我が国のサイバーセキュリティ戦略の欠点と展望

― 「平和国家」体制の桎梏への対応を考える

松村 昌廣　　桃山学院大学 法学部 教授

1 問題の設定と分析アプローチ

近年、我が国政府のサイバーセキュリティ政策に対する取り組みは、一見かなり充実してきた様相を呈している。しかし、日本国内の専門家の評価は全く逆の非常に否定的な評価が顕著である。笹川平和財団の政策提言書『日本にサイバーセキュリティ庁の創設を！』(2018 年 10 月）は米英独仏日の主要五カ国のサイバーセキュリティ政策について詳細な比較分析を行った結果、体制整備、法整備そして産業育成・人材育成の全てにおいて、我が国が極めてお寒い状態にあると評価した。

周知のように、覇権国であり我が国にとって唯一の同盟国である米国との関係が最も深いことから、この分野においても米国の圧倒的な影響を受けて来たのではないかと思われる。

そこで本研究では、米国のサイバー政策における主要な戦略概念をその変移の背景、長短そして含意を焦点に考察した。次に、日米政策連携・協調において制約条件となる既存の日本のサイバーセキュリティ戦略・体制の特徴を分析した。最後に、日本の抱える問題と課題を踏まえて、サイバーセキュリティ政策プロパーにおける展望と施策、そして他の政策領域を横断する総合的な展望と施策を模索した。(猶、本概要は成果論文を約半分に短縮したものである。)

2 米国のサイバー戦略における主要戦略概念の変移 ― 拒否的抑止(積極防衛)から懲罰的抑止(報復能力保持）へ

2-1 従来の欠点・弱点と 2018 年版「国家サイバー戦略」の意義

トランプ政権が 2018 年に公表した「国家サイバー戦略 (National Cyber Strategy:NCS)」はその基本的な発想を拒否的抑止 (積極防衛) から懲罰的抑止 (報復能力の保持と行使) に重点が移した。(こうした変化は、G.W.ブッシュ、オバマ両政権が 2001 年の同時多発テロ以後、国際テロリズムの脅威に対処するために採った戦略・政策を踏まえている)。

したがって、2018 年度「国家サイバー戦略」と「(国防総省) サイバー戦略」が中国、ロシア、北朝鮮、イラン、その他非国家行為主体を対象とするサイバー攻撃と抑止を強調したことは画期的であった。また、下位文書として、サイバー・コマンドが指揮ビジョン文書を策定し、相手方の情報通信システムに入り込んで未然に攻撃を防ぐ (defend forward： 前進防衛) こと、さらに常時、サイバー反撃を行う態勢を維持すること (「継続的従事 (persistent engagement)」戦略) を基本方針としたことは注目に値する。これに実効性を与えるため、トランプ大統領は安全保障政策覚書 (NSPM) 13 を発して、従来必ず大統領の承認がなければサイバー攻撃をできなかったところ、迅速に対処しなければならない状況では一定の手続きと制約条件の下で国防長官に発動権限を与え、サイバー・コマンド司令官に作戦指揮権を付与した。つまり、死者、施設破壊、重大な経済インパクトがなければ、国家安全保障会議の協議や関係省庁との調整を経ることなく、迅速にハッキングや敵の攻撃システムへの攻撃を行えることとなった。

組織・能力面でも、サイバー・コマンドはこの 10 年間で顕著に強化されてきた。従来、戦略軍の下位の統合部隊であったが、2010 年には独立した統合コマンドとなり、直属の部隊と陸海空軍と海兵隊のサイバー・コマンド関連部隊から構成される。

重要インフラ等の民間部門に対しては、2018 年、トランプ政権は国土安全保障省の国家防衛・プログラム局 (National Protection and Programs Directorate: NPPD)を発展的に解消して、外局としてサイバーセキュリティ・インフラセキュリティ庁 (Cybersecurity & Infrastructure Security Agency: CISA) を設置し

公益財団法人電気通信普及財団
研究調査助成報告書 第36号 2021年度

た。つまり、米国において軍事分野を除くサイバーセキュリティの一般主務官庁は国土安全保障省であり、その具体的担い手が同庁である。

したがって、この分野で日本が対米政策連携・協調を行っていくには、こうした米国のサイバー戦略・政策における基本方針と体制の大きな変化がどのような前提、発想、理論に基づいているのか、またそこに陥穽はないのかについて把握しなければならない。

2-2 概念整理と理論的背景

(1) サイバー空間の特徴

コンピューター機器のネットワークにより形成されるサイバー空間は物理的な現実世界にはない独特の特徴を有しており、有効なサイバー政策の策定を難しくしている。

第一の特徴は、サイバー空間へ入ることは、パソコン（端末機器）から回線を用いてサイバー空間へアクセスするだけであり、従来の兵器の操作と比して、極めて簡単且つ安価であり、非常に容易である。

第二には、攻撃者がその発信元を偽造し、事実上、匿名とできるため、そのアドレスを特定するのは容易ではない。また、仮にそこまで辿れたとしても、その端末の物理的所在を探し出すのは容易ではない。確かに、通常はログ（利用・データ更新の記録）により使用端末までは辿り着けることもあるが、それが乗っ取られた踏み台端末（所謂、ボットネット[botnet]による遠隔操作）である場合は、容易に真の攻撃者の端末は判明しない。特に、攻撃者が複数の踏み台端末を経由した場合には、一層困難になる。付言すれば、ログを見てパケットの発信元を確認しても、その発信元自体が虚偽のものに書き換えて送信されていれば、攻撃者を特定することはできない。さらに、攻撃が The Onion Router（Tor）などの匿名通信システムを利用してなされた場合には、攻撃者を特定するのは極めて困難となる。

第三には、仮想空間であるサイバー空間自体には、排他的管轄権(主権)を行使して取り締まる主体はいないし、定義上、その主体と締結する国際条約も存在しない。その結果、取り締まりは攻撃者が居る国家の当局によるものとならざるを得ないが、取り締まる意志或いは能力がない場合、特にその国家自身が直接に攻撃に従事していたり、攻撃を支持したりしている場合には、取り締まる術はなくなる。その結果、どのように対処するかは国際法の合法性や国際政治の利害得失の点で非常に厄介な問題となる。それを回避しようとすれば、明白な戦争や武力行使の一環としてなされるようなサイバー攻撃以外は、容易には強力なサイバー反撃や経済・武力報復に訴えることはできず、結果的に泣き寝入りすることになりがちである。つまり、サイバー攻撃は現実世界の武力行使へエスカレートしにくい。

第四には、サイバー空間はコンピューター通信ネットワークによって相互に繋がり、常時接続している必要がある。その結果、攻撃は任意の手法でいつでも好きな時に実行できるのに対して、防御はそれに対してあらゆる場所で常に備えていなければならないため、相対的に多大な費用、人員とエネルギーを要する。つまり、費用対効果の点から、攻撃側が防御側に対して非常に優位にある。

(2) サイバー事案の尺度・分類と対応責任・危機対処段階

ここまで、曖昧に「サイバー攻撃」と表記してきたが、有効なサイバー戦略・政策を策定するには、その規模や烈度によって事態を分類した上で、各々の条件に則して対処する必要がある。バンクス(Banks、2020、39）氏が、米国の国土安全保障省の下に置かれた連邦緊急事態管理庁（FEMA）が天災等の緊急事態への対処する長年に亘る経験に基づいた分類に準じて整理したのが「悪意あるサイバー活動（Cyber-enabled Malicious Activity: CEMA）の等級」である。つまり、規模、継続期間/頻度、影響力/効果/政治的動機付けを、程度の高いものから低いものへ、ⓐ国家重大サイバー緊急事態（Cyber Incident of National Significance: CINS)、ⓑ国家級・地域級戦略的重要サイバー事態(National or Regionally Strategically Momentous CEMA)、Ⓒサイバー攻撃(Cyber Attack)、ⓓサイバー事案（Cyber Incident)となっている。ⓐ～ⓓ は連続的であり、前後の分類と多分に重複するが、少なくとも概念的に峻別できる。ⓐが昂じて、現実の物理的世界の武力行使と一体化すれば、戦争に分類できるだろう。ⓐでは、サイバー・コマンドにより、攻撃者の情報システムに対してサイバー攻撃がなされる。さらに昂じて戦争となれば、サイバー攻撃は武力攻撃と一体化して、人の殺傷や物理的破壊を含むものとなる。ⓑは国土安全保障の観点からサイバーセキュリティ・インフラセキュリティ庁（CISA）が対処するが、ⓐに近づけば、当然、サイバー・コマンドとの連絡・調整から連携・協力に移行することになる。Ⓒは程度の低いものは情報システムやデータ情報に対するスパイ活動であり、さらに昂じれば対象情報システムの機能妨害や情報・データの窃盗等のサイバー犯罪となる。ⓓは愉快犯的なハッキング（不正アクセス）である。

これを対処責任者/機関と対処様態の組み合わせに落とし込むためには、横軸に被害・結果の程度、縦軸に責任帰属先の判断に関する信頼度とする、シュワブ氏（Schwab, 2018, 194）による CEMA の四類型、「行為主体と責任帰属先判断」が大変役立つ。現実には、ここでも容易には境界ケースを分類できないが、少なくとも概念的には明快である。四類型に対して複数の対処方法が同時に用いられても構わないが、類型別に示された当該対処方法が最も有効である。「類型１」は被害も責任帰属先判定の信頼性も低い場合で、全ての機関・組織が各自で消極防衛を強化・改善する。「類型２」では、被害は限定的であるが、責任帰属先がかなり判別できる場合であり、外交当局による政治・外交的圧力或いは警察力を用いて攻撃を止めさせる。「類型３」では、各国政府の民生分野のサイバー危機対応機関（米国の場合は、国土安全保障省/CISA）が被害緩和のための対抗策を含めた積極防衛を行う。最後に、「類型４」では、国防当局・軍が懲罰的抑止のためにサイバー攻撃だけではなく武力行使を含めた攻撃を行う。

留意すべきは、上記の四段階や四類型は実際には連続的で密接に繋がっており、概念的にはともかく、実践的には明確に分別不可能なことである。

懲罰的抑止を利かせるには、サイバー攻撃能力を保有しなければならないが、そのためには、どこにどのようなコンピューターやコンピューター・ネットワークがあり、どのような脆弱性があるのか等、予め攻撃対象の実態を把握せねばならない。具体的に言えば、それは事前に潜在的攻撃対象のネットワークに侵入して、マルウェアを埋め込むなどして、そのシステムの仕組みを掴んでおかねばならない。さらに言えば、そうしたスパイ活動に乗じて、そのシステムの機能を低下或いは破壊するため、コンピューター・ウイルス等を埋め込んでおき、任意のタイミングで外部からの指令で作動させる状況（つまり、システム管理ソフトを乗っ取る）状況にしておくことが望まれる。つまり、潜在的攻撃対象に対するハッキング、スパイ活動、サイバー犯罪はサイバー手段による積極防衛や懲罰的抑止にとって不可欠である。したがって、軍のサイバー部隊は独自にサイバー・スパイ能力を保有していなければならないし、かなりの程度、諜報機関のサイバー及び非サイバー・スパイ能力に依存することとなる。また、軍だけでなくサイバー諜報機関もサイバー攻撃能力を保有することを意味する。したがって、軍と諜報機関の双方がサイバー・スパイ能力とサイバー攻撃能力を持つのであり、両者の役割・能力保有・権限分担や予算・人員保有に関して緊張や対立を生じがちとなる。さらに言えば、サイバー防御能力は多分にハッキング、スパイ活動、サイバー攻撃による経験、技術、技能に裏打ちされたものであるから、両者は表裏一体であり、そもそも防御に専心すること（専守防衛）など成り立たないと言える。

2-3 困難な責任帰属先判定（attribution）とその克服への道

サイバー分野での抑止を考える際、一般に、①攻撃の利益が抑止の費用よりも高く、攻撃に有利である、②攻撃で利益を得る蓋然性が高ければ高いほど、抑止は難しい、③防御者が攻撃者に課すコストが高ければ高いほど、抑止の蓋然性は高くなる、④この蓋然性が高いと敵対者が見做せば見做すほど、抑止の蓋然性は強くなる、と言える。軍事安全保障研究で発展してきた抑止論、特に核抑止論には厚い知的蓄積が存在するが、それをサイバー分野に当て嵌めるには、以下の事情からかなり注意が必要である。

先ず、現実の物理的世界の軍事安全保障では、専ら兵器の数量増加による報復能力の向上によって抑止効果を高めることができるが、サイバー分野においては、ハードフェア、ソフトウェア、技術者の人員などの投入資源増によって情報システムのセキュリティを大幅に強化しようと試みても、敵対者がそれを打ち破る技術能力を持てば拒否的抑止は効かない。さらに、サイバー攻撃者がどこに存在するのかが分からなければ、報復攻撃を行うことができない一方、攻撃者が誰なのかが分からなければ、現実の物理的世界での懲罰的報復、あるいは法執行上の処罰はできない。留意すべきは、国外からのサイバー攻撃において、同盟国であれば協力関係を結び捜査を続行できる一方、敵国や第３国を経由された場合、捜査は断念せざるを得ない。逆に、誤った責任帰属先判断で、無実の潜在敵対者/国や第三者に報復攻撃を行った場合、当然、相手側は先制攻撃を被ったと理解し、反撃を行う可能性が排除できない。その結果、攻撃・反撃の連鎖が一気にエスカレートするリスクを犯すことになる。その際、反撃がサイバー/電子的手段に留まらず、経済制裁、その他政治外交的な敵対行為の形を取れば、武力紛争・戦争となる可能性が大きい。最悪、反撃が核兵器その他の大量破壊兵器の指揮統制システムに対するものであったり、或いはそう受け止められたりすれば、大量破壊兵器による応酬に発展するかもしれない。

それでは、責任帰属先判定の信頼度を高めることはできるだろうか。否であれば、エスカレーションのリスクが高いために、容易には報復はできず、その結果、いくら報復能力を持っていても使えず、サイバー空

間での抑止は効かないこととなる。既に言及したように、ボットネットや深層/ダークネットの使用のため、サイバー空間における責任帰属先判定は容易ではない。とはいえ、既に米国の軍事諜報コミュニティーが開発・実践しているように、諜報機関と協力して、攻撃のパターン分析や使用ウイルスその他のソフトウェア技術情報に加えて、知覚的、行動上の文脈を総合的に分析・理解すれば、判定の確度はかなり高まる。行動影響分析（Behavioral Influences Analysis: BIA）として知られるこの手法は、社会学、文化人類学、心理学やオペレーション・リサーチを組み合わせて、攻撃者や潜在的敵対者の動機、世界観、行動予測などを行う。

2-4 評価と課題

ここまで見てきたように、米国のサイバー戦略は、同国が近年ますます高い頻度で深刻なサイバー攻撃を被るようになったことから、従来の積極防衛重視から抑止と報復の方向へ大きく舵を切った。確かに、行動影響分析によってサイバー攻撃者を誤判定するリスクをかなり減じることができるようになったが、リスクは完全に排除できる訳ではない。さらに、軍と民生危機管理官庁は双方ともサイバー攻撃とサイバー諜報の能力を保有し、競合状態にあることから、全面的な連携・協力は容易ではない。

日本は、こうしたリスクと課題を抱えた米国のサイバー戦略・政策から多大の影響を受けつつ、様々な国内の制約条件の下で自国のそれを策定していかねばらない。それでは、どのような具体的な制約があり、何がどこまで可能なのであろうか。

3 日本のサイバーセキュリティ戦略・体制の欠点

3-1 2018 年度版『サイバーセキュリティ戦略』

この文書では、サイバー攻撃を受けてからの対処、つまり攻撃を受けることを前提に防御しか考えていない。つまり、どのようにすればサイバー攻撃を被らないようになるのか、或いは、少なくともどのようにすれば、その被害を程度や頻度の点で減じることができるのかが言及されていない。他方、サイバー攻撃を抑止するために、どのようなサイバー/非サイバー的手段による反撃・報復能力を保有・強化するのか、さらに、いかにそれを使用・行使するのかに関する方針が欠落している。両面を総合的に見れば、日本はサイバー空間のセキュリティを極めて受け身で防御する（サイバーセキュリティ）戦略を持っていても、国家安全保障の観点から軍事、外交、経済その他のパワーを駆使して総合的にサイバーによる脅威に対抗する（サイバー）戦略を持っていない。この状況は、本質的には国防における「専守防衛」と同じである。

もっとも、防衛省・自衛隊の方針は、米国の多大な影響を受けて「防衛省・自衛隊によるサイバー空間の安定的・効果的な利用に向けて（2012 年）」に策定し、①サイバー空間を陸海空、宇宙に次ぐ第 5 の作戦領域として初めて位置付け、②「武力攻撃への対処に際し自衛隊がこれを効果的に排除するため、相手方によるサイバー空間の利用を妨げることが必要となる可能性にも留意」するとし、サイバー攻撃の権利を留保し、③「武力攻撃の一環としてサイバー攻撃が行われた場合、自衛権発動の第一要件を見做すと判断」し、単なる受け身の防御から反撃・報復への志向を明らかにした。

しかし、この志向は『（日本）サイバーセキュリティ戦略』（2018 年度版）でも、2018 年度「防衛大綱」でも何ら具体化されないままとなっている。逆に言えば、細部が欠落している上記文書は立派に見えても到底戦略とは呼べない代物であり、曖昧な政策指針程度の内容しか有していない。

次に、制度面や組織面での制約条件を米国のケースと比較分析した。

3-2 NISC 体制と自衛隊サイバー防衛隊

サイバー分野における日米の体制の差異は政府民生部門の危機管理組織と軍担当部隊の間の役割分担と付与権限の差異を把握すればよい。つまり、前者は内閣サイバーセキュリティ・センター（NISC）と連邦サイバーセキュリティ・インフラセキュリティ庁（CISA）であり、後者は自衛隊サイバー防衛隊と米サイバー・コマンドである。

CISA は連邦政府のネットワークの防護、主要インフラの防護の調整、官民の調整等を担っている。その機能を果たすため、2018 年の発足時には既に 3400 名弱の人員を擁し、相当な要員、情報分析能力、事案対処能力と、防護活動を実施或いは支援する機能を有している。特筆すべきは、重要インフラ情報法（2002 年）と下位政令等に則り、CISA は民間部門から任意の情報提供を確実にする制度を確保した上で、その情報シス

テムを直接に監視し、連邦政府各機関や民間組織と協調・協力してサイバー攻撃から非政府民間部門の重要インフラを防護している点にある。

したがって、重要インフラを巡るサイバー危機対処においては、CISA とサイバー・コマンドが曖昧な分担で所管しているが、そこに外交部門は組み込まれておらず、危機対処の政策決定と執行における統合されたサイバーセキュリティ組織・枠組みは存在しない。その結果、サイバー攻撃に対する抑止や報復のための強制外交（coercive diplomacy）の実行においては、制度上、必要な行動の統一性は担保されていない。要するに、米国は未だサイバー分野において総合的な国家強制戦略（national coercive strategy）を有していないし、そのために必要な国家的意思を未だ十分固めていない。

他方、NISC は省庁その他政府機関の情報システムに対する不正な活動を監視・分析する役目を担い、必要な助言、情報その他の援助を提供する。また、行政各部のサイバーセキュリティ政策の統一性を保つための監査、調査研究、企画、立案そして総合調整に関する事務を担っている（内閣官房組織令第 4 条）。つまり、NISC は行政府のサイバーセキュリティ政策関連事務を所管するだけで、立法府や司法府のそれを所管しない。

また、重要インフラを含め民間部門のサイバーセキュリティに関しては、任意の情報の収集・分析・共有で連携、協力、援助するのみである。サイバーセキュリティ基本法は行政各部や民間組織に各々の保有する能力で危機対応することを求めている。したがって、国の機関や重要インフラに対する大規模サイバー攻撃に対する対処責任の主体は曖昧であり、国が主導的役割を果たす体制になっていない。実際、NISC は人員・予算で極めて小規模であり、そうした能力を有さない。

つまり、NISC は連絡・調整機関に過ぎないのであって、残念ながら、日本にはサイバー分野における国全体の危機管理を所管する官庁・機関が存在しない。

3-3 法的制約

こうした安全保障面における日本のサイバーセキュリティ戦略・体制の歪さは、既に触れたように、憲法第 9 条に起因している。自衛隊法改正を含む平和安全法制（2015 年）の下では、厳しい制約条件と手続きの下、自衛権に基づく武力行使を行うこととなっている。ところが、前述したように、サイバー分野における自衛権はそうした条件・手続きを満たすことができないことから、依然として発動できないままである。

さらに言えば､日本には主要国のような真正の諜報機関とそれを可能にするための法制が存在しないため、情報収集やそれに伴う諜報活動ができず、ハッキングなどを利用した積極的なサイバー情報収集活動が容易には許容されない。その結果、しばしばサイバー攻撃その他不正な活動の責任帰属先の判定ができず、抑止や反撃ができない。

具体的には、攻撃者/潜在的攻撃者のサーバーへの侵入は憲法第 21 条 2 項「通信の秘密」への抵触となるであろうし、(36)国境を越えた侵入であれば、主権侵犯に当たる虞が強い。また、サイバー情報収集のためのボット作成は不正アクセス禁止法のウイルス作成罪に該当するであろう。所管官庁は既存の業法による安全基準の設定や事業者に対する指示、命令、行政指導をおこなっているが、米国の重要インフラ情報法に当たる法律がないことから、事業者は物理的な障害発生後の報告義務しかない。つまり、情報システムに侵入されても、物理的な障害その他実害が顕在化しない限り、報道や社会的非難を恐れて報告せず、隠蔽する可能性が極めて高い。

もちろん、日本政府が「通信の秘密ガイドライン」の見直しや情報通信研究機構法の改正により漸進的な施策を取ったが、現体制の根本的な問題を解決できていない。

4 課題と展望

現サイバーセキュリティ体制・戦略の矛盾を克服するにはビッグバン・アプローチ（憲法改正その他の法制整備、それに基づく大幅な財源・人員の増加）を実施すればよい。しかし実際には、これは不可能ではないにしても極めて困難であることは、ここ数十年に亘る軍事安全保障・防衛政策、とりわけ武力行使を巡る議論を見れば明らかである。既に考察したように、この議論とサイバー攻撃・抑止を巡るそれとは本質的に同じであることから､サイバー分野の政策努力も憲法第 9 条の制約を前提にそれを非常に抑制的に再解釈し、細かく状況を分類し、許容される対応を網羅的な列挙方式で立法する同様の形（ポジティブ・リスト方式）で漸進的に進むと思われる。

しかし、変化に向けた原動力は安保・防衛政策の変容と同様、国際安全環境の変化を背景とした米国から

の影響・圧力になる可能性が高いとはいえ、外圧依存のアプローチは次善の策に過ぎない。

4-1 「サイバーセキュリティ庁」構想

現在の我が国政府のサイバーセキュリティ体制は行政各部の縦割りが顕著で、政府内の意志統一が容易ではない。NISC はこの構造的問題に対処するために設置された機関であるが、権限と人員・予算の点で、そうした機能を十分には果たすことができていない。また、行政府のサイバーセキュリティを所管としており、重要インフラを含め国全体のサイバーセキュリティを確保する権能を付与されていない。NISC は小規模な組織であり、独自/プロパーのサイバー危機管理人材を擁しておらず、事実上、実務はサイバーセキュリティ業界からの少人数の出向者に依存している状態にある。

この行政機構上の問題の解決はますます逼迫する財政緊迫の中、財源確保のため極めて難しい。

この点、笹川平和財団がインターネット通信に通信量単位当たりで少額の賦課金を徴収する方式で 2000 億円/年を捻出し、2000 人の要員を確保する「サイバーセキュリティ庁の創設」を提言したことは注目に値する。この規模の組織能力を保有すれば、常時、国家の安全保障を脅かすサイバー事案の危機管理に備えて対応チームを待機させることは可能であるから、ここにサイバー危機管理における命令権を付与してもよいだろう。また、米国の重要インフラ情報法に類する立法を行い、重要インフラのサイバー事案に関して「サイバーセキュリティ庁」が分析、判断、対処が可能となるように、検知その他の事実の報告義務を課することもできる。

しかし、仮に行政機構上の課題が改善されても、サイバー攻撃に対する抑止を確保するためのサイバー攻撃能力の保有とその使用に関する法的な制約は、憲法第 9 条や第 21 条 2 項（「通信の秘密」）に基づいているため、改憲若しくは解釈改憲をしなければ、取り除いたり、緩和したりできない。日本にとって政策上、現実的な選択肢は何であろうか。

4-2 米国による「サーバーの傘」

現在、自衛隊サイバー防衛隊は約 300 人の人員を擁しているが、2019 年（平成 31 年）「中期防衛力計画整備計画」では、同隊を 1 個隊（約 1000 名）に増強するとしている。

しかし、今のところ、日本政府が大胆なサイバー政策の路線変更に乗り出す気配はない。実際、2021 年 5 月 13 日、政府のサイバーセキュリティ本部が公表した「次期サイバーセキュリティ戦略の骨子について」（以下、「骨子」）は既存の体制とアプローチを変更せず、漸進的に従来の施策を強化するアプローチを明確にした。特に、抑止力の必要性を述べておきながら、攻撃力の保有、行使方法そして必要な法的整備については全く具体的な言及がない。依然、総合調整・情報共有機能しか有さない NISC を中核とした体制を維持することから、残念ながらこのままでは、「次期サイバーセキュリティ戦略」は妥当な政策目標を曖昧に記した優れた官僚作文の域を出ないものとなるであろう。

注目すべきは、「骨子」がサイバー空間における抑止を実現するために、日本自身がサイバー手段による抑止力（サイバー報復・攻撃力）を保持することに言及することなく、「２＋２」共同発表により（2019 年 4 月）、実質的に米国に抑止力に依存する方針を明らかにした点にある。もちろん、米国のサイバー攻撃能力が世界最高レベルであることから、一応、現時点では、日本が自前の能力を政治的意思と技術力の両面で保有しない方針である以上、次善の策ではある。

政治的には、この対米依存は日本の独立性に疑問を投げかける。さらに、仮に「サイバーの傘」が想定する攻撃者/潜在的攻撃者に対して有効に機能するとしても、諜報活動は同盟国・友好国の間にもなされることが常であることから、米国から我が国に対するサイバー・スパイ活動その他不正な活動にはかなりの程度無防備になることを意味する。

戦略的には、サイバー攻撃の責任帰属先判定に不確実性が伴うことから、誤判定による攻防によるエスカレーションから米国の始めた戦争に巻き込まれるリスクが排除できない。さらに、「核の傘」と同様に、米国が自国への反撃のリスクを犯しても日本のために攻撃するとの言質に対する信頼性の問題が「サイバーの傘」にも存在する。

4-3 綜括と展望

ここまで、本概要では我が国のサイバーセキュリティ体制・戦略が長年の努力にも拘わらず、日本国憲法による「平和国家」体制の下、非常に歪な形で形成されてきた現状を分析・考察してきた。既に述べたよう

に、今後のサイバーセキュリティ政策は既存の体制・組織を前提に漸進的に改善・強化していくことにならざるを得ないだろう。具体的には、NISC を危機管理権限、組織、人員・能力の点で強化しつつ、「サイバーセキュリティ庁」の実現を模索する一方、拒否的抑止（サイバー攻撃の阻止や被害限定）を強化することになる。ただ、サイバー攻撃による懲罰的抑止はおこなわず、その代わり、米国の「サイバーの傘」の下に入り、その有効性を高める対米政策連携・協力を推進することになるだろう。

とすれば、今後の日本のサイバー戦略は、サイバーセキュリティ政策プロパーでは、米国その他の主要同盟国の動向に立ち遅れないように努力する一方、法執行や外交など非サイバー政策手段を総動員して綜合的な取り組みを行うことが最も望ましい。特に、依然我が国が比較優位を保持する半導体や通信機器等、サイバー関連のハードウェアの技術や生産を通したサイバーセキュリティを強化し、この分野におけるパワーと影響力を高めることが望まれる。

【参考文献】

茂田忠良「サイバーセキュリティとシギント機関 ― NSA 他の UKSA 諸機関の取り組み」『情報セキュリティ総合科学』第 11 号、2019 年 11 月。

Banks, Ronald, Confronting t*he Cyber Storm: A Coercive Cyber Strategy to Defend the Nation,* independently published through Amazon.co.jp, 2020, p. 39.

Brantly, Aaron F, ed, *The Cyber Deterrence Problem,* Rowman & Littlefield International, 2020.

Canton, Jeffrey L. Caton, Evaluation of the 2015 DOD Cyber Strategy: Mild Progress in a Complex and Dynamic Military Domain, U.S. Army War College, 2017.

Gary Schaub, Jr, ed, *Understanding Cyber Security: Emerging Governance & Strategy,* Rowan & Littlefield, 2018.

Glaser, Charles L, ”Deterrence of Cyber Attacks and U.S. National Security,”Report GW-CSPRI-2011-5, June 1, 2011.

Whyte, Christopher, and Brian Mazanec, *Understanding Cyber Warfare: Politics, Policy and Strategy*, Routledge, 2019.

程琳(主编)『中美网络安全比较研究』中国人民公安大学出版社、2017 年。