サイバー空間における防御行為の武力紛争法上の評価

茂 木 隆 宏

1. はじめに

1.1. 問題設定の背景

1969年に現在のインターネットの起源となるARPANET（Advanced Research Projects Agency Network）[1]の運用が開始されてから、半世紀以上が経過した。この間にインターネット及び各種通信機器によって構成されるサイバー空間の利用は爆発的に拡大し、人々の生活において必要不可欠なものとなった。他方、インターネットの登場とともに出現したサイバー攻撃は、インターネットの発展に追従するように進化を続け、現在では国防に関わる分野にまで深刻な影響を与えている[2]。なお、サイバー攻撃による被害は国家の軍隊のみが直面しているわけではなく、非軍事的組織、特に官公庁や民間企業にとってBCP（事業継続計画）を考える上で看過できない問題とな

1） ARPANETとは、米国国防総省の国防高等研究計画局（DARPA）が開発した初のパケット通信ネットワークのこと。

2） 例えば、2015年には米連邦人事管理局がサイバー攻撃の被害を受け、現職・元連邦職員及び採用候補者420万人分の個人情報が閲覧された可能性があるほか、身辺調査対象者1970万人、採用候補者の配偶者など180万人の計2150万人分の社会保障番号を含む個人情報が窃取された。Office of Personnel Management, Cybersecurity Resource Center CYBERSECURITY INCIDENTS What Happened, at https://www.opm.gov/cybersecurity/cybersecurity-incidents/.

っている[3]。そのため、官公庁や企業では自組織で、またはサイバーセキュリティ企業のサービスを利用することでサイバー攻撃に対応するための体制（サイバー防御体制）を整えている。なお、サイバー防御には、ファイアウォールやウイルス対策ソフトといったサイバー攻撃対策製品による受動的な対策から、システムが出力する操作・アクセスログやセキュリティアラートの監視、サイバー攻撃を受けた際に被害を最小化し、迅速にシステムを復旧させる等の能動的な対応（いわゆる、インシデントレスポンス[4]）も含まれる。

上記の行為は、民間企業において平時から広く行われている行為であるが、行為の内容によっては軍隊によるサイバー軍事行動のような高度なサイバー攻撃にも影響を与えることができる。つまり、平時に民間企業が行っているサイバー防御を武力紛争時に実施する場合、状況によっては一方の紛争当事者の軍事行動に不利な影響を及ぼすことができ、サイバー防御を通じて意図せず文民自身が武力紛争の状況に巻き込まれることも考えられる。例えば、2022年２月24日より始まったロシアによるウクライナ侵略以降、ウクライナは数多くのサイバー攻撃に直面しているが、これらのサイバー攻撃の中にはCritical Infrastructure[5]（以下、重要インフラ）をターゲットとしたものが多

3）　2021年に発生した米国コロニアル・パイプラインへのサイバー攻撃（ランサムウェアへの感染）では、サイバー攻撃の影響範囲を封じ込めるためにパイプラインによる輸送業務を停止した。これにより、米国の一部地域へのガソリン供給が一時停止し、米国内のエネルギー安全保障に大きな影響をもたらした。Colonial Pipeline Company, Media Statement Update: Colonial Pipeline System Disruption, last update: May 17, 2021, at https://www.colpipe.com/news/press-releases/media-statement-colonial-pipeline-system-disruption. なお、2022年７月26日現在、米国外からのアクセスを遮断しているため、日本国内から上記URLへのアクセスはできない。

4）　インシデントレスポンスとは、インシデントの検知から解決までの協調的かつ体系的アプローチである。インシデントレスポンスには、インシデントの発生確認、ダメージコントロール、システムの正常復帰、加害者に対する刑事・民事訴訟への準備、将来的なサイバー攻撃に向けた予防の実施などが含まれる。Jason T. Luttgens, Matthew Pepe and Kevin Mandia（政本憲蔵、凌翔太、山﨑剛弥監訳）『インシデントレスポンス　コンピュータフォレンジックの基礎と実践　第３版』（日経BP社、2016年）６頁。

5）　重要インフラの定義は各国で異なる。米国は、化学、商業施設、通信、重要産業、ダム、防衛産業基盤、救急サービス、エネルギー、金融サービス、食料・農業、政府施設、ヘルスケア・公衆衛生、情報技術、原子炉・核物質・核廃棄物、輸送システム、水・排水システムの計16分野がサイバー攻撃対策を強化すべき重要インフラと位置付ける。Cybersecurity &

数確認されており、それらのサイバー攻撃への対応はウクライナのCERT-UAが従事している。CERT-UAはウクライナ国家特殊通信・情報保護局(SSSCIP: State Service of Special Communication and Information Protection of Ukraine)[6]の配下に位置する組織であり、サイバー攻撃によるインシデントの予防、検出、およびインシデントの解決に向けた実践的な支援や、サイバー攻撃に関するタイムリーな情報提供などを行い、平時・有事問わずウクライナ国内のサイバー空間の安全に寄与している[7]。世界中のCSIRT(Computer Security Incident Response Team)[8]が情報交換やインシデント対応に関する協力関係を構築することを目的として設立されたFIRST（Forum of Incident Response and Security Teams）によると、CERT-UAは国家の情報資源に関係する国家当局、地方当局、軍隊、国営企業等の関係者によって構成されているが[9]、CERT-UA自体は軍隊ではない。もし、軍隊に編入されていないCERT-UAが、武力紛争時に敵対する紛争当事国によるサイバー攻撃を防御し、無効化または効果を低減させた場合、CERT-UAは武力紛争法上いかなる法的地位を有するのだろうか。つまり、当該行為が敵対行為への

Infrastructure Security Agency, CRITICAL INFRASTRUCTURE SECTORS, at https://www.cisa.gov/critical-infrastructure-sectors. また、日本においては、情報通信、金融、航空、鉄道、電力、ガス、政府・行政サービス（地方公共団体を含む）、医療、水道、物流、化学、クレジット及び石油の計14分野を重要インフラと位置付けている。内閣サイバーセキュリティセンター「重要インフラの情報セキュリティ対策に係る第４次行動計画」（平成29年４月18日）、at https://www.nisc.go.jp/pdf/policy/infra/infra_rt4.pdf。

6) SSSCIPは国家通信システムである国家機密通信システムの機能と発展、暗号化記述の確保、サイバーセキュリティなどを担う国家機関である。Ukraine, Про Державну службу спеціального зв'язку та захисту інформації України（英訳：About the State Service of Special Communications and Information Protection of Ukraine),（Відомості Верховної Ради України（ВВР), 2006, №. 30, ст.258), Стаття 3, at https://zakon.rada.gov.ua/laws/show/3475-15#Text.

7) Computer Emergency Response Teams of Ukraine, Про CERT-UA（英訳：About CERT-UA), at https://cert.gov.ua/about-us.

8) 同様の活動を行う組織をCERT（Computer Emergency Response Team）と呼称する場合もある。なお、本稿では「CSIRT」の表記を用いる。

9) FIRST, CERT-UA, at https://www.first.org/members/teams/cert-ua.

直接参加と見なされ、文民が有する直接攻撃からの保護を喪失することになるのか[10]。

非軍事組織たる文民によるサイバー防御が常識となった現代においては、上記のような法的問題が生じる可能性がある。そこで本稿では、武力紛争中に文民が重要インフラのサイバー防御、特にサイバー攻撃の監視や対処といった「人が関与する防御」を行った際、武力紛争法上どのように評価されるかを整理・検討する。

なお、武力紛争法には、武力紛争における敵対行為から文民を保護し、その影響からの回復を支援することを目的とした「文民保護組織」「文民保護要員」（以下、まとめる場合は「文民保護組織・要員」と表記する）の役割が規定されている[11]。文民保護組織・要員と見なされる者は、文民を保護することを目的とした「特定の行為」を行うに際し、特別な保護を享受できる。詳細については本稿５. で触れるが、「特定の行為」には「不可欠な公共事業にかかる施設の緊急修復」なども含まれていることから、サイバー攻撃による影響への対応も文民保護組織・要員の役割と見なされる可能性があると考える。そこで、本稿では文民を保護するためにサイバー防御を担う文民の組織・要員が、文民保護組織・要員としてサイバー攻撃の対処を行うことができるのかについても注目し、検討を行う。なお、文民保護任務については軍隊構成員もその役割に就くことが可能であるが[12]、紙面の制約上、本稿では

10）　CERT-UA がロシアによるサイバー攻撃に対して警告などを行っているのは事実であるが、現時点で上記のような武力紛争法上の問題が顕在化しているとの情報はない。ロシアによるサイバー攻撃に対する対応の例としては、2022年６月５日にロシアの GRU（ロシア連邦軍参謀本部情報総局）と関係のあるサイバー攻撃集団である APT-28によるサイバー攻撃事例について、警告を行なっている。このことから、CERT-UA はロシアによるサイバー攻撃の防御や情報収集を実施していると推測できる。CERT-UA, Кібератака групи APT28 із застосуванням шкідливої програми CredoMap_v2（CERT-UA#4622）（英訳：Cyberattack by the APT28 group using CredoMap_v2 malware（CERT-UA#4622））, June 5, 2022, at https://cert.gov.ua/article/40106.

11）　ジュネーヴ第１追加議定書（以下、第１追加議定書）では第61条から第67条において文民保護に関する規定がなされている。

12）　第１追加議定書第67条。

文民が文民保護任務に従事した場合のみを扱うものとする。

1.2. 本検討における論点と狙い

民間企業は、日常的に多様なシステムのサイバー防御を行なっている。例えば、自社のECサイト[13]を運用するWebサーバへのサイバー攻撃を監視している者もいれば、電力施設や水道処理施設の基幹システムのサイバー防御を担っている者もいる。前者の例の場合、ECサイトを運用しているWebサーバが特定の軍事行動に貢献しているケースは、僅かであろう。よって、武力紛争の状況において、自社のWebサーバの防御を行うことで敵対する紛争当事国の軍事行動に不利な影響を与える可能性は限りなく低い。他方、後者の場合、一方の紛争当事者が敵対する紛争当事国内の電力を停止させる目的でサイバー攻撃を行い、当該攻撃を電力施設のサイバー防御要員が遮断、サイバー攻撃を無効化するケースが考えられる。この時、一方の紛争当事者による軍事行動としてのサイバー攻撃が失敗したことになるため、第2波以降のサイバー攻撃を成功させるために、時にはサイバー防御要員や当該人物の所在地（拠点）が戦闘に巻き込まれることも考えられる。このようなことから、本稿では軍民共用または民用物の重要インフラのシステムのサイバー防御業務に従事する組織及び個人を対象として検討を行う。

では、民用物たる重要インフラシステムのサイバー防御を行う者の法的地位を検討するにあたって考察すべき論点は何か。第1の論点は、「サイバー防御は人の法的地位、特に攻撃目標該当性[14]に影響を与えうるか」である。これまでの先行研究では、武力紛争時にサイバー攻撃を行う者の法的地位に

13) ECサイト（Electronic Commerce Site）とは、インターネット上でさまざまな商品の売買を行うことができるサイトのことである。

14) 攻撃目標該当性は、当該人物の法的地位または行為に基づいて直接の攻撃対象となり得るかどうかを表す。武力紛争法において、戦闘員は敵対行為に直接参加するための権利（戦闘員資格）を有する反面、常に合法的な攻撃目標（軍事目標）と見なされる。他方、文民は、第1追加議定書第51条1項～3項に基づき、敵対行為に直接参加していない間は軍事行動から生じる危険からの保護を享受する。ただし、敵対行為に直接参加していると見なされた場合は直接攻撃の対象となる。

ついて検討がなされる事例が多かったが、サイバー防御を行う者に関する研究例は少ない[15]。そこで、武力紛争法及びサイバー空間における攻撃と防御の定義を整理した上で、サイバー防御によって人の法的地位にいかなる影響を与えるか、つまりサイバー防御を行う者の攻撃目標該当性について検討する。

第２の論点は「サイバー防御が敵対行為への直接参加に該当する可能性があるのか、また、いかなる行為が敵対行為への直接参加に該当するか」である。後に紹介する赤十字国際委員会（以下、ICRC）による「国際人道法上の敵対行為への直接参加の概念に関する解釈指針」（以下、DPH に関する解釈指針）で示された３つの累積基準に基づくと、サイバー防御であっても敵対行為への直接参加に該当する可能性がある。よって、どのようなサイバー防御が敵対行為への直接参加に該当するかを検討することは、重要であろう。

第３の論点は「サイバー防御を行う組織や要員[16]が文民保護組織・要員と見なされる可能性があるか」である。文民保護に関する規定は、最新のものでも1977年に規定された第１追加議定書の規定であるが、当時、インターネットはごく一部の者が研究目的で利用していたに過ぎず、武力紛争の状況で使用される可能性は皆無に等しかった[17]。そのため、第１追加議定書の文民保護に関する規定はサイバー防御を念頭に置いていないと言える。そのような時代的背景がある中、果たしてサイバー空間での防御活動に第１追加議

15）　例えば、タリンマニュアルにおいても、戦闘手段に関連してサイバー防御に触れているのは、規則92「サイバー攻撃の定義」パラグラフ17、規則97「文民による敵対行為への直接参加」パラグラフ５に限られる。Michael N. Schmitt（ed.）, *Tallinn Manual 2.0 of the International Law Applicable to Cyber Operations*（Cambridge University Press, 2017）, pp. 419, 429.

16）　本報告におけるサイバー防御組織とは、サイバー攻撃への対応、具体的にはサイバー攻撃の監視（SOC）やインシデントレスポンス（CSIRT）を行う組織を指す。また、サイバー防御組織の要員とは、当該組織内でサイバー防御を行う者である。

17）　商用のインターネットが誕生したのは、1989年の PSINet の設立に始まり、それまでは学術・軍事研究用にのみインターネットが利用されていた。一般社団法人日本ネットワークインフォメーションセンター「インターネット歴史年表」（最終更新日　2022年２月28日）、at https://www.nic.ad.jp/timeline/。

定書の規定を適用できるのだろうか。

そして、第４の論点は「文民保護組織・要員が行うサイバー防御のうち、文民保護任務と見なされるものとそうでないもの（敵対行為への直接参加に該当するものを含む）は何か」である。文民保護組織・要員が行う行為の一部については、武力紛争中の敵対行為に不利な影響を与える可能性があることが長年主張されている[18]。このようなことから、文民保護任務として実施された重要インフラのサイバー防御も「敵対行為への直接参加」と同等の影響を生じさせる可能性がある。一方、文民たる住民を敵対行為から保護する上で当該任務の遂行が必要不可欠であることも、また事実である。よって、いかなる行為が文民保護組織・要員及び文民としての保護を喪失するケースであるかを検討し、文民保護任務の中に生じ得る危険性を表面化させることが必要である。

2.　サイバー空間における行為

2.1.　サイバー攻撃の概要

本稿の検討にあたり、最初にサイバー攻撃の概要について確認する。サイバー攻撃の流れについては、攻撃のフェーズを示すモデル（フレームワーク）がいくつか存在する。例えば、米国のセキュリティおよび航空宇宙企業である Lockheed Martin 社は、2009年に Cyber Kill Chain[19] と呼ばれるサイバー攻撃モデルを提唱した。Cyber Kill Chain はサイバー攻撃の流れを７つのフェーズに分類したモデルである[20]。一方、近年サイバーセキュリティ業界に

18）　例えば、消火活動が挙げられる。Yves Sandoz, Christophe Swinarski, and Bruno Zimmermann (eds.), *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949* (*ICRC, 1987*), para. 2346.

19）　Lockheed Martin, THE CYBER KILL CHAIN, at https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html.

20）　7つのフェーズは、①偵察（Reconnaissance）、②武器化（Weaponization）、③配送（Delivery）、

おいては、米国連邦政府が資金提供を行う非営利組織 MITRE が2013年に公表した MITRE ATT&CK のフレームワーク[21] が広く普及している。なお MITRE ATT&CK では、14のフェーズでサイバー攻撃の流れを整理する[22]。

このように「サイバー攻撃」と一言で言っても、サイバー攻撃の着手から攻撃の効果が生じるまでの間には、多くのフェーズを要する。そのため、近年のサイバー犯罪者は、サイバー攻撃のフェーズごとに分業するなどし、サイバー攻撃を効率的に実施できる体制を整えている[23]。

2.2.　サイバー防御の概要

インターネット空間の特性上、サイバー戦においては攻撃者が有利だと言われている。その理由として、大きく２つの点が挙げられる。第１に、インターネット空間の仕組みに基づく攻撃者の優位性である。インターネット空間は「情報を容易かつ自由に伝達・拡散することを目的として設計」[24] され

④エクスプロイト（Exploitation）、⑤インストール（Installation）、⑥ C2（Command & Control）、⑦実行（Action on Objectives）である。

21）　MITRE, ATT&CK Matrix for Enterprise, at https://attack.mitre.org/.

22）　MITER ATT&CK では、①偵察（Reconnaissance）、②リソース開発（Resource Development）、③初期アクセス（Initial Access）、④実行（Execution）、⑤永続化（Persistence）、⑥権限昇格（Privilege Escalation）、⑦防御回避（Defense Evasion）、⑧認証情報アクセス（Credential Access）、⑨探索（Discovery）、⑩横展開（Lateral Movement）、⑪収集（Collection）、⑫ C&C（Command and Control）、⑬持ち出し（Exfiltration）、⑭影響（Impact）の14フェーズでサイバー攻撃の流れを表す。

23）　分業化の一例として挙げられるのが、Initial Access Broker（初期アクセスブローカー）である。Initial Access Broker は、自身がさまざまなシステムへ侵入し、システムへのアクセスを維持、侵入先へのアクセス方法などをサイバー攻撃を行う犯罪者に売買し金銭を得るなどしている犯罪者である。例えば、2022 年 3 月 17 日、Google 社の Threat Analysis Group（TAG）が Microsoft 社の MSHTML の 0-Day を悪用している脅威アクター EXOTIC LILY を調査し、当該アクターが、FIN12 または Wizard Spider と呼ばれるロシアのサイバー犯罪ギャングと協働している Initial Access Broker であることを明らかにした。Vlad Stolyarov and Benoit Sevens, Exposing initial access broker with ties to Conti, March 17, 2022, at https://blog.google/threat-analysis-group/exposing-initial-access-broker-ties-conti/.

24）　川口貴久「第２章　サイバー空間における安全保障の現状と課題－サイバー空間の抑止力と日米同盟－」『平成25年度外務省外交・安全保障調査研究事業（調査研究事業）「グローバル・コモンズ（サイバー空間、宇宙、北極海）における日米同盟の新しい課題」』（日本国際問題研究所、平成26年３月）、16頁。

ているため、利用者が遭遇する可能性のあるリスクの対応などはインターネットの仕組みにおいて優先的に対処されていない。事実、インターネット空間及びそこに接続されるシステムにおいて、利便性とセキュリティはトレードオフの関係にある。利便性を求める場合、データへのアクセスコントロール、ウイルス対策ソフトによるスキャンなどを低いレベルに設定する必要性がある。一方、これらを高いレベルに設定する場合、何らかの作業を行うたびに認証が求められリアルタイム性が低下、システムの利便性が低下する可能性がある。また、パソコンやソフトウェアなどは人間によって設計・構築されるものであり、設定の誤りやバグが頻繁に発生し得る。攻撃者は設定の誤りやバグによる脆弱な箇所を突くことでサイバー攻撃を行う。このような設定の誤りやバグは、人間の目で確認し、全てを修正することが困難であるほか、日々新たなシステムやソフトウェアがリリースされている昨今において、すべての設定の誤りや脆弱性に対応することは極めて難しい。つまり、サイバー防御側が守る必要のある脆弱性や設定の誤りは日々発生しており、サイバー攻撃者は世の中に数多存在する脆弱性の中から「蟻の一穴」を突けば良いことから、攻撃者優位の状況となってしまうのである。

第２に、インターネット空間において行われる通信は、さまざまな国の通信インフラやコンピュータ、サーバなどを経由して目的のサイトに到達する。よって、サイバー攻撃者の追跡は一筋縄ではいかない[25]。また、仮想専用通信網（VPN：Virtual Private Network）[26]を用いることで通信自体を暗号化す

25）　例えば、海外のサーバを経由してサイバー犯罪が行われる場合、犯罪捜査においては海外のサーバに保管されている通信ログなどを解析し、犯人の特定を行う。しかし、海外に所在するサーバへの強制捜査は執行管轄権の関係から実施困難な場合も多く、サイバー攻撃者の特定に至らないケースも数多く存在する。そのような中、EUROPOL などは、EU 内の法執行機関が協力し、サイバー犯罪行為の発信元の機器や犯罪者を特定、機器の停止（テイクダウン）やサイバー犯罪者の逮捕などを行った実績も存在する。例えば、2021年には世界的に脅威を振るったマルウェアである EMOTET のボットネットをテイクダウンした。EUROPOL, World's most dangerous malware EMOTET disrupted through global action, January 27, 2021, at https://www.europol.europa.eu/media-press/newsroom/news/world％E2％80％99s-most-dangerous-malware-emotet-disrupted-through-global-action.

26）　仮想専用通信網とは、通常のネットワーク上に仮想回線を引くトンネリングという技術を用

る手法を用いる場合、または Tor（The Onion Router）[27] を利用することでさまざまなサーバを経由しサイバー攻撃を行う場合、攻撃の全容解明のためのハードルが著しく高くなる。そのため、ひとえにサイバー防御と言っても、サイバー防御の開始時点から防御側は不利な状況に置かれており、防御を維持するには相当の苦労が生じるのである。

このようにインターネット空間では攻撃者優位な状況があるが、サイバー防御側もさまざまな仕組みを整え、サイバー攻撃に対処している。一般的に、サイバー攻撃への対処においては、ユーザー、システム管理者、SOC（Security Operation Center）、CSIRT（Computer Security Incident Response Team）の４つの主体が関与する。ユーザーとは、システムの日々の利用者を指す。システム管理者とは、該当システムの保守や管理を行う担当であり、セキュリティ対策以外にもアクセス権限の付与、システムの稼働状況の確認などを行う。なお、SOC 及び CSIRT はサイバー防御において重要な役割を担っているため、改めて以下で紹介する。

2.2.1.　SOC（Security Operation Center）

SOC の主たる業務は、システムに対するサイバー攻撃の検知である。SOC では、システムに設置された各種セキュリティ製品（ウイルス対策ソフト、IPS/IDS、プロキシサーバなど）から出力されたログやアラートを24時間365日監視・分析する[28]。

い、２つの拠点間に仮想的な専用線を構築、拠点間でプライバシーを強化した通信を行う手法のことを指す。

27）　Tor とは、TCP/IP における通信を秘匿化するための規格及びソフトウェアである。Tor を使用して通信を行う場合、まずは利用者が使用する Tor ブラウザ上で通信自体が暗号化され、ガードリレー（通信の入り口となるノード）、中間リレー、出口リレー（対象の Web サイト等に接続する直前に使用されるノード）を経由する。出口リレーの通過後に通信が復号、対象となる Web サイトへ通常のリクエストを送信される。リレーの組み合わせは複数存在しているほか、どの経路で通信が行われるかは分からないため高い秘匿性が保たれる。

28）　なお、SOC と類似した名称で NOC がある。NOC は Network Operation Center の略で、主にネットワークの状況を24時間365日監視する。

SOC には、セキュリティ専門企業などが有償の契約に基づいて提供する SOC サービスのほか、自組織内にサイバー攻撃監視のための機能を置くプライベート SOC がある。プライベート SOC の設置は、24時間365日の監視対応が求められること、ログの分析及びインシデントの検知を行う能力を持った技術者の育成や確保に多くの時間とコストを要することなどから、一部の官公庁や大企業でのみ行われている。例えば日本においては、内閣サイバーセキュリティセンター情報統括グループに属する「政府関係機関情報セキュリティ横断監視・即応調整チーム（GSOC）」が政府機関及び独立行政法人等のシステムに対するサイバー攻撃を24時間365日で監視する[29]。

2.2.2.　CSIRT（Computer Security Incident Response Team）

CSIRT とは、主にサイバー攻撃が発覚した際にユーザー、システム管理者、SOC などと連携し、インシデントレスポンスの陣頭指揮または実働を担う組織である。なお、CSIRT の主な役割は、次の５つである。第１の役割は「準備」である。準備では、サイバー攻撃に即座に対応ができるよう、セキュリティポリシーの策定、対応手順の整理等を行う。第２の役割は「サイバー攻撃による影響の識別（トリアージ）」である。この役割では、組織内（利用者、システム管理者、SOC など）や組織外（国の CSIRT 機関を含む外部組織など）から寄せられたサイバー攻撃に関する情報を収集・分析し、入手した情報をもとに、即時的な対応が必要か識別（トリアージ）を行う。第３の役割は「影響の封じ込め」である。サイバー攻撃が確認された際は攻撃による被害の拡散を防ぐため、利用者、システム管理者と連携の上、感染端末及び感染が疑われる端末をネットワークから切り離し、必要に応じてサーバの停止、漏洩したと思われるアカウントの停止等を行う。なお、攻撃者が使用している Command &Control サーバ（以下、C2サーバ）が特定できる場合は、自組織内のシステムから C2サーバへのアクセスを遮断する。また、脆弱性を突

29）　内閣サイバーセキュリティセンター「情報統括グループ　グループの業務概要」、at https://www.nisc.go.jp/policy/group/toukatsu/index.html。

かれている場合は、脆弱性を有する機器にパッチの適用を行うことも有効であろう。第４の役割は「分析及び駆除」である。この役割では、システムから切り離した機器を調査し、サイバー攻撃の原因特定を行う。また、マルウェアに感染した端末が確認された場合は、デジタル・フォレンジック[30]によって当該端末を調査し、マルウェアの解析、パターンファイルの作成等を通じて、今後同様の感染が発生しないように備える。そして、第５の役割が「回復」である。「分析及び駆除」の完了後、利用者またはシステム管理者と連携の上、ネットワークから切り離したシステムを再接続し、業務の再開を図る。

2.2.3.　国家レベルでのサイバー防御の体制

国家機関や重要インフラに対するサイバー攻撃が多数発生している現在、国家レベルではどのようなサイバー防御体制が整備されているのか。本稿では、アメリカ、日本を例に、国家のサイバー防御体制について整理する[31]。

まずアメリカは、世界において最も高度なサイバー能力（サイバー攻撃能力、サイバー防御能力、サイバー諜報能力を含む）を有する国家であると評価されている[32]。サイバー防御に関しては、国土安全保障省（DHS）傘下のサイバーセキュリティ・インフラセキュリティ庁（CISA）が司令塔としての役割を担っている[33]。また、サイバー攻撃によるインシデントが発生した

30）　デジタルフォレンジックとは、「インシデントレスポンスや法的紛争・訴訟に対し、電磁的記録の証拠保全及び調査・分析を行うとともに、電磁的記録の改ざん・毀損等についての分析・情報収集等を行う一連の化学的調査手法・技術」である。安富潔、上原哲太郎『基礎から学ぶデジタル・フォレンジック 入門から実務での対応まで』（日科技連、2019年）2-3頁。

31）　本内容は、平時における国家レベルでのサイバー防御体制を前提とする。しかし、効果的なサイバー防御を行うには能力を持った要員が対象システムの挙動などを把握している必要があるため、武力紛争時においても同様の体制が維持されると考えられるだろう。

32）　2021年に国際戦略研究所（IISS）が各国のサイバー能力の分析を行ったレポートを公表した。その中で、アメリカは唯一 Tier1に分類された。The International Institute for Strategic Studies, Cyber Capabilities and National Power: A Net Assessment, June 28, 2021, Cyber Power- Tier One, at https://www.iiss.org/blogs/research-paper/2021/06/cyber-power---tier-one.

33）　Cybersecurity & Infrastructure Security Agency, Cyber Security, at https://www.cisa.gov/cybersecurity.

場合、国家サイバーセキュリティ・通信統合センター（NCCIC）がインシデント対応の実働を担う[34]。NCCIC はアメリカのナショナル CSIRT である US-CERT や ICS-CERT（Industrial Control Systems Cyber Emergency Response Team）を管轄しているほか、NCCIC の運用部門では24時間365日体制でサイバーセキュリティに関する調整を担っている[35]。なお、政府組織が有するシステムや電力・水道といった重要インフラに対するサイバー攻撃には NCCIC などが対応するが、軍隊のシステムに対するサイバー攻撃には米国サイバー軍（USCYBERCOM）が対応する。

対して、日本においてサイバーセキュリティ政策の中核を担っているのが、内閣官房の傘下に属する内閣サイバーセキュリティセンター（NISC）である。NISC は、政策対応機能、対処調整機能、情報収集・対処機能、情報集約・分析機能を持った11のグループで構成される[36]。多くのグループはサイバーセキュリティに関する政策立案や国家間・省庁間調整などに従事する一方、情報統括グループに属する GSOC は、政府機関及び独立行政法人等のシステムに対するサイバー攻撃を24時間365日で監視を行う。また、事案対処グループはサイバー攻撃に関する情報収集やマルウェア等の分析、注意喚起、情報提供などを行っている[37]。ただし、NISC には直接的にサイバー攻撃対処の実働業務を担う権限がないため、アメリカのように重要インフラなどがサイバー攻撃を受けた際に、直接または間接的にインシデントレスポンスを行うことはできない。

また防衛省自衛隊に関しては、2022年３月に自衛隊サイバー防衛隊が改編

34）　笹川平和財団「サイバー空間の防衛力強化プロジェクト　政策提言　“日本にサイバーセキュリティ庁の創設を！”」（2018年10月）10、12頁。

35）　経済産業省（株式会社アイ・ビー・ティ受託）「調査報告書 平成 29 年度サイバーセキュリティ経済基盤構築事業（米国から見た諸外国のサイバー空間における能力等の実態に関する調査）」（平成30年３月）22頁、at https://www.meti.go.jp/meti_lib/report/H29FY/000120.pdf。

36）　内閣サイバーセキュリティセンター「組織体制」、at https://www.nisc.go.jp/about/organize/index.html。

37）　内閣サイバーセキュリティセンター「前掲ホームページ」（注29）。

され、人数も540名態勢となった[38]。しかし、自衛隊サイバー防衛隊の任務は防衛省自衛隊のシステムに対するサイバー防御に限定されている[39]。そのため、民間の重要インフラ等に対するサイバー攻撃への対処は、重要インフラを有する各企業が一義的な責任を負うこととなる。事実、2022年６月には、政府が重要インフラ事業者向けのサイバーセキュリティ行動計画の改訂を行い、企業の経営陣に対して適切なサイバー攻撃対策を講じる義務を課すほか、対策の不備による情報漏洩が生じた場合には経営陣に対する賠償責任が発生する可能性があることが明記された[40]。そのため、重要インフラ事業者たる企業は、自社の責任でサイバー攻撃対策に従事する要員の確保及びサイバー攻撃対策の実装が求められることになる。なお、サイバーインシデントが発生した際には、NISC や重要インフラ所管省庁である金融庁、総務省、厚生労働省、経済産業省、国土交通省と連携し対応することとなるが、前述の通り、一義的な対応責任は企業が負うことになるだろう。

3.　サイバー防御がもたらす人の法的地位への影響

本章では、第１の論点である「サイバー防御は人の法的地位、特に攻撃目

38）　日本経済新聞、サイバー攻撃への対処向上、防衛省が新部隊、2022年３月17日、at https://www.nikkei.com/article/DGXZQOUA174SN0X10C22A3000000/。

39）　防衛省・自衛隊のホームページでは、防衛省・自衛隊のサイバー攻撃への対応に関し、「平成26年３月、自衛隊指揮通信システム隊の隷下に共同の部隊としてサイバー防衛隊を新編し、情報通信ネットワークの監視及びサイバー攻撃への対処を24時間態勢で実施」していると公表している。防衛省・自衛隊「防衛省・自衛隊の『ここが知りたい！』自衛隊のサイバー攻撃への対応について」、at https://www.mod.go.jp/j/publication/shiritai/cyber/index.html。また、2022年の自衛隊サイバー防衛隊の発足時には、読売新聞が「米国では平時からサイバー軍が重要インフラも防御するが、自衛隊サイバー防衛隊は平時に重要インフラを防衛することはできない」との見解を示している。読売新聞オンライン「自衛隊「サイバー防衛隊」540人態勢で発足…中国は17万人、北朝鮮も6800人」（2022年３月17日）、at https://www.yomiuri.co.jp/politics/20220317-OYT1T50257/。

40）　内閣サイバーセキュリティセンター サイバーセキュリティ戦略本部「重要インフラのサイバーセキュリティに係る行動計画」（2022年６月17日）、at https://www.nisc.go.jp/pdf/policy/infra/cip_policy_2022.pdf。

標該当性に影響を与えうるか」について考察する。先にも述べたように、先行研究でもサイバー防御について扱われる機会が少なく、サイバー防御がもたらす人の法的地位への影響についてはあまり触れられていない。よって、本章では、サイバー防御の法的特徴を整理することで、上記の影響について考察を行う。

なお、攻撃目標該当性の観点から、武力紛争中に行われる行為は大きく2つの類型に分類できる。第1の類型は「戦闘員、特に軍隊構成員によって行われる行為」である。軍隊構成員は、攻撃、防御、軍事行動の各種行為を通して戦闘員としての資格を有した上で武力紛争に従事する。なお、戦闘員は、前線から離れた場所で就寝している間など、戦闘行為以外に従事している場合でも合法的な攻撃目標と見なされる[41] よって、戦闘員たる軍隊構成員の攻撃目標該当性については、議論の余地はないだろう。

他方、第2の類型として挙げられるのが「文民によって行われる行為」である。文民は直接攻撃からの保護を享受するが、武力紛争への関与の度合いによっては攻撃の対象と見なされる可能性がある。よって、文民が行い得る活動にはどのようなものが存在し、それぞれの活動を行う文民が攻撃目標該当性を有するかどうかを整理・検討することが必要となる。なお、文民が行う活動は、攻撃、防御、敵対行為への直接参加、戦争遂行努力・継戦活動などがある。

以下では、直接攻撃からの保護を享受する可能性の低い行為から順に検討を行う。まず、第1の類型、第2の類型で共通した用語である「攻撃」「防御」の法的定義を確認した上で、第1の類型における「軍事行動」、第2の類型における「敵対行為への直接参加」、そして「戦争遂行努力・継戦活動」の定義について、物理空間、サイバー空間の両側面から確認する。なお、定義の確認に合わせ、各行為者の攻撃目標該当性についても検討するが、戦闘員たる軍隊構成員の攻撃目標該当性については議論の余地がないため、記載を

41) Gary D. Solis, *The Law of Armed Conflict International Humanitarian Law in War, 3rd Edition*, (Cambridge University Press, 2022), p.172.

割愛し、文民の攻撃目標該当性を中心に扱う。

3.1. 物理空間における定義

3.1.1. 攻撃

武力紛争法において、「攻撃」とは「攻勢としてであるか防御としてであるかを問わず、敵に対する暴力行為」[42]と定義される。第1追加議定書における定義では、文民たる住民に影響を与える可能性がある「攻撃」に加え、反撃といった「防御」も対象となる[43]。第1追加議定書の定義によると、武力紛争法上の「攻撃」に当たるかどうかの判断においては、「敵に対する暴力行為であるか否か」が重要な基準である。つまり、「暴力行為」に該当しない行為については、何らかの影響を及ぼしている場合でも、武力紛争法における「攻撃」とは見なされない。なお、「暴力行為」とは、物理的な力を意味するとされる[44]。「攻撃」の概念にはプロパガンダの流布、禁輸、その他の非物理的な手段による心理戦、政治戦、経済戦は含まれない[45]。また、通常、化学、生物、放射線による攻撃は、攻撃目標に対してキネティックな効果をもたらさないが、現代では「攻撃」に該当すると見なされているほか[46]、目標に対して何らかの結果を引き起こす紛争当事者の暴力行為を「攻撃」と解釈する傾向にある[47]。このようなことから、目標に対して何らかの結果を引き起こす行為が攻撃に該当すると言えるだろう。

42）　第1追加議定書第49条第1項。なお、「暴力行為」については、必ずしも物理的な力の発生を必要としない。現在では、「何かしらの特定の結果を目標に対して引き起こす」行為が「暴力行為」と解されている。黒﨑将広・坂元茂樹・西村弓・石垣友明・森肇志・真山全・酒井啓亘『防衛実務国際法』（弘文堂、2021年）354頁。

43）　Sandoz, Swinarski, Zimmermann, *supra* note 18, para. 1880. また、防御については、本稿3.1.2を参照。

44）　Michael Bothe, Karl Josef Partsch and Waldemar A. Solf（eds.）, *New Rules for Victims of Armed Conflicts: Commentary on the Two 1977 Protocols Additional to the Geneva Conventions of 1949*, 2nd ed. Reprint revised by Michael Bothe,（Martinus Nijhoff Publishers, 2013）, p. 329.

45）　*Ibid*., p. 329.

46）　Schmitt, *supra* note 15, p. 415.

47）　黒﨑ほか『前掲書』（注42）354頁。

3.1.2. 防御

武力紛争法における「防御」の定義は、前述の通り「攻撃」の定義の中で触れられている。つまり、防御として行われる敵に対する暴力行為が「防御行為としての『攻撃』」となる[48]。なお、武力紛争法における「防御」について第１追加議定書のコメンタリーには、「議定書における定義は、攻撃と同様に、防御（特に「反撃」）を当然に含むため、広範なものである。これは、双方ともに文民たる住民に影響を及ぼすことができる行為だからである」[49]との解説が付されている。上記の解釈は、第二次世界大戦後から第１追加議定書が起草された1977年当時の武力紛争の状況を反映していると思われるが、「特に反撃（particularly “counter-attacks”）」との文言があることから「反撃に相当しない防御行為」には焦点を当てていないと思われる。このようなことから、防御行為には「反撃に相当する防御」と「反撃に相当しない防御」の２種類が存在すると読み解くことができよう。

なお、第１追加議定書第49条第１項の規定は前者を含むように思われるが、後者については武力紛争法において特に定義がなされていない。これは、「反撃に該当しない防御」は人（文民たる住民など）への影響がないため、そもそも規制対象として想定されていない可能性もある。しかし、後述する敵対行為への直接参加の概念においては、敵に対して不利な影響を与える行為も、文民の保護喪失の要件になり得る[50]。よって、「反撃に相当しない防御行為」の存在を無視することはできないだろう。

なお、武力紛争法上の定義は存在しないものの、一般的には防御を「能動的防御（Active Defense）」と「受動的防御（Passive Defense）」に分別することができる[51]。「能動的防御（Active Defense）」とは、「敵に対し戦闘区域

48）　第１追加議定書第49条第１項。

49）　Sandoz, Swinarski, Zimmermann, *supra* note 18, para 1880.

50）　本稿4.1.1を参照。

51）　必ずしも意味が一致するわけではないが、前述の「反撃に相当する防御行為」は「能動的防御（Active Defense）」、「反撃に相当しない防御行為」は「受動的防御（Passive Defense）」と整理することができる。

や陣地の利用を拒否するために、限定的な攻撃行動や反撃を行うこと」[52] を指す。武力紛争の状況においては、前述の通り反撃としての銃撃、砲撃がこれに該当する。よって、反撃と能動的防御は近しい意味合いを持っていると言える。また、「受動的防御（Passive Defense）」は、「敵対行為によって引き起こされる損害の確率を減らし、その影響を最小限に抑えるために、主導権を取る意思を持たずに取られる措置」[53] である。主導権（イニシアチブ）を握る意思を持たずに行われるため、行為者が置かれた状況を受動的に維持するための行為などが該当する。武力紛争の状況においては、陸戦における塹壕の構築、バリケードの設置、海戦における自走式デコイ、空戦におけるフレアなどがその例として挙げられる。

3.1.3.　軍事行動

「軍事行動」は第１追加議定書において何度も登場する用語である[54]。第１追加議定書では、第３条に関するコメンタリーの中で「『軍事行動』とは、戦闘を目的に軍隊によって行われるあらゆる種類の移動（movements）、機動（maneuver）、行動（action）である」[55] とする。また第48条に関するコメンタリーでは、「辞書によると、『軍事行動』とは、軍隊によって行われる敵対行為に関連するすべての移動（movements）と行為（acts）」[56] と、第51条第１項に関するコメンタリーでは、「辞書によれば、『軍事行動』という用語は、議定書の他のいくつかの条文でも使用されているが、敵対行為に関連する軍隊によって行われるすべての移動（movements）及び活動（activities）

52）　US Department of Defense, DoD Dictionary of Military and Associated Terms, p. 7

53）　*Ibid.*, p. 165.

54）　例えば、第１追加議定書第３条、第39条第２項、第44条第３項・第５項、第49条、第51条第１項・第７項、第54条第３項（b）、第56条第２項（a）～（c）、第57条第１項・第４項、第58条（c）、第59条第２項（d）、第60条第１項・第６項に「軍事行動」という言葉が用いられている。

55）　Sandoz, Swinarski, Zimmermann, *supra* note 18, para. 152.

56）　*Ibid.*, para. 1875.

を意味する」[57] としている。このように、第1追加議定書に記載されている定義は完全に一致していないものの、軍事行動の主体は軍隊構成員（軍隊に属する非戦闘員を除く）であり、軍隊が戦闘行為または敵対行為を遂行する目的で行われる活動と解釈できるだろう。なお、軍事行動は前述の第1追加議定書第49条第1項の「攻撃」よりも大きな概念である[58]。よって、戦闘のための準備、展開、攻撃または防御、帰還までの一連の行為が軍事行動に含まれる。

3.1.4. 敵対行為への直接参加

「敵対行為への直接参加」とは、第1追加議定書第51条第3項の規定に基づく用語である。第51条第3項には「文民は、敵対行為に直接参加していない限り、この部の規定によって与えられる保護を受ける。」と規定されており、文民は敵対行為に直接参加しない限り、直接攻撃からの保護を享受する。他方、「敵対行為に直接参加」という条件は、第1追加議定書及び関連のコメンタリーでも具体的な記載がなされていなかった。そのため、紛争当事者が当該規定を広く解釈した場合、文民が有する保護を喪失する機会が拡大するおそれがあるなど、多くの議論を呼ぶ規定であった。

なお、「敵対行為への直接参加」が含む範囲は、攻撃及び軍事行動を包含し得る、広いものである[59]。第51条第3項における要件を具体化するためにICRCが作成したDPHに関する解釈指針では、敵対行為への直接参加と見なすための3つの累積基準を示している。その中の危害の敷居では、「当該行為は、武力紛争当事者の軍事行動もしくは軍事能力に不利な影響を及ぼすおそれがあるか、または直接の攻撃から保護される人や物に対して、死、傷害もしくは破壊を与えるおそれがあるものでなければならない」[60] と示してい

57） Sandoz, Swinarski, Zimmermann, *supra* note 18, para. 1936.

58） Marco Sassoli, International Humanitarian Law Rules, Controversies, and Solutions to Problems, Arising in Warfare (Edward Elgar Publishing, 2019), p. 349.

59） 敵対行為への直接参加に関する検討は、本稿4. を参照。

60） Nils Melzer, Legal adviser, ICRC, *Interpretive Guidance on the Notion of Direct*

ることから、敵対行為への直接参加は「攻撃」は包含しつつ、それよりも広い範囲をカバーしていると言える。

3.1.5.　戦争遂行努力・継戦活動

戦争遂行努力とは、「敵の軍事的敗北に客観的に寄与する全て活動」を指す[61]。例えば、具体的な軍事行動の文脈以外での武器や軍事装備の設計、生産および輸送、ならびに道路、港、空港、橋梁、鉄道その他インフラの建設または改修などがこれにあたる[62]。一般的に、軍隊に提供するために戦闘機や艦船、銃などを製造している企業は、戦争遂行努力に寄与しているだろう。また、継戦活動には「一般的な戦争遂行努力を支援する政治、経済またはメディアに関する活動（例えば政治的プロパガンダ、金融取引、農産物または非軍事産業製品の生産）」を含むことができる[63]。当然ながら、これらの行為は国家による武力紛争中の敵対行為に少なからず「間接的」な影響を及ぼしていると言えるだろう。

3.1.6.　攻撃目標該当性の検討

これまでの検討を踏まえ、物理空間における攻撃目標該当性について考察する。物理空間における武力紛争に軍隊構成員が関与する場合、軍隊構成員がいかなる行為を行っていたとしても合法的な攻撃対象となる。よって、「攻撃」「防御（反撃、能動的防御）」「受動的防御」「軍事作戦」をはじめ、前線から遠く離れた場所に所在し、基地の周りに塹壕や防御壁を構築するなどの受動的防御活動に従事している場合でも、攻撃目標となるだろう。

Participation in Hostilities under International Humanitarian Law（2009）, p. 46. なお、本稿における解釈指針上の用語・表現は、日本語訳（黒崎将広訳「国際人道法上の敵対行為への直接参加の概念に関する解釈指針」）の該当部分を参照。

61）　*Official Records of the Diplomatic Conference on the Reaffirmation and Development of International Humanitarian Law Applicable of in Armed Conflicts*, Volume XⅣ, CDDH/Ⅲ/SR.2, p. 14.

62）　Melzer, *supra* note 60, p. 51.

63）　*Ibid.*, p. 51.

以上を踏まえ、軍隊構成員の攻撃目標該当性は、下記の図1[64]のように表すことができる。

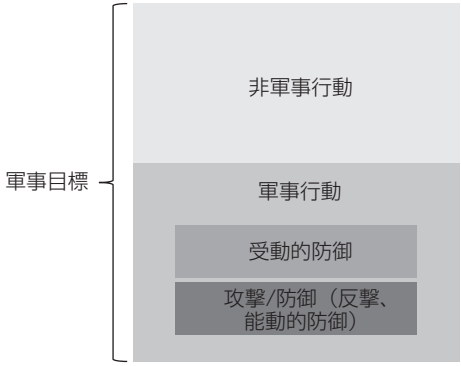

図1　軍隊構成員による行為

他方、文民についてはいかなる場合でも直接攻撃の対象となるわけではない。まず、DPHに関する解釈指針では、文民が直接攻撃からの保護を喪失する要件について「当該行為は、武力紛争当事者の軍事行動もしくは軍事能力に不利な影響を及ぼすおそれがあるか、または直接の攻撃から保護される人や物に対して、死、傷害もしくは破壊を与えるおそれがあるものでなければならない（危害の敷居）。」[65]と示していることから、軍隊構成員や軍事目標、文民や民用物などに対して「攻撃」または「防御（反撃、能動的防御）」を行なった場合には、文民としての保護を喪失する可能性がある。他方、「受動的防御」については、「武力紛争当事者の軍事行動もしくは軍事能力に不利な影響を及ぼすおそれ」[66]がある場合には、当該文民が敵対行為に直接参加していると見なされ、合法的な攻撃対象となり得る。「受動的防御」は武力紛争法における定義が存在しない概念であるが、文民の攻撃目標該当性を

64）　当該分類は行為の性質を整理するために行っているものであり、武力紛争法上の軍隊構成員の攻撃目標該当性に影響を及ぼすものではない。

65）　Melzer, *supra* note 60, p. 46.

66）　*Ibid.*, p. 46.

検討する上では重要な要素となる。「受動的防御」は主導権（イニシアチブ）を握る意思を持たずに行われる行為であるが、行為の内容によっては紛争当事者の軍事行動もしくは軍事能力に不利な影響を及ぼす可能性もある。よって、「受動的防御」の中には、敵対行為への直接参加と見なすか否か議論のあるグレーゾーンが存在していると言える。また、「戦争遂行努力・継戦活動」は ICRC の解釈では敵対行為への直接参加の要件を満たさないとされる[67]。他方、米軍の DoD Law of War マニュアルでは、敵対行為への直接参加に該当するか否かは、ケースバイケースでの判断となる。その際は、「当該行為が、一般的に敵対行為への直接参加と見なされている行為により、紛争当事国の戦争遂行努力にとって同等またはそれ以上の価値を及ぼすかどうか」[68] を、紛争当事者の戦争遂行努力に対する活動の軍事的重要性を考慮した上で判断すべきとする。そのため、「戦争遂行努力・継戦活動」の中にも、内容次第で敵対行為への直接参加となり得る領域（グレーゾーン）が存在するだろう。

なお、「受動的防御」及び「戦争遂行努力・継戦活動」が有するグレーゾーンは、２つの要素から文民に対する危害が生じさせうる。１つ目の要素は、「敵対行為への直接参加への近似性」である。第１追加議定書第51条３項では「文民は、敵対行為に直接参加していない限り、この部の規定によって与えられる保護を受ける。」と規定しているが、いかなる行為を敵対行為に直接参加していると見なすかは、依然として議論がある。よって、攻撃側の紛争当事者が「敵対行為への直接参加」を広く捉えている場合、「受動的防御」や「戦争遂行努力・継戦活動」に該当する行為を行う文民も攻撃対象になる可能性がある。

２つ目の要素は「軍事目標との地理的近接性」である。例えば、武力紛争が発生している国内で、戦闘の前線ではない場所へトラックで武器を運搬している文民ドライバーがいるとする。このケースにおいて、当該行為は敵対

67）　Melzer, *supra* note 60, p. 52.

68）　Office of General Counsel, Department of Defense, Department of Defense Law of War Manual, June 2015（Updated December 2016）, pp.229–230.

行為への直接参加に該当しないが、武器を積載しているトラックは軍事目標となり得る。よって、文民ドライバーが軍事目標への攻撃に巻き込まれる危険性があるだろう。なお、軍事目標の付近に文民が所在する場合、攻撃側は第１追加議定書第57条に規定される予防措置を取る必要があるほか、攻撃に際しては均衡性の観点から評価を行う必要性がある。よって、無制限に攻撃に巻き込まれる危険性があるわけではないが、攻撃側が必要な予防措置を行い、かつ当該攻撃による効果と巻き添えによる損失の間に均衡性があると判断した場合には、攻撃に巻き込まれる可能性がある。そのため、文民は「受動的防御」や「戦争遂行努力・継戦活動」に従事する場合も、関連する施設や物が軍事目標と見なされることにより、攻撃の影響を受ける可能性があることを認識しておくべきであろう。

以上の内容をまとめると、図２のように表すことができる。

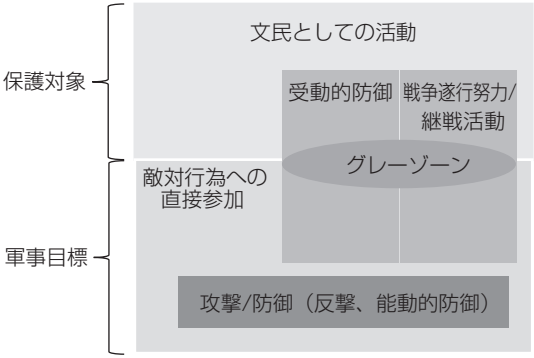

図２　文民による行為

3.2.　サイバー空間における定義

3.2.1.　サイバー攻撃

次に、サイバー攻撃の定義を確認する。まず、米国の NIST（米国国立標準技術研究所）は、サイバー攻撃とは「企業が利用するサイバー空間を標的

にコンピュータ環境やインフラストラクチャーを混乱、使用不能、破壊又は悪意を持って制御すること、またデータの完全性を破壊、制御された情報を窃取するためのサイバー空間を通じた攻撃」[69] であると定義する。この定義は、NIST が公表している情報セキュリティ対策の指針「NIST SP800シリーズ」[70] など、サイバーセキュリティ業界で権威ある文書にも記載されており、米国国内はもとより世界中において認知されている定義と言えよう。

対して、武力紛争法上のサイバー攻撃はどのように定義されるだろうか。まず、タリンマニュアルの規則92では、「サイバー攻撃とは、攻勢としてであるか防御としてであるかを問わず、人に対する傷害若しくは死又は物に対する損害若しくは破壊を引き起こすことが合理的に予期されるサイバー行動」[71] と定義する。タリンマニュアルのサイバー攻撃の定義に関する説明には「暴力行為」という用語が用いられていないが、「人に対する傷害若しくは死又は物に対する損害若しくは破壊を引き起こすこと」が「暴力行為」に包含されると言える。そのため、システムの挙動を変え、火災などを引き起こすサイバー行動も攻撃を構成し得る。なお、タリンマニュアルにおける攻撃の定義の検討にあたっては、サイバー手段による「攻撃目標の機能への干渉」が本規則の目的である“損害”もしくは“破壊”に該当するかについても議論が行われた。この点について一部の専門家からは、“損害”もしくは“破壊”に該当しないとする意見が出たが、多数派の専門家は、機能性の回復に物理的な部品の交換が必要な場合、機能への干渉は損害として認められるとの見解を示している。また、多数派の専門家の一部は、「機能への干渉は、

69）　National Institute of Standards and Technology, U.S. Department of Commerce, at https://csrc.nist.gov/glossary/term/cyber_attack.

70）　NIST SP800シリーズとは、NIST の中で情報技術に関する研究を行っている ITL（Information Technology Laboratory）の CSD（Computer Security Division）と呼ばれる部門が発行しているコンピュータセキュリティに関わる各種文書である。これらの文書は、米国の政府機関がセキュリティ対策を実装する際に利用することを目的に作成されているが、現在では米国に限らず、世界中の政府機関や民間組織のセキュリティ対策においても活用されている。独立行政法人情報処理推進機構「【概要説明】NIST 及び NIST 発行の情報セキュリティ関連文書」（2005年８月29日掲載）、at https://www.ipa.go.jp/security/publications/nist/nist_publications.html#r2。

71）　Schmitt, *supra* note 15, p. 415.

対象となるサイバーインフラが設計された機能を発揮するために、オペレーティングシステムや特定のデータの再インストールが必要となる状況にまで及ぶ」[72] との立場を取りつつ、「特に、特定のデータを操作したり、依存したりすることで個有の機能を果たすように設計された目的別のサイバーインフラ」[73] は「サイバー行動によってデータが削除または変更された結果、インフラが意図した機能を果たせなくなった場合、その行動は攻撃に該当する」[74] との見解を示している。一方、「国内のすべての電子メール通信を停止させるなど、大規模な影響をもたらすサイバー行動」[75] については、大多数の専門家が「この作戦を攻撃と見なすことには論理性があるかもしれないが、武力紛争法は現在のところそこまで及ばない」[76] との見解を示している。この点について、タリンマニュアルの編集責任者である Michael N. Schmitt は、「タリン・マニュアルの専門家の多くは、このような性質のサイバー行動が市民生活を混乱させる可能性があることを認識しているにもかかわらず、このような行動を攻撃として扱う法的根拠はまだ存在していないとの見解を示した」[77] と評している。

ICRC も「コンピュータやコンピュータネットワークなどの対象物を無効にすることを目的とした行動は、その対象物が物理的手段またはサイバー手段によって無効にされたか否かにかかわらず、敵対行為の実施に関する規則の下で攻撃を構成する」[78] との見解を示している。これは、第1追加議定書第52条2項に「軍事目標は、物については、(省略) その全面的又は部分的な破壊、奪取又は無効化がその時点における状況において明確な軍事的利益

72) Schmitt, *supra* note 15, p. 417.
73) *Ibid.*, pp. 417–418.
74) *Ibid.*, p. 418.
75) *Ibid.*, p. 418.
76) *Ibid.*, p. 418.
77) Michael N. Schmitt, "Wired warfare 3.0: Protecting the civilian population during cyber operations" International Review of the Red Cross, 100 (1), 2019, p. 339. Schmitt, *supra* note 16, p. 418.
78) ICRC, "International Humanitarian Law and the Challenges of Contemporary Armed Conflicts", Geneva, October 2015, p. 41.

をもたらすものに限る。」（下線は筆者追記）と規定している点からも述べることができる。つまり、「軍事目標の定義において、攻撃の結果として起こりうる対象物の無効化に言及していることから、電力網を破壊することなく停止させるなど、対象物を単に無力化することも攻撃と見なされるべきである」[79]と言える。

なお、サイバー作戦における「攻撃」の定義に関する一連の議論に関して、Schmitt は、タリンマニュアルも ICRC もサイバー行動を攻撃と認定する際には、ある程度、結果の性質が重要であり、必ずしもサイバー攻撃の重大性は重要ではないと評価する[80]。また、大多数のサイバー攻撃は物理的な領域に影響を及ぼす可能性が少ないことから、Schmitt は攻撃の概念を過度に制限してしまうと、①「文民用インフラに向けられる可能性のあるサイバー行動や、文民に深刻な悪影響を与えるサイバー行動の多くは、間違いなくサイバー攻撃とは認められず、したがって、国際人道法の攻撃に関する規則の適用範囲外となる」、②「機能喪失の基準が不明確であるため、文民に向けられた、あるいは文民に影響を与える特定のサイバー行動の法的特徴が曖昧になる」ことを主張している[81]。

3.2.2.　サイバー防御

サイバー防御（サイバーセキュリティ）に関する一般的な定義についても NIST による定義を確認したい。NIST は、「コンピュータ、電子通信システム、電子通信サービス、有線通信、電子通信（これらに含まれる情報を含む）の可用性、完全性、認証、機密性、および否認防止を確保するための損害防止、保護、および復旧」[82]がサイバー防御（サイバーセキュリティ）であると定

79）　Knut Dörmann, “Applicability of the Additional Protocols to Computer Network Attacks”, CICR Resources（19 November 2004）, p. 4.

80）　Schmitt, *supra* note 77, p. 339. 事実、ICRC は「諜報活動」や「ラジオ通信やテレビ放送のジャミングは、国際人道法の意味合いで伝統的に攻撃と見なされてきていない」との見解を示している。ICRC, *supra* note 78, pp. 41–42.

81）　Schmitt, *supra* note 77, p. 340.

82）　National Institute of Standards and Technology, U.S. Department of Commerce, at https://csrc.

義する。

なお、サイバー防御も能動的サイバー防御（Active Cyber Defense）と受動的サイバー防御（Passive Cyber Defense）に分けられる。能動的サイバー防御の定義については、識者によって含意される意味合いが大きく異なる。例えば、ハックバックのような行為を能動的サイバー防御に含み論じられる場合もある一方[83]、サイバーセキュリティに関する人材育成に携わるSANS Instituteのように「アナリストがネットワーク内部の脅威を監視し、対応し、そこから学習し、知識を適用するプロセス」[84]を能動的サイバー防御と呼ぶ場合もある。能動的サイバー防御の手法としては、攻撃者や攻撃手口に関する情報共有、拒否と欺瞞（D&D）、脅威ハンティング、ボットネットのテイクダウンなどさまざまな手法が挙げられる。ボットネットのテイクダウンについては法執行機関が令状に基づいて実施する必要があるが、民間企業などが同様の手法を独自に取った場合には、対象国の国内法上の犯罪を構成し得るだろう。

一方、受動的防御とは前述の通り「敵対行為によって引き起こされる損害の確率を減らし、その影響を最小限に抑えるために、主導権を取る意思を持たずに取られる措置」[85]である。ゆえに受動的サイバー防御とは、「サイバー攻撃によってもたらされる損害の可能性及び影響を最小限にするために能動的に行動する意思なく行使される手段」と言えよう[86]。

この受動的サイバー防御にはいくつかの手段が存在する。よく知られてい

---

nist.gov/glossary/term/cybersecurity.

83）　例えば、2019年に米国議会にて、トム・グレイブス議員が法案「Active Cyber Defense Certainty Act」を提出し、サイバー攻撃の被害者が攻撃者を突き止められるよう提案を行った。Active Cyber Defense Certainty Act, H.R. 3270, 116th Cong（2019-2020）, https://www.congress.gov/bill/116th-congress/house-bill/3270?s=1&r=1.

84）　Robert M. Lee, The Sliding Scale of Cyber Security, *SANS Institute White Paper*, 2021, p.12.

85）　US DoD, *supra* note 52, p. 165.

86）　SANS Instituteは、受動的（サイバー）防御を「常に人間が介在することなく、脅威に対する一貫した保護や洞察力を提供するためにアーキテクチャに追加されるシステム」と定義する。Lee, *supra* note 84, p. 10.

るものとしては、ファイアウォール[87]、IPS/IDS（侵入防止システム / 侵入検知システム）[88]、ウイルス対策ソフト[89] などを活用したものや、人の目によるネットワークやログの監視、コンピュータの脆弱性を改善する修正パッチなどがその手法として挙げられる。

一方、武力紛争法におけるサイバー防御の定義であるが、タリンマニュアルのサイバー攻撃に関する規則の中にサイバー防御の要素が含まれているものの[90]、サイバー防御単体での記載はなされていない。サイバー空間における防御のうち、敵に対する暴力行為と見なし得るものはわずかである。このようなことから、武力紛争法上の攻撃には該当し得ないとの前提があるように思われる[91]。

では、第１追加議定書第49条１項の攻撃の定義には反撃としての防御行為が含まれていたが、サイバー空間においても防御としてのサイバー反撃はあり得るか。この点については、すでに米国などが反撃としてのサイバー攻撃を行っている。例えば、2019年９月14日に発生したサウジアラビアの石油施設への無人機による攻撃を受け、米国は秘密裏にイランに対するサイバー作戦を実施、米当局者の発言によると、サイバー作戦によって物理ハードウェアに影響が生じたという[92]。また、2021年11月には、米国サイバー軍司令官であり、米国国家安全保障局（NSA）長官を務めるポール・ナカソネ陸軍大

87）　ファイアウォールは、インターネットなどの外部ネットワーク、または社内ネットワークなどの内部ネットワークからのアクセスをチェックし、通信のフィルタリングを行うツールである。

88）　IPS/IDS は、ネット上に流れるトラフィックを監視し、不正なパケットを検知すると通知を発したり防御を行ったりすることができる。

89）　ウイルス対策ソフトは、既知のマルウェアのパターンファイルを用いて通信内容にマルウェアが仕込まれていないかを判断し、マルウェアが仕込まれていた場合は隔離し削除する機能を有する。

90）　Schmitt, *supra* note 15, p. 415.

91）　ただし、後述する通り、サイバー防御は敵に対して不利な影響を及ぼすことができるため、文民が当該活動を行う場合は敵対行為への直接参加と見なされる可能性がある。

92）　Reuters by Idrees Ali, Phil Stewart, Exclusive: U.S. carried out secret cyber strike on Iran in wake of Saudi oil attack: officials, October 16, 2019, at https://www.reuters.com/article/us-usa-iran-military-cyber-exclusive-idUSKBN1WV0EK.

将が、米国に対するランサムウェア攻撃に対抗する目的で反撃を行ったことを明らかにした[93]。

なお、タリンマニュアルの規則92が第1追加議定書第49条1項の攻撃の定義を踏まえて作成されている点を考慮すると[94]、規則92における防御は、サイバー反撃を意味すると解釈できる。なお、能動的防御にはサイバー反撃に近しい意味が含まれることもあるため、場合によっては能動的防御とサイバー反撃で重なる部分があるだろう。

3.2.3. サイバー行動

サイバー行動については、武力紛争法上、明確な定義がなされていない[95]。他方、タリンマニュアルの用語解説において、サイバー行動（Cyber Operation）とは、「サイバースペースにおいて、またはサイバースペースを通じて目的を達成するために、サイバー能力を用いること。」と定義する[96]。また、規則92のサイバー攻撃の定義の中でサイバー行動が触れられていることも踏まえると[97]、サイバー行動の一部がサイバー攻撃を構成すると考えるのが妥当であろう。

3.2.4. サイバー空間における敵対行為への直接参加

「敵対行為への直接参加」の定義は、物理空間でもサイバー空間でもその定義は同じである[98]。つまり、文民によるサイバー空間における活動において、「危害の敷居」、「直接因果関係」「交戦者とのつながり」の3つの累積要

93） CNN.co.jp「米サイバー軍司令官、ランサムウェア攻撃への「反撃」認める」(2021年11月4日)、at https://www.cnn.co.jp/tech/35179001.html。

94） Schmitt, *supra* note 15, p. 415.

95） *Ibid.*, p. 451.

96） *Ibid.*, p. 564.

97） *Ibid.*, p. 415.

98） ICRC による DPH に関する解釈指針でも、危害の敷居の検討でサイバー攻撃に関する例示が含まれるなど、サイバー攻撃による敵対行為も含んだ上で検討がなされている。Melzer, *supra* note 14, p. 48. また、タリンマニュアルでも、規則97で敵対行為への直接参加の規定をサイバー空間における行為に適用する形で検討がなされている。Schmitt, *supra* note 15, p. 428.

件を満たした場合、当該人物は文民としての直接攻撃からの保護を喪失する。なお、サイバー空間での活動、特にサイバー攻撃やサイバー防御は軍隊構成員よりも文民技術者の方が高いスキルを有していること、文民はサイバー防御を平時から行っていることから、物理空間における行為よりも敵対行為へ直接参加するための敷居（行為の難易度）が低い可能性があるだろう。

3.2.5.　サイバー空間における戦争遂行努力・継戦活動

戦争遂行努力・継戦活動については、物理空間でもサイバー空間でも、その行為に対する法的評価に差はない。他方、サイバー空間における戦争遂行努力としては、具体的な軍事行動に関連せずにマルウェアやサイバー防御ツールを開発、製造、販売する行為などが該当し得る。例えば、イスラエルのNSO Group Technologies は、サイバー諜報などで使用されるスパイウェア「Pegasus」を国家に販売している。「Pegasus」は複数の国家に販売され、実際の諜報活動でも使用されている[99]。よって、NSO Group Technologies のような企業も、状況次第では、戦争遂行努力に寄与していると見なされるかもしれない。

また、マルウェアのような攻撃的なツールの製造のみならず、軍隊に提供するためのシステムを製造している企業も戦争遂行努力に該当する活動を行なっている場合がある。2022年７月現在、米軍は JWCC（Joint Warfighting Cloud Capability：統合作戦クラウド機能）の調達及び構築を推進している。JWCC の調達及び構築はこれからであるが、調達に際しては Google、Oracle、Microsoft、Amazon Web Services といった米国の最大手クラウド事業者が候補となっている[100]。仮にこれらの事業者が JWCC の調達及び構築を行なった場合、当該事業者は米国の戦争遂行努力に寄与していると見なさ

99）　時事通信社「スパイウエア、仏大統領も標的か　記者、政治家の情報抜き取り―イスラエル企業開発」（2021年７月22日）、at https://www.jiji.com/jc/article?k=2021072100979&g=int。

100）　U.S. Department of Defense, Joint Warfighting Cloud Capability Award Planned for December, March 31, 2022, at https://www.defense.gov/News/News-Stories/Article/Article/2984496/joint-warfighting-cloud-capability-award-planned-for-december/.

れる可能性がある。なお、戦争遂行努力に該当する活動を行なっていることで、必ずしも敵対行為への直接参加のように直接攻撃からの保護を喪失するわけではない。

3.2.6.　サイバー空間における攻撃目標該当性及びサイバー防御の特殊性

軍隊構成員及び文民のサイバー攻撃、サイバー反撃、能動的サイバー防御、受動的サイバー防御、サイバー行動、敵対行為への直接参加の関係性は、それぞれ図３[101]及び図４の通りである。

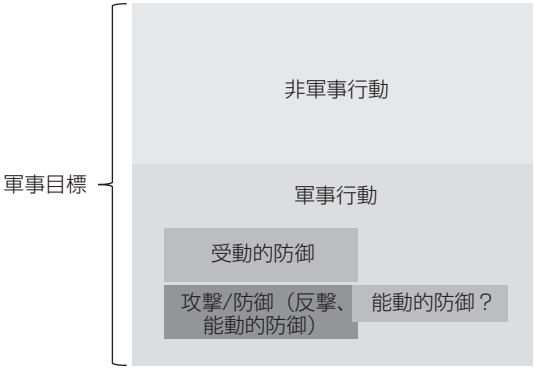

図３　軍隊構成員によるサイバー空間での行為

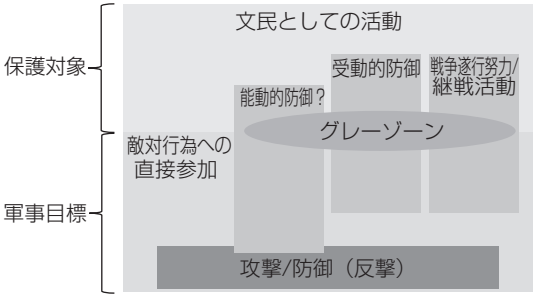

図４　文民によるサイバー空間での行為

101)　当該分類は行為の性質を整理するために行っているものであり、武力紛争法上の軍隊構成員の攻撃目標該当性に影響を及ぼすものではない。

大枠については、軍隊構成員、文民ともに物理空間における行為と同様である。異なる点としては、サイバー空間の場合、「反撃」と「能動的防御」が異なる行為と見なされる可能性がある。サイバー空間における「反撃」は、相手国にマルウェアを送付しシステムを停止させるような行為である。他方、能動的防御には、ハックバックのように攻撃国にマルウェアを送付し追跡、情報を秘密裏に収集する行為から、能動的に脅威情報を収集し対策を取ることまでが含まれ、その範囲も「攻撃」に該当するものから「文民として保護を享受できる活動」まで広い範囲が含まれる。よって、このように「反撃」と「能動的防御」の間に微妙なニュアンスの差が生まれる場合があるだろう。

その上で、物理空間、サイバー空間における防御の特性の差は、文民による行為の実行難易度の違い、つまり日常的に当該行為を行っているか否かにあると考える。物理空間における「攻撃／防御（反撃）」を行う場合、文民によって実施可能な行為は銃やナイフの使用に限られる。また、「受動的防御」においても、フェンスの設置による侵攻の妨害など、文民が取ることが可能な手法に限られる。他方、サイバー空間の場合、知識のある者であればサイバー攻撃を行うことも可能である。また、サイバー防御については、平時の企業活動において広く行われている行為であり、国家の重要インフラシステムにおいては、必ずサイバー防御が行われている。よって、サイバー空間の出現及びサイバー防御が一般に普及したことにより、文民が武力紛争の状況においてサイバー防御に従事できる機会が増加、結果的に直接攻撃からの保護を喪失する「敵対行為への直接参加」に近しい行為が行われる可能性があるだろう。

このようなことから、サイバー防御は人の法的地位、つまりサイバー防御に従事する文民の法的地位に影響を及ぼし得る行為であると言える。

4.　敵対行為への直接参加に関する検討

第２の論点である「サイバー防御が敵対行為への直接参加に該当する可能

性があるのか、また、いかなる行為が敵対行為への直接参加に該当するか」については、第1追加議定書第51条「文民たる住民の保護」の検討が重要である。そこで、2009年にICRCが発表したDPHに関する解釈指針（国際人道法上の敵対行為への概念に関する解釈指針」）に基づいて、敵対行為への直接参加の要件を詳細に確認、検討する。なお、DPHに関する解釈指針はICRCが独自に作成したものであるため法的拘束力はないが、DPHに関する解釈指針を元に各国軍事マニュアルの作成や検討が行われており、敵対行為への直接参加に関する議論に影響を与えていることは間違いないだろう。

4.1. 敵対行為への直接参加に関する累積要件

ICRCは文民の行為が敵対行為への直接参加と認められるには、以下の累積要件を満たすことが必要であるとする。つまり、1）当該行為は、武力紛争当事者の軍事行動もしくは軍事能力に不利な影響を及ぼすおそれがあるか、または直接の攻撃から保護される人や物に対して、死、傷害もしくは破壊を与えるおそれがあること（危害の敷居）、2）当該行為と、当該行為または当該行為が不可分の一部をなす協同軍事行動のいずれかから生じるおそれのある危害との間に、直接的な因果関係の結びつきがあること（直接因果関係）、3）当該行為は、一方の紛争当事者を支援しかつ他方の当事者を害する形で必要な危害の敷居を直接引き起こすことが明確に意図されたものであること（交戦者とのつながり）、である[102]。

以降では、上記3つの要件について検討を行う。

4.1.1. 危害の敷居

危害の敷居は、2種類で構成される。まず、第1の危害の敷居では、「武力紛争当事者の軍事行動もしくは軍事能力に不利な影響を及ぼすこと」が必要となる。つまり、「ある行為が明確に軍事的な性質を持つ危害を引き起こ

102） Melzer, *supra* note 60, p. 46.

すと合理的に予測できる」[103] 段階に達すれば、現実の損害の有無にかかわらず本敷居を満たすことになり、その際は、必ずしも物理的な損害または非物理的な損害が生じる必要はない。例えば、敵対する武力紛争当事者の軍事行動を妨害または効果を低減させる行為については、本敷居を満たす可能性があるだろう。よって、防御行為、特に受動的防御については、軍事行動や軍事能力に不利な影響を及ぼすという観点から、危害の敷居を満たし得る点に注目する必要がある。

次に第２の危害の敷居では、「直接の攻撃から保護される人や物に対して、死、傷害、または破壊を与えること」が必要となる。「直接の攻撃から保護される人」とは、文民や医療要員・宗教要員・文民保護要員などを指す。また、第１の危害の敷居では「不利な影響」がその敷居に含まれていたが、第２の敷居の場合は直接の攻撃から保護される人や物に対する不利な影響だけでは本敷居に達しない。なお、軍事能力に寄与するなどして軍事目標の要件に該当する施設（いわゆるデュアル・ユース）、例えば軍事施設に電力を供給している発電施設や送電網はここで言う「直接の攻撃から保護される物」に該当しない。よって、そのような目標に破壊が生じる攻撃が行われたとしても、第２の危害の敷居に基づくと敵対行為への直接参加には該当しない。他方、軍事能力に寄与することによって民用物として扱われていた物が軍事目標と見なされる場合もある。この場合、これらの物に対する攻撃によって引き起こされる破壊は、第１の危害の敷居を満たす可能性があるだろう。

では、上記の検討も踏まえ、物理空間ではいかなる行為が危害の敷居を満たすだろうか。DPH に関する解釈指針では、第１の危害の敷居に該当する行為として、軍隊の構成員の死や傷害及び軍事目標の破壊に加え、破壊活動やその他の軍隊の展開、兵站、通信への妨害のための活動（武力によらないものも含む）、軍事目標や領域の獲得及びそれらに対する支配の行使[104] など

103）　Melzer, *supra* note 60, p. 47.

104）　例えば、特定の物を敵の軍隊が使用するのを拒絶すること、敵が敷設した地雷を勝手に除去することがこれに該当する。

をその例として列挙している[105]。また、第２の危害の敷居に該当する行為としては、文民に対する狙撃、文民が所在する領域への砲撃や爆撃がこれに該当するとしている[106]。ただし、文民への死・傷害、民用物への破壊をもたらさない行為、例えば文民のみが使用する道路に障害物を設置することや電気・水道・食料などの供給網の断絶、通商に対する妨害といった文民に不利な影響を与える行為は武力紛争法上の違反を構成する可能性はあるものの[107]、敵に不利な影響を与えない範囲においては、本敷居を満たすことはないだろう[108]。

他方で、サイバー空間において、どのようなサイバー行為が危害の敷居を満たし得るだろうか。すでに述べているとおり、危害の敷居では必ずしも物理的な損害を必要としているわけではなく、敵に不利な影響を与えるだけでもその敷居を満たし得る。ゆえに、物理的損害を生じさせないサイバー攻撃も当該敷居を満たす可能性はある。例えば、敵の軍隊の展開計画を含んでいる軍事データベース内にあるデータを改ざんすることや、敵の指揮命令システムを妨害または作戦領域に展開できないように無人航空機（以下、UAV）の操作システムを遮断するようなサイバー作戦は、危害の敷居を満たし得るだろう[109]。一方、国防総省のウェブページを書き換えるような軍事ネットワークに対する低レベルの攻撃は、軍事作戦に不利な影響を与える可能性がないので当該敷居を満たすことはない[110]。なお、タリンマニュアルの作成において、国際専門家グループの一部のメンバーは、自国の軍事能力を高める行為、例えば軍事的なシステムに対する受動的防御を維持することは、敵

105）　Melzer, *supra* note 60, pp. 47–48.

106）　*Ibid*., p. 49

107）　例えば、第１追加議定書第54条２項において、文民の生存に不可欠なものを移動させることや、利用できないようにすることなどを禁止している。

108）　Melzer, *supra* note 60, p. 50.

109）　Marco Roscini, *Cyber Operations and the Use of Force in International Law*（Oxford University Press, 2014）, p. 205.

110）　Heather Harrison Dinniss, *Cyber Warfare and the Laws of War*（Cambridge University Press, 2012）, p. 270.

対者の相対的地位を弱めることから、危害の敷居を満たし得るとの立場をとった[111]。この点について Schmitt は自身の論文において、サイバー防御の開発や軍事システムの脆弱性を明らかにすることなど、味方の能力を高めるような行為も危害の敷居を越えるものと見なされるべきだと述べている[112]。

なお、サイバー防御の構築やサイバー攻撃対処は、従来の防御とは異なり死傷者が発生することもなく武力の使用も伴わないため、危害の敷居を満たさないという主張がなされるかもしれない。これについては、先にも述べたように第１の危害の敷居では武力の使用によって危害が引き起こされなければならないとは規定されていないことから、不利な影響を生じさせる行為も当該敷居を満たすと言えよう。ゆえに、サイバー防御の構築やサイバー攻撃対処であっても本敷居に達する可能性は十分にある。しかし、すべてのサイバー防御やサイバー攻撃対処が当該敷居を満たすわけではないことに注意すべきである。つまり、当該行為と後に生じた危害との間に直接因果関係のない行為や交戦者とのつながりを有さない行為は、当然に敵対行為への直接参加には該当しないだろう。

他方、DPH に関する解釈指針ではいわゆる第２の危害の敷居において、公共の安全、衛生及び通商に重大な影響を与える行為であっても、当該行為によって保護された人の死傷や物の破壊などの物理的損害が生じない限り本敷居を満たすことはないとする[113]。このような解釈に対して Marco Roscini はあまりに制限的であると主張している。なぜなら、もし目標となるインフラが軍民共用の物であり、かつそれゆえに機能の喪失が文民サービスのみならず軍事的にも危害を生じさせるのであれば、物理的な影響の有無に関わらず危害の敷居を超えることがあるからである[114]。また、文民または民用物

111）　Schmitt, *supra* note 15, p. 429.

112）　Michael N. Schmitt, “Cyber Operations and the Jus in Bello: Key Issues,” *Naval War College International Law Studies*, Vo. 87 (2011), p. 101.

113）　Melzer, *supra* note 60, p. 50.

114）　Roscini, *supra* note 109, pp. 205-206.

への物理的な損害と軍事的危害の双方を生じさせるような文民インフラへのサイバー作戦は、それらのネットワークが極めて重要な役割を果たしていることから、コンピュータネットワーク上の情報への損害も当該敷居に含むよう、危害の敷居の概念を延長すべきであると指摘する者もいる[115]。

4.1.2.　直接因果関係

第２の要件である直接因果関係では、「ある特定の行為と、当該行為または当該行為が不可分の一部をなす協同軍事行動のいずれかから生じるおそれのある危害との間」に直接的な因果関係が存在することを要件とする。

では、どのような敵対行為が後に発生した危害との間に「直接的」な因果関係があるか。ICRC は DPH に関する解釈指針において「直接因果関係とは、問題となる危害が１つの原因段階（one causal step）で引き起こされることを意味するものと解釈されるべき」[116] としている。例えば、経済制裁や敵に物品などを供与する行為を行った場合、これらの行為は敵の軍事能力や軍事行動に重要な影響を与える可能性はあるが、その影響が間接的であることから敵対行為への直接参加には当たらないとしている。

一方、現代の武力紛争では複数の者が各自の役割を果たすことによって１つの作戦が遂行されているという側面も存在する。１つの例として挙げられるのが UAV による攻撃である。攻撃を行うにあたっては、UAV を操縦する者、標的を照射するもの、データを収集する者、全体の指揮統制を行う者など複数の者が各自の任務を遂行することにより１つの攻撃が成立している。おそらくこれらの行為一つひとつを評価した場合、すべての行為が前述した危害の敷居を満たすわけではないだろう。しかしそのような解釈をすると、集団による組織化された敵対行為においては、一部の行為しか敵対行為への直接参加に該当しなくなってしまうおそれがある。そこで、ICRC は、「当該行為

115）　John R. Heaton, “Civilians at War: Reexamining the Status of Civilians Accompanying the Armed Force,” *Air Force Law Review,* Vol.57 (2005), p. 201.

116）　Melzer, *supra* note 60, p. 53.

が不可分の一部をなす協同軍事行動」という文言をその要件に加えることで、特定の行為それ自体では危害の敷居に達しなくとも、その行為が危害を直接引き起こす具体的かつ協同的な戦術行動の不可分の一部を構成する場合にもこれを満たすとしている[117]。

なお、直接因果関係において、因果関係の成立要件として時間的または地理的な状況は問題とならない。Yoram Dinstein は、敵対行為への直接参加は、戦闘状況で行われる全ての兵器の使用のケースを包含しており、その者の地理的な状況は問題ではないとしている[118]。例えば、サイバー攻撃やサイバー防御の場合は、その多くは遠隔地からなされるために地理的近接性が存在せず、ゆえに直接的な因果関係がないように思われる。しかし、DPH に関する解釈指針では、サイバー攻撃手段の使用とそれにより生じる危害との間には直接因果関係が存在するとしている[119]。一方、戦闘員への食料の配達などの行為は地理的近接性を有しているものの、食料の配達により直接にその後の危害が生じたとは言えないため、この場合は因果関係が間接的なままである[120]。

では、DPH に関する解釈指針に従うと物理空間ではいかなる行為が直接因果関係の敷居を満たす行為と言えるか。例として、弾薬工場で作業を行う文民労働者や兵器開発に貢献する研究者のケースを考える。まず、兵器工場の労働者については、かつては紛争当事国の軍事能力に不可欠な存在であったため当時の慣習法においては合法的な軍事目標と見なされていた可能性があるが、現在では軍事目標には当たらないというのが通説である[121]。そのため、兵器の製造、軍隊でのエンジニア作業、軍事的な輸送などの方法による戦争遂行努力への貢献は、直接因果関係が欠如していることから敵対行為

117）　Melzer, *supra* note 60, pp. 54–55.

118）　Yoram Dinstein, *The Conducts of Hostilities under the Law of International Armed Conflict, 2nd Edition*（Cambridge University Press, 2010）, pp. 149–150.

119）　Melzer, *supra* note 60, p. 55.

120）　*Ibid*., p. 55.

121）　Ian Henderson, *The Contemporary Law of Targeting*（Martinus Nijhoff Publishers, 2009）, p. 107.

への直接参加にはあたらないと言えるだろう。さらに、紛争当事国の軍事能力に貢献する兵器開発に携わる科学者や研究者についても、敵対行為への直接参加には該当しない可能性が高い。例えば、Hays W. Parks は第二次世界大戦時に英国空軍第604飛行中隊に貢献した文民技師の扱いを例に出し、文民技師は第二次世界大戦当時の法律では軍事目標となるものの、現代では第１追加議定書第51条３項に従って直接攻撃から保護されるとしている[122]。また、Ian Henderson も Parks の主張を引用した上で、文民は自身の戦争遂行努力への貢献のみを理由として攻撃からの保護を失うわけではないと主張している[123]。

しかしながら、研究者などの専門知識を有する文民の全てが直接の攻撃対象にならないわけではない点に注意しなければならない。DPH に関する解釈指針作成における専門家会合において、「ある特定の文民の持つ専門知識が武力紛争の結果について極めて例外的かつ潜在的に決定的な価値を有している場合」にも当該文民が敵対行為への直接参加に該当しないと言えるかは疑問があるとの主張がなされている[124]。そのため、戦争の行方を左右するような高度な専門知識を有する文民の場合は、敵対行為に直接参加していると見なされる可能性があるだろう。

一方、軍隊のために食料や衣服を提供している兵站部や食堂で働く事、国防総省で文民当局者として広報、経理、総務などの事務作業を行う事、または政府による税収で間接的に戦争を支援してしまうような商業施設で働く事などは、敵対行為への直接参加には該当しない[125]。

では、上記検討を踏まえ、サイバー空間において直接因果関係の敷居を満

122）　Hays W. Parks, “Air War and the Law of War,” *Air Force Law Review*, Vol.32, (1990), p. 127, footnote 386.

123）　Henderson, *supra* note 121, p. 108.

124）　Melzer, *supra* note 60, footnote 122. ICRC, “Clarification Process on the Notion of Direct Participation in Hostilities under International Humanitarian Law: Expert meeting report (2006), pp. 48-49を参照。

125）　Anthony P. V. Rogers, *Law on the battlefield, 3rd Edition* (Manchester University Press, 2012), pp. 14-15.

たし得るサイバー行為にはどのようなものがあるだろうか。例えば、敵の指揮命令システムをサイバー攻撃によって直接に妨害した場合は、当該基準は満たされるであろう。なお、サイバー攻撃は遠隔地から行うことができ、かつコンピュータやネットワークへの侵入から実損害の発生までの間に時間を要するケースがあるが、先にも述べたように直接因果関係の有無を判断する上で時間的・地理的状況は問題とならない。事実、イスラエル最高裁で争われた Targeted Killings 事件判決において、裁判所は「戦場から離れたところで違法戦闘員が使用する兵器を操作する者、またはそれらの作戦を指揮または作戦に貢献することは敵対行為への直接参加に該当する」ことを示している[126]。

他方、単にハッカーを雇用し、それらの者にサイバー攻撃やサイバー防御の訓練を行う者、システムやネットワークの一般的な技術メンテナンスを提供する者、インテリジェンス収集のためのサイバー作戦に従事する者は後の危害との間に「１つの原因段階」[127] が存在していないことから、直接因果関係を有しているとは言えないであろう[128]。

なお、DPH に関する解釈指針では「ある特定の行為がそれ自体では必要とされる危害の敷居を引き起こさないとしても、その行為が危害を直接引き起こす具体的かつ協同的な戦術行動の不可分の一部をなすのであれば、直接

126）　Israeli Supreme Court, HC_J 769/02, *Public Committee against Torture in Israel v. Israel* (*Targeted Killings judgment*), 11 December 2005, para.37, at　https://www.law.upenn.edu/institutes/cerl/conferences/targetedkilling/papers/IsraeliTargetedKillingCase.pdf. なお、上記 URL の判例は英語に翻訳されたものである。

127）　Schmitt は、「１つの原因段階」という文言にも問題があると主張する。Michael N. Schmitt, "Deconstructing Direct Participation in Hostilities: The constitutive Elements," *New York University Journal of International Law and Politics*, Vol.42, No.3 (2010), pp.714, 728. Schmitt は、戦場における戦術的な情報の収集は敵対行為への直接参加に該当すべきであるとの見解を持つ。ただし、情報はそのまま作戦に用いられるわけではなく、その情報を分析し、他の情報と統合させることによって初めて軍事的効果が生じる場合もあるため、必ずしも１つの原因段階を経て一方の紛争当事者に影響を与えるわけではないとし、「１つの原因段階」という用語を用いることが問題であるとし、「不可分性」の基準を用いるべきだと主張する。

128）　Roscini, *supra* note 109, p. 207.

因果関係の要件はやはり満たさせるだろう」[129] と述べている。さらに、「標的の識別や設定、戦術上のインテリジェンスの分析や攻撃部隊への伝達、特定の軍事行動を実施するために部隊に与えられる指示や支援」[130] は、例えそれ自体では危害を引き起こしていなくとも直接因果関係を有するとしている。ゆえに、サイバー戦においては、標的の識別や追跡を念頭に置いた戦術的サイバー作戦、戦術情報の分析や攻撃部隊への伝達、特定の軍事行動遂行のために派遣された部隊への命令や支援の提供、または軍用機やミサイルソフトウェアシステムに作戦指示データをロードするような行為が当該要件を満たすことになるだろう[131]。また、サイバー防御要員の育成を目的として実施されるサイバー防御訓練（トレーニング）において、特定の国家が、敵対する紛争当事国からのサイバー攻撃を防御するために訓練を行っていた場合、当該行為が「危害を直接引き起こす具体的かつ協同的な戦術行動の不可分の一部」を構成するのであれば、敵対行為への直接参加に該当する可能性があると言えるだろう。

また、サイバー戦において特にその地位について争いがあるのがマルウェア設計者や開発者である。これについては、紛争当事国の軍事能力に貢献する兵器開発に携わる科学者や研究者は敵対行為への直接参加には該当しないというのが一般的な見解である。しかし、サイバー兵器の設計者や開発者の場合については、議論があるだろう。先にも述べたように、敵対行為への直接参加の概念に関する専門家グループにおいて一部の学者から、第２次世界大戦中の核兵器専門家のようにある特定の文民の持つ専門知識が武力紛争の結果に極めて例外的かつ潜在的に決定的な価値を有している場合は、必ずしも敵対行為への直接参加に該当しないとは言えないという主張がなされていた。このようなことから、高度なサイバー兵器を開発できる専門知識を有する者は、直接因果関係の基準を満たし得る可能性がある。

129） Melzer, *supra* note 60, p. 54.
130） *Ibid.*, p. 55.
131） Roscini, *supra* note 109, p. 207.

4.1.3.　交戦者とのつながり

当該行為が敵対行為への直接参加に該当するか否かを判断する上では、上記２つの要件（危害の敷居と直接因果関係）に加え、交戦者とのつながりの有無についても検討する必要がある。この交戦者とのつながりという要件は、紛争当事者に影響を及ぼさない暴力（例えば紛争とは関係のない略奪行為など）をその敵対行為への直接参加の範囲から除外するために規定されている。例えば、武力紛争中に銀行強盗や無理心中を行った場合、それらの行為は文民に死や傷害を与えまたは民用物の破壊をもたらすおそれがあり、危害の敷居を十分に満たすことができる。しかし、これらの行為の多くは金銭的欲求や精神的衰弱などの個人的理由によってなされるケースもある。そのため、個人的な理由に基づいて当該行為がなされた場合は、交戦者とのつながりが認められずその行為は敵対行為への直接参加には該当しない。

そうなると、当該要件を満たすには交戦者との間にどの程度のつながりが必要なのかという問題が生じる。DPH に関する解釈指針によると、一般的には当該行為を「一方の紛争当事者を支援しかつ他方の当事者を害する形」でなすことを「明確に意図」している必要がある。ただし、武力紛争中に当該行為者が交戦者とのつながりを有しているか否かを厳格に判断することは困難である。そのため、つながりの認定には、当該認定を行う者が合理的に入手できる情報を基礎として行うことが求められ、認定は「客観的に検証可能な要因」によってなされれば良い[132]。つまり、関連する「時」とその場所での「状況」を踏まえ、当該文民が他者に対して危害を引き起こした行為が、一方の紛争当事者を支援しようと意図された行為であると合理的に考えられるか否かを判断する必要がある。

では、交戦者とのつながりが存在すると判断されるケースとしては、どのようなものが考えられるだろうか。例えば、文民に対する暴力から自己または他者を防御する目的でなされた行為によって危害が生じても、交戦者とのつながりは認められない。その理由としては、もしこのような違法な攻撃に

132）　Melzer, *supra* note 60, p. 63.

対する正当防衛によって交戦者とのつながりを認めてしまうと、それは間接的に先行する違法な攻撃を正当化することになるからである[133]。では、意図せずして一方の敵対当事者に不利な影響を与えてしまった場合はどうであろうか。例えば、戦時中に略奪が横行し、文民が特定の地区を頻繁に巡回し警備にあたっていたと仮定する。同時に当該地区で敵の軍隊が後の軍事作戦のための諜報活動を行っていたとすると、文民の警備行為によって敵の当該地区での軍事作戦に不利な影響を与えてしまう可能性がある。この場合、文民が巡回・警備している理由は「敵に不利益を与える」ためではなく、「略奪を予防する」ことにあるため、一方の紛争当事者を支援することが明確に意図されているとは言えないだろう。一方、文民が他の文民に対して暴力行為を行う場合はその判断は分かれる。まず、文民が一方の紛争当事者を支援することを明確に意図して暴力行為が行われた場合、当該行為は交戦者とのつながりがあると判断される可能性が高い。しかし、そのようなことを意図せず、個人的理由により暴力行為を行う場合は交戦者とのつながりは認められない[134]。さらに、文民が紛争とは無関係の動機から戦闘員を暴行した場合も、これと同様に交戦者とのつながりは認められない。なお、特定の紛争地域で文民による暴動や略奪などの社会的混乱が生じた際に文民当局が鎮圧を行う場合、文民当局の行為が危害の敷居を満たす可能性がある。しかし、これは「一方の紛争当事者を支援しかつ他方の当事者を害する形」で引き起こされたわけではないため、「武力紛争当事者間で行われる敵対行為の一部を構成」し得ない[135]。

その上で、サイバー空間における行為では、いかなる行為が交戦者とのつながりを有していると言えるだろうか。交戦者とのつながりでは、当該行為が一方の紛争当事者を支援しかつ他方の当事者を害する形で行われることを求めているが、これはサイバー戦だからと言って特別な解釈を必要とするわ

133）　Melzer, *supra* note 60, p. 61.
134）　*Ibid.*, p. 63.
135）　*Ibid.*, pp. 60–61.

けではない。特定の事例に基づいて考えてみると、例えば、南オセチア紛争時のロシアの愛国ハッカーによるサイバー攻撃の場合は、当然に交戦者とのつながりが認められるであろう。また、FireEye 社や Kaspersky 社のようなサイバーセキュリティ企業が国家の要請に基づき軍事施設のサイバー防御に従事した場合も、交戦者とのつながりは存在する。他方、軍隊に提供しているシステムの定期的なメンテナンス、定期的なソフトウェアのアップデート、修正パッチの適用などの行為は、システムの防護能力を向上させる役割があるが、日常的な行為として行われる場合は交戦者とのつながりを満たさないだろう[136]。なお Schmitt は、メンテナンス、積載及び紛争地帯から遠く離れた地から航空機を発進させる任務に携わっている文民航空エンジニアを引き合いに出し、定期的な性格を有さない緊急のメンテナンスや支援は敵対行為への直接参加に該当する可能性があるとしている[137]。

4.1.4.　保護喪失の時間的範囲

第１追加議定書第51条３項および DPH に関する解釈指針では敵対行為に直接参加している「間（for such time）」は保護を喪失するとしているが、この「間」とはどのような範囲を指すのか。まず、DPH に関する解釈指針によると、当該行為が特定の敵対行為の不可分の一部をなす「準備措置」、「展開」、「帰還」は敵対行為への直接参加に該当する[138]。つまり戦闘のための準備を行い、展開し、戦闘を行い帰還するまでの一連の行為が敵対行為への直接参加に該当することになる。その上で、「明確に軍事的な性質を有し、また事後の特定の敵対的な行為の実施と密接に結びついているもので、すでに当該行為と不可分の一部をなしているもの」[139] が準備措置に該当するとし

136）　Schmitt, *supra* note 15, p. 120.

137）　Michael N. Schmitt, "'Direct Participation in Hostilities' and 21st Century Armed Conflict," *in Horst Fischer, Ulrike Froissart et al., (eds.), Crisis Management and Humanitarian Protection: Festschrift für Dieter Fleck*, (Berliner Wissenschafts-Verlag, 2004), p. 512.

138）　Melzer, *supra* note 60, p. 65.

139）　*Ibid.*, pp. 65–66.

ている。そして、敵対行為への直接参加に該当する準備措置の一例として、DPH に関する解釈指針では「敵対行為が行われる区域にある軍事目標を直接攻撃するため航空機に爆弾を搭載すること」[140]、特定の敵対的な行為の実施のために遂行される「要員の装備、指示及び輸送、インテリジェンスの収集、ならびに武器及び装備品の準備、輸送及び配備」[141] を挙げる。一方、敵対行為への直接参加に該当しない準備措置としては、「武器の購入、密輸および隠蔽、要員の一般的な採用および訓練、ならびに武装行為主体への財政的、行政的および政治的支援」がこれに該当する[142]。なお、実際に保護を喪失する範囲については、「具体的な文脈や行動の時間と場所において、当面する状況を全体的に注意深く評価すること」が重要である[143]。つまり、敵対行為への直接参加に該当しない準備措置を行っている文民を保護するために、文民は敵対行為への直接参加のための「直前の準備をしている間」のみ攻撃対象となるべきというのが、DPH に関する解釈指針における見解である[144]。

しかし、このような見解に反対する意見も存在する。Bill Boothby は、解釈指針が「認識できる直近の準備措置」のみが攻撃からの保護を失うとしている点について、これは現代の武力紛争の様相を考慮できていないものであり、敵対行為への直接参加の概念を狭すぎるものにしてしまうおそれがあると主張する[145]。Boothby は、例えば一連の解釈指針の規定に従うと、定期的にまたは繰り返し武力紛争に参加する文民は敵対行為に直接参加していない限り文民としての保護を享受するが、もし当該文民が武器を準備し継続的に

140）　Melzer, *supra* note 60, p. 66.
141）　*Ibid.*, p. 70.
142）　*Ibid.*, p. 66.
143）　*Ibid.*, p. 67.
144）　*Ibid.*, p. 67, footnote 182.
145）　Bill Boothby, ""And for such time as": The Time Dimension to Direct Participation in Hostilities," *New York University Journal International Law & Politics*, Vol.42, No.3, (2010), p. 748.

隠し持っていたとすると、当該行為は後の戦闘に備えているとも見なすことができると述べる。よって、Boothby はこのような行為を行う文民は敵対行為に直接参加していると見なすべきだと主張する。その上で、敵対行為への直接参加に該当する準備措置であるか否かの区別は、明確な目的を持って戦闘の準備を行っているか否かで判断されるべきであるとする[146]。

解釈指針の見解とそれに反対する見解をまとめると、文民の保護喪失の範囲については「具体的行為アプローチ（制限的解釈）」「確定的離脱アプローチ」の２つのアプローチに基づく検討が可能である。まず具体的行為アプローチでは、当該行為が敵対行為への直接参加に明白に該当している限り文民は直接攻撃からの保護を喪失し続ける、言い換えると、当該行為が敵対行為への直接参加に該当している間のみ保護を喪失することになる。この ICRC によるアプローチは、ICRC が重きを置いている人道的必要性を重視したアプローチであるとも言えるが、当該アプローチの立場は ICTY の判例においても採用されているように思われる。現に Prosecutor v. Stakic 事件判決[147]や Prosecutor v. Limaj et al. 事件判決[148]などを見ると、違法な攻撃の被害者が文民として保護を受けるべき者であるのかを考慮する際に、「『その犯罪が行われた時に』被害者が敵対行為に直接参加していなかったかどうかを検討しなければならないと繰り返し述べ」られており[149]、敵対行為への直接参加の有無を「犯罪が行われた時」に限定して判断するという制限的な解釈がとられている。

ただし、先にも挙げた Boothby のように、このような文民の保護という側面を最大限に引き出したアプローチは、現実の武力紛争には不適合であると主張されている。例えば Schmitt は制限的解釈ではなく拡張的解釈、つま

146）　Boothby, *supra* note 145, pp. 749-750.

147）　ICTY, *Prosecutor v. Stakic,* Case No.IT-97-24-T, Judgment of 31 July 2003, paras. 579, 581.

148）　ICTY, *Prosecutor v. Limaj et al.*, Case No. IT-03-66-T, Judgment of 30 November 2005, para. 176.

149）　新井京「武力紛争法におけるテロリストの位置づけ」『国際法外交雑誌』第108巻第２号、45頁注釈71。

り敵対行為以外にもほとんどの軍隊がその役割として有しているすべての機能や行為を敵対行為への直接参加に含む、という解釈が現実の武力紛争に合致していると主張している。このような主張には２つの根拠が存在する。第１に、紛争の性質の変化である。かつては前線を中心に武力紛争が行われていたが、現代の武力紛争では、兵器技術の進化により近接性の概念、つまり「後方地域」と「最前線」の概念がなくなってきているという点がある[150]。確かにミサイルやUAVの出現により、遠方に居ながら人や物に死傷または破壊を生じさせる攻撃を行えるようになっている。第２の理由として挙げているのが、軍事の文民化である。現在の軍隊では、消防士、技術者、情報・電子兵器の操縦者など、軍隊において必要な任務を文民が担っており[151]、文民はもはや名目上及び外観上のみの文民に過ぎなくなっているのである[152]。

また、具体的行為アプローチのさらなる問題として挙げられるのが文民による地位の「回転ドア現象」である。具体的行為アプローチに従うと、敵対行為に直接参加した文民が攻撃からの保護を喪失するのは「敵対行為に直接参加している間」のみであるため、武器を捨て日常の生活に戻ることで文民が有する直接攻撃からの保護を回復すると解釈できる。つまり、「必然的に、敵対行為への直接参加に従事する間隔に応じて文民が直接の攻撃からの保護を喪失したり回復したりするという帰結」をもたらしているのである[153]。よって昼間は農民（文民）として働き、夜はゲリラ兵として戦闘を行うということも理論上可能になってしまう。また、Schmittも「文民が敵対行為への参加と離脱を繰り返し行い得るのであれば、それによって犠牲となる敵対戦闘員は法に対する尊重を即座に失ってしまうだろう。そのことによって文民たる住民全体が大きな危険にさらされることになる」と述べている[154]。

150） Schmitt, *supra* note 137, p. 511.
151） *Ibid.*, p. 515.
152） Parks, *supra* note 122, p. 132.
153） Melzer, *supra* note 60, p. 70.
154） Schmitt, *supra* note 137, p. 510.

なお、具体的行為アプローチの問題点については、ICRC もかねてより憂慮していた。第１追加議定書のコメンタリーにおいて「戦闘員が状況の変化に伴って、または軍事上の必要に応じて文民としての地位を回復し、その後に再び戦闘員の地位を得ることができるというように、自由に自らを動員解除すること」が許されるならば、「第１追加議定書第43条のもたらした進歩をないがしろにしかねない」としていた[155]。しかし、このような問題が生じているものの、ICRC は文民たる住民を直接の攻撃から保護することが必要であると主張し、「そのような参加が単に自発的、非組織的または散発的に生じているだけの間であれば、行動中の軍隊または武装集団にとっても回転ドアのメカニズムは容認できる」[156] として、具体的行為アプローチの正当性及び必要性を説いている。

そこで、このような問題点に対処するために主張されるようになったのが確定的離脱アプローチである。このアプローチは、直接の攻撃に対する文民の保護の喪失が、敵対行為への直接参加に該当する最初の行為から、敵に認識可能な客観的な方法で当該文民がそのような行為から離脱するまで続くというものであり[157]、敵対行為への直接参加の解釈指針作成に伴う専門家会合の中で、一部の専門家によって明確に支持されていたアプローチである[158]。

155）　Sandoz, Swinarski, Zimmermann, *supra* note 18, para. 1678. ただし DPH に関する解釈指針では、回転ドア現象は法の機能不全によってもたらされているわけではないとされている。つまり、個々の文民は組織された武装集団の構成員とは異なりその行為を予期することは困難であるが、「ある時点において軍事的脅威を示さない文民が攻撃されるのを防止」するという効果をもたらしていると主張している（Melzer, *supra* note 60, pp. 70–71.）。

156）　Melzer, *supra* note 60, p. 71.

157）　ICRC, “Clarification Process on the Notion of Direct Participation in Hostilities under International Humanitarian Law: Expert meeting report（2005）”, p. 59.

158）　例えば Schmitt は、「個人が一度敵対行為に従事したならば、その者は明確に敵対行為から離脱するまでは有効な軍事目標であり続けるべきだ」と述べている。また、Watkin は、攻撃目標区別原則の信頼性を維持するためには、第１追加議定書第51条３項において文民が攻撃から保護される条件も「明確性」及び「信頼性」を有していなければならないとしている。つまり、完全に敵対行為への直接参加から離脱したという証明のためには「投降、戦線へ復帰しないという宣誓をしたうえでの拘留からの解放、武器の返上」などの明確で信頼たる行為を行わなければならないとしている。Schmitt, *supra* note 137, p. 510. Kenneth Watkin, “Humans in the

この会合はチャタム・ハウス・ルールに則って開催されたため[159]、誰がこのアプローチを支持していたかは定かではない。しかし、数人の学者が本アプローチに関連した主張を述べている。

ただし、本アプローチの現実への適用において、敵対行為への直接参加からの「確定的離脱アプローチ」は、個々の文民あるいは現代の武力紛争の様相から考えると現実にそぐわないとの意見も存在している[160]。新井京は、「文民の中には敵対行為への直接参加を強制されている者も少なくはないであろうし、離脱によって報復を受ける可能性も想定しなければならない」と主張するほか、「多数の文民が敵対行為に直接参加し、その後敵対行為から離脱する場合、それぞれの個人を特定した離脱の確認は不可能」であると述べ、本アプローチの実施に関して疑問を唱えている[161]。このように、保護喪失の時間的範囲については、多くの課題が存在する。

では、上記の議論を踏まえ、サイバー戦における保護喪失の範囲はどのように解釈できるか。この点について解釈指針は「ネット攻撃または遠隔制御兵器システムの例のように、敵対的な行為の実施が地理的移動を必要としない場合、敵対行為への直接参加の期間は、当該行為の即時的実行及び当該行為との不可分の一部を形成する準備措置の間に制限されるだろう」[162]（下線は筆者追記）としている。よって、ここで問題となるのは、何が実行または準備措置に該当するかであろう。この点については、タリンマニュアルでは詳細な検討がなされている。まず、少なくとも当該行為の直前または直後の行為も敵対行為への直接参加に含まれることに対して、全会一致の合意を得られている。つまり、サイバー攻撃を行うためにコンピュータの所在地やネ

Cross-Hairs: Targeting and Assassination in Contemporary Armed Conflict," in David H. Wippman, Michael Evangelista (ed.), New Wars, New Laws?: Applying the Laws of War in 21st Century Conflicts (Martinus Nijhoff Publishers, 2005), p. 167.

159）　ICRC, "Clarification Process on the Notion of Direct Participation in Hostilities under International Humanitarian Law: Overview of the ICRC's Expert Process (2003-2008)", p. 3.

160）　Melzer, *supra* note 60, pp. 60-63.

161）　新井「前掲論文」（注149）49-50頁。

162）　Melzer, *supra* note 60, p. 68.

ットワークへの接続ができる場所へ向かう間またはその場所から離れる間は敵対行為への直接参加に含まれる[163]。なお、解釈指針でも示されているように、特定の敵対的な行為の実施のために遂行される要員の装備、指示及び輸送、インテリジェンスの収集、武器及び装備品の準備、輸送及び配備は敵対行為への直接参加に該当する準備措置であるとしていることから[164]、サイバー作戦実施のためのインテリジェンス収集やツールの準備などもこれに該当するだろう。

また、個人が敵対行為への直接参加に該当するようなサイバー作戦を繰り返し行う場合には、特に敵対行為の期間が問題となる。つまり、文民はサイバー攻撃を散発的に複数回行う可能性が高い。例えば戦時に組織化された攻撃者集団が紛争当事者の一方を支援しかつ他方の当事者を害する形でサイバー攻撃を行った場合、当該攻撃者集団の構成員の法的地位は敵の攻撃からの保護を享受する状態と敵対行為への直接参加の状態を行き来する回転ドア状態になる。しかし、具体的行為アプローチと確定的離脱アプローチのいずれの立場を取るべきかについては専門家グループの中でも意見が分かれている。解釈指針の立場、つまり文民がサイバー攻撃を行っている間のみ直接攻撃からの保護を喪失し、当該行為から離脱した段階で保護を回復するという立場（具体的行為アプローチ）であれば、当該攻撃者集団はサイバー攻撃時のみ直接攻撃からの保護を喪失する。他方、敵対行為への直接参加は最初のサイバー作戦ではじまり、断続的な活動中も直接攻撃からの保護の喪失は継続されるという立場（確定的離脱アプローチ）の場合は、最初のサイバー攻撃から確定的に離脱が示されるまでの期間、直接攻撃からの保護を喪失することになる。

4.2.　敵対行為への直接参加に関する各国の見解

ICRC が示した DPH に関する解釈指針は、第１追加議定書第51条３項の規

163）　Schmitt, *supra* note 15, p. 431.

164）　Melzer, *supra* note 60, pp. 66–67.

定を詳細に説明したものであるが、各国はICRCの示した解釈指針をどのように評価しているのか。以下では、各国の軍事マニュアルにおいて敵対行為への直接参加に関する３つの累積要件に対する評価をもとに、各国の立場を明らかにしていきたい。

なお、検討に先立ち、各国軍事マニュアルの国際法上の位置付けについて説明する。本稿で言う軍事マニュアルとは、各国の政府また軍当局が自身の名前・責任のもとに作成したマニュアルを指す。軍事マニュアルは、Law of War Manual、Military Manual、Manual of the Law of Armed Conflictなど、さまざまな名称で作成されたマニュアルを含む。各マニュアルの名称は異なるが、これらマニュアルはいずれも武力紛争法の諸規則に関する各国の見解や解釈を示している。なお、軍事マニュアルの作成目的は、第一に「自国軍隊による国際人道法履行を確保すること」[165]であり、第二に「人道法の個々の観点についての自国の解釈や政策表明を示すこと」[166]である。よって、軍事マニュアルは「当該国家の国際人道法上の個々の問題についての公式かつ明確な見解表明であることから、慣習国際人道法の形成・解釈について必然的に影響を及ぼす」[167]ため、ICRCが示した解釈指針に対し、各国がどのような見解を示しているかを整理することは有益である。以下、ICRCの解釈指針が発表された2009年以降に軍事マニュアルの更新を行い、マニュアルの中で敵対行為への直接参加について言及しているアメリカ、ニュージーランド、デンマークの３カ国について簡単に見ていきたい。

まず、米国国防総省は2015年にLaw of War Manual（以下、戦争法マニュアル）を公表し、武力紛争における武力紛争法の適用について米国の見解を示した。マニュアルでは、敵対行為への直接参加に関して、約11ページにもわたって見解を示す。戦争法マニュアルでは、「ICRCの敵対行為への直接参加を意味する解釈指針の一部は慣習国際法と一致しているが、米国はICRC

165）　樋口一彦「米軍2015年戦争法マニュアルについて」『琉大法学』96号（2017年３月）61頁。
166）　同上、63頁。
167）　同上、64頁。

の解釈指針の重要な部分が適切に慣習国際法を反映しているとは受け入れていない」[168] とし、ICRC による解釈指針の慣習法性を否定している。その根拠として、米国国務省政治・軍事問題のアシスタント・リーガルアドバイザーを務めた Stephen Pomper の論文を引用し、「運用に関する観点から、（ICRC の解釈指針に対する）フィードバックとしては、報告書があまりにも厳格で複雑であり、国家実行を正確に把握しておらず、（いくつかの点では）国家が現実的に目指すことのできる実行を示していない」[169] と主張する。つまり、米国としては ICRC が示した３つの累積基準を実際の戦場に適用することは困難であるとの立場を取っている。その上で、米国として考える敵対行為への直接参加に関する敷居として、「少なくとも、その性質及び目的から敵に実際の損害を与えることを意図した行為が含まれる」[170] ほか、「文民による行為が敵対行為への直接参加に該当するか否かは、紛争において文民が採用する兵器システムや戦争の手法に大きく依存する」[171] というケースバイケースでの判断によるとの見解を示しつつ、敵対行為への直接参加に関連する行動として以下のような例を示している。

A. 敵対する紛争当事者の人や物に危害を引き起こす行為の度合い、例えば

①当該行為が敵対する紛争当事者に属する人や物に死、傷害、損害に対する直接的な原因であるか、または「あれなければこれなし（but for test）」であるか

②当該行為が敵対する紛争当事者の軍事活動や軍事能力に悪影響を与える可能性の度合い

168）US DoD, *supra* note 58, p. 227.
169）*Ibid.*, p.227, foot note 232.
170）*Ibid.*, p. 228.
171）*Ibid.*, p. 229.

B. 当該行為が敵対行為に関連している度合い、例えば
①当該行為が時間的または地理的に戦闘と近接している度合い
②当該行為が軍事作戦に関連している度合い

C. 当該行為の根底にある具体的な目的、例えば
当該活動が、一方の紛争当事者の戦争目標を促進するために他方の紛争当事者を害することを意図している度合い

D. 紛争当事者の戦争遂行努力に関する活動の軍事的重要性、例えば
①当該行為が敵対する紛争当事者に対する一方の紛争当事者の軍事行動に貢献する度合い
②当該行為が、敵対行為に直接関与していると一般的に考えられている行為と比較して、一方の紛争当事者の戦争遂行努力にとって同等以上の価値があるかどうか
③当該行為が敵対する紛争当事者に重大な脅威を与えているか

E. 当該活動が本質的または伝統的に軍事的なものと見なされる度合い、例えば
①当該行為が、敵に対する軍事作戦（戦闘、戦闘支援、後方支援機能を含む）を行う際に、伝統的な軍事力によって行われているか
②当該活動が、戦闘力の使用または適用を決定などの敵対行為の実施に関する決定を行うことを含むか[172)]

上記 A は ICRC における危害の敷居に類似した基準である。本基準では、敵対行為への直接参加と見なす上では、人の死や傷害、物の破壊の存在、または敵対する紛争当事者への不利な影響を及ぼす可能性のある必要があるとしており、この点については、ICRC の DPH に関する解釈指針と同様の見解

172)　US DoD, *supra* note 58, pp. 230–231.

であろう。

上記Bの基準はICRCにおける直接因果関係の基準に該当するものであるが、その内容はICRCとは異なる。戦争法マニュアルでは、B-②で実際に行われる行為が敵対行為と見なされるには「軍事作戦に関連している度合い」からの判断が必要であると示している一方で、「時間的または地理的に戦闘と近接している度合い」という判断基準も示している[173]。他方、ICRCのDPHに関する解釈指針は、「直接因果関係の要件としては、ある程度の因果関係における近接性をあげることができるが、単に時間的または地理的近接性を示すだけの要素とこれを混同すべきではない」[174]とする。つまり、サイバー攻撃や無人航空機による攻撃などは時間的・地理的近接性を有していないが、当該手段とそれによって生じる危害の間には直接的な因果関係が存在しており、「結果として生じる危害との時間的または地理的近接性は、ある特定の行為が敵対行為への直接参加に該当することを示すことがある一方、直接因果関係のない場合には、これら諸要因だけでは十分ではないかもしれない」[175]として、単に時間的・地理的近接性に基づく判断は適切ではないとの見解を示している。この点において、米国はICRCの見解と反対の主張を行なっていると言えよう。

上記Cの基準はICRCにおける交戦者とのつながりと類似したものであり、明らかな相違は見当たらない。

なお、上記D及びEは、ICRCのDPHに関する解釈指針における３つの累積要件には存在しない基準である。特にDについては、戦争遂行努力を敵対行為への直接参加に含むか否かという重要な議論について触れている。DPHに関する解釈指針では、「確かに、一般的な戦争遂行努力と継戦活動は、突き詰めれば双方ともに敵対行為への直接参加の資格に必要な敷居に達する危害を引き起こしうる」[176]が、「一般的な戦争遂行努力や継戦活動は、その

173）　２つの基準は“or”で結ばれているため、累積要件ではない。
174）　Melzer, *supra* note 60, p. 55.
175）　*Ibid.*, p. 55.
176）　*Ibid.*, p. 51.

ような危害を引き起こす能力を単に維持しまたは構築する活動をも含んでいる」[177] として、一般的な戦争遂行努力は敵対行為への直接参加に含まれないとの認識を示している。他方、戦争法マニュアルでは、D-①のように、戦争遂行努力が敵対行為に該当する行為と同等以上の価値を有している場合には敵対行為への直接参加であるとの例示を示しており、DPH に関する解釈指針よりも敵対行為への直接参加の範囲を広く捉えている。

また、敵対行為への直接参加による文民の保護喪失の時間的範囲については、「敵対行為に直接参加した文民は、攻撃を行う軍事的必要性がないため、その参加を永久にやめた後は攻撃の対象にしてはならない」[178] としつつ、文民が敵対行為への直接参加と文民としての活動を交互に繰り返すことにより発生する回転ドアについては、「米国が適用している戦争法は、『回転ドア』保護を与えていない。すなわち、文民が、その正確な時点で敵対行為に直接参加しているか否かに応じて、攻撃対象からの保護を喪失したり回復したりすることを繰り返すという断続的な（off and on）保護である。したがって、例えば､敵対行為に直接参加するパターンに従事していると評価された者は、敵対行為に直接参加する間の期間には、攻撃の対象になることからの保護を回復しない」[179] とし、回転ドアを認めた ICRC の見解と反対の見解を示している。

次に、2019年にニュージーランド軍が公表した Manual of Armed Forced Law（以下、軍事法マニュアル）でも敵対行為への直接参加に関する見解が示されている。

軍事法マニュアルは、敵対行為への直接参加と見なすための独自の基準を示しているが、出典や参考文献において ICRC の DPH に関する解釈指針を触れられていない。

まず、軍事法マニュアルでは、「『敵対行為への直接参加』とは、本質的に

177） Melzer, *supra* note 60, p. 52.
178） US DoD, *supra* note 58, p. 234.
179） *Ibid.*, pp. 235-236.

軍事的な性質を有する意図的な行動であり、次を意図する、または引き起こす可能性があるものを指す」[180] とし、軍事的性質を有さない行為をその対象から除外している可能性がある。

その上で、敵対行為への直接参加に該当する行為として、以下を列挙している。

a. ニュージーランド軍または同盟国の要員に死傷をもたらす行為
b. ニュージーランド軍または同盟国の財産、またはその他の軍事目標を破壊または損傷する行為
c. ニュージーランド軍または同盟国の作戦を事実上妨害する行為
d. 敵対勢力を実質的に支援する行為
e. 文民たる住民や他の保護を享受する人に死や傷害を引き起こす行為、または民用物または軍隊が攻撃を回避する義務を負う他の保護された物に破壊や損傷をもたらす行為[181]

上記 a、b、c、e の行為は DPH に関する解釈指針における危害の敷居に類似する基準である。他方、d については、DPH に関する解釈指針にはない基準であり、米軍同様に一部の戦争遂行努力を敵対行為への直接参加と見なす立場をとっているように思われる。

また、DPH に関する解釈指針における直接因果関係の敷居に類似する基準として「敵対行為から地理的に離れた行為であっても、情報収集、指揮統制、部隊攻撃のための人の募集、サイバー攻撃など、敵対行為に不可欠な部分であれば、直接的な敵対行為の一部として認められる可能性がある」[182] との見解を示している。さらに、交戦者とのつながりに類似する見解として、「これらの例はすべて、その行為が基本的に軍事的性質を持つものでなけれ

180）　New Zealand Defence Force, Manual of Armed Forces Law, DM 69（2ed）, Volume 4, p. 6-15.
181）　*Ibid.*, p. 6-15.
182）　*Ibid.*, p. 6-15.

ばならないという文脈で理解されるべきである。」[183] とし、前述の通り軍事的性質を有さない行為を敵対行為への直接参加の枠組みから除外している。

敵対行為への直接参加の開始と終了については、「直接参加するのは攻撃の瞬間だけではなく、攻撃の前後の活動も『連続した参加』として知られている部分を形成している。敵対行為のための計画、準備、訓練、攻撃現場への展開、そこからの帰還などが明らかに含まれる。連続体の長さは、行動の性質によって異なる。」[184] とし、DPH に関する解釈指針同様に準備及び帰還もその範囲に含む。さらに、保護喪失の時間的範囲としては、「敵対行為に直接参加した文民は、その参加が継続している間に限り、攻撃に対する免責を失う。武器を捨てて平和な活動に戻った人は、もはや攻撃の対象とはならない。参加がいつ始まり、いつ終わるかは、NZDF の司令官または関係する NZDF のメンバーが判断する問題である。」[185] とし、ICRC 同様に敵対行為が終了次第、文民であれば直接攻撃からの保護が回復するとの見解を示している。

最後に、デンマーク国防省が作成した Military Manual でも敵対行為への直接参加について触れられているが、全体的に ICRC の DPH に関する解釈指針の立場に近しい見解が述べられている。

まず、「文民の参加が国際人道法の意味における敵対行為への直接参加となるためには、以下の３つの累積基準が満たされなければならない。」[186] とした上で３つの基準を示している。

基準１：当該行為は、武力紛争当事者の軍事行動もしくは軍事能力に不

183）　NZ Defence Force, *supra* note 180, p. 6-15.

184）　*Ibid.*, p. 6-17.

185）　*Ibid.*, p. 6-17.

186）　Danish Ministry of Defence, Military Manual On International Law Relevant to Danish Armed Forces in International Operations, September 2016, p. 168. なお、軍事マニュアルの該当部分の注釈には「第１追加議定書第51条３項。以下では、敵対行為への直接参加の定義について、例えば、ICRC の『IHL における敵対行為への直接参加の概念に関する解釈指針』（2009年）を参考にする」との記載がなされている。

利な影響を及ぼすおそれがなければならない。または、当該行為は直接の攻撃から保護される人や物に対して、死、傷害もしくは破壊を与えるおそれがあるものでなければならない（敵対行為への参加 - 危害の敷居）
基準２：当該行為と、当該行為または当該行為が不可分の一部をなす協同軍事行動のいずれかから生じるおそれのある危害との間に、直接的な因果関係の結びつきがなければならない（直接参加 - 直接的な因果関係）
基準３：当該行為は、一方の紛争当事者を支援しかつ他方の当事者を害する形で必要な危害の敷居を直接引き起こすことが明確に意図されたものでなければならない（交戦者とのつながり）[187]

上記３つの要件は、DPH に関する解釈指針の内容と完全に一致していることから、デンマークは ICRC の示した要件を受け入れていると解釈することもできる。

また、敵対行為への直接参加の開始と終了については、「保護が失われるのは、その行為自体の間だけではない。文民の保護が失われるのは、直接参加するための準備や、攻撃を開始する場所への往復（これが直接支援となる場合）にも及ぶ。」[188] とし、DPH に関する解釈指針同様に準備、展開、帰還をその範囲に含んでいる。

さらに、保護喪失の時間的範囲については、「敵対行為に直接参加している文民は、その参加が『継続的戦闘行為』の性格を持たない限り、攻撃に対する保護を一時的にしか受けない。言い換えれば、保護は、直接参加が継続される間、中断される。その後、その文民は再び直接攻撃に対する保護を受けることになる。」[189] とし、こちらも DPH に関する解釈指針と同様の見解を示している。

なお、上記３カ国の解釈における大きな違いの１つは、戦争遂行努力を敵

187）　Danish MoD, *supra* note 186, pp. 168-169.
188）　*Ibid.*, p. 172.
189）　*Ibid.*, p. 172.

対行為への直接参加と見なす可能性があるかどうかであろう。サイバー空間での活動、特にサイバー防御に関する技術や能力については、軍事組織よりも民間組織の方が高いレベルを有しているケースもある。そのため、サイバー防御に必要な脅威情報の提供、サイバー防御機器の提供、新たなサイバー防御技術の開発（ウイルス対策ソフトにおける検知ロジックの開発など）は、民間組織が担うこともある。よって、アメリカやニュージーランドの見解に立った場合、上記のような行為も場合によっては敵対行為への直接参加と見られる可能性がある。

5. 文民保護組織・要員の国際法上の扱いについて

重要インフラのサイバー防御に従事する文民は、文民保護組織・要員が担っている役割と類似した役割を担う可能性が考えられるが、そもそも文民保護組織・要員とはどのような者を指すのか。

一般的に、「文民保護」という用語は、文脈に応じて異なる意味で使用される。例えば、宮崎繁樹によると、日本において市民防衛（文民保護）は、武力紛争時の敵対行為による危険災害から一般住民を保護するだけでなく、「災害（disaster）の危険に対しても一般住民を保護し、一般住民が災害の直接的影響・損害から回復するのを援助し、また、一般住民が生き残るために必要な諸条件を備えることを目的として、救急、治療、消防、消毒、応急宿舎・必要品の共有、被災地帯の秩序の回復・維持、緊急な公共施設の応急修理、死者の応急処理、生き残るために不可欠な物資の保存援助などの人道的任務を行うものである」[190] とし、国内における文民保護は、災害救助の側面から枠組みが作られていると評価する。現に、1947年の災害救助法制定による救助枠組みの策定、1961年の災害対策基本法、1978年の大規模地震対策特

190） 宮崎繁樹「市民防衛（民間防衛）について」『法律論叢』第52巻第6号（1980年3月）、27-28頁。「市民防衛」「民間防衛」は「Civil Defense」の訳であるため、本稿における「文民保護」と同義である。

別措置法、そして自衛隊法第83条による災害救助活動の権限付与など、日本においては、災害救助の側面を中心に文民保護が発展していると言えるだろう。

しかしながら、武力紛争法の文脈における文民保護は、災害救助に限定されない。第１追加議定書では、文民保護とは「文民たる住民を敵対行為又は災害の危険から保護し、文民たる住民が敵対行為又は災害の直接的な影響から回復することを援助し、及び文民たる住民の生存のために必要な条件を整えるための人道的任務の一部又は全部を遂行すること」[191]と規定する。文民保護については、二度の世界大戦の教訓を経て、ジュネーヴ第４条約（文民条約）第63条２項に文民保護任務に関する規定が盛り込まれた[192]。当該規定は文民保護組織及び要員の法的保護を初めて明文化したものであったが、その内容にはいくつかの欠点がある。その欠点とは、１）当該規定の保護対象は占領地に所在する文民保護組織のみであること、２）文民保護組織自体は保護されるが、占領国が文民保護要員を徴用し、他の任務を強いることを妨げないこと、３）文民保護組織に対する保護は、「占領国の緊急の安全上の考慮から課される一時的かつ例外的措置に従う」ことが条件であるが、「緊急の安全上の考慮」が定義されていないため濫用の危険性が存在すること、４）第63条の規定の曖昧さにより、警告、避難、避難所の設置など、文民保護組織が行う予防措置はこの条文の対象外であるとの主張があること、５）保護される組織の種類が具体的に定義されておらず、保護が必要な文民保護組織の形態を包含していないこと、であった[193]。その後、ICRC が政府機関や民間組織等と議論を重ね、1977年の第１追加議定書において文民保護に関

191）　第１追加議定書 第61条（a）。

192）　文民条約第63条２項「同様の諸原則は、重要な公益事業を維持し、救済品を分配し、及び救援事業を組織化することによって文民たる住民の生活条件を確保することを目的として既に存在し、又は将来設立される非軍事的性質を有する特別の団体の活動及び職員に対しても、適用する。」

193）　ICRC, Civil defence 1977–1997 – from law to practice. Report from the meeting of experts, 02 July 1997, Introduction, available at https://www.icrc.org/en/doc/resources/documents/report/civil-defence-report-020797.htm.

する具体的な規則が盛り込まれ、現在に至っている。

以下では、第1追加議定書の規定を中心に、文民保護に関する諸規則について検討を行う。

5.1. 文民保護任務の概要

第1追加議定書第61条(a)では、以下の15項目を文民保護の対象となる「人道的任務」と規定する。

(i) 警報の発令
(ii) 避難の実施
(iii) 避難所の管理
(iv) 灯火管制に係る措置の実施
(v) 救助
(vi) 応急医療その他の医療及び宗教上の援助
(vii) 消火
(viii) 危険地域の探知及び表示
(ix) 汚染の除去及びこれに類する防護措置の実施
(x) 緊急時の収容施設及び需品の提供
(xi) 被災地域における秩序の回復及び維持のための緊急援助
(xii) 不可欠な公益事業に係る施設の緊急の修復
(xiii) 死者の応急処理
(xiv) 生存のために重要な物の維持のための援助
(xv) (i)から(xiv)までに掲げる任務のいずれかを遂行するために必要な補完的な活動(計画立案及び準備を含む。)[194]

上記で示した(i)から(xv)のリストは、網羅的なリストである[195]。仮

194) 第1追加議定書 第61条(a)。
195) Sandoz, Swinarski, Zimmermann, *supra* note 18, para. 2341–2342, 2344.

に上記リストを非網羅的なリストと解釈した場合、文民保護任務の中に人道的な性質を持たない機能を含むことが可能となり、文民保護組織及び要員の保護を向上させるための努力が損なわれるおそれがある[196]。一方、本リストに記載されている行為は人道目的で行われる必要があるが、空襲警報、停電対策、消火活動のように戦争遂行努力への貢献と見なされうる活動も含まれている。よって、これらの行為と人道的な行為を区別できるよう、どのような要素の活動を文民保護任務に割り当てるか、明確に定義する必要があるだろう[197]。このような観点から、文民保護任務は、以下の目的のいずれかに合致している必要がある。つまり、１）文民たる住民を敵対行為または災害の危険から保護すること[198]、２）文民たる住民が敵対行為または災害の直接的な影響から復帰するのを支援すること[199]、３）文民たる住民の生存に必要な条件を提供すること[200]、である。ただし、武力紛争の状況において、文民の行為が文民保護任務の一環として行われているのか、または戦争遂行努力、敵対行為への直接参加として行われているのかを瞬時に判断するのは困難である。よって、文民保護要員は、占領地域及び戦闘が現に行われている、又は行われるおそれのある地域において、文民保護の国際的な特殊標章及び身分証明書によって明示的に識別できるようにすることが求められる[201]。

なお、文民保護に関する議論は第二次世界大戦終了後、及び核戦争の危機があった冷戦期に最も活発な議論が行われていたが、近年は取り上げられる機会が減少している。事実、1997年６月30日から７月２日の間に国際民間防

196）　Sandoz, Swinarski, Zimmermann, *supra* note 18, para. 2341.

197）　*Ibid.*, para. 2346.

198）　*Ibid.*, para. 2348.

199）　*Ibid.*, para. 2353.

200）　*Ibid.*, para. 2355.

201）　第１追加議定書第66条３項。文民保護組織、要員、及び物品、建物は国際的な特殊標章によって区別が図られる必要がある（第１追加議定書第66条１項）。特殊標章は、オレンジ色地に青色の正三角形で示すことが求められる（同第66条４項）。また、文民保護組織の医療要員、宗教要員、医療組織及び医療用輸送手段の保護のための識別に関しては、第１追加議定書第18条の規定にも規律される。

衛機関（ICDO）及びICRCが主催した文民保護に関する専門家会合の場で、ICRCは「ICRCの内部でも、1977年以降、文民保護に関する国際人道法の規範がやや軽視されており、20年経った今、これらの規則が十分に現実的でありその有効性を維持しているかどうかを評価する時期に来ているという一般的な見解がある」[202]と述べている。ただし、「より有害な戦争手段の使用や紛争の性質の変化により、文民犠牲者の割合が大きくなっていることを考慮すると、その（文民保護を達成する手段と方法が複雑化している）傾向は顕著である。また、規則が対象となる人々に知られていなければ、このルールは死文化してしまうと認識されていた。そのため、文民保護に関する規則の認知度が低い現状を考えると、その知識を広める努力が必要であると考えられた。」[203]として、引き続き文民保護の発展、周知が必要との見解を示している。なお、7月1日の会合では、文民保護任務に関する武力紛争法の枠組みに関する議論、つまり第1追加議定書第61条に示すリストが有用であるか、実際にこのような任務が文民保護において行われているのかについて議論された[204]。この議論の中では、ある専門家は第61条のリストにおける保護を確保するには、これ以上任務の範囲を拡大しないことが重要だと主張した[205]。他方、参加者の中には、リストが制限的であっても、文章の趣旨に沿ったタスクを含むように広く解釈することができると主張する者もいた[206]。この点について議長は、「人道法は軍隊に受け入れられなければならないため、文民を守るために最大限の努力をしたいという願いと、戦争の現実を認識することの間でバランスを取る必要がある」[207]ことを強調した。なお、本会合でも一部の専門家が「文民保護任務としての文化財保護」の必要

202） ICRC, *supra* note 193.

203） *Ibid.*

204） ICRC, Civil defence 1977–1997 – from law to practice. Report from the meeting of experts, 02 July 1997, Report of meeting, available at https://www.icrc.org/en/doc/resources/documents/report/civil-defence-report-020797.htm.

205） *Ibid.*

206） *Ibid.*

207） *Ibid.*

性を主張していたが、これは軍事的利益と人道的保護のバランスを考慮しながら検討すべき事項であるとされる。このように、第61条（a）の任務内容については、文民の保護を目的とした人道性と武力紛争時の戦闘行為の現実、つまり軍事的必要性との間でバランスを取る必要があるが、バランスを取った上で文民保護任務の幅を維持・拡大することが可能であるとも解釈できる。また、文民保護に関する専門家会合が行われた1997年当時と異なり、現在では「文民による敵対行為への直接参加」に関する検討が進展している。敵対行為への直接参加は、文民保護任務の幅を拡大する上で考慮すべき重要な論点である。よって、第１追加議定書第61条（a）に規定された任務の範囲において、敵対行為への直接参加の要件及び第65条の保護喪失の条件を満たさない限り、文民保護任務の幅を解釈する余地があるだろう。

5.2.　文民による文民保護組織、要員、物品の保護の解釈

次に、文民保護任務を行うことができる主体について整理する。まず、文民保護組織とは、第１追加議定書第61条（a）に規定された任務の遂行にあたり、紛争当事者の権限ある当局によって「専ら」文民保護任務を行うことを目的として組織または認可された団体・組織でなければならない[208]。また、文民保護要員も、紛争当事者により「専ら」第１追加議定書第61条（a）に規定された任務に従事する者を指す[209]。さらに、文民保護組織の物品とは、第１追加議定書第61条（a）の任務のために文民保護組織が使用する機材、需品、輸送手段を指す。このような条件を満たした団体・組織・要員・物品であれば文民保護任務の実施範囲において、特別の保護を享受する[210]。また、文民保護組織の構成員ではないが、権限ある当局の要請に基づき文民保護任務に従事する文民にも保護が適用されるほか[211]、中立国の文民保護組織及

208）　第１追加議定書第61条（b）。
209）　第１追加議定書第61条（c）。
210）　第１追加議定書第62条１項、３項。
211）　第１追加議定書第62条２項。

び国際的な調整を行う団体の要員及び物品についても保護が適用される[212]。

5.3. 文民保護組織に配属された軍隊構成員及び部隊の保護の解釈

第1追加議定書の文民保護に関する規定では、文民保護組織に配属される軍隊構成員及び部隊に関する規定もなされている。しかし、戦闘員たる軍隊構成員による活動であるため、保護の条件が厳格となっている。文民保護組織に配属される軍隊構成員及び部隊は、①第1追加議定書第61条に規定された任務に常時かつ専ら従事する[213]、②文民保護の特殊標章を明確に明示する[214]、③携行する武器も秩序の維持及び自衛の範囲にて使用が可能[215]、④要員は敵対行為及び敵対する紛争当事者に有害な行為を行うことが禁止される[216]、⑤文民保護任務は自国領域内でのみ実行可能である[217]、など文民の文民保護組織・要員よりも厳格な条件が付されている。また、文民保護組織で任務に従事する軍隊構成員及び部隊が敵対する紛争当事者の権力に陥った場合、その者は捕虜となる[218]。

なお、前述の通り、本稿では文民による文民保護を中心に扱うことから、軍隊構成員による文民保護については簡単な紹介にとどめる。

5.4. 文民保護組織・要員としての任務

上記の通り、文民保護組織及び文民保護要員は、特別な保護を享受する存在であるが、実際の武力紛争ではどのような任務を行っているのであろうか。

第1追加議定書第61条第1項に規定された文民保護の任務を踏まえると、例えば、①防空要員、②警察官、②消防士、④水インフラに関わる事業者、⑤通信インフラに関わる事業者が挙げられる。以下で、それぞれの役割にお

212) 第1追加議定書第64条1項。
213) 第1追加議定書第67条1項 (a)(b)。
214) 第1追加議定書第67条1項 (c)。
215) 第1追加議定書第67条1項 (d)。
216) 第1追加議定書第67条1項 (e)。
217) 第1追加議定書第67条1項及び1項 (f)。
218) 第1追加議定書第67条2項。

いて、文民保護任務としてどのような行為を行うことができるのかを検討する。

まず、「①防空要員」が発令する空襲警報は、文民の安全を確保する上で必要不可欠な任務である一方、軍事的利益にも貢献し得る。しかし、文民たる住民を敵対行為による危険から保護することを目的に行われる空襲警報などの発令は、文民保護任務の一環と見なされる[219]。1950年に米国大統領行政府の国家安全保障資源委員会が作成したUnited States Civil Defenseによると、空襲警報の情報は防空警戒を行う軍から、軍の指揮センターに所在する連邦文民保護の空襲警報担当者に渡され、各地に展開、警報が発令されていた[220]。なお、現代においては、文民保護要員が防空監視を行うことは少なくなっているだろう。事実、警報システム自体もデジタル化がなされており、日本においてはＪアラート（全国瞬時警報システム）の整備が進んでいる。また、2022年２月24日より開始されたロシアによるウクライナ侵略では、同年３月10日に空襲警報システムをAndroidに組み込むことをGoogleが発表した。ウクライナ政府は、政府とウクライナ人開発者が作成した「Повітряна тривога（英訳：Air Alarm）」と呼ばれる空襲警報アプリを展開していたが、Googleは本アプリをAndroidに統合しつつ、Google Playでダウンロードできる形を取った[221]。Google社のエンジニアヴァイスプレジデントのDave Burkeによると、本アプリはAndroidに実装されている地震警報用に構築された低遅延警報メカニズムを利用しているが[222]、警報に使用されるデータソースはウクライナ政府が既存の警報システムから取得したものを活用しているという。よって、本システムはウクライナの既存の空襲警報システムを補完するものである[223]。

219）　Sandoz, Swinarski, Zimmermann, *supra* note 18, para. 2358.

220）　National Security Resources Board, United States Civil Defense, NSRB Doc. 128, 1950, p. 33.

221）　Kent Walker, Company Announcements Helping Ukraine, March 4, 2022, at https://blog.google/inside-google/company-announcements/helping-ukraine/.

222）　Dave Burke, https://twitter.com/davey_burke/status/1501996359875891216?s=20&t=0aq8QhPyOEQ6lEI83fUVlQ.

223）　Walker, *supra* note 221.

次に、「②警察官」も文民保護任務が付与された場合には文民保護要員としての地位を有する。警察官の文民保護任務としては、紛争地帯における治安維持の任務が主な役割となるが、敵の攻撃によるパニックの防止、警察通信の確保、交通整理などのほか、不発弾の偵察も警察官が担う場合もある[224]。前出の United States Civil Defense では、「警察は、一般市民や他の文民保護組織から不発弾の報告を受け、爆弾偵察員を派遣して報告を確認し、必要な場合には十分な安全対策を講じる用意が必要」[225] とする。また、「警察は、不発である爆弾やミサイルの場所を特定し軍に報告」[226] し、「不発弾やミサイルの現場での安全対策の適用に責任を負う」が、「実際の不発弾の解除と処分は、軍の責任」[227] であるとしている。なお、警察官は武器を所持している場合があるが、警察自体が軍に編入されていない限り、文民保護要員または文民としての地位を維持するだろう。他方、「犯罪（戦争犯罪を含む）を防止するために警察官が武力を行使（武器の使用を含む）する場合でも、警察官が合法的な攻撃対象になるわけではない」[228]。

「③消防士」については、第1追加議定書のコメンタリーにおいても第二次世界大戦の爆撃事例などから消火活動の重要性を認識しているものの、全ての消火活動が文民保護任務に含まれるとは述べていない[229]。現に、ICRCによる1973年の草案のコメンタリーにおいて、「この定義の文脈においては、消火活動は文民と戦闘に参加していない戦闘員のみを救助または保護し、民用物への損害防止の支援の中で提供すべきである」[230] として、軍事目標の消火活動を明確に除外している。しかしながら、「文民保護任務における消火活動」と「それ以外の消火活動」を区別するのは容易ではない。そのため、

224）　National Security Resources Board, *supra* note 220, p. 58.
225）　*Ibid.*, p. 58.
226）　*Ibid.*, p. 58.
227）　*Ibid.*, p. 58.
228）　Patrycja Grzebyk, “The Status of Police in Armed Conflict,” *Israel Yearbook on Human Rights*, Volume 48, Springer, 2018, p. 116.
229）　Sandoz, Swinarski, Zimmermann, *supra* note 18, para. 2375, 2378.
230）　*Ibid.*, para. 2376.

軍事目標の近郊で消火活動を行う消防士は、攻撃に巻き込まれる危険性がある。例えば、アルメザン人権センターが2009年３月に報告したイスラエルによる「Cast Lead 作戦」に関するレポートによると、2009年１月５日、ガザ市西方にある医療委員会連合広場を標的としたミサイル攻撃により火災が発生、消火を試みていた文民保護チームが爆撃される事例が発生した[231]。この時、死傷者はでなかったが、レポートの付属書によると、イスラエルによる2008年12月27日から2009年１月18日までの Cast Lead 作戦中に消防士として文民保護任務に従事していた９名が死亡、17名が負傷している[232]。死亡者のリストには合計23名、負傷者のリストには合計50名が記載されているが、死亡者数は１番、負傷者数は医療従事者に続いて２番目に多かった。

「④生活インフラに関わる事業者」の例として挙げられるのが、インフラ及び水関連インフラに従事する者である。水は文民の生存において不可欠な要素であり、水に関する事業者は第１追加議定書第61条第１項（xiv）「生存のために重要な物の維持のための援助」に該当する。武力紛争中の水インフラ[233]及び水道事業者の扱いについて、The Geneva Water Hub が2019年にレポートを公開している。そのレポートでは、原則７及び原則17にて以下のように主張する。

> **原則７：水インフラ及び水関連インフラに従事する要員に対する攻撃**
> 水インフラおよび水関連インフラの運用、維持、評価、修理、復旧に関連する活動を行う要員が文民と見なされる場合は、攻撃対象としてはならない[234]。

231）　Al Mezan Center for Human Rights, The Targeting of Medical Centers, Ambulance Teams and Civil Defense Teams during the Israeli Offensive “Operation Cast Lead” against the Gaza Strip 27 December 2008–18 January 2009, 18 March, 2009, p. 19.

232）　*Ibid.*, pp. 31–33.

233）　水インフラには、水道システム及び下水道システム、分散型給排水施設、民間の工場等施設における用水・排水施設などが含まれる。

234）　The Water Hub, The Geneva List of Principles on the Protection of Water Infrastructure, 2019, p. 31.

原則17：人道的アクセスと支援

１．水関連事業に従事する者を含む人道支援要員とその装備は、尊重され保護されなければならない。

２．紛争当事者は、水インフラ及び水関連インフラ、特に文民の生存に不可欠な水を供給するインフラの運用、維持、評価、修理及び復旧のため、水関連活動の従事者を含む人道支援要員とその機材の迅速かつ自由な通行を認め、促進しなければならない。

３．水インフラや水関連インフラの修理・復旧に携わる者を含む文民保護組織とその職員は尊重され、保護されなければならない。

４．紛争当事者は、水関連活動の従事者を含む人道支援要員の安全な通行を可能にするため､水に関する停戦協定を交渉することが奨励される。

５．紛争当事者は、水インフラ及び水関連インフラの運用、維持、評価、修理、復旧のために協力することが奨励される[235]。

原則７では、第１追加議定書第56条５項の規定をもとに、特にダムと堤防に関しては、保護された工作物または施設を防御することを目的として雇用される警備員も、敵対行為に従事しない限り、攻撃から保護されるとの見解を示している[236]。

最後に、「⑤通信インフラに関わる事業者」については、通信は文民保護任務において必要不可欠なものであるため、特に重要な役割を果たしているだろう。例えば、「①防空要員」に関しても、通信インフラが不通となっている場合、空襲警報等を発令することができない[237]。事実、前述のＪアラートでも、内閣官房にて武力攻撃情報を入手後、消防庁の送信システムから衛

235）　The Water Hub, *supra* note 234, p. 71.

236）　*Ibid.*, p. 32.

237）　United States Civil Defense によると、商用の電話サービスが軍司令部の航空担当者と全国の防空警報専用電話とを接続しているほか、「文民保護任務の神経系統は通信である」と述べている。National Security Resources Board, *supra* note 220, pp. 34, 85.

星通信またはインターネット通信を経て国民に警報が発令される[238]。警報の形式も複数あり、防災行政無線、テレビ、携帯電話等へのメール通知などがある。また、2022年に発生したロシア・ウクライナ間の武力紛争でも首都キーウに所在するテレビ塔への攻撃が発生しており[239]、現代の武力紛争において通信網は重要な役割を担っていると言えよう。

なお、ここまで見てきた①防空要員、②警察官、②消防士、④水インフラに関わる事業者、⑤通信インフラに関わる事業者は、いずれも文民保護組織・要員として保護を享受できる可能性があるが、その任務の危険性ゆえ、意図せず攻撃の対象になる可能性もある。いずれの文民保護任務も武力紛争中の最前線で活動が必要である「初動対応者」としての活動であるため、その行為が意図せず敵に対する軍事的な不利益をもたらし、攻撃の対象または攻撃に巻き込まれる可能性もあるだろう[240]。

5.5.　文民保護組織・要員としての保護及び保護の喪失

文民保護組織・要員として認められる者が第１追加議定書第61条（a）に示す文民保護任務に従事する限り、その者は特別な保護を享受できる。この特別な保護には２つの保護が存在する。第１に、文民保護組織・要員は第１追加議定書第１部「敵対行為の影響からの一般的保護」の規定に基づき、尊重されかつ保護される[241]。「尊重されかつ保護される」という用語は、文民保護組織・要員が故意に攻撃され、または文民保護としての任務を不必要に阻害してはならないことを意味する[242]。第２に、絶対的な軍事上の必要が

238）　総務省消防庁「特集10　全国瞬時警報システム（Ｊアラート）による情報伝達における課題と対応」（平成29年度版消防白書、2017年）、at https://www.fdma.go.jp/publication/hakusho/h29/topics10/46067.html。

239）　BBC News「ロシア、首都のテレビ塔砲撃　ウクライナ第二都市の中心部に巡航ミサイル攻撃」（2022年３月１日）、at https://www.bbc.com/japanese/60571213。

240）　他方、第１追加議定書第61条１項にある「(iii) 避難所の管理」「(iv) 灯火管制に係る措置の実施」「(xiii) 死者の応急処理」などは最前線での任務であるものの、上記①～⑤の任務のように緊急性を有するものではないため、攻撃に巻き込まれる可能性も低いと言えるだろう。

241）　第１追加議定書第62条１項。

242）　Bothe, Partsch, Solf, *supra* note 44, p. 447.

ある場合を除き、文民保護の任務を遂行する権利を有する[243]。つまり、文民保護組織・要員は、文民保護任務を敵対する紛争当事者等に妨害されずに実施することができる。ただし、絶対的な軍事上の必要がある場合は、活動の停止や縮小を求められる可能性がある。

なお、文民保護組織・組織の特別な保護も、一定の条件を満たすことで喪失する可能性がある。では、いかなる場合に保護を喪失するか。また保護を喪失した場合、どのような法的効果が発生するのか。

まず、軍の文民保護組織以外の文民保護組織・要員及び物品が受けることのできる保護は、文民保護組織・要員及び物品が本来の任務から逸脱して敵に有害な行為を行い、又は行うために使用される場合に消滅する。ただし、この保護は、適当な場合にはいつでも合理的な期限を定める警告が発せられ、かつ、その警告が無視された後においてのみ、消滅する[244]。つまり、保護の喪失においては、当該行為が「敵に有害な行為」[245]であるか否かが重要となる。1949年にICRCが検討した「敵に有害な行為」の定義は、「軍事行動を促進又は妨害することによって、敵対する当事者に損害を与えることを目的又は効果とした行為」であった[246]。また、「敵に有害な行為」は敵対行為への直接参加よりも広い概念であると解釈する者もいるほか[247]、DPHに関する解釈指針では、「敵に有害な行為」と「敵対行為行為への直接参加」は必ずしも同一ではないものの、類似の基準であると解釈している[248]。よって、

243）　第１追加議定書第62条１項。

244）　第１追加議定書第65条１項。

245）　なお、文民保護任務において、秩序の維持又は自衛のために軽量の武器（ピストル又は連発拳銃のような拳銃）を携行することは敵に有害な行為とは見なされない（第１追加議定書第65条３項）。また、文民保護任務における軍隊との関わり、つまり、１）文民保護の任務が軍当局の指示又は監督の下に遂行されること、２）文民保護の文民たる要員が文民保護の任務の遂行に際して軍の要員と協力すること又は軍の要員が軍の文民保護組織以外の文民保護組織に配属されること、３）文民保護の任務の遂行が軍人たる犠牲者特に戦闘外にある者に付随的に利益を与えることが発生した場合も、当該行為は敵に有害な行為とは見なされない（第１追加議定書第65条２項）。

246）　Sandoz, Swinarski, Zimmermann, *supra* note 52, para. 550.

247）　Bothe, Partsch, Solf, *supra* note 44, p. 457.

248）　黒﨑ほか『前掲書』（注42）、360頁、注18。

第１追加議定書第61条（a）に規定された文民保護任務から逸脱し、かつ当該行為が敵対する紛争当事者の一方に不利な影響を与えた場合は、「敵に有害な行為」と見なされる可能性があるが、その範囲は以下の図のように「敵対行為への直接参加＜敵に有害な行為＜文民としての活動」と表せるだろう。

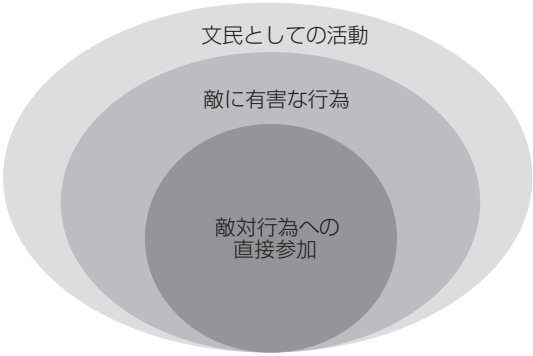

図５　「敵に有害な行為」の位置付け

なお、文民保護組織・要員としての特別の保護の喪失については、「文民保護任務の範囲外で行われる敵に有害な行為」と「文民保護任務の範囲内で行われる敵に有害な行為」の２つのパターンが考えられる。前者については上述の通り当該保護の喪失をもたらすが、後者に関してはどのように判断すべきか。この点について、第１追加議定書第13条の「軍の医療組織以外の医療組織の保護の終了」に関するコメンタリーにおいて、「医療部隊の人道的機能に従って行われた行為が敵に害を及ぼすようなことが実際に起こりうる」[249]とした上で、「このような行為は明らかに例外的行為であり、敵に有害な行為の性質が顕在化した段階で改善を図るべきである」[250]との見解を示した。上記は医療部隊に関する記述であるものの、文民保護組織も同様に解釈すべきかもしれない。ただし、「文民保護任務の範囲内で行われる敵に有

249）　Sandoz, Swinarski, Zimmermann, *supra* note 52, para 552.
250）　*Ibid.*, para 553.

害な行為」が顕在化した段階で改善を図ることを求められた場合、本来文民保護任務として実施すべきことが完遂できない可能性がある。例えば、軍事施設の近隣に所在する民家が敵対する紛争当事者のミサイル攻撃によって延焼したとする。この状況で民家に対して消火を行った場合、当該消火活動によって軍事施設への延焼を阻止することができ、敵対する紛争当事者の軍事行動を妨害したと解釈される可能性もある。よって、「敵に有害な行為」の解釈については、その境界線を示すことは困難であろう。

なお、第１追加議定書のコメンタリーは４つの段階を示し、保護喪失の範囲を説明する。４つの段階とは、①文民保護の任務に就き、専ら当該任務を遂行する場合、②専ら文民保護の任務に就くが、時には敵に害を与えない他の任務を行う場合、③敵に有害ではないが、文民保護任務以外の任務に一時的に割り当てられた場合、④敵に有害な任務への割当て又は敵に有害であることが明らかな任務の遂行の場合である[251)]。コメンタリーによると、①については特別の保護を有する。②については、特別な保護を有することができるものの、条文で規定されている保護の範囲が限定的に適用されるにとどまる可能性がある。③については、当該業務が文民保護任務の枠から外れるため、当然に特別の保護を享受することができない。他方、文民保護任務の枠内の活動に復帰した場合は、特別な保護も回復する。④については、特別な保護を享受できないほか、文民保護組織または要員として保護される権利を永久に喪失する可能性がある。

なお、前述の通り文民保護組織・要員は特別な保護を享受するとともに文民としての保護も当然に享受するため、上記①及び②の場合は文民保護に関する特別な保護及び文民としての保護を享受し、③の場合は文民としての保護を享受することになる。よって、文民保護に関する特別な保護を喪失したとしても、即座に直接攻撃からの保護を喪失するわけではない。また④のケースにおいては、「敵に有害な行為」である限りは文民保護組織及び要員としての特別の保護を喪失するにとどまるが、当該行為が敵対行為への直接参

251）　Sandoz, Swinarski, Zimmermann, *supra* note 52, para 2418.

加に該当する場合は文民としての保護も喪失し、直接攻撃の対象になり得る[252]。その上で、文民保護任務としての特別な保護、文民としての保護、敵対行為への直接参加の関係性は図６のように示すことができるだろう。

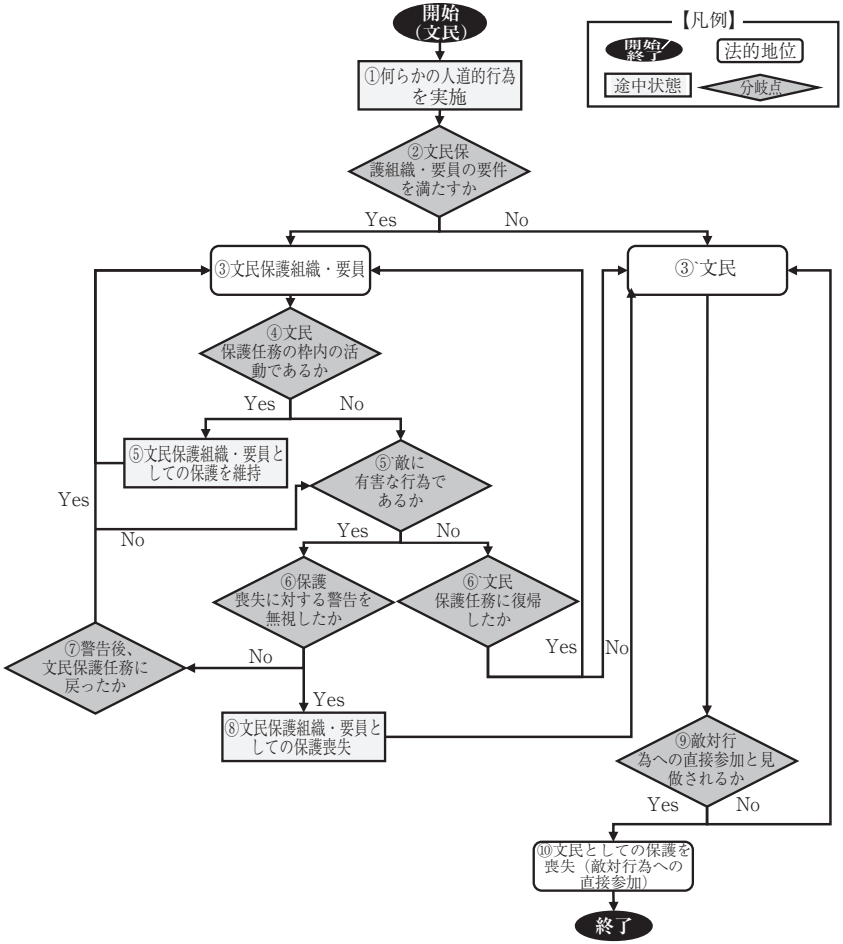

図６　文民及び文民保護組織・要員の法的位置付け

252）　Michael Bothe は、文民の消防団が軍の飛行場で消火活動を行った場合、当該行為は文民保護任務の範囲外であるため敵に有害な行為と見なされる可能性があるが、当該行為が敵対行為

文民が何らかの人道的行為（活動）を行う場合（①）、当該行為が第1追加議定書第61条（b）または（c）の要件を満たしているか否かで、その後の保護の内容が異なる（②）。第1追加議定書第61条（b）または（c）の要件を満たしている場合、その者は文民保護組織・要員と見なされ、特別な保護を享受する（③）。他方、文民保護組織・要員としての要件を満たさない者が行う人道的行為は文民の活動の一部であるため、文民と見なされる（③`）。なお、③で文民保護組織・要員と認められた者も無制限に活動できるわけではない（④）。当該行為が第1追加議定書第61条（a）に示された枠内の活動であれば、文民保護組織・要員としての保護を維持しながら活動できる（⑤）。仮に当該行為が第1追加議定書第61条（a）の枠外の行為である場合、当該行為が「敵に有害な行為であるか」が問題となる（⑤`）。敵に有害な行為である場合、攻撃側は合理的な期限を定める警告を発し（⑥）、その警告が無視された場合に保護を喪失する（⑧）。一方、警告に従い敵に有害な行為を停止し、文民保護任務に戻った場合は保護を回復することになる（⑦）。これは、敵対行為への直接参加における回転ドア同様に、状況に応じて直接攻撃からの保護を回復できるため、その保護の回復については議論の余地があるだろう[253]。なお、文民保護要員が文民保護任務に復帰した際には特別な保護が復活するが（⑦→③）、文民保護任務に復帰しない限り文民としての活動と見なされる（⑥`→③`）。

なお、文民保護組織・要員の行為が敵に有害な行為である場合、及び敵に

への直接参加に当たるかどうかは疑問が残るとしている。よって、この場合において、個々の消防士に対する発砲はおそらく合法ではないが、飛行場に投下された爆弾で死亡した場合は、巻き添え被害として正当化することができるとの見解を示す。Bothe, Partsch, Solf, *supra* note 44, p. 457.

253）　Michael Bothe は「明らかに敵に有害な行為を行った部隊が、嘘偽りのない文民保護任務に切り替えただけで保護を回復できるのであれば、それは適切ではないだろう。」との見解を示した上で、「敵に有害な行為を行ったという合理的な関連性がある限り、保護は停止されるべきである。」と主張する。Bothe, Partsch, Solf, *supra* note 44, p. 458, 459. なお、警告後に文民保護任務に戻らず、文民保護任務の枠外の活動を行なっている場合は、再度、当該活動が敵に有害な行為か否かを判断される状況に戻る（⑤`）。

有害な行為でないが文民保護任務の枠外の行為であり続ける場合、その者は文民と見なされ、直接攻撃からの保護を享受する（③`）。ただし、当該行為が敵対行為への直接参加と見なされる場合、文民としての保護を喪失し（⑨→⑩）、敵対行為への直接参加の要件を満たさない場合は文民としての地位に戻る（⑨→③`）。

上記の検討の通り、文民保護組織及び要員はその地位による特別な保護と文民としての保護の２つの保護を享受していると考えられるが、前者の保護を喪失することによる影響には、どのようなものがあるのか。この点について Michael Bothe は、文民保護組織とその要員の任務遂行が妨げられる可能性があること、及び特徴的な標識の使用が第１追加議定書第38条[254]で禁止されている不適切な使用に該当する可能性があるとしている[255]。よって、すでに述べている通り、文民保護組織・要員としての保護喪失は、直接攻撃からの保護の喪失を意味するわけではない。

その上で、当該保護を喪失した場合、保護喪失期間はどのように解釈されるのか。この点について、第１追加議定書第65条には具体的な規定がなされていない。他方、前述の通り、文民保護任務以外に従事する者が文民保護任務に復帰した場合、特別な保護が回復するというのが第１追加議定書の立場である[256]。また、「敵に有害な任務への配属、または敵に有害であることが明らかな任務の遂行は、特別な保護を受ける権利はなく、おそらくこの権利は永久に失われる。」[257]との見解を示していることから、敵に有害な行為を

254）　第三十八条　認められた標章

１　赤十字、赤新月若しくは赤のライオン及び太陽の特殊標章又は諸条約若しくはこの議定書に規定する他の標章若しくは信号を不当に使用することは、禁止する。また、休戦旗を含む国際的に認められた他の保護標章又は信号及び文化財の保護標章を武力紛争において故意に濫用することは、禁止する。

２　国際連合によって認められた場合を除くほか、国際連合の特殊標章を使用することは、禁止する。

255）　Bothe, Partsch, Solf, *supra* note 44, p. 458.

256）　Sandoz, Swinarski, Zimmermann, *supra* note 52, para. 2418.

257）　*Ibid.*, para. 2418.

行わない限り、文民保護組織・要員としての保護を享受できると解するべきだろう。

6. 文民保護組織・要員としてのサイバー防御の検討

本章では、これまでの検討を踏まえ、第1追加議定書における文民保護規定のサイバー防御への適用可能性について検討を行う。以下では、第3の論点である「サイバー防御を行う組織や要員が文民保護組織・要員と見なされる可能性があるか」、第4の論点である「文民保護組織・要員が行うサイバー防御のうち、文民保護任務と見なされるものとそうでないもの（敵対行為への直接参加に該当するものを含む）は何か」を中心に検討する。

6.1. サイバー防御を行う組織や要員が文民保護組織・要員と見なされるか

すでに検討した通り[258]、サイバー防御に従事する者も、紛争当事者の権限ある当局により組織・承認され、専ら特定のシステムのサイバー防御に従事している限り、文民保護組織･要員と見なすことができると考える。なお、サイバー空間において、文民保護要員と見なされる上で、どのような任務に従事することができるのだろうか。この点について、以下で分析を行う。

6.2. サイバー防御において文民保護任務と見なされる活動

サイバー空間における文民保護任務については､第1追加議定書第61条(a)(i) ～（xv）の各任務をサイバー空間における事象に当てはめることで、検討が可能であろう。事実､第1追加議定書のコメンタリーでも､「文民保護は、戦争の手段と方法の劇的な発展によって文民たる住民に与えられた損失、損害、苦痛を軽減するために国際人道法が行っている取り組みの中で重要な位

258） 文民による文民保護組織、要員、物品の保護の解釈の整理ついては、本稿5.2を参照。

置を占めている。特に、近代兵器が武力紛争法の原則や規則に反して使用されている場合はなおさらである」[259]（傍点は筆者追記）との立場が示されており、戦争手段の発展に合わせた文民保護任務が求められていると言える。また、第１追加議定書第61条（xv）の「補完的活動」によって、「（起草過程時の）各国の戦略的必要性の変化を表現し、技術の進歩に応じて文民保護任務が進化することを可能にする」[260]との見解もある。実際、コメンタリーでは文民保護任務に関する計画や組織化、文民保護要員の訓練、夜間に瓦礫に埋まっている人々を捜索するための一時的な照明設備の設置などを補完的活動として例示する[261]。また、「輸送、被災地へのアクセス、医療目的の発電、他の機能に必要な公共事業の運営（応急修理とは異なる）」といった運用レベルでの任務も追加が可能であるとの見解もある[262]。このようなことからも、人道的な任務の遂行を目的としたサイバー防御（必要な公共事業システムの修理、文民保護に関わるサイバー攻撃対処訓練など）は文民保護任務に含むことが可能であると主張できる。なお、1977年の第１追加議定書起草時には、武力紛争の一要素がサイバー空間で行われることは想定されておらず、物理的空間での敵対行為を念頭に置いていた。そのため、第１追加議定書の内容をサイバー空間に適用することは困難であるようにも思われる。しかしながら、サイバー戦においても、行為自体はネットワークやサーバなどで構成された物理的空間で行われること、そして最終的な影響は物理空間に生じ得ることから、第１追加議定書の規定をサイバー戦の状況に適用することが可能であろう。ただし、物理空間への影響を無視し、サイバー空間における行為のみに焦点を当てて分析を行うと、1977年当時の規定が有する本来の趣旨・目的から逸脱する可能性がある。例えば、サイバー空間への武力紛争法の適用に関しては、データを軍事目標（物）と見なすかどうかが議論されて

259）　Sandoz, Swinarski, Zimmermann, *supra* note 52, para. 2319.

260）　Daphné Richemond-Barak, Ayal Feinberg, “The Irony of the Iron Dome: Intelligent Defense Systems, Law, and Security,” Harvard National Security Journal, Vol.7（2016）, p. 510.

261）　Sandoz, Swinarski, Zimmermann, *supra* note 52, para. 2406-2407.

262）　Bothe, Partsch, Solf, *supra* note 44, p. 441.

いるが[263]、サイバー空間での事象に限定して検討を行う場合、第1追加議定書の規定を本来の趣旨･目的と異なった形で解釈してしまう可能性がある。そのため、検討自体は第1追加議定書の起草当時の趣旨・目的を踏まえ、慎重になされる必要があるだろう。

その上で、第1追加議定書第61条（a）(i) ～（xv）の文民保護任務のうち、サイバー防御に適用可能なものはどれか。適用可能性が高いものとしては、「(xii) 不可欠な公益事業に係る施設の緊急の修復」、「(xiv) 生存のために重要な物の維持のための援助」が挙げられる。以下、これら2つの任務について検討する。

まず、「(xii) 不可欠な公益事業に係る施設の緊急の修復」における「公益事業」について、コメンタリーでは「特に、治水設備（ダム、堤防、排水･放水路、排水溝、水門、閘門、水門、ポンプ設備など)」が含まれるとしているが[264]、「特に」とあるようにその他の公共事業についても含まれるものと解される。よって、一般公衆に供給されるサービス及び商品、例えば、水、ガス、電気、通信もここに含むことができる[265]。なお、文民保護任務において実施可能な修復は､必要不可欠な公共施設の緊急修理に限定されている。したがって、公共施設の欠陥の全てを修復することが許容されるわけではなく、例えば、飲料水の供給が停止した場合や、下水道の不調によって伝染病の危険が生じた場合など、必要不可欠な作業に限定されるべきである[266]。このような点から、公共事業の提供に必要不可欠な要素の修復、例えば公共

263）　例えば、タリンマニュアルにおいては、「国際専門家グループの大多数は、少なくとも現在の法律の状況において武力紛争法における『物』の概念にはデータ含むものと解釈されていない点に同意している」。Schmitt, *supra* note 15, p.437. 他方、ICRC は2015年のレポートにて、「データの削除や改ざんが国際人道法の意味での攻撃を構成しない、あるいは、そのようなデータが民用物への攻撃の禁止を構成する対象とは見なされないからという理由で、この種の作戦がますますサイバーに依存する今日の世界で国際人道法によって禁止されないという結論は、この規範の目的と趣旨に合致しないように思われる」との見解を示している。ICRC, *supra* note 78, p. 43.

264）　Sandoz, Swinarski, Zimmermann, *supra* note 52, para. 2394.

265）　Bothe, Partsch, Solf, *supra* note 44, p. 440.

266）　Sandoz, Swinarski, Zimmermann, *supra* note 52, para 2395.

事業（水道やガス、通信など）のシステムに対してサイバー攻撃が行われた際に、CSIRT がインシデントのトリアージを行い、システム担当者とともにマルウェアを駆除、システムの再設定を行い水道やガス、通信の提供を再開させる行為は、文民保護任務に含まれ得るだろう。

次に、（xiv）における「生存のために重要な物」は、第１追加議定書第54条の「文民たる住民の生存に不可欠な物の保護」よりも広い範囲を含むが、この差異は実務上重要ではなく、どのような行為が対象となるかは「常識が優先される」[267]。その上で、ここで実施される任務は、警備や武器の使用を必要としない任務、例えば破損した可能性のある農業用サイロの一時的な修理などが考えられる[268]。この点、サイバー防御の状況においては、（xii）の任務と同様に住民の生存に必要なものへのサイバー攻撃を監視し、攻撃が発生した際には当該機能が維持できるよう、システムの維持を行う活動が該当するだろう。

また、上記３つの任務については、「（xv）（i）から（xiv）までに掲げる任務のいずれかを遂行するために必要な補完的な活動（計画立案及び準備を含む。）」に則り、補完的な活動も文民保護任務として実施することができる。例えば、文民保護任務としてのサイバー防御を行うために必要となる情報収集（特定のサイバーオペレーションに関する情報、脆弱性情報などの収集）はここに含まれると解釈でき、文民保護任務のための情報収集も許容されると言えよう。なお、文民保護任務に関する先行研究ではサイバー防御に関する言及がほとんどなされていないが[269]、Marco Roscini は「第１追加議定書第61条（a）は文民保護任務の例として『不可欠な公益事業に係る施設の緊急の修復』と『生存のために重要な物の維持のための援助』を含む。専ら文

267）　Sandoz, Swinarski, Zimmermann, *supra* note 52, para. 2402. コメンタリーでは「石鹸が必須又は不可欠かどうかと屁理屈をこねても仕方がない」とし、常識的な判断が求められることを強調する。

268）　Bothe, Partsch, Solf, *supra* note 44, p. 441.

269）　例えば、タリンマニュアルにおいても第１追加議定書第61条から第67条の文民保護に関する規定については触れられていない。

民の国家重要インフラの防御、または破壊された文民の重要サービスの復旧に充てられた者は、文民保護要員に該当する可能性がある」[270] との見解を示している。

一方で、ケースバイケースでの適用が可能と考えられるのが「(i) 警報の発令」と「(viii) 危険地域の探知及び表示」である。コメンタリーによると「(i) 警報の発令」は、主に空襲の際に使用される警報システムを指すほか、敵の陸上部隊が接近した際に住民に警告を与え、適切な勧告を行うことなどを想定していた[271]。なお、文民保護要員として保護される活動は、人道目的で文民たる住民に発せられる警告であるが[272]、敵対行為や自然災害だけでなく、ガスや石油タンクの爆発、航空機事故など敵対行為に起因しない災害への警報も含まれる[273]。つまり、文民たる住民を敵対行為または災害の危険から保護するための警報の発令が含まれ得る。このようなことから、国家 SOC や CSIRT がサイバー攻撃に関する兆候や情報を確認し、人道的な目的で住民に向けて特定のサイバー攻撃の注意喚起を行うことは、文民保護任務と見なされる可能性がある[274]。ただし、警報の発令は、文民の生命に影響を及ぼすおそれがあるものでなければならない。つまり、単なるホームページの改ざんや個人情報漏洩を目的としたサイバー攻撃に関する警報を発するケースは文民保護任務とは言えず、文民として行う警報活動と見なされ得る。他方、飲み水を扱う水道施設のシステムを操作し、飲み水に投与される

270）　Roscini, *supra* note 109, p. 212.

271）　Sandoz, Swinarski, Zimmermann, *supra* note 52, para. 2357.

272）　*Ibid.*, para. 2358.

273）　CDDH/406/Rev.1 para. 41.

274）　実際、アメリカのサイバーインフラセキュリティ庁は、2021年4月26日にロシア対外情報庁（SVR）によるサイバーオペレーションについて注意喚起を公表しており、注意喚起には脅威の概要、攻撃に用いられる手段、対策事項等が含まれている。Cybersecurity & Infrastructure Security Agency, Russian Foreign Intelligence Service (SVR) Cyber Operations: Trends and Best Practices for Network Defenders, at https://us-cert.cisa.gov/ncas/alerts/aa21-116a。また、ロシアによるウクライナ侵略においては、CERT-UA がウクライナ国内のシステムを標的としたと思われるサイバー攻撃に関する注意情報などを公開している。CERT-UA, Новини (News), at https://cert.gov.ua/articles.

薬物の量を変更するようなサイバー攻撃の情報を掴んだ場合、該当する施設にサイバー攻撃の可能性に関する警報を実施し、または飲み水を利用する近隣住民へ飲用を控える旨の警報を実施できると考える[275]。

「（viii）危険地域の探知及び表示」は、「原則として危険区域をマークすることであり、特に許可されていない人の立ち入りを拒否できるようにすること」を想定している[276]。他方で、コメンタリーの中には「ある地域が地雷に覆われていることが判明した場合、文民保護組織がそのような地域への文民の立ち入りを禁止するイニシアチブ（主導権）を取ることを制限すべきではない」[277] との認識が示されていることに注目したい。例えば、国家 CSIRT などがフィッシングサイトや水飲み場攻撃に使用されているサイトへのアクセスに関する注意喚起しているとする。この際に、当該サイトが紛争当事国の軍事行動と直結しない場合は、注意喚起自体は問題とならないだろう。他方、当該サイトがサイバー軍事行動の一環として使用されていた場合、当該注意喚起が敵対行為への直接参加に該当する場合がある。事実、第１追加議定書のコメンタリーでは、地雷原の検知を例に「本項は、戦闘行為中の地雷原の探知、マーキングまたは除去を対象としない」[278] としている。よって、まさにサイバー軍事行動で使用しているフィッシングサイトなどの探知および表示を行うこと、また、入手した情報を自国などの軍事組織に提供するなどした場合は、敵対行為への直接参加に該当し得るだろう。ただし、サイバー空間において、どのサイトがサイバー軍事行動で使用されているか否かを即座に判断することは、極めて困難である。よって、多くの場合、「（viii）危険地域の探知及び表示」はサイバー防御に関する文民保護任務として、直

275）　2021年２月８日、米国フロリダ州の水処理システムにサイバー攻撃者が侵入、飲料水の水酸化ナトリウムのレベルを通常の100倍以上に改ざんする事象が発生している。CNN by Amir Vera, Jamiel Lynch and Christina Carrega, Someone tried to poison a Florida city by hacking into the water treatment system, sheriff says, February 9, 2021, at https://edition.cnn.com/2021/02/08/us/oldsmar-florida-hack-water-poison/index.html.

276）　Sandoz, Swinarski, Zimmermann, *supra* note 52, para. 2379.

277）　*Ibid.*, para. 2380.

278）　*Ibid.*, para. 2380.

接攻撃からの保護を享受しながら実施することは難しいだろう。

なお、「(ii) 避難の実施」、「(iii) 避難所の管理」、「(iv) 灯火管制に係る措置の実施」、「(v) 救助」、「(vi) 応急医療その他の医療及び宗教上の援助」、「(vii) 消火」、「(ix) 汚染の除去及びこれに類する防護措置の実施」、「(x) 緊急時の収容施設及び需品の提供」、「(xi) 被災地域における秩序の回復及び維持のための緊急援助」、「(xiii) 死者の応急処理」については、サイバー防御の文脈への適用は困難であると考えられる。

「(ii) 避難の実施」に関しては、サイバー攻撃によるマルウェア感染をした後に対象のシステムを切り離すなどの事後対応を「避難」と捉えることもできるが、「(ii) 避難の実施」の起草過程では「人の避難」を対象としており、「物の避難（移動、リスクの回避）」は対象となっていないだろう。

「(iii) 避難所の管理」は平時におけるシェルターの建設や組織化を想定しているが[279]、サイバー防御システムの構築や管理は「避難」には該当しないため、サイバー防御の文脈には適合しない。

「(iv) 灯火管制に係る措置の実施」、「(v) 救助」、「(vi) 応急医療その他の医療及び宗教上の援助」は、いずれの内容もサイバー空間への適用が困難だろう。

また、「(vii) 消火」については、ICRC の1973年草案では、「消火活動は、戦闘に参加していない文民と軍人のみを救助または保護し、民用物への損害を防止するための支援を提供」[280] することと解説されている通り、軍事的利益への影響が大きい活動である。サイバー防御の文脈では、インシデントへの対応をすることを日本語の「火消し」[281] と表現することがあるが、第1追

279）　Sandoz, Swinarski, Zimmermann, *supra* note 52, para. 2359.

280）　Draft Additional Protocols to the Geneva Conventions of August 12, 1949, Commentaries, ICRC, Geneva, October 1973 , p. 72 (Art. 54, sub-para. (a)).

281）　例えば、以下のようなものがある。東京海上日動「CSIRT とは？その役割や体制、SOC との違い」（2021年2月5日）、at https://tokiocyberport.tokiomarine-nichido.co.jp/cybersecurity/s/column-detail80。寺本直条、杉浦芳樹、林郁也ほか「我が国における CSIRT の現状と課題」『全国研究発表大会要旨集』（経営情報学会、2015年）、58頁。

加議定書における消火は、物理世界での炎の消火を意味しているため、サイバー防御の文脈には適用できない。

「(ix) 汚染の除去及びこれに類する防護措置の実施」に関しては、サイバー防御においてもマルウェアの感染などが発生するものの、これらの行為は直接的に人に影響を及ぼすわけではなく、物（システム）への感染である場合は「(xii) 不可欠な公益事業に係る施設の緊急の修復」の任務の枠内となるだろう。

「(x) 緊急時の収容施設及び需品の提供」、「(xi) 被災地域における秩序の回復及び維持のための緊急援助」、「(xiii) 死者の応急処理」についても、サイバー空間において文民を保護する上でこれらの任務が必要となる状況はほとんどないため、当該規定に基づく検討は不要であるだろう。

ここまでの検討をまとめると、第１追加議定書第61条１項 (a) に定義される文民保護に関する任務のうち、サイバー防御において適用される可能性があるものは表１の通りである。

表１　第61条１項（a）のサイバー防御への適用可能性

【凡例】○：適用可能性あり、△：ケースバイケース、×：適用可能性なし

第61条１項（a）における任務	サイバー防御への適用可能性	サイバー防御で想定される任務例
(i) 警報の発令	△	サイバー攻撃に関する注意情報の発令（人道的観点に基づく）
(ii) 避難の実施	×	−
(iii) 避難所の管理	×	−
(iv) 灯火管制に係る措置の実施	×	−
(v) 救助	×	−
(vi) 応急医療その他の医療及び宗教上の援助	×	−
(vii) 消火	×	−
(viii) 危険地域の探知及び表示	△	マルウェアに感染しているサイトの国民への共有
(ix) 汚染の除去及びこれに類する防護措置の実施	×	−
(x) 緊急時の収容施設及び需品の提供	×	−
(xi) 被災地域における秩序の回復及び維持のための緊急援助	×	−
(xii) 不可欠な公益事業に係る施設の緊急の修復	○	公益事業（水道やガス、通信など）システムに対するサイバー防御
(xiii) 死者の応急処理	×	−
(xiv) 生存のために重要な物の維持のための援助	○	住民の生存に必要なシステムへのサイバー攻撃の監視、サイバー攻撃発生時の対処
(xv) (i) から (xiv) までに掲げる任務のいずれかを遂行するために必要な補完的な活動（計画立案及び準備を含む。）	○	−

6.3.　サイバー空間における文民保護に関する見解

サイバー空間における文民保護の解釈については、数は少ないものの国際社会においてもいくつかの言及がなされている。

まず、2004年から始まったサイバーセキュリティに関する国連政府専門家会合（the Group of Governmental Experts：以下、GGE）では、2014年から2015年に開催された第４回期の報告書の「III.　国家の責任ある行動規範、規則及び原則」で以下の提案を行った。

> 「国家は、他国の権限が付与された緊急対応チーム（時には、コンピュータ緊急対応チームまたはサイバーセキュリティインシデント対応チームとして知られる）の情報システムに害を与える活動を行ったり、故意に支援すべきではない。国家は、権限が付与された緊急対応チームを悪意ある国際的な活動に従事するために利用すべきではない。」[282]

上記報告書の第４パラグラフでは「４. 複数の国家は、軍事目的の ICT 能力を開発している。将来の国家間の紛争における ICT の利用の可能性が高まっている。」[283] と述べているが、当該提案が平時または武力紛争時のいずれを想定して提案されているかは明らかにされていない。しかしながら、軍事的利益に貢献する活動をしている場合は除き、平時に制限されている内容が武力紛争の状況において許容されるとは考えにくい。よって当該提案は武力紛争の状況においても当てはめることができる可能性があるだろう。

なお、本提案は「オープン、安全、安定的でアクセシブルかつ平和的な ICT 環境の促進を目的とする自主的で非拘束的な責任ある国家の行動規範、規則又は原則を各国に検討」[284] してもらうための提案である点に留意する必

282）　U.N. Doc. A/70/174, para.13（k）.
283）　*Ibid.*, para. 4.
284）　*Ibid.*, para. 13.

要がある。

次に、ICRC の Avoiding Civilian Harm from Military Cyber Operations during Armed には、文民保護組織としての CSIRT について、以下のような記載がなされている。

> 「また、国連の責任ある行動の規範は、国家が他国のコンピュータ緊急対応チーム（CERT）を意図的に傷つけてはならないことを定めている。これに関連して、専門家は、物理的な世界で応急処置を行う医療従事者と同様に、サイバースペースにおける『初動対応者（First Responder)』を保護する必要性について議論した。何人かの専門家は、この文脈で類似性を見つけることは難しいと考えた。具体的には、サイバー空間の『初動対応者』の役割は、単に応急処置に相当するものを提供するだけでなく、一般的には、攻撃の原因を特定し、攻撃を終息させることでもあると仮定すると、サイバー空間の『初動対応者』は、医療従事者、消防士、文民保護組織とは大きく異なる。専門家の間では意見が一致しなかったが、サイバースペースの性質上、物理的な領域との直接的な比較は困難であるという点は概ね認められた」[285]。

上記 ICRC の見解は、医療従事者、消防士、文民保護組織同様に CSIRT が直接攻撃からの保護を享受する可能性について議論したものである。本検討の目的が、医療従事者や文民保護組織と同じ並びで「CSIRT」という人の法的カテゴリーの追加を検討しようとしたのか、または文民保護組織の中に CSIRT の任務を組み込むことができないのかを検討したのかは不明である。ただし、前者の視点で検討していた場合、軍事的観点と人道的観点のバランスを維持するという意味から、新たに保護のカテゴリーを増やすことができ

285) ICRC, Avoiding Civilian Harm from Military Cyber Operations during Armed, 21–22 January 2020, p. 28, at https://www.icrc.org/en/document/avoiding-civilian-harm-from-military-cyber-operations.

ないと考えるICRCの見解には同意できるだろう。他方、後者の視点で検討がなされている場合、すでに見てきたようにサイバー防御は、その一部を文民保護任務に組み込むことが可能であると言える。確かに、一般的なCSIRTの役割としては、攻撃の原因を特定し、攻撃を終息させることである。そのため、人命の維持に直結する医療従事者、消防士、文民保護組織とは異なる可能性がある。しかしながら、CSIRTにはサイバー攻撃を収束させることで人命の維持に必要な設備の回復、つまり「不可欠な公益事業に係る施設の緊急の修復」や「生存のために重要な物の維持のための援助」に寄与できる可能性もあるだろう。

なお、専門家の間で意見が一致しなかった理由としては、CSIRTの業務の幅が広い（またはCSIRT組織によって業務の範囲が異なる）点も挙げられるだろう。上記のように、人命の維持に直結する任務も考えられうるが、サイバー攻撃の原因究明など、人命に関わらない任務も対象となり得る。そのような点からも、サイバー空間における初動対応者の保護については、多くの議論を積み重ねていく必要があると考える。

6.4. サイバー防御における文民保護組織・要員としての保護喪失の可能性

前述の通り、サイバー攻撃を受けたシステムの復旧作業や、水道や電気システムの稼働を維持するため、当該システムへのサイバー攻撃を監視し、攻撃を受けた場合にはシステムの復旧作業を支援する行為は、文民保護任務と見なされる可能性がある。しかしながら、これらに関わる行為であっても、全てのサイバー防御が文民保護組織・要員としての保護を享受しながら実施できるわけではない。

なお、文民保護組織・要員の保護については、①文民保護組織・要員としての保護喪失と②文民としての保護喪失の２段階に分けて検討する必要がある。まず、①文民保護組織・要員としての保護喪失については、すでに述べている通り「敵に有害な行為」を実施しているか否かで判断される。「敵に

有害な行為」は「（文民保護組織・要員としての）本来の任務から逸脱」したものを指す[286]。これは、敵対行為への直接参加よりも広い概念であるが[287]、文民保護任務と敵に有害な行為、そして敵対行為への直接参加の境界線も不明確であり、保護の喪失についてはケースバイケースでの判断が求められることになる。特に、文民の関与における敷居が低いサイバー防御については、より判断が難しいだろう。さらに、文民保護組織・要員としてサイバー防御に従事する場合は、文民を保護する目的で実施されているか否かが重要な指標となるが、当該行為が「文民を保護する目的」で実施されているか否かを判断することは、物理空間での行為以上に判断が難しくなるだろう。

また、②文民としての保護喪失については、敵対行為への直接参加の累積要件に従って判断される必要がある。文民保護任務と敵対行為への直接参加の区分けにおいては、「当該行為の目的」が重要な要素となる。すでに述べている通り、文民保護任務では、１）文民たる住民を敵対行為または災害の危険から保護すること[288]、２）文民たる住民が敵対行為または災害の直接的な影響から復帰するのを支援すること[289]、３）文民たる住民の生存に必要な条件を提供すること[290]のいずれかの目的にて実施されなければならない。他方、ICRC による解釈指針でも各国軍事マニュアルにおいても、敵対行為への直接参加は、一方の紛争当事者を害することを意図していることが必要である。文民保護任務の範囲内の活動においては、上記３つの目的に基づき実施されるため、敵対行為への直接参加には該当しない可能性があるだろう。

286）　第１追加議定書第65条１項
287）　Bothe, Partsch, Solf, *supra* note 44, p. 457.
288）　Sandoz, Swinarski, Zimmermann, *supra* note 52, para. 2348.
289）　*Ibid.*, para. 2353.
290）　*Ibid.*, para. 2355.

7. まとめ／今後の課題

武力紛争の一手段としてサイバー攻撃が用いられているようになった現代において、サイバー攻撃の脅威から自国や重要インフラを防御する重要性は今後も増大することが考えられる。そのため、本稿では武力紛争の状況においても文民の生存に必要不可欠な重要インフラを維持できるよう、サイバー防御の観点から検討を行った。

検討に際しては、戦闘員たる軍隊構成員がサイバー防御を行うのではなく、文民が特別の保護を有しながら対処をできるような方法を探った。本稿の結論としては、サイバー防御に関する任務の一部は文民保護任務と見なされる可能性がある。また、文民保護組織・要員としての地位を認められれば特別の保護のもと、サイバー防御を行えることを確認した。他方で、無条件にサイバー防御を行えるわけではないことも明らかになっている。つまりサイバー攻撃に対処するということは、サイバー攻撃を行う側が期待する効果を低減、または無効化することを意味しており、場合によっては敵対する紛争当事者に対して不利な影響を及ぼす可能性がある。よって、サイバー防御として実施された行為が、文民保護任務の対象外、または敵対行為への直接参加と見なされ、文民保護組織・要員として、または文民としての保護を喪失し、直接攻撃の対象になり得る可能性がある。なお、いかなる行為が文民保護任務の対象外または敵対行為への直接参加と見なされるかについては明確な境界線が存在しないことから、文民が武力紛争時に重要インフラ等のサイバー防御に従事する際は、危険と隣り合わせの状況で対応しなければならないことも予見される。

一方で、あらゆる社会基盤の IT 化が進展していく社会において、今回検討した内容は今後、重要な論点となっていくだろう。そのため、サイバー防御と文民保護については、今後も検討が必要である。特に、技術の発展に伴い、従来戦に比べサイバー戦で用いられる手段、特にサイバー防御は文民が

武力紛争に関与するための敷居を低下させ、知らず知らずの間に武力紛争の状況に巻き込まれる可能性を高めているのは事実である。よって、直接攻撃から保護すべき者については、適格な保護を与えられるよう、本質的な前提から逸脱しない範囲で現状にあった法的解釈の整理・検討が必要であろう。

【付記】インターネット上の資料への最終アクセス日は、全て2022年7月26日である。