請書類には、そもそも国家安全保障上の脅威除去の観点からの質問項目が存在せず、②領事担当者によるインタビューも行われず、③ソーシャルメディアのアカウントとハンドル名の申告も義務付けておらず、裏付け調査も行われていない。つまり、査証発給手続の実態を見る限り、国家安全保障上の脅威を排除する具体的な手続的枠組が存在しない。更に、入国後も、警備警察部門は、留学生に対して国家安全保障上の脅威を調査し評価するために必要な情報収集権限が付与されていない。つまり、現在の我が国の体制では、中国共産党員たる留学生による機微技術の収集など、国家安全保障上の脅威に対抗する具体的現実的な枠組が存在しないと言わざるを得ない。

以上、中国共産党員の留学生を念頭に、米日両国の入国管理及び入国後の情報収集や監視の態勢を見てきたが、要約すると、米国においては、国家安全保障上の脅威対処という視点からの枠組が存在するのに対して、我が国にはその制度的枠組が存在していないのである。このような国家安全保障のための制度の脆弱性、或いは欠落こそ、戦後我が国の行政（法）体系、或いは国家体制の特徴の顕れであろう。

元国家安全保障局長である北村滋氏が就任時に、ゼミの担当教授であった東大名誉教授の塩野宏氏に挨拶に行ったところ、「僕は行政法を長くやっているけれども、安全保障のことは

よく分からないのだよ。」と言われたという[36]。行政法の大家である東大名誉教授のこの発言は、正に我が国の行政（法）体系において、国家安全保障上の脅威対処という視点が大きく欠落している現状を裏書きしている。　　（2024 年 5 月記）

[36] 北村滋「経済安全保障の現段階」『警察政策』第 26 巻（警察政策学会、2024 年 3 月）、16 頁。

ガザ戦争～シギント、AI、そして多数の民間人死傷者

茂田忠良

＜目次＞

1　ガザ戦争における死傷者数…… 15
2　イスラエル・シギント組織 8200 部隊のガザ地区監視能力 …… 18
3　イスラエル軍の戦い方…… 21
4　イスラエル軍の標的類型と「高価値標的」 …… 22
5　「戦闘員の自宅」を標的…… 23
6　まとめ …… 29

はじめに

2023 年 10 月 7 日イスラエル・ガザ戦争が始まった。ガザ地区のハマスやイスラミック・ジハードなどの戦闘員（以下、ガザ戦闘員）がイスラエル領内の軍事施設とキブツなどの民間施設を奇襲して、イスラエル兵士と共に多くの民間人を殺戮し又誘拐したことによって、戦争は始まった。その後、イスラエル軍の攻撃によって、ガザ地区の民間人に多大な死傷者が生じている。本稿では、ガザ地区の民間人に多大な死傷者が生じている要因、その背景にあるイスラエル軍のインテリジェンス能力と攻撃方法について、国連ほかの各種公表資料、イスラエル国内の調査報道、その他報道に基づいて記述する。

1　ガザ戦争における死傷者数

イスラエル･ガザ戦争の発端となった大規模越境テロ攻撃では､イスラエル側に､死者 1100 人以上（内、兵士、シンベト、警察官合計 400 人弱。他は民間人)、負傷者 3000 人以上、誘拐 240 人以上の被害を出した。他方、ガザ戦闘員の死者は 1000 人以上と推定されている。この当初の大規模越境テロに伴う死傷者を除くと、開戦後半年間の双方の死傷者数の大要は次の通りである。

（1）ガザ地区パレスチナ人の死傷者

ガザ保健省[1]によれば、開戦からほぼ 6 ヵ月経った 2024 年 4 月 8 日時点で、ガザ地区のパレスチナ人の死者は約 3 万 3207 人、負傷者 7 万 5933 人である[2]。ガザ保健省は、戦闘員

[1] ガザ保健省は、ハマスの支配下にあるが、2023 年 10 月以降、死者の一覧表を開示しており、その数値は概ね正確であると評価されている。

[2] OCHA, *Hostilities in the Gaza Strip and Israel / Flash Update # 151,* 8 April 2024.（以下、OCHA #151(2024.4.8)）

と一般民間人を区別していないので、この死者には戦闘員も含まれるが、死者の内、非戦闘員であることが明白な女性と子供の割合が約 7 割と非常に高い比率を占めている[3]。この他に、行方不明者が 1 月下旬時点で 1 万人以上いるが、その殆どは破壊された建物の瓦礫の下で既に死亡していると推定されている[4]。

死者数が 1 万人に達したのが開戦から 30 日目（2023 年 10 月 6 日）[5]、2 万人に達したのが 76 日目（12 月 22 日）[6]、3 万人に達したのが 145 日目（2024 年 2 月 29 日）[7]であり、開戦当初の 1～2 ヵ月間に死者が極めて多いという特徴がある。

なお、OCHA（国連人道問題調整事務所）資料[8]によれば、開戦約 1 ヵ月後の 11 月 10 日現在、ガザ地区の死者数の内、同一家族内で複数の死者が出ているのが 1340 家族、内 825 家族で 6120 人が死亡している。これは、戦闘員が自宅にいる所を家族ごと殺害されたことを示唆している。こうして殺害された家族では、戦闘員以外の殆どは女子供であるので、結果的に死者に占める女子供の死者の割合が高くなるのである。

（２）ガザ戦闘員の死傷者数

開戦前のガザ地区のハマスなどの戦闘員数は、イスラエル推定で 30000 人以上、米国推定で 25000 から 30000 人である[9]。

イスラエル軍によるガザ地区攻撃による戦闘員の死傷者数を見る。ハマスによれば、2024 年 2 月中旬時点で、死者数は約 6000 人であった[10]。これに対して、米国の推定では、2024 年 1 月中旬時点で、死者は 5000 から 9000 人、負傷者は 1 万 500 から 1 万 1700 人としている[11]。イスラエル推定では、同じ 1 月中旬時点で、死者 9000 人、負傷者 1 万 6000 人で、負傷者の内半数は戦闘復帰できない重傷と推定している[12]・[13]。2 月末の時点でのイスラエルによる死者数推定は、1 万人以上である[14]。

---

[3] OCHA#151(2024.4.8). 本資料に拠れば、女性子供の死者は合計 2 万 4060 人と死者全体の 72%を占めている。; Archie Bland, "The numbers that reveal the extent of the destruction in Gaza," *The Guardian,* 8 January 2024； "More than 25,000 women and children killed in Gaza: US defense secretary," *Al Jazeera,* 1 March 2024.

[4] Aya Batrawy, "Gaza's death toll now exceeds 30,000. Here's why it's an incomplete count," *National Public Radio*, 29 February 2024. 本報道によれば、ガザ保健省は 11 月末の時点では、行方不明者を 6800 人以上と推定していた。

[5] OCHA #31(2023.11.6)

[6] OCHA #76(2023.12.23)

[7] OCHA #129(2024.2.29)

[8] OCHA, *Hostilities in the Gaza Strip and Israel - reported impact / Day 45,* 20 November 2023.

[9] Nancy Youssef, Jared Malsin and Carrie Keller－Lynn, "Hamas Toll Thus Far Falls Short of Israel's War Aims, U.S. Says," *The Wall Street Journal,* 21 January 2024. (以下 WSJ①2024.1.21)

[10] Samia Nakhoul Jonathan Saul and Humeyra Pamuk, "Rafah attack: How Isarel plans to hit Hamas and scale back war," *Reuters,* 19 February 2024. (以下 Reuters①2024.2.19)

[11] WSJ①2024.1.21

[12] Ibid.

[13] Reuters①2024.2.19 によれば、イスラエル国防相ガラントは、2 月 16 日に、ガザには戦闘部隊が 24 個大隊あったが、侵攻によって内 18 個大隊を破壊したと述べた。

[14] Merlyn Thomas, Jake Horton and Benedict Garman, "Israel Gaza: Checking Isarel's claim to

これらの数字から総合的に推定すると、開戦 6 ヵ月後の 4 月上旬の時点で、ガザ戦闘員の死者数は 6000～1 万人[15]、負傷者は 1 万人以上であろう。

（３）イスラエル軍の死傷者数

イスラエル軍によれば、ガザ攻撃開始以降 4 月 8 日現在で、イスラエル軍の死者は 259 人、負傷者 1559 人である[16]。

（４）死傷数の対比

上記の死傷者数を比較すると、先ず、イスラエル側の死傷数と対比してガザ地区側の死傷者数が圧倒的に多い。ガザ地区の死者数を、行方不明者を含めて合算すると約 4 万 3000 人で、イスラエル軍 259 人と比べると、死者比率は実に 166 倍である。

次に、戦闘員の死者数をみると、ガザ戦闘員の死者を 8000 人と仮定し、イスラエル軍 259 人と対比すると死者比率は 31 倍である。

更に、ガザ地区のガザ戦闘員と民間人の比率をみると、全死者数を 4 万 3000 人と仮定して、戦闘員死者を 8000 人と仮定すると、約 5.4 倍となる。

これらの数字は大雑把なものであるが、特徴として、第 1 にイスラエル軍の損害と比べて、ガザ戦闘員の損害が極めて多いこと、第 2 にガザ戦闘員の損害と比較して、民間人の損害が大変多いことが明らかである。

（５）背景

イスラエル軍の損害が軽微でガザ戦闘員の損害が多大である主要因は、イスラエル軍のインテリジェンスと戦い方によると言えるであろう。即ち、高度なインテリジェス能力と AI を使用したデータ分析に基づいて、個々のガザ戦闘員を特定して、これを主として航空攻撃（ドローン攻撃を含む）によって殺害するという戦い方である。同時に、この戦い方が民間人に甚大な損害をもたらしている。

次に、イスラエル軍による攻撃方法について見る前に、攻撃の前提としてのイスラエルのガザ地区に対するインテリジェンス能力を見てみよう。

---

have killed 10,000 Hamas fighters," *BBC,* 1 March 2024

本文で後述するが、本戦争ではイスラエルはガザ戦闘員の損害評価を正確に行っていないので、あくまで推定値である。

[15] イスラエルは、後述するように、人的資源の制約のため、本戦争では全ての攻撃に対する詳細な損害評価は実施していない。戦闘員と認定して爆撃をし住宅を全壊させた場合には戦闘員の殺害に成功と評価しているものと考えられる。他方、戦闘員の認定をいい加減に行っている訳ではなく、正確性 90%程度は維持していると推定する。また、爆撃の際に戦闘員が既に他所に移動してしまう場合も想定できるが、比率は少ないと見込まれる。そこで筆者は、2024 年 4 月上旬時点のガザ戦闘員の実際の死者は、8000 人以上、9000 人前後ではないかと推定している。

[16] OCHA oPt 2024.4.8.

２　イスラエル・シギント組織 8200 部隊のガザ地区監視能力

イスラエル軍のガザ地区に対するインテリジェンス能力は、当然、ヒューミント、シギント、イミントなど多様な諜報源からなっているが、各種報道から判断して、シギントが中心的な役割を果たしていると見られる。

イスラエルのガザ地区に対するシギント能力は当然秘密事項であるので、公刊資料からは知る由もないが、各種報道を基に考察すると、結論を言えば、シギント組織である 8200 部隊が、ガザ地区における通話やインターネット通信のほぼ全てに対する監視能力を持っており、これが本戦争におけるインテリジェスの中核をなしていると推定できる。以下、この推定の根拠を示す。

（１）ガザ地区の通信網と通信環境

オスロ合意（1993 年、1995 年）に基づいて、イスラエルは西岸ガザの通信インフラに対する広汎な監督権を有している。西岸ガザ地区の主要な通信インフラ企業は、パレスチナ通信会社（パルテル）、ジャワル、オーレドーなどがあるが、これら企業はイスラエル政府通信省の監督下で厳しく統制されている。また、ガザ地区と外部を結ぶ通信回線は、全てイスラエル経由で構築されていて、海底ケーブルやエジプトとの陸路の回線は存在しない。更に、イスラエルとの通信接続点は非公表で秘匿されている[17]・[18]。当然、イスラエル側に都合の良いように構築されているであろう。

従って、衛星通信携帯電話などごく少数の例外を除いて、ガザ地区と外部を結ぶ通信は、全てイスラエル領内を通過することとなる。イスラエル当局はこの通過通信に対する監視システムを構築していると考えて間違いない。また、イスラエル当局は、彼らが支配する通信接続点からガザ地区内の通信網に自由に侵入できる。

次に、ガザ地区の通信状況を見ると、イスラエル当局の規制により、旧式の 2G のサービスしか提供されておらず、通信速度は遅く、高度なデータ暗号化ができず解読し易いとされている。また、端末機器の所在位置の特定も容易であるとされる[19]。

ガザ地区当局の報告[20]によれば、通信手段の中心は、スマートフォンなどの携帯電話であり、インターネットとの接続も携帯電話が中心である。また、フェイスブック、X、インスタグラム、TikTok、リンクトインなどのソーシャルメディアや、WhatsApp、iMessage などのメッセージアプリが多く使われている。

（２）イスラエル当局の通信監視能力の推定

---

[17] Ami Roikes Dombe, “Analysis | Gaza’s Internet Dependency on Israel,” *ISRAELDEFENSE,* 31 October 2023.

[18] Mohamad el Chamaa and Julia Ledur, “Why Caza keeps losing communications,” *The Washington Post,* 18 January 2024.

[19] Zeinab Ismail, “Internet in Gaza: Limited even before war,” *SMEX*, 1 November 2023.

[20] Gaza Strip, oPt, *Communications and Information Dynamics in Gaza*, 18 December 2023, https://www.etcluster.org/document/communications-information-dynamics-gaza-december-2023

上記のガザ地区の通信環境を前提として、イスラエル当局のガザ地区通信の監視能力を推定する。

先ず第1に、ガザ地区外との通信情報は全て、イスラエル領内の通信接続点で捕捉され、データ収集がなされていると見られる。即ち、外部のデータセンターと通信する必要のある通信、①フェイスブック、X、インスタグラム他のソーシャルメディアや、WhatsApp などのメッセージアプリによる通信、②グーグル検索やグーグルマップ検索などの各種検索、③G メールやヤフーメールなどのウェブメール通信、④Amazon などによるウェブによる物品購入やビデオ視聴など、インターネット利用の殆どはガザ地区外との通信であって、イスラエル当局によってデータ収集されていると推定できる。

また、携帯電話の使用者は各種アプリをダウンロードしているが、これらアプリの中には位置情報を収集しているものが多く、その場合、位置情報データは通信接続点で捕捉されるであろう。

第2に、ガザ地区住民は、域外に居住する親戚や出稼ぎの親族を多数持っており、彼らとの通話やインターネット通信は、ウェブメールを利用しない通信も通信接続点で捕捉できる。

第3に、ガザ地区内の携帯電話利用による通信回線使用料は、ガザ地区外のサーバーで管理されており、従って、使用料に関するデータもイスラエル領内を通過しているのであるから、これも当然に捕捉可能である。

第4に、スマートフォンなど区域内の携帯電話は電源 ON となっていれば、近くの通信塔に通信接続可能であることがシステム上登録されるが、これによっても位置情報の捕捉が可能である。

第5に、ガザ地区とイスラエル側の通信接続点を多数設置して、それらの通信接続点の間をイスラエル領内で高速回線で結べば、ガザ地区内は旧式の2Gで通信速度が遅いので、純然たるガザ地区内の通信であっても、これらの高速回線を経由する可能性が高くなる。従って、これを監視することも容易となるであろう[21]。これは、仮に筆者がイスラエルのシギント責任者であった場合、実施する方策である。

最後第6に、イスラエル当局は、ガザ地区内のスマートフォンに対して、容易にハッキングできる能力を持っている。イスラエル企業 NSO グループが「ペガサス」という極めて高性能なハッキングツールを世界中に販売していたのは公知の事実であるが、この NSO グループの技術者の多くはシギント組織 8200 部隊の OB であり、イスラエル 8200 部隊は当然「ペガサス」或はその同等品は使用できるとみて間違いない。即ち、ガザ地区内のスマートフォンの殆ど全ては、イスラエル当局にとってハッキングが可能である。

---

[21] 2013 年のスノーデン漏洩情報によれば、米国 NSA は、情報通信企業の協力による「ブルーゼーファ」計画によって、ブラジルとコロンビアの国内通信を傍受していたが、後にこれが「シルバーゼーファ」計画に移行した。後者は、米国内においてブラジル、コロンビアの国内通信を傍受するものであり、ブラジル、コロンビアの国内通信を高速回線によって米国を迂回させることによって、米国内での傍受を可能にしたものと推定できる。拙著『米国国家安全保障庁の実態研究』（警察政策学会資料 82 号、2015 年 9 月）57 頁参照。

（３）監視能力の具体例

以上から、シギント組織 8200 部隊は、ガザ地区における通話やインターネット通信のほぼ全てに対する監視能力を持っていると推定できる。これを裏書きする個別具体的な報道があるので、見てみよう。

○　2023 年 10 月のニューヨークタイムズ紙の報道[22]によれば、イスラエル当局は、ガザ北部地区（人口 110 万）に対する避難勧告によって北部地区の住民が減少していくのを、住民の携帯電話の位置情報からリアルタイムで把握していた。つまり、全携帯電話の現在位置を把握できる能力を持っていることが分かる。また、同報道によれば、避難指示に当たっていたイスラエル軍指揮官は、ガザの地域指導者、病院の医師、学校管理者など数百名の電話番号を手元に置いて、何時でも連絡を取れる態勢を採っていた。つまり、携帯電話の番号と使用者を把握する能力があることも示している。

○　2024 年 4 月のイスラエル国内の調査報道[23]によれば、ガザの社会慣習で女性は戦闘員にはならないので、イスラエル軍分析官は攻撃対象人物が女性ではないことを標的人物の通話記録を聞いて確かめている。これから、任意の携帯電話の通話傍受能力があること、そして過去の通話データも保管されていて、分析官が容易に通話内容を聞き得ることが分かる。

○　2021 年における 8200 部隊司令官の匿名出版によれば、8200 部隊は WhatsApp のグループ構成員、携帯電話の購入状態、携帯電話所有者の住所などを把握できている。また、同書によれば、携帯電話のデータから、写真や画像、通話相手、ソーシャルメディアの交友関係などのデータも収集可能である[24]。

○　2022 年 8 月のイスラエル国内の調査報道[25]によれば、インテリジェス部隊の元勤務者は、イスラエル軍は、ガザ地区住民の個人情報を完全に把握できるとしている。即ち「プライバシーなどというものは存在しない。彼らが何を考えているか。（携帯電話で）どんな写真を撮ったか。恋人がいるか。性的指向はどうか。全てが完全に露出している。任意のどんな人物についても、情報を収集できる。」と述べている。

これらの報道事例は、正にイスラエルの強大なシギント能力、ガザ地区における通話やインターネット通信のほぼ全てを監視する能力の存在を示唆している。但し、膨大なデータを収集できることと、それらのデータを分析活用していることは、同義ではない。即ち、データの分析活用には人的資源が必要であり、それが十分でない場合には、AI の活用など分析支援システムが必要となる。AI の活用については、後ほど第 5 章で述べる。

（４）10 月 7 日攻撃でのシギント・インフラの破壊失敗

---

[22] Patrick Kingsley and Ronnen Bergman, “Tracking Cellphone Data by Neighborhood, Israel Gauges Gaza Evacuation,” *The New York Times,* updated 18 October 2023.

[23] Yuval Abraham, “‘Lavender’ : The AI machine directing Israel’s bombing spree in Gaza,” *＋972*, 3 April 2024.（以下＋972③2024.4.3）

[24] ＋972③2024.4.3

[25] Yuval Abraham, “‘We killed a little boy, but it was within the rules’,” *+972,* 11 August 2022.（以下＋972①2022.8.11）

なお、イスラエル軍のシギント能力の強大さについては、その細部は別として、ハマスも認識していたと思われる。そのため、ハマスは攻撃前には通信保全や欺瞞戦術に努めると共に、2023 年 10 月 7 日のイスラエル領内攻撃では、イスラエルのシギント中枢を攻撃したのである。即ち、ウリム・シギント基地は、イスラエルで最大且つ最重要のシギント基地で、ガザ境界から 16 キロ程内陸にあるが、ハマス戦闘員は、同基地を攻撃占拠して施設を破壊したのである。

しかしながら、その破壊が不十分であったのか、或いは、イスラエル側が十分なバックアップ・システムを準備していたためか、イスラエル軍によるその後のガザ地区攻撃では、以下に見るように、シギント能力を遺憾なく発揮しているのである。

３　イスラエル軍の戦い方

イスラエル軍は、ガザ地区において民間人死傷者が多い理由を、ハマスが民間人を盾に使って戦っていることに帰している。例えば、長大なトンネル網を故意に病院・学校の地下を通したり、ハマス戦闘員が探知を回避するため救急車を移動で使用したり、民間建物の近くに膨大な軍事拠点を築いたりいることである。確かに、その側面はあるものの、主因は、イスラエル軍の戦い方である。

そもそも、市街地で民間人の中に混在する戦闘員を攻撃することは、民間人に付随的損害を及ぼし易いものであるが、本戦争では、それが一層増大している。背景には、イスラエル軍が、ガザ地区の人口密集地帯を攻撃していることと、そして戦闘員認定の正確性と付随的損害の許容基準を緩和したことがあると見られる。即ち、イスラエル軍は、従来の攻撃手順を変更して、精密性よりも、一人でも多くのガザ戦闘員の殺害を志向している。

それを示唆するのは、2023 年 10 月 11 日のイスラエル空軍参謀長オメール・ティシュラー准将の要旨次の発言である。即ち、「イスラエル軍は、常に軍事標的を攻撃しているのであって、民間人を標的にはしていない。しかし、攻撃は『手術的』(surgical)ではない。過去の攻撃では、一時に 1 人 2 人の特定の戦闘員や幹部を攻撃したが、今回はテロリスト達の区域全体を同時に攻撃しているのである」[26]。この発言は、外科手術のように特定の目標を精密に攻撃している訳ではなく、従って付随的損害も許容していることを示していると評価できよう。

この戦い方の背景には、未曽有のテロ攻撃を受けたイスラエル国民の恐怖と怒りがある。10 月 7 日のテロ攻撃では、イスラエルの民間人 700 人以上が虐殺され、数千人が負傷した。現代はインターネット時代であるため、犠牲者の多くは、WhatsApp などのメッセージアプリを使って家族友人と連絡を取りながら、殺されていったのである。彼らの家族友人はテロを疑似体験したのである。そのため、テロ攻撃に対する恐怖と怒りには激しいものがあり、それがガザ戦争における戦い方に影響を与えていると考えられる。

---

[26] Yonah Jerry Bob, "IDF bombs whole Gaza neighborhoods to hit Hamas targets – official," *The Jerusalem Post,* 11 October 2023. （以下 JP①2023.10.11）

４　イスラエル軍の標的類型と「高価値標的」

（１）イスラエル軍の標的類型

上記のイスラエル軍のシギント能力と戦争遂行の在り方を前提に、次にAIを使用した攻撃標的の選定、付随的損害の許容度、その他具体的な攻撃方法について見て行こう。

ガザ民間人の被害は、イスラエル軍による爆撃の結果が多いのであるが、イスラエルのジャーナリスト、ユヴァル・アブラハムは現職とOBのインテリジェンス将校7人を匿名で取材して、詳細な調査報道（2023年11月）[27]をしている。

それによれば、イスラエル空軍によるガザ地区での攻撃対象は、概ね4類型に分類される。第１類型は「戦術標的」で、武装した戦闘員集団、武器庫、ロケット発射機、対戦車ミサイル発射機、発射坑、迫撃砲、指揮所、監視所など、いわゆる通常の軍事標的である。第2類型は「地下標的」で、ハマスが市街地の地下に構築したトンネルである。本類型に対する航空攻撃は、トンネル近辺の住宅の破壊をもたらし得る。第3類型は「高価値標的」（power targets）で、市街地中心部の高層ビル（事務所、住宅）そして、大学、銀行、行政組織などの公共建築物である。第４類型は「戦闘員の自宅」で、戦闘員の殺害を目的としている。

第3と第4の類型に対する攻撃が、多くの民間人の損害をもたらしていると考えられるが、先ず、第3類型の「高価値標的」に対する攻撃を見てみよう。

（２）第3類型「高価値標的」

開戦4日後（10月11日）のイスラエル軍の広報によれば、当該時点での爆撃累計2687件の内、約50%（1329件）は第3類型の「高価値標的」であった。開戦当初に破壊された「高価値標的」は、高層ビルのほか、公共建築物ではガザ・イスラム大学、パレスチナ弁護士会館、優秀学生教育計画のための国連ビル、パレスチナ通信会社やガザ行政府の建物を含んでいる。

高層ビルや公共建築物を破壊する理由付けは、それら建築物がハマスによって使用されていることである。高層ビルにハマスの事務所が入居している場合は攻撃対象としている。但し、ハマス勢力は、ガザ地区に深く広く根を張っているので、ハマスに関係する「高価値標的」は大量に存在している。その多くには軍事的な価値はない。それをハマスとの関係を理由に破壊するのは、実際は、住民への圧迫を主目的としていると見られている。

但し、従来の攻撃手順では、事前警告をして、一般住民全員を退去させた後に爆撃していた。事前警告は、ソーシャルメディアを使ったり、住民に直接電話をしたり、高層ビルの屋上に小型の警告用爆弾を投下したりして行っていた。また、全住民の退去には2、3時間はかかるが、ドローン映像で住民の退去を確認した後に、爆撃をしていたという。

イスラエル軍は、本戦争でもこのような手順を踏んでいると広報している。しかし、現実には、住民全員が避難する前に爆撃したり、更には事前警告なしに爆撃して、住民多数を殺害した事例がある。2023年10月中に事前警告なしの爆撃によって、少なくとも10階建て

---

[27] Yuval Abraham, “”A mass assassination factory’: Inside Israel’s calculated bombing of Gaza,” *+972,* 30 November 2023.　（以下＋972②2023.11.30）

前後の高層ビル 2 棟が崩壊し、それぞれ 100 人以上の住民が生き埋めになったという。このようにして、本戦争では「高価値標的」の爆撃でも、民間人に被害を及ぼしているのである。

５　「戦闘員の自宅」を標的

ガザの民間人に多大なる死傷者を出している主因は、第４類型の「戦闘員の自宅」の爆撃である。イスラエル空軍は、戦闘員の殺害を目的として、戦闘員が家族と共にいる一般住宅を爆撃しているが、その際の戦闘員認定の正確性と付随的損害の許容基準に問題があると見られる。これについては、先にも紹介したジャーナリスト、ユヴァル・アブラハムがインテリジェンス将校 6 人から匿名で取材して、詳細な調査報道（2024 年 4 月）[28]をしている。彼はパレスチナ民間人に多くの死者を出した原因は、イスラエル軍が「戦闘員の自宅」の攻撃で、特に開戦初期に AI を利用した標的決定プログラムに強く依存し、また付随的損害の許容基準を緩和したためであるとしている。本章では、その実態を主として同人の調査報道を基に見ていく。

（１）AI「ラベンダー」による標的（戦闘員）抽出

ア　「ラベンダー」の概要

「ラベンダー」とは、ガザの戦闘員容疑者のデータベースを作成する AI システムである。

「ラベンダー」が具体的に如何なるものか、イスラエル政府による公表資料はないが、それを推定できる軍将校の書籍や発言がある。

先ずイスラエルのシギント組織 8200 部隊の現司令官（仮称 Y.S.准将）が、2021 年に、攻撃標的設定における AI 利用に関する書籍[29]を出版しているが、彼はそこで、AI の活用によって標的抽出と攻撃決定の迅速化を図ることができると主張している。また、同じ 8200 部隊のデータサイエンス・AI センター責任者ヨアヴ大佐は、2023 年にテルアビブ大学の AI 週間で講義をしたが、その際、既知の戦闘員の通信特徴（通信のシグニチャー）との近似性から戦闘員容疑者を探知するシステムを開発して 2021 年 5 月から運用していると述べている。彼は同システムの成果として、ハマスのロケット砲部隊の分隊指揮官たちを特定できたことを挙げている。ヨアヴ大佐は、システム名には言及していないものの、内容から判断して、「ラベンダー」と推定できる。つまり、戦闘員容疑者を発見するのにマンパワーだけでは情報分析に膨大な手間がかかるが、それを AI 分析によって迅速化するシステムと推定できる。

上記二人が 8200 部隊所属であることから判断して、「ラベンダー」は、イスラエルのシギント組織 8200 部隊[30]が運用するシステム、即ち、シギント情報主体のシステムと推定で

---

[28] ＋972③2024.4.3

[29] Brigadier General Y.S, *The Human-Machine Team: How to Create Synergy Between Human & Artificial Intelligence That Will Revolutionize Our World*（2021） cited by ＋972③2024.4.3

[30] Bethan McKernan and Harry Davies, '"The Machine did it coldly': Israel used AI to identify

きる。

調査報道によれば、「ラベンダー」AIは、ガザ地区住民230万人に対する8200部隊の監視システムから収集した膨大なデータを基に、既知の戦闘員の通信データを訓練データとして学習し、彼らと同様の特徴（シグニチャー）を示す者を検索抽出するのである。そして、特定人がハマスやイスラミック・ジハードの戦闘員である可能性の評価値を1～100で表示するという。

上記書籍によれば、戦闘員と同じWhatsAppグループに属する者、数か月毎に携帯を交換する者、住所を頻繁に変更する者は、戦闘員可能性の評価値が高くなる。また、同書によれば、データとしては、写真や画像、通話相手、ソーシャルメディアの交友関係、戦場における情報など、様々なデータを使用して評価しているとする。

イ　「ラベンダー」の運用方法

イスラエル軍広報官は、標的選定においてAIはあくまで補助手段として使用されていると主張している。実際、従来「ラベンダー」は、分析官が標的設定をするための補助手段として位置付けられており、「ラベンダー」のデータだけを根拠に標的として認定するものではなかったという。

戦闘員容疑者として抽出する際の評価値基準を上げれば、実際に戦闘員である可能性が高まるであろうし、逆に評価値基準を下げれば、戦闘員でない者が紛れ込む可能性が高くなる。要するに課題は、評価値基準の設定と、「ラベンダー」で抽出した容疑者に対してどれだけの追加的調査をして認定するか、という実際の運用方法であろう。

AI利用による標的抽出支援の成果は大きく、2023年初に、イスラエル軍の標的管理責任者（大佐）は、イスラエル軍創設以降初めて、攻撃頻度を上回って、新規標的を提示できるようになったと述べ[31]、AI支援システムの有効性を誇っている。

ウ　「ラベンダー」運用方法の変化

ところが、本戦争では、ガザの一般戦闘員を大量且つ迅速に殺害することが至上命題となった。

従来、個別戦闘員を標的とする殺害は、幹部に限られており、そのため標的が実際に軍事部門の幹部であるかどうかについて、住居、交友接触情報、在宅時間などを調査して、確実に自宅にいることを確認して攻撃していたという。ところが、この方法は、対象標的が数十人であれば可能な手順であるが、膨大な数の一般戦闘員に対しては、調査のための人的資源が不足しており、そこで結果としてAIへの依存を深めることとなったという。

具体的には、開戦当初に「ラベンダー」がハマス戦闘員として提示する人定情報から、数百のサンプルを無作為抽出して、サンプルの正確性を分析官が確認したところ、90％の正確性を確認したという。そこで、開戦約2週間後に、「ラベンダー」が戦闘員容疑者として提示する者については、分析官がその背景要因について個別に分析することなしに、戦闘員として扱うようになったという。

但し、仮にそうであるとしても、戦闘員としての評価値基準を当初のサンプル調査時より

37,000 Hamas targets," *The Guardian,* 3 April 2024.　（以下Guardian①2024.4.3）

[31] JP①2023.10.11

も高く設定していれば、正確性は 90%よりも高くなったであろう。

ところが、特に開戦当初は、インテリジェンス部門に対してより多くの標的の提示が要求されたため、評価値基準の点数は下がり気味であり、戦闘員として提示する人数は増え、最多時には 3 万 7000 人のリストが生成されていたという。つまり、そもそも、イスラエルが本戦争開始前に見積もっていたガザ地区の戦闘員は 3 万人以上というものなので、ここまで基準を緩めると、リストには戦闘員ではない者も含まれてきてしまう。具体的には、例えば、警察官や民間防衛担当者など戦闘員と似た通信特徴を持つ者、戦闘員の親族、たまたま戦闘員と同じ名前とあだ名を持っている者、戦闘員の携帯を譲り受けて使用する者などである。パレスチナ人は、携帯電話をしばしば友人や配偶者に譲ることがあり、これを迅速正確に把握することは難しい。

人的資源の不足のために、結果的に、一般戦闘員に対する攻撃決定においては、「ラベンダー」が提示する者に対して、追加調査をしないで、単に対象者の通話音声記録を聞いて性別を確認[32]するだけで、攻撃決定に至ることが通常であったという。性別を確認する理由は、ガザの社会慣習では女性は戦闘員にしないため、標的から女性を除外するためである。この実務慣行では、「ラベンダー」が戦闘員として提示した者について、誤認定を発見し是正する手続は実質的に存在しなかったという。

更に問題なのは、「ラベンダー」AI の学習過程では、ハマス支配下の治安省の職員までも、「ハマス工作員」として学習データに利用されたこともあるという。こうなると、ガザ地区の警察官や民間防衛担当者を戦闘員と判定する虞は高くなる。

このように「ラベンダー」AI による戦闘員認定では、誤認定があったと見られるが、他方、戦闘員認定が出鱈目という程、いい加減なものであった訳でもない。筆者は、AI による標的の抽出選定自体が、民間人死傷者の増大の最大の要因ではないと考える。但し、調査報道をしたジャーナリスト、ユヴァル・アブラハムは、この誤認定の存在自体が倫理的に許容できないと考えている様である。

（２）標的と住居

戦闘員が夜間などに自宅にいるところを爆撃するのは、地下トンネルなどの施設にいる戦闘員の攻撃と比べて、先ず戦闘員の所在地点の特定が容易であり、且つ、住宅爆撃による殺害が容易であるからである。

「ラベンダー」AI を使用するなどして攻撃標的を選定すると、標的ファイルにリスト化される。この標的ファイルには、自宅の所在地や当該住宅での付随的損害の見込人数も入力されている。付随的損害見込みは、住宅の大きさ、住民記録などから家族構成を推定するなどして設定される。そして、後述する付随的損害の許容基準に従って、最終的な攻撃標的の決定が行われる訳である。そして、位置評定システムに入力される。

従来は、自宅爆撃による殺害は、ハマスの幹部攻撃では行われていたが、一般戦闘員の攻撃では行われていなかったという。それが 10 月 7 日後は、先ず、戦闘員の中でも特殊作戦

---

[32] 筆者の経験でも、アラビア語やヘブライ語のセムハム語族においては、動詞の活用変化が男性話者と女性話者で異なるので、話者の性別は容易に推定できる。

部隊員、対戦車戦闘員、イスラエル領内攻撃参加者などの重要な一般戦闘員が入力され、次に、10 月 27 日地上軍がガザ北部に本格的に侵攻開始すると、普通の一般戦闘員がそのまま入力されるようになり、万を超える戦闘員が入力されるようになったという[33]。

位置評定システム[34]は、対象者の自宅所在地情報が既にデータベース化されており、数千人の対象者の現在位置をシギント情報で同時に追跡し、自宅に入ったところで、攻撃担当将校に通報が届くようになっている。

但し、攻撃担当将校への通報と実際の攻撃との間にはどうしても時間差があるので、この間にハマス戦闘員がいなくなって、残った家族だけが殺害されることも発生する。また、現実の居住者数は、避難した数家族が寄り集まって隠れ住む場合があるので、設定家族数よりも増えてしまうこともあるが、これは考慮外とされているという。

（３）攻撃での使用武器

付随的損害が大きくなった原因の一つに、イスラエル軍が住宅の攻撃において、精密誘導爆弾に加えて、通常爆弾を使用していることも挙げられている。　一般戦闘員の攻撃では、通常爆弾を使用する可能性が高く、結果的に付随的損害が大きくなるという[35]。

2023 年 12 月時点における米国インテリジェンス（国家諜報長官室）の推定では、それまでイスラエル空軍が使用した爆弾 2 万 9000 発の内、精密誘導爆弾は 55%から 60%で、残りの 40%から 45%は無誘導の通常爆弾である[36]。

高層ビルの爆撃では、付随的損害を少なく抑えるために炸薬量の少ない精密誘導爆弾を使用するが、一般戦闘員の殺害のために高価な精密誘導爆弾を使いたくない。そこで、一般戦闘員の殺害では数階建ての低層住宅にいるところを通常爆弾で攻撃することが多いという。通常爆弾は精密誘導爆弾よりも炸薬量が多く、一般住宅への打撃は大きく、付随的損害も大きくなる。

他方、イスラエル軍は付随的損害を少なくするために、通常爆弾を使用する場合は、急降下爆撃（divebomb）によって可能な限り標的を正確に打撃していると主張している[37]。米軍関係者によれば、イスラエルの精密誘導爆弾の着弾の正確性は標的地点から約 3m以内であるが、通常爆弾の急降下爆撃では 30m以内であるという[38]。

---

[33] 一般戦闘員の自宅爆撃は、イスラエル軍による警告に従って民間人のガザ北部から南部への避難が進んだ結果、北部残留者に占める戦闘員の割合が高まり、付随的損害の低減が見込めるようになったためと推定されている。

[34] Where's Daddy? という名前の位置評定システムがあると報道されている。＋972③2024.4.3

[35] イスラエル軍は、2002 年にハマスのカッサム旅団の当時の司令官サラー・ムスタファ・ムハマド・シェハデを殺害するのに 1 トン爆弾を使用し爆殺に成功したが、同時に、同人の妻と 14 才の娘に加えて、他に 14 人の民間人が死亡した。そのため、国内外から戦争犯罪であると非難された。そこで、翌 2003 年はカッサム旅団の当時の司令官モハメド・デイフを殺害するため 250 キロ爆弾を使用したが、デイフ殺害に失敗した経緯がある。＋972②2023.11.30

[36] Natasha Bertrand and Katie Bo Lillis, "Exclusive: Nearly half of the Israeli munitions dropped on Gaza are imprecise 'dumb bombs,' US intelligence assessment finds," *CNN*, 14 December 2023.

[37] ＋972③2024.4.3

[38] John Hudson, et. al., "Unguided 'dumb bombs' used in almost half of Israeli strikes on Gaza," *The Washington Post*, 14 December 2023。本記事によれば、米軍は爆撃では殆ど精密誘導爆弾のみ

（４）付随的損害の許容基準（非戦闘員の損害許容範囲）

戦闘員が自宅にいるところを爆撃することによって、付随的損害として家族である女性子供の死者が多数発生しているが、この付随的損害の許容基準は、時期や標的の重要性によって増減している。旅団指揮官、大隊指揮官など、ハマスの高級幹部であれば、イスラエル軍は従来から、1 人殺害のために民間人多数の死者も許容していたが、一般戦闘員の殺害目的では付随的な民間人の死者は許容していなかった。従って、一般戦闘員殺害のために住宅を爆撃することはなかったという。

ア　一般戦闘員殺害のための付随的損害の許容

ところが、10 月 7 日のテロ攻撃以降、方針が大きく変わった。一般戦闘員の殺害のためであっても付随的損害を許容するようになったのである。匿名取材対象者によって数値は異なるものの、戦闘開始当初の戦闘員 1 人殺害に対する付随的損害の許容基準は 15～20 人であり、この基準であれば一般住宅であれば自由に爆撃できた。1 週間後には 5 人まで削減されたものの、これでは家族全員が住宅にいると想定すると付随的損害予想が 5 人を超えて攻撃ができなくなるので、再び、許容範囲が緩和されたという。この許容範囲の緩和は直ぐに中止されたとも言われる。しかし、民間死者数の推移を見る限り、少なくとも当初 2 か月程度は、緩い許容基準による一般住宅に対する攻撃が続いていたと推定できよう。

また、ユヴァル・アブラハムの匿名取材によれば、2024 年 4 月現在、一般戦闘員殺害のための一般住宅の爆撃は中止されているという。要因の一つは、米国政府からの圧力であるが、他の要因は、ガザ地区の一般住宅の大部分は既に破壊されたか損害を受けており、住民の大多数が難民となってしまった現状では、軍が構築したインテリジェンスのデータベースと自動位置評定（自宅所在通報）システムの有効性が減少してしまったためという[39]。

しかし他方、最近の OCHA 資料を見ても、頻度は減少したかもしれないが、依然として一般住宅に対する爆撃による家族一緒の殺害は継続していることが伺われる[40]。これらの攻撃対象は幹部であった可能性もあるが、一般戦闘員殺害のための一般住宅の爆撃が本当に中止されたかは不透明である。

イ　高級幹部殺害のための大量の付随的損害の事例

なお、ハマスの高級幹部については、1 人殺害のために民間人 100 人以上の損害も許容されており、現在でも爆殺は続いている。過去の顕著な事例を紹介する。

2024 年 10 月 17 日の「中部ガザ旅団」旅団長のアイマン・ナファルの殺害では、精密な位置の特定ができなかったため 300 人の付随的損害が許容された。ブレイジ難民キャンプ内の大きなアパート数軒が完全に破壊され、爆撃当日だけで約 50 体の死体と重傷者 200 人を回収したが、死体と重傷者を救出するのに更に 5 日間を要した。

12 月 2 日の北部の「シェジャイヤ大隊」大隊長のウィサム・ファルハトの殺害では、100 人以上の付随的損害が許容された。この爆撃では、数十の建物が破壊され、数十人が死亡し、更に数百人が破壊された建物の下敷きになった。

を使用しており、特に市街地ではそうであるという。

[39] ＋972③2024.4.3

[40] OCHA #150(2024.4.5), OCHA #151(2024.4.8)等。

更に 12 月中旬南部では、「ラファ旅団」旅団長のモハメッド・シャバネーを殺害するため、高層ビルを破壊して、一般民間人数十人が死亡したが、司令官本人を殺害できたかどうかは、不明である。

このような大量の付随的損害の許容はイスラエル軍でも未曽有のことであり、10 月 7 日のテロ攻撃に対する復讐の側面があると見られる。

ウ　＜参考＞米軍における付随的損害の許容基準

参考までに、米軍における付随的損害の許容基準を見ておこう。イスラエルで適用されたような、一般戦闘員 1 名に対して民間人損害の許容基準が 15～20 人というのは、米国の基準では異常であるという[41]。米国中央軍の作戦・情報担当のゲルステン少将（2021 年当時）によれば[42]、オバマ政権では許容範囲が低く、2011 年のオサマ・ビンラディンという超重要人物の殺害でさえ付随的損害の許容範囲は 30 人であった。相手が下級指揮官であれば付随的損害許容範囲は実質的にゼロであったという。その後のイスラム国との戦闘でも、付随的損害 15 人というのは一般的に許容範囲外であり、そのような攻撃を実行するには中央軍司令官オースチン大将（2013 - 2016 年）の特別承認を受ける必要があったという。

このように米軍の許容範囲は低く、それと対比すると、今回の戦闘でのイスラエルの許容範囲は広い。今回、民間人死傷者が極めて大きい原因は、この付随的損害の許容基準が大きく影響していると見られる。

（５）付随的損害の把握態勢

イスラエルのインテリジェンスは、従来のガザ地区における戦闘員の殺害では損害評価を行ってきた。損害評価では、標的とした高級司令官が死亡したかどうか、何人の民間人が死亡したか（付随的損害）を調査してきた。

2022 年 8 月の調査報道[43]によれば、元ガザ師団のシギント分析官の証言として、当時の実際の殺害手順を説明している。即ち、ハマス戦闘員の殺害の際には、殺害対象の確認のために、事前に必ず複数の諜報源から殺害対象の人定を確認していたという。また、殺害直後には、戦闘員の家族の通話を傍受して、その通話から、対象戦闘員の殺害に成功したか否か（作戦の成否）、巻き添えで家族など民間人が何人死んだか、負傷したか（付随的損害）などを確認していたのである[44]。

しかし本戦争では、ハマスの幹部については、この手続を維持しているものの、一般戦闘員の殺害に関しては、省力化のため、この手続は省略されている。実際、それを行うための人的資源が不足しているためである。そのため、一般戦闘員攻撃に関しては、何人の付随的損害が発生したか、更に本人を殺害できたどうかも不明なままである。

---

41 Guardian①2024.4.3

42 Frank Wolfe, “Pentagon Removed Non-Combatant Casualty Cut-Off Value From Doctrine in 2018,” *Defense Daily,* 6 November 2021.

43 ＋972①2022.8.11

44 イスラエル軍では、損害評価を担当するシギント部隊アラビア語傍受員の教材として、戦闘員の家族が死を嘆く実際の通話の音声傍受記録が使われている。極めて実践的な教育をしていることが伺われる。＋972①2022.8.112022.8.

６　まとめ

本稿では、先ずイスラエル・ガザ戦争における損害（死傷者）について、イスラエル軍の死者と比べてガザ戦闘員の死者が極めて多いこと、ガザ戦闘員の死者と比べてガザ民間人の死者がとても多いことを示した。その背景にはイスラエル軍の戦い方があるのであるが、戦い方の分析の前提として同国のシギント組織 8200 部隊のガザ地区に対する絶大な監視能力を推定も交えて明らかにした。イスラエル軍は、この絶大な監視能力を活用して、一人でも多くのガザ戦闘員の殺害を指向した。そして、通常の軍事目標に加えて、高層ビルなどの「高価値標的」（power targets）や「戦闘員の自宅」に対して大規模な攻撃を加えてきた。特に、AI「ラベンダー」を使用して、ガザ地区の大量の通信データから、戦闘員の通信特徴を示す者を大量に抽出して、彼らが自宅にいるところを、爆撃して殺害する方法を取った。その結果、イスラエル兵の損害は軽微でありながらガザ戦闘員を大量に殺害できたが、また、同時に、戦闘員の家族親族などの民間人の大量の付随的損害（死傷者）を出すこととなった。

このような民間人に大量の死傷者を出す戦い方は、非人道的であるとして非難されているが、イスラエル軍の立場に立てば、ガザ地区のテロ組織を壊滅させるにはこれ以外の戦い方があるのか、他に選択肢はないということであろう。空爆や砲撃を主体とせずに、単に歩兵の市街戦に取り組めば、イスラエル軍の損害も甚大なものとなっていただろう。

他方、ガザ地区の一般住宅の多くは既に破壊されたか損傷を受けて、住民の大多数が難民となってしまっている。また、ガザ地区内の通信インフラもイスラエル軍の攻撃により大きな損傷を受けており、シギント情報を活用する開戦以来のイスラエル軍の戦い方の有効性も低減していると思われる。

今後、イスラエル軍が最後の大きな拠点と見做すラファに侵攻すれば、ガザ戦闘員が所在すると考える建物を爆撃主体で破壊する戦い方となろうが、ラファにはガザ地区住民の難民で溢れかえっており、民間人に甚大な損害が危惧される。

（2024 年 5 月記）

米国 ACD・Defend Forward とシギント機関の役割
～日本「能動的サイバー防御」と対比して～

茂田　忠良

＜目次＞

はじめに …… 31
1　米英公開文書における ACD の定義 …… 32
2　UKUSA シギント諸機関による「脅威情報の事前把握」 …… 34
3　英米 ACD と Tutelage …… 36
4　ACD の現在地 …… 38
5　結論 …… 39
6　補足①：CS 対策にも有効な他のシギント・プログラム …… 40
7　補足②：Defend Forward 戦略 …… 41
8　補足③　Defend Forward 的活動は、国際法上「軍隊」の任務か … 43

はじめに[1]

最近、Active Cyber Defense（以下「ACD」）という言葉をよく聞く。日本語では「能動的サイバー防御」と翻訳されているが、この「能動的サイバー防御」の言葉の使い方が人によって異なるようである。

例えば、2023 年 7 月に「日本戦略フォーラム」主催で台湾有事シミュレーションが政治家も参加して行われたが、この設定事例では、既に我が方のシステムが攻撃され実害が生じている段階で、攻撃源を探知して反撃する行為を「能動的サイバー防御」と呼んでいる。

他方、政府の「国家安全保障戦略」（2022 年 12 月閣議決定）の政府訳の英語版[2]によれば、「能動的サイバー防御」の取組を、「（政府や重要インフラに国家安全保障上の懸念を生じる虞のある）重大サイバー攻撃の可能性を未然に排除し、また攻撃発生時の被害拡大を防止すること」と説明しており、具体的な取組の一つに、「可能な限り未然に攻撃者のサーバー等に侵入し無害化すること」が記載されている。

つまり、前者は攻撃を受けた後の反撃、後者は攻撃を受ける前の先制的無害化措置（攻撃）に力点があり、必ずしも定義は一致していない。

「能動的サイバー防御」は英語の Active Cyber Defense を翻訳した用語と見られるので、そもそも英語国である米英では ACD はどういう意味で使われていたのか見てみたい。実は米英での ACD と我が国の「能動的サイバー防御」の定義にもズレがあり、このズレこそが、我が国と英米諸国とのサイバーセキュリティ対策の違いとズレを示しているのである。

---

[1] 本論考の脚注を除く本文の概要版を、『軍事研究』2024 年 3 月号に「サイバーセキュリティは『前方防御』へ」と題して掲載している。

[2] 邦文は必ずしも明晰な文章ではないので、より明晰な英語訳を使用した。

1　米英公開文書における ACD の定義

（1）米国における ACD の定義

ア　国防総省文書での言及

JPCERT/CC の佐々木勇人氏の指摘によれば、米国政府の公開文書における ACD の初出は、2011 年の「米国防総省サイバー戦略」[3]だそうである。本戦略では、国防総省におけるネットワークやシステム防護の取組 4 つ内の 1 つとして ACD が言及されており、ACD は次の様に説明されている。

> 「国防総省は、国防総省のネットワークやシステムへの侵入を阻止し、同ネットワークやシステム上での敵対的行為を無効化するために、ACD を導入した。」「センサーやソフトウェアやインテリジェンスを使用して悪意ある行為がネットワークやシステムに影響を及ぼす前に探知して阻止する」[4]。

この ACD 説明の要点は、第 1 に、国防総省のネットワークに事前の対策を施すこと、第 2 に、ACD は既に（本戦略公表の 2011 年の時点で）運用されていること、第 3 に、悪意ある行為の事前探知にインテリジェンスも使用されることである。

イ　NSA 文書での言及

次に、NSA（National Security Agency：国家安全保障庁）が ACD にどう言及しているか、見てみる。NSA は、米国政府の National Security Systems（国家安全保障システム）という国家安全保障に係わる国防総省やインテリジェンス諸機関のネットワークのセキュリティ担当部署であるから、担当部署による定義である。2015 年当時の NSA 情報保障局長カート・デュークス氏の発言[5]によれば、サイバーセキュリティの最大の課題は、如何にして敵対者が自己の防禦を突破するかを予測することであるとした上で、ACD については「ネットワーク防禦の全レイヤーにわたる侵入（compromise）徴候のリアルタイム共有を通じて、サイバー事案の探知と低減を統合し、同期し、自動化することを可能とするアーキテクチャー」であると説明している。

NSA の解釈においても、ACD とは、攻撃を予測して、ネットワークに事前の対策を施すことを意味している。

（2）英国における ACD の定義

次に、英国における定義を見てみる。少し古い資料であるが、2016 年の英国「国家サイバーセキュリティ戦略 2016-2021」[6]は、ACD を次の様に説明している。

> 「ACD とは、ネットワークやシステムに各種セキュリティ措置を施して、攻撃に対してより頑健であるように強化する方針である。民間では、ACD とは通常、サイバーセ

---

[3] DoD, *Department of Defense Strategy for Operating in Cyberspace*, July 2011.
[4] Ibid., p.6
[5] NSA, "In discussion with Curt Dukes (IAD)-Overview of NSA's Cyber Security Mission," *New*, 1 October 2015, retrieved 27 October 2023, https://www.nsa.gov/Press-Room/News-Highlights/Article/Article/1625846/in-discussion-with-curt-dukes-iad-overview-of-nsas-cyber-security-mission/
[6] UK, *National Cyber Security Strategy 2016-2021,* p.33.

キュリティ分析官が自己のネットワークへの脅威に対する理解を深め、攻撃を受ける前にこれら脅威と戦い又は防禦するための措置を考案して実施することと理解されている。政府も同じ方針をより大規模に適用する。」と述べた上で、政府は、その独特な専門性、能力、影響力を使用するとして、NCSC（註：シギント機関 GCHQ 傘下の国家サイバーセキュリティ・センター）の専門性を挙げている。

（３）ACD の共通事項と課題

米英の定義で共通するのは、脅威情報の事前把握と自己のネットワーク（システム）上の対抗措置である。

ところが、脅威情報の事前把握は容易ではない。佐々木勇人氏は「ACD を行う主体が『どの選択肢を選べば効果的か』を判断するための情報を鮮度の良い状態で入手することは容易ではありません。攻撃手法や攻撃インフラの全容は実際に攻撃が始まってみなければ知ることは出来ませんし、被害はどこで発生するのか予想が難しいため、攻撃を認知してから共有されるまでにギャップが発生します」と指摘している[7]。

そこで注目されるのが、ACD における脅威情報の事前把握に関連して、米国防総省文書がインテリジェンス（即ち、この場合はシギントを意味する）の使用について言及し、また、英国文書がシギント機関傘下の NCSC の専門性を挙げている点である。即ち、シギントが、脅威情報の事前把握に貢献することを示唆しているのである。次章では、UKUSA 諸国のシギント機関による「脅威情報の事前把握」に貢献するシステムを見てみる。

（４）余談：米英の ACD と我が国の「能動的サイバー防御」のズレ

なお以上見たように、米英の ACD の定義と我が国の「能動的サイバー防御」の定義にはズレがある。米英の ACD の基本は脅威情報の事前把握と自己のネットワーク上における対抗措置の設定であり、脅威源に対する攻撃は含まない。他方、冒頭記述の我が国における「能動的サイバー防御」の事例は、脅威源に対する反撃・攻撃であるので、米英の ACD には含まれないものである。即ち、「日本戦略フォーラム」シミュレーションでいう攻撃を受けてからの反撃は、英語では一般に Defensive Cyberspace Operation[8]（防御的サイバー作戦）の内の Cyberspace Attack 又は CNA（Computer Network Attack：コンピュータ・ネットワーク攻撃）に分類される行動である。また、我が国政府の「国家安全保障戦略」にいう可能な限り未然に攻撃者のサーバー等に侵入し「無害化する」ことは、後述する Defend Forward（前方防禦）の一環としての Cyberspace Attack 又は CNA と呼ばれる行動であり、攻撃が切迫した状況であれば、これも Defensive Cyberspace Operation に分類されるであろう。

---

[7] 佐々木勇人「『積極的サイバー防御』（アクティブ・サイバー・ディフェンス）とは何か―より具体的な議論に向けて必要な観点について―」（JPCERT/CC Eyes、2022 年 9 月 21 日）、https://blogs.jpcert.or.jp/ja/2022/09/active-cyber-defense.html

[8] オバマ政権時代の 2018 年に発出された大統領政策指令 PPD-20“U.S. Cyber Operations Policy”の定義では、Defensive Cyber Effect Operations と呼ばれる。また、2018 年作成の陸海空軍・海兵隊・沿岸警備隊の共同文書“Cyberspace Operations”では、Defensive Cyberspace Operations と呼んでいる。

２　UKUSA シギント機関による「脅威情報の事前把握」

UKUSA 諸国では、米国を除いて、シギント機関がサイバーセキュリティの所管官庁であり、また米国でも NSA がサイバーセキュリティで大きな役割を果たしている。そこで、ACD における「脅威情報の事前把握」でもシギント機関の貢献が予想される。ここでは、「脅威情報の事前把握」に貢献する UKUSA シギント機関のプログラムを、2013 年のスノーデン漏洩情報から見てみることとする[9]。

なお、米国の著名なサイバーセキュリティに関する論文[10]においても、シギント活動による「脅威情報の事前把握」を前提とした記述が見られる。

（１）カナダ CSE の取組

ア　Dynamic Defense

加シギント機関 CSE（Communications Security Establishment：通信安全保障局）の機密資料[11]は、passive defense と対照的な政策として Dynamic Defense を掲げている。その Dynamic Defense の構成要素は三つであり、三要素を統合して実施するものと定義している。三要素とは即ち、次の三つである。

① インターネットとの接続点における防禦

② インターネット空間（network core）におけるシギント活動[12]

③ 敵空間での CNE（筆者註：CNE とは Computer Network Exploitation コンピュータ・ネットワーク資源開拓であり、標的システムへのアクセス獲得と標的システムからのデータ取得の二つを含む。いわゆるハッキングである。）[13]

イ　EONBLUE[14]

②のインターネット空間におけるシギント活動の代表例は、EONBLUE というサイバー脅威探知センサーである。これは加 CSE が UKUSA 諸機関の協力を得て、世界のインターネット空間に設置されているシギント・インフラを活用して、そこにサイバー脅威探知センサーを 200 以上設置したものである。探知手法は、anomaly-based discovery と signature-

---

[9] 本項の記述は、茂田忠良「サイバーセキュリティとシギント機関～NSA 他 UKUSA 諸機関の取組～」（情報セキュリティ総合科学第 11 号、2019 年 11 月）（以下「茂田①」）、67-75 頁を基にしているが、原資料のスノーデン漏洩資料を再度確認して、加筆している。

[10] Robert M. Lee, “The Sliding Scale of Cyber Security,” *SANS Analyst Whitepaper*, SANS Institute, 15 August 2015. 論文中の 10 頁の Active Defense、13 頁の Intelligence についての記述を参照。

[11] スノーデン資料、*CSEC Cyber Threat Capabilities*, circa 2011, retrieved 14 May 2019, https://christopher-parsons.com/Main/wp-content/uploads/2015/03/doc-6-cyber-threat-capabilities-2.pdf

[12] カナダ CSE の資料では、②のインターネット空間におけるシギント活動には、インターネット空間における防禦行為、例えば通信制御などによる攻撃軽減対策も含まれている。その意味では、米英の ACD の定義より広い活動を想定していると見られる。スノーデン資料、*CSEC Cyber Threat Capabilities*。

[13] CNE とは、NSA による定義では、①標的システムへのアクセスを確保すること、②標的システムからデータを取得することであって、標的システムの機能に障碍を与える行為は含まれない。この行為は CNA（Computer Network Attack）に分類される。

[14] 茂田①、75 頁；スノーデン資料、CSE, *CSEC SIGINT Cyber Discovery: Summary of the current effort*, November 2010；*CSEC Cyber Threat Capabilities*, circa 2011.

based detection の二つある。anomaly-based discovery には SLIPSTREAM というプログラムがあり、ハッカー通信に特徴的な特異性を探知する。通信の周期性、暗号強度のレベル、或いは通信パケット内容の分析など 50 以上の特異性の検知方式によって、ハッカーによる通信を発見しようとしている。また、signature-based detection には SNIFFLE というプログラムがあり、これは既に解明したハッカー通信に特有な特徴点を基にハッカー通信を探知するものである。これらの取組により、インターネット空間におけるハッカー通信を解明して、脅威情報の事前把握に役立てようとしている。

ウ　CASCADE[15]

スノーデン漏洩資料によれば、加 CSE は、2011 年頃シギントとサイバーセキュリティを統合した CASCADE という壮大なシステムを構想していた（2015 年の完成目標）。このシステムの説明によれば、後述する米国 NSA の tutelage システム（③の敵空間における CNE と①インターネット接続点で防禦を統合したもの）の導入が予定されていたと推定できる。

このように、CSE の Dynamic Defense では、インターネットとの接続点での防禦を有効ならしめるために、シギント機関が、インターネット空間及び敵空間における情報収集によって、脅威を事前に把握する取組が想定されていた。

（２）英国 GCHQ の取組　LOVELY HORSE[16]

LOVELY HORSE は、英国 GCHQ（Government Communications Headquarters：政府通信本部）の開発したプログラムであるが、ハッカー間の議論を自動的にフォローするプログラムである。

民間ハッカーは、ブログやチャットルームで、自らのハッキングの技術を誇示したり、窃取したデータを公開したりしており、これらにはサイバーセキュリティに役立つ貴重な情報が含まれるので、収集して脅威分析に使用できる。ところが、シギント機関の分析官のマンパワーを使ってフォローするのは効率的でない。そこで、英 GCHQ は、各種のブログやツイッターなどソーシャルメディアに現れるハッカーによる議論の中から、分析官が関心あるものを自動的に検索し分類して提供するシステムを開発した。

これらのデータは、ハッカーの標的や技法を分析して、事前対処に役立てることが出来る。なお、本手法自体は民間人でも実行可能な手法であり、本プログラムに、固有のシギント・インフラが使用されているか否かは、不明である。

（３）米国 NSA の取組　Tutelage

次に米国の取組を見ると、興味深いものに Tutelage システム[17]がある。このシステムは、正に脅威情報を事前に把握して自己のネットワークに対抗手段を設置するものである。

脅威情報の事前把握の方法は、NSA の「ハッカー集団」である TAO グループによる CNE 活動（標的システムへのアクセス獲得とデータ取得）である。即ち、脅威グループのシステ

---

15 茂田①、71 頁；スノーデン資料、CSE, *CASCADE: Joint Cyber Sensor Architecture*, circa 2011.
16 茂田①、74 頁
17 詳細は、茂田①、68 - 71 頁；　スノーデン資料、NSA, *Tutelage,* circa 2011, https://www.aclu.org/foia-document/tutelage

ムに事前に侵入して、当該グループの技術（マルウェアの構造等、所謂 TTPs）、攻撃対象、攻撃時期等を事前に把握して、攻撃を受ける前に対抗手段をシステムのインターネット接続点に設置するものである。国防総省の情報ネットワークである NIPR Net[18]は米独日の 10 か所で世界のインターネットと接続されているが、Tutelage システムは遅くとも 2009 年までにはそれらのインターネット接続点に導入されている。

スノーデン漏洩資料によれば、2011 年 2 月現在、NSA は世界の 28 の脅威グループ（ハッカー集団）を解明して、これに対する対抗手段 operational effects798 個を NIPR Net に設置していた。operational effects とは、ネットワークに脅威が到達した場合に、これを探知して警告、インターセプト、代替、転送、遮断、遅延などの対抗措置を採るものである。対策を採っていた脅威グループの相当数は中国関係である。当時、NSA が解明対象としていた中国の脅威グループは 12 であるが、漏洩資料を分析すると、その内、7 つ又は 8 つの脅威グループについては全部又は一部を解明して対抗手段を設置していたことが分かる。

Tutelage システムの成果の例は、①2010 年 10 月統合参謀本部議長始め国防省高官 4 人に対するフィッシング攻撃対処である。中国のハッカー集団が攻撃をかけたが、2009 年の段階で既に計画を探知して対抗手段を開発していたので、実際の攻撃を探知して阻止することができた。また②2010 年 12 月のクリスマス・シーズンでは、クリスマス・メールを大量に送付してマルウェアに感染させようとする動きを探知したため、関連する特定ドメインの通信を事前に遮断して感染を防止している。

Tutelage システムは魅力的なシステムであったようで、漏洩資料によれば、2013 年春時点で、ドイツ BND と NSA 間で、ドイツへの Tutelage システム導入について協議の予定であり、NSA は Tutelage の提供に前向きであった。更に、New Zealand はサイバーセキュリティのため CORTEX システムを導入（2014 年導入開始 2017 年完成）したが、NZ の Cyber Threat Report 2017/2018 を見ると、CORTEX システムには Tutelage システムが導入されたと推定できる[19]。

3　英米 ACD（Active Cyber Defense）と Tutelage

ここで、米英の ACD に Tutelage システムが含まれているかどうか、確認しておこう。

（1）米国防総省の ACD

国防総省の文書[20]では、ACD にはインテリジェンスで得られた情報も利用されていると明示されている。従って、カナダの EONBLUE や英国の取組 LOVELY HORSE のようなインターネット空間におけるシギント活動で得られた情報、更に Tutelage などの敵空間におけるシギント活動（CNE）で得られた情報が使用されているのは間違いない。実際、既述

18 NIPRNet は、内部利用者が sensitive but unclassified information の相互通信に使用すると共に、外部インターネットとの接続のために使用するネットワークである。国防総省のネットワークはこの他に、secret 情報の通信に使う SIPRNet、top secret 情報の通信に使う JWICS があり、後二者はインターネットとは接続されていない。

19 詳細は、茂田①、72 頁。

20 DoD, ibid.

したようにTutelageシステムによるハッカー集団による侵入阻止の事例もある。

（２）米連邦一般官庁のサイバーセキュリティ Einstein 3

米連邦政府の一般官庁のネットワーク・セキュリティの責任官庁は CISA であるが[21]、CISA（Cybersecurity and Infrastructure Security Agency：サイバーセキュリティ・重要インフラ安全保障庁）は2010年にEinstein 3というシステムの導入を計画した。本計画では、民間通信事業者が一般官庁に繋ぐインターネット回線をNSAの設置する監視装置を経由させることによって、NSAが持つ情報を基にして、マルウェア等の侵入を阻止する構想であった。報道[22]によれば、Einstein 3にはTutelageシステムが導入される予定であった。

2010年当時、Tutelageシステムの具体的内容は知られていなかったが[23]、一般官庁の通信を全てNSAの設置する監視装置を経由させることについては、NSAが勝手に情報を抽出する虞があるとの批判が強く、結局Einstein 3計画は撤回された。

そこでCISAは、2012年に至りEinstein 3 Accelerated（E3A）という代替計画を策定して、現在は連邦の一般官庁の殆どに導入されている。E3Aは、主要なインターネット・サービス提供会社（ISP）が広く使用している民間技術を使って侵入防止を図るものであるが、同時に、全通信が数か所の集中点を通過するようにして、そこでCISAが最新且つ高度な保護措置を適用できるようにしている[24]。

公開情報からは、E3AにおいてTutelageシステムが運用されているか否かは不明であるが、Tutelageシステム又はその派生型が運用されている可能性は高いと考えられる。サイバーセキュリティ上有効なシステムを殊更使用しない理由がないからである。但し、Tutelageシステム自体は、NSAのNTOC（脅威作戦センター、NSA/CSS Threat Operation Center）が管理しているが、E3AではNSAの情報に基づきCISA自体が管理している可能性が高い。

このように、米国でいうACDでは、Tutelageシステムを含むシギント情報が直接或は間接に貢献していると言えるであろう。

（３）英国の ACD

では、英国ではどうであろうか。

先にも紹介した2016年の「国家サイバーセキュリティ戦略2016-2021」[25]によれば、ACDの目的の一つに「重大な国家支援型脅威 state-sponsored threat の阻止」も記載されている。その趣旨からすれば当然Tutelageシステムの導入が含まれていると見るべきであろう。

---

21 軍やインテリジェンス機関が使用する National Security Systems のセキュリティ担当官庁はNSAである。

22 Ellen Nakashima, “Cybersecurity Plan to Involve NSA, Telecoms”, *The Washington Post,* 3 July 2009, retrieved 8 October 2023;
Robert Sesek, “Unraveling NSA’s TURBULENCE Programs,” *rovert.sesek.com*, 15 September 2014, retrieved 8 October 2023.

23 Tutelageシステムについてのスノーデン漏洩資料の初報道は2015年1月である。

24 CISA, *Einstein*, undated, retrieved 8 October 2023, https://www.cisa.gov/einstein

25 UK, *National Cyber Security Strategy 2016-2021,* p.33.

４　ACD の現在地

ここまで、米英の ACD の定義、ACD に対するシギント機関の「脅威情報の事前把握」における貢献、そして、Tutelage システムについて見て来た。さて、それでは、UKUSA 諸国における ACD の現状はどうであろうか。

実は、UKUSA 諸国のサイバーセキュリティ当局で、現在、ACD という用語を使っている国は、英国一国しかないのである。また、その英国でも、ACD の内容に微妙な変化が見られる。

（１）米国の ACD

先ず、ACD を使用していた米国では、国防総省、NSA、CISA のウェブサイトを検索しても、ここ 5 年間ほどの文書からは ACD という用語が見つからない。つまり、米国では現在政府の政策の形容としては ACD という用語は使用されていないということである。

米国政府のサイバーセキュリティ対策の重点は、2018 年以降、ACD から、Defend Forward 戦略に移行しているのである。

（２）加、豪、NZ の ACD

次に、米英以外の UKUSA 諸国では、ACD がどう使われているか調べてみると、サイバーセキュリティを所管する加豪 NZ のシギント機関、加 CSE、豪 ASD（Australian Signals Directorate）、NZ の GCSB（Government Communications Security Bureau）、そして傘下の各国のサイバーセキュリティ・センターの何れのウェブサイトを検索しても、ACD という用語自体がヒットしないのである。つまり、加豪 NZ 諸国は、そもそも ACD という用語をサイバーセキュリティ対策用語としては使用してこなかったのである。

但し、各国が実際のサイバーセキュリティ対策として実施している施策内容は、英国が ACD の名の下に実施している施策と余り変わらない。

（３）英国の ACD

さて、英国ではどうであろうか。

実は、英国では ACD の内容に微妙な変化が見られる。先述したように 2016 年の文書では、ACD に Tutelage システムが含まれていると推測できたのであるが、現在、英国は、ACD から Tutelage システムを除外しているようである。

即ち、現在の戦略文書「政府サイバーセキュリティ戦略 2022-2030」では、ACD の目的から「重大な国家支援型脅威 state-sponsored threat の阻止」が削除されている[26]。更に、現在の NCSC（National Cyber Security Centre）のウェブサイトの説明[27]では、英国の ACD の目的は、「英国の大部分の人々を、大部分の時間にサイバー攻撃の大部分が惹き起こす損害の大部分から守ることである」として、「ACD は人々の日常生活を脅かす大量の標準的

[26] UK, *Government Cyber Security Strategy 2022-2030*, p.45.
[27] NCSC website, *Active Cyber Defence,* retrieved 9 October 2023, https://www.ncsc.gov.uk/section/active-cyber-defence/introduction.

な攻撃に対処することを意図したものであって、高度に洗練された標的型攻撃ついては、NCSC は別途対応している。」と述べている。

Tutelage システムは、基本的には高度な標的型攻撃を対象に、シギント活動（CNE）によって事前にハッカー集団のシステムに侵入して、その攻撃技法、攻撃対象、攻撃時期などの情報を入手して、事前に対抗措置を採るものであるから、英国の NCSC はこれには取り組んではいるものの、それを英国の ACD からは除外したのである[28]。

このように ACD という用語を、現在政府の政策として使用しているのは、UKUSA 諸国の中で英国だけであり、また、その内容にも過去とは変化が見られるのである。

５　結論

以上の分析から、次の結論が導かれる。

（１）ACD と「能動的サイバー防御」という用語の使用

先ず、ACD という用語については、現在我が国で使われている「能動的サイバー防御」で議論の中心となっている行為、即ち、サイバー攻撃に対する反撃や先制的無害化措置は、そもそも米英の ACD には含まれていない行為である。そこで、我が国の議論で ACD という用語を使用することは混乱を招くだけであるので、使用は慎むべきであろう。仮に使用するのであれば、英国政府の定義と同様とすべきである。

次に、「能動的サイバー防御」については、使う人によって定義が異なるようである。この用語を無限定に使用することは、共通理解を妨げる虞が高い。もし仮に使用するならば、その際、先ず言葉の定義を明示してから使うべきである。またこのような用語を英訳する際には、誤解を招かないように ACD と翻訳すべきではないであろう。

（２）CNE（いわゆるハッキング）と ACD

シギント機関による CNE（Computer Network Exploitation：コンピュータ・ネットワーク資源開拓）は、標的システムへのアクセスを確保する行為、及び標的システムからデータを取得する行為であるが、これは ACD の一環として開始されたものではなく、ACD に先行する平常の対外インテリジェンス、シギント活動である。

即ち、ACD のためにシギント機関による CNE は有用ではあるが、CNE は ACD のために初めて認められるものではない。CNE はシギント機関にとってシギント・データ収集のための重要業務である。その CNE は、政治軍事経済などの国家安全保障上必要な情報収集に貢献すると同時に、ハッカー集団に対する情報収集にも貢献するのである。そして後者の情報が ACD や後述する Defend Forward 等のサイバーセキュリティ対策に役立っているということである。

---

[28] 英国 NCSC が高度な標的型攻撃は ACD の対象外であるとした理由は良く分からないが、推測するところ、英国の ACD は広く民間を対象とする政策として実施されているが、スノーデン漏洩資料で Tutelage システムを知った民間からも、Tutelage システムの保護対象にしてくれるのかという問合せが相次いだのではないか。そこで、Tutelage システムは、一般的な ACD には含まれず、NCSC が特別な保護対象にのみ適用するとせざるを得なくなったのではないかと考える。

従って、ACD を可能とするために CNE を合法化するのではなく、それに先立って、シギント機関の基本的権能として対外 CNE を認める必要がある。仮にサイバー防衛目的に限定して CNE を認めるならば、世界のインテリジェンスの物笑いとなるだろう。

（３）ハックバックと CNE と CNA

ハックバックが、ACD の一部として認められるかという議論がある。民間組織が実施する ACD でハックバックを認めるかは微妙な課題であるが、政府シギント機関では議論の必要はないであろう。実際、先述した Tutelage システムにおいても、2011 年頃既に自動ハックバック対抗措置の開発が議論されていた[29]。それは、ハックバックを ACD を機として行うものであり、ACD の一部として初めて認められるものではない。シギント機関はもともと CNE（いわゆるハッキング）が認められているものなのである。従って、ハッカー集団の侵入を機に逆侵入するのは、当然に許されるのである。

但し、ハックバックすべき標的システムが、国外のシステムではなく、国内のシステムである場合には、法制度的議論が必要であろう。つまり、民主主義国家においては、国民の人権保障の観点から、通信傍受にしろネットワークへの侵入にしろ、対象システムや対象者が国外にあるか国内にあるかで、実施主体や手続要件を変えるのが基本である。つまり、国内通信の傍受や国内ネットワークに対する CNE は、基本的にセキュリティ・サービスの任務であって、対外シギント機関の任務ではないことに留意する必要がある。

６　補足①：CS 対策にも有効な他のシギント・プログラム

本論考第 2 章、第 3 章では、米英の ACD の関連で、「脅威情報の事前把握」に貢献する NSA・UKUSA のプログラムを見たが、それ以外にも、サイバーセキュリティ対策に貢献するシギント・プログラムが存在する。代表的なものを簡単に紹介する。

（１）X-Keyscore（以下「XKS」）[30]

XKS とは、NSA が大量に取得するデータの一次記憶装置であり、また、この装置から必要なデータを検索抽出し分析するための分析システムである。NSA 版の「グーグル」とも言われる。本来は、シギントのためのシステムであるが、同時にサイバーセキュリティ対策でも有用なシステムである。

XKS が具体的にどのように Attribution（ハッカーの探知特定）や Counter-CNE（ハッカー対策）に使われているか明瞭ではないが、例えば、嘗てスノーデンは XKS を使用して中国のハッカーを追跡したことがあると述べている[31]。また、スノーデン漏洩の英 GCHQ 機密資料 Cyber Defence Operations Legal and Policy[32]は、サイバー防衛に使用可能なデー

---

[29] スノーデン資料、NSA, *Tutelage,* circa 2011, pp.22-23.
[30] 茂田①47-48 頁。茂田『米国国家安全保障庁の実態研究』（警察政策学会資料 82 号、2015 年 9 月）（以下、茂田②）115 - 122 頁。
[31] 茂田①66 頁。
[32] スノーデン資料 GCHQ, *Cyber Defence Operations Legal and Policy,* GCWiKi

タについて説明しているが、その記述の中心が XKS である。また、米 NSA の機密資料 XKEYSCORE for Counter-CNE[33]は、C-CNE での XKS の利用法を記述している。これらの資料から見ても、XKS がサイバーセキュリティ対策に大きく貢献していることが伺われる。

（２）Treasure Map[34]

Treasure Map 宝地図は、いわば、「インターネットのグーグルマップ」であり、端末機器やその使用者を含むインターネットの世界地図を作成し利用しようとするものである。このシステムは、本来シギント目的のものであるが、同時に、敵対者や潜在的脅威に関するネットワークの現況を把握し、Attribution や C-CNE 活動に役立てることが出来るのである。

（３）CNE 能力[35]

NSA の TAO グループは、世界最強の「ハッカー集団」であるが、同時に巨大な装置産業であり、CNE（Computer Network Exploitation ハッキング）のためのシギント・インフラを構築している。スノーデン漏洩資料によれば、TAO は内部組織として、ハッキングの実行部隊の他、ハッキング用のソフトウェアとハードウェア開発担当の ANT、通信網からのデータ収集の技術開発担当の TNT、ハッキングした標的システムとの通信用ソフトウェア開発担当の DNT、作戦用インフラ・ハードウェアの開発配備担当の MIT などの組織まである。そして、秘密裡に中国国内のデータ・センター2 か所に秘匿サーバー設置していたとされる位である[36]。

そのシギント・インフラを基礎とする強大な CNE 能力が、同時にサイバーセキュリティ対策において、敵対的ハッカー集団に対する情報収集力、C-CNE として活用できるのである。

以上のように見てくると、真に有効なサイバーセキュリティ対策を実行するには、本格的なシギント機関の設置が不可欠であり、且つ、自国のシギント機関を通じた NSA、そして UKUSA シギント同盟との協力が必要なことが分かるであろう。

7　補足②：Defend Forward 戦略

現在の米国のサイバーセキュリティ対策は、Defend Forward 戦略が中心となっている。

その理由は、もはや ACD や Tutelage システムでは守り切れないからである。第 1 に、Tutelage システム自体が完璧なものではない。世界の脅威グループを全て事前に解明することは、NSA の CNE 能力を以てしても不可能である。第 2 に、Einstein 3A の保護対象にもならない重要な地方行政機関や民間のネットワークやシステムが多数存在するのであり、これらも保護する必要もあるからである。

そこで、米国は 2018 年からは Defend Forward 戦略へと移行した。即ち同戦略では、脅

---

[33] スノーデン資料 NSA, *XKEYSCORE for Counter-CNE*, March 2011, retrieved 2 May 2019, https://theintercept.com/document/2015/07/01/xks-counter-cne/

[34] 茂田①47 頁；茂田②27-29 頁

[35] 茂田①48－55 頁；茂田②80-100 頁

[36] 茂田②28 頁脚注参照。

威がインターネット接続点に到達する前に、敵空間内或いはインターネット空間で脅威を阻止しようというものである。つまり、必要とあれば、脅威グループのサーバーに対する先制攻撃も厭わない政策である。そしてそのため Persistent Engagement(継続的関与)という活動方針を採用している。これは当初 constant contact（継続的接触）と呼ばれていたように、前方で脅威と継続的に接触を持って、脅威情報を収集し脅威を解明し、そして対処しようというものである。

この Defend Forward 戦略では、必要に応じて脅威グループのシステムに対して攻撃を行うために、サイバー軍が正面に出て、これを NSA が支援する形になっている。

そしてサイバー軍による機動的な攻撃を可能とするため、2019 年国防授権法（2018 年 8 月成立）[37]によって、サイバー空間における秘匿の軍事活動や軍事作戦が、国家安全保障法 502 条（大統領による covert action の承認と報告）の適用を受けない「traditional military activity（伝統的軍事活動）」と定義された。covert action（秘密工作）は、その実施には大統領の個別承認と議会報告が必要であり[38]、その前提として「国家安全保障会議」の審議を経る必要がある[39]など、様々な手続制度的な制約がある。そのため、サイバー空間における脅威集団に対する対応を適時に行うことが困難であったが、本改正でその手続制度上の制約を取り除いたのである。

本改正と共に、2018 年 8 月トランプ大統領が国家安全保障大統領覚書第 13 号(NSPM13)「United States Cyber Operations Policy 米国サイバー作戦政策」（内容非開示）に署名して、サイバー軍による機動的な Defend Forward 戦略の実施が可能となった。即ち、一定の作戦の決定権限が国防長官に委任され、事実上、国防長官又はサイバー軍司令官（＝NSA 長官）の判断で作戦実施が可能となったのである。決定権限が委任された作戦の範囲は、「武力の行使 use of force」に至らないもの、即ち、死者、施設の破壊、又は重大な経済的影響を及ぼすに至らないものと報道されている。従って、敵対的サイバー行為者のハッキング用或いは攻撃用のシステムに対する攻撃については、権限が委任されたと見られる。2019 年 5 月のサイバー軍司令部作戦部長ムーア少将（当時）によれば、Defend Forward 戦略に従い、一定の実施規則（rules of engagement）に基づき、米国のシステムに攻撃がなされる前に、防禦的攻撃をしているという[40]。

---

[37] John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Public Law 115–232) (13 August 2018), Section 1632.

[38] 国家安全保障法 502 条は covert action（秘密工作）について次の様に規定している。「秘密工作」を実施するには原則として大統領による事前の文書決裁（当該工作の国家安全保障上の必要性を明らかにするもの）が必要であり（同条(a)項）、且つ、上下両院の諜報委員会に報告する必要がある（秘密保全上の必要がある場合は、報告対象者を上下両院の諜報委員会の委員長と少数党指導者、下院の議長と少数党院内総務、上院の多数党院内総務と少数党院内総務の 8 人に限定することができる）（同条(c)項）。秘密の活動であっても本条の「秘密工作」から除外されるものは、①諜報を得るための活動、伝統的防諜活動など、②伝統的外交活動、伝統的軍事活動、③伝統的法執行活動、④米国諸官庁による海外における公然活動に対する支援活動である（本条(e)項）。従って、「伝統的軍事活動」と定義されると、(a)項や(c)項の手続的規制が除外される。2019 年国防授権法は、一方で規制を緩和したものの、他方で秘匿の軍事活動や軍事作戦を含むサイバー空間における軍事作戦は、上下両院国防委員会に対する 4 半期毎の報告対象である（合衆国法典第 10 篇 484 条）ことを再確認している。

[39] インテリジェンス活動としての covert action の実施については、大統領令第 12333 号「米国諜報活動」1-2（b）の規定により、国家安全保障会議による審議と勧告が必要とされている。

[40] 茂田①、80-81 頁。

Defend Forward 戦略の実施例を二つ挙げると、第1は、2018 年米国中間選挙における Synthetic Theology 作戦が挙げられる。これは 2016 年選挙でロシアが偽情報を流すなど情報作戦を展開したことを教訓に、サイバー軍と NSA が合同チームを編成してその阻止に当たったものである。具体的には、ロシアの偽情報作戦の担当者達に直接、警告メッセージを送付して担当者達の行動が露見していることを知らしめると同時に、関与組織 Internet Research Agency のサーバーをインターネットとの接続から遮断したのである[41]。第 2 は、2021 年 10 月のランサムウェアの REvil 対策である。REvil は悪名高いランサムウェア集団であるが、2021 年夏に友好国インテリジェンス機関が同集団のサーバー複数への侵入に成功して、その情報が FBI を通じサイバー軍と共有されたという。そこでサイバー軍が、REvil のダークウェブ上のウェブサイトのドメインを乗っ取ってアクセスできないようしたのである[42]。このように Defend Forward 戦略に基づく CNA（コンピュータ・ネットワーク攻撃）が行われ、一定の成果を挙げている。

なお、Defend Forward 戦略においても、その重要な要素は、攻撃を受ける前に脅威グループの脅威を解明することであり、この点において、NSA とサイバー軍は密接に協力しており、CNE とシギント活動の重要性は変わらない。

8　補足③　Defend Forward 的活動は、国際法上「軍隊」の任務か

第 7 章で見たように、米国では、サイバー脅威が自己のシステムに到達する前に、敵空間内或いはインターネット空間で阻止する活動を、Defend Forward 戦略として、サイバー軍による軍事活動として構成している。その理由は、「伝統的軍事活動」と定義しないと、covert action（秘密工作）に該当し、その実施手続が煩雑で実効性に支障が生じていたという米国国内法制上の必要からである。

ところで、一部の論者は、サイバー脅威に対して国外で対抗措置をとる行為は、国際法上「軍隊」が実施することとされていると主張する[43]。それに従えば、我が国政府が「国家安全保障戦略」で打ち出した「能動的サイバー防御」の活動は、米国の Defend Forward 同様、「国際法上」軍隊の任務ということになる。

筆者は国際法の専門家ではないので、国際法上「サイバー脅威に対して国外で対抗措置をとる行為」が軍事活動と定義されているのか否かについて広汎な知識を持ち合わせていないが、ここで一例として英国はどう定義付けているか見てみよう。

英国は、米国のサイバー軍の類似の組織として、2020 年に National Cyber Force（国家サイバー部隊）を創設した。本部隊の任務は、サイバー攻撃と共にサイバー脅威の阻止、即ち

---

[41] Julian Barnes, "U.S. Cyber Command Bolsters Allied Defenses to Impose Cost on Moscow," *The New York Times,* 7 May 2019, last accessed 15 May 2024.

[42] Ellen Nakashima and Dalton Bennett, "A ransomware gang shut down after Cybercom hijacked its site and it discovered it had been hijacked," *The Washington Post,* 3 November 2021, last accessed 15 May 2024.

[43] 例えば、大澤淳「サイバーでも反撃できない日本」（『産経新聞』2024 年 4 月 28 日付）。但し、大澤氏はその論拠を示していない。「伝統的軍事活動」という言葉に惹かれて、Defend Forward 戦略による活動は、「伝統的に」軍事活動と見做されてきたと理解したのであろうか。

「サイバー脅威に対して国外で対抗措置をとること」が挙げられている。本部隊は、国防省と GCHQ（政府通信本部）を主体に、国防科学技術研究所と SIS（秘密諜報サービス）が加わった 4 組織共同[44]の部隊であり 4 組織から要員が派遣されている。所管は、（GCHQ と SIS の主任の大臣でもある）外務大臣と国防大臣の共管である[45]。

さて、この国家サイバー部隊の活動は軍事活動と位置付けられているのであろうか。所管の大臣及び参加組織を見れば、本部隊の活動全体がインテリジェンス活動及び軍事活動として位置付けられているのは明白である。そこで、「サイバー脅威に対して国外で対抗措置をとる」活動の位置付けを詳しく見るために、同部隊の詳細な解説書[46]を見ると、同部隊の根拠法規としては、任務と責務については諜報機関法、令状と権限については同法と調査権限法及び調査権限規制法、武力紛争に至った場合は国際人道法（或は武力紛争法）が挙げられている[47]。調査権限法と調査権限規制法は、何れもインテリジェンスや警察活動における調査権限に係わる法律であるから、武力紛争に至らない場合の国家サイバー部隊の活動根拠として挙げられた法律は 3 つとも、インテリジェンス活動に関するものと言って良い。ここから判断すると、英国の国内法制においては、武力紛争に至らない「サイバー脅威に対して国外で対抗措置をとる」活動はインテリジェンス活動と位置付けられていると推定できる。

即ち、武力紛争に至らない「サイバー脅威に対して国外で対抗措置をとる」活動を、米国は軍事活動と位置付け、英国はインテリジェンス活動と位置付けているが、それは両者ともそれぞれの国内法制上の整合性からの位置付けである。ここから分かるのは、武力紛争に至らない「サイバー脅威に対して国外で対抗措置をとる」活動を、一義的に軍事活動又はインテリジェンス活動と定義する国際法なるものは存在しないのではないかということである。国によって、軍事活動、インテリジェンス活動、或いは警察活動と位置づけることもあるだろう[48]。そもそも、このような活動の法的根拠の議論自体が目新しいものであり、国際法上の位置付けはこれからの課題であろう。

（以上）

---

[44] National Cyber Force ウェブサイト, *About us*, last accessed 15 May 2024, gov.uk/government/organisations/national-cyber-force/about

[45] GCHQ と SIS の両インテリジェンス機関は、それぞれ独立組織であって英外務省の附置組織ではないが、慣例的に外務大臣が両インテリジェンス機関の主任の大臣を務めている。

[46] National Cyber Force, *The National Cyber Force: Responsible Cyber Power in Practice*, March 2023, retrieved 15 May 2024, https://assets.publishing.service.gov.uk/media/642a8886fbe620000c17dabe/Responsible_Cyber_Power_in_Practice.pdf

[47] Ibid., p.22. ; National Cyber Force, *National Cyber Force Explainer*, 13 December 2021, retrieved 15 May 2024, https://assets.publishing.service.gov.uk/media/61b9f526d3bf7f05522e302e/Force_Explainer_20211213_FINAL__1_.pdf

[48] 豪州は、対外的な攻撃的サイバー能力については、シギント機関である ASD 内に設置しているが、その活動の法律的な位置付けを軍事活動と法執行活動の 2 系統と位置づけている。従って、本稿で議論した武力紛争に至らない「サイバー脅威に対して国外で対抗措置をとる」活動については法執行活動と位置付けている可能性が高い。Fergus Hanson and Tom Uren, “Australia’s Offensive Cyber Capability,” Australian Strategic Policy Institute, 2018, accessed 16 May 2024, https://www.jstor.org/stable/resrep23053.8

また、ドイツ警察法のように強制権限の一般条項を規定している場合は、同条項を根拠に活動することも可能ではないか。

Hunt Forward 作戦とは何か

茂田　忠良

＜目次＞

1　背景 …… 45
2　HF 作戦の実施組織と実施状況 …… 46
3　HF 作戦の成果と能力の源泉 …… 47
4　ウクライナにおける HF 作戦 …… 49

米国サイバー軍は、Hunt Forward 作戦と称して、海外にチームを派遣して活動している。Hunt Forward 作戦とは、一言でいえば、ホスト国のネットワーク中の中でマルウェアなどの脅威を hunt（狩る）する活動、マルウェア狩りである。米国がわざわざ海外にまで組織的に人員を派遣してマルウェア狩りをするのは、なぜなのか、その実態や効果はどうなのか、サイバー軍の公表資料や報道を基に見てみよう。

1　背景

本作戦が開始された背景[1]は、米国が 2018 年にサイバー戦略を改定して Defend Forward 戦略を採用し、これをサイバー軍の任務としたことである。Defend Forward とは、敵対者のサイバー脅威が米国のシステムやネットワークに到達する前に可能な限り敵対者の策源地近くで対処する戦略であり、そのためには事前に敵対者のサイバー脅威を把握する必要がある[2]。

敵対者からのサイバー脅威を把握する活動としては、国家シギント機関である NSA（国家安全保障庁）のハッカー集団 TAO による C-CNE（Counter-Computer Network Exploitation）がある。ハッカー集団のシステムをハッキングすることにより、直接、ハッカー集団のハッキングツールや攻撃目標などの脅威を明らかにすることである[3]。

一方、サイバー軍の活動方針として打ち出されたのが、persistent engagement（継続的関与）である。自分のネットワークで敵対者が攻撃するのを待つのではなく、サイバー空間で敵対者と継続的に接触し、迅速に対峙する方針で、その重要な要素が Hunt Forward 作戦（以下、HF 作戦）である。つまり、米国から進出して外国のネットワーク中でマルウェア狩りをする。それによって、脅威情報をいち早く把握するとともに、関係国のサイバーセキュリティ向上にも寄与できる訳である。

---

[1] Martin Matishak, “Nakasone on the military’s cyber strategy, surveillance powers and ‘hunt forward’ missions,” *The Record,* 8 May 2023, July 2023, https://therecord.media/nakasone-cyber-strategy-section-702-hunt-forward-russia-ukraine-nato

[2] 拙著「米国 ACD・Defend Forward とシギント機関の役割～日本の『能動的サイバー防御』と対比して」（警察政策学会資料第 134 号、2024 年 6 月）第 7 章参照

[3] 拙著『国家安全保障庁の実態研究』（警察政策学会資料第 82 号、2015 年 9 月）95 - 97 頁

２　HF 作戦の実施組織と実施状況

（１）HF 作戦の実施組織

HF 作戦の実施主体は、サイバー軍の直轄部隊であるサイバー国家任務部隊（Cyber National Mission Force、以下 CNMF）である。サイバー軍は、全体で約 6200 人の組織であるが、CNMF は 2022 年 12 月現在約 2000 人の軍人とシビリアンで構成されている。前のサイバー軍司令官ナカソネ陸軍大将、そして現在のサイバー軍司令官ホー空軍大将も共に CNMF 司令官を経験しており、CNMF がサイバー軍の中核組織であることが分かる。

（２）HF 作戦の実施状況

現在までの HF 作戦の実施状況を見ると、2018 年に作戦開始以来 2023 年まで、27 カ国にチームを 55 回派遣し、75 以上のネットワークを調査している[4]。2023 年中には、22 回派遣しており、活動が活発になって来ている[5]。

HF 作戦はホスト国とネットワーク管理者の同意を得て行うものである。また派遣先の国名はホスト国の同意がなければ公表されない。政治的な考慮から、米サイバー軍の人員が来て活動したことを知られたくない国もあるからである。現在判明している派遣先は、ウクライナ、リトアニア、エストニア、ラトビア、クロアチア、モンテネグロ、北マケドニア、アルバニアであるが、他に中南米、アフリカ、中近東を含むアジアにも派遣されている。

チームの派遣期間は通常 2～3 月間であるが、現在、常に 6～10 チームが HF 作戦に派遣されている。その効果が高いためか、派遣を要請する国が増加しているという。

（３）活動手順[6]

派遣チームの具体的な活動手順であるが、通常は、先ず先遣隊を 10 日程派遣する。ホスト国の担当者との協議で必要な情報を交換して、調査対象のネットワーク図や必要なデータを入手して、一旦帰国する。そこで、調査の詳細計画を作成して、必要な機材を準備する。その後、本隊チームが機材を持って派遣される。ホスト国では担当組織とネットワーク管理者の同意を得て、調査対象のネットワークに機材を接続する。そして、マルウェアが隠れていないか、外部から侵入されていないか、システムに脆弱なところはないかなど脅威を調査するのである。この調査は、派遣チームのネットワーク分析官、マルウェア分析官、そして

---

[4] Cyber National Mission Force Public Affairs, “About the Cyber National Mission Forces,” *News,* 6 December 2023, accessed 23 May 2024, https://www.cybercom.mil/Media/News/Article/3610711/about-the-cyber-national-mission-forces/
—US Cyber Com, *2023 POSTURE STATEMENT OF GENERAL PAUL M. NAKASONE*, 7 May 2023, accessed July 2023, https://www.cybercom.mil/Media/News/Article/3320195/2023-posture-statement-of-general-paul-m-nakasone/

[5] Chris Riotta, “US Cyber Command Expanded 'Hunt Forward' Operations in 2023,” *bank info security,* 12 April 2024, accessed 23 May 2024, https://www.bankinfosecurity.com/us-cyber-command-expanded-hunt-forward-operations-in-2023-a-24851

[6] US Cyber Command, “CYBER 101: Hunt Forward Operations,” *News,* 15 November 2022, last accessed 22 May 2024, https://www.960cyber.afrc.af.mil/News/Article-Display/Article/3219164/cyber-101-hunt-forward-operations/

ホスト国の分析官などが協力して当たることになっている。

マルウェアやシステムの脆弱性、不適当箇所を発見した場合には、ホスト国担当者に知らせて、マルウェアの除去などの作業はホスト国に任せる。その際、派遣チームはネットワークをより安全にするための助言をするが、この助言は派遣チームの HF 作戦の経験や、IT 業界のベストプラクティスに基づく助言なので、納得してもらえるそうである。

なお、持参する機材は、特別な秘密の機材ではなく、商用機材である。それであれば、ホスト国の担当者も使えるからである。

この作業は、大体、ホスト国の担当者と協同して行うが、信頼関係ができるまでは、ホスト国の担当者も米国派遣チームが知らない間にバックドアを仕掛けるのではと疑念を持って監視する場合もあるという。

（４）対象脅威

HF 作戦が対象とする脅威は主に国家プレーヤであり、ロシアと中国が最大の脅威で、次にイランと北朝鮮。また他に、国際犯罪組織の脅威もある。

３　HF 作戦の成果と能力の源泉

（１）HF 作戦の成果

HF 作戦の成果であるが、先ず当然のことながら、派遣先国のサイバーセキュリティの向上がある。

他方、米国にとっての成果もある。それは、敵対国のサイバー攻撃の戦術 tactics、技術 techniques、手順 procedures を探知把握し知識経験を蓄積して、それを米国のセキュリティ強化に役立てることである。実際、マルウェアについては、敵対国は、米国のネットワークに対して使う前に、米国外でテストする傾向があるという。そこで米国としては、HF 作戦によって、国外でいち早くマルウェアを入手して自国防衛のため対策を講じることができるのである。

サイバー軍は、HF 作戦で探知した知見やマルウェアを、FBI や DHS（CISA）、そして民間企業とも共有する。2018 年以来、HF 作戦で入手したマルウェア・サンプル 90 以上をサイバーセキュリティ関係者に開示している。 なお、ホスト国の中には、感謝の印として、米国派遣チームにマルウェアを提供する例もあるという。そのマルウェアは、米国派遣チームの調査対象ではない別のネットワークから、ホスト国担当者が独自に発見したものであるが、米国派遣チームにとっては最高のプレゼントである。

（２）能力の源泉

HF 作戦に従事する国家任務部隊 CNMF の能力の源泉はどこにあるのだろうか。2023 年 6 月の CNMF 司令官のハートマン少将（当時）のインタヴュー[7]によれば、第 1 に NSA サ

[7] Dina Temple-Raston, “Exclusive: Inside an American hunt forward operation in Ukraine,” *The World,* 30 June 2023, accessed 20 July 2023, https://theworld.org/stories/2023-06-30/exclusive-

イバーセキュリティ局との緊密な協力である。CNMF は NSA 本部とフォートミード基地で同居しているので、サイバーセキュリティ局が保有する敵対国のシギント部隊（ハッカー集団）についての情報を容易に入手できる。第 2 に民間企業との協力である。NSA は民間企業との協力組織 Cybersecurity Collaboration Center（サイバーセキュリティ協働センター）を設置している。その目的は、NSA のシギント活動から得た機密の知見と民間企業の持つ脅威情報・専門技術とを総合して、脅威対抗のための有効情報を民間企業に迅速に提供することである。2023 年 6 月現在の参加企業は、IT 企業、サイバーセキュリティ企業など 500 社近くに及んでいる。CNMF はそこに「Under Advisement（相談中、又は検討中）」と称するチームを派遣して民間企業からの情報収集に努めている。ハートマン少将によれば、米国の民間企業のサイバーセキュリティ能力は極めて高いそうである。NSA や民間企業との協力から、HF 作戦に従事するチームは、派遣前に、（敵対国の）容疑性の高い特定 IP アドレス情報を入手し、或は、既知のマルウェアの特徴指標（signatures）を集めたキットを持参するのである。

更に、HF 作戦の派遣チームの能力自体が向上している。メンバー個人もそれまでの HF 作戦で得た経験を蓄積している。2023 年現在、各回の派遣チーム員の半数は派遣経験者であるという。また、経験を基礎に訓練方法も向上し、一定の対処法が定着している。その結果、以前は 60 日間の派遣任務で対象ネットワークに本当に詳しくなるのに 50 日も掛っていたが、現在は 2 週間以内で成果が上がるようになっているという。

（３）「Under Advisement」

最後に「Under Advisement」の活動について、2023 年 6 月の隊長シールズ中佐の取材記事[8]を基に説明する。

「Under Advisement」の発端は、2020 年米大統領選挙のサイバー防衛である。当時、IT 業界から、大統領選挙を外国の不当な干渉から守るために協力の意向が寄せられた。そして、IT 民間企業はシステムへの侵入（Compromise）徴候や潜在的悪意あるサイバー活動の情報を提供したのである。これを契機に、民間企業も政府も同様にサイバー攻撃を受けているのだから、互いに協力しようという機運が高まったそうである。「Under Advisement」はその民間との協力の窓口である。成果が大きいために、人員は 2023 年現在 12 人であるが、2024 年には倍増する予定であった。

その成果としては、例えば、サイバー軍は 2022 年には、民間企業 22 社と協力して、悪意あるサイバー活動の特徴指標 149 を提供した。これに対して、民間企業は、怪しい IP アドレス情報やマルウェアの断片を「Under Advisement」に持ち込んでくる。それが外国のものと判定されれば、他の企業や政府諸機関と共有し、HF 作戦の担当チームにも提供される。他方、HF 作戦チームが海外で新種のマルウェアを発見すれば、「Under Advisement」

---

inside-american-hunt-forward-operation-ukraine

[8] Martin Matishak, “Cyber Command to expand 'canary in the coal mine' unit working with private sector,” *The Record*, 28 June 2023, last accessed 22 May 2024, https://therecord.media/cyber-command-under-advisement-team-cyberthreat-collaboration

が NSA の Cybersecurity Collaboration Center（サイバーセキュリティ協働センター）を通じて民間企業に警告を発し、民間企業は攻撃される前に対策を採れるわけである。

米国企業は収益重視の印象があるが、やはり国益のためには国に協力していることが伺える。

4　ウクライナにおける HF 作戦

HF 作戦の典型例として、ウクライナの例を取り上げる。ウクライナでは 2022 年 2 月のロシアの全面侵攻直前から HF 作戦が実施されていたのであるが、この HF 作戦について、サイバー軍の CNMF 司令官ハートマン少将（当時）のインタヴュー記事[9]に基づいて説明する。

（1）HF 作戦の実施状況

ウクライナにおける HF 作戦は、2018 年に HF 作戦自体が始まって以来複数回行われているが、ロシア軍の全面侵攻直前の 2021 年 12 月から 2022 年 2 月末までと、正に全面侵攻開始の時期にも行われた。

HF 作戦の通常の手順では、先遣隊を 1 週間～10 日間程派遣して予備調査を実施する。ウクライナでは、2021 年 12 月初旬に海兵少佐（勤務経験 12 年の女性）指揮で先遣隊が派遣されたが、同海兵少佐は現地で、情勢が緊迫して時間が足りず、通常手順では HF 作戦の実施が間に合わないと判断した。そこで、計画を変更して、先遣隊はそのまま残留し、即座に本隊を派遣するように要請したのであるが、サイバー国家任務部隊 CNMF 本部はその要請に応えた。米国では 12 月下旬はクリスマスの休暇期間で家族と一緒に過ごすのが恒例であるが、隊員はそれを諦めたのである。その時のウクライナへの派遣チームは約 40 人[10]と、HF 作戦史上最多となった。

ウクライナでは、派遣チームは 3 つのネットワークを担当して、マルウェア等の調査に取り組んだが、2022 年 1 月中旬には、ロシアによるウクライナに対するサイバー攻撃第一波が始まった。これは数十のネットワークに対するワイパー攻撃でネットワークの機能を麻痺させるマルウェアである。そこで、HF 作戦チームは、ワイパー攻撃対処の支援にも取り組んだ。現地でマルウェアの分析に協力し、同時に米国に送付して米政府と米民間企業とも情報を共有したのである。米国に対する大規模ワイパー攻撃が行われる可能性もあり、米国におけるサイバー防衛態勢を整えるためにも必要だった。当時は、数日にしてキーウは占領されると予測されていた時期で、その中で HF 作戦チームは危険を冒してロシアの全面侵攻（2 月 24 日開始）後の 2 月末までウクライナに残留して活動したのである。この間、現地の派遣チームから本部に対して滞在期間の延長要請が 2 度もあったいう。その結果、ウク

---

[9] Dina Temple-Raston, ibid.

[10] Gordon Corera," Inside a US military cyber team's defence of Ukraine," *BBC,* 30 October 2022, last accessed 22 May 2024, https://www.bbc.com/news/uk-63328398;
US Cyber Command, "Before the Invasion: Hunt Forward Operations in Ukraine," *News*, 28 November 2022, accessed July 2023,
https://www.cybercom.mil/Media/News/Article/3229136/before-the-invasion-hunt-forward-operations-in-ukraine/

ライナ担当者との絆は深まり、その後も相互に連絡を取って協力しているという。

（２）HF 作戦の成果

HF 作戦チームがウクライナで挙げた成果は 2 つ挙げられる。第 1 に、派遣チームが担当して調査した 3 つのネットワークは、2022 年 1 月中旬のワイパー攻撃の被害を受けなかったことである。第 2 に、ウクライナ当局との協力で相当量のマルウェアを入手したこと、そして、侵入（compromise）の特徴指標を 6000 以上共有できたことである。これらの情報は米国の民間協力企業もアクセス可能である。

ウクライナは 2014 年のロシアのサイバー攻撃には適切に対処できなかったが、今回は上手く対処できている。ハートマン少将によれば、その要因は第 1 に、ウクライナ自身の努力である。米サイバー軍は 2018 年に HF 作戦チームの派遣を始めたが、それ以降のウクライナの取組を見ても、ウクライナは資源を投入して強靭さを向上させてきたのである。第 2 に、外部の協力であり、米サイバー軍、NATO 諸国担当者、そして米国企業からの支援が大きな役割を果たしている。その中でも米企業は素晴らしい支援をしており、特に（マイクロソフト社やアマゾンウェブサービス社による）データのクラウド化支援は重要だったそうである。

ロシア・ウクライナ戦争では、2022 年 6 月に NSA 長官兼サイバー軍司令官ナカソネ大将（当時）が、米国は防禦作戦、攻撃作戦、情報作戦の全ての領域で作戦を実施してきたと述べている[11]が、その一端が、防禦作戦中の Hunt Forward 作戦である[12]。

---

[11] Alexander Martin, “US military hackers conducting offensive operations in support of Ukraine, says head of Cyber Command,” *Sky News,* 1 June 2022, accessed 2 June 2023, https://news.sky.com/story/us-military-hackers-conducting-offensive-operations-in-support-of-ukraine-says-head-of-cyber-command-12625139

[12] 上記以外の参考資料は次の通り。

■ Suzanne Smallery, “Nakasone says Cyber Command did nine ‘hunt forward’ ops last year, including Ukraine,” *CyberScoop. Com*, 4 May 2022, accessed July 2023, https://cyberscoop.com/nakasone-persistent-engagement-hunt-forward-nine-teams-ukraine/

■ Dustin Vols, “Russia’s War on Ukraine Deepens International Cyber-Defense Cooperation,” *The Wall Street Journal,* 6 September 2022, accessed July 2023, https://www.wsj.com/articles/russias-war-on-ukraine-deepens-international-cyber-defense-cooperation-11662436289

■ Martin Matishak, “Cyber National Mission Force elevated in fight against foreign hackers,” *The Record*, 19 December 2022, accessed July 2023, https://therecord.media/cyber-national-mission-force-elevated-in-fight-against-foreign-hackers,

■ Colin Demarest, “US cyber team unearths malware during ‘hunt-forward’ mission in Latvia,” *C4ISRNET*, 11 May 2023, accessed July 2023, https://www.c4isrnet.com/cyber/2023/05/10/us-cyber-team-unearths-malware-during-hunt-forward-mission-in-latvia/

■ *Fact Sheet: 2023 DoD Cyber Strategy,* undated, accessed July 2023, https://media.defense.gov/2023/May/26/2003231006/-1/-1/1/2023-DOD-CYBER-STRATEGY-FACT-SHEET.PDF

■ Mark Pomerleau,“DOD sends new cyber strategy to Congress, releases unclassified fact sheet,” *DefenseScoop*, 26 May 2023, accessed July 2023, https://defensescoop.com/2023/05/26/dod-sends-new-cyber-strategy-to-congress-releases-unclassified-fact-sheet/

■ Mark Pomerleau, “US Cyber Command conducts ‘hunt forward’ mission in Latin America for first time, official says,” *DefenseScoop,* 8 June 2023, updated 9 June 2023, accessed July 2023, https://defensescoop.com/2023/06/08/us-cyber-command-conducts-hunt-forward-mission-in-latin-america-for-first-time-official-says/

米国サイバー任務部隊（通称、サイバー軍）の惨状と教訓

茂田 忠良

＜目次＞

はじめに …… 51
1　サイバー司令部、サイバー任務部隊の概況 …… 52
2　面接調査に現れた課題 …… 53
3　まとめと教訓 …… 58

はじめに[1]

米国サイバー司令部（Cyber Command[2]）は、2010 年に発足し 2018 年には国防長官に直結する戦闘司令部に格上げされた。報道によれば、Hunt Forward 作戦というマルウェア狩りを多数の国で実施してきた他、2018 年米中間選挙ではロシアの情報工作組織のサーバーのインターネットへの接続を遮断したり、2021 年にはランサムウェアの REvil のウェブサイトを遮断したり、Defend Forward（前方防禦）戦略で実績を挙げ、順調に実力を強化しているように見えた。しかし、実情はどうも異なるようである。

2024 年 3 月 25 日にサイバー司令部麾下のサイバー任務部隊（Cyber Mission Force）の実情について衝撃的な報告書が発表された。報告書は、国家安全保障分野のシンクタンク「民主主義防衛基金」（Foundation for Defense of Democracies）の「米国サイバー軍～国防で必須なこと」（United States Cyber Force: A Defense Imperative）[3]で、執筆者は、コロンビア大学のエリカ・ロナガン博士とマーク・モンゴメリー退役海軍少将である。

本報告書は、76 人の現役・退役軍人と国防総省シビリアンに対する面接調査を行って、サイバー司令部麾下部隊の現状を詳細に分析している。結果は、現状は余りにも多くの問題点を抱えており、むしろ「惨憺たる」と形容しても良いほどのものである。その主因はサイバー分野の専門性に適合しない人事・教育・装備体系であり、現状では真の専門家集団を養成することは難しいというものである。

我が国でも 2022 年に陸海空自衛隊の統合部隊としてサイバー防衛隊が創設されている。本報告書は米国に関するものではあるが、そこに示された課題と教訓は、我が国にとっても

---

[1] 本報告書は、2024 年 4 月 13 日のサイバーセキュリティ法制学会の研究会において、永野秀雄理事長の発表で紹介されたものであるが、筆者が同教授の了解を得て、より詳しい分析・まとめを行ったものである。

[2] Cyber Command は通常、「サイバー軍」或は「サイバー軍司令部」と訳されることが多いが、本論考では、軍種と戦闘司令部の機能の違いが議論の焦点であるので、戦闘司令部としての Cyber Command は「サイバー司令部」、軍種としての Cyber Force を「サイバー軍」と訳すこととする。

[3] Erica Lonergan and Mark Montgomery, *United States Cyber Force: A Defense Imperative,* Foundation for Defense of Democracies, 25 March 2024.

貴重な「他山の石」となるのではないかと考える。そこで、本報告書（40 頁）の概要を要約して紹介したい。

１　サイバー司令部、サイバー任務部隊の概況

米軍は 1986 年に、戦力生成機能（force generation）と戦力運用機能（force deployment）を分離している。戦力生成とは、兵士を採用し訓練し装備する機能であり、現在は陸軍、海軍、空軍、海兵隊、宇宙軍がこれを担当している。これに対して、戦力運用は、戦闘司令部（Combatant Command）が各軍種から必要な戦力の提供を受けて実施する機能であり、地域戦闘司令部と機能的戦闘司令部の 2 種類がある。地域戦闘司令部は、アフリカ司令部、中央司令部、欧州司令部、インド太平洋司令部、北方司令部、南方司令部、宇宙司令部の 7 つがあり、機能的戦闘司令部には、サイバー司令部、特殊作戦司令部、戦略司令部、輸送司令部の 4 つがある。

サイバー司令部は、2010 年に発足したが、2018 年に国防長官に直結する機能的戦闘司令部 11 の内の 1 つに昇格しており、サイバー作戦を実施する責任を負っているが、そのための戦力は、陸海空軍・海兵隊の 4 軍種から提供を受ける形になっている。

サイバー司令部麾下の「サイバー任務部隊」（Cyber Mission Force）は、現在、人員 6200 人で、①「サイバー国家任務部隊 CNMF」13 チーム、②「サイバー戦闘任務チーム CCMT」27 個、③「サイバー防護チーム CPT」68 個、④「サイバー支援チーム CST」25 個、合計 133 チームからなっている。「国家任務部隊」の任務は、敵の行動を監視し、攻撃を阻止し、勝利するためにサイバー空間で活動することである。作戦の大部分は、他の戦闘司令部の支援ではなく、独自作戦として実行されている。「戦闘任務チーム」の任務は、他の戦闘司令部の作戦支援のための軍事的サイバー作戦の実行である。「防護チーム」の任務は、国防総省や戦闘司令部の情報ネットワークの防護、優先任務の保護、戦闘任務の準備である。「支援チーム」の任務は、「国家任務部隊」や「戦闘任務チーム」を分析や計画能力面で支援することである。

2018 年にサイバー司令部のサイバー任務部隊 133 チームは、完全作戦能力（full operational capacity）を獲得したと認定され、一人前の部隊となったと見られていた。しかし、本報告書によれば、実態は、限定された有能な人員を各チームの間を移動させて各チームの作戦能力達成を認定するという誤魔化しの認定であったという。

また、現状の 133 チームに加えて、14 チームを 2022 年から 2026 年の間に増強する予定であったが、2023 年半ばの段階で、人材不足のため実現延期を決定せざるを得なくなった。2022 年には、サイバー任務部隊 7000 人への増員が報道されていたが、まだ実行に着手されていないのである。（注：現状の定員 6200 人でさえ能力を充足できていないのであるから、当然であろう。）

更に、2024 年度予算におけるサイバー司令部の要求額は約 29 億ドルであるが、国防総省の「サイバー空間活動予算」（Cyberspace Activities Budget）は 135 億ドルであり、予算の多くは各軍予算に計上されている。そして、サイバー司令部は、装備資機材の調達、資機材

の研究開発、サイバー作戦のためのインフラ面で、各軍、時にはNSA（国家安全保障庁）にまで依存している。

なお、2018年夏成立した2019年国防授権法によって、サイバー作戦が「伝統的軍事活動」と定義され、国防総省（つまりサイバー司令部）に、米国政府と米国民をサイバー攻撃から守るため国外のサイバー空間で行動する権限が付与された。その後、サイバー司令部は、Hunt Forward作戦を実施したり、米国の選挙防衛[4]、アルバニアにおけるイラン・ハッカーへの対処、ウクライナへのサイバー支援など重要な作戦上の成功を収めたりしてきたが、これらの成果の背後には多くの課題が隠されていたのである。実際、2023年12月の連邦議会公聴会で、サイバー司令官兼NSA長官（当時）のナカソネ大将は、「米国のサイバー作戦の現状は維持できない。現状以外の選択肢を取る必要がある」旨を述べているのである。

それでは、報告書に基づいて、サイバー司令部麾下のサイバー任務部隊の課題を見ていこう。

２　面接調査に現れた課題

サイバー司令部麾下のサイバー任務部隊での勤務経験のある現役、予備役、退役の軍人のインタビューを基に、課題を見ていこう。面接調査に応じた軍人の発言を多く引用しているが、理解し易いように、意訳した部分が多いことを附言しておく。

（１）総論

現在のシステムは、戦力運営はサイバー司令部の責任で、戦力生成は５軍種に分散されているが、このシステムは、訓練や資機材調達面で、サイバー分野に特有な必要を満たせていないというのが面接調査の結論である。

○　某将官は「現在の戦略、即ち、必要なサイバー専門能力を既存の各軍種に依存する戦略は、非効率的、非効果的で成功しそうもない。唯一の有効な方策は、サイバー空間に必要な組織、訓練、装備に特化した新しい軍種を創設することである」と述べている。

　サイバー分野は、特に高度なレベルの技術的訓練を必要としている。某空軍中佐は、現在のサイバー任務部隊では「10%の人員が 90%の成果を挙げている」と述べている[5]。（注：つまり、人員の90%は、能力技能が不十分であることを暗示している。）

○　また、装備資機材の調達も、技術は日進月歩なので、既存軍種とは比較にならない程に迅速に実行しなければ瞬時に陳腐化してしまう。また、多くの最新の先端技術が既存軍需産業の外の民間部門にある。更に、サイバー分野では、制服組ではないシビリアンに、より大きな役割の可能性がある。（注：シビリアンの重要性の指摘には注目を要する。）

○　課題の根本には、既存の各軍種がサイバー分野を最重要分野として位置付けていない

[4] 2018年米国中間選挙の対策など、サイバー司令部とNSAの共同作戦が行われているが、共同作戦の背景には、NSAのシギント・インフラの活用の他に、サイバー司令部側の人材不足が存在すると見られる。

[5] 本報告書の付属資料では、某陸軍大佐は「10%の人員が 80%の作戦任務を果たしている」と述べている。

ことがある。某退役海軍大佐によれば、この根本的な齟齬が、「各レベルでのサイバー作戦に対するバラバラな対応に現れている。人事の一貫性の欠如、キャリアパスの不確かさ、経験の不足、幹部の多くがサイバー未経験者であること、サイバー作戦を支援的な作戦と位置付けること」などを弊害として例示している。

それでは、以下、採用、人事計画、昇任制度、装備資機材など、各分野別に課題を詳細に見ていくこととする。

（２）採用と継続雇用の課題

現在、有能なサイバー人材を必要数、採用し、雇用を継続することが出来ていない。某空軍大佐は「サイバー任務部隊に必要な有能な人材の欠如が、発足以来の重大な限定要因である」と述べている。

○　シビリアン官庁は、給与は民間に及ばないまでも、サイバー人材を柔軟に昇任させるなど処遇に努力している。これに対して、各軍種は、手当その他の既存の報奨制度すら十分使いこなしていない。某陸軍大尉によれば、「サイバー司令部は、報奨制度を自ら運用する権限がない。他方、権限を持っている各軍種は、サイバー分野が各軍種にとっては最重要分野ではないため、報奨制度をサイバー人材に優先して適用しようとしない」という。

○　また、各軍種によって処遇に格差がある。同じ経験を持つ同一職場の勤務員でも軍種によって給与や報奨制度が異なっているのである。同じ 4，5 年間の勤務経験を有し同一職場で同一任務に従事している兵士の月給が、軍種によって 700 ドル（現在の為替レートで 10 万円）以上もの差がある。更にこれに住居手当や（サイバー業務手当などの）各種報奨制度の各軍種での適用格差が加わる。その上、その報奨制度の運用の実態が、必ずしも、個々の兵士の専門能力に対応したものになっていないのである。

○　その結果、継続雇用（任期延長）率は、極めて低い。某退役海軍大佐によれば、「継続雇用率は、悲惨な状況である。人材が流失している最大要因は、サイバー勤務員が重要扱いされていないと感じるからである。」そして、某退役陸軍大佐はその例証として、「戦闘部隊の上級将校が、サイバー研究を『読書感想文』と呼んだり、サイバー勤務員を『おたく[6]』と呼んだりするのを聞いたことがある」と述べている。

（３）人事計画、技能、訓練面での一貫性の欠如

各軍種がサイバー司令部に提供する勤務員の初期訓練は、各軍種の学校で実施されているが、訓練内容が各軍種間で標準化されておらず、内容も不十分である。

○　陸軍と空軍は、従来からサイバー作戦に特化した将校を養成したきたが、海軍は、2023 年に至るまでサイバー作戦担当将校とインテリジェンス・情報作戦担当将校を一括していたので、専門能力の向上を阻害してきた。

○　某海軍大佐によれば、「各軍種は、それぞれ独自の訓練モデルと道筋を持っていて、軍種間で訓練内容の一部は共通するものの大部分は同期していない。軍種によって訓練の到達目標が異なっており、共通の全体像が欠けている。各軍種がそれぞれの異なるキャリ

[6] nerd

アパスを優先するため、現状の訓練では、不均衡で非効果的な部隊を創り続けるであろう」と述べている。

また、某海軍少佐は「調査分析、機材開発、企画など各軍種とも同種の業務を行う勤務員を養成しているが、軍種間で訓練内容の標準化が全く行われていない。これが、技術的専門性や訓練に関して解決不可能な障碍を生み出しており、これでは一体的で統合されたサイバー任務部隊の構築は不可能である」旨を述べている。

○　多くの将校が訓練内容の専門特化の欠如を挙げている。個別具体に特化した訓練ではなく、一般的概論的な訓練になってしまっている。例えば、システム運用であれば、特定のシステムの運用技法を訓練するのではなく、システム運用の概論になっている。空軍パイロットの訓練に例えれば、本人が操縦する特定機種について訓練するのではなく、航空機全機種について概論を教えているようなものであるという。

某空軍少佐は次の様に述べている。「空軍は、真の専門的能力の養成ではなく、机上の要求を満たすことを重要視している。『サイエンス・フィクションではない。日々の業務だ』というスローガンに魅せられてサイバー分野を選択した。しかし、サイバー将校としての初期教育は、多くの民間企業が提供するものより低レベルの基本訓練であり、機材は自分が自宅用に買ったものより低レベルの性能であった。」[7]

○　サイバー将校への投資が少ない。ランド研究所の報告によれば、空軍の戦闘機パイロットの初期訓練費用は 1 人 560 万から 1090 万ドル、海軍・海兵隊のパイロットの年間訓練費用は 1 人 220 万ドルであるが、議会監査局（GAO）によれば、サイバー工作員（interactive on-net operator）の訓練費用は、1 人 22 万ドルから 50 万ドルに過ぎない。

○　各軍種とも将校団の継続訓練が欠如している。2023 年国防大学の報告書は、サイバー分野は変化が速いので、18 から 24 ヵ月毎に技術的訓練を反復継続して行う必要があるとしているが、行われていない。

○　サイバー人材が、サイバー司令部と各軍種間を異動する場合に、その人事を追跡するシステムが存在しない。そのために、各軍種に戻った際にサイバー分野に従事するかどうかが不明であり、サイバー分野での継続勤務が保証されていない。

（４）必要とする専門能力に昇任制度が見合っていない

各軍種が昇任権限を持っているが、各軍種の昇進制度は非サイバー分野に適合したものであり、専門能力よりも指揮経験に重きを置いている。その結果、各軍種には、指揮能力は優れているかも知れないがサイバー分野の技能や経験を持たない将校、下士官が満ち溢れている。

他方、某空軍中尉は「現在の昇任制度は、サイバー分野の最適任の専門家が彼を必要とする高度に技術的な職務に就けない制度となっている。昇任するには、指揮経験を積むためにサイバー分野から転出しなければならない。」と語っている。

○　各軍種の標準的な昇任制度では、昇任に一定の職務経験を要求しているが、これはしばしばサイバー司令部で必要とする能力とは無関係である。例えば、陸軍では小隊長

[7] 本報告書の付属資料

（platoon leader）を経験しないと大尉には昇任できない。その結果、技術に秀でたサイバー工作員（cyber operator）の多くは、小隊長を経験しないので昇任できない一方で、サイバー専門能力のない将校が上司として配属される結果になる。

○　また、各軍種の人事管理担当者には、サイバー分野の知識が欠落している。某陸軍大佐は、「人事担当者には、一流教育機関の高度なコンピュータサイエンスの学位と情報管理のオンライン講座の終了証の違いさえ分からない者がいる。脳外科医と衛生兵を同一視するようなものだ。」と語っている。

○　海軍予備役少佐エリック・セリグマン氏の某軍事雑誌 2023 年 6 月号への寄稿によれば、サイバー戦争未経験の将校達が、サイバー作戦ではリスク評価をしている。彼らは、自ら決定できず、部下の配置が不適切で、作戦目的達成に必要な技術的方策を実行できない。サイバー戦争の理論や方針を理解しても、実地体験には代えられない。このような将校は「自動小銃の概念や威力を学習したが、一度も射撃したことのない将校」のようなものである。

某海兵隊大尉によれば、「サイバー分野における指揮は、12 ヵ月の学校教育では教えられない技術的能力を必要とする。どんな状況であろうともサイバー将校に戦闘機中隊の指揮はさせないだろうが、その逆は平然と行われているのである。」

○　サイバー司令部発足以来 13 年も経過したが、サイバー分野には同分野の経験が殆どない高級将校がたくさんいる。2023 年夏時点でサイバー分野に関与する米軍の将軍は 45 人いるが、その内サイバー分野の技術的な経験を有する者は 5 人未満である。一方、某空軍中佐は「有能なサイバー攻撃作戦の経験者で、大佐以上に昇任した者は殆どいない」と述べている[8]。

○　サイバー司令部には、優秀な人材がいるが、その人材を活用できていない。某海兵隊大尉は、「自分は、軍の高級幹部過程（military war-college certificate[9]）に進まずに、コンピュータサイエンスの大学院修士課程に進んだために、昇任で不利益を被っている」と語っている。

サイバー分野で優秀な者が、上級将校の実態に失望して、他の分野に転出するか、軍を辞めてしまうため、経験豊かな指導者の育成ができずにいる。

（５）種々の支援機能の欠如（業務管理、インテリジェンス、精神衛生）

○　各軍種がサイバー司令部に業務管理要員を十分提供していないため、しばしば、数少ない有能なサイバー工作員が、管理業務に従事せざるを得ない。某空軍少佐によれば、「同一チームに 1 年以上勤務しているのは、チームに 10%しかいない。そのため、少数の熟練者が、作戦遂行と新人訓練の両者を担当しており負担が重い」。陸軍サイバー司令部の 2019 年内部調査によっても、任期満了による離職理由の一つは、管理業務に精力を奪われて、本来のサイバー作戦任務に集中できないことであった。

○　「サイバー国家任務部隊[10]」が 2022 年 12 月にサイバー司令部内の統合司令部に昇格

---

[8] 本報告書の付属資料。
[9] 基本は、期間 2 年間の教育課程で、一般大学の修士相当の卒業資格を得られる。
[10] 各種報道では、サイバー国家任務部隊の人員は約 2000 名とされている。

したために、「国家任務部隊」については業務管理要員が整備されたが、サイバー司令部麾下の他の部隊、全体の 3 分の 2 は未だに業務管理支援を受けていない。

○　他軍種とは異なり、敵対国のサイバー部隊の能力と戦力組成についての基本情報を常時収集し整備する、オールソースのサイバー空間インテリジェンス・センターが今以て未設置である。2023 年にサイバー司令部は、DIA（国防諜報庁）と NSA（国家安全保障庁）の協力を得て設置すると発表したが、2024 年度予算には計上されなかった。仮に同センターが発足したとしても、その適任者をどうやって確保するのか課題が残る。

○　特殊作戦部隊、パイロットやドローン操縦員など向けに、国防総省には精神衛生保持のためのプログラムが存在するが、サイバー工作員についてはそのようなプログラムが存在しない。サイバー任務の特質を理解した精神衛生保持プログラムが必要である。

（６）各軍種の統制・干渉による作戦能力の低下

○　某将官によれば、「何年もかけて育成したサイバー工作員を、各軍種がサイバー任務外に異動させてしまう。」と述べているが、各軍種による人事権の保持が、「サイバー任務部隊」133 チームの完全作戦能力保持の障碍となっている。

○　某予備役陸軍中佐は、「国家任務部隊」における勤務経験では、「各軍種の要望に配慮して、サイバー工作員を、作戦任務から外して、当該軍種関連業務に就けざる得ないことがある。これが、士気を下げ、継続勤務の障碍となっている。」と述べている。

○　某空軍少佐は、「実員が定員の 60%以下しかいない部署に対して、軍種の 12 週間にも及ぶ生活技術基礎講習への参加割当が来たりする」。更に、「ある司令官は、空軍サイバー要員の勤務時間の 20%は空軍のもので、NSA[11]には 80%しか提供しないという不文律がある。」などと語っている。

○　某陸軍大佐によれば、「一人前のサイバー工作員を育成するのは、大変なことで何年も掛かる。漸く一人前になった所で、軍種はサイバー任務部隊からその軍種の任務に異動させてしまう。人材は、サイバー任務部隊から流出し続けている。」

○　2018 年にサイバー司令部麾下 133 チームが全て公式に完全作戦能力を獲得したとされるが、実情はほど遠い。

　そもそも、各軍種は 133 チームを充足する人員を提供していない。某陸軍大佐によれば「人材不足は作戦能力を大きく阻害しており、サイバー司令部発足以来の課題である。或るチームが完全作戦能力を獲得したと言っても、実員は 67%から 75%しかいない。」と語っている。完全作戦能力を獲得したチームですら、定員が満たされていないのである。

　また、全てのチームが完全作戦能力を獲得したように見せかけるために、有能なサイバー工作員が複数チームに重複計上されている。某陸軍大尉によれば、「完全作戦能力を獲得するために、同じ有能な勤務員がチーム間を異動している。Ａチームが達成したらＢチームに異動し、Ｂチームが達成したらＣチームに異動する。こうして、全てのチームが完

11 報告書には NSA と記述されているが、実際はサイバー司令部を指していると思われる。発言した空軍司令官の意識では、サイバー司令部麾下部隊を NSA と同一視していると見られる。

全作戦能力を達成したのであるが、では現在全てのチームが完全作戦能力を維持しているかと言えば、能力のあるチームは少ないのである。」

某陸軍予備役少佐によれば、「陸軍サイバー司令部は、全てのチームの定員が充足され訓練が完了しているように見せるために、常に数字を操作し解釈を変更し要員を異動させている。『サイバー防護チーム』の殆どは実員が定員の 75%を超えたことはなく、十分に訓練された中核グループに依存しているのである。」と語っている。

○　某陸軍少佐によれば、「サイバー司令部の直面する様々な最困難の課題に対処するために、同じ 50 人が部署を超えて様々な課題に取り組んでいる。」という。

（7）装備資機材の調達

米国軍隊では新しい装備の調達運用には通常 10～15 年かけている。しかし、サイバー分野の機材は頻繁に更新され、開発 1，2 年で陳腐化してしまう。これに、各軍種による機材の調達速度が追い付かない。結果として、サイバー司令部は旧式機材（tools）で立ち往生しており、NSA から機材を拝借せざるを得ない状況である。サイバー司令部の NSA からの分離は有害であるという評価が継続している理由である[12]。

サイバー司令部の装備資機材の調達部署は現在数十人で、各軍種に遥かに及ばない。また、某空軍少佐が言うには、「各軍種や各戦闘司令部は、それぞれがサイバー能力を調達しようとしているが、結果として、その間に重複を生じ、また、防衛企業への依存によって疑問、無駄な調達をしている」。別の某空軍少佐は、「同じ企業が 1 億ドルの製品を名前を変えて二つの軍種に売り込んでいるのを見た。各軍種の調達部門が、決して使われることのない製品に 10 億ドル以上を支出しているのも見た。資源を統合して国家的な優先順位に沿った調達をしようとしても、各軍種によって妨害されている。」と語っている。

3　まとめと教訓

米国サイバー軍は 2010 年に発足し、2018 年には国防長官に直結する戦闘司令部に格上げされた。筆者は、サイバー司令部の成果に関する報道を読んで、順調に戦力が強化されていると理解していた。また、サイバー司令部の将官達の折々のインタビュー記事もその印象を裏書きするものであった。ところが、以上見てきたように、本報告書によれば、サイバー司令

---

12 サイバー軍司令官は発足以来 NSA 長官が兼務している。筆者はその理由は、NSA の専門知識技能と世界に展開したシギント・インフラ利用による協力をサイバー司令部が必要としているためと考えていたが、本報告書によれば、更にそれ以前に、機材面での支援も受けているのである。

2018 年以降、サイバー司令部は、Defend Forward 戦略に従い、米国選挙への干渉対策などで成果を挙げているが、その多くは NSA との共同作戦となっているようである。共同作戦部署は、NSA の TAO で、CNE（コンピュータ・ネットワーク資源開拓）、いわゆるハッキングの専門集団である。TAO は情報収集のために諸外国のコンピュータ・ネットワークに侵入しているが、同時に諸外国のハッカー集団のコンピュータ・ネットワークにも侵入しているのである。本報告書の内容から判断すると、サイバー司令部の作戦では、NSA の人材支援も必要としていると見られる。

なお、本報告書の付属資料には、某陸軍大尉が「サイバー司令部と NSA 間の任務と責任の分担について共通のビジョンがない。そのため混乱が生じ、常に方針が変更される」と述べている。これが、サイバー司令部と NSA の関係の現状であるとすれば、トップの兼任解除などができる状態ではないことが分かる。

部の実情は惨憺たるもので、現状を放置できない程のものであることが明らかにされた[13]。

（１）報告書の提言

本報告書は、諸課題を解決するには、新たな軍種としてサイバー軍を創設して、サイバー戦力の生成機能を担当させる必要があるとしている。具体的には、現在のサイバー司令部麾下のサイバー任務部隊 6200 人の他に、各軍種に分散しているサイバー戦力の生成機能を移管する。つまり、人事管理機能、教育訓練機能、装備資機材の開発調達機能などを、担当人員と共に移管して、初期人員 1 万人規模での発足を提言している。設置場所としては、陸軍省を提示しているが、現在、海兵隊は海軍省、宇宙軍は空軍省に置かれれている例に倣うものである。

本報告書は、この改革によって、各種の課題が解決できるとしているが、興味深いのは、人事において、有能な民間人を将校として直接採用ができるとしている点である。これは、第二次世界大戦前に、米国陸軍のコミント機関が、民間の優秀な数学者や言語学者を採用して暗号解読で成果を挙げた故事を想起させる。また、本報告書は、軍種としてのサイバー軍創設が、NSA にも利益をもたらすとしている。現在、NSA で勤務する軍人は各軍種から提供されているが、サイバー軍種が創設されれば、サイバー軍種で訓練を受けた現在よりも能力の高い軍人の提供を受けられるとしている。

（２）教訓

本報告書の最大の教訓は、サイバー分野のように特殊な専門能力を必要とする部門には、通常の軍種の人事・教育・装備体系は適合しないということである。

そこで、同様に高度な専門能力を必要とする NSA を見てみよう。我が国には、NSA が国防総省に置かれているために、軍事情報機関と位置付ける者がいる。しかし、NSA は、シビリアン主体の国家シギント機関なのである。本報告書でも、NSA 勤務員の 4 分の 1 が軍人であるとしており、従って大多数の 4 分の 3 はシビリアンであり、シビリアン主体の組織である。2018 年時点の報道によれば、NSA の勤務員は全体で約 5 万 5 千人、内、約 4 万人が派遣職員を含むシビリアンで、1 万 5 千人弱が軍人であった。NSA 長官が軍人であるので、NSA は軍人が中核となって多数のシビリアンを指揮していると誤解する者がいるが、軍人の多くは現場の収集拠点の勤務員であり、NSA 本部の主体はシビリアンなのである。つまり、NSA の専門性を支えているのはシビリアンなのである[14]。そして、そのシビリアンの人事は 1959 年以来、各軍種ではなく NSA の独自権限によって行われている。NSA の情報開示文書には、この人事権の独立が NSA の発展にとって重要であったと記載されている。

本報告書によれば、サイバー司令部は、今でも NSA に依存している姿が見える。つまり、シビリアン主体の専門家集団に依存しているということなのである。

---

13 秘密保全の壁に逃げ込まずに、本報告書のような課題を鋭く指摘する報告書が公刊された事実に、米国の開放性と強さが見られると考える。

14 シビリアン中心であるということは、シビリアンに軍人経験がないことを意味しない。軍人からシビリアンに転換する者もいるし、若者が軍でシギント部隊勤務を経験した後に通称 GI ビルという奨学金を得て大学を卒業した後に、NSA に就職する例もあると言われている。

なお、米国のサイバー軍に類似の組織として、英国は 2020 年に 2000 人規模の National Cyber Force（国家サイバー部隊）を設置しているが、本部隊は、国防省とシギント機関 GCHQ（政府通信本部）を主体に、国防科学技術研究所とヒューミント機関 SIS（秘密諜報サービス）が加わった 4 機関共同の部隊で 4 機関から要員の派遣を受けており、シビリアンが過半を占めるとみられる[15]。また、豪州は、攻撃的サイバー作戦部署もシギント機関 ASD（豪信号局）内に設置しているが、その人員の大部分はシビリアンである[16]。英豪両国は、サイバー作戦の専門能力をシビリアンに託しているように見える。

教訓の結論は、サイバー分野においても、インテリジェンス分野においても、特殊な専門家集団の組織を円滑に機能させるには、独自の人事・教育・装備体系が必要であり、また、シビリアンの活用が重要であるということである。

[15] 拙著「米国 ACD・Defend Forward とシギント機関の役割～日本の『能動的サイバー防御』と対比して」（警察政策学会資料第 134 号、2024 年 6 月）第 8 章参照。

[16] Fergus Hanson and Tom Uren, *Australia's Offensive Cyber Capability*, Australian Strategic Policy Institute, 2018, accessed 16 May 2024, https://www.jstor.org/stable/resrep23053.8

警察政策学会資料　第 134 号

国家安全保障に関する諸論考

令和 6（2024）年 6 月

編集　警察政策学会
　　テロ・安保問題研究部会

発行　警察政策学会

〒 102－0093
東京都千代田区平河町 1－5－5　後藤ビル 2 階
電話（03）3230－2918・(03－3230－7520)
FAX（03）3230－7007