武力紛争法における『データ』の法的地位

―― AP1第52条における『物』としての解釈可能性――

茂　木　隆　宏

Ⅰ．はじめに

現代の日常生活において、IT技術は欠かせない存在となっている。例えばX（エックス、旧Twitter）やLINEは、国や自治体からの情報を取得する上で重要なツールとなっているほか、ここ数年様々な分野で利用され始めたマイナンバー制度（マイナンバーカード）により、日本においても日常生活（特に納税や医療機関への受診など）とITの関係性がより緊密になり始めている。

X（エックス）、LINEそしてマイナンバー制度は、それぞれのサービス提供において「データ」が重要な地位を占めるが、これは上記のサービスが停止した場合の影響を考えれば容易に想像がつく。例えば、X（エックス）で自治体が記載した情報が改ざんされ、偽の情報が国内に拡散したらどのような影響が生じるだろうか。LINEの基幹インフラの設定が変更され、家族や友人と連絡を取れなくなったらどうなるか。または、マイナンバー制度で利用されている「マイナンバー（個人番号）」がマイナンバーシステムのデー

タベースから削除された場合、日本国内での生活にどのような影響が発生するだろうか。これらの影響は想像に難くない。それだけ、IT 技術やシステムの根幹を成すデータへの影響は、我々の生活に大きな影響を及ぼしうることを意味している。

このようなデータに対するサイバー攻撃の懸念は、武力紛争の状況においても同様である。例えば以下のようなシナリオを考えることができよう。

> 20XX 年４月、赤国と青国の間で長年国境が未確定であった地域をめぐり軍事的な衝突が発生、紛争の激化に伴い赤国と青国は国際的武力紛争に突入した。20XX 年６月、赤国は青国の軍事システム、特に軍隊の指揮システムに対するサイバー攻撃の実施を計画した。赤国のサイバー部隊による偵察活動の結果、青国軍隊の指揮システムは、複数の物理サーバで構成されたシステム基盤上に仮想サーバ[1)] が構築され、仮想サーバ内で赤国軍隊の軍事能力分析、作戦の立案、作戦のシミュレーションなどが行われていることが判明した。赤国は当該システムを停止させることが青国の軍事能力を妨害する上で重要であると判断し、サイバー攻撃を実施した。

上記の内容は、筆者が考えた仮想的なシナリオであるが、シナリオで示されたシステムの構造を図示すると図１のようになる。

図１で示したシステム構造に対し、赤国サイバー部隊による攻撃オプションは以下の３つが考えられる。つまり、①物理サーバに対する攻撃、②指揮システム（仮想サーバ）への攻撃、③軍事作戦データベース内の情報に対する攻撃である。

---

1) 仮想サーバとは、物理サーバの上に仮想化技術を用いて構築されたサーバを指す。物理サーバは筐体を有するが、仮想サーバの場合は特定のソフトウェアを利用してサーバ機能を実現しているため、仮想サーバ自身では物理的な筐体を有さない。しかしながら、物理サーバと同じような機能を実現することができる。なお、本稿では「仮想マシン」という用語も使用しているが、仮想サーバは仮想マシンの一分類である。

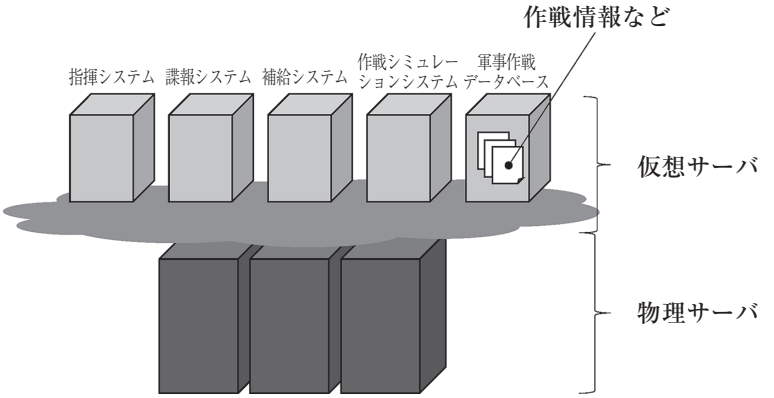

図１　システム構造

それぞれの攻撃対象の用途、性質、攻撃手法、効果などは表１に示す通りである。

表１　シナリオにおける赤国の軍事オプション

	①「物理サーバ」に対する攻撃	②「仮想サーバ（指揮システム）」に対する攻撃	③軍事作戦データベース内の「情報」に対する攻撃
攻撃対象の用途	軍隊のシステム基盤	軍隊の指揮システム	作戦の立案に使用される赤国軍隊に関する情報
攻撃対象の性質（ファイルタイプ）	有形物（ファイルタイプなし）	無形物（例：.vmdkファイル）	無形物（例：.dbファイル）
攻撃手法の例	物理的な破壊、サイバー攻撃（DDoS、BIOSの脆弱性を突く攻撃など）	サイバー攻撃（仮想化ソフトの脆弱性を突く攻撃など）	サイバー攻撃（データ改竄、削除、暗号化など）
攻撃による効果	軍のシステム全体の停止、物理サーバの物理的な損壊	指揮システムの停止、仮想サーバの削除（非物理的な損壊）	作戦の停止・遅延、情報の削除（非物理的な損壊）

攻撃対象となる「物理サーバ」「仮想サーバ」「情報」の３種類が考えられるが、「物理サーバ」は有形物であるのに対し、「仮想サーバ」及び「情報」はファイル形式で構成される「無形物」である。これら３つへの攻撃を実行した場合、物理サーバであれば軍隊のシステム全体の停止や、物理サーバの物理的な損壊を生じさせることができる。対して、仮想サーバへの攻撃であれば対象のシステム、または仮想サーバの削除（非物理的な損壊）が発生する。また、軍事データベースに格納されている情報ファイルを削除した場合、特定の軍事作戦の停止や遅延、情報の削除（非物理的な損壊）といった影響を生じさせる可能性がある。

このように、攻撃対象によって得られる軍事的利益の種類が異なるものの、武力紛争法の適用を検討する上で肝となるのが「攻撃対象の性質」である。例えば、軍事目標について規定した第１追加議定書（以下、AP1）第52条２項では、「物については」との前置きのもと、軍事目標の要件を示している。第52条２項の要件に基づくと、「物理サーバ」についてはここで言う「物」に該当するため、軍事目標または民用物としての判断は比較的容易である。一方、「仮想サーバ」及び「情報」については無形物であることから、「物」としての軍事目標の要件が適用されるのか、または民用物とみなすべきなのかという疑問が生じる。

上記疑問に関して、ファイルが「物」に該当する場合、武力紛争法における軍事目標の要件に従って攻撃の可否を判断することが求められるため、新たな問題は生じ得ない。他方、ファイルが「物」に該当しない場合、当該サイバー攻撃は AP1において「物」に対する攻撃や軍事行動を規律している規則の制約を受けない可能性がある。もちろん、AP1第52条２項で規定されている「物については」との文言に注目し、データは軍事目標ではないとの見解も成り立つ可能性がある。この場合、第52条１項の民用物の定義をもとに「データはすべて民用物である」と主張することも可能であろう。他にも、AP1第52条１項では「民用物とは、２（項）に規定する軍事目標以外のすべての物をいう。」（括弧は筆者追記）と規定されているため、ファイルが物に

該当しない場合は、軍事目標でも民用物でもない第３のカテゴリーの存在が主張できるかもしれない。加えて、第51条４項の無差別攻撃に関する規則では、(a)では「特定の軍事目標のみを対象としない攻撃」、(b)では「特定の軍事目標のみを対象とすることのできない戦闘の方法及び手段を用いる攻撃」が無差別攻撃に該当すると規定する。しかしながら、ファイルを軍事目標でも民用物でもないと解釈する場合、ファイルは上記(a)(b)に該当しないため、無差別攻撃が可能であるようにも解釈でき、これまで武力紛争法が規律してきた軍事的利益と人道性のバランスを崩しかねないであろう。

さらに、仮にデータを「物」とみなすことができたとしても、第52条２項のそのほかの規定、つまり「その性質、位置、用途又は使用が軍事活動に効果的に資する物であって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をもたらすもの」を満たしうるのかという論点もある。特に、データへの攻撃においては人や物に対する物理的な影響を及ぼさずに軍事的利益を得られる場合も考えられる。そのような場合に、軍事目標としての要件を満たしていないと解釈するべきか否かは、本稿において検討するに値する。

本稿は、上記の疑問解決ための糸口を見つけることを主眼に置き、検討を行う。まず、Ⅱ章では、そもそも本稿におけるデータが何を指すのかについて、一般的な見地から確認を行う。Ⅲ章では、サイバー攻撃が武力紛争法の規律対象である「軍事行動」「攻撃」に該当するか否かを論じる。そもそも、サイバー攻撃が「軍事行動」「攻撃」に該当しない場合、武力紛争法における区別原則、予防措置などの規律対象外となるため、「データが物に該当するか」という議論自体が不要となる。他方、特定のサイバー攻撃が「軍事行動」「攻撃」に該当する場合、ファイル、特にデータが軍事目標に該当するか否かで、当該サイバー攻撃に対する武力紛争法上の評価することができよう[2)]。Ⅳ章では、AP1第52条における「物」にデータが含まれるか否かを検

2)　データとは、「０」と「１」の二進数によって構成された、情報を保存、加工、伝送できる形式のことである。また、ファイルとは特定のデータの集合体を指す。よって、以下では最小単

討する。データが物に該当しない場合は、前述のように一部の武力紛争法が適用されない。一方、データが物に該当する場合は、武力紛争法における標的法（Law of Targeting）における規律対象としてあり続ける。また本稿ではデータが「性質、位置、用途または使用が軍事活動に効果的に資する」、及び「全面的または部分的な破壊、奪取、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をもたらす」という軍事目標の要件を満たすかについても、考察していく。Ⅴ章では、データに限らず、武力紛争法において非物理的対象に対する攻撃をどのように扱ってきたかを検討する。結論としては、武力紛争法の大部分が形成された1977年以前において、非物理的対象が軍事作戦に大きな影響を与える場面が少なかったため、武力紛争法の検討における主題にはならなかった。だが、過去の経緯を振り返ることで、今後、データの法的解釈を検討する上での参考になるだろう。

なお、本稿ではAP1第52条の規定を中心に検討を行うが、当該規定はすでに慣習法化されている。事実、多くの国の軍事マニュアル等でもその定義が採用されているため[3)]、本検討はAP1の締約国、非締約国の双方に関わる内容であることを述べておく。

Ⅱ．データとは

そもそも、本稿で検討の対象となるデータとは何か。「データ」という用語は日常的にも幅広く使用されるため、比較的想像がしやすいであろう。身近な例で言うと、パソコンを動かすOperation System（OS）、パソコンに保存されているPDF、Webページを閲覧した際に格納されるキャッシュデータ、またはパソコン等の電子機器に感染するマルウェアなどがデータに含まれる。

位である「データ」の法的扱いを検討していくが､検討内容は「ファイル」にも適用可能である。

3) Jean-Marie Henckaerts, Louis Doswald-Beck, *Customary International Humanitarian Law, Volume I :Rules*（Cambridge University Press, 2005）, p. 29-p. 32.

しかしながら、データの定義を問われた際には、すぐに思い浮かぶ人は少ないのではないか。辞書における「データ」の定義としては、Cambridge Dictionary によると「情報、特に事実や数字を調査・検討し、意思決定に役立てるために収集された情報、またはコンピュータで保存・利用できる電子形式の情報」がある。広辞苑では「①立論・計算の基礎となる既知のあるいは認容された事実・数値。資料。与件。②コンピューターで処理する情報」と記されている。

他方、技術的視点における定義としては、NIST（National Institute of Standard and Technology）による定義が参考になる。NIST が出版する文書の中で幾つかの定義がなされているが、「０バイト以上（８ビット）の可変長文字列」[4]、「特定の方法でフォーマットされた個別のデジタル情報」[5] 等がある。また、「人間または自動手段によるコミュニケーション、解釈、または処理に適した方法での事実、概念、または指示の表現。」[6] といった定義もなされている。一方、サイバー戦への国際法の適用について扱ったタリンマニュアル[7] では、「情報を伝達するためにコンピュータによって処理または生成することのできる基本的要素。基本的なデジタルデータの単位はバイトである」[8] とする。

4）　NIST, *Recommendation for Pair-Wise Key Establishment Using Integer Factorization Cryptography*, NIST Special Publication 800–56B Revision 2, March 2019, p. 10.

5）　NIST, *Guide to Integrating Forensic Techniques into Incident Response*, NIST Special Publication 800–86, August 2006, C-1.

6）　NIST, *Engineering Trustworthy Secure Systems*, NIST Special Publication NIST SP 800–160v1r1, November 2022, p. 52.

7）　タリンマニュアルは、2013年に発刊された Tallinn Manual on the International Law Applicable to Cyber Warfare（通称、タリンマニュアル1.0）と、2017年に発刊された Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations（通称、タリンマニュアル2.0）がある。本稿では、特別な区分が必要な場合以外は、タリンマニュアル1.0とタリンマニュアル2.0を総称し、「タリンマニュアル」と表記する。

8）　Michael N. Schmitt（ed.）, *Tallinn Manual 2.0 of the International Law Applicable to Cyber Operations*（Cambridge University Press, 2017）, p. 564.

上記の内容から、データには固有の定義が存在していないものの、「コンピュータ内で、二進数で扱われる０バイト以上の文字列」がデータに該当すること、また、データの定義を考える上ではデータの形式は特に問題とならないことが言える。よって、本稿ではデータの定義を「パソコン、サーバ、ストレージ、スイッチ、その他アプライアンス機器の動作に必要となる、またその内部で生成・管理される情報」とし、以後の検討を行う。

なお、上記の定義も範囲が広範であるため、本稿の検討対象となる「データ」を個別に列挙することは困難である。しかしながら、どのようなものがデータに該当するかをイメージしなければ検討を行うこともできない。そこで、サイバー作戦において影響を受ける可能性があり、かつシステム上で扱われることが多いデータの例を表２に示す。

表２　データの例

データ	サイバー攻撃手法（例）	サイバー攻撃による効果（例）
仮想マシン（仮想サーバ）[9]	仮想ソフトウェアの脆弱性を突く攻撃	リモートコード実行によるサーバの制御取得など
個人情報（例：マイナンバー）	情報の改ざん、削除、窃取	個人情報流出による社会混乱の誘発など
Web サイト（HTML コード[10] など）	Web サイトの改ざん	Web サイトの利用停止や異なる Web サイトへの誘導、誤情報の表示など
文書ファイル（PDF、Word など）	情報の改ざん、削除、窃取、暗号化	文書ファイルの利用停止など

9）　仮想マシンは、サーバ上または PC のコンピューティング環境内に別の OS やアプリケーションを作る技術である。仮想マシンは、例えば Mac OS の PC 上で Windows OS を利用する場合、Windows OS の PC 上で Linux OS を利用したい場合などに利用される一般的な技術である。サイバーセキュリティにおいては、Windows 環境で動作するマルウェアの解析時に、マルウェアの感染拡大を予防するため、Mac OS の PC 上に Windows OS で検証環境を構築する場合などがある。

10）　HTML（Hyper Text Markup Language）とは、Web ページを作成するための言語である。HTML を使用して Web ページのコードを記述し、その内容をブラウザ上に表示する。

データベース[11]	SQL インジェクション[12]	データベース内容の情報窃取、改ざん、削除など
アプリケーション	バッファオーバーフロー[13]	アプリケーションの停止、情報の漏洩など
ログ[14]	ログの改ざん	インシデントの検知遅れなど

Ⅲ.「軍事行動」及び「攻撃」の定義の検討

そもそもサイバー攻撃には、AP1に定義される「軍事行動」や「攻撃」に相当するものが存在するのであろうか。以下、この点について、検討を行う。

1．軍事行動

AP1のコメンタリーでは、軍事行動の定義についていくつかの記載がなされている。例えば、AP1第３条コメンタリーでは、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」[15] と定義される。またAP1第48条のコメンタリーでは「辞書によると、『軍事行動』とは、軍隊によって行われる

11）　データベースとは、構造化した情報またはデータの組織的な集合を指す。マイナンバーで利用される氏名、性別、生年月日、住所などの情報もデータベースに格納され、必要に応じてデータベースに検索をかけて情報を利用する。

12）　SQL インジェクションとは、データベースに送信されるデータに SQL 文を挿入し、不正にデータベースを操作できるようにする攻撃手法のことである。

13）　バッファオーバーフローとは、サーバのメモリなどに対して大量のデータを送信し、メモリ領域を枯渇させることでシステムの誤作動などを発生させる攻撃手法のことである。

14）　ログには、PC のログイン履歴やファイル編集履歴などの操作ログのほか、セキュリティ機器（例えばファイアウォールや Endpoint Detection and Response など）で検知されたものも含まれる。

15）　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. 152.

敵対行為に関連するすべての移動（movements）と行為（acts）」[16]と、AP1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）を意味する」[17]との説明が付されている[18]。

一方で、サイバー文脈における「軍事行動」については、AP1及びコメンタリーのいずれにおいても定義されていないが、タリンマニュアルでは定義がなされている。つまり、タリンマニュアルではサイバー行動とは、「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。このサイバー行動という用語は、この後に検討する「攻撃」や「サイバー攻撃」よりも広い範囲を含む用語である。よって、心理的サイバー行動[19]やサイバー諜報など、攻撃の概念に含まれない行為がサイバー行動に該当すると言える[20]。

２．攻　撃

武力紛争法における攻撃の定義は、辞書的かつ一般的に広く知られている定義とは異なる[21]。AP1では、「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」[22]と定義する。「攻撃」の定義には、攻撃行為のみならず防御行為（特に反撃）も含まれており[23]、「戦闘行為」という意味合いに近い。なお、AP1の定義によると、武力紛争法上の

16）　Sandoz, *supra note 15*, para. 1875.

17）　*Ibid.,* para. 1936.

18）　AP1において軍事行動への規制を行っている規定としては、第44条３項、５項、第48条、第51条１項、７項、第54条３項(b)、第56条２項(a)～(c)、第57条１項、４項、第58条、第59条、第60条１項などがある。

19）　心理的サイバー行動（Psychological Cyber Operation）は、ソーシャルエンジニアリングなどをもとに人間の心理的脆弱性に付け込み、サイバー攻撃を成功させることを指す。

20）　Schmitt, *supra note 8*, p. 415.

21）　広辞苑では、攻撃とは「攻めてうつこと。進んで敵を攻めうつこと。」であると定義する。

22）　AP1第49条第１項。

23）　Sandoz, *supra note 15*, para. 1880.

「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」の要素が重要となる。ここで言う「暴力行為」とは、物理的な力を意味する[24]。「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、経済戦が含まれない[25]。他方、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ものの、「攻撃」に該当すると見なされている[26]。さらに、攻撃目標に対してキネティック、非キネティックを問わず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」と解釈する論者も多い[27]。

その上で、サイバーの文脈における攻撃の定義を見ると、前述のタリンマニュアルでは「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」[28] と規定される。なお、タリンマニュアルのサイバー攻撃の定義に関する説明では、「暴力行為」という用語が用いられていない。よって、システムの挙動を変え、火災などを引き起こすような、「暴力行為」に該当するか否かの判断が難しい行為も攻撃の概念に含まれることになる。

タリンマニュアルのコメンタリーでは、どの程度の被害を「攻撃」とみなすかについても議論されている。多数派の見解としては、「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」との立場をとっている。さらに、多数派の一部は、「機能への干渉は、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

24）　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.

25）　Bothe, *supra note 24*, p. 329.

26）　Schmitt, *supra note 8*, p. 415.

27）　黒崎将広・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。

28）　Schmitt, *supra note 8*, p. 415.

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」[29] と主張する。その上で、「特に、特定のデータを操作したり、特定のデータに依存したりすることで特定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」[30] 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」[31] との見解を示した。しかしながら、インフラの意図した機能を停止させるサイバー攻撃全てが武力紛争法の対象となるわけではない点には注意が必要である。現に、「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」[32] 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」[33] との見解を示している。

一方、ICRC はタリンマニュアルよりも攻撃の範囲を広く解釈している。ICRC は、「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」[34]（下線は筆者追記）と主張する。これは、AP1第52条２項における「無効化」という要件に注目した考え方である。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、対象物を単に無効化することも攻撃とみなされるべきであると結論づけることができる」[35] という考えが、ICRC による見解である。

29）　Schmitt, *supra note 8*, p. 417.
30）　*Ibid.*, pp. 417–418.
31）　*Ibid.*, p. 418.
32）　*Ibid.*, p. 418.
33）　*Ibid.*, p. 418.
34）　ICRC, “International Humanitarian Law and the Challenges of Contemporary Armed Conflicts”, Geneva, October 2015, p. 41.
35）　Knut Dörmann, “Applicability of the Additional Protocols to Computer Network Attacks”, *CICR Resources*（November 19, 2004）, p. 4.

上記のようなタリンマニュアル及びICRCの見解に対し、Schmittは「タリンマニュアルの専門家と同様に、ICRCの見解もサイバー作戦を攻撃と認定する際には、ある敷居までは必ずしも結果の重大性ではなく結果の性質が重要であることを認識している」と分析する[36]。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っている」ことを課題として挙げている[37]。

武力紛争法における攻撃の規制については、AP1第52条２項の「攻撃は、厳格に軍事目標に対するものに限定する。」との規定から、軍事目標に対する攻撃は合法、民用物に対するものは違法となる。また、「軍事行動」は「攻撃」を包含する概念であるため、軍事目標に対する軍事行動も合法である。一方、AP1第57条１項では、日本語訳の条文で「軍事行動を行うに際しては、文民たる住民、個々の文民及び民用物に対する攻撃を差し控えるよう不断の注意を払う」ことが規定されているため、「攻撃」のみが禁止されているように解釈できる。しかし、英語の正文では「In the conduct of military operations, constant care shall be taken to spare the civilian population, civilians and civilian objects.」（下線は筆者追記）と規定されており、日本語訳における「攻撃（attack）」よりも広い範囲で文民や民用物に対する危害を控えるよう求めている。よって、AP1第57条１項の規定に基づき、民用物に対する軍事行動は禁止されないものの不断の注意を行う必要がある。

36）　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. 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みなされてきていない」との見解を示している。ICRC, *supra note 34*, pp. 41–42.

37）　Schmitt, *supra note 36*, p. 340.

Ⅳ．データはAP1第52条に言う「物」か？

AP1では、「物」という用語をいくつかの規定で用いているが[38]、「物」の解釈において特に重要となる「軍事目標」と「民用物」の関係では、AP1第52条１項及び２項にて以下のように規定される。

> １　民用物は、攻撃又は復仇の対象としてはならない。民用物とは、２に規定する軍事目標以外のすべての物をいう。
> ２　攻撃は、厳格に軍事目標に対するものに限定する。軍事目標は、物については、その性質、位置、用途又は使用が軍事活動に効果的に資する物であって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をもたらすものに限る。（下線は筆者追記）

上記の通り、軍事目標と民用物は表裏一体の関係性にあるが、「物」という同じ用語を用いて定義されている。そこで、以下ではまず「軍事目標としての要件」と「軍事目標への攻撃時に求められる要件」の２つの観点について検討を行った上で、本稿の目的でもある「物」の解釈について、検討を行う。

１．軍事目標としての要件

「性質、位置、用途又は使用が軍事活動に効果的に資する物」の要件をデータに当てはめると、どのように解釈ができるであろうか。

第１に「性質」とは、「武器、装備、輸送機、要塞、倉庫、軍隊が占有する建物、軍隊の本部、通信センターなど軍隊によって直接使用されている全

38)　例えば、AP1第20条、第53条(b)(c)、第54条２項、３項、第56条１項、６項、７項などがある。

てのもの」[39] を指す。よって、データにおいても軍隊で使用されているもの、例えば C4ISR システムに蓄積されているデータベース情報、当該システムの設定情報ファイルなどは「性質」の要素を満たす。また、軍隊がサイバー作戦に使用するマルウェアについても、性質の観点から軍事目標に該当すると言える。

第２に、「位置」とは、「その場所によって軍事行動に効果的に資するもの」[40] をいう。例えば、橋や道路、建物といった民用物も、その所在地ゆえに軍事行動にとって特別に重要な場所である場合は、軍事活動に効果的に資する「位置」に所在するとみなされる可能性がある。一方、データについては物理的な空間に所在するわけではないため、「位置」については議論の対象にならないであろう。また、データが所在するシステム内の場所（ディレクトリ）は、たとえ軍事システム用のディレクトリに所在していたとしてもシステム全体が軍事目標に該当するため、軍事目標としての評価には影響を及ぼさない。

第３に、「用途」とは、ある物の想定された将来の使用をいう。よって、大部分の民用物は軍隊にとって活用可能なものとなる[41]。なお、「ここで問題となるのは想定された将来の使用であり、実際の使用と区別される基準である」[42] 点に留意する必要がある。ゆえに、建設されてまもない軍事施設や軍隊の艦船を建造・整備・維持するための民間造船会社の設備は、実際に機能しているかどうかに関わらず「用途」の基準を満たしうる[43]。データの観点では、民間企業で構築されたマルウェアやサイバー攻撃に利用可能な仮想マシン（例えば、Kali Linux など）が軍事的に利用されることになった場合、対象のマルウェアや仮想マシンが民間企業内に所在していたとしても、「用途」の観点から軍事目標の要件を満たす可能性がある。

39）　Sandoz, *supra note 15*, para 2020.

40）　*Ibid.*, para 2021.

41）　*Ibid.*, para 2022.

42）　*Ibid.*, para 2022.

43）　黒﨑ほか『前掲書』（注27）364頁。

第４に、「使用」とは、ある物の「現在の機能」に関することをいう[44]。例えば、民用物の建物が軍隊によって占有され、基地や司令部として使用されている場合は「使用」の基準を満たしうる。またデータにおいては、本来は文民が使用していた特定の仮想マシンが軍事作戦に用いられている場合、当該仮想マシン（データ）は軍事目標となる。

第５に、「軍事活動に効果的に資する」との要件に関しては、例えば、ある工場が軍で使用されるコンピュータ等を製造している場合は当該要件を満たしうる。また、敵の勢力に対して暗号文を伝達するウェブサイトも「軍事活動に効果的に資する」例として挙げられるだろう。よって、厳密に見ていくと、敵の勢力に対して暗号文を伝達するウェブサイトの Web サーバはもとより、Web ページを構成する HTML なども軍事目標の要件を満たす可能性がある。ただし、HTML の改ざんは Web サーバへの攻撃とみなすこともできる。通常、Web サーバは他のサーバ機能と同居せず、Web サーバ用に１つの筐体を使用する。よって、この２つを区別することに大きな意味はないだろう。

２．軍事目標への攻撃時に求められる要件

続いて、「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をもたらすもの」について検討する。

まず、「破壊」については特に説明の必要がないであろう。AP1において「破壊」の定義は示されていないが、武力紛争の目的の１つでもある「敵対する紛争当事者の戦争遂行能力の低減」においては、建物や橋を破壊することが必要不可欠となる。よって、データの場合も、敵対する紛争当事者が軍事作戦のために使用するデータを削除する行為や、軍事システムや軍事目標たるインフラ施設を停止させるためにシステム（データ）に対してサイバー攻撃を行うことなどが破壊に該当する。なお、「破壊」は「攻撃」の定義における「暴力行為」に含まれる概念であるが、どのようなサイバー攻撃が「攻撃」

44）　Sandoz, *supra note 15*, para 2022.

に該当するかという議論同様、どのようなサイバー攻撃が「破壊」に該当するかについては、明確な基準が示されていない。ただし、52条２項は、「性質、位置、用途又は使用」の要件を満たす物を「破壊」する場合が対象となるため、紛争当事国の解釈で破壊の範囲を無制限に広げたり狭めたりできるわけではない。

「奪取」及び「無効化」は、ICRC の草案やエジンバラ決議で提案された方式にはなかった用語を AP1起草作業における第３委員会で追加されたことに端を発す[45]。なお、「奪取」及び「無効化」については定義自体の説明もほとんど行われずに文言が追加されている[46]。

「奪取」は、敵対する紛争当事者の兵器などを奪い取り、利用できなくする行為などが該当する。サイバー攻撃のケースでは、軍事作戦に必要なデータをランサムウェアに感染させて利用できなくすること、またはデータ自体を窃取する行為が該当し得る。ただし、後者の「窃取」については、第49条の攻撃の定義で示される「暴力行為」とみなすことができるのかについては、詳細な検討が必要であろう。

「無効化」は、砲撃を扱う限りにおいて、必ずしも破壊することなく、敵の物体の使用を拒否することを目的とした攻撃を指すものであった。例えば、特定の土地に「地雷を敷設することで無力化し、敵にその使用を認めないようにすること」や、敵の大砲や地対空ミサイルを十分な時間無力化することで計画された作戦に支障をきたさないようにするため、そのような目標に向けて対人弾を発射し、射手を避難させることも無効化と言える[47]。サイバー

45）　1974年３月12日の条文の修正提案の中でオランダ代表団によって「奪取及び無効化」が提案され、のちに条項に採用された。初期のオランダ代表団による提案は、「攻撃は、厳格に軍事目標に対するものに限定する。つまり、軍事目標は、その性質又は使用が軍事活動に効果的に資するもの、または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をもたらすものに限る。」という文言であった。Protection of War Victims_Protocol 1 to the 1949 Geneva Conventions Volume 3, p. 177, 181.

46）　Heather Harrison Dinniss, *Cyber Warfare and the Laws of War* (Cambridge University Press, 2012), p. 198.

47）　Bothe, *supra note 24*, p. 367.

攻撃においては、上記のランサムウェアによる攻撃は、相手がデータを利用することを「無効化」する行為に該当する。

なお、サイバー攻撃の状況において「破壊」「奪取」「無効化」は比較的近しい行為を示す概念である。よって、軍事目標に対する攻撃の合法性を検討するに際しては、これら３つの定義を個別に検討する必要性は少ないのかもしれない。

一方で、どのようなサイバー攻撃が「破壊」「奪取」「無効化」に該当し得るかは引き続き検討が必要である。例えば、Knut Dörmann は、物理的な損害は攻撃の要件ではないと主張する。Dörmann は、52条２項で「無効化」に言及していることを元に、「電力網を破壊することなく停止させるなど、対象物を単に無効化することも攻撃として認定されるべき」と主張する[48]。また、タリンマニュアルにおいては、軍事的利益は軍事目標の破壊または損傷のみでしか得られないわけではないため、奪取や無力化への言及はこの点において重要であると述べる。例えば、敵の指揮統制施設の通信に利用されているサーバへのサイバー攻撃では、指揮統制施設にはダメージがないが、その施設は攻撃側の軍事的優位性を決定的にする方法で無効化されていると言えるのである[49]。Marco Roscini も「第52条２項は攻撃対象となった物の全面的または部分的な破壊のみならず、奪取や無効化も想定する。これには止むを得ず物を破壊することなく、敵の物の利用を拒絶する目的の攻撃が含まれる。」[50] と主張する。このように、無効化については、物理的な損害が必ずしも必要でないとの見解もある。

最後に、「明確な軍事的利益」とは、軍隊の前進（拠点の確保）ならびに

48）　Dörmann, *supra note 35*, pp. 142-143. Dörmann の主張は、軍事目標の定義が文民に対する攻撃を規律する「第四編　文民たる住民 第一部　敵対行為の影響からの一般的保護」に含まれていることにも依拠している。しかしながら、無害化は軍事目標についてのみを対象としていること、軍事目標という用語は攻撃の許容対象を詳述する条文や段落に限定されず幅広く使われているため、この主張には問題があると Dinniss は述べる。Dinniss, *supra note 46*, p. 198.

49）　Schmitt, *supra note 8*, p. 443.

50）　Marco Roscini, *Cyber Operations and the Use of Force in International Law*（Oxford University Press, 2014）, p. 187.

敵の軍隊の殲滅及び弱体化を指す[51]。ここでは、明確な軍事的利益をもたらさない攻撃、例えば潜在的または不確定な利益しかもたらさないような攻撃は違法とみなされる[52]。そのため、データを改ざん、削除することによって敵国軍隊の軍事活動の弱体化を期待できる場合、データへのサイバー攻撃も「明確な軍事的利益」を得るために行い得るだろう。

以上のように、データは軍事目標における「物」という要件以外についても十分に満たせる可能性がある。

3.「物」の解釈の検討

1967年に世界初のネットワーク[53]が構築されたが、世間一般にインターネットが普及したのは1989年以降であると言われている[54]。対して、第52条を含むAP1が採択されたのは1977年であり、第52条２項において、当時あまり普及していなかったデータの存在を念頭に置いていたとは言い難い。そのため、情報通信技術が幅広く普及した現代において、第52条における「物（Object）」にデータが含まれるか否かが大きな論点となっている。

第52条をはじめとしたAP1における「データ」の法的扱いについては、既に多くの議論がなされており、データが物に該当するとの立場と（本稿では、以下、物体説とする）、データが物には該当しないとの立場（以下、非物体説）で見解が分かれている。

国際法学者の中でデータの扱いについて大々的に議論がなされたのは、2013年のTallinn Manual on the International Law Applicable to Cyber Warfare（以下、タリンマニュアル1.0）の発刊がきっかけである。タリンマニュアル1.0は、サイバー空間に適用される国際法について、lex lataの観点から整理

51）　Sandoz, *supra note 15*, para 2218.

52）　*Idid.*, para 2024.

53）　米国防総省高等研究計画局の資金提供により実施されたARPANET（Advanced Research Projects Agency Network）が世界初のネットワークである。

54）　1995年にMicrosoft社がWindows 95を発売したことをきっかけに、世界中でインターネットの利用が広く普及したと言われている。

を行ったマニュアルであるが、規則38には以下のような記述がなされた。

> 規則38　民用物と軍事目標
>
> 民用物は、軍事目標ではないすべての物をいう。軍事目標は、その性質、位置、用途又は使用が軍事活動に効果的に資する物であって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をもたらすものをいう。軍事目標は、コンピュータ、コンピュータ・ネットワーク及びサイバーインフラを含みうる[55]。
>
> （中略）
>
> 本マニュアルでは、コンピュータ、コンピュータ・ネットワーク、及びサイバー・インフラのその他の有形の構成要素が物体を構成する[56]。

上記のように、タリンマニュアル1.0では非物体説の立場をとった[57]。これに対し Heather Harrison Dinniss[58] 及び Kubo Macak[59] が物体説の観点から Israel Law Review に反論の論考を投稿した。さらに両者の反論に対し、タリンマニュアル1.0の編集責任者でもある Michael N. Schmitt が Israel Law Review に再反論の論考を投稿し、データの法的解釈に関する議論が本格的に行われ始めた[60]。三者の論文はデータの法的解釈について集中的に検討した内容であるため、データが物に該当するかを検討する上で有用な視座をい

55）　Michael N. Schmitt（ed.）, *Tallinn Manual on the International Law Applicable to Cyber Warfare*（Cambridge University Press, 2013）, p. 125.

56）　*Ibid.,* p. 127.

57）　2013年当時はタリンマニュアル1.0の規則38に民用物と軍事目標の規則が明記されていたが、2017年にタリンマニュアル2.0が発表され、規則38の内容が規則100に引き継がれている。以下、区別が必要な場合を除き、1.0及び2.0の見解をまとめて「タリンマニュアルの見解」として記載する。

58）　Heather Harrison Dinniss, “The Nature of Objects: Targeting Networks and the Challenge of Defining Cyber Military Objectives”, *Israel Law Review*, Vol. 48, No.1（2015）.

59）　Kubo Macak, “Military Objectives 2.0: The Case for Interpreting Computer Data as Objects under International Humanitarian Law, *Israel Law Review,* Vol. 48, No.1（2015）.

60）　Michael N. Schimitt, The Notion of ‘Objects’ during Cyber Operations: A Riposte in Defence of Interpretive and Applicative Precision, *Israel Law Review*, Vol. 48, No.1（2015）.

くつか提供している。つまり、AP1の趣旨及び目的に基づく解釈の可能性、条約に用いられている用語の意味の解釈の可能性、そしてAP1の趣旨及び目的の発展的解釈や条約を適用する時代に合わせた解釈の可能性である。以下では、タリンマニュアル、Dinniss、Macak、Schimittの論考に加え、他の先行研究も交え検討を行う。

A）AP1の趣旨及び目的、条約中の用語の意味に基づく解釈の可能性

まずは、AP1の趣旨及び目的に基づき「物」を解釈する観点から検討する。AP1のコメンタリーでは、物について以下の説明がなされている。

> 英語表記の「物」が使われているが、それは「目の前に置かれたもの、または、視覚や他の感覚によって存在するもの、見られたり知覚されたりする個別のもの、または見られたり知覚されたりする可能性のあるもの、物質的なもの」を意味する[61]。

AP1において、「物」は英語の「objects」、フランス語の「biens」を採用しているが、「英語でもフランス語でも、この単語は目に見えるもの、具体的なものを意味することは明らかである」[62]ことがコメンタリーでも述べられている。なお、「objects」という用語は、軍事作戦の一般的な目的・目標を指す「objective」と区別するために使用されている[63]。

非物体説の立場をとるタリンマニュアルでは、コメンタリーにおける「目に見える有形のもの」という説明を根拠に、コンピュータ、コンピュータ・ネットワーク、およびサイバー・インフラストラクチャーのその他の有形要素が物を構成するとした上で、「国際専門家グループの大多数は、武力紛争法における『物』の概念は、少なくとも現在の法律の状態では、データを含

61）　Sandoz, *supra note 15*, para 2007.
62）　*Ibid.*, para 2008.
63）　*Ibid.*, para 2010.

むと解釈すべきではないという点で合意」[64] しているとの見解を示した。また、条約の通常の意味としての解釈についても、「データは無形であるため、『物』という用語の『通常の意味』には該当せず、ICRC 追加議定書1987年版のコメンタリーで示されている説明にも合致しない。」[65] との見解を示し、データは「物」に含まれ得ないとの立場を主張する。

一方、物体説の立場をとる Dinniss は、AP1コメンタリーにおける「物（objects）」は「目的または目標（aim or purpose）」という意味の「objectives」と区別するために設けられた記述であることを主張した上で、情報通信技術で構成される要素（component）についても第52条２項で設けられた要件を満たしさえすれば、正当な軍事目標になる可能性があると述べる[66]。加えて、「コードは物質性を欠いているかもしれないが、五感、特に視覚によって確実に認識可能であり、それゆえに目に見えると考えられる」[67] との見解を示す。

同じく物体説の立場に立つ Macak も、タリンマニュアルでは「物」の「通常の意味」を説明していないとの前置きをした上で、そもそも1977年当時はサイバー作戦が出現する前であったことから AP1のコメンタリーの作者が「物」からデータを除外していたわけではないと主張する[68]。その上で、コメンタリーにおける「物」と「軍事作戦における目標」の区別の意義について、「もし紛争当事者の目標（aim）が敵対する紛争当事者の攻撃を正当化する正当な目標（target）を意味するのであれば、標的選定における詳細かつバランスの取れたルールが意味を失ってしまうだろう。交戦国は、オーソドックスな理解に合致しない物に対する攻撃を追求したい場合の切り札を得ることになる。」[69] とし、軍事目標の選定に関するバランスを取るには必要な区別であると述べる。

64）Schmitt, *supra note 8*, p. 437.
65）*Ibid.*, p. 437.
66）Dinniss, *supra note 58*, p.43.
67）*Ibid.*, p.43.
68）Macak, *supra note 59*, p.67.
69）*Ibid.*, p. 68.

一方、非物体説の立場をとるSchimittは、タリンマニュアルにおいて示された非物体説の主張について、単にAP1第52条２項の文言をテキスト分析したわけではなく、条約における文脈や趣旨・目的を考慮した上での見解であるとし、タリンマニュアルにおける見解は条約の「趣旨」、「目的」及び「通常の意味」に基づいて十分に分析を行った上での結論であろうことを主張している[70]。

また、同じく非物体説の立場であるOri Pomsonは、AP1で明示的に示されている「物」としての例示に注目し分析をおこなっている。例えば、AP1第52条３項では「礼拝所、家屋その他の住居、学校」、第53条では「歴史的建造物、芸術品又は礼拝所」、第54条２項の「農業地域、作物、家畜、飲料水の施設及び供給設備、かんがい設備」、第56条１項における「ダム、堤防及び原子力発電所」といった例示をもとに、これらはすべて目で見たり触れたりできる物質的な物であることから、データは物に含まれないとする非物体説の立場を主張する[71]。

このように、AP1の起草時の議論では「データ」を念頭に置いていたわけではないため、条約の「趣旨」、「目的」及び「通常の意味」に基づく解釈に関しては、物体説と非物体説の主張が平行線を辿っている。よって、現時点においてデータを「物」とみなすか否かの最終的な結論を導くことが難しい状況であると言わざるを得ない。

B）AP1の趣旨及び目的の発展的解釈や条約の発展的解釈の可能性

それでは、条約の「趣旨」、「目的」を単純に読み解くのではなく、「趣旨」、「目的」、及び技術の発展による時代の潮流に合わせた新たな解釈、いわゆる「発展的解釈」に解決の糸口を求めることはできないのであろうか。

非物体説の立場をとるタリンマニュアルはコメンタリーの中で、少数派で

70）　Schmitt, *supra note 60*, pp. 88-89.

71）　Ori Pomson, "'Objects'? The Legal Status of Computer Data under International Humanitarian Law", *Journal of Conflict & Security Law*, Oxford University Press, 2023, pp. 14-15.

ある物体説の主張についても記載している[72]。少数派は、軍事目標のターゲティングの目的を勘案すると、特定のデータは物とみなすべきだと主張する。これは、「データ自体を標的とするサイバー作戦を『攻撃』という用語の範囲に含めないと、社会保障データ、納税記録、銀行口座などの重要な民間データセットを削除する行為が武力紛争法の規制対象から外れる可能性があり、（AP1第48条に反映されている）文民は敵対行為の影響から一般的な保護を享受するという原則に反する」[73] との見解に基づいている。物体説に立つ立場は、「AP1第52条の根本的な目的と趣旨に基づき、重要な要素は、被害の性質ではなく、作戦の結果の重大性である」[74] とし、物体説の重要性を主張している。

また Dinniss は、文民や民用物への被害を最小限に抑えた上でサイバー戦においてターゲットに対する効果的な軍事作戦を行うには、物理インフラではなくコードに対して直接攻撃を行うことが求められる可能性があるとの前提を述べた上で、「法律の現代的な解釈（modern interpretation）は、この必要性を反映し、それを可能にするべきである。」[75]（括弧は筆者追記）と主張する。

さらに Macak は、以下の３つの理由から「物」という用語の意味を発展的に解釈できるとの立場を支持する。第１に、コスタリカとニカラグアの間で締結されていた条約の履行について ICJ で争われた航行権および関連する権利に関する紛争事件の判決を引用し、「非常に長い期間にわたって締結さ

72）　タリンマニュアルは、太文字で規則を記載した後に、コメンタリー部分に規則の定義、説明、専門家の意見が一致した点、一致しなかった点などを記載している。前者の規則は、タリンマニュアルの検討に参加した全ての専門家の同意が必要であった。他方、専門家の間で見解の一致を見なかった部分、例えば、専門家集団による議論の中で多数派と少数派の立場が明確に分かれた場合、専門家の見解を二分した問題、１～２人の専門家のみが主張した立場などは、コメンタリーに記載することで全会一致の欠如に対応しようとしている。Eric Talbot Jensen, “The Tallinn Manual 2.0: Highlights and Insights”, *Georgetown Journal of International Law*, Vol. 48, 2017, pp. 739-740.

73）　Schmitt, *supra note 8*, p. 437.

74）　*Ibid.,* p. 437.

75）　Dinniss, *supra note 58*, p.45.

れる条約において当事者が一般的な用語を選択した場合、そのような用語が発展的な意味を持つことを意図したと推定されるべき」[76] と主張する。第２に、人権条約同様にAP1は個人の保護を目的とした多国間条約であるため、原意主義解釈ではなく、発展的解釈を取るべきである[77]。第３に、AP1を含む武力紛争法は、マルテンス条項に基づき軍事技術の急速な進化に対応してきた背景があるため、発展的に解釈が可能であるとする[78]。

この点、Schimittも「変化した現実を背景として開発された規則は、受け入れられた解釈規則の枠内で、新しい現実に適応させる動的な解釈を取らなければならない」[79] と述べたイスラエル最高裁の見解を引用し、新たな解釈の可能性については理解を示している。しかし､データを物と解釈する上で、新しい規範の出現や国家による物の概念の再解釈を示す証拠がない限り、物体説の立場をとることは難しいとの見解を述べている[80]。

またSchimittは、国家は「軍事的必要性と人道的考慮のバランスがこの現実（民間データの破壊が深刻な結果をもたらす可能性）によって大きく変化し、データの新しい解釈が必要であると確信的に主張する準備はできていなかった」[81]（括弧は筆者追記）とし、論考を発表した2015年当時には物の概念を拡張することはやり過ぎであると考えていた。なお、本稿を執筆している2023年時点では、いくつかの国が武力紛争法におけるデータの解釈について見解を述べている。この点については、後ほど検討を行う。

さらに、Marco Sassoliは、無形であるデータを物と解釈できるかどうかがポイントであるとした上で、「我々は有形のもののみが軍事目標とみなさ

76）　Macak, *supra note 59*, p. 70. Dispute regarding Navigational and Related Rights（Costa Rica v. Nicaragua）, Judgment, I.C.J. Reports 2009, para. 66.

77）　Macak, *supra note 59*, p. 70.

78）　*Ibid.,* p.71.

79）　HCJ 769/02, Public Committee Against Torture in Israel and Palestinian Society for the Protection of Human Rights and the Environment v Israel and Others ILDC 597（IL 2006）, 2006, para 28.

80）　Schmitt, *supra note 60*, p. 94.

81）　*Ibid.,* p. 94.

れることを明確に規定している。もしデータが定義上の『物』でない場合、それは軍事目標でもない。しかしながら、この定義はサイバー戦の特性を考慮して見直されるべきである。」[82] とし、時代に合わせた解釈の必要性を主張する。ただしどのように見直す必要があるかについては触れられていないため、今後も検討が必要になるであろう。

C）国家による見解

上記でも触れた通り、データが物に含まれるか否かの学者間の議論は2015年に行われたものであり、国家自身も「物」に関する新たな解釈が必要であると確信的に主張する準備はできていなかった。しかし、2019年以降、いくつかの国家がデータの解釈について立場を表明している。以下では、物体説及び非物体説の２つの視点から、各国の立場を見ていく。

まず、物体説の立場をとる国家としては、フィンランド、ドイツ、ルーマニア、フランスがある。フィンランドは、「不可欠な文民インフラ、文民サービス及び文民データを含む文民及び民用物の保護を確保するために、一定の注意を払うものとする」[83] とし、民用物の中にデータを包含するとの解釈を示す。

ドイツは、「国際人道法の文脈におけるサイバー攻撃を、通信、情報、その他の電子システム、これらのシステム上で保存、処理、伝送される情報、または物理的な物体や人物に有害な影響を与えるためにサイバースペースで、またはサイバースペースを通じて開始された行為または行動と定義する」[84] とし、武力紛争法の文脈で規制対象となるサイバー攻撃には情報（データ）への攻撃が含まれると示唆する。さらにドイツは、「通常兵器の効果に匹敵する物理的損害、人に対する傷害若しくは死亡又は物に対する損害若

82） Marco Sassoli, *International Humanitarian Law Rules, Controversies, and Solutions to Problems, Arising in Warfare* (Edward Elgar Publishing, 2019), p. 538.

83） Finland, *International law and cyberspace - Finland's national position*, 2020 , p. 7.

84） Federal Government of Germany, *'On the Application of International Law in Cyberspace'*, Position Paper (March, 2021) , p. 8.

しくは破壊の発生は、第49条の意味での攻撃においては必要ではない。」[85] とし、人に対する傷害若しくは死亡又は物に対する損害若しくは破壊が発生しないサイバー攻撃でも、AP1第49条の攻撃に該当する可能性を主張している。

ルーマニアも、「我々は、データに対するサイバー作戦は国際人道法の適用を引き起こすという予備的見解を有している。したがって、サイバー攻撃は、国際人道法に従って軍事、目標を表すデータに対してのみ実施することができ、区別原則の下で保護されなければならない民用物に該当するデータに対して実施することはできない」[86] とし、データにおいても民用物と軍事目標の区別が必要であると主張する。

なお、フランスもデータが物（軍事目標）とみなされることを述べているが、一部、他国とは異なる見解を示す。フランスは、「デジタル依存の現状を考慮すると、コンテンツデータ（民間、銀行、医療データなど）は区別原則の下で保護される」[87] とする。この見解を理解するには Dinniss による考え方を参考にするのが最適である。データの解釈において、Dinniss は「コンテンツデータ」と「オペレーショナルデータ」との２つに分類して検討するべきであると主張する[88]。ここで言うコンテンツデータとは、PDF データや、医療データベース、図書館のカタログなどである[89]。他方、オペレーショナルデータとは、一般的にはプログラムデータと呼ばれ、ハードウェアに機能性を与え、我々が必要とするタスクを実行する能力を発揮するデータである[90]。Dinniss は、コンテンツデータは武力紛争法における保護対象ではないとしつつ、オペレーショナルデータは武力紛争法における規律対象、つ

85）　Germany, *supra note 84*, p. 8.

86）　Official compendium of voluntary national contributions on the subject of how international law applies to the use of information and communications technologies by States, UNODA, A/76/136, August 2021, p. 78.

87）　Ministry of Defense of France, *International Law Applied to Operations in Cyberspace*, （September 9, 2019）, p. 14.

88）　Dinniss, *supra note 58*, p. 41.

89）　Dinniss, *supra note 58*, p. 41.

90）　*Ibid.,* p. 41.

まり物に該当すると主張する[91]。他方、フランスはDinnissが武力紛争法の保護対象であると考えている「コンテンツデータ」までをも区別原則に基づいて考慮すべきと主張しており、Dinnissよりも「物」の定義を広く捉えていると言えよう。

次に、非物体説をとる立場としては、デンマーク、チリ、イスラエルによる見解がある。まず、デンマークは、「国際人道法の下では、物は、小さな要素、大きな地形の対象物、領域から構成されることがある。しかし、一般的に言えば、（デジタル）データは一般的な物に該当しない。」[92]とし、データが物ではないことを主張する。なお、2023年７月４日に公表された最新のポジションペーパーでは、「デジタルデータは一般的にそれ自体では国際人道法の対象とはみなされないが、いずれにしてもデータの破壊は、該当の作戦が攻撃とみなされるほどの個人または物理的な物に対する二次的な被害を及ぼすかもしれない。これは、データの破壊が傷害、死亡、または物理的損害をもたらすことが予見できる場合である。同様に、物の機能を担っているデータを標的にした作戦は、当該作戦から予見される損害の性質と規模によっては、攻撃と認定される可能性がある。」[93]との見解を示し、データが物理的な損害が予見される場合はデータへのサイバー攻撃が「攻撃」に該当する可能性を述べている。

チリも「チリの回答は、データに対するサイバー作戦には、その作戦のノックオン効果に基づいて間接的に区別原則が適用されうることを示唆した。これは、AP1のコメンタリーにおける物は『目に見える有形のもの』でなければならないという考えを引用している。これは、データは本質的には無形であり、データを保持する物理的要素（例えばハードウェア）を損なうことはないため、現在の国際人道法に基づくと、前述のデータは原則的には物と

91）　Dinniss, *supra note 58*, p. 42.

92）　Ministry of Defence of Denmark, Military Manual on International Law Relevant to Danish Armed Forces in International Operations（2016）, p. 292.

93）　Government of Denmark, Denmark's Position Paper on the Application of International Law in Cyberspace, Nordic Journal of International Law, 1-10（2023）, p. 10.

みなされないであろう」[94] との見解を示す。チリの見解は AP1第52条２項のコメンタリーにおける物の定義をもとに、用語の通常の意味の観点から見解を述べていると言えよう。

最後にイスラエルは、「武力紛争法の目的における物は、常に有形物であると理解されており、この理解はドメイン固有のもの（domain-specific）ではない。したがって、武力紛争法の下では、現状では、有形物のみが物を構成することができるというのが我々の立場である。」[95] と主張する。他方、データへの攻撃については「コンピュータ・データに悪影響を与えるサイバー作戦が規制されないということではない。特に、コンピュータ・データの削除や改変を伴う作戦が、物や人に物理的な損害を与えることが合理的に予想され、攻撃を構成するのに必要な他の要素を満たす場合、その作戦は武力紛争法のターゲティングの規則による適用を受けることになるであろう。」[96] とし、データに対するすべての攻撃が許容されるわけではないことを示している。イスラエルの後段の見解はデータに対する武力紛争法の適用において重要な主張であるが、イスラエルがどのような根拠に基づいてこのような主張をしているのかは明らかになっていない。しかしながら、同様の主張はタリンマニュアルにおいてもなされていることに注目したい。タリンマニュアルでは攻撃の定義について規定した規則92において、「本規則における個人または物理的な物に対する作戦という限定は、（非物理的実体である）データに対するサイバー作戦を攻撃という用語の範囲から除外するものとして理解されるべきではない。データに対する攻撃が、個人の傷害または死亡、あるいは物理的な物の損害または破壊をもたらすことが予見できる場合は、常にそれらの個人または物は『攻撃の対象』を構成し、したがってその作戦は

94）　Chile, Response submitted by Chile to the OAS Inter-American Juridical Committee Questionnaire（14 January 2020）, cited in OAS, Improving Transparency: International Law and State Cyber Operations: Fifth Report, OAS Doc. CJI/doc. 615/20 rev.1（7 August 2020）para. 36.

95）　Roy Schöndorf, Israel's Perspective on Key Legal and Practical Issues Concerning the Application of International Law to Cyber Operations, *International Law Studies*, Volume 97（2021）, p. 401.

96）　*Ibid.,* p. 401.

攻撃とみなされる。」[97] と述べる。さらに、規則100では、データへの攻撃はAP1第49条における「攻撃」には該当しないことを述べた後に、「規則92に記載されているように、データを標的としたサイバー作戦が、サイバーインフラの機能に影響を与えたり、問題のサイバー作戦を攻撃として認定するような他の結果をもたらす場合には、攻撃として認定されることがある」[98] という点で専門家内での見解の一致がなされたという。

イスラエル、タリンマニュアルの見解を分析すると、両者ともにデータを物とみなさない点、そしてデータに対するサイバー攻撃によって人や物に物理的な影響が生じた場合はAP1第49条における「攻撃」とみなしている。他方、データへのサイバー攻撃が攻撃とみなされた際に武力紛争法の規制対象になるかについては、イスラエルは具体的な適用規則を示していないものの、適用可能性を明示的に示している。タリンマニュアルは武力紛争法の適用について明示的に示していないものの、「攻撃」に該当する以上、「攻撃」に関連した規則が適用されるとの推測ができる。よって、イスラエル、タリンマニュアルの見解の方向性は一致しているように思われるが、いずれの見解も具体的な適用規則に言及されていない。また、サイバー攻撃が「攻撃」とみなされた際に、攻撃対象が「軍事目標」または「民用物」とみなされるのかについても言及されていない。よって、いずれの見解もやや説得力に欠ける部分があるが、「攻撃」「データ」「軍事目標」「民用物」の関係性を導く上でのヒントになるだろう。

物体説、非物体説のいずれにも立たないものの、データの法的解釈に関する問題提起を行う国家としては、ブラジルがある。ブラジルは、「国際人道法はサイバースペースにも適用されるという見解を持ちつつも、AP1第49条の目的におけるサイバー攻撃の定義のような追加の検討に値する問題も所在する。例えば、国際人道法による保護を伴う民用物としての文民データの検討、サイバースペースで行動する文民が敵対行為に直接参加するとみなされ

97) Schmitt, *supra note 8*, p. 416.
98) *Ibid.*, p. 437.

る場合などである」とし、文民が保有するデータの保護に関する検討の必要性を述べるに留まる。

ここまで見てきた通り、武力紛争法上のデータの扱いについて見解を述べている国家は、2023年６月末時点で８カ国に限定される[99]。物体説の立場に立つ国家の見解は、AP1の趣旨や目的などに依拠するものではなく、サイバー空間という新たな領域の出現に合わせて武力紛争法を解釈しようとしているように思われる。他方、非物体説の立場に立つ国家は、AP1における「物」の定義や「攻撃」の定義に則する形で解釈を行おうとしている。よって、どのような立場に立ってデータの法的解釈を行うかが整理されない限り、または大多数の国家の意思表明や国家実行により物体説、非物体説のいずれかが国際社会における大多数の見解とならない限り、データの法的解釈を確定させることは難しいであろう。

４．小　括

ここまでの検討のとおり、AP1第52条において「データ」が「物」に該当するかに関しては、学者及び国家の見解の双方において決着を見ていない。ゆえに、本稿で物体説、非物体説のいずれの立場が妥当であるかを明言することはできないが、仮に非物体説の立場を取ることになった場合、武力紛争法の適用においていかなる影響が生じるだろうか。

データが「物」とみなされる場合、武力紛争法において規定される区別原則[100]、比例性原則[101]、予防原則[102]などの関連規則はすべて適用される。他方、データが「物」とみなされない場合、AP1において「物」を対象として規定している規則の適用外となる。具体的には、「攻撃」の場合は区別原則、比

99）　2023年７月６日にはアイルランドがサイバー空間における国際法の適用に関するポジションペーパーを公表したが、AP1第49条における「攻撃」については見解を述べているものの、「物」の法的解釈については言及しなかった。Ireland, Department of Foreign Affairs, *Ireland Position Paper on the Application of International Law in Cyberspace*, para. 31.

100）　例えば、AP1第48条、第52条１項などを参照。

101）　例えば、AP1第51条５項(b)、第83条３項(b)(c)などを参照。

102）　例えば、AP1第57条、第58条などを参照。

例性原則、予防原則であり、「軍事行動」の場合は区別原則、予防原則が該当する。対して、非物体説においても一定の規則は適用されると考えられる。例えば、イスラエル、タリンマニュアル、そしてICRCにおいても、医療用システムのデータの改ざん、削除などを行うことを禁止している[103]。よって文民条約第18条「文民病院」、AP1の第８条(e)の「医療組織」に関する規定などが適用され、医療施設で使用するデータの保護を享受することができる。また、特別の保護対象である文化財（武力紛争文化財保護条約第４条１項）、文民たる住民の生存に不可欠な物（AP1第54条２項）に関わるデータも、攻撃からの保護を享受する。

このように、非物体説の立場が採用された場合、AP1において民用物を保護するいくつかの規定が適用されなくなり、武力紛争法における人道的考慮が低下する可能性がある。例えばMacakは「データを物ではないと解釈することは、戦争において許容される標的の種類を大幅に拡大することになる。このような拡大は、文民を保護する代わりにさらなる危険にさらすことになり、AP1の目的および趣旨に反する」[104]との懸念を示している。また、ICRCも「社会保障データ、納税記録、銀行口座、企業の顧客ファイル、選挙リストや記録など、このような特別な保護の恩恵を受けない民間用データが、敵対行為の遂行に関する既存の一般規則によってすでに保護されている範囲を明確にすることは重要であろう。このようなデータの削除や改ざんは、政府サービスや文民企業をたちまち完全に停止させる可能性があり、物理的な物体の破壊よりも文民に大きな被害を与える可能性がある。このような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ため、あるいは、このようなデータが民用物への攻撃の禁止を作動させる対象とは見なされないため、サイバーにますます依存する今日の世界では、この種の作戦が国際人道法によって禁止されないという結論は、この規範群の目的および趣旨と

103）　Michael N. Schmitt（ed.）, Schmitt, *supra note 8*, p. 515. ICRC, *supra note 34*, p. 43. Schöndorf, *supra note 96*, p. 401.

104）　Macak, *supra note 59*, p. 79.

調和させることが難しいように思える。」[105] との見解を示している。

上記のような懸念から、Macak は、AP1における軍事目標には該当するが、「物」には該当しないという選択肢についても試験的に検討を行った。「物」には該当しないものの「軍事目標」に該当する場合、軍事目標としての規則（例えば、AP1第52条２項など）は最低限適用されることになる。一見すると、Macak の案は非物体説が採用された場合に最悪な状況を回避できる最善策であるかのようにも思われるが、この考え方には２つの問題点がある。第１に、武力紛争法において軍事目標を構成する要素が「人」と「物」に限定されていたにもかかわらず、第３のカテゴリーを生み出すことになってしまう[106]。第２に、軍事目標たる「人」と「物」については、それぞれ軍事目標の要件が示されているが、「物」に該当しないデータが軍事目標とみなされるための要件が存在していない[107]。よって、「物」に該当しない軍事目標の存在を認めることは困難であろう。

他方、仮に物体説の立場が採用された場合、「文民のデータを操るあらゆる作戦は、『民用物』に対する『損害』（データの改変）または『破壊』（データの削除）とみなされ、違法となる」[108] 可能性を指摘する見解もある。この見解においては、例として「文民の掲示板やブログの投稿を削除すること」[109] を挙げているが、このようなサイバー作戦は AP1第49条における攻撃の定義に該当する程度の暴力行為と見なすことはできないだろう。

改めて、物体説、非物体説と軍事目標、民用物の関係性をまとめると以下のように結論づけることができる。まず、物体説の立場に立つ場合、特定のデータに対する攻撃（AP1第49条に相当するもの）は、性質、位置、用途ま

105）　ICRC, *supra note 34*, p. 43.

106）　Macak, *supra note 59*, p.64.

107）　*Ibid.*, p.65.　「人」の場合の軍事目標の要件はハーグ陸戦規則第１条、捕虜条約第４条 A、AP1第44条、第51条３項などに、「物」の場合の軍事目標の要件は AP1第52条２項に規定されている。

108）　Michael N. Schmitt, The Law of Cyber Targeting, *Naval War College Review*, Volume 68, No. 2, Spring（2015）, p. 17.

109）　Schmitt, *supra note 109*, p. 17.

たは使用が軍事活動に効果的に資するものであり、かつ攻撃によって明確な軍事的利益を得られる場合は合法である。なお、同様の攻撃を民用物に向けて行う場合は、当然に違法となる。一方、非物体説の立場に立つ場合、特定のデータに対する攻撃（AP1第49条に相当するもの）は、軍事目標の要件に拘束されないため、性質、位置、用途または使用が軍事活動に効果的に資さないもの、または攻撃によって明確な軍事的利益を得られない場合でも合法となる。同様に、データは民用物にも該当しないため、医療組織、文化財、文民の生活に不可欠なものなど、特定のデータ以外は合法的な攻撃対象と見なされる。

繰り返しとなるが、データを物とみなすかについては見解が分かれる。物体説の立場が採用されれば問題は生じないものの、非物体説の立場をとる場合、データは「軍事目標」にも「民用物」にも該当しないため、武力紛争法の規制対象外に置かれることになる。これは、武力紛争法における「軍事目標」と「民用物」、または「人」と「物」という二項対立の構図による、避けられない結果であろう。

しかしながら、なぜ武力紛争法においては「物」のみにフォーカスを当て、規制対象の議論がなされてきたのであろうか。最後にこの点について考察する。

Ⅴ．武力紛争法における非物理的対象の扱い

ここまで、武力紛争法におけるデータの法的地位について一通りの検討を行ってきたが、武力紛争法は根本的には非物理的対象への規律の必要性をどのように捉えているのか。この点を確認するに際しては、武力紛争法における軍事目標主義の考え方の移り変わりを再確認することが有益であろう。例えば、軍事目標とみなす上での要件については、攻撃対象の属性（防守都市・無防守都市）の区別を重視した時代（以下、カテゴリー別選定基準期）、カテゴリー別選定基準から機能的選定基準への移行を試みる上で、双方の基準

が併用されようとした時代（以下、移行期）、そして軍事目標としての機能要件を採用した時代（以下、機能的選定基準期）の３つに大別することができる[110]。本章ではそれぞれの時代において、攻撃対象をどのように考えていたかを整理することで、武力紛争法における攻撃対象、特に軍事目標としての非物理的対象の扱いについて検討を行う。

１．カテゴリー別選定基準期

まず、軍事目標の概念の起源とも言える規則として、リーバー法典が挙げられる。リーバー法典はアメリカ南北戦争において北軍総司令官であったHenry Halleck 少将による相談に応える形で、Francis Lieber が作成した[111]。リーバー法典の第15条では、「財産の破壊、交通、旅行、通信の経路の妨害、敵からの糧食や生活手段の提供の停止」[112] が戦争において認められることが示されている。

1868年に Alexander Ⅱ世がサンプトペテルブルグで国際軍事委員会を招集し兵器法について議論を行った、いわゆるサンプトペテルブルク宣言においては、軍事目標について言及がなされなかった[113]。

1874年のブリュッセル宣言では、砲撃が禁止される対象として、防御されていない街（open towns）、住居密集地（agglomerations）、村（dwellings）が列挙された[114]。William Boothby によると、これは「重要な、初期の、非

110）　黒﨑ほか『前掲書』（注27）362頁。

111）　Emily Crawford, *Non-Binding Norms in International Humanitarian Law: Efficacy, Legitimacy, and Legality*（Oxford University Press, 2021）, p. 41.

112）　Francis Liber, *Instructions for the Government of Armies of the United States in the Field*, April 24, 1863, pp. 7–8

113）　サンプトペテルブルグ宣言では、文明の進歩により戦争の惨禍をできる限り軽減すべきであること、戦争において国家が目指すべき目標は敵の軍事力の弱体化であることなどが盛り込まれた。*Declaration Renouncing the Use, in Time of War, of Explosive Projectiles Under 400 Grammes Weight*, Saint Petersburg, 29 November / 11 December 1868.

114）　Project of an International Declaration concerning the Laws and Customs of War, Brussels, August 27, 1874, Art. 15.

公式な、法的拘束力のない、区別の原則の主張」であるとする[115]。また、ブリュッセル宣言第17条には「芸術、科学又は慈善の目的に供される建物、病院及び傷病者を収容する場所は、その時点において軍事目的で使用されていないことを条件として、できる限り避けるために必要なすべての措置を執らなければならない。」と規定されており、建物や場所をできる限り攻撃の対象としないことを謳っている。

1889年のオックスフォード・マニュアルでは、戦争の目的上、必要がない場合は公有財産又は私有財産の破壊が禁止されていたほか、無防備都市への攻撃、砲撃も禁止されていた[116]。

1899年のハーグ陸戦規則においては、ブリュッセル宣言及びオックスフォード・マニュアルの一部の規則を反映し、防守都市、村落、住宅又は建物に対する攻撃の禁止[117]、及び宗教、芸術、科学及び慈善に寄与する建造物、病院並びに病者及び負傷者を収容する場所に対する攻撃をできる限り避けるよう、規定された[118]。つまり、ブリュッセル宣言からハーグ陸戦規則までは「防守都市」であるか否かに基づいて攻撃の合法性を判断していたのである[119]。

1907年の戦時海軍砲撃条約においては、防守されていない港、都市、村落、住宅又は建物に対する砲撃を禁止した[120]。一方、陸海軍建設物、兵器又は軍用材料の貯蔵所、敵の艦隊又は軍隊の用に供している工場、設備並びに港内の軍艦は砲撃禁止の対象から除外されている[121]。

このように、1907年までの軍事目標主義の考え方においては軍事目標たる対象の属性を示すことに注力していた。なお、カテゴリー別選定基準期に採用されていた「防守都市」「無防守都市」は、AP1第59条で規定されている「無

115）　William Boothby, *The Law of Targeting,* Oxford University Press, 2012, p. 15.
116）　The Laws of War on Land, Oxford, September 9, 1880, Art. 32（b）（c）.
117）　陸戦ノ法規慣例ニ関スル規則第25条。
118）　陸戦ノ法規慣例ニ関スル規則第27条。
119）　竹本正幸『国際人道法の再確認と発展』（東信堂、1996年）117頁。
120）　戦時海軍力ヲ以テスル砲撃ニ関スル条約第１条。
121）　戦時海軍力ヲ以テスル砲撃ニ関スル条約第２条。

防備地区」とは異なる概念である点に注意が必要である。AP1第59条の無防備地区は、当該地区に対する攻撃を手段のいかんを問わずに禁止している[122]。一方、防守都市と無防守都市という区別は、無差別砲撃が許されるか否かの基準であり、国際法上の攻撃の合法・非合法を扱う基準ではない。事実、「地上兵力が或る都市を占領しようとするのに対してその都市が抵抗する場合には、攻撃軍による砲撃がたとえ都市内にある一般住民の身体財産にまで損害を及ぼしたとしても違法とはされない」[123]。また、無防守都市に所在する軍事上重要な施設に対する攻撃も違法とは見なされない。

2．移行期

1922年のハーグ法律委員会が作成し、条約草案のままとなっている空戦に関する規則案の第24条１項では、「空襲は、軍事目標、すなわち、その破壊または毀損が明らかに交戦国に軍事的利益を与えるような目標に対して行われた場合に限り、適法とする」との規定が盛り込まれた。これは、AP1における「軍事目標」の定義と共鳴するものである[124]。さらに、第24条２項では、爆撃の合法な目標として「軍隊、軍事工作物、軍事建設物又は明らかに軍需品の製造に従事する工場であって重要で、公知の中枢を構成するもの、軍事上の目的に使用される交通線又は運輸線」[125]を挙げた。藤田久一によると、これらはほとんど本質的な軍事目標に限定されており、総力戦下の第二次世界大戦やその他の武力紛争の経験から、今日ではこの列挙は狭すぎると言える[126]。また、第24条３項及び４項では「陸上部隊の作戦行動の直近地域」という文言が採用され、攻撃の合法性を判断するための要素が、カテゴリー別選定基準期に重要視されていた「防守都市」から変化している。よって、

122）　AP1第59条１項。
123）　竹本『前掲書』（注120）118-119頁。
124）　Boothby, *supra note 116*, p. 23.
125）　Rules concerning the Control of Wireless Telegraphy in Time of War and Air Warfare, Drafted by a Commission of Jurists at the Hague, December 1922 -February 1923.
126）　藤田久一『新版　国際人道法 再増補』（有信堂、2003年）114頁。

「陸上部隊の作戦行動の直近地域」という要件が採用された点は、機能的選定基準の検討に向けた第一歩と見ることもできよう。

しかし、1922年の空戦規則に関する規則案以降は、カテゴリー別選定基準に基づく規定が大半を占めた。例えば、1949年のジュネーヴ諸条約においては、武力紛争の犠牲者のカテゴリーを特定し、犠牲者が危険に対処するために設計された一連の保護と規則を提供したものであり、軍事目標に関する記述は僅かであった[127)]。一方、1954年の武力紛争文化財保護条約においては、再びカテゴリー別選定基準が採用された。つまり、文化財として保護される特別の保護を付与するための条件の１つを「(a)　大規模な工業の中心地又は攻撃を受けやすい地点となっている重要な軍事目標（飛行場、放送局、国家の防衛上の業務に使用される施設、比較的重要な港湾又は鉄道停車場、幹線道路等）から十分な距離を置いて所在すること。」とし、保護対象の要件の説明の中で軍事目標を例示した。

1956年、ICRC が作成した「戦時一般文民の蒙る危険を制限するための規則 案（Draft Rules of the Limitation of the Dangers Incurred by the Civilian Population in Time of War）」では、軍事目標となりうるもののリストを以下のように列挙している。

(1)　軍隊（補助的又は補充的組織を含む）、および上述の編隊（formations）には属していないが戦闘に参加する者。
(2)　上の（1）に示された部隊によって占領された陣地、設備又は建造物、ならびに戦闘目標（すなわち、空輸部隊を含む陸軍、又は海軍部隊の間で直接に争われる目標）。
(3)　兵営、要塞、軍事省（たとえば、陸軍省、海軍省、空軍省、国防省、供給省）、ならびに他の軍事行動活動の命令および執行のための機関

127)　これは、ジュネーヴ諸条約の目的が「武力紛争犠牲者のカテゴリーを特定し、彼らが戦争で直面する危険に対処する」ために規則の検討がなされていたからである。Boothby, *supra note 116*, pp. 25-26.

のような軍事的性質を有する施設、建造物およびその他の工作物。

(4)　軍需品集荷所のような武器又は軍用品の貯蔵所、装備品又は燃料の貯蔵所、車両駐車場。

(5)　飛行場、ロケット発射台および海軍基地施設。

(6)　根本的な軍事的重要性を有する交通線および交通手段（鉄道線、道路、橋梁、トンネルおよび運河）。

(7)　放送局およびテレビ局の施設、根本的な軍事的重要性を有する電話電信交換局。

(8)　戦争遂行のために基本的重要性を有する産業。

a)　武器、弾薬、ロケット、装甲車両、軍用航空機、軍艦のような武器の製造（附属品および他のすべての軍需品の製造を含む）のための企業。

b)　輸送および交通の資材、軍隊の装備品のような軍事的性質を有する供給品および物資の製造のための企業。

c)　その性質又は目的が本質的に軍事的である冶金、機械および化学企業のような、戦争遂行のために根本的な軍要性を有する他の生産および製造のセンターを構成する工場又は設備。

d)　上記 a)～ c)にかかげる産業に役立つことがその基本的機能であるような貯蔵および輸送の施設。

e)　主として国防のための動力（たとえば、石炭、その他の燃料、または原子力）を供給する施設、ならびに主として軍事上の消費にあてるためのガス又は電力を生産する設備。

(9)　武器および軍用資材の実験および開発のための実験研究センターを構成する施設[128]。

このように AP1採択前の条約においては、空戦に関する規則案の第24条以

128)　ICRC, *Draft Rules for the Limitation of the Dangers Incurred by the Civilian Population in Time of War*, 1956, p. 72–73.

外では軍事目標たる対象の例示がなされており、特定の要件が示されることはなかった。そのため、各国は攻撃の対象が軍事目標に限定される旨を把握していたが、軍事目標の定義が定まっていなかったため「実際、第二次世界大戦中及びそれ以降に起こったいくつかの武力紛争において、各交戦国はその目標によって何を理解すべきかを好き勝手に決定」[129] できたと言われている。よって、当時の軍事目標の説明上、データに限らずあらゆる非物理的対象を軍事目標が含まれうるとの主張も可能であっただろう。例えば、第二次世界大戦において、連合国はドイツ文民の士気（morale）に対する直接的かつ意図的な攻撃を承認した[130]。承認された文書では、「都市と文民への爆撃を通じて、ドイツの産業労働力、およびドイツ国民の士気にのみ焦点を絞るよう空軍に命じていた」[131] ため、「事実上、戦略爆撃と民間人の士気に影響を与えることを意図した攻撃の継続」[132] を軍事目標に対する正当な攻撃と見なしていたと言える[133]。

なお、AP1採択以前の世界において、サイバー空間を通じて敵対する紛争当事者が軍事作戦に用いるデータに直接攻撃を行うことはできなかった。また、第二次世界大戦時の非物理的対象の「士気」とデータは実際に触ることのできない「無形物」であるものの、同列に語るのは困難である。例えば、国民の士気の低減は、国民自身や民用物に対する攻撃を行うことで実現できる。つまり、直接の攻撃対象が「士気」なのではなく、人や物を攻撃することにより、副次的効果として士気を低下させているのである。他方、データは直接的に攻撃可能な対象であるため、士気に関する議論と異なる部分があるだろう。

129）　Sandoz, *supra note 15*, para 2000.

130）　Office of the Combined Chieds of Staff, Casabranca Conference, January 1943, Papers and Minutes of Meetings, January 20, 1943, p. 88.

131）　Agnieszka Jachec-Neale, *The Concept of Military Objectives in International Law and Targeting Practice* (Routledge, 2014), p. 31.

132）　*Ibid,*, p. 31.

133）　*Ibid,*, p. 31.

3．機能的選定基準期

すでに示している通り、1977年に採択されたAP1では、第52条１項及び２項において民用物と軍事目標の要件を示している。なお、AP1第52条には、AP1以前に採用されていた軍事目標または民用物の具体列挙はなされていない。さらに、無差別攻撃の禁止[134]、特定の物の保護[135]、自然環境の保護[136]、攻撃に際しての予防措置[137]などについても記載がなされ、ターゲティングに関わる法的要素を新たに明記している点がAP1採択前と大きく異なるであろう。

このような相違点はあるものの、AP1の検討において、従前の議論が無視されたわけではない。例えば、AP1の起草過程において、軍事目標の例示がなされた。第52条２項における「性質、位置、用途又は使用が軍事活動に効果的に資する物」に該当する軍事目標として「武器、装備品、輸送機、要塞、発着所、軍隊が使用する建物、幕僚本部、通信センターなど、軍隊が直接使用するすべての物」[138]が該当する。また、位置の観点から橋やその他の建造物、軍事作戦上重要な場所などが該当しうる[139]。目的の観点からは、学校やホテルなどの民用物が軍隊の司令部などとして利用されている場合は該当する[140]。しかし、AP1では上記の例示をそのまま採用するのではなく、抽象的要件を示すことで軍事的利益と人道性のバランスを維持しながらも、攻撃対象の状況に応じて軍事目標であるか否かを判断できる形を取り入れた。また、AP1のコメンタリーでは、AP1以前の軍事目標の定義に関する試みについて触れられている[141]。よって、AP1における軍事目標の定義は1977年以前

134）　AP1第51条４項、５項。
135）　AP1第53条、第54条、第56条。
136）　AP1第55条。
137）　AP1第57条。
138）　Sandoz, *supra note 15*, para 2020.
139）　*Ibid,*, para 2021.
140）　*Ibid,*, para 2022.
141）　*Ibid,*, paras. 1994-2004.

の軍事目標の概念と全く別のものではなく、過去の議論の上に成り立ったものであることは重要である。

４．小　括

AP1採択前後の条約などにおいては、物や建物、場所を軍事目標と見なしており、データなどの非物理的対象を軍事目標とみなそうとする議論はなされていなかった。これは、これまでの武力紛争が「人間対人間」を前提としているほか、人間が立ち入ることができる領域や建物、1977年以前の技術に基づいて人間が操作可能であった物（例えば、海底ケーブルなど）を軍事目標とみなしていたことが一つの要素として挙げられるだろう。また、武力紛争法の基盤の一つである「人道的考慮」の存在も影響していると思われる。人道的考慮は「人間の本質的感情に従い、敵対行為の正当な軍事目的（敵戦力の剥奪または弱体化）の達成に必要でない苦痛、傷害、破壊」[142]を禁じている。ここで注目すべきは、「苦痛」「傷害」「破壊」である。いずれも人間の健康に影響を及ぼす可能性があるため、武力紛争法において特に保護が求められていると考えられる。他方、非物理的対象は、人間の健康に影響を及ぼす可能性が少ない。このような観点から、武力紛争法の発展において特に重視されていなかった可能性はあるだろう。

昨今では、武力紛争とメンタルヘルスの関係性について扱われる論文が出てきているが、メンタルヘルスの議論はデータの議論と類似している部分もある。例えば、データもメンタルヘルスもAP1において明確な規定がなされていない。もちろん、AP1第51条２項において文民に恐怖を広めることを目的とした暴力行為、暴力による威嚇を禁止しているが、恐怖を広めることを「主たる目的」としていない場合は禁止されていない[143]。用語の定義につい

142）　黒﨑ほか『前掲書』（注27）305頁。

143）　Eliav Lieblich, Beyond Life and Limb: Exploring Incidental Mental Harm Under International Humanitarian Law, *Applying International Humanitarian Law in Judicial and Quasi-Judicial Bodies, International and Domestic Aspects*, T.M.C. Asser Press, 2014, p. 196.

ても同様である。AP1第51条５項(b)などで規定される「傷害（injury）」に精神的損害を含めるのか、または物理的損害のみに限定されるのかという議論がまさにそれにあたる[144]。そもそも、精神的損害の例として挙げられるものにPTSD（心的外傷後ストレス障害）があるが、PTSDという心理学上の名称が設けられたのは1980年である[145]。データやサイバー攻撃と同様に、1977年のAP1起草時には問題とみなされていなかった点も同じであろう。よって、メンタルヘルスの法的扱いの議論は、武力紛争におけるデータの法的解釈の検討においても有用な視座を提供する可能性がある。

もちろん、メンタルヘルスは人間自身に影響を及ぼすものであるが、データは人間自身への影響が不透明であるため、メンタルヘルスにおける議論を一概に適用できないとの見解もあるだろう。しかしながら、近年、ICRCがデータの武力紛争法上の扱いについて見解を述べている背景には、「データが人間の健康に影響を与える可能性がある」という観点がある。前述の通り、ICRCがデータの削除や改ざんが文民に大きな被害を与える可能性があると考えているように[146]、IT化が進むにつれてメンタルヘルス同様、人間の健康に直結する影響を及ぼす可能性がある。例えば、近年、Microsoft社やApple社がMRデバイス（Mixed Reality：複合現実）の販売を開始した。米軍においてもMicrosoft社のMRデバイス（HoloLens2）の導入に向け実証実験が行われていたが、デバイスを装着した80％以上の兵士が吐き気や不快感などを示したことが報じられている[147]。実証実験においてはMRデバイスを正常に利用していたにもかかわらず健康に害が発生していたが、MRデバイスに表示される情報を改ざんすることが可能であれば、デバイス着用後、早い段階で吐き気などの身体的症状を引き起こすことも可能になるだろう。

144）　Lieblich, *supra note 143*, p. 200.

145）　菊池浩光「わが国における心的外傷概念の受け止め方の歴史」『北海道大学大学院教育学研究員紀要』、第119号（2013年12月）117頁。

146）　ICRC, *supra note 34*, p. 43.

147）　Anthony Capaccio of Bloomberg, Microsoft's Army Goggles Left US Soldiers With Nausea, Headaches in Test, October 13, 2022.

よって、今後、情報通信技術がさらに発展し、人間の健康とデータの関係性が緊密になればなるほど、物体説の立場をとる論者が増えていく可能性があると考える。

Ⅵ. ま と め

本稿では、AP1第52条２項における「物」に「データ」が含まれるかについて、学者・国家の見解及び武力紛争法における非物理的対象の扱いの観点から幅広く検討を行った。結論としては、学者・国家も多様な見解を表明している段階であり、現時点では統一的な結論は見られていない。このような議論状況を踏まえると、冒頭で示したシナリオの「①物理サーバに対する攻撃」については、AP1第52条２項に従って判断されることになる。対して、「②指揮システム（仮想サーバ）への攻撃」、「③軍事作戦データベース内の情報に対する攻撃」については、AP1第52条における「物」に該当するかが未確定であるため、非物理的対象への影響をどのように捉えるべきかが定まっていない。

本稿第Ⅲ章でも検討した通り、「攻撃」の定義における「暴力行為」をサイバーの文脈でどのように解釈すべきかについては議論がある。タリンマニュアルの多数派の見解に立つと、単なるデータの削除は「攻撃」に該当せず、データの改ざん・削除による物理的な損害の発生が必要となる。これは、データへのサイバー攻撃において考えられないような基準ではないものの、このような基準を満たすサイバー攻撃は限られるだろう。

本稿第Ⅳ章で検討した物体説と非物体説の議論についても、学者及び国家の双方において、見解の一致を見ていない。物体説は、IT 技術の進歩が著しい現代において、データへの攻撃が文民に与える影響を重要視し、既存の武力紛争法の適用を目指している。他方、非物体説は AP1の用語を拡大解釈することの危険性、及び物体説が唱える懸念がどの程度蓋然性があるのか断言できないことなどから、慎重な立場を示している。

データを「物」とみなすかに関わる議論は、単なる用語の解釈の問題ではなく、ある意味で「軍事的必要性」と「人道的考慮」という、武力紛争法の存在意義に基づいた問題である。つまり、非物体説はAP1コメンタリーにおいて想定されていた「物」の定義、データを「物」と解釈するための国家実行の少なさなどからデータに対するサイバー攻撃の過度な規律を避けている。対して物体説は、文民の生活に必要となるデータへの攻撃を制限できていない可能性を懸念し、サイバー攻撃が軍事作戦の一環として扱われるようになった現代に則した「物」の解釈の必要性を主張している。このように、両者の見解は平行線を辿っており、データの法的解釈に関する問題の結論を導き出すには、多くの議論と時間、そして国家実行が必要と言える。ただし、国家による高度なサイバー攻撃事例が世間に公表されることは少ない。これはサイバー戦の特性上、システムの不具合がサイバー攻撃によるものか、単なるシステムの不具合なのかを判断しづらい点も影響しているだろう。ゆえに、今後の議論がどのように進んでいくかを注視していくことが重要であろう。

【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2023年７月30日である。