「平時のサイバー諜報」概念の問題性――日本のインテリジェンス政策にとって有用な枠組みか

防衛大学校
黒﨑 将広*

諜報または諜報活動（espionage; spying）とは、秘密情報を一方的に（つまり関係権利者の同意なく）かつ秘密裏に収集または取得する行為を広く指す。従来、諜報活動とはどの国にとっても治安維持・安全保障上必要なものであるため、各国もいわば「公然の秘密」に属する事項として当該活動を規制することに慎重であったとされる[1]。ところが ICT の発展により諜報活動が国境を越えて一層活発になると、2013 年のスノーデン事件を契機に、国家による当該活動に対する国際法規制の必要性が注目を集めるようになった。こうした背景の下で 2017 年にサイバー空間への国際法の適用を論じたタリン・マニュアル 2.0（TM2.0）が公刊され、日本でも大きな影響力を及ぼしてきたことは周知の通りである。以降、同マニュアルが採用し、そのスポンサーである NATO サイバー防衛協力センター（CCDCOE）も支持してきた「平時のサイバー諜報（PCE: peacetime cyber espionage）」と呼ばれる概念が国内外（とくに欧米）の専門家の間で広く用いられているが、これが TM2.0 と NATO CCDCOE が目指す政策に適うよう便宜的に定立された造語であることを知る者は少ない。したがって、とりわけ日本の政策実務家がこの概念を用いる際には、その含意を正しく見極め、果たして日本の目指す政策にとって有益であるのか否かを慎重に検討しておく必要がある。

1．造語としての「平時のサイバー諜報」

まず、PCE が国際法上確立した概念でないことは、TM2.0 自身次のように述べていることからも確認できる――「なお、この用語は本規則の目的のために提示されたものであり、独立した法的意義を有しないことに留意すべきである」[2]。

ここで重要なのは、当該活動が「平時」のそれである点が強調されていることである。これは、国際法上確立した諜報活動の規律枠組みが現時点では戦時（国際的武力紛争時）に限定されていることによるものと思われる[3]。つまり、戦時の場合以外に行われる諜報活動については国際法規律が明確でない

---

* 防衛大学校総合安全保障研究科教授

[1] *See, e.g.,* Christian Schaller, "Spies," Max Planck Encyclopedia of Public International Law, September 2015, para.2.

[2] Michael N. Schmitt (ed.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (hereinafter: TM2.0) (Cambridge University Press, 2017), p. 168, para. 2（傍点黒﨑）.

[3] 戦時における諜報活動の国際法規律は、交戦当事者に属する実行者が間諜（spy）として捕らえられた場合の処罰および捕虜待遇を中心に 19 世紀から発展してきた。関係条約規定としては、1899 年・1907 年陸戦法規慣例条約附属規則第 29 条～31 条および 1977 年ジュネーヴ第 1 追加議定書第 46 条がある。詳しくは、黒﨑将広他『防衛実務国際法（第 2 版）』（弘文堂、2026 年）段落 722-724、791-793 を見よ。

ため、その分だけ造語を用いた枠組みをサイバー空間に適用可能な既存の国際法解釈のために新たに提示することも可能であるといった、TM2.0 作成者の政策的意図がそこに見て取れるわけである。

では、こうした新たな解釈枠組みを用いて TM2.0 は一体何を目指そうとしているのだろうか。

2. 「平時のサイバー諜報」の射程とその含意――それ自体は禁止されないとすることの意味

この点について TM2.0 は、「規則 32（平時のサイバー諜報）」で「国家による平時のサイバー諜報はそれ自体は国際法に違反しないが、それを遂行する方法は国際法違反となりうる」と規定している[4]。これは、PCE がやり方次第では国際法上許容される、あるいはそれ自体は国際法上問題ないと解する余地を残しておくことに主眼が置かれたものとして重要である。なぜなら、このような解釈を採用することで、国境を越えたサイバー諜報活動はいかなる場合でも対象所在地国の主権侵害になると主張する立場を牽制し、当該活動の合法性問題にくさびを打ち込むことができるからである[5]。

問題は、このようにして TM2.0 が合法性を確保しようとする諜報活動とは一体何なのかである。上述の戦時における諜報活動については、国際法上の定義が（敵の支配地域における）情報収集のみに条約で限定されているのに対し、PCE についてはそうではない。実際、情報収集だけでなく、情報収集に付随する行為までをも可能な限り国際法上広く許容される行為の範囲に含めようとする TM2.0 の意図が、次の注釈からもうかがうことができる。

> 「サイバー諜報」とは、情報を収集するまたは収集しようとするためにひそかな方法でまたは虚偽の口実で行われる、サイバー能力を用いたあらゆる行為を指す。サイバー諜報には、電子的に送信または蔵置された通信、データ、その他の情報を監視し（surveil）、モニタリングし、獲得し（capture）、または流出させるためのサイバー能力の使用が含まれるが、これに限定されない[6]。

このように TM2.0 における PCE とは、域外・域内の情報収集にとどまらず、そのための方法となる国の行動のすべてを網羅する概念的射程を潜在的に有している。それゆえ、本来であれば情報収集とは区別されるべき破壊工作（sabotage）や影響工作（influence operations）であっても、その目的が情報収集である限りはこれに含まれうることとなり[7]、「それ自体は国際法に違反しない」ものと立論することも理論上は可能になる[8]。TM2.0 が「第 5 章 国際法によってそれ自体は規制されていないサイバー行動（Cyber operations not *per se* regulated by international law）」という項目を特別に設けた上で PCE をそこに位置づけたことの意味は、まさにここにあるように思われる。

---

[4] 中谷和弘他『サイバー攻撃の国際法――タリン・マニュアル 2.0 の解説（増補版）』（信山社、2023 年）42 頁（傍点黒﨑）。

[5] この点に関する議論状況については、例えば Patrick C. R. Terry, “Cyber Espionage and Public International Law: The African Union Rejects the Tallinn Manual’s Relativist Approach to Cyber Sovereignty,” *Harvard International Law Journal*, May 4, 2024, Eliza Watt, *State Sponsored Cyber Surveillance: The Right to Privacy of Communications and International Law* (Edward Elgar, 2021), pp. 85-92、黒﨑将広「サイバー空間における主権――その論争が意味するもの」森肇志＝岩月直樹（編）『サブテクスト国際法』（日本評論社、2020 年）31-43 頁。

[6] TM2.0, p. 168, para. 2.

[7] 実際、NATO CCDCOE も選挙干渉の項目で TM2.0 に基づき PCE を紹介している。*See* NATO CCDCOE, International Cyber Law in Practice: Interactive Toolkit, Scenario 01: Election interference. 日本でもサイバー諜報という概念は広く捉えられているようである。例えば、SentinelOne「サイバー諜報活動とは？その種類と例」。

[8] むろん、そうした場合であっても、実行国および被害国双方の国内法上の制約に服する点は TM2.0 も強調するところである。*See, e.g.,* TM2.0, p. 174, para. 17.

3. 日本の現行インテリジェンス政策との親和性

このような含意を有するPCEという概念枠組みは、TM2.0のスポンサーであるNATO CCDCOEやNATO諸国、Five Eyes諸国にとっては有用であるかもしれないし、実際、そのような役割が期待されている側面もあるだろう[9]。しかし、それが日本のインテリジェンス政策にとっても同様に有用になりうるのかと問われれば、現時点では疑わしいように思われる。理由は少なくとも2つある。

1つは、TM2.0がPCE概念を用いて合法性を確保しようとするサイバー・インテリジェンス活動と日本が目指す同様の活動が今後どこまで一致するのかは未知数だからである。TM2.0がこのように包括的かつ柔軟なPCE概念を用いて合法性を確保しようとする行為とは、情報収集そのものというよりもむしろ、そのための方法と位置づけられる、米国の「前方防御政策（policy of defending forward）」の下で行われるような武力行使未満の破壊工作や情報工作などの多岐にわたる攻勢的行動であると推察される[10]。しかし、日本は、サイバー空間における脅威ハンティングの能力構築でさえ緒に就いたばかりであり[11]、こうしたNATO・Five Eyes諸国が想定する各種インテリジェンス活動の実施体制を整える方向に今後進むかどうか定かではない。米国のような前方防御政策をとらない国にとって、国際法上の正当化のためにPCEを積極的に活用する実益がどこまであるのかは疑問が残るところである。

もう1つは、TM2.0におけるPCEの正当化枠組みが、日本で重要視されるいわゆるポジリスト・アプローチに馴染まないからである[12]。上述のように、TM2.0は国家による諜報活動それ自体が国際法上禁止されないことを強調するためにPCEという概念を考案したと推察されるが、その背景にあるのは、禁止されないものは許容されるとする米国的な国際法の考え方である。日本的な表現でいえばネガリスト・アプローチ（あるいは主権の残余原理）ということになるだろう。実際、米国では、国際法によって禁止されない事項は主権国家の自由に属するものとして正当化されると見る傾向が強い[13]。ところが、対照的に日本のような国では、自国のサイバー行動を正当化しようとしても国際法で禁止されないから許容されると主張するだけでは不十分であり、むしろ（国内法上の「法律の留保」原則のように）それを認める国際法上の権限規範に基礎づける方が重要となるように思われる。とするなら、それ自体が国際法上禁止されないことを強調するPCEを敢えて日本が積極的に援用する実益はこの点においてもやはりないということになる。

---

[9] この点で、領域国の同意なく行われる国家の「純粋な諜報活動（pure espionage activity）」は必ずしも当該領域国の主権を侵害するわけではないとの見解をFive Eyes構成国のニュージーランドが明言しているのは興味深い。*See* New Zealand, The Application of International Law to State Activity in Cyberspace, December 1, 2020.

[10] *See, e.g.,* U.S. Department of Defense, 2023 U.S. Cyber Strategy of the Department of Defense: Summary, September 12, 2023, pp. 1-2. *See also* Josh Gold, "The Five Eyes and Offensive Cyber Capabilities: Building a 'Cyber Deterrence Initiative,'" CCDCOE, Tallinn, 2020.

[11] 2022年の防衛力整備計画で日本政府は、「ネットワーク内部に脅威が既に侵入していることも想定し、当該脅威を早期に検知するためのサイバー・スレット・ハンティング機能を強化する」ことを明確にしたばかりである。「防衛力整備計画について」令和4年12月16日国家安全保障会議決定・閣議決定、6頁。

[12] この点については「参議院議員浜田和幸君提出防衛法制における「ポジリスト」、「ネガリスト」に関する質問に対する答弁書」内閣参質186第105号（平成26年6月3日）（安倍晋三内閣総理大臣答弁）を参照。

[13] この考え方に影響を与えているのが、1927年のローチュス号事件常設国際司法裁判所判決である。同事件で裁判所は次のように述べた。「国際法はこの点で各国に広範な裁量を認めており、その裁量は特定の場合においてのみ禁止規則によって制限されるにすぎない。それ以外の場合では各国は自国が最善かつ最適と考える諸原則を採用する自由を引き続き有している」。The Case of the S.S. Lotus, PCIJ, Series A., No. 10, September 7, 1927, p. 19. 近年でも国際法上の諜報活動は自由の問題であると主張する論考が注目を集めているが、これもまた国際法を禁止規範として捉えていることを示唆している。*See, e.g.*, Asaf Lubin, "The Liberty to Spy," *Harvard International Law Journal*, Vol. 61, No. 1 (Winter 2020), pp. 185-243.

4. 日本は「平時のサイバー諜報」概念を採用すべきなのか

以上を踏まえるなら、今後日本が平時における特定のサイバー情報収集を国際法上正当化する際、TM2.0 の提唱する（欧米的な）PCE の枠組みに依拠するのは有用でないということとなる。さらに言えば、諜報活動や間諜という用語でさえ、国際法上は戦時における敵対行為の方法としてのみ確立した概念である以上、それが意味することについて無用の混乱を避けるためにも、平時の場合には使用を避けるべきであるように思われる。

むしろ日本の場合は、適用国際法規の違いに即して分類し、禁止規範と権限規範の双方の観点から適法な情報収集活動を特定していくのが良いだろう。たとえば、国家による情報収集については、「監視（surveillance）」であれ「傍受（interception）」であれ、自国内で行われる場合もあれば国外に向けて行われる場合もある。前者の場合には自由権規約を中心とする国際人権法が主たる適用法規となるだろうし、外国の日本駐在外交・領事機関が対象となる場合にはさらにウィーン外交・領事関係条約の通信保護規定もこれに加わるだろう。これに対して、域外情報収集活動の場合は主権原則が適用法規の中心を占めることになるが、それが外国領海で行われる場合には国連海洋法条約（無害通航）が、また、犯罪捜査として行われるのであれば欧州評議会サイバー犯罪条約（越境リモートアクセス）が主たる適用法規となるだろう。

他方、TM2.0 では PCE に含められうるような、情報収集のための破壊工作・影響工作その他域外活動については、日本の能動的サイバー防御として行われるアクセス・無害化措置の場合と同じく、武力行使禁止原則・不干渉原則・主権原則・国家責任法（とりわけ違法性阻却事由としての対抗措置・緊急避難）が主たる適用法規となるだろう[14]。

ともあれ、これらいずれの場合についても、PCE を積極的に援用することで国際法上の正当性が強化されるとは限らない点には留意しておくべきである。

本稿は、東京海上ディーアール株式会社が運営する調査研究プロジェクト「サイバー安全保障と能動的サイバー防御（ACD）」の成果の一部です。
https://www.tokio-dr.jp/thinktank/acd/

[14] 詳しくは、西村弓「能動的サイバー防御に関する国際法上の論点」『ジュリスト』1613 号（2025 年 8 月）88-93 頁、黒﨑将広「能動的サイバー防御の国際法枠組み―武力未満と違法性阻却による正当化の可能性―」『国際問題』No. 716（2023 年 12 月）29-37 頁参照。