《研究ノート》

サイバーセキュリティ戦略の国際比較
―目的と対象範囲に基づく四類型―

小宮山　功一朗・土屋　大洋

はじめに

サイバーセキュリティが、今日我々が生きる社会における重要課題の１つであることは論を待たない。世界経済フォーラムが主導する世界的な重大リスクに関する調査の結果(1)を例にとれば、サイバー攻撃は異常気象、自然災害、大規模不随意移民、テロリストによる攻撃につぐ５番目に大きなリスクとされている。政策としてのサイバーセキュリティ対策を容易ならざるものにする要因としてたびたび指摘されているのは、第一に、サイバー空間の土台ともいえるインターネット技術が現在も急速に進歩しているということである。クラウドサービスやIoT（モノのインターネット）(2)や暗号通貨などの新たな技術は、新たな攻撃手法や新たな脆弱性を生み出す。そして、それに対応した制度が求められるからである。

第二に、サイバーセキュリティ対策とサイバー空間の開放性の適切なバランスが求められることである。自由な情報の流通を阻害することなく、技術革新を妨げることなく、公序良俗に反する情報だけをインターネット上からとりのぞくことは難しい。とりわけ民主主義体制の国においては、サイバーセキュリティ対策は開放性や自由な情報の流通と安全性の両面への配慮が求められる。

第三に、インターネットやサイバー空間の多様な利害関係者（ステークホルダー）の存在が挙げられる。一国のサイバーセキュリティを確保するためには国内の関係組織、民間事業者、教育機関などの連携が不可欠である。

第四に、国家がサイバー攻撃の実行者となっている事実がある。2014 年 11 月に発覚したソニー・ピクチャーズエンタテイメント社へのサイバー攻撃による社内メールの暴露事案、2015 年６月に政府職員約 2150 万人の個人情報が漏えいした米国人事管理局（OPM）へのサイバー攻撃、そして 2016 年２月にバングラデシュ中央銀行がサイバー攻撃を受け約 8100 万米ドルの不正送金の被害にあった事案などは、全て国家による関与が疑われている。情報機関、軍隊のサイバー担当部門の機能強化が進められ、インテリジェンス活動における情報技術の重要性が高まった。国家は近隣諸国からのサイバー攻撃の脅威を感じながら、単に防御に専念するのではなく、自らの安全を確保するために攻撃を行うようになった(3)。

これら様々な課題を認識した上で、各国政府はサイバー空間における自国の利益を最大化するという共通の目標を持ち、サイバーセキュリティ対策を進めている。

サイバーセキュリティ戦略はその国におけるサイバーセキュリティ対策の重要な要素である。サイバーセキュリティ戦略の定義については現在も検討が行われているが、本稿で

は「一定の期間にわたって特定の国家の目標を達成するために作成される、情報通信インフラに存在する情報・非情報資産の保護のための計画、もしくは方法論(4)」と定義する。2011 年には少なくとも 20 の国がサイバーセキュリティ戦略を策定し、公開していたが、2017 年の本稿執筆時にはその数が少なくとも 78 カ国に増加している。

本稿の出発点は、多くの政府がサイバーセキュリティ戦略と呼ばれる文書を策定している一方で、その内容が極めて多様であることへの関心である。国家サイバー戦略ポリシー、情報セキュリティ戦略など文書の名前が異なるだけでなく、策定の時期、その文書の国内における位置づけ、取りまとめを行った政府機関などが大きく異なっている。なぜそれらは策定されるのか。それによって各国政府はどのような課題を解決し、いかなる読者に、どのようなメッセージを届けようとしているのであろうか。サイバーセキュリティ戦略から主要国のスタンスを明らかにしていきたい。

サイバーセキュリティの犯罪対策の側面については「当該分野の唯一の多国間条約(5)」であるサイバー犯罪条約（ブダペスト・コンベンションと呼ばれることも多い）が存在するが、批准している国は少ない。アジア太平洋地域では日本とオーストラリアとスリランカのみである(6)。国際的なサイバー空間の安全保障に関する議論が国際連合総会第一委員会に設置されている政府専門家会合（GGE）において協議されているが、加盟国を拘束する形での合意はできていない。いまだサイバー空間は、古典的な国際政治でいうアナーキー状態にあり、そのガバナンスが問われている状態である。

本稿ではまず第１節で先行研究における発見と本稿の分析の枠組みを明らかにする。第２節では主要８カ国のサイバーセキュリティ戦略の内容の質的な差異を見出す作業を通じて、サイバーセキュリティ戦略の多様性が生まれる背景を考察する。第３節ではサイバーセキュリティ戦略をその内容をもとに４つの類型に分けることを試みる。それぞれの類型に応じたサイバーセキュリティ戦略策定者の狙いを考察するための視座を提供する。

１．サイバーセキュリティ戦略の国際比較

(1) 先行研究

ヨーロッパ情報セキュリティ庁（ENISA）や北大西洋条約機構（NATO）サイバー防衛センター（NATO CCD COE）は、サイバーセキュリティ戦略が各国の思惑についての透明性を高め、緊張を緩和する役割を果たすものとして捉えており、各国の新旧サイバーセキュリティ戦略を収集し、保管している(7)。CCD COE による『サイバーセキュリティ戦略フレームワークマニュアル(8)』はサイバーセキュリティ戦略を策定する際に検討すべき論点、解決すべきジレンマを提示している。サイバーセキュリティ戦略を策定する国々にマニュアルを提供することを通じて、サイバーセキュリティ戦略の標準化を図り、国際的な比較を容易にするためのアプローチと考えられる。

分析の対象を限定し、緊張関係にある二国間のサイバーセキュリティ戦略を比較することにより両者の思惑を読み取ろうという試みも行われている。リザ・アズミ（Riza Azmi）らは 54 カ国のサイバーセキュリティ戦略の調査を通じてサイバーセキュリティ戦略が現在のサイバー空間における自国の保護だけを目的としておらず、技術革新が進行中のサイバー空間における将来の権益確保のための法的動機（jurisprudence motive）としての側面を持つと結論づけた(9)。また、キョンシク・ミン（Kyoung-Sik Min）らは米国、欧州、日本のサイバーセキュリティ戦略について政府の役割と民間事業者の役割の多寡の観点から分析を行い、サイバーセキュリティの分野における官民の役割の分担の難しさを指摘する(10)。エリック・ルイーフ（Eric Luiijf）らは 2003 年の 19 のサイバーセキュリティ戦略を対象とした研究においてサイバーセキュリティ戦略を具体性、測定可能性、達成可能性、現実性、適時性の５つの尺度で評価するアプローチを提案した(11)。

本稿とこれらの違いは、次項で提示する４つの分類に基づき、各国の思惑を再整理した上で、各国がそれらを作成・公表する意義を検討することになる。サイバーセキュリティ戦略はなぜ出されるのか、言い換えれば、なぜ、誰に向けて出されるのかを分析する。

(2) 分析の枠組み

本稿では分析の対象を国連安全保障理事会常任理事国５カ国（米国、英国、フランス、ロシア、中国）、それに日本とドイツとオーストラリアを加えた８カ国に限定した。その上でアズミらが検討しなかった 2015 年後半から 2017 年前半までの関連文書と分析対象国が過去に策定したサイバーセキュリティ戦略を分析対象に加え、それらの国のサイバー空間に関する認識の差異、政策転換などの変化を明らかにすることを試みた。対象としたサイバーセキュリティ戦略は以下の表１の通りである。

表１　本稿の分析対象としたサイバーセキュリティ戦略

国名	文書名（成立もしくは公開年）
米国	“Cyberspace Policy Review” (2009)(12) “International Strategy for Cyberspace” (2011)(13) “Executive Order - Improving Critical Infrastructure Cybersecurity” (2013)(14) “The Department of Defense Cyber Strategy” (2015)(15)
英国	“National Cyber Security Strategy 2016-2021” (2016)(16) “The UK Cyber Security Strategy Protecting and Promoting the UK in a Digital World” (2011)(17)
ロシア	“Basic Principle for State Policy of the Russian Federation” (2013)(18)
フランス	“French National Digital Security Strategy” (2015)(19)
中国	国家互聯網信息弁公室『国家網絡空間安全戦略』(2016)(20) 中華人民共和国政府『網絡空間国際合作戦略』(2017)(21)
日本	『サイバーセキュリティ戦略』(2015)(22) 『サイバーセキュリティ国際連携取組方針』(2013)(23) 『重要インフラの情報セキュリティ対策に係る第 4 次行動計画』(2017)(24)
ドイツ	“Cyber Security Strategy for Germany” (2011)(25)
オーストラリア	“Australia's Cyber Security Strategy” (2016)(26)

それぞれの戦略文書について特に以下の点を確認した。

基本情報として収集したのは、成立または公開の時期、文書の有効期限、所管する省庁、関連する戦略文書や法律などの国内文書体系との関係における文書の位置付けである。次に、記述があれば各国の現状認識に着目した。例えばサイバーセキュリティおよびサイバー空間といった言葉の定義、重要インフラの定義、サイバー空間に関する現状の認識などである。サイバーセキュリティ戦略そのものの内容については、戦略策定の目的、目的達成のための特徴的な施策、施策実施のための予算措置の有無などに着目した。合わせて国家による攻撃的サイバー能力の準備、サイバーセキュリティ技術を活用したインテリジェンス活動についても記述を収集した。

２．サイバーセキュリティ戦略の比較

(1) サイバー空間のあるべき姿の相違

一般的にサイバー空間におけるセキュリティの確保を目的とするのがサイバーセキュリティ戦略であるが、サイバー空間のあるべき姿について主要国の中には意見の相違がある。例えば、日本政府のサイバーセキュリティ戦略は自国の施策を示す前に、まず現在のサイバー空間について「情報の自由な流通の確保」「法の支配」「開放性」「自律性」「多様な主体の連携」という５つの基本原則が国境を超えて確保されるべきであると掲げている。同様の記述は中国とロシアを含めた多くの国で見られる。

逆に中国とロシアの戦略のみに見られたのが、内政干渉への警戒感を示す記述である。ロシアは「国際情報セキュリティに関する４つの主要な脅威」の１つとして「主権国家の内政への干渉、公的秩序の破壊」などを明記している。中国はサイバーセキュリティ戦略の目的として「サイバー空間における平和、安全、開放、合作、秩序」を掲げており開放性を否定しているわけではない。他方、同文書後半に「ネットワークを利用した他国の内政への干渉、政治制度への攻撃、社会的動乱の扇動（後略）」をサイバー空間の脅威として挙げて、やはり内政への干渉への警戒感を示している。それぞれ内政干渉の具体的事例についてサイバーセキュリティ戦略には記述されていないが、国内の治安維持の必要性からサイバー空間の利用に制限を行っている中国とロシアに対して、「言論の自由」を理由に規制の撤廃を求める西側諸国の主張を横槍と捉えていると解釈すべきであろう。

ロシアにおいて情報セキュリティとサイバーセキュリティの言葉は明確に使い分けられている。サイバーセキュリティはソフトウェアやハードウェアなどを含めシステムそのもののセキュリティを意味し、情報セキュリティはその上でやりとりされる情報の中身（コンテンツ）も含めた保護を意味する。「ネットワークやシステムのセキュリティだけでなくコンテンツのセキュリティも国家により管理しないと、国家の安全を担保できない[27]」との考え方から、今後もロシアはコンテンツの規制に前向きな姿勢を持ち続けるであろう。

(2) サイバー攻撃能力の保持・使用

政府・軍隊がサイバー攻撃を行う能力を保持することについて各国のサイバーセキュリティ戦略はどのような記述をしているのだろうか[28]。分析対象の中で最も直接的にサイバー攻撃能力に触れているのは「攻撃的サイバー能力について世界のリーダーの地位を目指す」という英国、そして「抑止のためにサイバー攻撃能力を使用する」とするオーストラリアのサイバーセキュリティ戦略である。

サイバー攻撃能力に言及するのはこの２カ国が初めてではない。振り返れば米国、ロシア、イスラエルを始めとするいくつかの「サイバー先進国」が、サイバー攻撃能力を高め、サイバー兵器開発を行っているという推測は複数の専門家によってなされていた[29]。しかしながらサイバー攻撃能力について政府がその存在を対外的に認めることはなかった。

2010 年に転機が訪れる[30]。まず米国においてサイバー軍が公式に発足した。さらに米国がイランの核処理施設をサイバー兵器によって攻撃したいわゆるスタックスネット事件[31]が公に知られることとなった。サイバー攻撃能力を有していることを否定することが難しくなったのである。

そのような状況下、2011 年３月に公表された米国の『サイバー空間に関する国際戦略』は、サイバー攻撃能力について「(米国は) サイバー空間での自衛の権利を保持する」という表現ではあったものの、「サイバー空間での敵対的行為に対して軍事力の使用も辞さない」という姿勢を明らかにした。それから約４年後の 2015 年４月に公表された『国防総省サイバーセキュリティ戦略』は、イスラム国がサイバー空間を活用し、人員のリクルート活動を行っていることなどを引き合いに、国防総省におけるサイバーセキュリティ対処能力強化の正当性と重要性を強調した。この中でサイバー攻撃能力について「(大統領からの命令あらば)、国防総省はサイバー作戦を用いて、敵方の指揮通信ネットワーク、軍事関連の重要インフラ、および兵器使用能力を混乱させる能力を持つべきであり、そのための準備を進める」とある。2011 年の国際戦略との比較においてサイバー攻撃実施の可能性がより具体的に記述されている。

2010 年以前、公に言及される機会がなかった国家のサイバー攻撃能力は、2011 年以降、段階的にその「保持」が表現の手段を変えて明言されるようになった。本節冒頭で紹介した 2016 年に公開されたオーストラリアと英国のサイバーセキュリティ戦略には「保持」からさらに一歩進んでサイバー攻撃能力の「使用」を強く想起させるものとなっている。今後これに対抗して、他の国がサイバー攻撃能力についてアピールすることが予想される。

(3) パートナーシップ政策の相違

サイバーセキュリティは最適なグローバル・ガバナンスが模索されている分野であり、国の枠を超えた議論は欠かせない。現段階では本稿の対象とする８カ国中、フランスとドイツを除く６カ国がサイバーセキュリティについて自国が重視する国際機関や会議体を列挙している。６カ国の全てが名指しで重要としているのが国連である。とりわけ総会決議

によって招集される国連政府専門家会合（GGE）[32]については法の支配を議論する場として期待が高いことが分かった。中国は「国連の主導を支持し、各方面が普遍的に受け入れられる、サイバー空間国際規範、サイバー空間国際反テロ公約の制定を推進し、サイバー犯罪を打撃する司法協力メカニズムを整備する」と国連によるサイバー空間のガバナンスを明確に望んでいる。ロシアと中国は 2011 年に「情報セキュリティに関する国際行動規範」[33]という文書を提案し、サイバー空間国際規範の国連総会での議論を求めた。両国らの提案した規範は国家による情報空間での主権管轄（国家によるサイバー空間における主権と領土の保全）、サイバー兵器や関連技術の規制、サイバー空間における資源の公平な配分などを認めるという内容であった。とりわけ「主権国家は情報空間の管理に同等の権利と責任を有する」という原則は、現在のサイバー空間に大きな影響力を持つ米国[34]および国内に大規模な情報通信事業者を有する西側先進国にとっては受け入れがたいものであったと考えられる。ロシアと中国は 2015 年にも同様の提案を行っているが、いずれも総会で議論されることはなかった。

国連に次いで重要と考えられるのが６カ国の戦略で重要性が指摘されるのが G20 である。G7 に言及した国が３カ国であったことを考えると、東西の主要国が集う G20 の交渉の場としての価値が広く認められていると考えられる。2017 年３月に開催された G20 財務大臣・中央銀行総裁会議の成果文書に「悪意ある情報通信技術の利用は、各国のそして世界の金融システム停止を引き起こす可能性があり、安全性と信頼を危険にさらし、金融の安定を脅かす」とあることからも、G20 の枠組みの中で継続して議論が行われている。

(4) 多様な重要インフラの定義

重要インフラの保護の重要性については疑問の余地がないものの、保護する対象となる産業分野に国ごとの考え方の違いが現れる。例えば日本は「情報通信、金融、航空、鉄道、電力、ガス、政府・行政サービス（地方公共団体を含む）、医療、水道、物流、化学、クレジット及び石油の 13 分野」を重要インフラとして定義している。多くの国で金融は重要インフラとして名前が挙がるが、クレジットを重要インフラとして指定しているのは日本だけである[35]。それに対して中国における重要インフラの定義[36]は「公共通信、テレビ放送の伝送等サービスのインフラ情報ネットワーク、エネルギー、金融、交通、教育、科学研究、水利、工業製造、医療衛生、社会保障、公共事業等の国家機関の重要情報システム、重要なインターネットアプリケーションシステム等（これらを含み、これらに限らない）」である。「水利」が重要インフラに含まれるのは、治水が伝統的な政治課題であった中国らしいといえる。ドイツは食糧産業を重要インフラに含めているという特色がある。食糧、クレジット、治水などを重要インフラと定義する背景にはそれぞれの産業分野が各国固有の事情からサイバーセキュリティ対策の重要性が特に高いことを伺わせる。

重要インフラ保護政策の課題の１つとしてセキュリティ問題が発生した際の生活への影響が大きいクラウドホスティングサービス、電子メールサービス、チャットサービス、ニ

ュースなどを提供する規模が小さい、歴史が浅い IT 企業が重要インフラに指定されていない点が挙げられる。本調査で英国と中国の戦略からこの課題解決への努力がみられる。英国のサイバーセキュリティ戦略では、政府が直接関与し、重要ネットワーク企業（Critical Network Infrastructure）を重点的に防衛するとした。CNI の例として「大量の個人情報を保有する企業、メディアなど攻撃者に狙われやすい企業、オンライン小売企業など」があるという。中国も重要インフラに重要なインターネットアプリケーションシステムを含めた。検索サービスを提供する百度（バイドゥ）、オンラインマーケットサービスを提供するアリババ・グループなどの企業が保護の対象となる可能性がある。公的機関、重厚長大産業の保護を優先してきた重要インフラ保護政策が、個人情報保護や国民生活への影響度を元に再考されていく潮流が各国のサイバーセキュリティ戦略から読み取れた。

(5) マーケット・アプローチへの期待と失望

サイバーセキュリティ戦略に民間事業者の役割に関する記述は多くなかったが、官民連携（Public-Private Partnership）については、基本的な価値観や安全保障上の課題を共有する英国とオーストラリアのサイバーセキュリティ戦略が対照的な方針をとっていることが分かった。

オーストラリアは首相と民間企業トップとの年次会合実施などを通じて官民の連携を強化するだけでなく、民間主導サイバーセキュリティ成長センター（Industry-led Cyber Security Growth Centre、2015 年設立）に 3000 万豪ドル（約 27 億円）以上を出資し、国内サイバーセキュリティ産業の拡充を目指す。国内サイバーセキュリティ市場の活性化がオーストラリア全体の対策推進に寄与するというマーケット・アプローチの考え方をとっている。

英国は過去のサイバーセキュリティ戦略でマーケット・アプローチを重視していた。2016 年版の英国のサイバーセキュリティ戦略は 2011 年から 2015 年の５年間に８億 6000 万ポンド（約 1259 億円）を投じた過去のサイバーセキュリティ戦略の下での施策を振り返って、「英国のサイバーセキュリティ産業を活性化し、その結果として国全体のセキュリティ能力の向上をはかるマーケット・アプローチは充分な成果を出すことができなかった」と結論づける。その上で政府、特に情報機関がより直接的に関与する必要があることを強調する。

(6) 政策ツールとしての自由度の高さ

本稿を通じて各国のサイバーセキュリティ戦略は極めて自由度の高い政策ツールであることが確認された。共通するのはどの国のサイバーセキュリティ戦略も法律ではないため立法府における検討を経ていない。「自国が望むサイバー空間のありかたを国際社会に対して明らかにすることを目的とした宣言政策型[37]」の記述が含まれることは全てのサイバーセキュリティ戦略に共通して見られたが、それ以外の共通項を見出すことはできなかっ

た。

まず戦略を策定した省庁、あるいは公布を行っている省庁が多様である。大まかには以下の３つのパターンに分けて考えることができる。第一に、ホワイトハウス（米国）、首相府（オーストラリア）のように国家元首を直接に補佐する組織が主となるパターンである。第二に、国家サイバーセキュリティセンター（英国）、内閣サイバーセキュリティセンター（日本）のようにサイバーセキュリティに関する各省間の政策の集約を担う組織が主となって策定、公布するパターンである。第三に、外務省（ロシア）、連邦情報技術安全局（ドイツ）などのような個別の省庁が公布するパターンである。背景にはサイバーセキュリティが、外交・防衛・警察・司法・通信・経済・科学技術政策などに幅広く影響を及ぼす分野であると考えられる。

サイバーセキュリティ戦略の政府文書体系における位置づけも異なる。フランス、英国のサイバーセキュリティ戦略はそれぞれフランスが「防衛と国家安全保障白書(38)」、英国が「英国家安全保障戦略（2015）」をサイバーセキュリティ戦略の上位文書として位置付けている。他方でドイツ、ロシアなどのサイバーセキュリティ戦略は位置付けを示唆する記述がなく、文書の政府内における重要性が不明瞭である。さらに中国の『サイバー空間国際合作戦略』、日本の『サイバーセキュリティ国際連携取組方針』のようにサイバーセキュリティ戦略全体における国際戦略に限定したいわばサイバーセキュリティ政策の下位文書も存在する。真の戦略把握の観点からはサイバーセキュリティ戦略という名前の単一の文書にとらわれず、安全保障戦略、防衛白書、国際連携の指針そして関連法規までを視野に入れた「サイバーセキュリティ戦略文書群」として分析することが必要である。

本節でこれまで述べてきたサイバーセキュリティ戦略の自由度の高さは、同時にそこに記述された政策が実際に履行されるかという点について予測することを困難にさせる。多くのサイバーセキュリティ戦略は戦略自体の有効期限が決められておらず、個別の政策についていつまでにそれを達成するかのタイムラインが示されない。予算措置まで記述されることは稀である(39)。他方で、サイバーセキュリティ戦略は各国の政府が目指す姿が、制約を無視して、表現できるツールとして重要なものともいえる。

３．サイバーセキュリティ戦略の四類型

８カ国のサイバーセキュリティ戦略の調査から質的な差異を踏まえた上で、想定される文書の読者に着目すると、４つの類型に分けられることが分かった。

(1) 政府内における組織の役割を明確化するための「政府内調整型」

本来国内外に向けてサイバーセキュリティ政策を打ち出すことがサイバーセキュリティ戦略の本来の役割であるところ、政府内での役割分担に言及するものがこれにあたる。外

務省における取り組み、外務省の国際交渉の指針を細かく記述したロシアのサイバーセキュリティ戦略が代表的なものとして挙げられる。

各政府機関に分散したサイバーセキュリティ対応能力をサイバーセキュリティセンターに集約・統合することを打ち出したオーストラリアのサイバーセキュリティ戦略、2020 年の東京オリンピック・パラリンピック競技大会に向けオリンピック・パラリンピック CSIRT（Computer Security Incident Response Team）を政府内に新設することを打ち出した日本のサイバーセキュリティ戦略、有事の際には内務省長官が率いる危機管理対応チームに報告を行う国家サイバーレスポンスセンターを連邦情報技術局の下に設置し、情報の集約と分析をはかるとしたドイツのサイバーセキュリティ戦略も同様に「政府内調整型」の代表例である。

政府内での各組織の役割が不明確な部分を、対外的にサイバーセキュリティ戦略の形で公開することにより誘導していく狙いがある。

⑵ 自国内における官民の役割の明確化などを目的とした「国内政治型」

自国内の民間企業、学術研究機関、地方政府などの役割分担に言及するものがこれにあたる。大学含む高等教育機関や、民間業界団体によるサイバーセキュリティ情報共有の強化を打ち出したフランスのサイバーセキュリティ戦略が代表的なものとして挙げられる。

国内の様々な利害関係者に対して指針を示し、重点課題への協力を求める狙いがあると考えられる。サイバー空間を構成する要素の多くは民間事業者が所有あるいは管理していることから、そのセキュリティ対策についても民間に役割と責任を与えるという考え方は論理的である。既存分野の安全保障戦略との対比において、政府以外の役割が重要なサイバー空間の特徴がサイバーセキュリティ戦略に現れているともいえる。

⑶ 自国が望むサイバー空間のありかたを国際社会に対して明らかにすることを目的とした「宣言政策型」

自国のサイバー空間に対しての基本的な原則を主として国外に向けて示すことを目的とする。今回分析対象とした全ての戦略に宣言政策型の記述がある。特にロシアのサイバーセキュリティ戦略は全体として「国内政治型」の記述がほとんどない、最も典型的な「宣言政策型」といえる。

サイバーセキュリティ戦略の多くが「宣言政策型」の記述を多く含む理由の１つとしては、サイバー空間に明示的な管理者が存在せず、自国の立場を直接的に訴える相手がいないことが挙げられる。国家は自国の利益を最大化するサイバー空間のあり方について国内外に理解を促していくことが必要なのであろう。

「宣言政策型」戦略はサイバー空間における信頼醸成の観点からも重要である。信頼醸成とは透明性を相互に確保し、危機発生時の過激化（エスカレーション）を防ぐための手段である。キューバミサイル危機に際して、当時のソ連と米国の指導者を結ぶホットライ

ンが設置されたことなどが信頼醸成措置の例として挙げられる。この分野の議論をリードする欧州安全保障協力機構は 2013 年に『欧州安全保障協力機構 1106 号　サイバー空間における信頼醸成のための初期セット(40)』を全会一致で決定した。この決定の中ではサイバー空間やサイバー戦争に関する各国のスタンスを公開し、相互理解をすすめることが求められている。このような地域安全保障機構からの要求を受け、今後も多くのサイバーセキュリティ戦略が「宣言政策型」となることが予想される。

(4) 報復サイバー攻撃の存在を明らかにする「懲罰抑止型」

「宣言政策型」の派生として「懲罰抑止型」を４つ目の類型として指摘したい。他国からのサイバー攻撃の増加を背景に、攻撃的サイバー能力の強化や先制攻撃を受けた際の報復措置について記述するサイバーセキュリティ戦略である。「攻撃的サイバー能力について世界のリーダーの地位を目指す」という英国や「抑止のためにサイバー攻撃能力を使用する」とするオーストラリアのサイバーセキュリティ戦略がこれにあたる。サイバーセキュリティ戦略において明確にサイバー攻撃能力を保持することを認め、それを使用する可能性に言及したのは英国のサイバーセキュリティ戦略が初めてである(41)。

「抑止とは恐怖を通じて相手を思いとどまらせること(42)」だとすれば、今後サイバーセキュリティ戦略にはさらなる抑止効果を得るためにより強いメッセージが並ぶ可能性がある。英国と、それに続いたオーストラリアのサイバーセキュリティ戦略が他国にどのような影響をもたらすのかは継続的な検証を要する。

本稿で見てきたサイバーセキュリティ戦略はその多くが、上記４類型の複数の型にあてはまるものであった。各サイバーセキュリティ戦略について、記述に占める「政府内調整型」「国内政治型」「宣言政策型」「懲罰抑止型」それぞれの割合を調査することによって、その性質を定量的に評価することが可能である。

４．考察

サイバーセキュリティ戦略はなぜ策定されるのか。それによって各国政府はどのような課題を解決しようと試みているのであろうか。

本稿では戦略の読者という視点からそれらが４つに分類されることを示した。つまり、政府内を意識した「政府内調整型」、政府と民間を合わせた国内関係者を意識した「国内政治型」、一国を超えて国際社会を意識した「宣言政策型」、そして、潜在敵国を意識した「懲罰抑止型」である。それらは対象範囲に広さという点では、政府内調整型＜国内政治型＜懲罰抑止型＜宣言政策型、ともいえるだろう。

しかし、同じ「サイバーセキュリティ戦略」あるいは同様の表現で提示される文書にお

いて、想定されている読者が違うということは何を意味するのだろうか。国際条約に基づいた各国における国内措置のための法整備などとは違い、サイバーセキュリティ戦略では必ず盛り込むべき内容が固定されているわけではない。法律や条約ではないため、立法府の承認を得る必要性もない。サイバーセキュリティ戦略は、その名の下に国内外に対して自国政府の主張を比較的自由に表現できる手段になっている。

それぞれの読者層が示すのは、どこまで政府ないし国内において調整が済んでいるか、そして、被害の範囲・深刻度が関係しているといえるかもしれない。つまり、サイバーセキュリティをめぐる問題が深刻度を増しているにもかかわらず、政府内での意識統一ができていないため、それを促す手段としてサイバーセキュリティ戦略が使われる場合、それは政府内調整型にならざるを得ない。

政府内での調整がある程度済んでいるものの、国内における民間との調整が十分でない場合には、それを促す国内調整型になる。重要インフラの多くは民間事業者が保有するものである。本稿で取り上げた多くの国は民主主義体制をとっており、そうした国では平時から軍が直接的に民間事業者を防衛するという体制を取りにくい。そのため、いかにして民間の意識を高め、設備やシステムの防衛のためにコストを負担させるかという点が政策課題になる。利益追求を求められる企業にとって、サイバーセキュリティはコストとしてしか認識されない。そうではなく、より大きな被害を防止するための投資だと認識させることが重要になる。そうした認識変化を促すためにサイバーセキュリティ戦略が使われることもある。

また、すでに多くのサイバー犯罪、サイバーエスピオナージ（スパイ活動）、サイバー攻撃の被害に遭っている国は、その抑制・抑止が政策上、重要な課題になっている。具体的な攻撃者ないし攻撃国が見えている場合には、そうしたアクターに対しどのような対応を取るかを明確にするために懲罰抑止型が用いられることになるだろう。

しかし、そうした具体的な被害が多くないものの、潜在的なそれが予期されており、それに備えることを目的としてサイバーセキュリティ戦略が使われる場合には宣言政策型になるだろう。

このように、その国のサイバーセキュリティ戦略がどの型になっているかを分析することで、その国のサイバーセキュリティの状況、そして課題が見えてくることになる。しかし、それは当然ながら、その国が置かれている状況が変われば、サイバーセキュリティ戦略の内容が変わるということを意味する。

サイバーセキュリティ戦略が頻繁に更新されている国は多くないが、例えば、日本を見てみれば、2010年に「国民を守る情報セキュリティ戦略[43]」が作成され、2013年に最初のサイバーセキュリティ戦略[44]が作成され、2015 年に新しいサイバーセキュリティ戦略が作成されている。それらの変化は、2012年に政権が民主党から自民党主導の連立内閣に変わったこと、2014年にサイバーセキュリティ基本法が成立したことが関係している。政府与党の変化や基本法の成立はサイバーセキュリティに関する認識変化を促し、それが新

たな戦略の策定につながったと考えることができるだろう。

おわりに

各国政府はサイバーセキュリティ戦略を作成・公表するという手段を通じて、国内外の利害調整や国際社会に向けた意見表明を行っていることが明らかになった。加えて、昨今、サイバーセキュリティ戦略がサイバー攻撃を抑止するためのメッセージを発する手段として使われるケースが見られるようになってきた。

自由度の高さ故にサイバーセキュリティ戦略には各国の利益追求のための意思が直接的に記述される。しかしサイバーセキュリティ戦略には国家の取り組みがもれなく記述されるわけではない。例えばアトリビューション問題(45)はグローバル・ガバナンスの観点から重要な研究課題であり、多くの国にとっては根本的政策課題であるが、これを解決する具体案を示すサイバーセキュリティ戦略はなかった。このような各国の恣意的な取捨選択が行われている点を踏まえることが、サイバーセキュリティ戦略通じて政策への理解を深める際に不可欠である。そして各国の政策を調査する際の資料としての有用性は今後も変わることはないと考えられる。

本稿は分析の対象を８カ国に限定した。今後、国際的な議論の場で繰り返されてきた先進国と発展途上国の意見の相違の源を探るという観点からは、ASEAN 諸国や中東およびアフリカ地域のサイバーセキュリティ戦略を含め研究対象の拡大が求められると考える。

サイバー空間は国益追求する国同士のエゴがぶつかる場に変容しつつある。本稿では政府の関与が疑われるサイバー攻撃の増加、軍隊におけるサイバー攻撃能力の強化、そしてサイバーセキュリティ戦略が国家安全保障戦略に内包されつつある状況を描いてきた。サイバー空間の緊張はかつて無いほどに高まっているのである。

《注》

(1)World Economic Forum, *The Global Risks Report 2017 12th Edition* (Geneva: World Economic Forum, 2017).

(2)従来インターネットに接続されるのはパソコンやスマートフォンといった情報機器に限定されていたのに対し、例えば冷蔵庫や炊飯器などの生活家電や車などあらゆる「モノ」が接続されインターネットを構成している現状を Internet of Things（IoT またはモノのインターネットなどとも）と表現する。

(3)ベン・ブキャナン（Ben Buchanan）は攻撃と防御の境界が明確にできないサイバー空間においては、国家は「防御志向の侵入行為（defensive-minded intrusion）」あるいは「積極的防御（active defense）」などの攻撃活動を行う強いインセンティブをもつことを論じた。Ben Buchanan, *The*

Cybersecurity Dilemma: Network Intrusions, Trust and Fear in the International System (C Hurst & Co Publishers Ltd, 2017).

(4)リザ・アズミ（Riza Azmi）らにおけるサイバーセキュリティ戦略の定義、すなわち「a careful plan or method of protection both informational and non-informational assets through the ICT infrastructure for achieving a particular national goals usually over a long period of time 」を参考にした。Riza Azmi, William Tibben, and Khin Than Win, "Motives behind Cyber Security Strategy Development: A Literature Review of National Cyber Security Strategy," Australasian Conference on Information Systems, 2016, Wollongong, https://www.researchgate.net/publication/308470260_Motives_behind_Cyber_Security_Strategy_Development_A_Literature_Review_of_National_Cyber_Security_Strategy. （2017 年 9 月 14 日確認）

(5)須田祐子「サイバーセキュリティの国際政治ーサイバー空間の安全をめぐる対立と協調ー」『国際政治』第 179 号、2015 年、57-68 頁。

(6)Council of Europe, "Chart of signatures and ratifications of Treaty 185, Convention on Cybercrime," http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures （2017 年 9 月 14 日確認）

(7)NATO CCDCOE, "Cyber Security Strategy Documents," https://ccdcoe.org/cyber-security-strategy-documents.html（2017 年 9 月 14 日確認）ENISA, "National Cyber Security Strategies (NCSSs) Map," https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map （2017 年 9 月 14 日確認）

(8)NATO CCDCOE, "National Cyber Security Framework Manual," http://www.ccdcoe.org/369.html （2017 年 9 月 14 日確認）

(9)Azmi, Tibben, and Win, op.cit.

(10)Kyoung-Sik Min, Seung-Woan Chai and Mijeong Han, "An International Comparative Study on Cyber Security Strategy," International Journal of Security and Its Applications, vol. 9, no. 2, 2015, pp. 13-20, http://dx.doi.org/10.14257/ijsia.2015.9.2.02.

(11)Eric Luiijf, Kim Besseling, and Patrick De Graaf, "Nineteen National Cyber Security Strategies," International Journal of Critical Infrastructures, vol. 9, nos. 1/2, 2013, pp. 3-31, https://www.researchgate.net/profile/Eric_Luiijf/publication/261950643_Nineteen_National_Cyber_Security_Strategies/links/543545380cf2bf1f1f286509.pdf.

(12)Government of United States, "Cyberspace Policy Review," https://www.dhs.gov/sites/default/files/publications/Cyberspace_Policy_Review_final_0.pdf （2017 年 9 月 14 日確認）

(13)The White House, "International Strategy for Cyberspace - Prosperity, Security, and Openness in a Networked World-," https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf （2017 年 9 月 14 日確認）

(14)The White House, "Executive Order-Improving Critical Infrastructure Cybersecurity," https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity （2017 年 9 月 14 日確認）

(15)The Department of Defense, "The Department of Defense Cyber Strategy," https://www.defense.gov/Portals/1/features/2015/0415_cyber- strategy/Final _2015_DoD _CYBER_STRATEGY_for_web.pdf （2017 年 9 月 14 日確認）

(16)Government of United Kingdom, "National Cyber Security Strategy 2016-2021,"

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf （2017年9月14日確認）
(17)Government of United Kingdom, “The UK Cyber Security Strategy Protecting and promoting the UK in a digital world,” https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/UK_NCSS.pdf （2017年9月14日確認）
(18)Government of Russia, “Basic Principle for State Policy of the Russian Federation in the Field of International Information Security to 2020,” https://ccdcoe.org/sites/default/files/strategy/RU_state-policy.pdf (2017年9月14日確認。なお英訳作成者は不明)
(19)National Cybersecurity Agency of France, “French National Digital Security Strategy,” http://www.ssi.gouv.fr/uploads/2015/10/strategie_nationale_securite_numerique_en.pdf （2017年9月14日確認）
(20)国家互聯網信息弁公室『国家網絡空間安全戦略』http://www.cac.gov.cn/2016-12/27/c_1120195926.htm （2017年9月14日確認）
(21)中華人民共和国政府『網絡空間国際合作戦略』http://news.xinhuanet.com/2017-03/01/c_1120552767.htm （2017年9月14日確認）
(22)内閣サイバーセキュリティセンター『サイバーセキュリティ戦略』http://www.nisc.go.jp/active/kihon/pdf/cs-senryaku.pdf （2017年9月14日確認）
(23)内閣サイバーセキュリティセンター『サイバーセキュリティ国際連携取組方針 ～j-initiative for Cybersecurity～』 https://www.nisc.go.jp/active/kihon/pdf/InternationalStrategyonCybersecurityCooperation_j.p（2017年9月14日確認）
(24)サイバーセキュリティ戦略本部『重要インフラの情報セキュリティ対策に係る第4次行動計画』https://www.nisc.go.jp/active/infra/pdf/infra_rt4.pdf （2017年9月14日確認）
(25)The German Federal Office for Information Security, “Cyber Security Strategy for Germany,” https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/strategies/cyber-security-strategy-for-germany/view/++widget++form.widgets.file/@@download/DE_NCSS.pdf（2017年9月14日確認）
(26)Australian Government, “Australia's Cyber Security Strategy: Enabling Innovation, Growth & Prosperity,” https://cybersecuritystrategy.dpmc.gov.au/assets/img/PMC-Cyber-Strategy.pdf （2017 年9月14日確認）
(27)佐々木孝博「ロシアのサイバー戦略―『サイバー戦コンセプト』を中心に―」『日本大学大学院総合社会情報研究科紀要』第13号、2012年、1～12頁。佐々木孝博「サイバー空間の施策に関するロシアと欧米諸国のアプローチ」『日本大学大学院総合社会情報研究科紀要』第14号、2013年、1～12頁。
(28)各国のサイバーセキュリティ戦略にサイバー攻撃能力について言及されるケースが増えてきたが、例えば中国、ロシアについてはサイバー攻撃能力についてサイバーセキュリティ戦略の中で触れることを避けている。ロシアについては佐々木の前掲論文が、そして中国については以下の報告書に詳しい。横山恭三「中国のサイバー能力の現状」 http://www.drc-jpn.org/annual_report/yokoyama_report_20170308.pdf (2017年9月14日アクセス)
(29)例えば2007年4月にエストニア政府が同国を解放した旧ソ連軍兵士の像を首都タリン市郊外に移設しようとしたことをきっかけとして、エストニアのコンピューター・ネットワーク及び銀行などの重要インフラに対し、サイバー攻撃が行われた。2週間以上に渡って断続的に銀行や電子政府サ

ービスが利用できないという自体が発生した。この事件は多くの耳目を集め、その経緯からエストニア政府は攻撃をロシアによるものと非難したが、現在に至るまでロシア政府が関与したという確かな証拠は確認されていない。

(30)アダム・シーガル（Adam Segal）は、2012 年 6 月から 2013 年 6 月がサイバー空間をめぐる戦いの「イヤー・ゼロ（Year Zero）」だとしている。ジェイソン・ヒーリー（Jason Healey）はサイバー空間の歴史を Realization 期（1990 年~1997 年）、Takeoff 期（1998 年~2002 年）そして Militarization 期（2002 年~現在）という 3 つに分類し、サイバー空間の軍事化は 2002 年から本格化しているとしている。本稿ではサイバーセキュリティ戦略の記述に依って 2010 年という立場を取るが、それ以前からサイバー空間での軍事作戦の準備が進められてきたという見解を否定するものではない。Adam Segal, *The Hacked World Order: How Nations Fight, Trade Maneuver, and Manipulate in the Digital Age (Second Edition)* (New York: PublicAffairs, 2017). Jason Healey, *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012* (Arlington: Cyber Conflict Studies Association, 2013).

(31)Kim Zetter, *Countdown to Zero Day: STUXNET and the Launch of the World's First Digital Weapon* (New York: Crown Publishers, 2014).

(32)サイバーセキュリティの専門家の間では「サイバーGGE」あるいは単に「政府専門家会合」と呼ばれているが、正式な名称は「国際安全保障の文脈における情報とテレコミュニケーションの開発（Developments in the Field of Information and Telecommunications in the Context of International Security）に関する国連政府専門家会合」である。国家のサイバー空間における攻撃を規制するために、国連憲章を含む既存の国際法がサイバー空間に適用されるのか否か、新しいルールや国際法を打ち立てるべきかなどについて議論が行われてきた。2004 年から本稿執筆時点までで 5 回招集されている。直近の 2016-2017 年会合は日本を含む 25 カ国が参加し、既存国際法がいかにサイバー空間に適用されるかについて意見が対立し、合意文書を残すこと無く解散した。

(33)情報セキュリティに関する国際行動規範は 2011 年に中国、ロシア、タジキスタン、ウズベキスタンの 4 カ国によって共同提案されたが、事務総長はこの提案を総会の議案に追加しなかった。その後 2015 年には前述 4 カ国にキルギスタンとカザフスタンが加わり 6 カ国の共同提案という形で再度提案されたが、またしても不調に終わった。2011 年提案では情報通信技術、ネットワーク技術を「敵対的行為や侵略行為」あるいは「国際平和と安全保障の妨げとなる行為、情報兵器や関連技術の拡散」を目的として利用することを禁ずるという提案である。

(34)インターネットにおける重要な資源（IP アドレスやドメイン名）については IANA（Internet Assigned Numbers Authority）という組織が管理を担っている。この IANA 機能を監督する権限は歴史的な経緯から米国商務省が持っていた。2016 年からこの IANA 機能の監督権限はマルチステークホルダーコミュニティに移管されている。米国政府の直接的影響力は弱まる。

(35)日本以外の国ではクレジットにおける金融取引は金融分野に含まれているが、日本では経済産業省の所轄とされているので、クレジットが別立てになっている。

(36)中国における重要インフラ保護の対象となる産業分野については前掲の『国家網絡空間安全戦略』に加えて 2016 年に成立した『網絡安全法（いわゆるサイバーセキュリティ法）』内の記述を参考にしている。

(37)詳しくは第 3 節を参照。

(38)Government of France, "2013 French White Paper on Defence and National Security," (2013 年) http://www.defense.gouv.fr/english/content/download/206186/2393586/file/White%20paper%20

on%20defense%20%202013.pdf（2017年9月14日確認）

(39)オーストラリアと英国のサイバーセキュリティ戦略においては一部、記述された政策の実施に必要な予算の確保を約束している。

(40)OSCE, “Decision No.1106 Initial Set of OSCE Confidence-Building Measures to Reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologies,” http://www.osce.org/pc/109168（2017年9月14日確認）

(41)例えば前掲米国のCyberspace Policy Review（2009）では能動的サイバー防御（Active Defense）能力の強化が謳われていた。第2節2項で示した通り、米国防総省のサイバーセキュリティ戦略もサイバー攻撃能力強化の必要性を訴えている。従ってサイバー攻撃能力の使用を仄めかすことは2016年より前にも存在した。しかし能動的サイバー防御とサイバー攻撃能力では周辺国に与える印象が大分異なり、「サイバー攻撃能力世界一を目指す」という直接的なメッセージの周囲への影響も加味して、ここは英国のサイバーセキュリティ戦略が初めての「懲罰抑止型」というスタンスを取る。

(42)ジョセフ・S・ナイ・ジュニア、ディヴィッド・A・ウェルチ（田中明彦／村田晃嗣訳）『国際紛争―理論と歴史［原書第9版］』（有斐閣、2013年）、174頁。

(43)情報セキュリティ政策会議『「国民を守る情報セキュリティ戦略」の概要』https://www.nisc.go.jp/active/kihon/pdf/senryaku_gaiyou.pdf　（2018年1月14日確認）

(44)情報セキュリティ政策会議『サイバーセキュリティ戦略 ～世界を率先する強靭で活力あるサイバー空間を目指して～』 https://www.nisc.go.jp/active/kihon/pdf/cyber-security-senryaku-set.pdf（2018年1月14日確認）

(45)誰がサイバー攻撃を行っているのかを特定するのが極めて困難であることを「アトリビューション問題」と呼ぶ。サイバーセキュリティの分野で単にアトリビューションという場合には攻撃の実行者を指すことが多い。

（小宮山　功一朗　慶応義塾大学大学院政策・メディア研究科 後期博士課程）
（土屋　大洋　慶応大学大学院政策・メディア研究科・教授）