サイバー攻撃に対する「抑止」の現状
―米国の安全保障政策の事例から―

国立国会図書館　調査及び立法考査局
外交防衛課　　栗田　真広

目　　次

【要　旨】
冷戦期の核戦略と結びついて発展してきた抑止、特に報復の威嚇によって相手に攻撃を思い止まらせる懲罰的抑止は、近年、米国においてサイバー攻撃対策の一つのアプローチとしての位置付けを得つつある。本稿では、かねてからサイバー攻撃に対しては「抑止が効かない」とする主張が指摘してきた、攻撃主体の多様性や攻撃の発信源特定の難しさ、サイバー兵器の秘匿性などの問題点に照らして、近年の米国のサイバー抑止政策を分析する。

はじめに

2014年10月、米サイバー軍（United States Cyber Command）を統括するマイケル・ロジャース（Michael Rogers）司令官は、大半のハッカーは現在、サイバー攻撃を仕掛けてもその代償を払わされることはほとんどないと考えているが、そうした状況はいずれ是正されなければならないこと、米軍はいかなる攻撃型のサイバー兵器をも用いる法的な枠組みを有していることに言及し、これはサイバー攻撃に対する抑止、すなわちサイバー抑止（Cyber Deterrence）に言及したものとして受け止められた(1)。

米国の戦略思考の中で、抑止（deterrence）というアプローチは、冷戦期の核戦略と分かちがたく結びつき、ゲーム理論や心理学を援用した極めて高度な抑止理論の体系へと発展してきた。しかし本来、抑止とは必ずしも核兵器の文脈に限定されるものではなく、「犯罪抑止」といった形でも用いられるし、国際政治学の議論に限定してみても、核兵器の登場以前は、通常兵器を用いた抑止が常々議論の対象となってきた。結局のところ、抑止を達成する手段が何であれ、特定の好ましくない事象や行動をそもそも生起させないというアプローチは、そうした事象や行動が発生してからこれに対処するよりも望ましいものとして考えられているのである。

こうした事情から、冷戦が終結して超大国間の核戦争の脅威が遠のくと、抑止理論はそれまで周縁的とみなされていた他の問題領域へと拡がりを見せたが、その中で重要な焦点の一つとなったのが、サイバーセキュリティの分野であった。核攻撃とサイバー攻撃の間に、程度は違えども社会を機能不全に陥らせるような広範かつ甚大な損害をもたらしうることや、攻撃側に優位があることなどの共通性があったことも、そうした援用を後押ししたものと思われる。その後今日に至るまで、米国の安全保障政策関係者の間では極めて活発な形で、サイバー抑止に関する議論が蓄積されている(2)。

本稿の目的は、そうしたサイバー抑止がいかなるものであるのか、そしてそれが米国の政策上いかなる形で取り入れられ、そうした施策がどのように評価できるのかを概観することにある。本稿は以下のとおりに議論を展開する。まず、第Ⅰ章において、議論の前提となる抑止の概念を整理するとともに、サイバー空間(3)に特有の性質が、抑止の成立にどう影響しているのかを論じる。次いで第Ⅱ章において、近年の米国のサイバー攻撃対策の中で、サイバー抑止に関する政策がどのように展開されてきたのかにつき、主要な政策文書や組織の設置から考察す

＊　本稿におけるインターネット情報の最終アクセス日は、2014年12月20日である。
(1)　“US Eyes Cyber ‘Deterrence’ to Stop Hackers,” *Securityweek*, October 28, 2014. <http://www.securityweek.com/us-eyes-cyber-deterrence-stop-hackers> 米サイバー軍の詳細については、第Ⅱ章で詳述する。また、肩書きは全てその当時のものである。
(2)　サイバー抑止の議論は一般に、必ずしもサイバー空間だけで完結するものではなく、例えばサイバー攻撃に対して物理的な報復を威嚇することによって抑止を行うことなども含んでいる。

る。その上で、第Ⅰ章、第Ⅱ章の議論を踏まえて、米国のサイバー抑止に関する政策の評価及び今後の課題について、米国内の専門家の議論を参照しながら考察する。

なお、本論に入る前に、いくつかの点について断っておきたい。第一に、抑止の概念には、大きく分けて、報復の威嚇に依拠する懲罰的抑止（deterrence by punishment）と、強固な防衛力などに依拠する拒否的抑止（deterrence by denial）があるが、本稿の焦点は基本的に前者である。両者は対置されることが多く、第Ⅱ章の米国のサイバー抑止政策を論じる上で、拒否的抑止に一部言及せざるを得ないため、後者にも必要に応じて触れているが、その詳細、特に拒否的抑止に必要なサイバー攻撃に対する防衛力を米国が具体的にどのように構築しているかについては、紙幅の都合もあり基本的に割愛した。

第二に、サイバー攻撃はその形態や実施主体が多様であることから、その対策を行う主体も、民間のセキュリティ企業から国内法執行機関、さらには国防・軍事組織まで多様であり、当然サイバー抑止を担いうる主体も幅広い。しかし、紙幅の都合上、本稿は基本的に、懲罰的抑止に関する議論が最も活発になされている、国防・軍事組織によるサイバー抑止政策を中心に議論を展開することとした。

第三に、第Ⅱ章では米国のサイバー抑止政策について考察を行うが、サイバーセキュリティ関係の政策の中でも、本稿の関心事項である懲罰的抑止に関わるサイバー攻撃能力等については、具体的な施策の内容がほとんど開示されていない。それゆえ、具体的な施策の有効性に関する評価については、専門家等の議論の中で触れられているものに言及するに留めている。

Ⅰ　サイバー抑止の理論的考察

1　抑止の概念整理

（1）懲罰的抑止の概要

米軍の作戦指針に関するJoint Publication 3-0: Joint Operationでは、抑止の概念を、「受け入れがたい対抗措置を取るという信頼性のある威嚇か、ある行動を取るコストが予期される利得を上回るとの考えによって、その行動を防止すること」として定義付けている(4)。また、国際政治学における抑止理論の代表的な研究者であるパトリック・モーガン（Patrick Morgan）カリフォルニア大学教授は、「ある主体が他の主体に対し、特定の行動を取った場合には深刻な損害を与えるとの威嚇を行うことによって、自身にとって望ましくない行動を取らせないこと」であると述べている(5)。そして、この場合の「行動」は、国際政治学では概ね軍事的な攻撃を指すものとして扱われてきた(6)。

---

(3)　サイバー空間の定義は、論者によっても異なるが、2010年に米軍の統合参謀本部副議長名義で軍内部に向けて発出された覚書では、「ネットワーク化されたシステムと関連する物理的なインフラを通じて、データを保管、修正及び交換するための、電子及び電磁スペクトル（electromagnetic spectrum）の使用によって特徴付けられる領域」としている。The Vice Chief of the Joint Chiefs of Staff, *Memorandum for the Chiefs of Military Services, Commanders of the Combatant Commands, and Directors of the Joint Staff Directorates: Joint Terminology for Cyberspace Operations*, 2010, p.7. <http://www.nsci-va.org/CyberReferenceLib/2010-11-joint%20Terminology%20for%20Cyberspace%20Operations.pdf>

(4)　Joint Chiefs of Staff, *Joint Publication 3-0: Joint Operation*, August 11, 2011, p.GL-9. <http://www.dtic.mil/doctrine/new_pubs/jp3_0.pdf>

(5)　Patrick M. Morgan, *Deterrence Now*, Cambridge: Cambridge University Press, 2003, p.1.

(6)　*ibid*., p.2.

厳密に言えば、こうした定義は、本来は二つある抑止の概念のうち一方のみに焦点を当てたものである。軍事攻撃を試みようとする相手国に対して、耐え難い損害を与えるとの報復の威嚇を発することでそれを未然に防止しようとするアプローチは、いわゆる懲罰的抑止と呼ばれる(7)。これとしばしば対置されるもう一つの抑止の形態が、報復の威嚇に拠らない、いわゆる拒否的抑止である。これは、何らかの利得を得るために行動を起こそうとする相手に対し、そうした行動による利得を与えないだけの能力を持つことによって、抑止を達成しようとするものである。軍事的な例で言えば、敵対国の軍隊がこちらの領土を占領するのを防ぐことができるような軍事力を保有することによって、そもそも敵対国の攻撃を未然に防ぐことが拒否的抑止に当たる。(8)

抑止の文脈で懲罰的抑止が想定されやすいのには、冒頭で述べたとおり、国際政治学における抑止論は核戦略に関する議論と密接に関連する形で発展してきており、核戦略の基本は戦略核戦力を用いた報復核攻撃の威嚇による抑止であったことがあるものと思われる(9)。加えて、拒否的抑止は、実際に発生した攻撃を排除する防衛（defense）と概念上は区別されるものの、必要となる能力は防衛と変わらないことから、両者の境界は曖昧になりがちである。こうした事情もあり、抑止と言えば懲罰的抑止が想起されやすい。以下本稿では、基本的には懲罰的抑止に焦点を当てた形で議論を進める。

（2）懲罰的抑止の成立要件

こうした懲罰的抑止が成立する上では、以下の三つの要件が満たされる必要がある(10)。第一に、抑止の対象となる攻撃が発生した場合に、それがどの国家や組織からのものであるのかを特定できることが必要になる。これは、帰属問題（attribution problem）と呼ばれるものであり、いざ攻撃が発生したとしても、その発信源を特定できないのであれば、抑止側は威嚇した報復を履行することができないことから、被抑止側、すなわち潜在的な攻撃者に対して、攻撃を思い止まらせる抑止は働かなくなる。第二に、伝達（signaling）の問題がある。抑止のためのメッセージとして、抑止側が何を思いとどまらせようとしているのか、仮に抑止側の警告を無視して攻撃に踏み切った場合にはどのような報復を招くことになるのかが、被抑止側に明確な形で伝達され、かつ理解されなければならない。第三に、信頼性（credibility）の問題がある。抑止が成立するか否かは、究極的には被抑止側の意思決定によって決まるから、いざ抑止が失敗した場合には、抑止側が威嚇する報復を履行する意思と能力を有することを被抑止側が信じなければ、抑止は成立し得ないことになる。

理論的には、これら三つの要件が満たされる場合に、被抑止側は、攻撃に踏み切ることによって得られる利得と、それによって抑止側が履行する報復攻撃で負わされるコストを比較衡量し、後者が上回る場合に、攻撃を思い止まることになる(11)。だが、ここにも一つ重要な前提条件

(7)　Robert Jervis, *The Illogic of American Nuclear Strategy*, Ithaca: Cornell University Press, 1984, p.75.
(8)　Glenn H. Snyder, “Deterence and Power,” *Journal of Conflict Resolution*, vol.4, no.2, June 1960, p.163.
(9)　ただし、厳密に言えば冷戦期の核抑止論の中でも、懲罰的抑止と拒否的抑止の間は明確に分かれていたわけではなく、両方の側面が重なり合う部分があった。Glenn H. Snyder, *Deterrence and Defense: Toward a Theory of National Security*, Princeton: Princeton University Press, 1961, p.15.
(10)　以下、懲罰的抑止の三つの要件については、特に注記がない限り、Clorinda Trujillo, “The Limits of Cyberspace Deterrence,” *Joint Force Quarterly*, Issue.75, 2014.10, p.45 を参照して記述した。
(11)　ただし、1970年代以降に主流となった、意思決定における認識の役割を重視する抑止理論では、これよりも要件が複雑化する。こうした議論をまとめたものとして、土山實男『安全保障の国際政治学―焦りと傲り第2版』有斐閣, 2014, pp.167-204.

が存在しており、それが合理性（rationality）の要件である[12]。すなわち、前述の比較衡量が合理的な計算に基づいて行われないのであれば、他の要件が満たされていようとも、抑止は成立しない。例えば、たとえ抑止側の報復によって負わされるコストが軍事攻撃に訴えることによって得られる利益よりも大きくても、それでも攻撃に踏み切ることを是とするような信念を攻撃側が抱いているとすれば、これは合理性の要件が満たされないがために抑止が成立しない場合となる。

2　サイバー空間の特徴と抑止の限界

社会の情報化が進み、またそれにつれてサイバー攻撃への懸念が高まる中で、こうした懲罰的抑止のアプローチをサイバー攻撃の抑止に応用していくことが議論されるようになった背景には、サイバー空間の攻撃優位性がある。すなわち、サイバー空間はその主要な特徴の一つとして、構造上、侵入（intrusion）や攻撃が極めて容易な空間であり、それらに対する防御が困難とされる面を持つ[13]。そうした性質の要因は複数あるが、根本的には、サイバー空間、とりわけインターネットがその設計上、情報の伝達・拡散を自由かつ容易にすることを目的としているために、リスクマネジメントや安全保障が優先されていないこと[14]、また攻撃側は、自身が付け込むと決めた防御側の脆弱性さえ理解すれば済むが、防御側は予想される膨大な攻撃に対して、ネットワーク全体を守り続けなければならないことがある[15]。

この防御の困難性は、同様に攻撃側に優位があった冷戦期の核抑止からの類推もあり、サイバー攻撃に対する懲罰的抑止に関する活発な議論へと繋がった。しかしながら、それらの議論の中では、核戦略と結びついて発展してきた従来の抑止論を、サイバー空間での抑止に適用することは困難であるとする見方が数多く提示されてきた[16]。これらは、サイバー空間に特有の性質が、先述した懲罰的抑止の成立要件のうちいくつかの側面に支障をきたす可能性が高いとするものである。そうした主張の中で主な論点として挙げられているのは、以下の点である。

（1）攻撃主体及び攻撃形態の多様性の問題

サイバー攻撃の最大の特徴は、攻撃の実施にかかるコストが、他の物理的な軍事攻撃などと比べて小さい点である。インターネットに繋がったコンピュータが1台あれば、電力や金融と

⑿　Snyder, *op.cit.*⑼, p.16.

⒀　Jarno Limnéll, “Offensive Cyber Capabilities Need to be Built and Exposed Because of Deterrence,” *Infosec Island*, October 9, 2012. <http://www.infosecisland.com/blogview/22534-Offensive-Cyber-Capabilities-Need-to-be-Built-and-Exposed-Because-of-Deterrence.html>

⒁　川口貴久「サイバー空間における安全保障の現状と課題―サイバー空間の抑止力と日米同盟―」日本国際問題研究所編『平成25年度外務省外交・安全保障調査研究事業（調査研究事業）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』2013.6, p.16. <http://www2.jiia.or.jp/pdf/resarch/H25_Global_Commons/03-kawaguchi.pdf> なお川口は、サイバー空間とインターネットの違いについて、インターネットは「個別のネットワークやシステム同士をつなぐネットワーク」であり、サイバー空間は「インターネットを含め、クローズド・ネットワークや周辺デバイスを含む」として区別している。同, p.25.

⒂　Lucas Kello, “The Meaning of the Cyber Revolution: Perils of Theory and Statecraft,” *International Security*, vol.38, no.2, fall 2013, p.28.

⒃　例えば、Patrick M. Morgan, “Applicability of Traditional Deterrence Concepts and Theory to the Cyber Realm,” *Proceedings of a Workshop on Deterring CyberAttacks: Informing Strategies and Developing Options for U.S. Policy*, National Academirs Press, 2010, pp.55-76; ウィリアム・リン「ペンタゴンの新サイバー戦略―なぜアメリカはサイバー軍を立ち上げたか」『Foreign Affairs Report』2010.10, pp.18-27.

いった社会の根幹を為すシステムを混乱させたり、インフラの一部を物理的に破壊したりといった攻撃を行うことも可能である上に、攻撃は世界のどこからでも、どこに対しても行うことができる。このコストの小ささゆえ、国家に限らず、組織や個人も含め、極めて多くの主体がサイバー攻撃を実行することが可能である。(17)

攻撃主体が多様であることは、必然的に攻撃の目的や攻撃に用いることのできる資源の寡多にも幅があることを意味し、またその結果として、一口にサイバー攻撃と言っても、形態は極めて多様である。ウェブサイトの改ざんや、あるホストの通信量を飽和させてインターネットから一時的に切断させるような比較的軽微なものから、秘密裡にネットワークに侵入して情報を操作又は窃取するもの、さらには物理的なシステムに壊滅的な損害を与えるものまである(18)。これらの攻撃では、当然ながら被害の程度も様々である。

このような攻撃主体及び攻撃形態の多様性は、主に三つの点で懲罰的抑止の成立を困難にする。第一に、極めて多様かつ膨大な数のサイバー攻撃が日々発生しており、かつその被害の程度も様々である以上、何を安全保障政策上の抑止の対象とするのかが問題となる。報復を威嚇する懲罰的抑止は、その履行にもコストがかかるために、全てのサイバー攻撃を抑止の対象とするのは現実的ではない(19)。しかしながら、深刻なサイバー攻撃のみに対してこれを試みようとしても、毎日膨大な数のサイバー攻撃が発生している中で、深刻なものとそうでないものを見分けるのは至難の業であり(20)、それらに適合した報復の威嚇を発出することは困難を極める。

第二に、攻撃主体の多様性は、従来の抑止論が依拠してきた、被抑止側の合理的意思決定という前提を危うくする面がある。抑止の対象となる潜在的な攻撃者が、サイバー攻撃を行った結果として、攻撃によって得られる利得を上回る報復を被ることを認識していながら、何らかの信念などによってそれでも攻撃に訴えるのであれば、抑止は機能しないことになる。例えば、過激なイデオロギーを有していたり、もしくは単純に技術的な好奇心から強固なサイバー防御措置を突破することそのものを目的としてサイバー攻撃を行ったりといった主体に対しては、基本的に抑止は機能しにくい(21)。これは、飽くまで相対的にではあるものの、合理的な意思決定が期待できる国家が抑止対象である場合とは異なる。

---

⑰　Michael J. Philbin, “Cyber Deterrence: An Old Concept in a New Domain,” *Strategy Research Project*, March 2013, pp.4-5. <http://public.carlisle.army.mil/sites/Landpower/Shared%20Documents/Philbin%20Michael%20SRPA.pdf>

⑱　Jonathan Solomon, “Cyberdeterrence between Nation-States: Plausible Strategy or a Pipe Dream?” *Strategic Studies Quarterly*, vol.5, no.1, spring 2011, p.11. <http://www.au.af.mil/au/ssq/2011/spring/solomon.pdf> なお、サイバー攻撃について厳密性を期すのであれば、ハーバート・リン（Herbert Lin）の定義が参考になる。これによれば、「攻撃的サイバー作戦（Offensive Cyber Operation）」の中に、「サイバー攻撃（Cyber Attack）」と「サイバー利用（Cyber Exploitation）」の二つがある。「サイバー攻撃」は、「敵対者のコンピュータ・システムやネットワーク、又はそれらの内部に存在するか通過するデータやプログラムを、改変、混乱、偽造、劣化、破壊することを目的として、情報技術及びその関連活動を故意に使用すること」を指す。他方、「サイバー利用」は、「目標や任務を達成するため、通常は敵対者のコンピュータ・システムやネットワークに存在するか通過する情報を獲得することを目的として、故意に情報技術関連活動を使用すること」である（Hebert Lin, “Escalation Dynamics and Conflict Termination in Cyberspace,” *Strategic Studies Quarterly*, vol.6, no.3, fall 2012, p.48.）。本来であれば、これらを明確に区別することが望ましいが、一般的にサイバー攻撃という語は、情報の窃取なども含めて、極めて広い意味で用いられている（土屋大洋「米国のサイバーセキュリティ政策―スノーデン事件のインパクト―」『海外事情』62巻3号, 2014.3, p.48.）。この点を踏まえ、本稿でも便宜上、「サイバー攻撃」と「サイバー利用」の両方について、サイバー攻撃と呼称することとした。

⑲　Emilio Iasiello, “Hacking Back: Not the Right Solution,” *Parameters*, vol.44, no.3, autumn 2014, p.107.

⑳　Emilio Iasiello, “Is Cyber Deterrence an Illusory Course of Action?” *Journal of Strategic Security*, vol.7, no.1, 2013, p.67. さらに言えば、重大かつ多段階にわたるサイバー攻撃は、その前段階として、攻撃対象についての情報を得るための情報の窃取などを伴う場合が多い。Kello, *op.cit.*⑮, p.21.

第三に、攻撃主体の多様性がもたらすもう一つの問題点として、懲罰的抑止の前提となる報復の対象が存在しない場合がある。冷戦期の核抑止の場合のように、特定の領域を持ち、そこに報復の対象となる「資産（asset）」を有している国家と異なり、世界中にネットワークを有する非国家組織などが抑止の対象である場合には、報復の対象の選定が極めて難しい(22)。もちろん、サイバー攻撃の発信源となっているコンピュータの機能を停止させるような反撃は可能であろうが、攻撃側は他のコンピュータに攻撃元を切り替えれば良いだけであり、報復措置としての意義はおろか、進行中の攻撃を停止させる上での有効性についても疑問が呈されている(23)。

（2）帰属問題

攻撃主体の多様性と並んでサイバー攻撃の特徴として言及され、また部分的にはその多様性の帰結でもあるのが、攻撃の発信源特定の困難さ、すなわち帰属問題である。先述のとおり、懲罰的抑止が成立する上では、被抑止側に、攻撃を行った場合には抑止側が攻撃元を特定して報復を加えると確信させる必要がある。だが、物理的な攻撃、典型的には冷戦期の核弾頭を搭載したミサイルによる攻撃などとは異なり、攻撃の形態もどちらかと言えば諜報活動に近い「曖昧な」ものが多く、かつ乗っ取られた第三国のサーバーを経由することの多いサイバー攻撃の発信源の特定は、極めて難しい(24)。

サイバー攻撃の帰属問題は、インターネットの構造、アプリケーション及びプログラムの設計、国家と非国家主体の関係といった攻撃者の政治・社会的属性などに起因する複雑なものであるが、大きく分けて、技術的な帰属問題と社会・政治的な帰属問題に区分できるとされる(25)。前者の技術的な帰属問題の代表的なところでは、個別のコンピュータ端末に振られた識別番号であるIPアドレスの偽装や、近年顕在化しつつある、ウイルスによって乗っ取られたコンピュータの集合体を利用し、攻撃者の指示を複数の中継サーバー経由で受信して攻撃を行う、ボットネットと呼ばれる攻撃の手法などが、攻撃の発信源の特定を困難にする。仮に特定が可能であったとしても、数か月を要することもあるという(26)。

さらに、発信源が特定できた場合でも残る問題が、攻撃者の政治・社会的属性の特定である。すなわち、攻撃者となっている個人が単なる単独犯であるのか、それとも背後に特定の国家や組織が存在し、その指示や支援を受けて攻撃を行っているのかを断定するのは困難を極める。実際、ロシア政府の関与が疑われた2007年のエストニアや2008年のグルジアへのサイバー攻撃事例でも、攻撃を実施したとされるロシアの愛国主義的な組織と、ロシア政府の関係の証明にまでは至らなかった。サイバー攻撃の実施主体と国家の関係が立証できるとしても、通常兵器等の軍事力と比べて、サイバー攻撃に用いられる「兵器」の使用に対しては政治指導者の統制が効きにくいため、当該攻撃が政府の承認の下で行われたのかを判断しがたいという側面もある(27)。

---

(21) International Security Advisory Board, *Report on A Framework for International Cyber Stability*, July 2, 2014, pp.9-10. <http://www.state.gov/documents/organization/229235.pdf>; Charles L. Glaser, *Deterrence of Cyber Attacks and U.S. National Security*, June 1, 2011, p.3. <http://static.squarespace.com/static/53b2efd7e4b0018990a073c4/t/542044fee4b02b592c3ec599/1411400958491/2011-5_cyber_deterrence_and_security_glaser.pdf>

(22) Iasiello, *op.cit.*(20), p.65.

(23) *ibid*., p.66.

(24) リン　前掲注(16), p.20.

(25) 以下、帰属問題に関する記述は、特に注記がない限り、川口　前掲注(14), pp.14-16 に依拠した。

(26) リン　前掲注(16), p.20.

後述するように、米国などは帰属問題の解決に向けた取組を続けているが、その活用にもジレンマが存在する。すなわち、抑止を成立させるためには、そうしたより確実に攻撃の発信源を特定できる技術の存在をある程度開示し、被抑止側に認知させておくことが必要になるが、一方で技術の開示は、それらによって発信源を特定されないための手法を考案する上でのヒントを潜在的な攻撃者に与えることに他ならない[28]。

（3）伝達及び信頼性の問題

サイバー攻撃に対する懲罰的抑止において、抑止側もサイバー攻撃による報復の威嚇に依拠する場合には、サイバー兵器特有の問題点が障害になる。すなわち、サイバー兵器による攻撃を行う上では、分散型サービス拒否（Distributed Denial-of-Service: DDoS）攻撃のような例外を除いて[29]、標的となるコンピュータ・システムやネットワークに、攻撃側が付け込むことのできる脆弱性が存在していなければならないが、当然その所有者は随時脆弱性を発見してこれを塞いでいく。そのため、抑止側が特定の形態のサイバー攻撃による報復を想定していたとして、いざ抑止が失敗して威嚇を履行せざるを得なくなった時点で、予定していた形態のサイバー攻撃がまだ実行可能であるとは限らない。仮に有効なサイバー報復手段があるとしても、自身の保有するサイバー攻撃手段について喧伝すれば、潜在的な攻撃者に、その形態の報復攻撃を履行されないための防御手段を取るよう促すことになるばかりか、場合によっては新しいサイバー攻撃手法に関する示唆を与えてしまう。[30]

一方で、実験や演習などによってその威力を誇示することが可能であった通常兵器と異なり、サイバー攻撃能力は基本的には不可視であり、敵対的なシステムに対して実際にテストされていないことも多い[31]。こうした側面は全て、結果として抑止側の威嚇の信頼性に対して、潜在的な攻撃者が能力面で疑念を抱くことに繋がり得る。

もちろん、サイバー攻撃に対する報復手段は、何もサイバー攻撃しか取り得ないというわけではない。後述するとおり、米国は既に、サイバー攻撃に対して通常戦力による報復を行うこともあり得るとの考えを示している。しかしながら、そうした通常戦力などの物理的な手段による報復攻撃は、そもそも対国家以外の文脈では困難であるし、国家に対しても二つの点で履行に躊躇が生じる。第一に、いかなる形態のサイバー攻撃に対して、どのような反撃が許容されるのかについて、国際的な規範は依然として形成過程にあり、いざ通常兵器での反撃を行った場合に、国際社会の理解を得られるかが定かではない。第二に、サイバー攻撃に対して通常兵器による報復攻撃に訴えることは、そこから通常戦争へのエスカレーションを招き、事態の収拾をより困難にする可能性が非常に高い。サイバー攻撃に対してサイバー報復攻撃で応じることの最大の利点は、被抑止側に対して、これが最初のサイバー攻撃に対する報復であることが明確に伝わると同時に、サイバー攻撃と物理的暴力の間の「敷居」を踏み越えないことで、それ以上のエスカレーションを回避するシグナルを送ることができる点である。[32]

---

(27) Solomon, *op.cit.*(18), p.10.
(28) *ibid*., p.9.
(29) Philbin, *op.cit.*(17), p.9. DDoS攻撃とは、「複数のネットワークに分散する大量のコンピュータが一斉に特定のサーバに対して通信し、通信路を溢れさせて機能を停止させてしまう攻撃」を指す。名和利男「サイバー空間における事象の変化と既存対策の限界」『海外事情』59巻6号, 2011.6, p.58.
(30) Solomon, *op.cit.*(18), p.18.
(31) Glaser, *op.cit.*(21), p.2.

これら二つの点からすれば、抑止側が報復の履行の際に躊躇する要因が多く存在する、物理的な手段による報復という威嚇が、被抑止側にとってどの程度信頼性を持つものとして受け止められるのかには疑問が残る[33]。

（4）攻撃の帰結の問題

サイバー攻撃に固有の特徴として、それが意図せずしてもたらし得る帰結の複雑性という問題にも目を向ける必要がある。

一つは付随的被害の問題である。サイバー空間の相互連結性ゆえに、サイバー攻撃に使用されたマルウェア（悪意のあるソフトウェア）などが、攻撃者が意図しなかったような形で拡散してしまうという事態がしばしば発生してきた。例えば、2010年に、イラン中部のナタンツにある核施設に対して、スタックスネット（Stuxnet）と呼ばれるマルウェアを用いたサイバー攻撃が発生し、米国とイスラエルによるものであると報じられた[34]。このマルウェアは、同核施設に設置されていた、独シーメンス社製の遠心分離機のみを標的として用いられたはずだったが、意図せずしてインターネット上に流出し、アゼルバイジャン、インドネシア、インド、パキスタン、さらには米国のコンピュータにまで感染した[35]。こうした付随的被害の予測不可能性は、報復としてのサイバー攻撃の利用を難しくする。

もう一つは、特に国家対国家の文脈において、サイバー攻撃の応酬に発展した場合のエスカレーション管理の困難さである。すなわち、サイバー空間では、物理的な空間での戦争と異なり、紛争の中で当事国が取る措置の烈度の段階、いわゆるエスカレーション・ラダーについて、主要国間で共有された認識が存在しない。それゆえ、いざサイバー攻撃が発生した場合に、抑止側がその攻撃に「比例する」ものとしてある形態のサイバー報復攻撃を行い、エスカレーションの抑制を望むというシグナルを送ったとしても、被抑止側はその攻撃を元の攻撃と比例しない、より烈度の高いものであると解釈し、さらに強力なサイバー攻撃による、報復への報復に訴えるリスクが大きい。こうした状況は、最初は低烈度のものとして発生したサイバー攻撃が、急速により深刻なサイバー攻撃の応酬、最終的には物理的な戦争へと発展する危険性をはらんでいる。[36]

これらの問題はいずれも、抑止側にとって、いざ抑止が失敗した場合の報復の威嚇の履行を躊躇させうるものであり、前項で述べた内容と併せて、サイバー攻撃に対する懲罰的抑止の信頼性に支障をきたす可能性がある。

---

32 *ibid*., pp.2-5.

33 ただし、通常戦争の一環、とりわけ従来型の近代戦争における電子戦の延長のような形で行われるサイバー攻撃に対する報復とそれによる抑止については、この限りではないものとされる。詳細は、*ibid*., pp.5-6を参照。

34 ニューヨーク・タイムズ紙の報道による。David E. Sanger, "Obama Order Sped Up Wave of CyberAttacks against Iran," *New York Times*, June 1, 2012.

35 「W32.Stuxnet」2013.7.11. シマンテックウェブサイト <http://www.symantec.com/ja/jp/security_response/writeup.jsp?docid=2010-071400-3123-99>

36 Kello, *op.cit.*(15), p.35.

Ⅱ　米国におけるサイバー抑止

1　ブッシュ政権までの動き

米国の安全保障政策政策の中で、サイバー攻撃に対する抑止、とりわけ懲罰的抑止の発想自体は、それほど新しいものではない。1998年には、中央情報局（Central Intelligence Agency: CIA）のジョージ・テネット（George Tenet）長官が、米国が他国のインフラを攻撃できるコンピュータ・プログラムを開発していることに言及した。この事実自体は目新しい情報ではなかったものの、そうしたプログラムの存在が公言されたのは初めてであり、これは米国に対するサイバー攻撃を試みようとする潜在的な敵対国への抑止のシグナルであると受け止められた(37)。

ただし、政策文書等の中でのサイバー抑止の位置付けは、2000年代に入ってもそれほど大きな発展を見たわけではなかった。2006年に、ジョージ・W・ブッシュ（George W. Bush）政権下で発表された「四年ごとの国防見直し（Quadrennial Defense Review: QDR）」では、米国の領土、国民、軍隊に対する攻撃と同様に、サイバー空間を通るものを含む重要インフラに対する攻撃に対しては、米国からの圧倒的な反撃を招くと潜在的な攻撃者に確信させられるだけの抑止態勢を維持する方針が示された(38)。しかし、この方針に基づき、何らかの軍事ドクトリン等が形成されたわけではない(39)。

2006年12月には、サイバー抑止に言及した二つの文書が発表されている。一つは、サイバー空間に限らず、幅広く米国の抑止政策に焦点を当てた、国防総省の「抑止作戦：統合作戦概念第二版（Deterrence Operations: Joint Operating Concept Version 2.0）」である。文書の性質上、サイバー抑止に関する言及は少なく、「サイバー空間での戦争のような情報作戦は、敵対国の意思決定者が、自国に有利な形で武力を行使できるとの自信を損なわせることができる」とした上で、ネットワーク防御能力などが、拒否的抑止のような形で、サイバー攻撃に対するものを含む総合的な抑止の向上に寄与することが指摘されるに留まっている(40)。

もう一つの文書は、統合参謀本部の「サイバー空間作戦のための国家軍事戦略（The National Military Strategy for Cyberspace Operations）」である。こちらは、米国がサイバー空間で軍事的・戦略的な優位を保つための包括的な戦略を提示するもので、具体的な目標の一つとして、サイバー空間において、敵対者による米国の国益に対する攻撃能力の確立や使用を抑止することを掲げ、政治的・経済的・軍事的なコストを負わせること、また米国が持つ能力を誇示することで抑止が達成できると述べている(41)。これは懲罰的抑止のアプローチに比較的明確な形で言及したものではあったが、この文書自体、当時は機密扱いとなっていた(42)。

2008年1月には、「包括的国家サイバー安全保障イニシアティブ（The Comprehensive National

---

(37)　John Christensen, “Bracing for Guerrilla Warfare in Cyberspace,” *CNN.com*, April 6, 1999. <http://cyber.law.harvard.edu/eon/ei/elabs/security/cyberterror.htm>

(38)　Department of Defense, *Quadrrenial Defense Review Report*, February 6, 2006, p.25. <http://www.defense.gov/qdr/report/Report20060203.pdf>

(39)　Trujillo, *op.cit.*(10), p.46.

(40)　Department of Defense, *Deterrence Operations: Joint Operating Concept Version 2.0*, December 2006, p.43. <http://www.dtic.mil/doctrine/concepts/joint_concepts/joc_deterrence.pdf>

(41)　Chairman of the Joint Chiefs of Staff, *The National Military Strategy for Cyberspace Operations（U）*, December 2006, p.13. <http://www.dod.mil/pubs/foi/joint_staff/jointStaff_jointOperations/07-F-2105doc1.pdf>

(42)　現在でも、一部公開されていない部分があり、全容が確認できるわけではない。

Cybersecurity Initiative: CNCI）」が策定された。この文書はサイバーセキュリティ向上のための12項目のイニシアティブから成っており、その1項目として、「揺るぎない抑止戦略及びプログラムを定義し発展させること」を掲げていた(43)。だが、この文書についても、体系的な政策を明示するところまでは至らなかったとの見方がなされている(44)。

2　オバマ政権下での動き

2009年5月にオバマ大統領が発出した、サイバーセキュリティに関する声明は、米国のサイバー政策全体にとって一つの転機となった。この声明は、デジタル・インフラを米国にとっての「戦略的国家資産（strategic national asset）」に指定し、それを防護することが国家安全保障上の優先事項であること、またその防護の手法の一つとして、抑止が含まれることに言及したものであった(45)。これを契機に、米国の国家戦略及び軍事戦略上の目標として、サイバー空間での抑止が組み込まれるようになり、サイバー空間内で、又はサイバー空間を通じて、敵対者を抑止するために、サイバー能力を用いる必要性が認識されるようになった(46)。

（1）政策文書

サイバーセキュリティに関して積極的な姿勢を取ったオバマ政権は、その後もサイバー攻撃に対する抑止について、政策文書の中で言及を重ねていった。例えば、デジタル・インフラを「戦略的国家資産」と位置付け、その保護のために抑止のアプローチを用いることを表明した前期の大統領声明の内容は、そのまま2010年の「国家安全保障戦略（National Security Strategy: NSS）」に受け継がれた(47)。また、2011年の「国家軍事戦略（National Military Strategy: NMS）」では、空中、宇宙及びサイバー空間における抑止を強化すること、そのために劣化した環境下でも戦闘が可能な能力を保有するとともに、システムや支援インフラへの攻撃の発信源を特定し、これを打倒する能力を向上させることを謳っている(48)。

こうした流れの中で、2011年中には、サイバー抑止の観点から重要な三つの文書が発表された。すなわち、「サイバー空間の国際戦略（International Strategy for Cyberspace）」、「サイバー空間における作戦のための国防総省戦略（Department of Defense Strategy for Operating in Cyberspace）（以下、「国防総省戦略」とする）」、「国防総省サイバー空間政策報告（Department of Defense Cyberspace Policy Report）」がそれである。

---

(43)　The White House, *The Comprehensive National Cybersecurity Initiative*. <http://www.whitehouse.gov/sites/default/files/cybersecurity.pdf>

(44)　川口　前掲注(14), pp.12-13. なお、この文書が公開されたのは、バラク・オバマ（Barack Obama）政権期の2010年3月のことである。

(45)　The White House, *Remarks by The President on Securing Our Nation's Cyber Infrastructur*e, May 29, 2009. <http://www.whitehouse.gov/the_press_office/Remarks-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure/>

(46)　Trujillo, *op.cit.*(10), p.44.

(47)　The White House, *The National Security Strategy*, May 2010, p.27. <http://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf>

(48)　Chairman of the Joint Chiefs of Staff, *The National Military Strategy of the United States of America 2011: Redefining America's Military Leadership*, February 8, 2011, p.8. <http://mercury.ethz.ch/serviceengine/Files/ISN/154942/ipublicationdocument_singledocument/4839f9fe-388c-47c2-a5bf-61cce5eb0aa8/en/US+National+Military+Strategy+2011.pdf>

（i）サイバー空間の国際戦略

米大統領名義で2011年5月に発表された、「サイバー空間の国際戦略」は、「サイバー空間の将来に関するビジョンを提示し、それを実現するために他国や人々と協同していく上での重要課題を提示する」[49]ことを主たる目的としており、比較的抽象度の高い文書である。冒頭では、米国が追求する目標として、国際的な商取引や国際安全保障、表現の自由、イノベーションに資するような、開放的で相互運用性があり、安全で信頼性の高い情報・通信インフラ構築を促進することが謳われている[50]。

サイバー抑止の観点から着目されるのは、「防衛：諫止と抑止（Defense: Dissuading and Deterring）」の節である[51]。ここではまず、サイバー空間での平和と安定を脅かすような行動を諫止及び抑止するために、警戒能力を有する国内・国際ネットワークの回復力（resilience）と多様で信頼性のある反応オプション（credible response options）を活用するとの意思を示した上で、「諫止」と「抑止」の二項に分けて議論を展開している。

「諫止」では、主に拒否的抑止に繋がるような防御的措置の強化が論じられている。すなわち、米国は引き続き、ネットワーク防衛と、攻撃に耐える能力と並んで攻撃を受けた後に損害から回復する能力の強化を追求するとした上で、国内での施策の面では、米政府横断的な取組や民間・個々の市民とのパートナーシップ、さらに官民を横断した健全な情報技術慣行の重要性や、リスクに関する情勢認識能力の向上と情報共有に関する取組などに触れている。海外での施策面では、技術的・軍事的な協力による国家間での総合的な情勢認識・事態対処能力の向上がなされてきたこと、今後も引き続き、そうした能力のグローバルな向上を目指すことが表明されている。

他方、「抑止」の項目では、より軍事的な、懲罰的抑止の側面に関する記述が為されている。本稿の関心から重要なのは、この項目において、米国がサイバー空間での特定の敵対的な行為に対しては、物理的な空間での脅威に対するものと同様の形で対処することを明言した点である。そして、固有の自衛権に言及した上で、サイバー空間での特定の敵対的な行為が、同盟国との相互防衛条約上の義務を発生させうること、また米国自身、同盟国、パートナー国及び米国の国益を守るためには、関連する国際法に沿った形で、必要なあらゆる手段を用いることを明言し、そうした手段として、外交、サイバー、軍事、経済を列挙した。この他、犯罪者や非国家主体によるサイバー攻撃や情報の窃取を抑止するために、全ての国家が国内的にこうした行為を取り締まる手続を整えるとともに、国際的な協力を推進することや、適正手続と法の支配が貫徹される必要性についても言及がなされている。

（ii）サイバー空間における作戦のための国防総省戦略

続いて発出されたのが、2011年7月発表の国防総省戦略である。サイバーセキュリティに関する国防総省の取組の方向性を示したこの文書には、ウィリアム・リン（William Lynn）国防副長官の発表時の説明から明らかであるように、懲罰的抑止に関する記述はほとんど見られない。リン副長官は記者会見で、「米国は深刻なサイバー攻撃に対しては、米国が選ぶ場所とタイミ

---

[49] The White House, *Fact Sheet: International Strategy for Cyberspace*, p.1. <http://www.whitehouse.gov/sites/default/files/rss_viewer/International_Strategy_Cyberspace_Factsheet.pdf>

[50] The White House, *International Strategy for Cyberspace*, May 2011, p.8. <http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf>

[51] *ibid*., pp.12-14.

ングで、武力紛争法（Law of Armed Conflict）に従って、均衡的かつ正当化される軍事的対応を取る権利を留保する」とはしつつも、そうした報復による抑止は米国の戦略の一部でしかなく、むしろ攻撃者がサイバー攻撃を行っても何ら利得を得られないような防御態勢を整えることで、そもそも攻撃を行う誘因を低減することに重点が置かれていると説明した(52)。これはすなわち、拒否的抑止を重視した戦略であることを意味する。

戦略には五つの柱があり、①サイバー空間の作戦領域化とそれに合わせた組織・訓練・装備の整備、②国防総省のネットワーク及びシステムを防護するための新防衛作戦概念の採用、③他省庁や民間部門との連携、④集団的サイバーセキュリティ強化のための同盟国や国際的パートナーとの関係強化、⑤人材開発及び技術革新への投資から成る。これらそれぞれの項目の中にも、懲罰的抑止はもちろんのこと、サイバー攻撃能力に関する記述もほぼ存在しない(53)。

ただし、第二の柱の中で採用された、「積極的サイバー防御（active cyber defense）」は、拒否的抑止・懲罰的抑止の両面から注目する必要がある。積極的サイバー防御は、「脅威及び脆弱性を発見し、検知し、分析し、緩和するための、シンクロナイズされたリアルタイムの能力」であり、「センサーやソフトウェア、インテリジェンスを用いてネットワークの速度で稼働し、悪意のある活動が国防総省のネットワークやシステムに影響を及ぼす前に、センサーやソフトウェア、インテリジェンスを用いてこれを探知し、停止させる」(54)。端的に言えばこれは、「サイバー攻撃を事前に検知し、リアルタイムに分析・検出し、ネットワークを防衛すること」(55)であるとされる。

リン国防副長官は積極的サイバー防御について、攻撃者に攻撃を行うことによる利得を与えないようにするものである(56)として、拒否的抑止の文脈で説明している。だが、懲罰的抑止の文脈から積極的サイバー防御の有効性を指摘する向きもある。こうした見方によれば、リアルタイムで侵入を検知できるのであれば、それは当然ながら攻撃者に対する報復が可能であることを意味することから、「積極的サイバー防御」は懲罰的抑止の文脈でのメッセージになるという(57)。

（iii）国防総省サイバー空間政策報告

国防総省はさらに、2011年11月、連邦議会に宛てて「国防総省サイバー空間政策報告」を提出した。これは、2011会計年度国防権限法の規定に基づき作成されたもので、議会が提示した13項目の質問事項に対して、国防総省が回答する形式となっている。これらの質問事項には、サイバー攻撃に対する懲罰的抑止に関連したものが多く含まれており、議会向けの報告書ではあるものの、潜在的な攻撃者に対して国防総省としてのメッセージを送る一種の宣言政策（declaratory policy）となっている点で注目に値する。

---

(52) Department of Defense, “Remarks on the Department of Defense Cyber Strategy,” July 14, 2011. <http://www.defense.gov//speeches/speech.aspx?speechid=1593>

(53) Department of Defense, *Department of Defense Strategy for Operating in Cyberspace*, July 2011, pp.5-12. <http://www.defense.gov/news/d20110714cyber.pdf> なお、「国防総省戦略」には、公開されているものより長い非公開部分があり、こちらの中では、攻撃能力について論じられているとする見方もある。Thomas M. Chen, *An Assessment of the Department of Defense Strategy for Operating in Cyberspace*, September 2013, pp.7, 29. <http://www.strategicstudiesinstitute.army.mil/pdffiles/PUB1170.pdf>

(54) Department of Defense, *ibid*.

(55) 川口　前掲注(14), p.18.

(56) Department of Defense, *op.cit.*(52)

(57) Chen, *op.cit.*(53), p.15.

サイバー抑止に直接関連するのは、主として13項目中最初の4項目であるが、この中で注目されるのは、サイバー空間での抑止の形態が、懲罰的抑止と拒否的抑止の両方の形態を取り得るとの見解を明示した点である[58]。まず、懲罰的抑止の面では、「サイバー空間の国際戦略」の記述に沿った形で、サイバー空間での敵対行為を他の空間でのそれと同様に扱い、必要なあらゆる手段を用いてこれに対処することが述べられている。サイバー攻撃に対する報復の形態として、サイバー攻撃と物理的な攻撃の両方があり得ることも明言された。なお、サイバー空間の性質上、本来であれば懲罰的抑止において必要な攻撃能力の誇示が困難であることを認めつつも、確かにそうした攻撃能力を国防総省としては保持しているとの主張がなされている。他方、拒否的抑止については、国防総省として行う防衛力や損害からの回復力の向上と並んで、国土安全保障省を中心とした他の政府機関や民間部門との連携の下で、重要インフラのセキュリティ確保をはじめとした各種の施策に取り組む意向を示した。

懲罰的抑止の観点からは、もう一つ重要な点として、攻撃の発信源を特定する能力の向上に向けた努力と、その成果を強調している点が挙げられよう。報告中では、攻撃の物理的な発信源を追跡する新手法と、行動を基にしたアルゴリズムによる攻撃者の属性評価という二つの手法の研究が進められていることに加えて、過去数年間に国防総省がサイバー・フォレンジック（cyber forensics）[59]の技術を大幅に向上させてきており、そうした技術を扱うことのできる人材の確保が現在進行中であることなどに言及がなされている。

（2）米サイバー軍の創設

オバマ政権下で行われた、サイバーセキュリティに関するもう一つの重要な政策として、2010年5月に行われた、米サイバー軍の創設がある。米サイバー軍は、懲罰的抑止の履行を主眼とした組織というわけではないが、攻撃的なものも含め、米軍のサイバー作戦を担う組織として設立されたことから、ここで取り上げておきたい。

米サイバー軍の設立は2009年6月に決定されたものである。それ以前の軍のサイバー防衛を担ってきた組織を統合し、戦略核戦力などを管轄する米戦略軍の隷下に、大将クラスの司令官が率いる副統合軍（sub-unified command）として、米サイバー軍が設立されることになった[60]。米サイバー軍司令官が、情報機関である国家安全保障局（National Security Agency: NSA）長官を兼ねていることに加えて、米サイバー軍の司令部とNSAの本部は同じ場所にあることから、両組織間の関係は極めて深い。米サイバー軍の指揮下には、各軍種のサイバー部隊である、陸軍サイバー部隊、海軍サイバー艦隊、第24空軍、海兵隊サイバー部隊が収められている。当初は1,000人規模で設立され、2010年10月から完全な運用を開始したが、2016年までに6,000人規模

⑸⑻　Department of Defense, *Department of Defense Cyberspace Policy Report: A Report to Congress Pursuant to the National Defense Authorization Act for Fiscal Year 2011, Section 934*, November 2011, pp.2-5. <http://www.defense.gov/home/features/2011/0411_cyberstrategy/docs/NDAA%20Section%20934%20Report_For%20webpage.pdf>

⑸⑼　サイバー・フォレンジックとは、「証拠の完全性、検出情報の正式報告、また、法廷における専門家としての証言などを含んだコンピュータによる証拠を特定・抽出・解釈・文書化する技術的捜査手段」を指す。渡辺弘美「サイバー攻撃に対する米国政府の取り組みとセキュリティ技術市場の動向」『ニューヨークだより』2004.12, pp.9-10. <http://www.jif.org/column/pdf2004/200412.pdf>

⑹⓪　リン　前掲注⑽, pp.22-23. 以下、米サイバー軍の概要については、特に注記がない限り、同論文及び*Statement of General Keith B. Alexander, Commander United States Cyber Command, before the House Committee on Armed Services*, September 23, 2010, pp.1-3. <http://www.defense.gov/home/features/2010/0410_cybersec/docs/USCC%20Command%20Posture%20Statement_HASC_22SEP10_FINAL%20_OMB%20Approved_.pdf> を参照して記述した。

に増員される[61]。

米サイバー軍の任務について、2010年の国防総省の発表は、①国防総省の情報ネットワークの作戦及び防衛の指揮と、②全ての作戦領域での活動を可能にするとともに、米国と同盟国のサイバー空間における行動の自由を確保し、敵対者にはそれを与えないことを目的とした、フルスペクトラムの軍事作戦の遂行を挙げている[62]。これらを達成するために、米サイバー軍は米軍が行う、攻撃・防御両面のあらゆるサイバー作戦の中核となることを想定して設立されたのである[63]。

米サイバー軍が、実際にいかなるサイバー攻撃能力を有しているのかは非公開とされたままである[64]。しかしながら、初代の米サイバー軍司令官を務めたキース・アレクサンダー（Keith Alexander）陸軍大将は、2012年の議会証言において、「我々のサイバー能力は、抑止の中核的要素である」とした上で、「適切な状況下で国家指揮権限当局（National Command Authority）からの指示が与えられた場合には、我々は国防総省が言う、米国に対する甚大なサイバー攻撃を検討する者は深刻なリスクを負うことになるとの主張を裏付けることが可能である」と発言している[65]。また、2013年3月の議会証言で、アレクサンダー司令官は、米国がサイバー空間で攻撃を受けた場合の防衛を担う複数のチームの編成を進めており、これらは攻撃的な任務を担うものであること、加えて各統合軍（combatant command）の攻撃的サイバー能力構築の計画を支援するチームについても編成中であることを明言した[66]。これはオバマ政権が初めて、公の場で攻撃的なサイバー能力の構築について述べた事例であった[67]。

なお、こうした流れの中で、攻撃的なサイバー能力については、サイバー軍から各地域別の統合軍への移管が進められている[68]。

---

61 Ellen Nakashima, "U.S. Cyberwarfare Force to Grow Significantly, Defense Secretary Says," *Washington Post*, March 28, 2014. <http://www.washingtonpost.com/world/national-security/us-cyberwarfare-force-to-grow-significantly-defense-secretary-says/2014/03/28/0a1fa074-b680-11e3-b84e-897d3d12b816_story.html> 増員に併せ、任務も拡大しつつある。現在、国防総省ウェブサイトの記述では、「コア・ミッション」として、①地球全体にわたって統合軍にサイバー面での支援を提供する、②国防総省の情報ネットワークの運用及び防衛を行う、③指令に基づき、国家の重要インフラ及び重要資源の防衛を行う、の三点が掲げられている。

62 Department of Defense, *U.S. Cyber Command Fact Sheet*, May 25, 2010. <http://www.defense.gov/home/features/2010/0410_cybersec/docs/CYberFactSheet%20UPDATED%20replaces%20May%2021%20Fact%20Sheet.pdf>

63 Paul Rosenzweig, "The Organization of the United States Government and Private Sector for Achieving Cyber Deterrence," *op.cit.*(16), p.252.

64 Zachary Fryer-Biggs, "U.S. Military Goes on Cyber Offensive," *Defense News*, March 24, 2012. <http://www.defensenews.com/article/20120324/DEFREG02/303240001/U-S-Military-Goes-Cyber-Offensive>

65 *Statement of General Keith B. Alexander, Commander United States Cyber Command, before the House Committee on Armed Services*, *Subcommittee on Emerging Threats and Capabilities*, March 20, 2012, p.8. <http://www.au.af.mil/au/awc/awcgate/postures/posture_cybercom_20mar2012.pdf>

66 *Hearing to Receive Testimony on U.S. Strategic Command and U.S. Cyber Command in Review of the Defense Authorization Request for Fiscal Year 2014 and the Future Years Defense Program*, March 12, 2013, pp.8-9. <http://www.armed-services.senate.gov/imo/media/doc/13-09%20-%203-12-13.pdf> なお、米軍における統合軍とは、複数の軍種（陸海空軍及び海兵隊）から構成される部隊であり、機能別統合軍と地域別統合軍の2種類がある。

67 Mark Mazzetti and David E. Sanger, "Security Leader Says U.S. Would Retaliate Against Cyberattacks," *New York Times*, March 12, 2013. <http://www.nytimes.com/2013/03/13/us/intelligence-official-warns-congress-that-cyberattacks-pose-threat-to-us.html>

68 Fryer-Biggs, *op.cit.*(64)

3　その他の主な動き

（1）政府及び軍高官の発言

ここまで取り上げてきた政策文書や米サイバー軍の発展の方向性などを見る限り、サイバー攻撃に対する懲罰的抑止は、米国のサイバーセキュリティ政策の中で、一定の地位を得るに至ったようである。もちろんそれは、冷戦期の核報復の威嚇による懲罰的抑止が享受していたような、安全保障政策上の支配的な位置ではなく、抑止のアプローチの中でも拒否的抑止と並列されるような形ではあるが、それでも重要な構成要素とみなされていることは間違いがない。

この点で象徴的なのが、リン国防副長官の懲罰的抑止に対する評価である。同副長官は2010年に発表した論文の中で、「抑止を機能させるには、報復措置でコストを強いるのではなく、攻撃者のあらゆる利益を否定することを重視する必要がある」[69]として、サイバー空間における懲罰的抑止の有効性については消極的に評価しており、また、そうした評価は、当時の一般的な見方を総括したものでもあったとされる[70]。だが、国防副長官の任を降りた後の2013年8月、米紙のインタビューに答えた際には、「政策議論は、攻撃的なオプションがより顕著になる方向に向かっている」とした上で、「特定の敵を抑止する上では、攻撃的なサイバー・オプションが重要な要素になり得るとの議論が説得力を増している」との見解を示している[71]。

こうした懲罰的抑止に対する積極的評価の背景には、拒否的抑止には、それが元来有する弱点が、サイバー攻撃特有の性質によって助長されているという問題点があるとの指摘がなされている[72]。すなわち、どれだけ強固な防衛力を整え、攻撃側が得られる利得を極限まで小さくしたところで、攻撃を実行する上でコストがかからないのであれば、攻撃の誘因はなくならないことになる。サイバー攻撃の実行にかかるコストが小さいことは既に述べたとおりであるが、それに加えて、弾薬やミサイルといった物理的な兵器と異なり、攻撃のツールは必ずしも一度限りの使い捨てではないのである[73]。

サイバー攻撃に対する懲罰的抑止の模索は、前章で触れた政策文書の発表以降も、現在に至るまで続いており、そうした流れは、リン副長官以外にも、多くの米政府及び軍高官等の発言から明確である。2012年5月の講演で、元米戦略軍司令官のジェームズ・カートライト（James Cartwright）は、サイバー空間での抑止について、攻撃的手段による懲罰的抑止を拒否的抑止と併用することの重要性について触れた上で、米国のサイバー空間における攻撃能力は物理的空間のそれが有しているレベルの信頼性を得るには至っていないが、同様の信頼性を達成する方向で努力が進められていること、また今後どこかの時点で、国家安全保障のためにそうしたサイバー空間での攻撃能力を用いる意思があることを示す必要があることに言及した[74]。

69　リン　前掲注16, p.20.

70　Jason Healey, “Commentary: Cyber Deterrence is Working,” *Defense News*, July 30, 2014. <http://www.defensenews.com/article/20140730/DEFFEAT05/307300017/Commentary-Cyber-Deterrence-Working>

71　Barton Gellman and Ellen Nakashima, “U.S. Spy Agencies Mounted 231 Offensive Cyber-Operations in 2011, Documents Show,” *Washington Post*, August 30, 2013. <http://www.washingtonpost.com/world/national-security/us-spy-agencies-mounted-231-offensive-cyber-operations-in-2011-documents-show/2013/08/30/d090a6ae-119e-11e3-b4cb-fd7ce041d814_story.html>

72　川口　前掲注14, p.18.

73　Philbin, *op.cit.*17, p.5.

74　Aliya Sternstein, “U.S. Must Strut Cyber Might to Stop Attacks, Cartwright Says,” Nextgov, May 15, 2012. <http://www.nextgov.com/cybersecurity/2012/05/us-must-strut-cyber-might-stop-attacks-cartwright-says/55745/>

2012年には、レオン・パネッタ（Leon Panetta）国防長官が、帰属問題に関する国防総省の取組と抑止について発言した。パネッタ国防長官は、国防総省はこれまでサイバー空間での抑止を複雑にしてきた帰属問題の解決に向けて大きく前進しており、特に過去2年間、サイバー・フォレンジックの面で成果を出しつつあると述べた。その上で、潜在的な攻撃者は、米国が彼らを探知して責任を取らせる能力を有していることを認識すべきであると警告するとともに、サイバー攻撃を防ぐには防衛の向上だけでは不十分で、深刻な攻撃に対しては、攻撃者への対抗措置を取る必要があり、国防総省はそのための有効な能力を保持していることを表明している。(75)

2014年3月には、米サイバー軍の司令官の交代が行われ、ロジャース海軍大将がその任に就いた。この人事の承認を行った上院軍事委員会での指名公聴会の事前質問への回答において、ロジャース司令官は、サイバー攻撃を抑止するためには、攻撃者に目的を達成させない防御的な能力と併せて、コストを負わせる攻撃的な能力を示すことが必要であること、サイバー空間での抑止戦略上は、他の空間での抑止と同様に、防御や反撃、さらには必要であれば攻撃を行う能力を示すことが重要であり、米軍には、攻撃元が特定された場合に、物理的・非物理的両方の手段によって反撃を行う能力が存在していることに言及している(76)。

（2）スノーデン事件の含意

2013年6月以降、NSAの関係企業の技術者であったエドワード・スノーデン（Edward Snowden）容疑者が、NSAを中心とした米国のサイバー空間での活動に関する内部告発を行った事件は、米国内でも国際的にも大きな反響を呼んだ。

この事件の全容については、本稿の射程を超えるため扱わないが、サイバー攻撃に対する懲罰的抑止を主眼とした本稿の関心上、この事件の一つの側面として、米国のサイバー攻撃の実態に関する重要な情報が公になった点には着目する必要がある。こうした情報としては、主に二つのものを挙げることができる。

一つは、2012年10月にオバマ大統領が署名したとされる、大統領政策指令20号（Presidential Policy Directive-20: PPD-20）である。この文書は、内容の一部をワシントン・ポスト紙が2012年11月に報じていたが、文書自体は2013年6月にスノーデン容疑者によって暴露された(77)。

PPD-20は、米政府として、サイバー空間における攻撃的な活動と防御的な活動を定義するとともに、米政府の機関がサイバー空間において、いかなる活動を誰の許可で行うことが許されるのかを定めたものである(78)。

同指令中の重要な点は以下のとおりである。まず、攻撃的サイバー効果作戦（Offensive Cyber Effects Operations: OCEO）を、「米政府自身か米政府に代わって行われる、サイバー空間内又はサイバー空間を通じて、米政府のネットワークの外にサイバー効果を生じさせるかそれを可能にすることを意図した作戦並びに関連の活動及びプログラム」として定義付けている(79)。そして、OCEOの実施は必ずしもサイバー攻撃に対する報復に限定されず、米国の国家目標のグ

---

(75) Department of Defense, “Remarks by Secretary Panetta on Cybersecurity to the Business Executives for National Security, New York City,” October 11, 2012. <http://www.defense.gov/transcripts/transcript.aspx?transcriptid=5136>

(76) *Advance Questions for Vice Admiral Michael S. Rogers, USN, Nominee for Commander, United States Cyber Command*, March 11, 2014, p.10. <http://www.armed-services.senate.gov/imo/media/doc/Rogers_03-11-14.pdf>

(77) Gellman and Nakashima, *op.cit.*(71)

(78) *ibid*.

ローバルな推進のために行いうること、重大な結果（人命の損失や米国への重大な反撃、大きな物的損害、米国の対外政策又は経済への深刻な悪影響）を招くと予想されるOCEOの実施には、大統領の承認を必要とすること、また外国でのOCEOの遂行に際し、米国の国益と公平（equities）上必要であるならば、当該国政府の同意がなくともその遂行を認めることに言及している。その上で、国防長官、国家情報長官及びCIA長官に対し、PPD-20の承認後6か月以内に、米国がOCEO能力を確立・維持すべき、標的となり得るシステムやプロセス、インフラを特定した計画を策定するように命じている。(80)

もう一つは、2013年8月に、スノーデン容疑者からの情報を基にワシントン・ポスト紙が報じた、米国の情報機関によるサイバー攻撃に関する報道である。ここでは、米国の情報機関は2011年中に231件もの攻撃的サイバー作戦を遂行しており、その3分の1近くはイランやロシア、中国、北朝鮮を標的としたものであること、外国のネットワークに侵入して膨大な数の標的コンピュータ等に遠隔操作でマルウェアを植え付ける「ジニー」と呼ばれるプログラムには、約6.5億ドルの予算が充当されていることが報じられている。そうした攻撃的サイバー作戦の実施は、NSAがその中心となっているが、CIAも近年、同種の活動を拡大しているという。ただし、攻撃的作戦のほとんどは、標的のデータにのみ影響を与えたり、コンピュータの正常な動作を妨げたりといったものに留まり、スタックスネットのような物理的損害を生じさせるレベルの攻撃は例外的と見られる。(81)

Ⅲ　米国のサイバー抑止の評価

ここまでに見てきたとおり、サイバー攻撃に対する懲罰的抑止のアプローチが、米国のサイバーセキュリティ政策の中で定着してくる中で、当然ながら、第Ⅰ章で触れた、サイバー空間に特有の性質が生み出す懲罰的抑止の有効性に対する制約をどう克服するのかについては、多くの議論が為されてきた。本章では、それらの議論を参照しながら、米国のサイバー抑止政策について一定の評価を試みるとともに、課題を指摘することとしたい。

1　懲罰的抑止の対象

米国のシンクタンクである大西洋評議会（Atlantic Council）は、2013年発表の報告書で、サイバー空間での安全保障政策において「テイラード抑止（tailored deterrence）」を採用することの重要性を提唱した(82)。テイラード抑止は、米国の戦略文書中では2006年のQDRで初めて用いられた用語であり、単一の懲罰的抑止をあらゆる対象に適用する形の抑止態勢を転換し、対象

---

(79)　ただし、ネットワーク防衛やサイバー情報収集はこの定義に含まれないとされている。なお、「サイバー効果」とは、「コンピュータや情報システム、又はその中に存在する情報によってコントロールされている、コンピュータ、情報又は通信システム、ネットワーク、物理的若しくはバーチャルのインフラの、操作・混乱・否認（denial）・劣化・破壊」を指すものとして定義されている。米国科学者連盟（Federation of American Scientists）が公開している、PPD-20の記述に基づく。*Presidential Policy Directive/PPD-20*. Federation of American Scientistsウェブサイト <http://www.fas.org/irp/offdocs/ppd/ppd-20.pdf>

(80)　Glenn Greenwald and Ewen MacAskill, “Obama Orders US to Draw up Overseas Target List for Cyber-Attacks,” *Guardian*, June 7, 2013. <http://www.theguardian.com/world/2013/jun/07/obama-china-targets-cyber-overseas>

(81)　Gellman and Nakashima, *op.cit.*(71)

(82)　Franklin D. Kramer and Melanie J. Teplinsky, “Cybersecurity and Tailored Deterrence,” *Atlantic Council Issue Brief*, December 2013. <http://www.atlanticcouncil.org/images/publications/Cybersecurity_and_Tailored_Deterrence.pdf>

ごとに異なる形態のアプローチを組み合わせて採用するもので[83]、懲罰的抑止が効きにくいテロリストなどに対しては、拒否的抑止を重視した抑止態勢を取る[84]。

前章でも述べたとおり、各アプローチ間の組み合わせのバランスについては議論こそあれ、サイバー攻撃に対する米国の抑止政策は、基本的にはこの方向に向かいつつあると言える。繰り返しになるが、米国のサイバーセキュリティ政策の中で、懲罰的抑止は唯一でも支配的でもなく、飽くまで防御措置や損害からの回復力の向上、それらに基づく拒否的抑止、さらには国内法執行など、多様なアプローチの中の一つとして位置付けられている[85]。

このような流れの中で、サイバー空間での懲罰的抑止の有効性を主張する側も、その焦点をより限定した形で、物理的な損害や人命の損失を引き起こし、米国の国家機能を麻痺させる、いわゆる戦略的サイバー攻撃（strategic cyber attack）のような形態の攻撃に対する抑止の有効性を挙げている[86]。例えば、2012年にパネッタ国防長官が、そうしたサイバー攻撃がある日突然米国に対して行われる、「サイバー真珠湾」の可能性を指摘したものの、その懸念は20年前から既にあったにもかかわらず今日に至るまで実際には起こっていないとの指摘や[87]、アレクサンダー米サイバー軍司令官が在任中の議会証言で述べた、「大まかではあるが、サイバー空間の戦略レベルにおいては、事実上の抑止が存在している」との見解がこれに当たる[88]。

そうした攻撃に焦点を絞る場合には、懲罰的抑止の対象も自ずと絞り込まれることになる。サイバー攻撃を行いうる主体は確かに多様ではあるものの、戦略的サイバー攻撃を仕掛けるような能力が、どの主体にも備わっているわけではない。すなわち、標的となるシステムをサイバー攻撃によって一時的にダウンさせることは可能であっても、強固な防衛措置を突破して、一時的にではなく、継続的に標的をダウンさせ続けるような能力は、依然としてサイバー大国にしか存在しないという[89]。

なお、特定の烈度や形態のサイバー攻撃のみを懲罰的抑止の対象とする場合に、問題となるのは、それを超えた場合に報復に訴えるという「レッドライン」を明示するか否かである。抑止の原則からすれば、「何が許容されないのか」を明確にすることは、抑止側と被抑止側の認識ギャップに起因した抑止の失敗を防ぐ上で重要と言える。だが、エリック・ローゼンバッハ（Eric Rosenbach）国防次官補は、そうした「レッドライン」を明確にすると、攻撃側はそれを目安に、許容される行動の限界を追求しようとするようになるため、米政府としては「レッド

---

(83) Department of Defense, *op.cit.*(38), p.49.

(84) Ryan Henry, "Deterrence and Dissuasion in the 21st Century," *The 36th IFPA-Fletcher Conference Report on National Security and Policy—Implementing the New Triad: Nuclear and Non-Nuclear Forces in Twenty-First-Century Deterrence*, 2006, pp.3-5. <http://www.ifpa.org/pdf/IFC36.pdf>

(85) 米国政府のサイバーセキュリティを所管する機関は数多いが、大まかな整理としては、2012年のアレクサンダー米サイバー軍司令官の議会証言での整理が参考になる。まず、国防総省、情報機関、NSA、米サイバー軍が、外国の領域内での探知・防止・防衛、外国のサイバー脅威に関するインテリジェンスと帰属特定、国家安全保障及び軍のシステムのセキュリティ、米国が全射程能力を持つ主体（a full scope actor）によってサイバー攻撃を受けた場合の本土防衛に責任を負う。国土安全保障省は、米国の重要インフラのサイバーセキュリティ向上に関する国家の総合的施策に関する調整の主導と、米国政府の文民部門のネットワーク及びシステムの保護を担当する。連邦捜査局（Federal Bureau of Investigation: FBI）は、国内の領域において、同機関が持つ法執行・インテリジェンス・防諜・対テロの権限に従い、探知や捜査、防止、対処に責任を持つ。*op.cit.*(65), p.13.

(86) Healey, *op.cit.*(70)

(87) *ibid*.

(88) Statement of General Keith B. Alexander, Commander United States Cyber Command, before the House Committee on Armed Services, Subcommittee on Emerging Threats and Capabilities, March 16, 2011, p.8. <http://armedservices.house.gov/index.cfm/files/serve?File_id=50aeaaff-808b-4f43-a8d0-ad86ec9357f6>

(89) Healey, *op.cit.*(70)

ライン」の表明はしない方針であると述べている(90)。

この種の曖昧性に依拠した抑止は、確かに実際の「レッドライン」よりも烈度の低いレベルの攻撃までをも抑止できる可能性を持つために有用性が高いが、一方で、攻撃側が抑止側の「レッドライン」の位置について何らかの理由により誤って確信し、実際には抑止側にとって許容されないはずの行動に出る危険が残る。サイバー攻撃に対する懲罰的抑止に当たり、米国は体系的な宣言政策を策定すべきとの意見があるが(91)、仮に今後それが実現するのであれば、「レッドライン」の扱いについては、重要な検討事項の一つになることが予想される(92)。

2　帰属問題の深刻さ

前出のパネッタ国防長官の発言において典型的に見られるように、米国は懲罰的抑止の大きな障害である帰属問題の解決に向けて多くの投資を行い、前進してきていることに繰り返し言及してきた。こうした声明は、「前進」の詳細について明かすことが難しい中で、それ自体が一種の宣言政策として、抑止を強化する目的の下で発せられているものと思われる。だが一方で、依然として帰属問題の完全な解決は遠いとの見方が強く(93)、米サイバー軍のロジャース司令官も、帰属問題の解消に向けた努力は前進してはいるものの、まだ多くの場合、時宜を得た形で攻撃の発信源を特定できるものではないことを認めてもいる(94)。

しかしながら、前項で述べたような、抑止の対象とする攻撃の形態及び主体をより限定的に捉えることを前提とすれば、帰属問題は、それほど深刻な障害とはならないとの指摘がある。戦略的サイバー攻撃を行うような能力を有するサイバー大国はそう多くない以上、そうした攻撃があれば、「おそらくこの国である」という国を特定するのは比較的容易であり、実際その烈度に至らなかった攻撃、例えば2007年のエストニア、2008年のグルジア、2010年のスタックスネットの事例でも、「おそらくこの国である」との特定はすぐになされている(95)。

攻撃の目的の観点から、「帰属問題の限界」を指摘する議論もある(96)。米国の経済・社会インフラに大規模なサイバー攻撃が仕掛けられるような事態が起こるとすれば、攻撃者が米国に対して何らかの政治的な譲歩を迫るためにそうした攻撃を行うと威嚇し、米国がこれを拒否した場合か、通常戦争の前に、米国の戦争遂行能力を低下させることを意図した場合である。だが、前者の場合では、攻撃者は米国に対して要求の内容と威嚇を伝えるコミュニケーションを行わねばならず、その過程では攻撃者が誰なのかは自ずと明らかになるであろうし(97)、後者の場合、後に続く通常戦争を仕掛けてくる主体が先立つサイバー攻撃の実行者であることはほぼ確実である。

---

(90)　Jared Serbu, "DoD to be More Transparent about Strategy to Deter Cyber Attacks," *Federal News Radio*, October 3, 2014. <http://www.federalnewsradio.com/394/3714846/DoD-to-be-more-transparent-about-strategy-to-deter-cyber-attacks>

(91)　例えば、Glaser, *op.cit.*(21), p.5.

(92)　「レッドライン」を明確に伝達すべきであるとの見解を示したものとして、Iasiello, *op.cit.*(19), p.107.

(93)　例えば、Philbin, *op.cit.*(17), p.7.

(94)　*op.cit.*(76), p.18.

(95)　Healey, *op.cit.*(70)

(96)　Glaser, *op.cit.*(21)

(97)　単に要求と攻撃の威嚇を突き付けるだけであれば匿名のままでも可能であろうが、その威嚇が実際に履行されうると米国に信じ込ませるためには、威嚇を発している側が、それを履行しうるだけの能力を持った主体であることを米国に信じ込ませなければならないためである。

だが、これらの主張が正しいとしても、依然残る問題は、国家による非国家主体を介したサイバー攻撃の抑止であろう。「反撃の観点からは、重要なのは攻撃主体が誰であるのかではなく、敵対的なサイバー活動の責任を特定の国家に帰することができるか」であるとの指摘もある[98]。実際、過去の大規模サイバー攻撃の事例であるエストニアへの攻撃などでは、実施主体とされた愛国主義的な組織とロシア政府の関係が疑われたものの、それが立証されたわけではない[99]。

これに対して、「攻撃を行ったのは誰か」を問うのではなく、「誰が責任を取るのか」を追及する方向で、国家による非国家主体を介したサイバー攻撃に伴う帰属問題を解決していくことを主張する見解もある[100]。これは、ある国の領域内にあるコンピュータが攻撃の発信源であるとき、それに関与していなくとも、当該国にはその攻撃を止める責任があるという規範が共有されれば、攻撃を実行している非国家主体と国家の関係が立証されずとも当該国は責任を問われるようになるため、結果として非国家主体を介したサイバー攻撃も困難になるとするものである。とはいえ、現に国際社会においてそうした規範が共有されているわけではないし、仮にそうした規範が今後形成されることがあるとしても、当該国を非難する程度ならともかく、それに基づいて当該国に対する懲罰的報復措置までが許容されるには相当高いハードルがある。

ただし、一つ留意しておくべきなのは、この種の国家による非国家主体支援と帰属問題の関係についての議論は、サイバー空間に固有の新しいものではない点である。近年の核抑止論の重要な命題の一つとなっている、いわゆる「安定－不安定のパラドックス（stability-instability paradox）」は、まさにこうしたサイバー空間の状況に通じるところがある。これは、核保有国間では、核戦争へのエスカレーションをおそれて、いずれの国家も核攻撃やそこにエスカレートする危険性の高い通常戦争に訴えることを抑制する一方、より暴力の烈度が低いレベルでの挑発行動が惹起されるとするもので、その典型的な形態として、国家の関与が完全には断定しにくい、相手国内での反乱やテロの支援が挙げられている[101]。この種の国家支援テロをいかに抑止するかについて、明確に議論の決着がついているわけではないが、そうした議論の帰趨は、サイバー空間での同様の問題を考える上では一つの参考になり得る。

3　信頼性

（1）サイバー攻撃による報復威嚇の信頼性

第Ⅰ章で述べたとおり、懲罰的抑止の信頼性の観点からは、抑止側は自身が威嚇した報復を履行できるだけの攻撃的な能力を有していることを、潜在的な攻撃者に対して示す必要がある一方で、サイバー攻撃能力は性質上、その詳細を秘匿しなければ有効性を維持できないという点で、サイバー懲罰的抑止にはジレンマが伴う。

98　Eric F. Mejia, “Act and Attribution in Cyberspace: A Proposed Analytic Framework,” *Strategit Studies Quarterly*, vol.8, no.1, spring 2014, p.118. <http://www.au.af.mil/au/ssq/digital/pdf/spring_2014/Mejia.pdf>

99　Wil Goodman, “Cyber Deterrence: Tougher in Theory than in Practice?” *Strategic Studies Quarterly*, vol.4, no.3, fall 2010, p.111. <http://www.au.af.mil/au/ssq/2010/fall/goodman.pdf>

100　そうした見解を示した論考の例として、Jason Healey, “Beyond Attribution: Seeking National Responsibility for Cyber Attacks,” *Atlantic Council Issue Brief*, January 2012. <http://www.atlanticcouncil.org/images/files/publication_pdfs/403/022212_ACUS_NatlResponsibilityCyber.PDF>

101　この問題について詳しく論じた例として、S. Paul Kapur, *Dangerous Deterrent: Nuclear Weapons Proliferation and Conflict in South Asia*, Stanford University Press, 2007.

米国は今日に至るまで、どのようなサイバー攻撃能力を保有しているのか具体的に明らかにはしていない。「国防総省サイバー空間政策報告」は、サイバー空間の性質ゆえに、抑止の信頼性を向上させるための攻撃能力の開示が困難であると認めている(102)。前章で見てきた米国の政策文書や米サイバー軍司令官らの発言において、米国が報復を行う能力を有しているとの声明が繰り返し出てきていることや、サイバー軍の創設自体も含め、組織整備などの面で「サイバー戦争を遂行する」態勢を整えつつある点に関する情報を発表していることは、そうした困難がある中で、抑止の信頼性を担保するための一種の宣言政策としての側面を持つと言える。

報復の威嚇の信頼性を担保するという面では、2010年のスタックスネットによるイランの核施設へのサイバー攻撃には重要な意義があった。スタックスネットは当時、「これまでで最も技術的に洗練された、標的攻撃型のための悪意のあるプログラム」(103)と呼ばれ、かつ歴史上初めて物理的損害をもたらしたサイバー攻撃でもあった。もちろん、米政府は公には攻撃への関与を認めていないが、そうした米政府の立場に関わりなく、これが米政府の関与した攻撃であるとの認識は定着しており、結果として、米国のサイバー攻撃能力と、それに立脚した米国のサイバー空間での懲罰的抑止の信頼性が大きく向上したことは間違いがない(104)。さらに言えば、米政府が意図していたわけではないとはいえ、スノーデン事件によって、米国によるサイバー攻撃に関する情報の一部が明るみに出たこともまた、米国のサイバー報復能力の信頼性を向上させる影響を持ったと解釈することができよう。

とはいえ、先に挙げた2012年のカートライト元米戦略軍司令官の発言に見られるように、依然として米国のサイバー攻撃能力が、物理的な空間でのそれと並び立つレベルの信頼性の確保に至っていないとの認識は残っている。抑止における信頼性の問題の難しさは、それが究極的には、抑止の対象となる潜在的な攻撃者の認識に関わるものであるため、充分な信頼性が確保されたかどうか、検証できないことにある。この点を踏まえれば、米国のサイバー報復攻撃能力の信頼性の模索は、今後も続いていくものと考えられる。

（2）物理的攻撃による報復威嚇の信頼性

もう一つ信頼性の問題の焦点となるのは、サイバー攻撃に対して物理的な軍事力で報復するという威嚇の信頼性である。この問題の解消には、そうした威嚇の履行を躊躇させ得る二つの要因、すなわちサイバー攻撃に対する物理的報復措置への国際社会の反応と、通常戦争へのエスカレーションが発生した場合の対処について、何らかの手当てがなされる必要がある。通常戦力面での圧倒的優位を誇る米国の場合、より大きな問題となるのは前者である。

現時点では、サイバー攻撃に対する物理的な軍事力での反撃がどこまで認められるのかについて、明確な国際法上の規範が確立されているわけではない。米政府としては、2012年に国務省の法律顧問であったハロルド・コー（Harold Koh）が、「直接的に、死傷者や重大な破壊を引き起こすようなサイバー活動は、武力の行使とみなされる可能性が高い」と述べた上で、「武力攻撃かその差し迫った脅威に相当するようなコンピュータ・ネットワーク活動は、国連憲章第51条で認められた、国家の自衛権の発動に繋がり得る」という立場を示している(105)。

---

(102)　Department of Defense, *op.cit.*(58), p.5.

(103)　Aleksandr Matrosov, et.al., *Stuxnet Under the Microscope（Revision 1.31）*, January 2011, p.70. <http://www.eset.com/us/resources/white-papers/Stuxnet_Under_the_Microscope.pdf>

(104)　Robert M. Lee, “Stuxnet and Cyber Deterrence,” *Infosec Island*, August 13, 2012. <http://www.infosecisland.com/blogview/22168-Stuxnet-and-Cyber-Deterrence.html>

物理的な軍事力による懲罰的抑止の信頼性を確保するためには、この米国の立場、さらにはより具体的に、軍事力に訴える場合の「基準」が、国際的に共有されることが必要になる。この観点からすれば、米政府は、それらが反映された規範の形成に向けて、一定のイニシアティブを発揮しているようにも見える。例えば、規範が依然流動的な現状においては、サイバー先進国として、前出のコーの見解のような立場表明や、さらには政策文書及び政府当局者の発言において、米国はサイバー攻撃に対して物理的な軍事対応を取り得ることを繰り返し述べていることは、今後形成される国際規範の方向性に一定の影響を持つことは間違いない。また、「国防総省サイバー空間政策報告」では、「サイバー空間と物理空間での軍事作戦の関係を含む、サイバー空間での宣言的抑止態勢の発展」という項目中に、目標を共有する国々との間で、サイバー空間での行動規範確立に向けた協力を進めているとの言及がある(106)。この文脈からは、米国を含むNATOの専門家会合が2012年に発表した「タリン・マニュアル」が、武力攻撃に相当するようなレベルのサイバー攻撃を受けた国は自衛権を行使できるとの見解を示したことは(107)、サイバー攻撃への物理的な手段での対応を許容する規範の国際化に資するものとの評価ができる(108)。

一方で、これまでに極めて多くのサイバー攻撃が行われてきたにもかかわらず、その大半が何ら報復措置等を受けることなく許容されてきたことによって、既にサイバー空間での攻撃に対し、物理的な空間での武力の行使に訴えることを許容しない強固な敷居（threshold）が事実上確立されてきているとする見方もある(109)。この点については、今後の国際社会における議論の帰趨を見極める必要があろう。

おわりに

サイバーセキュリティの問題は、まさに現在進行中の問題として、日々新たな動きが発生しているものであり、その一部であるサイバー攻撃に対する懲罰的抑止に関しても、当然それが当てはまる。本稿では取り上げられなかったが、例えば、ここ最近米中間で、中国軍が関与しているとされる米企業などへの情報窃取型のサイバー攻撃が大きな摩擦要因になっており、これに関して米司法省が中国軍関係者5人を訴追したことについて、相手方の評判を落とす、一種の懲罰的抑止の手法であると見る向きもある(110)。また、依然として反対論が根強いが、大半のサイバー攻撃の被害者である米国の民間企業に、攻撃を受けた場合に反撃する権限を与える可能性について、議論が活発になってきており、これはサイバー攻撃に対する懲罰的抑止のあり方を大きく変える可能性がある(111)。こうした新たな動きについて、今後も注視していく

(105) Harold Hongju Koh, “International Law in Cyberspace,” September 18, 2012. <http://www.state.gov/s/l/releases/remarks/197924.htm>

(106) Department of Defense, *op.cit.*(58), p.2.

(107) Michael N. Schmitt, ed., Tallinn Manual on the International Law Applicable to Cyber Warfare: Prepared by the International Group of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence, Cambridge: Cambridge University Press, 2013, pp.54-61.

(108) 「タリン・マニュアル」は、NATOが設置した、サイバー戦争における既存の国際法の妥当性を検討するための専門家委員会の報告書である。NATOの公式文書ではないため、何らかの法的拘束力を持って加盟国や他の国の行動を規定するような性質の文書ではないが、多数国間で調整された見解の表明は、米単独のそれと比べて、今後の国際規範形成の方向性に与える影響はより大きいものと思われる。

(109) Trujillo, *op.cit.*(10), p.49.

(110) Geoff Dyer, “US Cyber Charges Risk Retaliation from Beijing,” Finanial Times, May 19, 2014.

必要がある。

米国のサイバー抑止政策が持つ我が国への含意は、二つの点から指摘できる。第一に、第Ⅱ章で見てきたとおり、米国はサイバー攻撃への対策において同盟国などと協力を進める意向を示すとともに、集団防衛を規定した同盟国との条約上の義務を、サイバー空間にも適用するとしている。また、2014年10月に発表された、「日米防衛協力のための指針（ガイドライン）」の中間報告でも、サイバー空間における協力の重要性が指摘された(112)。これらの点を踏まえれば、日米同盟を安全保障政策の基軸とする我が国にとって、米国のサイバー抑止政策のあり方を理解しておくことは、極めて重要であると言える。

第二に、本質的に攻撃優位のサイバー空間での安全保障政策を考える上で、我が国においても、懲罰的抑止までいかずとも、サイバー攻撃に対する一定の反撃能力の保有について検討すべきであるとの議論が出てきていることがある(113)。防衛省でも、サイバー攻撃を受けた場合に、攻撃元を探知して反撃を行うプログラムの研究を行っている(114)。他方で、そうした反撃手段を行使することは、憲法の下での専守防衛原則から逸脱する可能性もあり、難しさも指摘されている(115)。こうした反撃能力の保有に関する議論を進めるに当たり、先行する米国において、サイバー攻撃に対する懲罰的抑止の議論がどのような展開を見せているのかについては、我が国として注視していくことが求められよう。

（くりた　まさひろ）

---

(111)　例として、David E. Sanger, “As Chinese Leader’s Visit Nears, U.S. Is Urged to Allow Counterattacks on Hackers,” *New York Times*, May 22, 2013; Craig Timberg, Ellen Nakashima and Danielle Douglas-Gabriel, “Hacked Firms Quietly Talk about Fighting Fire with Fire,” *Washington Post*, October 10, 2014.

(112)　「日米防衛協力のための指針の見直しに関する中間報告」2014.10.8. 防衛省・自衛隊ウェブサイト <http://www.mod.go.jp/j/approach/anpo/sisin/houkoku_20141008.html>

(113)　例えば、大澤淳「WEDGE OPINION 現実化するサイバー戦争　集団的自衛権と対外諜報の容認を」『WEDGE』25巻7号, 2013.7, pp.18-20.

(114)　「［スキャナー］サイバー有事　対応遅れ　自衛隊「これからが勝負」」『読売新聞』2013.10.14.

(115)　「自衛隊にサイバー防衛隊　90人態勢、24時間監視　反撃能力の可否を検討」『47news』2014.3.26. <http://www.47news.jp/47topics/e/251798.php>