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

「サイバー空間の安全保障をめぐる課題とアメリカの動向」

川口貴久 *

1. 争点化するサイバーセキュリティ

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。2013 年 6 月のアジア安全保障会議で、ヘーゲル（Chuck Hagel）米国防長官がこのように指摘した。続く米中首脳会談でも、オバマ（Barack Obama）大統領が習近平（Xi Jinping）国家主席に同様の懸念を伝えた。サイバーセキュリティが米中間の主要アジェンダとなっている。背景にあるのは、激化するサイバー空間を通じた剽窃活動である。米民間セキュリティ会社マンディアント（Mandiant）による報告書（2013 年 2 月）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。またワシントンポスト紙の報道（2013 年 5 月 28 日）では、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。

こうした中国発のサイバー攻撃は平時のスパイ活動・エクスプロイテーション（exploitation）としてのみならず、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付けられている。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。攻撃は米軍の即応展開・兵站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。

このような戦略環境をふまえ、アメリカ政府は連邦予算が「強制削減」される中、サイバー関連予算を維持・増加し、米統合軍サイバー軍司令部（CYBERCOM）の要員を 5 倍に増やすなど、サイバーセキュリティ分野に投資を行っている。

2.「帰属問題」と抑止メカニズムの限界性

サイバーセキュリティ分野への投資にも関わらず、残された課題は大きい。その 1 つは、サイバー攻撃の発信源を即座に断定することが出来ない（困難である）という点である。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。 “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、使用された端末/サーバの所有者、行為主体が国境を超えるため、帰属が複雑化する。帰属問題とは簡単に言えば「誰がやったか分からない」状態を指す。帰属問題の所在はインターネットの構造（特に IP レベル）、マルウェア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

* 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）。

岐にわたる。

そして「帰属問題」がもたらす安全保障上の帰結は重大であり、「抑止（deterrence）」に関するものである[1]。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」事であり、その一般的なモデルは、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（deterrence by punishment））」である。こうした抑止モデルは、第二次世界大戦以降の国際安全保障の中心的メカニズムである。

しかし、サイバー空間のように攻撃元を特定できなければ、懲罰的・報復的な抑止メカニズムは機能しない。国防省・米軍でのサイバーセキュリティ対策の強力な推進者であり、オバマ政権で国防副長官を務めたリン（William J. Lynn）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。（2010年5月26日、STRATCOMサイバーシンポジウム）

その一方で、こうした見方は「帰属」を重視し過ぎていると言える。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）を追求すれば事足りるという事である。サイバー空間におきかえれば、技術的な帰属（technical attribution）よりも、攻撃の責任（responsibility of attack）を特定することが重要である。

3. サイバー空間における懲罰的抑止力の追求

影響の程度に議論はあるが、帰属問題は抑止メカニズムに負の影響を与えている。では、サイバー空間では抑止メカニズムは破たんしているのであろうか。アメリカの防衛・安全保障政策ではどのように位置付けられているのだろうか。

2010年末頃までの米国防省の見解は、リン国防副長官の先ほどの発言と同様、以下のとおりであった。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。後者は主にリアルタイムでの攻撃検知システムを指し、CYBERCOMが掲げる「積極的なサイバー防衛（active cyber defense）」という考え方に通ずるものである。

---

[1] 「帰属問題」だけが、抑止メカニズムに影響を与えているわけではない。サイバー空間の他の特徴、つまり①「サイバー戦争」「サイバー武力攻撃」をいつ/どのように認定するかという共通認識がないこと（閾値問題、threshold problem）、②サイバー空間では防御に対して攻撃側が有利であること（攻撃優位のアーキテクチャ）、③アクター間の資源・パワーやサイバー空間への依存度の非対称性も抑止メカニズムを機能しにくくしている。

しかしながら、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、かねてより懲罰的抑止の必要性が訴えられてきた。それゆえ、現在ではサイバー空間で拒否的抑止力と懲罰的抑止力の双方を追求する試みが進んでいる。2011年11月、国防省が議会に提出した「サイバー空間政策報告（Department of Defense Cyberspace Policy Report）」では、「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」との見方を示している。より決定的なのは、2012年10月のパネッタ国防長官（Leon E. Panetta）のスピーチである。

> 国防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［筆者注：懲罰的抑止力］、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［筆者注：拒否的抑止力］、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。（2012 年 10 月 11 日、ニューヨーク）

パネッタがいう「進展」の具体的内容については不明だが、物理的攻撃元の追跡手法、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）の向上、省庁横断・国際的な情報共有システム、ビッグデータを用いた分析・予測を含んでいるだろう。

更に言えば、こうした特定能力に基づく報復は、サイバー空間に限定されない「ドメイン横断」型である。すなわち、サイバー攻撃に対して陸海空宇宙といったドメインでの物理的能力（kinetic capabilities）による対応オプションを含んでいる（国防省「サイバー空間政策報告」）。こうした報復オプションには、核戦略を含めるべし、という見解もある。

4．日米同盟の新しい課題

「帰属問題」は重大な課題であるものの、アメリカではサイバー空間における懲罰的抑止力の模索が進展している。既にアメリカの同盟ネットワークでも、拡大抑止のメカニズムにサイバー攻撃対処を取り組む方向である。例えば、2011 年 9 月、米豪2＋2は「領土保全、政治的独立性、米豪の安全保障を脅かすようなサイバー攻撃」は ANZUS の集団的自衛権行使の対象である点を確認した。

日米同盟でもサイバーセキュリティは重要なアジェンダとして認識されつつある。2011 年 6 月の日米2＋2ではサイバーセキュリティが「共通の戦略目標」であると初めて明示され、2013 年 5 月からは日米サイバー対話が始まった。しかし、日米がサイバー空間で抑止力をどのように構築するかの議論は道半ばである。この議論を進めるとともに、それに伴う法的基盤の構築とオペレーションでの整備が必要である。

2013 年 8 月 1 日