［研究論文］

米国におけるサイバー抑止政策の刷新
アトリビューションとレジリエンス

Renewing Cyber-Deterrence Policy in the US
“Attribution” and “Resilience”

川口 貴久*
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

Takahisa Kawaguchi
Senior Consultant, Tokio Marine & Nichido Risk Consulting Co., Ltd. /
Senior Researcher, Keio Research Institute at SFC

Abstract:　サイバー空間で抑止は機能するのか？　どのような条件・環境下でサイバー抑止は機能するのか？　本稿は米国の外交・安全保障政策におけるサイバー抑止概念の変遷を詳述しながら、この問いに答える。米国の外交・安全保障政策における「サイバー抑止」の概念はこれまで一貫性のないものであったが、それは米国が環境変化や技術革新をうけて、サイバー抑止政策を刷新してきた結果である。刷新の背景にはサイバー空間の生来的課題である「アトリビューション」「レジリエンス」があり、これらによって、サイバー抑止は効果を上げつつある。

Can deterrence work in cyberspace? What kinds of situations does cyber-deterrence work in? This paper explores these questions, while describing the transition of “cyber-deterrence” concept in the US. The cyber-deterrent policy has been inconsistent in the past. It is because the U.S. government has attempted to renew the cyber-deterrence policy in response to changes in security environment and technical innovations. The renewing of cyber-deterrence policy has been driven by the inherent problems of cyberspace: “attribution” (identifying the cyber attackers) and “resilience” (restoring networks and data damaged by the cyber-attacks), and they make cyber deterrence be more effective.

Keywords: 国際安全保障、抑止、サイバー空間、アトリビューション、レジリエンス
international security, deterrence, cyber space, attribution, resilience

＊　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。

はじめに

サイバー空間は紛争のリスクが高い。国際政治学・安全保障論の分野では、攻撃と防御の区別と優劣は国家間の紛争に影響を与えると考えられてきた。ジャービス (Robert Jervis) の研究によれば、攻撃と防御の区別がつかないほど「安全保障のジレンマ」が発生し、防御に対して攻撃が有利であるほど「力による現状変更」のリスクが高くなる [1]。

サイバー空間では攻撃と防御の区別がつきにくく、そもそも何がサイバー「兵器」なのかも分からない。そして、サイバー空間は防御側に対して攻撃側が有利である。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。だが、防衛側は全ての脆弱性を網羅・検証し、セキュリティ対策を更新し続け、24 時間 365 日体制で攻撃を検知・監視し続けなければならない。そうしなければサイバーセキュリティは崩壊する。極端な例は、1000 万行のセキュリティプログラムがわずか 125 行の強力なマルウェアに破られるケースである [2]。攻撃と防御の区別が曖昧で、防御に対して攻撃が有利なサイバー空間は大きな紛争リスクを抱えている。

「安全保障のジレンマ」にしろ、「力による現状変更」にしろ、「いかにしてサイバー戦争を抑止するか」という国際安全保障上の中心的問題につながる。抑止 (deterrence) 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、第二次世界大戦後の国際安全保障を構成する重要なメカニズムである。

しかし、サイバー空間では抑止が機能するか否かについて大きな議論がある。この議論は実際のサイバー抑止政策にも影響を与えている。米国の外交・安全保障政策におけるサイバー抑止の概念は過去、一貫性のないものであった（後述）。しかし、言い換えれば、米国は国際安全保障環境の変化や技術的な革新をうけて、「サイバー抑止」を刷新してきたともいえる。

そこで、本稿は米国の外交・安全保障政策におけるサイバー抑止に注目しながら、その変遷および背景となる環境・認識変化を詳述する。サイバー空間の安全保障をめぐる本稿の問題関心は、サイバー空間で抑止は機能するのか、という点である。だが、「抑止は最良の戦略だ」「抑止は機能しない」といった包括的な言明 (blanket statement) は避けなければいけない。新しい安

全保障環境下で、抑止は成功する可能性もあれば失敗する可能性もある[3]。そこで本稿は、どのような状況・条件下でサイバー抑止は機能するのか、という点を明かにしたい。

第一章「サイバー空間の抑止論」では抑止論の概要とこれまでの抑止論に関する理論的・政策的な刷新について触れる。第二章「米国におけるサイバー抑止政策の変遷」では、2008 年以降の政策を 3 つの時期に分け、サイバー空間の抑止力の概念の変化を詳述したい。第三章「抑止論の『刷新』の背景」では、サイバー抑止政策の変遷の背景、すなわち米国が認識するサイバー抑止成立の条件について触れたい。具体的には、サイバー空間の「アトリビューション」「レジリエンス」についてである。いずれも後述するが、「アトリビューション」とはサイバー攻撃の攻撃元を特定することであり、「レジリエンス」とはサイバー攻撃による被害を前提とし、データやシステムの早期復旧に焦点をあてる概念である。

1　サイバー空間の抑止論

1.1　国際安全保障と抑止

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・精緻化は冷戦期の核戦略の発展と密接に関連していた[4]。そのため、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、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、前述のとおり「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、その形態は様々である。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。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[5]。

そして、サイバー空間の抑止論で議論の焦点となってきたのは後者である。懲罰的抑止力の前提は、攻撃者を特定していることである。ところが、サイ

バー空間では攻撃者を即時に特定できない。米国防総省・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）ははっきりと言う。「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[6]」。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うえでは何ら重要な役割を果たさない[7]」。抑止研究の第一人者であるモーガン（Patrick Morgan）も「その（冷戦期の）抑止のもっと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[8]」という。

1.2　国際安全保障環境の変化と抑止論の「刷新」

サイバー空間では攻撃者を即時に特定できないため、懲罰的抑止は機能しないと考えられてきた。しかし、抑止論がこのような理論的・政策的な挑戦を受けたのは初めてではない。米ソ冷戦終結以降、冷戦期の核及び通常戦力で構成された懲罰的抑止論は大きな挑戦をうける。挑戦者はアル・カイダを始めとする国際テロ・ネットワークであり、高度に相互依存環境下での新興国（特に中国）の台頭であった。こうした国際安全保障環境の変化に対して、抑止の理論と政策は「刷新」されてきた。テロ・ネットワークに対しては、拒否的抑止力の再評価[9]や抑止概念を延伸した「先制行動（preemptive action）」への転換が提起された[10]。また、相互依存環境下における新興国（中国）の拡張主義的行動をいかに抑止するかという課題に対しては、「リベラル抑止」という概念が生み出された[11]。

１つの抑止モデルをあらゆる環境・脅威に適応するのではなく、おかれた

戦略環境や抑止対象の価値をふまえて抑止モデルを再構築することが求められる。つまり、「ワンサイズ（one size fits all）」ではなく、「テイラーメイド（tailor-made）」型の抑止が必要とされる[12]。

サイバー空間における抑止も、その戦略的環境をふまえて「刷新」されなければいけない。米サイバー軍（United States Cyber Command: CYBERCOM）司令官兼国家安全保障局（National Security Agency: NSA）長官・アレグザンダー（Keith B. Alexander）大将は、CYBERCOM が本格運用を開始する直前の議会で次のように述べている。「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[13]」。では、その後の米国におけるサイバー抑止はどのように刷新されてきたのだろうか。

2　米国におけるサイバー抑止政策の変遷

米国はサイバー空間を陸、海、空、宇宙に続く「第五の作戦領域」と位置づけ、外交・安全保障政策を展開している。オバマ政権は政権初の『米国家安全保障戦略 2010』で「デジタル・インフラストラクチャーは戦略的国家資産であり、この防衛は…中略…国家安全保障上の優先事項[14]」と位置付けた上で、その後の政策を形成してきた（表１）。

しかし、米国の外交・安全保障政策における「サイバー抑止」の概念は過去、一貫性のないものであった。言い換えれば、米国は国際安全保障環境の変化や技術的な革新をうけて、アレグザンダー大将がいうとおり「サイバー抑止」を刷新してきたのである。本章では米国のサイバー抑止政策を３つの時期に分けて詳述したい。時期については厳密ではないが以下のように整理できる（表２）。

2.1　第１期：2008 年～ 2011 年　「拒否的抑止力」への傾倒

米国の政策文書でサイバー抑止が最初に明示されたのは、ブッシュ政権で作成（2008 年１月）され、オバマ政権で公表（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）』であろう。CNCI はその具体的取り組みの

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、事案等（米国）

年月	主な政策文書、スピーチ、事案等
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（CNCI）』 ※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』
2009 年 6 月	CYBERCOM の設立指示（運用は 2010 年 5 月から）
2010 年 2 月	国防総省『四年毎の国防政策報告（QDR）2010』
2010 年 5 月	ホワイトハウス『米国国家安全保障戦略（NSS）2010』
2010 年 5 月	ホワイトハウス『サイバー空間における国際戦略』
2010 年 夏	イラン核関連施設への stuxnet 事件が発覚
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省戦略』
2011 年 11 月	国防総省『国防総省サイバー空間政策報告』（議会報告）
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
2013 年 2 月	マンディアント社が中国発のサイバー攻撃についての報告書を公表
2013 年 2 月	大統領令 13636 号および大統領政策指令 21 号に署名（重要インフラのサイバー攻撃対策などを明示）
2013 年 6 月	エドワード・スノーデンが機密を漏えい
2014 年 3 月	国防総省『四年毎の国防政策報告（QDR）2014』
2014 年 7 月	国務省国際安全保障諮問委員会『国際的なサイバー安定性の枠組みに関する報告』
2014 年 12 月	北朝鮮によるソニー・ピクチャーズ・エンターテイメント社へのサイバー攻撃が激化
2015 年 2 月	ホワイトハウス『米国国家安全保障戦略（NSS）2015』
2015 年 4 月	大統領令 13694 号に署名（サイバー攻撃に対する金融制裁措置を指示）
2015 年 4 月	国防総省『国防総省サイバー戦略』

（出典）筆者作成

表 2　米国のサイバー抑止政策の変遷

時 期	サイバー抑止力の構成要素
第 1 期（2008 ～ 2011 年）	拒否的抑止力
第 2 期（2011 ～ 2014 年）	拒否的抑止力 ＋ 懲罰的抑止力
第 3 期（2014 年～）	拒否的抑止力 ＋ 懲罰的抑止力 ＋ レジリエンス抑止力

（出典）筆者作成

1つとして「揺るぎない抑止戦略及びプログラムの構築・発展」を掲げたが、体系的な抑止政策を明示するに至らなかった[15]。

その背景にあったのは、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、という懸念である。ミサイルとは異なり、サイバー攻撃は発信源を即座に特定できない。サイバーセキュリティの専門家はこれを「アトリビューション」問題（attribution problem）という。 アトリビューションとは「行為の原因・因果関係を特定すること」と定義されるが、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、アトリビューションが複雑化する。こうしたサイバー空間の特徴により、報復を示唆することによる冷戦型の抑止は機能しないと考えられてきた。（第3章で詳述）

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。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」（2010年10月）に反映されている[16]。

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、これはCYBERCOMが掲げる重点分野の1つである[17]。『サイバー空間における作戦行動についての国防省戦略』（2011年7月）によれば、国防省は「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[18]。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）とされたが、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。インテリジェンス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。

2.2　第 2 期：2011 年～ 2014 年　「懲罰的抑止力」の再興

サイバー空間では即座に攻撃元を特定できないため、つまりアトリビューション問題ゆえ、米国のサイバー安全保障政策は懲罰的抑止力よりも拒否的抑止力に傾倒していた。しかし、サイバー空間の拒否的抑止力には生来的な問題がある。拒否的抑止が成立するためには、攻撃者に対して「攻撃が成功する期待」を引き下げることが重要である。しかし、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。こうした背景もあり、米国は懲罰的抑止力を追求することになる。

アレグザンダー大将から CYBERCOM 司令官と NSA 長官を引き継いだロジャース提督（Michael S. Rogers）は、2015 年 3 月 19 日の上院軍事委員会で次のような考え方を明かにした。2010 年以降活動している CYBERCOM は主に防衛に焦点を当てたものであり、「純粋に防衛的で、反応的な戦略は求められるものはなくなり、コストも信じられないくらい高騰するだろう [19]」。ただし、ロジャース提督がこのように振り返る前から懲罰的抑止力の必要性と構築が宣言されてきた。

米国がサイバー空間の懲罰的抑止力を明示的に宣言したのは、国防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）である。同報告は、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 [20]」。『サイバースペース政策報告』は国内向けの文書だが、米国のサイバー抑止態勢を明示するなど、ある種の宣言政策となっている側面もある。そのわずか 4 カ月前に公表された『サイバー空間における作戦行動についての国防省戦略』（2011 年 7 月）が抑止についてほとんど触れていないのとは対照的である。

懲罰的抑止力成立の阻害要因であったアトリビューション問題も一定の方向性を見出した。パネッタ国防長官（Leon E. Panetta）は 2012 年 10 月、懲罰的抑止力の重要性を指摘した上で、次のように述べた。

> 国防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年間で国防省は特定問題を解決するためのフォレンジック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[21]。

アトリビューション問題の「進展」として、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などが指摘されているが[22]、実態はよく分かっていない。

それでも、後にロジャース提督はCYBERCOM司令官指名の公聴会で、アトリビューション問題はあるものの、効果的な抑止態勢を構築できると証言した[23]。その3年前、リン副長官がアトリビューション問題故に、抑止が機能しにくいと論じた[24]ことと対照的である。

こうした懲罰的抑止力が機能するか否かは「報復」の信頼性が担保されているかどうかである。報復は、国際法上の自衛権行使の問題に関係する。現在、日米欧を中心に、武力攻撃に相当するようなサイバー攻撃は自衛権行使の要件となりうるという認識が広がりつつある[25]。

この問題に関する米国の姿勢は一貫していて、米国はサイバー攻撃に対する個別的および集団的自衛権を保有していることを宣言している[26]。そしてサイバー攻撃に対して、外交、情報、経済、軍事的な必要なあらゆる措置をとる権利を有し[27]、軍事的措置には、サイバー空間の軍事行動と現実世界の物理的能力（kinetic capabilities）のいずれか、あるいは双方を含むとしている[28]。

サイバー攻撃に対する報復措置がおこなわれた代表的な例は、2014年の米ソニー・ピクチャーズ・エンターテイメント（SPE）へのサイバー攻撃事件であろう。後に連邦捜査局（FBI）は、この攻撃はSPE社が制作したパロディ映画『ジ・インタビュー』の上映中止を求めて、北朝鮮が行ったものであると結論づけた。度重なるサイバー攻撃や社員への脅迫等を受け、同社は上映中止を決定した。ホワイトハウスのアーネスト（Josh Earnest）報道官は本件

を「深刻な安全保障問題」と位置づけ、2015 年 1 月 2 日、オバマ大統領は北朝鮮の人民武力部偵察総局等の 3 組織と 10 名の個人を新たに金融制裁の対象とする大統領令に署名した。

その後、サイバー攻撃への金融制裁措置は一般化される。4 月 1 日、新たな大統領令により、米国の国家安全保障、外交政策、経済を脅かす外国からのサイバー攻撃に対して、資産凍結、取引停止、渡航禁止等の制裁が実行可能となった。対象となるサイバー攻撃は重要インフラへの攻撃に加えて、商業的優位性を確保するためのエクスプロイテーション等が含まれる。

2.3　第 3 期：2014 年～ 「レジリエンスによる抑止力」の誕生

サイバー空間の抑止政策が確立されていく中、新たに「レジリエンスによる抑止（deterrence by resilience）」という概念が追加されつつある。上院議員ハート（Gary Hart）を議長とし、専門家によって構成される国務省国際安全保障諮問委員会は『国際的なサイバー安定性の枠組みに関する報告』（2014 年 7 月）の中で、サイバー空間の抑止力を次のように指摘している。効果的な抑止は、潜在的な攻撃者に対して、攻撃が失敗するまたは有用でないと思わせること（拒否的抑止）、耐えがたい損害を被ると思わせること（懲罰的抑止）、攻撃対象のアーキテクチャがレジリエントであると思わせること（レジリエンスによる抑止）から構成される [29]。また 2015 年 4 月に公表された『国防省サイバー戦略』も、抑止の中核的要素として、「報復（response）」「拒否（denial）」「レジリエンス（resilience）」の 3 つを掲げている [30]。

レジリエンスとは近年、国際安全保障やグローバルなリスクマネジメントの議論で強調される概念であり、その意味は攻撃や被害を前提にし、システムの早期復旧に焦点を当てるものだ。ここで重要なのは、国防総省のいうレジリエンス概念はその組織に限定されず、他の連邦機関や民間セクターを対象としている点である。『国防省サイバー戦略』によれば、

> 国防総省の能力は必ずしも全てのサイバー攻撃を拒否することを保証していないため、国防総省はレジリエントで冗長なシステムへの投資を行わなければいけない。その目的は、国防総省のネットワークが破壊的

または妨害的なサイバー攻撃を受けたとしても、機能を継続させるためである。しかし、国防総省はその管轄外の組織のレジエンスを強化することはできない。レジリエンスを効果的な抑止の要素まで引き上げるには、連邦政府の他の機関が重要インフラの所有者や運用者、より広範な民間セクターと連携し、潜在的リスクに耐えうるレジリエントで冗長なシステムを開発していく必要がある[31]。

こうした考え方の前提にあるのは、サイバー空間は米軍だけでは防衛できないという認識であろう。実際、米軍は民間のサイバー空間を防衛する機能を持つように変容しつつある。国防総省・米軍のサイバーオペレーションについては、CYBERCOM 下の 3 つの機能のサイバー任務部隊が担うが、その構成は①重要インフラなどの民間セクターの防衛を担う国家防衛（National Mission Force）、②米軍のネットワークの防衛を担うサイバー防衛（Cyber Protection Force）、③全世界の統合軍をサポートする戦闘支援（Combat Mission Force）である。2016 年までに CYBERCOM 要員を現行の約 1800 名（当時）から 3 倍超（約 6000 名）に引き上げ、133 を超えるサイバー任務部隊の運用が開始される。

現在、「レジリエンスによる抑止」の全体像はあまり分かっていない。だが、こうした米軍のネットワークと民間を含めたインフラストラクチャーの防衛と攻撃を受けた場合の被害管理が「レジリエンスによる抑止」の構成要素の 1 つであろう。

3　抑止論の「刷新」の背景

以上が、米国のサイバー空間における抑止政策の変遷である。ここでは抑止論が刷新された要因について検討してみたい。第一期から第二期への変遷の要因であるアトリビューション、第二期から第三期への変遷の要因であるレジリエンスをキーワードに検討する。

3.1　アトリビューション問題

サイバー空間で懲罰的抑止メカニズムが機能するか否かは、アトリビュー

ションに依存する。前述のとおり、アトリビューションとは「行為の原因・因果関係を特定すること」と定義されるが、その特徴は次のとおりである。

第一に、アトリビューションは白黒がはっきりする二者択一の問題ではなく、程度の問題である[32]。あるサイバー攻撃と国家・個人の行為の関係を明らかにする時、1つの事実をもってアトリビューションが判断されるのではなく、複数の事実を積み重ね、アトリビューションの程度が高まっていくということである。

第二に、アトリビューション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）と多岐にわたるが、問題となっているのは技術的アトリビューションよりも、政治的アトリビューションである。「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。「アトリビューション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[33]」。つまり、アトリビューション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。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。

2013年2月に米マンディアント社が発表した報告書『APT1』はアトリビューションを明かにした数少ない例であろう。同報告書は詳細な添付文書とともに、前例のない規模での米国へのサイバー攻撃（exploitation）の発信源が、上海の人民解放軍61398部隊であると指摘した[34]。だが、比較的アトリビューションが明確に公表された場合であっても、中国政府は「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[35]」と反論している。

アトリビューションの特徴をふまえて抑止成立の要件を整理すると、重要な点は「政治的アトリビューションの程度」についての国際的規範が形成できるか否かである。大西洋評議会のヒーリー（Jason Healey）はあるサイバー攻撃が国家による支援といえるかどうかを、「あるサイバー攻撃を特定の政府機関にまでさかのぼることができるか」「攻撃のコードは特定の言語でかかれ

ているか」「疑惑の国はサイバー攻撃の調査に協力的か」「サイバー攻撃は実際の物理的行動と関連しているか」等 14 の設問で判断しようとしている[36]。

ただし、「政治的アトリビューションの程度」を明かにするのは、軍よりもインテリジェンス機関の方が適切に対応できる[37]。こうした事情もあり、米国では CYBERCOM 司令官と NSA 局長が兼務しているといえる[38]。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[39]」が求められる。この点については、米国の政策は一貫している。

3.2　レジリエンス問題

近年、国務省や国防総省で提起されている「レジリエンスによる抑止」の背景にあるのは、①民間セクターの重要性、②サイバー攻撃を必ずしも防げないという認識である。

サイバー空間にしめる民間セクターの重要性はますます高まっている。『国家安全保障戦略（NSS）2010』や『四年毎の国防見直し（QDR）2010』等の米国の政策文書では、サイバー空間は「グローバル・コモンズ（global commons）」と位置づけられてきた。だが、サイバー空間は誰でもアクセスできるわけではなく、アクセスによって他の人のアクセスが制限されないわけでもない。海・空・宇宙といった自然のドメインとは異なり、サイバー空間は人工的ドメインである。我々がサイバー空間と呼ぶ時、実は相互接続された通信装置、通信チャネル、データストレージを指しているのであり、それは民間の所有物の複合体ともいえる[40]。それゆえ、『国家安全保障戦略（NSS）2015』ではサイバー空間を「コモンズ」ではなく、「共有された空間（shared space）」と位置づけた[41]。

サイバー空間は電力、上水道、運輸、医療・緊急サービス等の重要インフラを支える基盤であるとともに、それ自体が重要インフラである。こうした現実に基づいて、重要インフラ防衛が CYBERCOM の任務の 1 つとなっている。

「レジリエンスによる抑止」が現在提起されているもう 1 つの背景は、サイバー攻撃は完全に防げないという認識である。自律的で分散されたアーキテ

クチャを基本原理とするインターネット空間では、結果的に、攻撃者による優位性が形成されてきた。米国でオバマ政権が誕生後、オバマ大統領はサイバー空間の安全保障環境のレビューを命じた。この『サイバー空間政策レビュー』(2009 年 3 月) によれば、サイバー空間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、米国のシステムの重大な破壊を引き起こしうるものになっている」と総括している [42]。

「インターネットは消えゆく運命にある」。これは反インターネット主義者の主張ではなく、Google 会長のシュミット (Eric Schmidt) が 2015 年 1 月の世界経済フォーラムで発言したものである。その意味は、インターネットは社会インフラや生活機器など、我々の生活の隅々までに浸透し、インターネットを意識しなくなるということである。同じ意味で「サイバー攻撃は消えゆく運命にある」かもしれない。これは、サイバー攻撃の被害を受けることが常態になるという意味である。サイバー攻撃は日常の「風邪」のようなものであり、治療や早期復活も重要な対策なのである。すぐに修復されてしまうアーキテクチャをもっていれば、サイバー攻撃をしかけようというインセンティブは下がるだろう。このメカニズムは「攻撃成功の利益」が小さいという意味で拒否的抑止力と類似する部分もある。

現実問題として、サイバー攻撃を完全に防ぐことは不可能である。米国で確立しつつあったサイバー抑止論 (拒否的抑止と懲罰的抑止で構成される) は、この現実に対応するため、「レジリエンスによる抑止」を提起していると見ることができる。サイバー攻撃者にとっては、攻撃が成功しても、被害をほとんど与えられなければ、攻撃のインセンティブが下がるかもしれない。

おわりに

米国の外交・安全保障政策における「サイバー抑止」の概念と位置づけは過去、一貫性のないものであったが、それは米国が国際安全保障環境の変化や技術的な革新をうけて、サイバー抑止政策を刷新してきた結果である。今日では、サイバー抑止力の構成要素として、懲罰的抑止力と拒否的抑止力、

そしてレジリエンス抑止力が形成されつつある。

こうした米国のサイバー抑止政策の変遷は、サイバー空間の本来的な性質に関係する認識変化に基づいている。1つは、サイバー攻撃の発信源を即時に特定することが難しいというアトリビューション問題である。このアトリビューションに対する認識変化が、懲罰的抑止力の再興をもたらした。軍やインテリジェンス機関が攻撃者の「政治的アトリビューションの程度」を明かにすることで、懲罰的抑止力の信頼性は向上する。

もう1つは、サイバー空間では防御に対して攻撃が有利であり、サイバー攻撃の被害をうけることが常態化しつつあるという現実である。こうした認識に基づき、「レジリエンスによる抑止力」という概念が打ち出されている。レジリエンスの範囲は連邦政府だけでなく、まして国防総省・軍のネットワークだけでもなく、民間セクターのインフラを含むものである。社会全体のレジリエンス向上が抑止成立の要件と認識されつつある。

しかし、こうした米国の現状の抑止態勢をサイバー抑止政策の完成型と見るべきではなく、政策の変化過程の1つとみるべきである。将来の国際安全保障環境や技術革新は誰も予見することはできない。重要なことは、将来の環境に応じてサイバー空間の抑止論と抑止政策を「刷新」し続けることである。

注

[1] Robert Jervis, “Cooperation under the Security Dilemma,” *World Politics*, Vol. 30, No. 2, January 1978, pp.167-214.

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

[3] Jeffrey W. Knopf, “Three Items in One: Deterrence as Concept, Research Program and Political Issue,” in T. V. Paul, Patrick M. Morgan & James J. Wirtz, ed., *Complex Deterrence: Strategy in the Global Age*, Chicago: University of Chicago Press, 2009, p.37.

[4] 第二次世界大戦後の抑止論の発展には3つの大きな「波」があった。第一の波は核兵器登場後のブロディ (Bernard Brodie) やウォルファーズ (Arnold Wolfers) らの研究であり、核兵器の目的を戦争の抑止と位置づけたものである。第二の波は、シェリング (Thomas Schelling) に代表されるゲーム理論を用いて、合理的なアクター間で成立する抑止理論である。第三の波は合理的アクターを前提とする抑止論への批判であり、アクターの認識・認知・バイアスの重要性を主張した。Robert Jervis, “Deterrence Theory Revisited,” *World Politics*, Vol.31, No.2, January 1979, pp.289-324.

[5] 一般に抑止は「コストを課すこと」「利益を否定すること」の２つのアプローチで議論されるが、第３のアプローチも提起される。例えば、米国防省は抑止のメカニズムとして３点を挙げている。①利益を否定する抑止（Deterrence by Denying Benefits）、②コストを課す抑止（Deterrence by Imposing Costs）、③敵対者の自制を促す抑止（Deterrence by Encouraging Adversary Restraint）である。③は不作為による利益を敵対者に認識させ、自制を促すアプローチである。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；Joint Chief of Staff, Department of Defense, *Deterrence Operations Joint Operating Concept*, Version 2.0 December 2006, pp.24-28.　ただし、本稿では第三のアプローチとして、「レジリエンスによる抑止」を論じる。

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

[7] リチャード・クラーク、ロバート・ネイク（北川知子訳）『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。

[8] 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.75-76.

[9] 抑止論はアクター間の合理的計算を前提する。一般的にテロリストは合理的ではなく、抑止は機能しないと考えられていた。しかし、テロリストは自身の生命を惜しまないかもしれないが、決して非合理的な存在ではない。自身に与えられた使命を遂行するという意味で、テロリストは合理的な存在であり、テロリズムによる目的達成が困難な状況（例えば、自爆テロが成功する見込みがほとんどない状況など）を形成すればテロ行為は抑止できると考えられる。神保謙、高橋杉雄、古賀慶『日本の対テロリズム政策:多層型テロ抑止戦略の構築』東京財団研究報告書、2005 年 2 月。

[10]「先制行動」は自衛権に基づく行動であり、抑止が失敗する前に先制的に行動し、危険を取り除くという考え方・戦略である。George W. Bush, Jr., *The National Security Strategy of the United States of America*, Washington D.C.: The White House, March 2006, p.18.

[11] 植木(川勝)千加子「世界構造変動と日米中関係:『リベラル抑止』政策の重要性」『国際問題』No. 586、2009 年 11 月、16-17 頁。

[12]「テイラーメイド型抑止」のアイデアは米国防省のヘンリー（Ryan Henry）に求められる。神保 謙「安全保障」、日本国際政治学会編『学としての国際政治』日本の国際政治 1、有斐閣、2009 年、142-144 頁。

[13] Statement of Gen. Keith B. Alexander, Commander United States Cyber Command, Before the House Committee on Armed Service, September 23, 2010.

[14] Barak Obama, *National Security Strategy of the United States 2010*, Washington D.C.: White House, May 2010, pp.27-28.

[15] The White House, *Comprehensive National Cybersecurity Initiatives*, Washington D.C.: White House, March 2, 2010.

[16] William J. Lynn, III, “Defending a New Domain: The Pentagon’s Cyberstrategy,” *Foreign Affairs*, Vol.89, No.5, September/October 2010, pp.99-100.

[17] CYBERCOM は５つの戦略を掲げる。(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。Alexander, *Op. Cit.*

[18] Department of Defense, *Department of Defense Strategy for Operating in Cyberspace,*

July 2011, p.7.
[19] Ellen Nakashima, “Cyber chief: Efforts to deter attacks against the U.S. are not working,” *The Washington Post*, March 19, 2015.
[20] 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.
[21] Secretary of Defense Leon E. Panetta, Remarks on Cybersecurity to the Business Executives for National Security, New York City, October 11, 2012.
[22] Department of Defense, *Department of Defense Cyberspace Policy Repor*t, pp.4-5.
[23] Advanced Questions for Vice Admiral Michael S. Rogers, USN, Nominee for Commander United States Cyber Command, March 11, 2014.
[24] Lynn, “Defending a New Domain,” pp.99-100.
[25] サイバー攻撃への自衛権行使の前提は、国連憲章第 51 条（自衛権）を含む既存の国際法体系がサイバー空間に適応されることである。米国は『サイバー空間の国際戦略』（2011 年 5 月）などで、サイバー空間の新たな条約や法の「再発明」は不要であり、既存の法体系を適用すべしとの立場をとっている。一方で、中国やロシアはサイバー空間に新しい行動規範を構築すべきだと考え、対立が生じている。サイバー攻撃と自衛権に関する詳細は、川口貴久「民間セクターへのサイバー攻撃と自衛権：重要インフラ攻撃とグレーゾーン事態」、公益財団法人 日本国際問題研究所編『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』平成 26 年度外務省外交・安全保障調査研究事業、2015 年 5 月、11-26 頁。
[26] 米国は「サイバー空間を通じた特定の悪意ある行為が軍事的取極めを結ぶパートナーとのコミットメントを発動させる」と明言している。The White House, *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World*, May 2011, p.14.
[27] *Ibid*.
[28] Department of Defense, *Department of Defense Cyberspace Policy Report*, p.4. こうした物理的能力には核戦力を含むという見解もある。国防総省諮問機関である国防科学委員会はサイバー攻撃への抑止力として核戦力を維持すべし、と勧告している。Defense Science Board, *Task Force Report: Resilient Military Systems and the Advanced Cyber Threat*, January 2013, pp.40-43.
[29] International Security Advisory Board, United States Department of State, “Report on A Framework for International Cyber Stability” July 2, 2014, pp.10-11. この提言では deterrence by resilience という用語が用いられている。
[30] The Department of Defense, *The DoD Cyber Strategy*, April 2015, pp.10-11.
[31] *Ibid*.
[32] Thomas Rid and Ben Buchanan, “Attributing Cyber Attacks,” *The Journal of Strategic Studies*, Vol.38, No.1-2, 2015, pp.4-37.
[33] 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, p.39.
[34] Mandiant, *APT1: Exposing One of China’s Cyber Espionage Units*, February 2013.
[35] 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>
[36] Jason Healey, eds., *A Fierce Domain: Cyber Conflict, 1986 to 2012*, Vienna: Cyber

Conflict Studies Association, 2013, pp.266-272.
[37] 土屋 大洋「サイバーセキュリテイとインテリジェンス機関：米英における技術変化のインパクト」『国際政治』第 179 号、2015 年 2 月、44-56 頁。
[38] 両役職の兼務は所与のものはない。アレグザンダー大将の後任であるロジャース提督の指名にあたり、スノーデン事件の影響もあり、CYBERCOM 司令官と NSA 長官の兼務を解くべし、との意見も根強かった（結果的には兼務となった）。
[39] Lynn, “Remarks at STRATCOM Cyber Symposium,” May 26, 2010.
[40] 土屋 大洋『サイバーセキュリティと国際政治』千倉書房、2015 年。
[41] Barak Obama, *National Security Strategy of the United States*, Washington D.C.: White House, February 2015, pp.12-13.
[42] White House, *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure* (May 2009), iii.

参考文献

植木（川勝）千加子「世界構造変動と日米中関係：『リベラル抑止』政策の重要性」『国際問題』No. 586、2009 年 11 月、15-28 頁。
川口 貴久「サイバー戦争とその抑止」土屋 大洋（監修）『仮想戦争の終わり：サイバー戦争とセキュリティ』角川インターネット講座第 13 巻、KADOKAWA、2014 年、279-315 頁。
川口 貴久「民間セクターへのサイバー攻撃と自衛権：重要インフラ攻撃とグレーゾーン事態」、公益財団法人 日本国際問題研究所編『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』平成 26 年度外務省外交・安全保障調査研究事業、2015 年 5 月、11-26 頁。
クラーク，チャード、ロバート・ネイク（北川 知子訳）『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。
神保 謙・高橋 杉雄・古賀 慶『日本の対テロリズム政策：多層型テロ抑止戦略の構築』東京財団研究報告書、2005 年 2 月。
神保 謙「安全保障」日本国際政治学会編『学としての国際政治』日本の国際政治 1、有斐閣、2009 年、131-150 頁。
土屋 大洋「サイバーセキュリティとインテリジェンス機関：米英における技術変化のインパクト」『国際政治』第 179 号、2015 年 2 月、44-56 頁。
土屋 大洋『サイバーセキュリティと国際政治』千倉書房、2015 年。
土山 實男『安全保障の国際政治学：焦りと傲り』有斐閣、2004 年。

Boebert, W. Earl, “A Survey of Challenges in 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.41-52.
Clark, David D., and Susan Landau, “Untangling Attribution,” in *Proceedings of a Workshop on Deterring Cyberattacks*, pp.25-40
Healey, Jason, eds., *A Fierce Domain: Cyber Conflict, 1986 to 2012*, Vienna: Cyber Conflict Studies Association, 2013, pp.266-272.
Jervis, Robert, “Deterrence Theory Revisited,” *World Politics*, Vol.31, No.2, January 1979, pp.289-324.
Kahn, Robert E., “The Role of the 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.203-216.

Knopf, Jeffrey W., "Three Items in One: Deterrence as Concept, Research Program and Political Issue," 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.31-57.

Lynn, William J., III, "Defending a New Domain: The Pentagon's Cyberstrategy," *Foreign Affairs*, Vol.89, No.5, September/October 2010, pp.97-108.

Morgan, Patrick M., "Applicability of Traditional Deterrence Concepts and Theory to the Cyber Realm," in *Proceedings of a Workshop on Deterring Cyberattacks*, pp.55-76.

Nakashima, Ellen , "Cyber chief: Efforts to deter attacks against the U.S. are not working," *The Washington Post*, March 19, 2015.

Rid, Thomas, and Ben Buchanan, "Attributing Cyber Attacks," *The Journal of Strategic Studies*, Vol.38, No.1-2, 2015, pp.4-37.

〔受付日　2015. 7. 31〕
〔採録日　2015.12.18〕