公益財団法人 日本国際問題研究所（外務省外交・安全保障調査研究事業）
平成 26 年度研究プロジェクト「グローバル・コモンズにおける日米同盟の新しい課題」分析レポート

# 昨今のサイバー安全保障政策の課題：サイバー攻撃と自衛権

川口 貴久*

## １．転換期の外交・安全保障政策とサイバーセキュリティ

日本の外交・安全保障政策は転換期にある。2012 年 12 月に発足した第二次安倍政権は「積極的平和主義」や「セキュリティ・ダイアモンド[1]」といったコンセプトを打ち出し、国際的な安全保障環境の変化に適応しようとしている。実際、同政権は国家安全保障戦略の策定、国家安全保障会議の設置、武器輸出三原則の見直しなど次々と重要な決定を下し、2014 年 7 月 1 日には集団的自衛権行使容認を含む安保法制についての閣議決定を行った。サイバー安全保障についても、国家安全保障戦略や防衛大綱でその重要性が確認され、日米協力やマルチ外交も進展している。

それでもなお、サイバーセキュリティ分野に残された課題は多い[2]。その１つが、サイバー攻撃と自衛権の問題である。つまり、国家・社会の安全を脅かすような大規模なサイバー攻撃に対して、自衛権を行使し対処できるのかという問題である。

しかし、日本国内での法的基盤整備に向けた議論が尽くされているとは言い難い。少なくとも、政府や与党が検討しているいくつかの具体的事例ではサイバー攻撃対処は明示されていない。

本レポートでは、サイバー攻撃に対する自衛権行使および周辺課題を整理したい。まず、どの種類のサイバー攻撃が自衛権行使との関係で特に問題になるのかを確認する。その上で、サイバー攻撃への自衛権行使に関する環境整備と日米協力を示したい。

## ２．どの種類のサイバー攻撃が「武力攻撃」に相当するのか

サイバー攻撃に自衛権は行使可能か。2012 年 4 月 26 日、情報セキュリティ会議において外務省は、国際法体系がサイバー空間に適応可能であり、サイバー攻撃が外国からの「武力攻撃」とみなせるのであれば、「サイバー攻撃に自衛権行使可能」との見解を示した。2013 年 10 月 23 日の衆議院予算委員会では、安倍首相が「武力攻撃の一環としてサイバー攻撃が行われた場合には、自衛権を発動して対処することが可能と考えられる」と答弁している。

つまり、「国連憲章を含む既存の国際法体系をサイバー空間に適応できるならば」（仮定。後述）、武力攻撃に相当するサイバー攻撃は自衛権行使の要件となる。問題は、どの種類のサイバー攻撃が武力攻撃に相当するか、である。

北大西洋条約機構の研究者・実務家が作成した『タリン・マニュアル（Tallinn Manual on the International Law Applicable to Cyber Warfare)』によれば、「国際法上の戦争」「武力攻撃」に相当するサイバー攻撃とは、通常の動学的な（kinetic）軍事行動・武力攻撃に相当するもので、「規模」と「影響」を勘案し認定される。米国務省の法律顧問クー（Harold Hongju Koh）は「直接的に

* 東京海上日動リスクコンサルティング株式会社 主任研究員、慶應義塾大学SFC研究所 上席所員（訪問）。本稿の内容は、筆者の個人的見解であり、所属する組織や機関を代表するものではない。

死者、負傷者、重大な破壊行為を引き起こすサイバー攻撃は武力行使と見なしうる」とした上で、①原子力関連施設のメルトダウンを引き起こす攻撃、②ダムを開放し、居住地域へ放水させる攻撃、③航空管制への攻撃を武力攻撃相当として列挙している[3]。

もちろん原則はケース・バイ・ケースだが、以上の議論をふまえるとサイバー攻撃の類型ごとの武力攻撃の認定可能性は以下に整理できる。

表： サイバー攻撃の種類と武力攻撃の認定可能性 （出典：筆者作成）

| サイバー攻撃の種類 | 武力攻撃の認定可能性 | 具体例や留意事項 |
|---|---|---|
| 窃取型攻撃（exploitation） | 低 | 対象の情報を窃取するサイバー攻撃（スパイ活動）。「ゴーストネット［GhostNet］」（2009）、「タイタンレイン［Titan Rain］」（2003）など先端技術・防衛機密へのアクセス。 |
| 妨害型攻撃（disruptive attack） | 低 | 対象のサービスやシステムを一時的に機能停止させるサイバー攻撃。エストニア（2007/4）、グルジア（2008/8）、ウクライナ（2014/3）への DDoS 攻撃など。 |
| 破壊型攻撃 （destructive attack）<br>①データ消去 | 低 | 対象のデータやシステムを破壊するサイバー攻撃（被害はサイバー空間内にあるもの）。shamoon によるサウジ国営石油会社アラムコのデータ消去（2012/8）、韓国の中央銀行・報道機関への攻撃（2013/3）など。 |
| 破壊型攻撃 （destructive attack）<br>②制御系システムへの攻撃 | 高 | 対象のシステムなどを破壊するサイバー攻撃（被害はサイバー空間外に及ぶ）。stuxnet によるイラン・遠心分離機の産業統制システムへの破壊工作（2009）、同種の標的型攻撃（Flame、Duqu、Gaus）など。※Harold Hongju Koh の指摘する類のサイバー攻撃。 |
| 通常の軍事行動と一体のサイバー攻撃（Cyber-Conventional Combination） | 高 | 通常の軍事行動と一体化しているサイバー攻撃。イスラエルによるシリア空爆直前の防空レーダー網へのハッキング（2009）、中国による接近阻止・領域拒否（A2AD）戦略としてのサイバー攻撃など。 |

まず、通常の軍事行動と一体的なサイバー攻撃（Cyber- Conventional Combination: CCC）[4]は武力攻撃に相当する。例えば 2009 年のイスラエルによるシリア空爆の際、シリアの対空レーダー網がサイバー攻撃を受けた事案はまさにこれに該当する。

次に Stuxnet に代表される制御系システム（Supervisory Control And Data Acquisition: SCADA）への破壊型攻撃である。これは現実に物理的実害が生じれば、武力攻撃と認定される可能性が高い。

一方で、2012 年のサウジアラビ国営石油会社「アラムコ」の約 30000 万台の端末データが消去された攻撃などは認定できる可能性は低い。単に経済的損害だけでは認定可能性は低く、市場暴落などの大規模な経済的破綻の場合は意見が分かれる[5]。

また、ネットワーク上の通信量（トラフィック）を増大させ、対象のサーバやシステムに処理不能な負荷を与える分散型サービス拒否攻撃（Distributed Denial of Service attack: DDoS 攻撃）や日常的な情報窃取（exploitation）が武力攻撃と見なすことはほとんど難しいだろう。こうした類の攻撃はただちに「武力攻撃」「国際法上の戦争」とは言えないが、「グレーゾーン事態」に該当する。「グレーゾーン事態」とは、『国家安全保障戦略』や『防衛計画の大綱』といった最近の安全保障政策文書が指摘する「純然たる平時でも有事でもない事態」である。

ただ、マンディアント社の最高セキュリティ責任者（当時）のベトリッチ（Richard Bejtlich）が指摘しているように、エクスプロイテーションと破壊的・攻撃的活動はシステムの脆弱性を探しだすという点で共通していて、両者は表裏一体である。また、DDoS 攻撃のような比較的低強度の武

力行使もそれが繰り返し行われ集積すると「武力攻撃」とみなせる場合がある。武力攻撃か否かの線引きは難しい。

## ３．サイバー攻撃に対する自衛権行使にむけた整備と日米協力

こうしたサイバー攻撃の類型ごとに武力攻撃の認定可能性を整理することは可能だが、実際の認定はケース・バイ・ケースである。また武力攻撃を認定したとしても、自衛権行使は政策的判断・政治的決定である（実際、全ての武力攻撃に自衛権が行使されてきた訳ではない）。したがって重要なことは、危機における自衛権行使の政治決定のため、サイバー攻撃への自衛権行使に関する環境を予め整備しておくことである。ここでは、日米協力の観点でいくつかのポイントを示したい。

### （１）サイバー空間における既存規範の強化

第一に、サイバー空間における既存規範の強化である。サイバー攻撃への自衛権行使の前提は、国連憲章第 51 条（自衛権）を含む既存の国際法体系がサイバー空間に適応されることである。アメリカは『サイバースペース国際戦略』(2011 年 5 月）などで、サイバー空間の新たな条約や法の「再発明」は不要であり、既存の法体系を適用すべしとの立場をとっている。一方で、中国やロシアはサイバー空間に新しい行動規範を構築すべきだと考え、対立が生じている。

この問題は、国連総会第一委員会のサイバーセキュリティに関連の政府専門家会合（Group of Governmental Experts: GGE）の報告書（2013 年 6 月）で「国連憲章を含む既存の国際法体系はサイバー空間に適応可能」という一定のコンセンサスが形成されているが[6]、日米はこうした規範をより強化していく必要がある。

### （２）重要インフラストラクチャの日常的監視と防護

次に、重要インフラストラクチャをはじめとする民間セクターへの攻撃の継続的監視の構築である。2014 年 3 月に発足したサイバー防衛隊は自衛隊ネットワークの防護がメインだが、政府は原発や通信などの重要インフラへの防護に自衛隊アセットが展開できないか検討を始めた。

重要なことは、どのセクターに防衛省・自衛隊、国防総省・米軍が関与するか、である。日米では重要インフラの設定が異なる（表を参照）。この差は、日本は内閣官房情報セキュリティセンター（NISC）が中心となり、情報セキュリティの観点で重要インフラを検討したが、アメリカは 9.11 テロ直後、より広範な国土安全保障の文脈で検討し、従来からの重要インフラを大統領政策指定 21 号（2013 年 2 月）でサイバーセキュリティの観点で確認した結果である。

表: 重要インフラの日米比較

| 日本 13 分野 | アメリカ 16 分野 |
|---|---|
| 情報通信 | 情報技術 |
| | 通信 |
| 金融 | 金融 |
| 航空 | 運輸 |
| 鉄道 | |
| 物流 | |
| 電力 | 原子力関連 |
| | ダム |
| | エネルギー |
| ガス | |
| 水道 | 上下水道 |
| 政府･行政サービス | 政府機能 |
| | 救急サービス |
| 医療 | 医療･公衆衛生 |
| 化学 ＊ | 化学 |
| 石油 ＊ | 該当なし |
| クレジット ＊ | |
| 該当なし | 重要製造業 |
| | 商業施設 |
| | 防衛基盤産業 |
| | 農林水産 |

出典: 情報セキュリティ会議「重要インフラの情報セキュリティ対策に係る第3次行動計画」(2014 年 5 月)、Presidential Policy Directive 21: Critical Infrastructure Security and Resilience(February 12, 2013)を基に筆者作成。いずれも比較のため順序を変更している。
＊は第3次行動計画で新たに追加されたセクター。

こうした重要インフラの設定は見直しと日米の整合が必要である。例えば、農林水産業のサイバーセキュリティは重要だが、それが原子力関連施設と同程度ではないことは明らかである。日米それぞれの重要インフラをサイバーセキュリティ、特に有事における優先度で再定義する必要がある。

また、こうした重要インフラへのサイバー攻撃を継続的に監視するにあたっては、憲法（第 21 条）が保障する「通信の秘密」との整合をはかる必要がある。報道（読売新聞、2014 年 8 月 13 日）によれば、総務省はこれまで厳密に運用してきた解釈を緩和し、悪意あるサイバー攻撃をモニタリングし、場合によっては攻撃を遮断できる環境を整える予定である。

### （3）武力攻撃認定の「閾値」設定

最後に、武力攻撃を認定する基準、つまり「閾値（threshold）」の設定である。「規模」と「影響」を鑑みて、あるサイバー攻撃が通常の武力攻撃に相当するかどうかは結果的に判断可能だが、どの時点で認定できるかが重要である。サイバー攻撃による有事は通常の有事とは異なり、平時から有事への移行が早い。したがって、武力攻撃認定・自衛権行使を判断する時間はほとんどないだろう。

それゆえ日本および日米は武力攻撃認定の「閾値」を予め設定する必要がある。つまり、どの種の、何を対象にしたサイバー攻撃が（実際の被害に至っていなくとも）武力攻撃に相当するかを設定し、自衛権行使の判断材料とすべきである。そのためにも、前述の重要インフラへ継続的監視が不可欠となってくる。

このような環境では、サイバー攻撃による被害が顕在化する前に自衛権を行使するケースも想定される。こうした自衛権行使の形態は「先制行動（preemptive action）」と呼ばれる。「先制行動」のような差し迫った危機に対する自衛権行使も検討していく必要がある。

## ４．おわりに

日本の外交・安全保障政策は国際環境の変化に対応しているものの、サイバーセキュリティ分野については残された課題が多い。自衛権行使の整備は有事における安全保障政策の最重要分野の 1 つである。

しかし、サイバー攻撃への自衛権行使は日本だけでなく国際的にみても整備途中である。日本は国際的議論を「注視する」「見守る」のではなく、自らがリードして環境を整備していく必要がある。その際、既存の国際規範強化、重要インフラの設定・監視、サイバー攻撃の「閾値」設定などを日米で取り組んでいく課題である。

【2014 年 8 月 15 日】

---

[1] セキュリティ・ダイアモンドとは日米豪印など自由や民主制といった価値を共有する諸国による連携を指す。Shinzo Abe, “Asia’s Democratic Security Diamond,” Project Syndicate (December 27, 2012)

[2] 例えば、サイバー攻撃の抑止（deterrence）については、平成 25 年度の研究プロジェクト「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」を参照。

[3] Remarks by Harold Hongju Koh, Legal Advisor U.S. Department of State, "International Law in Cyberspace," USCYBERCOM Inter-Agency Legal Conference, Ft. Meade, MD (September 18, 2012)

[4] 土屋大洋『日サイバーテロ：米 vs.中国』（文藝春秋、2012 年）、37 頁。

[5] コロンビア大学のワクスマン（Matthew Waxman）による見解。Ellen Nakashima, "When is a cyberattack an act of war?," *The Washington Post* (October 26, 2012).

[6] 合意された重要なコンセンサスとしては、“International law, and in particular the Charter of the United Nations, is applicable and is essential to maintaining peace and stability and promoting an open, secure, peaceful and accessible ICT environment.”*Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, UN. Doc., A/68/98 (June 24, 2013), para.19.