商用スパイウェア規制の課題（サイバー攻撃能力の民営化）

小宮山 功一朗*

国家が企図するサイバー作戦において民間企業が実行主体・供給主体・能力増幅主体となり得ることは、以前から指摘されてきた。近年の複数の重大事例から、国家のサイバー作戦が、①民間企業が提供する侵入・監視ツール（以下「商用スパイウェア」）の利用、②国家と密接に連携する民間企業への委託・外注という形で、民間に強く依存していることが確認されている。

本稿では、特に商用スパイウェアの利用拡大に焦点を当て、その脅威、国際的な規制の現状と課題、日本の政策への含意を論じる。

2025 年 5 月に成立したサイバー対処能力強化法および整備法により、日本でもアクセス・無害化措置の実施が可能となった。警察、防衛省・自衛隊は重大なサイバー被害を防止するため、国内外のサーバ等に対する措置を実施し得る。この文脈において、商用スパイウェアの利用や民間企業への委託の可能性も否定できない。したがって、その規制の現状を理解することは、能動的サイバー防御の実装に不可欠である。

1．商用スパイウェアの拡散とスパイウェア産業複合体の誕生

商用スパイウェアとは、イスラエルの NSO 社が開発した「Pegasus（ペガサス）」や、北マケドニアの Cytrox などが属する Intellexa 社による「Predator（プレデター）」などに代表される、政府や法執行機関向けに販売される高度なサイバー監視ツールである。現在少なくとも 40 社の商用スパイウェアベンダー(以下「ベンダー」)が存在している。

これらのソフトウェアは、アップル社の iOS やグーグル社の Android の脆弱性を攻撃し、ユーザーの操作を必要としない「ゼロクリック脆弱性」を用いて対象のデバイスに密かに侵入する。侵入後は、エンドツーエンドで暗号化されたメッセージの抽出、GPS 位置情報の追跡にとどまらず、ユーザーに気付かれずにカメラやマイクを起動してリアルタイムでの録音・録画も可能となる。多くの場合、商用スパイウェアは製品ラインアップの一つであり、長期間にわたる大規模な情報収集を可能とするツールなどが合わせて提供されている。

これらのベンダーは、多くの未修正のゼロデイ脆弱性を保有し、悪用している。グーグル社によれば、Android OS や Google Chrome などの主要製品を標的としたゼロデイ脆弱性のおよそ半数以上はベンダーによって発見され、悪用される[1]。

近年、これらのベンダーは「スパイウェア産業複合体（Spyware Industrial Complex）」と呼ばれる不透明なエコシステムを形成している[2]。ベンダーは規制を逃れるために複雑な企業構造を用いている。NSO グループや Intellexa は、イスラエル、ルクセン

* 慶應義塾大学 SFC 研究所 上席所員

1 Shane Huntley. 2024. “Buying Spying: How the Commercial Surveillance Industry Works and What Can Be Done about It.” Google. Retrieved March 18, 2026 (https://blog.google/threat-analysis-group/commercial-surveillance-vendors-google-tag-report/).

2 Brooke Spens. 2024. The Spyware Industrial Complex. Tech4Humanity Lab.

ブルク、キプロスなどにまたがる子会社ネットワークを構築し、当局による規制を困難なものとしている。

ベンダーは「素性の明らかな政府」に対してのみライセンスを販売していると主張する。また、自国で類似の技術がない途上国において、このような製品が犯罪捜査などに用いられること自体は、直ちに否定されるべきものではないとの見方もある。

商用スパイウェアに対する警戒がかつてなく高まっている最大の要因は、利用のカジュアル化と運用のアウトソーシングである。ベンダーは表向き、「テロリストや重大犯罪者の追跡のために、素性の明らかな政府にのみライセンスを販売している」と主張している。しかし現実には、UAE（アラブ首長国連邦）の副大統領兼首相がロンドンで進行中だった元妻との親権裁判において、個人的動機で商用スパイウェアを濫用した事例が示すように、商用スパイウェアは濫用され、政治活動家、宗教関係者、ジャーナリスト、人権活動家などのプライバシーを侵害している。

日本近隣のアジア諸国でも商用スパイウェアの利用が広がっていることを示唆する調査は興味深い。中国、香港、シンガポール、タイ、インドネシアなどの比較的経済規模が大きい国・地域でも利用が確認されている。とりわけ 2021 年のクーデター以来軍政が敷かれているミャンマーでは、14 社のベンダーおよびフォレンジックサービス企業と取引をしている事実が確認されている[3]。

2．主要な規制動向と課題

商用スパイウェアの拡散対策は、各国が足並みを揃えなければ実効性を持たない。この分野の国際的議論は、まず 2022～2023 年に民間団体による提言を契機に本格化した。

2023 年 6 月には EU の PEGA 委員会が最終報告を公表し、NSO 社の Pegasus がマクロン仏大統領を含む政治家に対して使用されていた実態を明らかにした[4]。さらに複数の加盟国での運用実態を調査し、EU 輸出管理規則の強化や統一基準の策定、政府による使用を厳格な条件下に限定することを勧告した。

2024 年 2 月には英仏主導のポール・モール（Pall Mall）プロセス宣言が採択され、政府、産業界、市民社会を含むマルチステークホルダー協議が進展した。日本もこれに加わった。ここでは既存の輸出管理枠組を活用した対策やガイドライン策定が確認された。

さらに 2025 年 1 月には米国主導で国連安保理において非公式討議が開催され、日本も共同スポンサーとして参加し、商用スパイウェアの拡散と濫用防止に関する国際的支持の広がりが示された。

続く 2025 年 4 月のポール・モール・プロセス行動規範では、参加 21 か国が国内規制の強化、未報告脆弱性の囲い込みの自制、企業の責任に基づく分類など、より具体的な対応方針を打ち出した。これらは国際的ガバナンス形成に向けた重要な進展である。

しかし、本稿執筆時点で商用スパイウェア規制は暗礁に乗り上げている状態にある。その主たる要因は以下の 3 つである。

まず、安全保障環境の悪化により、より多くの国が商用スパイウェアを必要としている。民主主義国家も例外ではない。プライバシーや言論の自由への配慮をしつつ、一定のルールや手順を設けたうえで、商用スパイウェアの使用自体は肯定する国が増えている。

スパイウェア産業複合体のロビー活動も活発である。たとえば前述の英仏主導のポール・モール・プロセスでは NSO 社が、具体的な改革の約束をしないまま、プロセスへの参加を続けている。同社が「透明性レポート」において、多国間枠組みへの関与を誇示することで、自らが「厳格な輸出管理に従う責任ある防衛技術プロバイダー」であるかのように振る舞っているという

3 Steven Feldstein and Brian Kot. 2023. Why Does the Global Spyware Industry Continue to Thrive? Trends, Explanations, and Responses.

4 ローラン・リシャール、サンドリーヌ・リゴー. 2025. 世界最凶のスパイウェア・ペガサス. 早川書房.

批判もある[5]。

ロビー活動との直接的関連は明らかでないが、米国の方針転換はスパイウェア規制を難しくしている。米国は、バイデン政権下の 2023 年 3 月に、一部の商用スパイウェアの利用を禁ずる大統領令を出した[6]。大統領令は、外国製の商用スパイウェアを米国政府が運用上使用しないという方針を打ち出した。あわせて各省庁が保有する外国製の商用スパイウェアの情報の集約、商用スパイウェアを製造・販売している企業の調査などを命じている。

このような方針は現トランプ政権には引き継がれていない。2026 年 3 月に公表された米国の新たなサイバーセキュリティ戦略においては「無法な外国ハッキング企業」に対する強力な制裁や、「常識的な規制緩和」を目標として掲げている[7]。スパイウェア規制の分野においては、海外のスパイウェア企業には容赦ない制裁を科して市場から排除する一方で、米国内のセキュリティ企業やサイバー産業に対する規制は大幅に緩和する可能性がある。

以上を踏まえると、商用スパイウェアの全面的禁止は現実的ではなく、濫用防止を前提とした政策が求められる。

3．日本のサイバーセキュリティ政策への示唆

商用スパイウェアを完全に禁止できないとすれば、日本はいかに、これと向き合っていくべきだろうか。

他国を攻撃する強力なサイバー能力を持たない日本にとって、国際的な商用スパイウェアの規制強化は自国の安全を直接的に高める「サイバー軍縮」である。能動的サイバー防御の整備を進める日本が推進すべき次の一手として、以下の 3 点が挙げられる。

第一に、商用スパイウェアを「軍用／民生用」や「合法／違法」という基準で分け、規制する仕組みが機能不全に陥っていることを踏まえた、新しい分離の仕方を検討する必要がある。例えば、英国のシンクタンクはサイバー攻撃を「許可された侵入」と「無許可の侵入」に法的・制度的に大別し、それぞれについて対策を考えることを提唱する[8]。

ターゲットとなるデバイスの所有者やユーザーの同意がある「許可された侵入（Permissioned intrusion：ペネトレーションテストなど）」と、同意のない「無許可の侵入（Unpermissioned intrusion：諜報活動やスパイウェアなど）」という明確な基準で市場を区別すれば、正当な研究調査を阻害することなく、効果的な対策を講じることが可能になるという趣旨である。

背景には、ワッセナー・アレンジメントで 2013 年に「侵入ソフトウェア」が輸出管理の対象に加えられたにもかかわらず、軍用ではなく、民生用のプログラムという説明のもと、厳格な輸出管理の対象とされていないという現状がある。

これまでサイバー空間における国家の責任ある振る舞いを議論する場では、常に「倫理的な」ハッキング、「責任ある」脆弱性情報開示、「合法的な」サイバーエスピオナージとは何かが論じられてきた。多極化する国際社会、多極化するサイバー空間において、価値相対主義的な議論を離れ、対象からの許可という基準を拠り所にするという点に、この考え方の意義がある。

第二に、「Know Your Vendor（KYV：ベンダー

5 Suzanne Smalley. 2026. “Spyware Maker Is Hijacking Diplomatic Efforts to Limit Commercial Hacking, Civil Society Warns.” (https://therecord.media/spyware-maker-pall-mall-process-reputation).
6 Executive Office of the President. 2023. “Prohibition on Use by the United States Government of Commercial Spyware That Poses Risks to National Security.” Federal Register. (https://www.federalregister.gov/documents/2023/03/30/2023-06730/prohibition-on-use-by-the-united-states-government-of-commercial-spyware-that-poses-risks-to).
7 The White House. 2026. “President Trump’s Cyber Strategy for America.” The White House. (https://www.whitehouse.gov/wp-content/uploads/2026/03/President-Trumps-Cyber-Strategy-for-America.pdf).
8 James Shires. 2024. Principles for State Approaches to Commercial Cyber Intrusion Capabilities: Navigating the Policy Challenges of Cyber Intrusion Markets. RUSI.

の身元確認）」の徹底による特定ベンダーの排除である。

スパイウェア企業が EU の規制を逃れるためにペーパーカンパニーや複雑な持株構造を利用する現状に照らせば、表面的な企業名や所在地だけを信用することはできない。日本の政府調達網から「無法なベンダー」を完全に排除するため、実質的な事業拠点や中核となる人材の所在を厳格に確認する KYV のプロセスを制度化すべきである。

第三に、国際 NGO やプラットフォーマーとの連携強化と外交的リーダーシップの行使である。

商用スパイウェアを規制するためにも、日本企業の製品が過度に規制対象とならないようにする観点からも、アクセス・ナウやシチズンラボなどの国際 NGO との連携が不可欠である。日本の立場を継続的に発信していくことが求められる。

あわせて、商用スパイウェアによって脆弱性を攻撃される側であるグーグル社やアップル社などとの情報交換を拡大すべきである。

日本はこれらの企業や NGO の活動を支援し、外交プロセスから人権侵害企業を排除するための厳格な「参加基準」の策定を国際社会に働きかけるなど、価値観を共有する東アジアのリーダーとしての存在感を示していくべきである。

４．おわりに

商用スパイウェアの台頭による「サイバー攻撃能力の民営化」は、一国の技術的な問題ではなく、基本的人権と民主主義、そして国際的な安全保障秩序を揺るがす深刻な脅威である。既存のデュアルユース規制の限界や、米国の方針転換などもあり、規制への道のりは険しい。それでも日本は、自らの安全の確保という目的のために、国際的な規制プロセスに主体的に関与していくことが求められる。

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/