サイバー空間を通じた監視活動の法的評価
――間諜行為、主権侵害と人権法（プライバシーの侵害）の観点から――

河野　桂子

〈要旨〉

本稿ではサイバー空間を通じて行われる監視活動について国際法上生じる論点として間諜行為、主権侵害、人権法（プライバシーの侵害）の問題を考察する。従来、他国に対する諜報活動は一定の条件を満たす限り国際法上の間諜行為とみなされてきたが、サイバー空間を通じた活動については対象国領域に対する電子的又は仮想的な所在が従来の場所的要件を満たさないという理由で国際法上の間諜行為とは区別される傾向にある。また平時の監視については対象国の主権侵害という問題も生じ得る。他方、自国領域外の外国人を対象とする通信監視活動は、人権法の域外適用という観点から近年注目を集めているが、電子的又は仮想的な文脈から従来の要件を整理することが重要である。

はじめに

他国のサイバー空間上の活動を監視することは、国際法上どのような問題を生じるか。本稿ではこの問題を、間諜行為、他国の主権侵害、そして人権侵害への該当性という観点から考察する。

サイバー空間上の活動には様々なものが挙げられるが、例えば本国と在外公館との間でやりとりされるインターネット通信や、政府の機密情報を保管した自国内の情報システムが他国の情報機関によって侵入され、重要な情報が漏えいする場合がある。2013年にNATOサイバー防衛センター（NATO Cooperative Cyber Defence Centre of Excellence: NATO CCD COE）によって刊行された『サイバー戦に適用される国際法タリン・マニュアル（Tallinn Manual on the International Law Applicable to Cyber Warfare）』（以下、『タリン・マニュアル』）は、監視目的でマルウェアを他国の情報システムに設置する場合の問題点を取り上げているが、こうしたマルウェアの設置が物理的被害なしに対象国の主権

を侵害するか否かについて審議にかかわった専門家は合意に達することができなかったと記述している[1]。また『タリン・マニュアル』監修者である米海軍大学のマイケル・シュミット（Michael Schmitt）教授は自身の論説のなかで、自国領域内を通過する信号を取得して他国の活動を監視することは（物理的被害も他国に対する強制の意図もなければ）法的にいかなる障害もない、なぜなら国際法は間諜行為（espionage）を禁止していないからであると述べている[2]。信号取得が自国領域内で行われる点で他国の主権を侵害する恐れもないと同教授は考えているようである。

ところで平時に監視目的で他国のシステムにマルウェアを設置することについては、それが対象国の情報システムへの無断侵入（日本法令の用語では不正アクセス）を伴うのであれば、主権侵害に該当する可能性は高いと考えられる。ただし間諜行為としての評価については、サイバー空間上の行為が国際法上の間諜行為にあたるか否かで結論が変わりうる。そもそも、サイバー空間を通じて他国の機密情報を取得することが既存の間諜行為の定義にあてはまらないのであれば、その文脈で評価を議論する意義はない。間諜行為は戦時の制度として確立して久しいが、サイバー空間上の監視行為はとりわけ敵支配地域外から遠隔で行われている場合には、国際法上の間諜行為に該当しないとタリン・マニュアルは論じている。しかし私見では従来の要件に照らしても該当の余地は十分あると考える。また、タリン・マニュアルは平時の間諜行為は国際法上禁止されないと論じるが[3]、このことを対象国の主権侵害性との兼ね合いで最終的にどのように整理するかも課題である。陸海空などの物理領域において偵察航空機や艦船が間諜行為に従事する場合に、領域国は容易に国連憲章 2 条 4 項に依拠して侵入国による武力行使認定を行うことができたのに対して、サイバー空間についてはそうした認定がなされた例は今のところ見当たらない。

また『タリン・マニュアル』では言及されていないが、サイバー監視活動に伴う国際法上の問題として、人権法のプライバシー侵害の論点が近年急速に重要性を帯びてきている[4]。仮にある国の情報機関が正当な業務として自国内の在外公館職員に対する諜報活動を行っていた場合でも、その過程で偶然取得した自国民の通信について政府は当該私人のプライバシーを尊重する仕方で取得したデータを取り扱わなければならない（ヨーロッパ人権裁判所〔ECHR〕アマン対スイス事件〔2000 年 2 月 16 日判決〕）[5]。

1　Michael Schmitt, ed., *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge University Press, 2013), p.16, Rule 1, para. 6.
2　Idem., "The Law of Cyber Warfare: Quo Vadis?" *Stanford Law and Policy Review*, Vol.25 (2014), p.275.
3　Idem., *Tallinn Manual*, p.30.
4　国際人権法の問題は 2017 年 2 月に公表される『タリン・マニュアル 2.0』で扱われる予定である。
5　European Court of Human Rights (ECHR), Case of Amann against Switzerland, Application no. 27798/95, Judgment (February 16, 2000), http://hudoc.echr.coe.int/eng?i=001-58497

この種の問題は、自国内の私人にとどまらず、自国領域外の、とりわけ外国人の通信についても生じていることが昨今世間をにぎわせているが、監視を行っている国（又は企図している国）のうち、このような領域外の外国人との関係でプライバシー尊重義務を肯定している国はほとんどないと言ってよい。この論点は近年の国際法学者の論説において人権法の域外適用の問題として論じられることが多い[6]が、国際人権条約が一定の条件の下で自国領域外に適用されうることは、国際司法裁判所（ICJ）やヨーロッパ人権裁判所の判例において確認されている。もっとも従来の判例はいずれも戦時占領当局や駐留外国軍隊が物理的な文脈で行う活動についてである。それに対してサイバー空間という非物理的な文脈で行われる国家の活動が従来の諸事例と同列に論じることができるのか否かが本稿の検討課題である。仮にサイバー空間を通じた活動を従来の諸事例の延長線上に位置づけられるのであれば、領域外の外国人に対する政府のプライバシー尊重義務を導き出すことができるはずである。逆に一部の国が唱えるように領域外の外国人との関係でプライバシー尊重義務が生じないのであれば、そこにはサイバー空間に特有の事情が関係しているものと推測される。

以下本稿では、まず戦時の文脈においてサイバー間諜行為が成立する可能性について、次に平時の文脈における評価を主権侵害性に触れつつ考察する。また、サイバー監視活動は、戦時か平時かにかかわりなく、監視対象下におかれた個人のプライバシーの侵害という意味で人権法に違反する場合があり得る。本稿では犯罪捜査ではなく諜報活動に着目した上で、人権法の域外適用に関する論点を整理する。なお本稿でもっぱら考察対象とするのは、領域外の外国人がサイバー空間を通して行う国際通信である。

1．戦時におけるサイバー監視活動の評価

本節では戦時における間諜行為の問題を論じるが、物理的領域の文脈で成立した既存の国際法がサイバー空間との関係でどのように適用されるかが焦点となる。また、戦時におけるプライバシー権が比較的新しい問題として生起していることを併せて紹介する。

6　Marko Milanovic, “Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age,” *Harvard International Law Journal*, Vol.56 (2015), pp.81-146.

（1）サイバー間諜行為

間諜行為の定義は、「1949 年 8 月 12 日のジュネーヴ諸条約の国際的な武力紛争の犠牲者の保護に関する追加議定書（議定書Ⅰ）」（以下、第 1 追加議定書）46 条におかれている。すなわち、「紛争当事者の軍隊の構成員であって、当該紛争当事者のために及び敵対する紛争当事者が支配する地域において、情報を収集又は収集しようとしたもの」が、「そのような活動の間に自国の軍隊の制服を着用してい」ない場合、さらに、こうした情報収集が「虚偽の口実に基づく行為による場合又は故意にひそかな方法で行われた場合」を指す（下線は筆者）。これらの要件のうち、「敵対する紛争当事者が支配する地域」の部分を本稿では便宜上、場所的要件と呼称する。また、「自国の軍隊の制服を着用」しないことを標章非着用要件、「虚偽の口実に基づく」ことを虚偽隠密要件と呼称する。これらの諸要件が国際慣習法化していることについては、『タリン・マニュアル』[7]、赤十字国際委員会（ICRC）がまとめた『慣習国際人道法研究』（2009 年）[8] に加えて第 1 追加議定書非締約国の米国[9] も認めているところである。

①場所的要件

『タリン・マニュアル』によれば、敵支配地域ではない場所から遠隔操作でサイバー・オペレーションを行うことは従来の場所的要件を満たさないため、国際法上の間諜行為に該当しない。このような考え方は『タリン・マニュアル』が初めてではなく、ハーバード大学人道政策紛争研究プログラムによる 2009 年『空戦・ミサイル戦に適用される国際法マニュアル（HPCR Manual on International Law Applicable to Air and Missile Warfare）』（以下、『空戦・ミサイル戦マニュアル』）に同旨の見解を確認できる[10]。さらに遡る 1999 年には、米国防総省が「電子的又は仮想的な所在」は物理的な所在とは同義ではないことを根拠に挙げて、遠隔で行う電子的情報収集を国際法上の間諜とはみなさないとする立場を説明している[11]。

もっとも、犯罪捜査の文脈に目を転じると、クラウドなど海外に保管されたデータについて、データ所在国との間で司法共助の手続きをとらず無断で遠隔入手すれば所

7 Schmitt, *Tallinn Manual,* p. 193.

8 ICRC, *Customary International Humanitarian Law* (2009), ICRC website, Rule 107.

9 Michael Matheson, "Additional Protocol I As an Expression of Customary International Law," in International and Operational Law Department, the US Army Judge Advocate General's Legal Center and School, ed., *Law of War* Documentary Supplement (2005), pp.396-398.

10 Program on Humanitarian Policy and Conflict Research (HPCR), ed., *Commentary on the HPCR Manual on International Law Applicable to Air and Missile Warfare* (May 2009), p.259, Rule 118, Commentary para. 6, http://www.ihlresearch.org/amw/manual/

11 U.S. Department of Defense, Office of the General Counsel, *An Assessment of International Legal Issues, 2nd ed. (Nov. 1999), in Naval War College International Law Studies*, Vol.76 (2002), p.516.

在国の主権を侵害するという見解が昨今ますます有力になりつつある。このような状況に鑑みれば、ある国の当局が電子的又は仮想的に侵入するか、あるいは物理的に侵入するかを区別することはほとんど意味がないと思われる（表1の「敵国内への電子的侵入」の場合」）。さらに問題であるのは、敵国の軍事情報の敵国領域外における取得である。この場合には、物理的にせよ電子的にせよ、なんら敵国支配地域への侵入を伴わないため、従来の場所的要件に照らして判断すると間諜行為が成立しない（表1の「敵国外での電子的侵入」の場合）。さらに、戦時に間諜として取り扱われるのは、「諜報活動を行っている間に敵対する紛争当事者の権力内に陥った」場合のみであり（第1追加議定書46条1項）、作戦を終了して部隊に復帰した後で敵に捕らえられても、過去の間諜行為に関する責任を問われることはない（1907年「陸戦ノ法規慣例ニ関スル条約付属書　陸戦ノ法規慣例ニ関スル規則」（以下、ハーグ陸戦規則）31条）。仮に自軍の支配地域から遠隔でサイバー監視活動に従事する兵士をその最中に捕らえることがほとんど不可能であるなら、この者がサイバー間諜に該当するか否かを議論する実質的意義は確かに乏しいのかもしれない。

表1　戦時における国際法上の間諜行為（侵入/監視）場所的要件

侵入/監視		間諜行為の場所的要件
形態	領域	
物理的	敵国内	満たす
電子的	敵国内	満たさないという見解が大勢
	敵国外	満たさない

註：電子的侵入／監視は、遠隔監視となる。
出所：筆者作成。

②虚偽隠密要件及び標章非着用要件

『空戦・ミサイル戦マニュアル』は、間諜の定義として条約で用いられているclandestine（日本語公定訳では、「ひそかな」（第1追加議定書46条3項）、又は「隠密」（ハーグ陸戦規則29条）の語は、敵からの捕捉を逃れる目的で夜間に作戦を遂行したり、高高度で飛行する状況を指す語であり現代の間諜を必ずしも十分に表現しておらず、むしろ活動従事者（又は機材設備）の身元・特性の隠匿という趣旨のcovertの語（本稿では便宜上、「非公然」と訳す）を充てるほうがふさわしいと説明する[12]。

なお、標章非着用要件は独立の要件というよりは、むしろ虚偽隠密要件に含まれると理解するのが正しい。とりわけ航空偵察の場合は、偵察に従事する軍用機が国籍や

12　HPCR, *Commentary on the HPCR Manual*, p.258, Rule 118, para.1; ICRC, *Commentary on the Additional Protocol I to the 1949 Geneva Conventions* (1987), ICRC website, p.567, para. 1776.

軍用機である旨を表示していれば標章は十分に掲示したものとみなされるため、偵察機の搭乗者が制服を着用していなくとも身分を隠したことにはならず制服非着用を理由に間諜とみなされることはない[13]。サイバー空間についても航空偵察と同列に捉えられるのであれば、標章未着用の兵士が軍用端末を用いて公然と監視活動に従事する場合は、国際法上の間諜に該当しないはずである。同様に、例えば軍と契約関係にある文民であっても公然性を条件として国際法上の間諜に該当しないかもしれない。しかし、文民については間諜に該当しないとしても、別途敵対行為に直接参加した不法戦闘員とみなされる可能性がある。とりわけ、軍事作戦に直接利用可能な情報の収集[14]や、特定の作戦を前提に攻撃対象物の脆弱性を探索する行為[15]については、直接参加への該当を肯定する学説もみられる。文民がそのような評価を受ければ、国際法上文民に与えられている（攻撃から免除されるという意味での）保護を失い敵による攻撃にさらされる恐れがある。あるいは直接的ではないとしても、少なくとも間接的には敵対行為に参加したことを理由に身柄捕捉後に文民としての権利を一部制限される恐れがある[16]。このように、サイバー空間を通じた活動がいかなる条件の下で間諜行為に該当するのかという論点については、国家実行が集積していないこともあり、実際の取り扱いがどうなるかは現時点では不明であるが、文民について一つ懸念されるのは、間諜であれ敵対行為への直接参加であれ当該活動に従事した文民が不法戦闘員に分類される点では変わりがなく、いずれにしても文民として本来与えられる保護を喪失する点である。こうした事情をふまえて、学説の中には、敵対行為への直接参加の有無を判別する際には、その文民自身がそのことを自覚しているか否かという心理的要素を加味すべきであると説くものもある[17]。

（2）戦時における文民のプライバシー権

サイバー空間を通じた監視活動は、場所的要件を満たさないことを理由にサイバー間諜行為に該当しないと仮定する場合、一般的には禁止されない「軍事行動」に分類される。第 1 追加議定書 51 条は、文民が「軍事行動から生ずる危険からの一般的保護

13 HPCR, *Commentary on the HPCR Manual*, p.260, Rule 120, para.2.
14 Hans-Peter Gasser,” Protection of the Civilian Population,” in Dieter Fleck, ed., *The Handbook of International Humanitarian Law*,” 2nd. ed.(Oxford University Press, 2008), p.262, para.5.
15 Schmitt, *Tallinn Manual*, p.120, Rule 35, para.5.
16「戦時における文民の保護に関する 1949 年 8 月 12 日のジュネーヴ条約（第 4 条約）」（以下、文民条約）によれば、「紛争当事国の安全に対する有害な活動」（5 条）に従事しているものと疑われた文民は、同条約が保障する文民としての権利を制限される場合がある。
17 Avril McDonald, “The Challenges to International Humanitarian Law and the Principles of Distinction and Protection from the Increased Participation of Civilians in Hostilities,” A Paper Presented at the University of Teheran at a Round Table on the Interplay Between International Humanitarian Law and International Human Rights Law (April 2004), p.23.

を受ける」と定めるが、ここで言及されている「軍事行動」とは、ICRC による同議定書注釈によれば「敵対行為に関連して紛争当事国軍隊によって遂行されるすべての活動」を指す[18]。伝統的な例としては、宣伝流布（1923 年空戦規則案[19] 21 条）などの物理的な破壊効果を伴わない心理戦がこの「軍事行動」に該当する。

第 1 追加議定書を含む武力紛争法関係諸条約、及び国際慣習法のいずれにおいても「軍事行動」を行うこと自体は禁止していないため、サイバー空間を通じて監視を行うこともまた合法である。しかしこうした監視活動の過程で、武力紛争とは全くかかわりを持たない文民のインターネット通信が取得され仮にその情報が軍によって悪用されたとしても、武力紛争法には文民のプライバシー権を十分に保護する規定が存在しない。

戦時における文民のプライバシー権という観点から近年話題になったのは、イラクやアフガニスタンで米軍やカナダ軍などが行った生体認証プログラムである。これは、一般住民に紛れて潜伏したテロリストの身元判別を目的として、光彩、指紋、顔の画像などの情報を採取し数百万人分のデータベースを作成するプログラムである。後に簡易爆発物（Improvised Explosive Device: IED）の爆破後の残存物の破片、自爆テロ犯の死体や脱走兵などから入手した情報をデータベースと照合することによりテロリストの身元を容易に割り出すことができたそうである[20]。しかし単に肉体的に戦闘適性があるというだけで 15 歳から 70 歳までの男性住民の個人情報を無差別に収集し保有することは一般住民のプライバシー権を侵害する恐れがある。またこのデータベースは領域国政府に移管された後で宗派や民族を理由とする虐殺に悪用される危険性が高いという懸念から、米国では複数の人権団体が国防長官に対して見直しの要請を行ったことが知られている[21]。このような問題についても、武力紛争法は文民のプライバシー権を保障するための規定を持ち合わせていない。しかし、だからといって、こうしたプログラムを運用する駐留外国軍隊が、現地住民との関係でなんら責任を負わないことにはならない。「パレスチナ占領地における壁建設の法的帰結」諮問事件の勧告的意見（2004 年）[22] では、イスラエルが占領地住民との関係で 1949 年文民条約に定める各種の規定

18 ICRC, *Commentary on API*, p.617, para. 1936.

19 Hague Rules Concerning the Control of Wireless Telegraphy in Time of Warfare and Air Warfare, Drafted by a Commission of Jurists at The Hague (December 11, 1922-February 17, 1923), Part II Rules of Air Warfare.

20 "To Track Militants, U.S. Has System That Never Forgets a Face," *The New York Times* (July 13, 2011), http://www.nytimes.com/2011/07/14/world/asia/14identity.html; "The Eyes Have It: Biometric Data and the Afghan War," *The Economist* (July 7 2012), http://www.economist.com/node/21558263/print

21 Electronic Privacy Information Center (EPIC), "Iraqi Biometric Identification System," EPIC website, https://epic.org/privacy/biometrics/iraq.html; Alison Mitchell, "Distinguishing Friend from Foe: Law and Policy in the Age of Battlefield Biometrics," *Canadian Yearbook of International Law*, Vol.50 (2013), p.298.

22 Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory, Advisory Opinion, *I. C. J. Reports 2004*, p. 136.

に違反したことが ICJ によって認定されたが、そこでは併せてイスラエルが批准している国際人権条約の規定にも違反したことが認定されたからである。本件では争点とならなかったものの、国際人権法上のプライバシー権を占領地住民に対して尊重する義務がイスラエルに課されていることは同勧告的意見の中でも確認されている [23]。

したがって生体認証プログラムであれ、サイバー空間を通じた監視であれそれ自体は武力紛争法上の特段の制限を受けてはいないものの、敵対行為とは全くかかわりのない現地一般住民のプライバシー権を不当に侵害する場合には国際人権条約に基づく責任を問われる可能性がある。

2．平時におけるサイバー監視活動の評価

ここでは平時のサイバー監視活動を間諜行為と主権侵害との関連で論じ、人権法（プライバシーの侵害）については第 3 節以降で述べることとする。間諜行為は平時と戦時とで同じ形態で行われたとしても、その法的評価は両者で全く異なる。戦時は「敵対紛争当事国の領域を尊重すべき一般的義務は存在しない」故に「戦時の間諜は合法とみなされる」からである [24]。それに対して、平時は他国の領域を尊重すべき一般的義務が存在する故に、他国への侵入を伴う間諜行為は基本的にその国の主権を侵害する行為である。

平時の間諜行為として頻繁に引用される事例としては 1960 年の U-2 撃墜事件（表 2 の「敵国内への物理的侵入」の場合）が挙げられる。同年 5 月 1 日、米国の偵察機 U-2 はパキスタンを離陸して旧ソ連領空を偵察飛行していたところ、同国領域内で撃墜され搭乗員の身柄が拘束される事態が発生した。撃墜された U-2 は、機体上に国籍を掲示していなかったが、事件に先立つ 4 年前から続けられてきた一連の偵察活動は旧ソ連によって既に把握されていたともいわれている。ただし旧ソ連側は撃墜の事実をすぐには公表せず、それ故事実を知らない米国政府は当初同機について米国航空宇宙局（National Aeronautics and Space Administration: NASA）が気象観測目的で運行していたとの虚偽の説明を行っていた。米国のアイゼンハワー（Dwight D. Eisenhower）大統領が全面的に U-2 による偵察飛行の責任を認めたのは 5 月 11 日になってからであった。旧

23　Ibid., p.188, para.128

24　Quincy Wright, “Espionage and the Doctrine of Non-Intervention in Internal Affairs,” in Roland J. Stanger, ed., *Essays on Espionage and International Law* (Ohio State University Press, 1962), p.12; Craig Forcese, “Spies Without Borders: International Law and Intelligence Collection,” *Journal of National Security Law and Policy*, Vol.5 (2011), p.202.

ソ連政府は同月 18 日、国連安全保障理事会に対して米国非難決議案を提出し、その中で「ソヴィエト連邦に対する米空軍の侵略行為」は、国連の原則及び目的と両立しない、旧ソ連に対する主権侵害であり、そのような侵略行為は普遍的な平和に対する脅威を構成すると主張したが、最終的にこの決議案は西側諸国からの賛成票を得ることができず否決された[25]。

この事件において米国の偵察機が旧ソ連の領空を侵犯したのと同様に、ある国が他国の情報システムに対して電子的に侵入すれば被侵入国の主権を侵害する（表 2 の「敵国内への電子的侵入」の場合）。2015 年に判明した米国連邦人事管理局（U.S. Office of Personnel Management : OPM）へのサイバー攻撃と大量の個人情報の漏えいは、その典型例である。2015 年、OPM は連邦職員の個人情報を保管した情報システムが 2 度にわたり外部からのサイバー攻撃を受け大量の個人情報が漏えいした事実を発見した。被害者の範囲は連邦機関の現職員（契約社員などの非常勤を含む）のみならず退職者や出願者にまで及び、その数は約 2,150 万人に達した。このうち 2,090 万人については氏名、社会保障番号、住所、生年月日、居住地、学歴、職歴、渡航歴、直近家族、交友関係などの身元調査記録に記された情報が漏えいした。また指紋情報が漏えいした職員がいることも確認されている[26]。最初のサイバー攻撃が判明した同年 6 月段階から、米国政府は中国政府による関与を疑ってはいたものの、結局、経済制裁などの措置は講じていない。中国政府が事件の容疑者らを逮捕したとの報道もあるが、中国政府の関与を疑う米国政府高官などはこの事件を伝統的な間諜行為として見ており[27]、場所的要件がここでは厳格に解されていないことがうかがえる。

もっとも、間諜行為が国際法上禁止されていない故に許容されるとする前提に立つ場合には、間諜実施国には実質的な非難可能性が存在しないため、主権侵害を理由とする責任の追及はほとんど意味をなさない。さらには、自国領域内の施設などにおいて他国の情報を取得する場合は他国への電子的侵入すらなく、それ故対象国の主権を侵害する恐れもない（表 2 の「敵国外での電子的侵入」の場合）。なお、平時の間諜行為については国際条約などに明文の定義規定がみあたらない状況に鑑み、各国の国内法に一任するという考え方もある[28]。各国の定義は必ずしも同一ではないが、保護された公的情報の入手を間諜行為と定義する場合には、間諜行為を行った場所が海外で

25　Quincy Wright,“Legal Aspects of the U-2 Incident,”*American Journal of International Law*, Vol.54 (1960), pp.836-841; Ingrid Delupis,“Foreign Warships and Immunity for Espionage,”*American Journal of International Law*, Vol.78 (1984), pp.53-75.

26　U.S. Office of Personnel Management website, https://www.opm.gov/cybersecurity

27　“Chinese Government Has Arrested Hackers It Says Breached OPM Database,”*The Washington Post* (December 2, 2015).

28　Wright,“Espionage and the Doctrine of Non-Intervention in Internal Affairs,”p.13.

あっても処罰可能という解釈も成り立ち得る。

表2　平時における間諜行為（侵入/監視）場所的要件と主権侵害の有無

侵入/監視		主権侵害	間諜行為の場所的要件
形態	領域		
物理的	敵国内	有り	満たす
電子的		有り	満たさないという見解が大勢
	敵国外	無し	満たさない

註：電子的侵入の際の監視は、遠隔監視となる。
出所：筆者作成。

3．サイバー監視活動と人権法（プライバシーの侵害）

本節では、国境を越えて行われる通信がサイバー空間を通じて監視される場合に生ずる人権法の問題を考察する。なお前節までで扱った間諜行為や主権侵害の観点からの評価は、人権法を考える上で全く関連性を有さない。第 1 節で触れた「パレスチナ占領地における壁建設の法的帰結」事件においてイスラエルによる人権条約違反を認定した際 ICJ は戦時占領そのものの合法性には触れなかったが、これは戦時占領が合法であるか違法であるかにかかわりなく、現実に支配下においた個人との関係において当局は当該個人の人権を保障する義務を免れないからである。ところで、サイバー監視活動の関連でプライバシー権の問題が生ずるのは国内通信と国際通信の双方についてであるが、人権法の域外適用性の観点から論争の的となっているのは主に国際通信についてである。本稿の関心もこの国際通信に対する監視の法的帰結にあるため、以下では便宜上「国境を越えた監視（越境監視：Transnational surveillance）と「域外監視（Extra-territorial surveillance）」の区分に応じて議論を進める[29]。なお、本節では法制度や裁判例が広く紹介されていることから、国別の事例として米英独の 3 ヶ国を取り上げることとした。

（1）「国境を超えた監視（越境監視）」と「域外監視」

各国の情報機関による通信の監視は、様々な方法によって行われていたことが現在徐々に明らかになっているが、「国境を超えた監視（越境監視）」と「域外監視」の具体例を表 3 に示した。ここでは、主要国による監視活動がこれらの区分との関係でど

29　本文に示した監視の類型は以下の論説にならった。Ashly Deeks, “An International Legal Framework for Surveillance,” *Virginia Journal of International Law*, Vol. 55 (2015), p.9.

のように批判の対象となっているのかを概観するが、人権法においてある監視活動が違法であるか否かの評価基準となる条文は、主に 1950 年「人権及び基本的自由の保護のための条約」（以下、ヨーロッパ人権条約）8 条及び 1966 年「市民的及び政治的権利に関する国際規約」（以下、自由権規約）[30] 17 条である。

ヨーロッパ人権規約 8 条[31]（私生活及び家族生活の尊重についての権利）1　すべての者は、その私的及び家族生活、住居及び通信の尊重を受ける権利を有する。
2　この権利の行使については、法律に基づき、かつ、国の安全、公共の安全若しくは国の経済的福利のため、また、無秩序若しくは犯罪の防止のため、健康若しくは道徳の保護のため、又は他の者の権利及び自由の保護のため民主的社会において必要なもの以外のいかなる公の機関による干渉もあってはならない。

自由権規約 17 条 1　何人も、その私生活、家族、住居若しくは通信に対して恣意的に若しくは不法に干渉され又は名誉及び信用を不法に攻撃されない。
2　すべての者は、1 の干渉又は攻撃に対する法律の保護を受ける権利を有する。

ただし、これらの人権条約は全世界的に適用されるわけではなく、一定の条件を満たした場合に限り領域外に居住する者への域外適用が認められてきた。その条件として事件が起こる度に争点となるのが、ヨーロッパ人権条約 1 条、自由権規約 2 条の以下の条文である。

ヨーロッパ人権条約 1 条　締約国は、<u>その管轄内にあるすべての者</u>に対し、この条約・・・（略）・・・に定義する権利及び自由を保障する。

自由権規約 2 条 1　この規約の各締約国は、その領域内にあり、かつ、<u>その管轄下にあるすべての個人</u>に対し、・・・（略）・・・この規約において認められる権利を尊重及び確保することを約束する。
※下線は筆者。

30　1976 年 3 月 23 日効力発生。日本については、1978 年 5 月 30 日署名、同 6 月 21 日批准書寄託、同 9 月 21 日効力発生。
31　1953 年 9 月 3 日効力発生。和訳は、薬師寺公夫・坂元茂樹・浅田正彦編集代表『ベーシック条約集 2016』（東信堂、2016 年）を参照した。

本稿で取り上げる「国境を超える監視（越境監視）」又は「域外監視」が上記の条件を満たすことを確認できれば、監視によって悪影響を被った被害者はその居住場所や国籍のいかんにかかわらず監視を行った国に対して権利の回復を求めることができる。なお、さきに引用したパレスチナ占領地とこれらの監視活動とでは決定的な違いがある。前者については物理的な文脈で戦時占領が行われており、その占領地の全体にわたり占領当局は、パレスチナ住民との関係で自由権規約に定める自由や権利を保障しなければならない（公の緊急事態を理由に適用を制限した部分を除く）。他方、サイバー空間を通じて監視を行う国は、必ずしも領域外の人やモノに対して物理的な権力を及ぼしていない。そのため、監視を行う国は、被害者が自らの「管轄内」又は「管轄下」にあることを否定し、よって人権条約の域外適用も否定する傾向にある。

表3　「国境を越えた監視（越境監視）」と「域外監視」

●「国境を越えた監視（越境監視）」 Z 国に居住する外国人 a と b がインターネット通信を行ったが、この a-b 間通信がたまたま X 国領域内を通過した。X 国の情報機関は、この a-b 間通信がちょうど X 国領域内を通過するところをデータ取得した。あるいは Z 国に居住する外国人 a と X 国内に居住する c がインターネット通信を行った。X 国の情報機関は、この a-c 間通信が X 国領域内を通過するところをデータ取得した。
●「域外監視」[32] Z 国に居住する外国人 a と b がインターネット通信を行ったが、この a-b 間通信がたまたま Y 国領域内を通過した。X 国の情報機関はこの a-b 間通信がちょうど Y 国領域内を通過するところをデータ取得した。又は Y 国領域内に保管されているデータを取得した。

（2）各国の事例[33]

①米国の場合

米国の情報機関による通信の大量監視は、同時多発テロが起こった 2001 年 9 月に遡る。当時米国政府は同時多発テロを阻止できなかった反省に加えて、引き続き発生が懸念されるテロ攻撃に備えて国家安全保障局（National Security Agency: NSA）に対して新たに電子的諜報活動（シギント）の開始を認めた。これは、連邦議会が大統領に認

32　従来から NSA はドイツ国内拠点での一定の監視活動を認められてきたが、米独間の了解覚書で定めた範囲をはるかに上回る監視活動が NSA によって行われていたことが明らかになり、後にドイツ当局の関与の程度がドイツ国内で問題となった。“GCHQ and NSA Targeted Private German Companies and Merkel,” Spiegel Online (March 29, 2014); “German Intelligence Under Fire for NSA Cooperation,” Spiegel Online (April 24, 2015).

33　フランスの「国際電気通信の監視に関する 2015 年 11 月 30 日法」（LOI n° 2015-1556 du 30 novembre 2015 relative aux mesures de surveillance des communications électroniques internationales）は、フランス国外が発受信先である通信を監視対象とする。他方、ヨーロッパ人権裁判所にはフランスの諜報活動関係法がヨーロッパ人権条約 10 条（表現の自由）に反する旨の申立がなされているが、それらはフランス国内に拠点をおく組織からの申立であるため、本稿では省略する。“Europe: Queue of Complaints Against Snooping Laws Grows by the Month,” *Internet Policy Review* website (March 12, 2016), https://policyreview.info/articles/news/europe-queue-complaints-against-snooping-laws-grows-month/397

めた「軍事力使用授権」の決議（AUMF）[34] の一環として諜報活動が許されるという理解に基づいており、NSA は裁判所の令状を得ずに米国が発受信先である一定の国際的通信を傍受する権限を与えられた[35]。ここで対象となる国際的通信とは、通信の一方の側がアルカイダの構成員か、アルカイダと連携している者か、又はアルカイダと連携した組織の構成員であると結論づけられる合理的な理由が存在する場合である。この諜報活動は「テロリスト監視プログラム」と区分されているが、その細部は公開されていない[36]。このプログラムは「その他諜報活動」とあわせて「大統領監視プログラム」と呼ばれ、大統領による約 45 日ごとの更新によって継続されてきた。しかし 2004 年頃に司法省からその法的根拠の妥当性について疑義を示されたのを契機として枠組みが見直され、2007 年以降 NSA は既存の国内法である「外国諜報監視法（FISA）」[37] の規律の下に戻された。分水嶺となるのは 2007 年 8 月「米国保護法」[38] を経て 2008 年 7 月に制定された「FISA 改正法」[39] である。これによって俗に PRISM 及び Upstream プログラムと呼ばれる FISA702 項の監視プログラムが開始された。これらはいずれも米国領域内で実施され、米国外にいるものと合理的に推測される外国人を対象にする点で表 3 の「国境を超える監視（越境監視）」にあたる[40]。この FISA702 項に基づく監視活動は、司法長官と国家情報長官に対して外国諜報監視裁判所（Foreign Intelligence Surveillance Court）への年次報告書の提出を課した点で少なくとも名目上は裁判所を関与させており、それ以前の大統領監視プログラムが令状を不要としたことと比較すると一歩前進したと言える。その一方で NSA の監視対象はもはやアルカイダに限定されず外国のインテリジェンス情報（国際テロや大量破壊兵器に関する情報など）に改められた点で、

34　Joint Resolution to Authorize the Use of United States Armed Forces Against Those Responsible for the Recent Attacks Launched Against the United States, Public Law. No.107-40,115 Stat. 224 (September 18, 2001) (AUMF).

35　菊地茂雄「補論　非常事態における大統領の権限」平成 22（2010）年度防衛省防衛研究所特別研究成果報告書『主要国における軍の権限に関する法制度』を参照。

36　U.S. Department of Justice, *Legal Authorities Supporting the Activities of the National Security Agency Described by the President* (January 19, 2006), p.5; Offices of Inspectors General of the Department of Defense, Department of Justice, Central Intelligence Agency, National Security Agency and Office of the Director of National Intelligence, *Unclassified Report on the President's Surveillance Program*, Report No. 2009-0013-AS (July 10, 2009), p.6.

37　Foreign Intelligence Surveillance Act (FISA) of 1978, 50 U.S.C. § 1801 et seq.

38　Protect America Act of 2007, 50 U.S.C. § 1805a.

39　Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008 (Public Law 110-261).

40　Privacy and Civil Liberties Oversight Board (PCLOB), *Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act* (July 2, 2014), p.21. なお本文書によれば、両プログラムの違いは、PRISM が監視対象者の電子メールアドレスが発受信先である通信（"to" and "from" communications）データをインターネット通信事業者（ISP）から取得するのに対して Upsream は、PRISM 同様に監視対象者の電子メールアドレスが発受信先である通信データのほか、同アドレスが言及された第 3 者間の通信（an "about" communication）データも取得対象とし、また、これらのデータは、「インターネット・バックボーン」を管理する通信事業者から取得することにある。Ibid., p.33,

従来の大統領監視プログラムと比較すると NSA の監視活動の範囲は大幅に拡大した[41]。

他方、本稿では詳しくは立ち入らないが大統領令 12333（E.O. 12333）[42] に基づく監視活動は、米国外で行われる監視活動を想定しているため、表 3 の「越境監視」にあたる[43]。NSA による監視活動に関しては、米国内の人権団体がいくつかの訴訟を起こしているが、これらはいずれも国内居住者による訴訟であるため、本稿の関心ではなく詳細は割愛する。

いずれにしても、米国政府は自国領域外に在住する外国人との関係では、人権条約の域外適用には消極的である[44]。ちなみに、FISA 702 項に基づく監視活動については 2014 年 1 月に「シギントに関する大統領政策指令 28」（PPD-28）[45] が公表され、人権保護の観点から一定の改善策が示された。同政策指令は、国家安全保障や外交上の利益を追求する目的からシギントが不可欠な手段であることを認めつつ、その一方ですべてのシギント被対象者がその国籍や居所を問わず尊厳と尊重をもって扱われるものとし、その個人情報の取り扱いにあたっては彼らのプライバシーに関する法律上の利益を考慮しなければならないとの立場を明らかにして様々な保障措置を講じると述べている。例えば、同政策指令による最大の改善点とされる、取得された個人情報の保持（retention）期限について、同政策指令 4 項は、米国民であるか否かにかかわらず原則 5 年後に廃棄しなければならないと規定する。しかしながら実際には被監視者が外国人である場合の個人情報は 5 年を超えて保持される場合が広く認められており、実質的に従来の運用が変更される部分はほとんど何もない、という悲観的予測もみられる[46]。

②英国の場合

「国境を超える監視（越境監視）」の違法性を追及する事例としては、英国にまつわるものが好例である。英国では 10 の人権団体が 2013 年 6 月から 12 月にかけてそれぞれ英国の捜査権限裁判所（Investigatory Powers Tribunal）に対して提訴を行っているが、いずれの申立も英国の情報機関である政府通信本部（Government Communications Headquarters : GCHQ）が NSA の取得した情報を共有し、また GCHQ 自身も英国国内法

41 Offices of Inspectors General, *Unclassified Report on the President's Surveillance Program*, p.31; PCLOB, *Report on the Surveillance Program Operated Pursuant to Section 702 of FISA*, pp.24-25.

42 Executive Order 12333- United States Intelligence Activities (December 4, 1981).

43 PCLOB, *Report on the Surveillance Program Operated Pursuant to Section 702 of FISA*, p.107.

44 Public Hearing Regarding the Federal Government's Surveillance Program Before the PCLOB, Testimony of John B. Bellinger III (March 19, 2014), pp.2-3, https://www.pclob.gov/events/2014/march19.html

45 Presidential Policy Directive - Signals Intelligence Activities, Policy Directive 28, 2014 WL 187435 (January 17, 2014) (PPD-28), http://www.whitehouse.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities

46 Daniel Severson, "American Surveillance of Non-U.S. Persons: Why New Privacy Protections Offer Only Cosmetic Change," *Harvard International Law Journal*, Vol.56, no.2 (2015), pp.485-486.

である「捜査権限規制法」（RIPA）[47] に基づく監視プログラム（いわゆる Tempora）の下で独自に通信データを取得し、よって英国政府はヨーロッパ人権条約の主に通信のプライバシー権を保障する 8 条に違反したという内容であった。しかも、この事件の 10 の原告のうち 7 つは英国外に拠点をおく人権団体であった [48]。しかし、これらの申立は捜査権限裁判所によって一部を除きほとんどが認容されなかったため [49]、同一の原告団によってヨーロッパ人権裁判所に対して提訴がなされ、現在、事件は係属中である。

さらにこれらの申立とは別に、2015 年には 663 件もの同種の申立が捜査権限裁判所に対して行われたが、うち 369 件は英国外に拠点をおく原告からの申立であった [50]。これらの 663 件のうち、10 件の申立が先行して審理されたが、捜査権限裁判所は、英国に居住しないか、又は英国に拠点を持たない原告 5 件 [51] の通信について英国政府はヨーロッパ人権条約 8 条の義務を負わないと判断して、裁判所の管轄権を否定した [52]。この事件も近いうちにヨーロッパ人権裁判所に提訴されることが予想される。そのほかにもヨーロッパ人権裁判所には、ビッグ・ブラザー・ウォッチ等対英国事件 [53] など同種の事件も係属しており、同裁判所の今後の判断が注目される。

③ドイツの場合

ドイツ政府は、過去に類似の事件において行った主張を見る限り、英国の捜査権限裁判所とほぼ同じ立場に立つものと分類することができる。インターネット通信ではな

47 Regulation of Investigatory Powers Act 2000 (RIPA).RIPA に基づく監視権限は、2016 年 11 月 29 日に国王の裁可を受け成立した「捜査権限法（Investigatory Powers Act 2016）」第 6 部に引き継がれている。

48 7 件の原告はパキスタン、米国、カナダ、エジプト、ハンガリー、アイルランド、南アフリカに拠点をおく人権団体である。ECHR First Section, 10 Human Rights Organisations and Others against the United Kingdom, Statement of Facts, Application no.24960/15 (May 20, 2015), communicated to the UK Government on November 24, 2015, Appendix.

49 Investigatory Powers Tribunal(UKIPT), Case Nos: IPT/13/77/H(Claimant; Liberty), IPT/13/92/CH(Claimant; Privacy International), IPT/13/168-173/H(Claimant; (1)American Civil Liberties Union, (2)Canadian Civil Liberties Association, (3) Egyptian Initiative for Personal Rights, (4)Hungarian Civil Liberties Union, (5)Irish Council for Civil Liberties, (6)Legal Resources Centre), IPT/13/194/CH(Claimant; Amnesty International Limited), IPT/13/204/CH(Claimant; Bytes For All), Amended Open Determination (June 22, 2015), [2015] UKIPTrib 13_77-H 2, http://www.ipt-uk.com/docs/Final_Liberty_Ors_Open_Determination_Amended.pdf

50 その内訳はドイツ 94 件、イタリアとスウェーデン 12 件、フランス 11 件、米国 145 件、それ以外の諸国 33 件（カナダ 12 件、オーストラリア 10 件を含む）である。UKIPT, Human Rights Watch Inc & Others v. The Secretary of State for the Foreign & Commonwealth Office & ORS, Judgment (May 16, 2016), [2016] UKIPTrib15_165-CH, p.5, para.12, http://www.ipt-uk.com/docs/Human_Rights_Watch_FINAL_Judgment.pdf

51 Ibid., pp.4-5, para.11.

52 まだ審理に付されていない残りの数百件の申立についても捜査権限裁判所は本件と同様の結論を下すことを示唆した。Ibid., pp.24-25, paras.58, 60-63.

53 本件申立は、米国当局から英国へのデータ共有は英国国内法上根拠がないこと、また GCHQ の RIPA8 項 (4) に基づく外部通信の包括的傍受は、曖昧かつ予見不可能な安全保障概念に依拠しており均衡を失する故にヨーロッパ人権条約 8 条 2 の「法律に基づ」く干渉とは言えず違法であるというものである。本件原告団のうちクルツ（Dr Constanze Kurz）博士はベルリンに拠点をおく研究者であり同条約の域外適用の論点にかかわる。ECHR Fourth Section, Big Brother Watch and Others against the United Kingdom, Statement of Facts, Application no. 58170/13 (September 3, 2013), communicated to the UK Government on January 9, 2014.

く衛星通信をドイツ国内の施設において電波傍受した事例ではあるが、ともにウルグアイに在住のドイツ人とウルグアイ人がヨーロッパ人権条約 8 条に依拠して申し立てた際、ドイツ政府は両原告ともドイツの管轄下にはないことを挙げて同条約の本申立への適用を否定した（ヨーロッパ人権裁判所ウェーバー及びサラビア対ドイツ事件[54]）。本件で争われた衛星通信の傍受は、ドイツ国内法である「信書、郵便及び電気通信の秘密の制限に関する法律」（基本法 10 条関係法。以下、G10 法）[55] に基づき実施されたものであるが、インターネットの国際的通信についても同法が根拠規定とされていることから、ドイツ政府はドイツ領域外に在住するとりわけ外国人の通信については管轄の不存在を主張することが予測される。

さらにドイツにおいて対外的な情報収集を任務とする連邦情報庁（Bundesnachrichtendienst (BND), Federal Intelligence Service）は、この G10 法に基づく監視活動の他にも、「連邦情報庁法」（BND 法）[56] に基づく監視活動を従来から実施している。2016 年に改正法案が提出された同法 6 条によれば、BND はドイツ国外に在住の外国人が相互に行う通信を対象とする戦略的監視活動を担当している[57]。ドイツ政府は、通話者の国籍にかかわりなく同法及びドイツ基本法の規定に従い人権を保障すると述べてはいるが[58]、それが果たして厳密な意味における法的義務としてであるのか、あるいは米国の「シギントに関する大統領政策指令 28」（PPD-28）と同様に政策的考慮にすぎないのか真意は不明である。なお、国連の人権問題特別報告者は、ドイツ国外でドイツ当局が行う監視活動についてドイツ国内法上の枠組みが整えられていないことに懸念を提起しているが[59]、このことはこうした域外監視についてドイツ政府が人権法の域外適用を想定していないことを想起させる。

54 ECHR Third Section Decision Gabriele Weber and Cesar Richard Saravia against Germany, the Admissibility of Application no. 54934/00 (June 29, 2006), http://hudoc.echr.coe.int/eng?i=001-76586

55 Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses, Artikel 10-Gesetz, Acts Restricting the Privacy of Correspondence, Posts and Telecommunications (Article 10 Act).

56 Gesetz über den Bundesnachrichtendienst (BND-Gesetz (BNDG)), Act on the Federal Intelligence Service (BND Act).

57 A Consolidated Version of the BND [Federal Intelligence Service] Act [BND-Gesetz] based on the bill that the German government published on June 28, 2016, Reporters Without Borders website, https://www.reporter-ohne-grenzen.de/fileadmin/Redaktion/user_upload/BNDGE_English_Translation_by_RSF.pdf

58 Note Verbale to the Office of the High Commissioner for Human Rights by the Permanent Mission of the Federal Republic of Germany to the Office of the United Nations and to the Other International Organisations in Geneva (October 21, 2016), Note No.: 424/ 2016.

59 Letter to Germany's Ambassador to the UN in Geneva by the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression & the Special Rapporteur on the Situation of Human Rights Defenders & the Special Rapporteur on the Independence of Judges and Lawyers (August 29, 2016), p.7, http://www.ohchr.org/Documents/Issues/Opinion/Legislation/OL_DEU_2.2016.pdf

（3）国際的な機関における評価

「国境を超える監視（越境監視）」と「域外監視」について通信のプライバシー権が成立するか否かの論点は、それを真正面から扱った国際判例がまだ存在しないこともあり法的な評価は定まっていない。2013 年には NSA による監視活動の一部が明るみに出た後、「デジタル時代のプライバシー権」と題する国連総会決議[60]が採択され、諸国の抱く憂慮が示されたものの、明確な国際法違反の認定には至っていない。

インターネット通信の大量監視の事例では必ずしもないが、参考となる先例として挙げることができるのは、ヨーロッパ人権裁判所のリバティ対英国事件（2008 年 7 月 1 日判決）[61]である。本件は、英国とアイルランドにそれぞれ拠点をおく人権団体が相互に行う通信（電話、ファックス、電子メール）が英国国防省の設備によって傍受されたことに関する申立であったが、ヨーロッパ人権裁判所は、この傍受によって取得されたデータがその後どのように処理されるかの手続を英国政府は十分に公表しておらず、よってヨーロッパ人権条約 8 条に反する通信への干渉であると認定した。本件における裁判所の判断がインターネット通信の大量監視の事例についても踏襲される場合には、領域外の外国人についても政府の管轄が肯定され、被害者のプライバシー権に対する違法又は恣意的な干渉の有無が審理に付される余地があるものと思われる。

4．サイバー監視活動への人権法適用

前節では、主要国によるサイバー空間を通じた監視活動をとりわけ国境を超えた通信に焦点を絞って概観した。第一次資料の入手困難さもあり、本稿における考察はほとんど「国境を超える監視（越境監視）」に偏った内容になり「域外監視」については十分な検討を行うことができなかった[62]。この点は今後の課題としたい。とりあえず本稿において確認した各国の監視活動をその種別ごとに人権条約適用の有無を分類したのが以下の表 4 である。

まず物理的領域の場合については、全事例においてではないが A の国家領域外における戦時占領当局や駐留外国軍等の作戦や治安活動については人権条約の域外適用が一定の条件の下に認められており、既に複数の国際判例も蓄積している。また、B の

60　A/RES/68/167 (December 18, 2013), preamble; A/RES/69/166 (December 18, 2014), preamble.

61　ECHR Forth Section, Liberty and Others against the United Kingdom, Application no. 58243/00, Judgment (July 1, 2008).

62　Douwe Korff, “Note on European & International Law on Trans-national Surveillance Prepared for the Civil Liberties Committee of the European Parliament to Assist the Committee in its enquiries into USA and European States’ Surveillance,” European Parliament, Committee on Civil Liberties, Justice and Home website (August 23, 2013).

国境を超える活動についても域外適用が認定された判例が存在する。表 4 の① B に引用した事例は、自国領域内で兵士が発砲したところ自国領域外にいる外国人に着弾し、被害者が重傷を負った事件である（ヨーロッパ人権裁判所アンドリュー対トルコ事件 2008 年 6 月 3 日判決[63]）。銃弾の着弾地点は、事件当時、発砲した兵士の本国であるトルコの支配地域ではなかったが、裁判所は、被害者の被った傷害は当該兵士が至近距離から発砲した直接かつ即時の結果として生じたものであり、よって被害者は事件当時トルコの管轄下にいたものとみなすべきであると結論付けた。この考え方を推し進

表4　領域外在留外国人に対する活動の種別と人権条約適用の有無

		A〈国家領域外で行われる活動〉 国家領域外で活動が実施される場合	B〈国境を超える活動〉 自国内で実施された活動が 他国に影響を与える場合
① 物理領域の場合			
	領域外在留外国人に対する活動例	・戦時占領当局による占領行政 ・駐留外国軍の受入国における活動	・領域外の人への発砲
	人権条約の適用	適用	適用
② サイバー空間の場合			
	領域外在留外国人に対する活動例	域外監視 （Extra-territorial surveillance） 米：E.O 12333 英：ISA 7 項	国境を超えた監視（越境監視） （Transnational surveillance） 米：FISA702 項 独：G10 法 5 条、BND 法 6 条 英：RIPA8 項 (4)
	人権条約の適用 （通信の秘密保護）	専門家の見解は分かれている	専門家の見解は分かれている

註１：
- FISA（外国諜報監視法：Foreign Intelligence Surveillance Act）702 項に基づく監視は「非米国民」を対象として「外国諜報情報」の入手を目的とし、米国領域内で実施される。俗に PRISM, Upstream と呼ばれる。
- G10 法（信書、郵便及び電気通信の秘密の制限に関する法律（基本法第 10 条関係法）：Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses, Artikel 10-Gesetz）に基づく監視は「国際的な電気通信」を対象とし、ドイツ領域内で実施される。
- BND 法（連邦情報庁法：Bundesnachrichtendienstgesetz, Federal Intelligence Service Act）に基づく監視は「外国に在留する外国人相互間の電気通信」を対象とし、ドイツ領域内で実施される。
- RIPA（捜査権限規制法：Regulation of Investigatory Powers Act 2000 (RIPA)）8 項 (4) に基づく「対外通信」の傍受は、英国領域内で実施される。俗に Tempora と呼ばれる。
- E.O12333（大統領令 12333 号：Executive Order 12333 of December 4, 1981）に基づく監視とは、米国外で行うカウンターインテリジェンス活動のことである。
- ISA（情報機関法：Intelligence Services Act 1994）7 項は、英国領域外に所在する機材に対して電磁的放射等に干渉して情報を取得する。

註２：
１「物理領域の場合」は領域外に在留する外国人を対象とする活動であるが、２「サイバー空間の場合」は領域外に在留する外国人の通信データを対象とする活動である。２については通信者が在留する国と通信データの所在国は必ずしも同一ではない。

出所：UK Home Office, Equipment Interference: Code of Practice 2016 (January 2016): ECHR Press Unit, “Factsheet: Extra-territorial Jurisdiction of States Parties to the European Convention on Human Rights,” ECHR website (February 2016) などから筆者作成。

63　ECHR Fourth Section, Andreou against Turkey, Application no. 45653/99, Judgment (October 27, 2009), http://hudoc.echr.coe.int/eng?i=001-95295

めれば、サイバー空間を通じた「国境を超える監視（越境監視）」（表4の②B）についても同様に、監視国の管轄の存在を肯定できる可能性がある。もっとも、①Bが人に対する国家の権力作用であるのに対して、②Bはデータに対する権力作用である点で両者には差異が見られる。また①Bは領域外の者への着弾を待って初めて行為が完成するのに対して、②Bはデータの取得、開封、解析から保持や廃棄に至るまで全て一連の行為が国内で完結する。しかし、そうした違いにもかかわらず、②Bの状況が人権法の域外適用の文脈で議論されるのは、通信にかかるデータはその通信主体である個人に帰属するからである。したがって、②Bの状況についても被害者の受けた損害（プライバシーの侵害）が、ある国による監視活動の直接的かつ即時的な結果として生じたものであると言えるのであれば、被害者は監視国の管轄内にいたとみなすことに支障はないものと思われる。

他方、サイバー空間を通じた「域外監視」（表4の②A）についても、「域外」への権力作用という点では物理的な暴力行為（同①A）と同じであるとしても、データ主体の所在国（表3の区分におけるZ国）とデータ取得地点（同Y国）が分散している状況の下では、人権条約適用に消極的な国は、申立人（被害者）が自国の管轄内にいる旨を否定する可能性がある。しかしながら、越境監視の場合と同様に、被害者の受けた損害（プライバシーの侵害）が、ある国による監視活動の必然的な帰結として生じたものである場合には、電子的な意味においてその被害者は監視国の管轄内にいたことに他ならないのではないだろうか。

一方においてデータへの電子的な権力作用を行いながら、人権諸条約に定める「管轄」の語の意味を物理的な文脈のみに限定して捉えようとするのであれば、結論は常に政府による管轄の不存在であり、監視の対象者は勿論のこと、監視活動の過程で付随的な影響を被った人々のプライバシー権はいつまで経っても保護や尊重を受けることができない。しかしながら、ある国が現に世界中に遍在するデータを取得する技術や能力を有しているのであれば、その権力作用をより現代の文脈に即して説明する努力を払うことが重要であると思われる。

おわりに

本稿では、サイバー空間を通じて情報機関が行う監視活動を、間諜行為、他国の主権侵害そして人権法という主に3つの論点に即して考察を加え、それが従来の国際法上の概念とのかかわりの上でどのように評価されるかという問題を検討した。

とりわけ米国の NSA による大量監視活動は、2001 年 9 月当初は戦時の作戦の一環として位置づけられていたことに照らして、戦時の間諜行為の論点から考察を始めた。戦時の間諜行為が成立するためには場所的要件や虚偽隠密要件を満たす必要があることを確認したが、『タリン・マニュアル』などの学説は場所的要件を厳格に解する故に、サイバー空間を通じた遠隔の監視活動が国際法上の間諜行為に該当する可能性は極めて低いと結論づけているようであった。平時についてはそもそも禁止規則がない故に許容されるとする有力説[64]も見られるが、その見解を前提とすれば、他国の情報システムに侵入して機密情報を窃取するサイバー攻撃は、形式上は主権侵害を構成してもそれのみを根拠に加害国を非難するには実質的な意義がほとんど見出しにくいと思われる。本国と在外公館との間でやりとりする国際通信を自国領域内にいながら取得できる場合は、対象国の主権を侵害する恐れさえない。

しかしながら、今日、国家の権力（管轄権）行使の法的側面を論じる際に、それが物理的手段によるのか電子的手段によるのかで果たして質的な差異が生じるのか検討の余地があるものと思われる。むしろ電子的又は仮想的所在は、領域国の許可なく行われればその国の主権を侵害する行為に相当すると考えるのが自然である[65]。こうした状況からは、場所的要件の厳格な解釈だけを理由に間諜行為であることを否定するのは説得力に欠けると思われる。

他方、サイバー空間を通じた監視活動は、国際法上合法であり、かつ国内法上正当な業務として行われている場合であってもプライバシー権侵害の論点を惹起する可能性があることを確認した。とりわけ領域外に居住する外国人の通信データについて監視国は、一方でそのデータを容易に取得しながら、他方では人権法に基づく権利保障や尊重に消極的である傾向がうかがえた。そのことを正当化する根拠として監視国が挙げるのが、自国領域外の外国人は、自国の「管轄内」又は「管轄下」にいないとする説明である。人権諸条約に規定する「管轄」は、果たして電子的な文脈では観念できない性質のものなのだろうか。人権法についても、サイバー空間という電子的又は仮想的な観点から従来の概念を整理することが重要であると思われる。本稿で見たよ

64　Julius Stone, “Legal Problems of Espionage in Conditions of Modern Conflict,” in Stanger, *Essays on Espionage and International Law*, pp.29-43;Stefan Talmon, “Tapping the German Chancellor’s Cell Phone and Public International Law,” *Cambridge Journal of International and Comparative Law* website (November 6, 2013); Katharina Ziolkowski, “Peacetime Cyber Espionage: New Tendencies in Public International Law,” in idem, ed., *Peacetime Regime for State Activities in Cyberspace* (NATO CCE COE, 2013), pp.425-464; Schmitt, *Tallinn Manual*, p.30; Deeks, “An International Legal Framework for Surveillance,” pp.301-302.

65　2014 年のソニー・ピクチャーズ・エンターテイメント（SPE）に対するサイバー攻撃についてシュミット教授は、SPE 攻撃が北朝鮮に帰属することを条件として米国の主権を侵害すると述べている。Michael Schmitt, “International Law and Cyber Attacks: Sony v. North Korea,” Just Security website (December 17, 2014), https://www.justsecurity.org/18460/international-humanitarian-law-cyber-attacks-sony-v-north-korea/

うに、現在のところその方向性は学説と実務とで必ずしも一様ではない。サイバー空間での安全保障は急速に重要性を帯びるようになっており、日本においても理論・実務両面での世界的な動向を把握した上で、本稿で対象とした3つの論点を含めてサイバー空間での監視活動に関する国際法の知見を蓄えることは喫急の課題である。

（こうのけいこ　政治・法制研究室主任研究官）