第２章　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－

川口　貴久*

はじめに

サイバー空間へのアクセスとその安定的利用は各国の安全保障や社会・経済的な繁栄に不可欠である。同時に、サイバー空間は国家の排他的管轄権の外にあるため、「グローバル・コモンズ」としての性格を有している[1]。それゆえ、サイバー空間では諸国家や民間組織による自律的な秩序が求められている。

抑止力（deterrence）は自律的な秩序形成・維持に貢献する。抑止とは、相手にネガティブなメッセージを送ることで「相手が本来したであろう行為を思いとどまらせる」ことであり、その一般的モデルは武力による報復を示唆しながら相手方行為を思いとどまらせる「懲罰的抑止」である。冷戦期、核および通常戦力によって構成される抑止メカニズムが米ソ対立構造に一定の安定性を与え、ある歴史家はこれを「長い平和」とさえ呼んだ。

しかし、従来の国際安全保障の中心であった抑止メカニズムはサイバー空間で大きな問題に直面している。同時に、直面する課題を超えて、サイバー空間で抑止力を整備する動きもある。

そこで本章では、近年のアメリカのサイバー防衛・安全保障政策を中心に、サイバー空間での抑止力の限界性と可能性を検討する。特に議論の焦点となっているのは、攻撃元を特定し、報復や懲罰を示唆する抑止メカニズム（懲罰的抑止）が機能するか否かである。

結論からいえば、従来、アメリカの防衛・安全保障コミュニティでは、いくつかの理由によって懲罰的抑止力の構築は難しいと考えられてきた。しかし、現在ではサイバー攻撃の発信源を特定し、報復を示唆するような抑止力が整備されつつある。こうしたサイバー空間の防衛・安全保障政策の変化、つまり懲罰的抑止力の追求を前提に、日米同盟も適応していく必要がある。

まず、サイバー空間の抑止論の現状を俯瞰し（第 1 節）、サイバー空間で伝統的な抑止が機能しにくい理由を論じたい（第 2 節）。そうした限界性を踏まえて、アメリカの防衛・安全保障コミュニティで抑止論がどのように変化したかを論じ（第 3 節）、最後に日米同盟の課題について触れたい（第 4 節）。

* 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の意見を代弁するものではない。

１．サイバー空間における安全保障

1-1．サイバー空間の抑止論

安全保障政策におけるサイバーセキュリティの優先度が高まっている。アメリカはサイバー空間を陸、海、空、宇宙に続く「第 5 の戦場」ととらえ、『米国家安全保障戦略』(2010 年 5 月）では「デジタル・インフラストラクチャーは戦略的な国家資産であり、この防衛は…中略…国家安全保障上の優先事項[2]」と位置づけた。また、ホワイトハウスや国防総省が中心となって、サイバーセキュリティに関する戦略・方針をたて続けに発信している（表 1)。

2010 年 10 月には、米軍のネットワークを防護するためサイバー軍司令部（Cyber Command: CYBERCOM）の運用が開始された[3]。今後数年で、CYBERCOM は要員を 5 倍に増やし、重要インフラの防衛、国防総省ネットワーク防護、海外での戦闘任務支援の部隊を整備する予定である[4]。連邦予算の「強制削減（sequestration)」下であっても、サイバーセキュリティ分野への投資は増えている。

表 1　サイバー安全保障にかかわる主な政策文書・スピーチなど（アメリカ）

年月	タイトル
2008 年 1 月	ホワイトハウス「包括的国家サイバーセキュリティ・イニシアティブ (Comprehensive National Cybersecurity Initiative)」　※公表は 2010 年 3 月
2009 年 3 月	ホワイトハウス「サイバー空間政策レビュー（Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure)
2010 年 1 月	クリントン国務長官「インターネットの自由」演説
2010 年 10 月	CYBERCOM 本格運用開始
2010 年 2 月	国防総省「4 年毎の国防報告 2010（Quadrennial Defense Review Report: QDR)」議会報告
2010 年 5 月	ホワイトハウス「アメリカ国家安全保障戦略（National Security Strategy)」
2011 年 5 月	ホワイトハウス「サイバー空間における国際戦略（International Strategy for Cyberspace)」
2011 年 7 月	国防総省「サイバー空間における作戦行動についての国防総省戦略」(Department of Defense Strategy for Operating in Cyberspace)
2011 年 11 月	国防総省「国防総省サイバー空間政策報告 (Department of Defense Cyberspace Policy Report)」
2012 年 10 月	パネッタ国防長官「国家安全保障についてのビジネス経営者向けサイバーセキュリティ」演説

一方で、サイバー安全保障政策の中での抑止の位置づけは不明瞭であり、模索が続いている。ブッシュ政権下で作成（2008 年 1 月）され、オバマ政権誕生後に公表（2010 年 3 月）された「包括的国家サイバー安全保障イニシアティブ（Comprehensive National Cybersecurity Initiative: CNCI)」は、その具体的取り組みの 1 つとして「揺るぎない抑止戦略およびプログラムの構築・発展」を掲げたが、体系的な政策を明示するに至ってはいな

い[5]。

そして、サイバー空間の抑止についての政策・研究[6]の多くは、冷戦期の懲罰的抑止モデルはサイバー空間で機能しない、という見方を示している。国防総省・米軍でのサイバーセキュリティ対策の推進者であり、オバマ政権で国防副長官を務めたリン（William J. Lynn, Ⅲ）ははっきりという。

> 一度のクリックは 0.3 秒で地球を 2 周する。その一方で、攻撃元を特定するのに必要な捜査は数カ月を要する。ほぼリアルタイムでサイバー攻撃者を特定しなければ、我々の抑止プログラムは破綻する。ミサイルは「返信先」を明らかにしてやってくるが、サイバー攻撃の多くはそうではない。こういった理由で、抑止についての既存モデルは、サイバー空間では全く当てはまらない[7]。

ブッシュ・オバマの両政権でサイバーセキュリティ政策に携わったクラーク（Richard A. Clarke）曰く、「戦略的核戦争防止の必須条件である抑止理論は、現段階では、サイバー戦争を阻止する上では何ら重要な役割を果たさない[8]」。抑止研究の第一人者であるモーガン（Patrick M.Morgan）も「その（冷戦期の）抑止の最も顕著な特徴の多くは、今日ではほとんど使いものにならない。現在のサイバー攻撃の問題は規模と特徴の面で全く異なっている。冷戦期の抑止から最も適用されうるいくつかの教訓は本質的にネガティブなものである。つまり、適用しない理由や避けるべき根拠といったものだ[9]」という。

しかし、こうした見方は変化しつつある。端的にいえば、2013 年 12 月現在、アメリカの安全保障政策はサイバー空間において攻撃元を特定し、報復や懲罰を示唆する抑止メカニズム（懲罰的抑止力）を模索し、一定程度の能力を有している。この変化は、2011 年 11 月に議会に提出された「国防総省サイバー空間政策報告（Department of Defense Cyberspace Policy Report）」に反映されている。詳細は後述するが、その前に抑止のメカニズムに触れたい。

1-2. 抑止のメカニズム

抑止の概念は第二次世界大戦以前にも存在したが、その理論化・精緻化は核戦略の発展と密接に関連していた。というのは、核兵器の誕生により、防衛・安全保障政策の目的（あるいは軍組織の役割）は「戦争に勝つ」ことから「戦争を起こさない」ことに変化したからである。こうした事情もあり、抑止といえば、冷戦に象徴される報復を示唆しながら相手方行為を思いとどまらせる「懲罰的抑止」が想像されるだろう。しかし、核兵器であれ

サイバー兵器であれ、「抑止は複雑で、単なる報復（retaliation）より多くのものを伴う[10]」。安全保障政策で想定される抑止はより広い概念である。

抑止とは、相手にネガティブなメッセージを送ることで、「相手が本来したであろう行為を思いとどまらせる」ことである。このように抑止を定義するならば、その形態は様々である[11]。特に注意すべきは抑止のメカニズムである。2 つのアクター間で抑止が成立するのは、攻撃失敗のコストの期待値が攻撃成功の利益の期待値を上回る場合である[12]。このような抑止メカニズムを成立させるためには、2 つの方法がある。1 つは相手の利益を否定する拒否的抑止（deterrence by denial）であり、もう 1 つは相手にコストを課す懲罰的抑止（deterrence by punishment）である。そして、サイバー空間の抑止論で議論の焦点となっているのは後者である。

２．サイバー空間における抑止力の限界性:「帰属問題」と「攻撃優位」

しかし、サイバー空間では従来的な抑止メカニズムは機能しないと考えられてきた[13]。いくつか理由はあるが、ここでは①サイバー攻撃の発信元の特定が困難である点、②インターネット空間では防御に対して攻撃が有利な点に焦点を絞りたい[14]。すなわち、サイバー空間の現状は、防御に対して攻撃が優勢であり、その攻撃の発信源の特定は難しい。こうした状況では懲罰による抑止メカニズムは機能しない。

2-1.「帰属問題（attribution problem)」

サイバー空間では攻撃の発信源を即座に断定することができない、少なくとも困難である。サイバーセキュリティの専門家はこれを「帰属問題（attribution problem)」と呼ぶ[15]。“attribution”とは「行為の原因・因果関係を特定すること」と定義されうるが、サイバー空間では攻撃が行われた物理的場所、使用されたコンピュータ端末、サーバの所有者、実際の攻撃者が国境を超えるため、帰属が複雑化する。

帰属問題の所在はインターネットの構造、アプリケーションやプログラムの設計、攻撃者の社会的属性（特に国家との関係）と多岐にわたる。ここでは帰属問題の階層性をある程度、単純化して、①技術的な帰属問題、②社会・政治的な帰属問題について検討してみたい。

技術的な帰属問題は、インターネットの構造と密接に関連している。インターネットとは、相互接続されたコンピュータ間で、情報を小分けにし、これらを任意の宛先に届ける世界大のネットワークである。そこでは、データを正確に届ける仕組み（通信プロトコル）が必要となる。データの送受信を保障する標準的規格が TCP/IP（Transmission Control

Protocol/Internet Protocol）であり、端末ごとにふられた固有の識別番号が IP アドレス（Internet Protocol Address）である。

だが、サイバー攻撃では発信元の IP アドレスが偽装されるケースが多い。この問題は、2013 年初頭の米セキュリティ会社マンディアント（Mandiant）による報告書と中国の対応でも顕在化した。同社の報告書によれば、中国政府および人民解放軍はアメリカの公的機関・民間企業に対して恒常的なエクスプロイテーション（exploitation）を行っている[16]。しかし、中国国防部はこうした攻撃に彼らが関与していないとした上で、「インターネットの世界では周知のことであるが、IP アドレスを根拠にサイバー攻撃の発信源を特定することはできない。IP アドレスの偽造は毎日のように起こっている[17]」と述べている。

さらに、ここ 10 年で顕在化したボットネットと呼ばれる攻撃手法も帰属問題を複雑にする。ボットネットとは、ウイルス感染等により“乗っ取られた”コンピュータの集合体を指す。ボットネットは、攻撃者からの指示をいくつかの中継サーバを経由して受信し、対象に攻撃を仕掛ける。ボットネットの規模は数万の IP アドレスに及ぶ。2009 年 5 月に発覚したボットネット「mariposa」（スペイン語で「蝶」の意味）は全世界で 1200 万以上の IP アドレスが感染する史上最大規模のボットネットであった。サイバー攻撃の帰属は、ボットネットの興隆により以前にも増して複雑化した。

このように、攻撃元の偽装やボットネットにより、技術的な階層で帰属が複雑化している。しかし、技術的なレベルよりも政治・社会的なレベルの帰属問題の方が深刻である。「インターネットの父」の 1 人とされるマサチューセッツ工科大のクラーク（David D. Clark）は断言する。「帰属問題とは全くもって技術的なものではない…中略…その解決は、技術的領域の外にある[18]。」　つまり、帰属問題は端末の前でクリックする人間の社会・政治的属性を特定しなければならず、それは政策的な解決を要する。

そして、サイバー攻撃の行為者と責任ある主権国家の関係を立証できなければ、抑止は機能しない。仮に攻撃者（個人や端末）を特定したとしても、攻撃者と責任ある国家・組織の関係を断定することは難しい。時間をかけて外国からのサイバー攻撃を特定したとしても、その外国政府との関連は明らかにされない。例えば、ロシアからエストニアへのサイバー攻撃（2007 年）、グルジアへのサイバー攻撃（2008 年）の背景には愛国的な青年組織が存在したと報道される。しかし、彼らのような「サイバー民兵」「クレムリン・キッズ」によるサイバー攻撃とロシア政府の関係を証明することは難しい[19]。

しかし、こうした見方は社会的帰属問題を過大視しているといえる。大西洋評議会（Atlantic Council）のヒーリー（Jason Healey）によれば、サイバー抑止はサイバー攻撃の実行者を特定する必要はない。彼は、1999 年の駐中米大使館への投石事件（NATO による

駐ユーゴ中国大使館への誤爆が原因）から教訓を導き出す。それは大使館の安全確保には実際の投石者を特定する必要はなく、投石事件の責任（この場合、投石を看過した所管警察と中国政府）を追及すれば事足りるということである。つまり、「誰がやったか」ではなく「誰が責任をもつのか」が重要である[20]。

実際、こうしたモデルに近いのは、民間の ISP（Internet Service Provider）事業者や CSIRT（Computer Security Incident Response Team）[21]による国際的連携・調整メカニズムであろう。インシデント発生時、さらなる被害を食い止めるために CSIRT 間で連携し、特定の IP アドレスをインターネットから切り離すなどの処置を行う。この過程は「誰がやったか（attribution）」ではなく、「誰が対処すべきか（responsibility）」という点で連携が行われ、これは一般的に機能しているといわれる[22]。もちろん過大な期待はすべきではない。CSIRT はあくまでも調整機関であり、法的強制力や執行機能はないし、昨今の国家主導（state-sponsored）の攻撃に対処できるかは分からない。

いずれにせよ、帰属問題が抑止メカニズムに与える影響は大きい。攻撃元を即時に断定できないため、報復による懲罰的抑止が冷戦期ほど機能しない。

2-2.「攻撃優位」のアーキテクチャ

もう 1 つの大きな問題は、サイバー空間は「攻撃優位」のアーキテクチャが形成されている点である。この「攻撃優位」の問題は、「帰属問題」と密接に関連している。

サイバー空間、特にインターネット空間[23]は情報を容易かつ自由に伝達・拡散することを目的として設計された。こうしたインターネットの「自由」「効率性」といった設計思想は必ずしもリスクマネジメントや安全保障を最優先事項とはせず、結果、攻撃者が有利なアーキテクチャが形成された。オバマ政権発足後、ハサウェイ（Melissa Hathaway）が中心となり、それまでのサイバーセキュリティ政策の見直しを行った。その成果文書は『60 日レビュー』と呼ばれ、現状に警鐘を鳴らした。

> デジタル・インフラストラクチャーのアーキテクチャは、**セキュリティよりも相互運用性や効率性を考慮して、設計された**。その結果、国家および非国家アクターが情報を危険にさらし、盗み、改竄し、破壊している。そして、アメリカのシステムに重大な破壊を引き起こしうるものになっている[24]。（強調筆者）

利便性とセキュリティはトレードオフであり、インターネット空間は利便性を求めた設計である。インターネット空間を行きかう情報（パケット）は善悪の価値判断が下されな

いどころか、識別番号さえない。ヴィントン・サーフ（Vinton G. Cerf）とともに、TCP/IP プロトコルを開発し、「インターネットの父」として知られるロバート・カーン（Robert E. Kahn）もインターネットの脆弱性の 1 つとして、「優先取極めのないコミュニケーションの自由」を挙げる。現状では、あらゆるコミュニケーションは基本的には同じ重要性として扱われる。したがって、許容できるコミュニケーションと不明・望ましくないコミュニケーションを区別することは難しい[25]。

「自律・分散・協調」を基本原理とするインターネット空間[26]では、結果的に、攻撃者による優位性が形成されてきた。端的にいって、サイバー空間の競合は「攻撃優位をめぐる競合であり、攻撃者と防衛者に等しく資源が与えられれば、攻撃側が勝つ[27]」のである。実際には、攻撃側は少ないコストや資源で防衛側に打ち勝つことができる。攻撃側は無数のプログラムから 1 つまたは複数の脆弱性を探し出せば目的を達成するが、防衛側は全ての脆弱性を網羅・検証し、アップデートし続けなければいけない。そのコスト差はあまりに大きい。例えば、1000 万行のセキュリティプログラムに対して、わずか 125 行の強力なマルウェアが作成されることもある[28]。

そして攻撃側が有利な環境では、「先制」は魅力的なオプションであり、現状変更を試みる者による侵攻のリスクが高まる[29]。このような世界では、既存の防衛・安全保障政策は変化を迫られる。日本でいえば、「専守防衛」に基づく政策体系は通用しないかもしれない。リン前国防副長官の言葉を借りれば、「要塞主義のメンタリティ（a fortress mentality）は通用しない」し、「ファイヤーウォールというマジノ戦線の後ろへ下がることはできない」のである[30]。攻撃優位の世界における抑止はきわめて困難な課題として浮上する。

３．サイバー空間における抑止力の模索

サイバー空間は攻撃者優位であり、攻撃元を特定することが難しい。それゆえ、アメリカの防衛・安全保障コミュニティでは、冷戦期のような懲罰的な抑止力は機能しないと考えられてきた。しかし、現在では、サイバー空間において懲罰的抑止力を追求する安全保障政策が形成されつつある。

3-1．リンの抑止論と「積極的防衛」

冷戦期に確立された懲罰的な抑止政策は、サイバー空間に適応できない。これが、2010 年末頃までのサイバー抑止に関する米国防総省の見解であった。CYBERCOM 司令官・アレクサンダー大将（Keith B. Alexander）は、2010 年 9 月の上院公聴会でサイバー抑止の困難さについて率直に述べている。「サイバー分野の抑止はその他分野とは異なるものである。

冷戦期のような機能は担えない。…中略…我々は幅広い観点で抑止を刷新する研究をしなければならない[31]。」

冷戦期の懲罰的抑止に代わって強調されたのが、拒否的抑止力である。つまり、サイバー空間では報復によりサイバー攻撃者にコストを課す「懲罰的抑止力」は難しいが、サイバー攻撃者の利益を否定する「拒否的抑止力」は実現可能である。こうした考え方は、リン国防副長官が『フォーリンアフェアーズ』誌に寄せた論説「新しいドメインの防衛」に反映されている[32]（もともとアメリカは懲罰的抑止政策を明示的に展開しようとしたが[33]、「サイバー空間における作戦行動についての国防総省戦略」等の政策文書では報復や攻撃的オプションは明示されなかった）。

サイバー空間の拒否的抑止力は、政策文書の中では「積極的防衛（active defense）」と表現される[34]。これは、CYBERCOM が掲げる重点分野の 1 つである[35]。「サイバー空間における作戦行動についての国防総省戦略」によれば、国防総省は「同省のネットワークとシステムへの侵入を予防し、侵入した敵対行為を打破する積極的なサイバー防衛（active cyber defense）を展開する」とした上で、積極的なサイバー防衛を「脅威と脆弱性を発見し、検知し、分析し、被害を低減するためのシンクロナイズドされた、リアルタイムの能力」と定義する[36]。つまり、積極的防衛と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、およびそのための一連の投資と更新である。

積極的防衛の考え方は、防衛大綱に示される「動的抑止力」（2010 年）や「統合機動防衛力」（2013 年）に近い。核兵器はその強力さ故に、存在するだけで抑止力を有している（実存的抑止）とされた。しかし、サイバー空間の抑止力は「存在」することではなく、常に「運用」されることに意味がある。早期警戒やセキュリティシステムの更新といった運用がサイバー抑止の核心である。

しかし、そもそも拒否的抑止力のメカニズムには本来的に制約がある。というのは、どれほどサイバー攻撃の利益や成功確率を極小化しようとも（仮にそれらが限りなくゼロに近くとも）、サイバー攻撃によるコストがゼロであれば、攻撃のインセンティブが常に存在する。それゆえ、アメリカのサイバー抑止政策が拒否的抑止力だけでなく、懲罰的抑止力を追求することとなる。

3-2. パネッタ演説と懲罰的抑止力

こうした事情もあって、攻撃元の特定能力を備えた懲罰的抑止力が模索されてきた。統合参謀本部副議長［当時］のカートライト海兵隊大将（James E. Cartwright）をはじめ、かねてより米国は懲罰的抑止と攻撃オプションの必要性を訴えてきた。彼によれば、「21 世

紀の抑止は、それが核兵器であれ、生物兵器であれ、サイバーであれ、広義では匿名性（anonymity）と帰属（attribution）に関するもの」である。そして、効果的な抑止力は防衛的なオプションだけでは不十分であり、攻撃的なオプションが必要である[37]。

こうした見方が支配的となっていく。国防総省が議会に提出した「サイバースペース政策報告」（2011 年 11 月）では、サイバー空間における 2 つの抑止メカニズムを強調した。つまり、「サイバー空間での抑止は、他のドメインと同様に 2 つの基本的メカニズムに立脚する。つまり、敵の目的を否定することであり、必要であれば侵攻する敵対者にコストを課すことである[38]。」従来、焦眉の課題であった「帰属問題」についても、一定の方向性がみえているようである。2012 年 10 月のパネッタ国防長官（Leon E. Panetta）のスピーチはサイバー抑止を考える上で、大きな転換点となった。

> 国防総省のネットワークを防衛するために、我々は攻撃者への抑止を支援する。我々がサイバー攻撃者をたどることができる、あるいはサイバー攻撃は強固な防衛能力によって失敗する、と攻撃者が認識していれば、彼らが我々を攻撃する可能性は低くなる。
> 国防総省はサイバー攻撃の抑止を複雑にしている問題、つまり攻撃元を特定するという問題を解決する点で非常に進展を続けている。
> この 2 年間で国防総省は特定問題を解決するためのフォレンジック（forensics）に大きな投資をしてきた。そして我々は投資にみあう成果をつかみつつある[39]。

パネッタがいう「進展」の具体的内容については不明だが、国防総省「サイバースペース政策報告」で取り組みの方向性や一端が垣間見える。具体的には、攻撃の物理的な発信源を追跡する手法、ふるまいを基にしたアルゴリズム（behavior-based algorithms）による攻撃者評価、サイバーフォレンジック（cyber forensics、サイバー攻撃が行われた場合にコンピュータやネットワークなどのログを通じた証拠保全と攻撃元調査）、インテリジェンス・コミュニティと CYBERCOM を中心とする専門家育成、国土安全保障省との連携などである[40]。また、省庁間や国家間で新しいマルウェアのインディケーターを交換することも効果的であろう。

サイバー空間では攻撃元を特定することが難しい。しかし、こうした問題を超えて、懲罰的抑止力が形成されつつある。重要な点は、積極的防衛（拒否的抑止力）と懲罰的抑止力は相当程度、重なる部分が多いということである。冷戦期は攻撃用と防御用の核兵器・ミサイルが区別できたかもしれないが、サイバー空間では拒否的抑止力・懲罰的抑止力、攻撃・防御を明確に分けることはできない。サイバー「兵器」は 1 つのシステムの中で、

複数の要素を兼ね備えたものである。それゆえ、サイバー空間での「抑止は攻撃的であり、防衛的であり、インテリジェンス・オペレーションであり、これらを融合させたもの[41]」が求められる。

3-3. ドメイン横断型の抑止とエスカレーション・コントロール

サイバー空間の抑止力はサイバー空間だけに限定されず、攻撃に対する報復や懲罰行為は「ドメイン横断（cross-domain)」的である[42]。実際、アメリカはサイバー攻撃に対して、陸・海・空・宇宙で動力学的（kinetic）な方法による報復を示唆している。「国防総省サイバー空間政策報告」では、次のような見解が示されている。

> サイバー空間の悪意ある行為から、合衆国、同盟国、パートナー、国益を守るために、合衆国大統領は必要なあらゆる手段（all necessary means）を用いて対応する権利をもつ…中略…大統領の指示に基づき、対応オプションは国防総省によって提供されるサイバー能力および物理的能力（kinetic capabilities）のいずれか、あるいは双方を含む[43]。

こうした物理的能力には核戦力を含むという見方もある。国防総省の諮問機関である国防科学委員会（Defense Science Board）は最近の報告書の中で、「効果的な国防総省のサイバー戦略には抑止の要素が不可欠である」とした上で、サイバー攻撃への抑止として核戦力を維持すべし、と勧告している[44]。それは核兵器システムが最もサイバー攻撃に強く、抗堪性が高い（resilient）という評価に起因すると推察される。

しかし、物理的な軍事行動を示唆することで、危機がエスカレートするリスクが常に存在する。これを防ぐためにはエスカレーション・コントロール、「対象」と「手段」を考慮した段階的オプションが求められる。検討する際の視点としては、攻撃対象が軍事関連施設か民生用の社会インフラを含むか[45]、サイバー第一攻撃および報復攻撃がどの程度可視化されているかという点が挙げられる[46]。

４．サイバーセキュリティと日米同盟

サイバー空間の安全保障政策は変化の渦中にある。それは、サイバー脅威の顕在化というだけでなく、対抗する安全保障メカニズムの観点でも変化している。こうしたサイバー空間の防衛・安全保障政策の変化、つまり懲罰的抑止力の追求を前提に、日米同盟も変化する必要がある。

2013 年 10 月に開催された日米の外務相・防衛相による「２＋２」（Security Consultative

Committee: SCC）で、1997 年に改定された日米防衛ガイドラインを 2014 年末までに見直すことに合意した。サイバー空間での協力も新たな課題として認識され、作業部会を設置する。サイバー空間に関する日米協力の具体化が進む中、ここでは日米同盟によるサイバー抑止力強化にあたっての課題を検討したい。

4-1．政策：中国発のサイバー攻撃を“フルスペクトラム”で評価する

日米同盟におけるサイバー抑止を検討する場合、日米同盟の“本丸”の議論から外れるわけにはいかない。それは、「力による現状変更」を試みているとみられる中国との関係である。加えて、平時から有事、そしてそれらの「中間領域」「グレーゾーン」のリスク管理について検討する必要がある。つまり、中国発のサイバー攻撃をフルスペクトラムで評価し、抑止力の適応範囲を示す必要がある。

2013 年 6 月のアジア安全保障会議で、ヘーゲル（Chuck Hagel）米国防長官は、「アメリカを狙ったサイバー攻撃に中国政府および人民解放軍が関与し、その攻撃対象は米政府機関や軍だけでなく、米産業や民間企業にも及んでいる」と指摘し、続く米中首脳会談でもオバマ（Barack H.Obama）大統領が習近平（Xi Jinping）国家主席に同様の懸念を伝えた。

だが重要なことは、こうした中国発のサイバー攻撃は平時のエクスプロイテーションとしてだけでなく、有事におけるアクセス拒否・接近阻止（Anti-Access, Anti-Denial: A2AD）戦略の要としても位置づけられている。マンディアント社の最高セキュリティ責任者のベトリッチ（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[47]。米中経済安全保障検討委員会に提出された中国のサイバー戦能力に関する報告書（2009 年、2012 年）は、東アジアでの紛争時、中国は平時のエクスプロイテーション活動で得られた脆弱性を活用し、アメリカにサイバー攻撃を行うことはほぼ間違いないと結論づける。攻撃は米軍の指揮統制・兵站ネットワークに対するオペレーショナルな妨害活動であると同時に、アメリカ政府の（介入するか否かの）意思決定を遅延・複雑化する狙いがある[48]。

サイバー空間の拡大抑止は、平時から有事および中間領域における中国発のサイバー攻撃のリスクを評価し、抑止力による対処の範囲を設定することが必要である。

4-2．法的基盤：“どの時点で”武力攻撃を認めるのか

次に法的基盤の整備である。サイバー空間の懲罰的抑止力の法的基盤を整備する上で、集団的自衛権に関する議論を決着させる必要がある。実際、第 2 次安倍政権下で設置され

た「安全保障の法的基盤の再構築に関する懇談会」で、集団的自衛権の見直しが進んでいる。2013 年 8 月、「懇談会」座長代理の北岡伸一は集団的自衛権の見直しを従来の「四類型」にとらわれず、シーレーンや宇宙、サイバー空間への攻撃対処を含む全面解禁とする方向性を示した。

もちろん個別自衛権の議論も進んでいる。2012 年 4 月 26 日、情報セキュリティ政策会議において、外務省は既存の国際法体系がサイバー空間に適応可能とした上で、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」という見解を表明した。2013 年 10 月 23 日の参議院予算委員会では、安倍首相もサイバー攻撃に自衛権行使可能との旨を述べた。

個別であれ、集団的であれ、サイバー空間における自衛権行使の要件は「通常の武力攻撃と同程度の損害を与えるか否か」という点に収斂するだろう。しかし、これは不十分である。2010 年のイランの遠心分離機制御システムへの攻撃（Stuxnet）であれ、2012 年のサウジアラビアの国営石油会社のデータ消去（Shamoon）であれ、結果的にあるサイバー攻撃が「武力攻撃」相当かどうかは判断・認定できるだろう。しかし、どの時点で「武力攻撃」相当と認定するかは難しい問題である。サイバー空間での対応はスピードが求められる。『ワシントンポスト』紙の国家安全保障問題担当記者のナカシマ（Ellen Nakashima）がいうように、結局のところ、「どのようなサイバー攻撃が戦争行為なのか」を決めるのは政治的判断であり、それは軍事的決定や法的決定以上に重要である[49]。そうした権限を予め決めておく必要がある。

4-3. 運用：2 つの“世界と言語”が理解できる人材を確保する

最後は日米同盟のサイバー抑止力を維持するための運用、そのための人材確保である。

東日本大震災における日米協力は有事の協力モデルとなった。震災直後、市ヶ谷、横田、仙台に日米調整所を設置し、米軍および自衛隊のコミュニケーションと運用調整を行った。2011 年 6 月の「２＋２」では、こうした経験を「将来のあらゆる事態への対応のモデル」と評価した。2014 年のガイドライン再改定では、日米の調整・協力メカニズムがより具体化されるだろう。

サイバーセキュリティ分野の協力がどういったスキームで構築されるかは定かではないが、いずれにせよ、日米同盟のサイバーセキュリティ強化には「スーツ」と「ギーク」、2 つの世界と言語を理解する人材が必要とされている[50]。「スーツ」、つまり防衛・安全保障政策の形成者たちには独特の価値体系や専門性がある。一方で「ギーク」、つまりサイバーセキュリティの世界や言語も同様である。

両者の価値体系（世界）と専門性（言語）を理解しなければ、サイバー攻撃対処の日米連携は困難であろう。教育や研修プログラムを通じて、「2 つの世界」を同時に理解する人材を輩出するのは難しい。現実的には、「スーツ」あるいは「ギーク」がもう一方の分野に歩み寄るしかないだろう。

またサイバーセキュリティの専門家、特に外交・安全保障分野で活躍する「ギーク」は不足している。業界団体や政府主導のワークショップ型ハッキング大会(いわゆる Capture The F1ag:CTF)などを通じて、有能な人材を積極的に登用していく必要がある。

おわりに

サイバー空間は「開かれ、グローバル（open & global）」であるが故に脅威にさらされている。リスクを管理し、「安全で強靭（secure & resilient）」な空間を構築しなければならない[51]。だが、「グローバル・コモンズ」としての性格を有するサイバー空間は単一の国家の統制下にあるわけではなく、諸国家による自律的な秩序が必要とされる。

一般的にいえば、抑止メカニズムは国際安全保障・秩序を構成する重要要素だが、サイバー空間の抑止メカニズムは問題に直面している。サイバー空間では、防御に対して攻撃が優勢であり、その攻撃の発信源の特定は難しい。「帰属問題」と「攻撃優位」のアーキテクチャにより、サイバー空間で懲罰的な抑止力は機能しないと考えられてきた。

しかし、ここ数年で、アメリカの防衛・安全保障政策はサイバー攻撃者を特定し、報復を示唆するような抑止力（懲罰的抑止力）を模索している。そして、サイバー抑止力は各国によるサイバー空間へのアクセスと安定的利用を保証する。日本そして日米同盟もこうした動きに呼応し、日米によるサイバー抑止力を整備していく必要がある。

－注－

1 The White House, *National Security Strategy of the United States* (Washington D.C.: White House, May 2010), pp.49-50.

2 The White House, *National Security Strategy of the United States*, pp.27-28.

3 CYBERCOM は戦略軍司令部（Strategic Command: STRACOM）隷下だが、司令官は他の統合軍司令部と同様に大将が務める。また、CYBERCOM 司令官アレクサンダー大将（Keith B. Alexander）は国家安全保障局（National Security Agency: NSA）長官を兼務する。

4 Ellen Nakashima, “Pentagon to boost cybersecurity force,” *The Washington Post* (January 28, 2013).

5 The White House, *Comprehensive National Cybersecurity Initiative* (Washington D.C.: White House, March 2, 2010)。

6 サイバー抑止に関する研究・考察として、Martin C. Libicki, *Cyberdeterrence and Cyberwar* (RAND, 2009); Richard L. Kugler, “Deterrence of Cyber Attacks,” in Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz, eds., *Cyberpower and National Security: Cyberpower and National Security* (Washington, D.C: National Defense University and Potomac Books, 2009), pp.309-340; Thomas J. Mowbray, “Solution Architecture for Cyber Deterrence,”: SANS Institute (April 12, 2010); Patrick M. Morgan, “Applicability of Traditional

Deterrence Concepts and Theory to the Cyber Realm," in National Academy of Sciences, eds., *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options of U.S. Policy* (National Academies Pr., 2010), pp.55-76; William J. Lynn, III, "Defending a New Domain: The Pentagon's Cyberstrategy," *Foreign Affairs*, Vol.89, No.5 (September/October 2010), pp.97-108; David C. Gompert, and Phillip C. Saunders, "Mutual Restraint in Cyberspace," in *The Paradox of Power： Sino-American Strategic Restraint in an Age of Vulnerability* (Washington D.C.; Institute for National Strategic Studies, National Defense University, 2011), pp.115-151;　Charles L. Glaser, "Deterrence of Cyber Attacks and U.S. National Security," Report GW-CSPRI-2011-5, Cyber Security Policy and Research Institute, The George Washington University (June 1, 2011); Joseph S. Nye, "Nuclear Lessons for Cyber Security?" *Strategic Studies Quarterly*, Vol.5, No.4 (Winter 2011), pp.18-38; Andrew F. Krepinevich, *Cyber Warfare: A "Nuclear Option"?* (Center for Strategic and Budgetary Assessments, 2012); Martin C.Libicki, *Crisis and Escalation in Cyberspace* (Ca: Santa Monica: RAND, 2012); Jason Healey, eds., *A Fierce Domain: Cyber Conflict, 1986 to 2012* (Vienna: Cyber Conflict Studies Association, 2013); Thomas Rid, *Cyber War Will Not Take Place* (London: Hurst & Company, 2013).

[7] William J. Lynn, III, Deputy Secretary of Defense, Remarks at STRATCOM Cyber Symposium, Omaha, Nebraska (May 26, 2010).

[8] リチャード・クラーク、ロバート・ネイク（北川知子ほか訳）『核を超える脅威　世界サイバー戦争：見えない軍拡が始まった』（徳間書店、2011 年）、228 頁。

[9] Morgan, "Applicability of Traditional Deterrence Concepts and Theory to the Cyber Realm," pp.75-76.

[10] Nye,"Nuclear Lessons for Cyber Security?," p.33.

[11] 例えば、誰を抑止するか（自国抑止 central deterrence,　同盟国を含める拡大抑止 extended deterrence）、いつ抑止するか（有事抑止 immediate deterrence、平時抑止 general deterrence）などが想定される。Lawrence Freedman, *Deterrence* (London; Polity, 2004).

[12] ①敵対者がある行為をとった場合に得られる利益［Benefits: B］、②ある行為が達成される確率［Probability: P］、③ある行為をとった場合に生じるコスト／抑止する者が課すコスト［Costs: C］とすると、抑止が成立するのは **C*(1-P)> B*P** の場合である。より詳細は、土山實男『安全保障の国際政治学：焦りと傲り』（有斐閣、2004 年）、178-179 頁。

[13] 抑止成立の条件は諸説あるが、端的にいえば、それは抑止をする「意思」と「能力」、抑止する側とされる側の「相互認識」の三要素が不可欠である。ただし、抑止成立の要件は論者により微妙に異なる。例えば、ポール（T.V. Paul）によれば、伝統的な抑止が成立する要件は、①抑止を成立させるべく、抑止する側に十分な能力があり、②その抑止が信頼性・信憑性があるものであり、③それが敵対者に伝達されること、である。 T. V. Paul, "Complex Deterrence: An Introduction," in T. V. Paul, Patrick M. Morgan & James J. Wirtz, ed., *Complex Deterrence: Strategy in the Global Age* (Chicago: University of Chicago Press, 2009), pp.2-3.

[14] 本稿で掲げる課題以外に、①サイバー空間の「戦争」「武力攻撃」についての共通認識がない点、どの時点で「戦争」「武力攻撃」となるか判断が難しい点（閾値問題 threshold problem）、②サイバー空間における「二重の非対称性」（アクターやパワーの非対称性、サイバーインフラへの依存度・脆弱度の非対称性）、がサイバー空間の抑止を困難にしている。

[15] Attribution についての詳細分析は、米下院科学技術委員会・技術とイノベーション小委員会のテーマ「将来のサイバー攻撃の帰属をプランニングする」（2010 年 7 月 15 日）、2010 年に開催された米国科学アカデミー（National Academy of Sciences）によるプロジェクトの分科会での検討『サイバー攻撃の抑止についてのワークショップ報告書』を参照。特に、Robert K. Knake, "Untangling Attribution: Moving to Accountability in Cyberspace," Prepared Statement Before the Subcommittee on Technology and Innovation, Committee on Science and Technology, United States House of Representatives(July 15, 2010); David D. Clark and Susan Landau, "Untangling Attribution," in National Academy of Sciences, eds., *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options of U.S. Policy* (National Academies Pr., 2010), pp.25-40; W. Earl Boebert, "A Survey of Challenges in Attribution ," in *Proceedings of a Workshop on Deterring Cyberattacks*, pp.41-52.

[16] 報告書によれば、人民解放軍は単一の攻撃目標から 6.5 テラバイト（TB）のデータを入手した。これは、新聞紙朝刊の約 12 万年分の情報量に相当する。Mandiant, *APT1: Exposing One of China's Cyber Espionage Units* (Feburary 2013) 。また、報道によれば、高高度ミサイル防衛（THAAD）、F-35 統合打撃戦闘機、新型オスプレイなど最先端の防衛機密情報がサイバー攻撃によって剽窃された可能性がある。"Pentagon aircraft, missile defense programs target of China cyber threat," *The Washington Post* (May 28, 2013).

[17] Chinese military never supports cyberattacks: defense ministry, Ministry of National Defense, The People's Republic of China (February 20, 2013)
http://eng.mod.gov.cn/Press/2013-02/20/content_4433574.htm

[18] Clark and Landau, "Untangling Attribution," p.39.

[19] Noah Shachtman, "Kremlin Kids: We Launched the Estonian Cyber War," Danger Room: What's Next in National Security, the Blog by *Wired* (March 11, 2009).

[20] Jason Healey, "Beyond Attribution: Seeking National Responsibility for Cyber Attacks," Issue Briefs, Atlantic

Council (January 2012).

[21] CSIRT とは、インターネットを媒介とするサイバー攻撃やインシデントの状況監視、攻撃・インシデント発生時の対処、その他組織との調整を行う組織体の一般名称である。日本では一般社団法人 JPCERT コーディネーションセンター（Japan Computer Emergency Response Team Coordination Center: JPCERT/CC）などが代表的である。

[22] 国内 CSIRT 関係者へのヒアリング。

[23] インターネットとサイバー空間は同議ではない。前者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る。後者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ものである。

[24] The White House, *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure* (Washington D.C.: White House, May 2009), iii.

[25] Robert E. Kahn, “The Role of Architecture in Internet Defense,” in Kristin M. Lord and Travis Sharp, eds., *America’s Cyber Future: Security and Prosperity in the Information Age*, Vol.2 (Washington, D.C.: The Center for New American Security, June 2011) pp.208-209.

[26] 土屋大洋「サイバースペースのガバナンス」、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 25 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（2013 年 8 月）。

[27] Krepinevich, *Cyber Warfare,* p.40.

[28] William J. Lynn , III,　Remarks on Cyber at the RSA Conference, San Francisco, California (February 15, 2011).

[29] 国際政治学・安全保障研究では、攻撃と防御の区別と優劣は国家間の安定性（戦争と平和）に大きな影響を与えていると考えられてきた。安全保障研究では、攻撃と防御の区別がつかないほど、安全保障のジレンマが発生する。そして、防御に対して攻撃が優勢であるほど、侵攻のリスクが高くなる。前述のとおり、サイバー空間は攻撃有利であり、攻撃と防御は区別が難しい。それゆえサイバー空間は「二重のリスク」（doubly dangerous）を抱えている。Robert Jervis, “Cooperation Under the Security Dilemma,” *World Politics*, Vol. 30, No. 2 (January 1978), pp. 167-214.

[30] Lynn, “Defending a New Domain,” p.99.

[31] Statement of Gen. Keith B. Alexander, Commander, United States Cyber Command, before　the House Committee on Armed Services(September 23, 2010).

[32] Lynn, “Defending a New Domain,” pp.99-100.

[33] Siobhan Gorman and Julian E. Barnes, "Cyber Combat: Act of War: Pentagon Sets Stage for U.S. to Respond to Computer Sabotage with Military Force," *Wall Street Journal* (May 31, 2011).

[34] 安全保障研究では、抑止（deterrence）と防御（defense）を区別する場合がある。抑止は敵対者に攻撃を思いとどまらせることであり、防御は抑止が失敗した際に攻撃の被害を抑えることである。Glenn H. Snyder, *Deterrence and Defense: Toward a Theory of National Security* (Princeton: Princeton University Press, 1961). しかし、サイバーセキュリティは攻撃・防御、抑止力・防衛力は峻別できず、両者を一体的に扱っている。

[35] CYBERCOM の 5 つの戦略（a five-pillared strategy）とは、(1)サイバー空間が戦争・防衛の新たなドメインであると認識すること、(2)積極的・能動的な防衛、(3)死活的に重要なインフラの保護、(4)集団的防衛、(5)技術的優位の確保と活用である。Statement of Gen. Keith B. Alexander, Commander United States Cyber Command, Before the House Committee on Armed Service (September 23, 2010).

[36] Department of Defense, Department of Defense Strategy for Operating in Cyberspace (July 2011), p.7.

[37] Developments in China's Cyber and Nuclear Capabilities, Hearing Before the U.S.-China Economic and Security Review Commission, One Hundred Twelfth Congress Second Session (March 26, 2012), pp.11-13. Aliya Sternstein, “U.S. must strut cyber might to stop attacks, Cartwright says,” *Nextgov* (May 15, 2012).

[38] 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), p.2.

[39] Secretary of Defense Leon E. Panetta, Remarks on Cybersecurity to the Business Executives for National Security, New York City (October 11, 2012).

[40] Department of Defense, *Department of Defense Cyberspace Policy Report*, pp.4-5. なお、同様のプログラムは防衛省も開発を進めている。「防衛省が対サイバー兵器、攻撃を逆探知し無力化」『読売新聞』（2012 年 1 月 1 日）。また、日本国内でもサイバー空間における攻撃オプションの検討が始まった。中期防衛力整備計画（2013 年）では、「攻撃側が圧倒的に優位であるサイバー空間での対処能力を確保するため、相手方によるサイバー空間の利用を妨げる能力の保有の可能性についても視野に入れる」としている。

[41] Lynn, Remarks at STRATCOM Cyber Symposium.

[42] James A. Lewis, “Cross-Domain Deterrence and Credible Threats,” Center for Strategic and International Studies (July 2010).

[43] Department of Defense, *Department of Defense Cyberspace Policy Report*, p.4.

[44] Defense Science Board, *Task Force Report: Resilient Military Systems and the Advanced Cyber Threat* (January 2013), pp.40-43.

[45] グレイサーは「対価値サイバー攻撃（countervalue cyber attacks）」と「対軍事施設サイバー攻撃（counter-military cyber attacks）」という概念で、リビッキは「戦略的なサイバー戦争（strategic cyberwar）」と「作戦行動としてのサイバー戦争（operational cyberwar）」という定義で攻撃対象についての議論を進めている。Glaser, Deterrence of Cyber Attacks and U.S. National Security,”　Libicki, *Cyberdeterrence and Cyberwar*.

[46] リビッキは「公然たる（overt）攻撃／報復」「明白な（obvious）攻撃／報復」「秘密裏の（covert）攻撃／報復」という観点でリスク評価を行う。Libicki, *Crisis and Escalation in Cyberspace*, pp.155-158.

[47] Richard Bejtlich, “Don‘t Underestimate Cyber Spies: How Virtual Espionage Can Lead to Actual Destruction,” Snapshots on *Foreign Affairs* (May 2, 2013).
http://www.foreignaffairs.com/articles/139357/richard-bejtlich/dont-underestimate-cyber-spies

[48] Bryan Krekel, Patton Adams, *George Bakos, Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage*, Prepared for the U.S.-China Economic and Security Review Commission (McLean, VA: Northrop Grumman Corporation, March 2012), p.15［公益財団法人 防衛基盤整備協会訳「情報優位の獲得：コンピュータ・ネットワーク作戦及びサイバースパイ活動のための中国の能力」（公益財団法人 防衛基盤整備協会、2012 年 9 月）、10 頁］; Bryan Krekel [Principal Author], *Capability of the People’s Republic of China to Conduct Cyber Warfare and Computer Network Exploitation,* Prepared for The US-China Economic and Security Review Commission (McLean, VA: Northrop Grumman Corporation Information Systems Sector, October 2009)［財団法人 防衛調達基盤整備協会訳「中華人民共和国のサイバー戦とコンピュータ・ネットワーク・エクスプロイテーション能力」BSK 保全小冊子、第 22-5 号（平成 22 年 9 月）］。

[49] Ellen Nakashima, “When is a cyberattack an act of war?” *The Washington Post* (October 26, 2012)　ナカシマによれば、判断基準の 1 つは、サイバー攻撃が通常の「武力攻撃」と同様の「耐え難い」損害を与えるのかどうかである。「耐え難い」損害とは、物理的または動的な（kinetic）な損害を指す。それゆえ、経済的損害のみが発生するサイバー攻撃や情報収集目的のサイバー・インテリジェンス活動は「戦争行為」「武力攻撃」とはみなしにくい。

[50] ギーク（geek）とは元々「オタク」「変人」の意味であり、情報技術の専門家を指す。スーツ（suits）とは官僚や軍人などの政策形成者を指す。土屋大洋『情報による安全保障：ネットワーク時代のインテリジェンス・コミュニティ』（慶應義塾大学出版会、2007 年）、3-13 頁。

[51] John D. Negroponte and Samuel J. Palmisano, Chairs, Adam Segal, Project Director, *Defending an Open, Global, Secure, and Resilient Internet*, Independent Task Force Report No.70(New York: Council on Foreign Relations, 2013).