サイバー戦争の革命性
――「スタックスネット」を事例に――

千草　歩実
（宮岡研究会４年）

はじめに

現在、情報技術の急速な発展につれて、国際社会経済のサイバー空間への依存が進んでいる。そのため、各国の重要なコンピュータ・ネットワークやインフラストラクチャーはますます魅力的な標的となり、サイバー技術を悪用した行為も増加傾向にある。例えば、2014年にはソニー・ピクチャーズ・エンタテインメントに対するハッキング事件があった。攻撃側は膨大な数の機密文書を盗み、インターネット上に投稿した[1)]。それにより、直近の映画製作に関する詳細から従業

員の個人情報まであらゆるデータが漏洩した。また、2019年には北朝鮮が銀行や仮想通貨取引所に対してサイバー攻撃を加え、最大約2,100億円を違法に取得した[2)]。

一方、このようなサイバー活動が目立つようになり、各国政府もサイバー政策の整備にこれまでになく力を入れている。2019年４月に行われた主要７カ国外相会合では、デジタル防衛が論点となり、「サイバー規範イニシアチブに関するディナール宣言」が採択された[3)]。そして、日本国内でも半導体チップなどを使う「埋め込み型」のスパイ行為を排除するための官民協力が模索され始めた[4)]。サイバーセキュリティが多くの国々にとって大きな関心ごととなっている今、これからも進化し続けるサイバー技術とその国家安全保障戦略における役割の検討が重要性を増している。

そこで、本研究では、サイバー戦争の革命性に焦点を当てる。ところが、サイバー戦争に関する主要な命題の再検討を通して、これまでの研究の過度に悲観的な傾向を指摘し、サイバー戦争は革命的ではないと主張している先行研究も存在する。しかし、それは具体的な事例による理論の立証を欠いていた。

これを踏まえて、本研究では「サイバー戦争が革命的ではないという主張は、現実的な事例と照らし合わせた場合にも妥当なのか」を研究の問いとして設定する。そして、「サイバー戦争は革命的である」という仮説を検証する。

研究の方法としては、事例研究による。これにあたり、事例として2010年のイラン・ナタンツの核施設に対するサイバー攻撃を採用する。利用する資料およびデータは、関係機関がまとめた報告書や米国の有力紙の記事を中心に、サイバー戦争を題材にした論文などの２次資料を含む。

最後に、本研究の構成を説明する。第Ⅰ章では、サイバー戦争の概要を説明し、先行研究の批判的考察と問題提起を行い、仮説と構想を設定する。また、鍵概念の定義も整理する。第Ⅱ章では、事例研究を通して仮説を検証し、研究の問いを考察する。なお、仮説の検証においては、サイバー戦争に関する四つの主要な命題が実際にあったサイバー攻撃においてどのように作用したかに着目する。まとめとして、本研究の結論を踏まえて、理論的含意と政策的含意、そして今後の研究課題について述べる。

Ⅰ　問題提起とアプローチ

本章では、サイバー戦争の革命性に関する先行研究の批判的考察と問題提起を行い、本研究の仮説と構想を設定する。第１節では、サイバー戦争の概要をまとめる。第２節では、先行研究の批判的考察と問題提起を行う。第３節では、仮説と研究方法を述べる。

１　サイバー戦争の概要

サイバー戦争の革命性について研究するにあたり、まず、サイバー技術の定義と戦争に与える影響を説明する。サイバーとは、コンピュータとインターネットに関わるものの総称である[5)]。これは、コンピュータなどのハードウェアや無形なネットワークに加えて、戦略論や法的問題などの幅広い事柄を含む。その一要素がサイバー技術である。サイバー技術は、コンピュータ技術とネットワーク技術の総称であり、日々発達しながら、現代の社会経済活動だけでなく軍事にも大きな影響を与えている。

多くの軍隊が積極的にサイバー技術を取り入れているのは、戦争を効率化できるからである。例えば、通信システムは軍隊の様々な通信用機材を相互に連接し、異なる場所にいる兵士がお互いに情報を共有したり、効率的に目標を配分できる。それにより、肝要な場所に戦力を集中させて、戦勝を得られる。

軍隊がサイバー技術を利用すれば、戦争の姿も多少なりとも変化する。サイバー技術が戦争に与える影響は、主に以下３点においてである[6)]。第一に、サイバー技術は交戦距離を無限大に広げる。インターネットに接続していれば、世界中どこにいる敵でも攻撃できる。第二に、新しい戦闘方式を提供する。自分のシステムを守りながら、同時に敵のシステムを攻撃することができる。第三に、新しい戦場を追加する。米国国防総省の戦略ドクトリンはサイバー空間を戦闘領域として認識し、サイバー防衛、回復力、およびサイバー能力の軍事作戦への全範囲的かつ継続的な統合に投資するとしている[7)]。

次に、サイバー戦争とはどのようなものなのか。サイバー戦争の定義はまだはっきりとしておらず、様々な説がある。例えば、クラーク（Richard Clarke）元米国サイバーセキュリティ担当大統領特別顧問は、サイバー戦争は「損害または混乱をもたらす目的で、国家が別の国家のコンピュータもしくはネットワークに

侵入する行為（訳は引用者による）」であるとしている[8]。一方、ナイ（Joseph Nye）元米国国防次官補は、サイバー戦争を「大きな物質的暴力を増大させる、ないしはそれに匹敵する効果をもたらす、サイバー空間における敵対行動（訳は引用者による）」と定めている[9]。両者の定義付けには、細部は違えど、対立している当事者が何かしらの政治的・戦略的な目的でサイバー技術を利用しているという共通点がある。

最後に、サイバー技術が重要な役割を果たした国際的対立の事例を紹介する[10]。例えば、2006年のレバノン侵攻では、シーア派系イスラム教徒の政治組織であるヒズボラがサイバー技術を活用して情報環境を支配した。また、2007年には世界中の数百万台のコンピュータがボットネットとして利用されたため、エストニアの銀行および行政システムが停止した[11]。同様に、2008年の南オセチア紛争では、ジョージアの政府・省庁が大規模な分散型サービス妨害攻撃（distributed denial-of-service attack、以下 DDoS 攻撃）を受けた[12]。しかし、これらの事件はいずれもサイバー戦争にまで至ってはいない。

2　先行研究の批判的考察

サイバー戦争の革命性に関する先行研究としては、リフ（Adam Liff）著「サイバー戦争：新しい「絶対的な兵器」？　サイバー戦争能力の拡散と国家間戦争」（2012年）がある[13]。この論文において、リフは、サイバー戦争は革命的ではないと主張している。この主張のために、以下の通りに議論を展開している。

まず、筆者はサイバー戦争の定義付けをしている。サイバー戦争は「二者以上の間の政治的交渉過程の一部としての戦争（訳は引用者による）」の性質を持ち、サイバー空間に制限されるものではないことを強調している。手段としては、コンピュータ・ネットワーク・オペレーション、コンピュータ・ネットワーク攻撃（以下 CN 攻撃）、そしてコンピュータ・ネットワーク防御（以下 CN 防御）を含む。

これを踏まえて、先行研究はサイバー技術の拡散による戦争への影響について議論を進めている。筆者は、サイバー戦争に関する四つの主要な命題の再検討を通して、サイバー技術の拡散による戦争への影響は小さいことを証明する。第一に、非対称性である。これまでの研究では、CN 攻撃はコストと参入障壁が低く、標的までの距離を短縮するため、通常戦力における格差を均一化するとされてきた。しかし、CN 攻撃を開発する資源は強国にしかなく、その戦略的計算は交渉による解決を好むから、非対称性は戦争の増加には繋がらないと筆者は言う。

第二に、攻撃優位性である。CN 防御のコストは高く、サイバー戦争では攻撃に要する時間が短縮されるため、攻撃側が優位であるとされてきた。しかし、これにより通常戦力における勢力関係が変化することはないに等しいから、国家間戦争に対するサイバー技術の影響は限定的であるとリフは考える。

第三に、匿名性（plausible deniability）である。サイバー戦争では、攻撃元の特定が難しいため、攻撃側は報復を恐れない。そして、攻撃元の誤った特定とエスカレーションにより、戦争は増加するとされてきた。しかし、戦争には政治的・戦略的な目的があり、攻撃側は自己識別をしなければ強制力がない。よって、国際システムの安定に対するサイバー技術の影響は小さいと筆者は言う。

第四に、サイバー抑止の無効性である。攻撃元の特定、CN 防御の開発、そして軍備管理協定の締結が難しいため、サイバー抑止は無効であるとされてきた。しかし、CN 攻撃が及ぼしうる危害には不確実性がある。加えて、サイバー抑止が効くか否かは、主体が運用できるサイバー技術のみならず、高い紛争レベルにおける報復能力にも従属する。よって、サイバー抑止は機能するとリフは考える。

この先行研究は、サイバー戦争に関する主要な命題の再検討を通して、これまでの研究の過度に悲観的な傾向を指摘している。サイバー技術の拡散による影響は小さく、サイバー戦争は革命的ではないと主張している。筆者は、冷静にサイバー戦争の発展性について論じており、理論の構築において非常に包括的である。

しかし、この先行研究には二つの疑問がある。まず、政策的含意が欠如している。築き上げた理論をもとに、国家がどのような対策を練る必要があるのかを提案できていない。国家がどのような相手を想定し、どのように準備をするべきなのかについて、今後の政策的な展望を見据えることをしていない。次に、具体的な事例による理論の立証をしていない。例えば、CN 攻撃により通常戦力における勢力関係が変化することは実際にないと言えるのか。提唱する理論の根拠を提示できていないため、信憑性が低くなっている。

これら二つの疑問のうち、本研究ではサイバー戦争が革命的ではないと言える証拠に着目し、「サイバー戦争が革命的ではないという主張は、現実的な事例と照らし合わせた場合にも妥当なのか」を研究の問いとして設定する。

3　研究構想

本研究の仮説は「サイバー戦争は革命的である」とする。その理由としては、以下 4 点が挙げられる。第一に、CN 攻撃は非対称兵器であり、通常戦力の格差

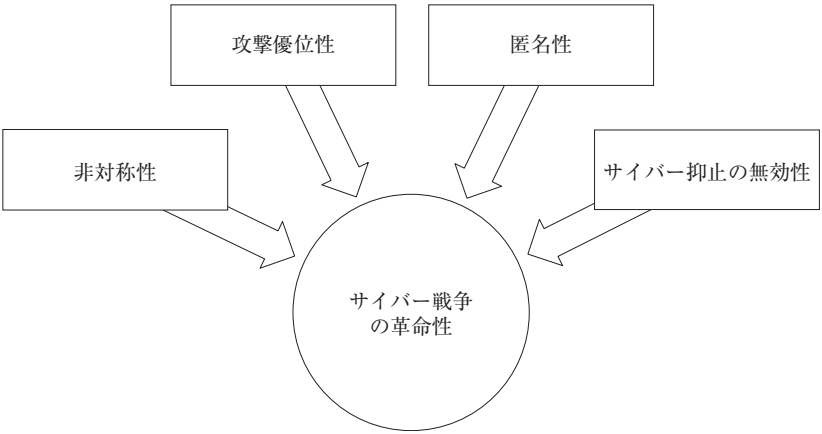
を均一化できる。第二に、攻撃に要する時間の短縮と困難なCN防御が攻撃側に優位性を与える。第三に、攻撃元の特定が難しいサイバー戦争では、攻撃側の報復に対する恐怖が減少する。第四に、匿名性と攻撃優位性により、サイバー抑止は無効となる。

この仮説に対し、本研究では事例研究による検証を試みる。サイバー活動は、形態と目標ともに非常に広範囲にわたる。例えば、2007年のエストニアに対するサイバー攻撃や2014年のソニー・ピクチャーズ・エンタテインメントに対するハッキングなどが挙げられる。しかし、これらの活動は、DDoS攻撃による妨害行為とデータ抽出を目標としたサイバー搾取とにあたり、厳密にはサイバー戦争ではなかった[14]。そこで、事例選択においては、サイバー技術が政治的・戦略的な目的を以って利用されたことを条件にした。よって、本研究では2010年のコンピュータ・ワーム「スタックスネット」によるイラン・ナタンツの核施設に対するCN攻撃を事例として採用する[15]。

続いて、事例研究にあたり鍵概念の定義を整理する。まず、サイバー戦争の性質である。第一に、非対称性である。非対称性とは、低い参入障壁により、通常戦力において弱い主体が強い国家を脅かすことができる状態を指す[16]。第二に、攻撃優位性である。攻撃優位性とは、自分を守るよりも相手の部隊を滅ぼす方が容易である状態を指す[17]。それとは反対に、防御優位性とは、相手の部隊を滅ぼすよりも自分を守る方が容易である状態を指す。ちなみに、攻撃防御バランスは、目的を果たすために必要な攻撃側のコストと防御側のコストとの比率により計測できる[18]。第三に、匿名性である。匿名性とは、攻撃側の責任を証明することが困難な方法により、標的に対してCN攻撃を加えられる能力を表す[19]。第四に、サイバー抑止である。一般的に、抑止とは、敵に望ましくない行為を始めることを思い留まらせるための脅威の使用である[20]。ただし、サイバー抑止の定義はまだはっきりとしていない。先行研究はサイバー抑止を「攻撃側と防御側の両者が特定されていて、より高い紛争レベルへのエスカレーションが可能な政治的交渉における抑止」としているが、それとは異なる考え方も多く存在する[21]。例えば、懲罰的抑止や拒否的抑止といった区別に加え、サイバー抑止をサイバー攻撃に対する抑止とする場合と通常攻撃に対するサイバー手段による抑止とする場合とでは、効果の有無が変わるかもしれない。

次に、仮説に含まれている「革命的」の意味である。「軍事革命」の定義についても様々な見解があるが、本研究では、サイバー戦争に関する四つの主要な命

図１　仮説に関するアロー・ダイアグラム



出所：筆者作成

題がいくつ立証されたかに応じてサイバー戦争の革命性を判断する。命題がどれも立証されなかった場合は、サイバー戦争の革命性を０％とする。それに対して、命題が全て立証された場合は、サイバー戦争の革命性を100％とする。つまり、命題が一つ立証されるごとにサイバー戦争の革命性は25％上がる。

最後に、利用する資料およびデータを紹介する。攻撃の方法や効果に関する情報の収集は、科学国際安全保障研究所などの機関がまとめた報告書をもとにする。一連の政治的な背景や余波については、ニューヨーク・タイムズやワシントン・ポストなどの新聞記事を参考にする。また、サイバー戦争を題材にした論文などの２次資料も含む。

Ⅱ　事例研究――スタックスネット

本章では、事例研究を通して本研究の仮説を検証し、研究の問いを考察する。第１節では、スタックスネットの概要をまとめる。第２節から第５節では、事例と照らし合わせて、サイバー戦争に関する四つの主要な命題を分析する。第６節では、研究の問いを考察する。

1　スタックスネットの概要

事例として、イランの核施設を攻撃したスタックスネットと呼ばれるコンピュータ・ワームを取り上げる。概要については、攻撃の理由、手段、そして成果に着目する。

まず、スタックスネットによるCN攻撃に至った理由である。2006年から2008年にかけて、国際連合の安全保障理事会はイランに対してウランの濃縮と再処理を停止するよう繰り返し要求していた。例えば、2008年の決議第1803号では、イランが全ての濃縮および再処理の活動を停止しなかったとして、常任理事国は交渉においてより具体的な措置を取ることを厭わないと強調されていた[22)]。しかし、イランは協力しなかった。

これを受けて、米国とイスラエルはイランの核武装化を遅らせるための軍事的な選択肢を検討し始めた。当時、イランのウラン濃縮プログラムで最も重要な施設とされていたのはナタンツだった。ナタンツは、2007年に生産工程を開始した。地下には二つの生産ホールがあり、50,000もの遠心分離機を収容できた[23)]。当初は、この地下生産ホールを空爆することが一つの措置として挙げられていた。しかし、これには多くの死傷者と深刻な外交的余波のリスクがあったため、米国の戦略家はより消極的な代案を模索した。その結果、彼らはナタンツのウラン濃縮プログラムを操作する産業用制御システム（industrial control system、以下ICS）を標的にCN攻撃をすることにした[24)]。

次に、攻撃の手段について説明する。ナタンツのICSネットワークはインターネットに接続されていなかったので、コンピュータ・ワームを物理的に挿入しなければならなかった。そのため、感染はICS機器を扱っているイラン国内の企業の従業員がスタックスネットを収容したメディアを受け取り、ICSネットワークに直接挿入したことで広まったとされている[25)]。

ICSに接続された機器にコンピュータ・ワームが挿入されると、自動化された攻撃プロセスが始まる。スタックスネットのツールキットは、ナタンツの核施設を標的にカスタマイズされていた[26)]。これにより、スタックスネットは遠心分離機の周波数変換器を制御するICSに接続し、攻撃を始めた[27)]。周波数変換器に遠心分離機の速度を15分間1,410 Hz（最大値）まで上げ、27日間1,064 Hz（通常値）に戻し、50分間2 Hz（ウラン濃縮には遅すぎる）まで下げ、また27日間1,064 Hzに戻し、これを無限に繰り返すように指示し、遠心分離機を慢性的に疲労させた

のである[28)]。

しかし、ナタンツでのウラン濃縮プログラムにそれなりの危害を加えるには、スタックスネットはICSを攻撃した数ヶ月間にわたって隠れたままでいなければならなかった。そのため、スタックスネットはICSには誤った指示を送りながら、異常を知らせる警告をオペレーターから隠し、正常のフィードバックを偽装していた[29)]。つまり、「中間者攻撃」（man-in-the-middle attack）を行っていたのである[30)]。

最後に、攻撃の成果についてである。長年にわたり、各国政府はイランの核武装化を妨げるための方法を模索してきた。米国とイスラエルの目標がナタンツの核施設にある遠心分離機を全て破壊することだったのであれば、スタックスネットによるCN攻撃は失敗に終わったと言える。一方で、目標が限られた数の遠心分離機を破壊し、ナタンツにおけるウラン濃縮プログラムをただ疲弊させることだったのであれば、成功したと考えられる[31)]。

2　非対称性

まず、サイバー戦争の非対称性を判断するために、上述の事例を四つの視点から分析する。

第一に、諜報能力である。スタックスネットによるCN攻撃を成功させるためには、情報工学、原子力工学、そしてICSに関する高度な専門知識が必要であった[32)]。特にICSについては、ナタンツにおけるネットワークの構成や周辺機器に加え、それに制御されているウラン濃縮プロセスに関する幅広い情報を収集しなければならなかった。現に、2012年のワシントン・ポストの記事によると、米国とイスラエルは2000年代半ばからすでに諜報活動に労力と資金を投資していたとされている[33)]。

第二に、工学的能力である。ナタンツにおけるCN防御を打破するためには、二つのゼロデイ脆弱性を同時に利用できるマルウェアを開発しなければならなかった[34)]。だが、そのような仕組みは、メーカーにより対策が講じられていないソフトウェアの弱点を見つけて悪用するため、作成が非常に難しい[35)]。そこで、開発者らは、マルウェアが意図した通りに作動するか否かを2003年にリビアのカダフィ（Muammar Gaddafi）大佐が核兵器計画を放棄した際に受け取った古い遠心分離機を実験台に試した[36)]。これらの遠心分離機は、イランの核施設にあるものと同様に、パキスタンのカーン（Abdul Khan）博士により販売されていたもの

であった。試験は、米国内の複数の異なる国立研究所で実施された。

第三に、人員の確保である。スタックスネットが目的を果たすためには、数年間にわたる攻撃の計画、資金調達、そして監視が必要だった。あるヨーロッパの諜報機関は、スタックスネットの開発に少なくとも3年はかかったと推測している[37)]。この準備段階においては、多数の複雑な計画を統合しなければならなかった[38)]。また、攻撃が始まれば、緊迫性のあるミッションにミスなく対応できなければならなかった。そのため、米国はこれらの業務を難なく遂行できる人員を揃え、計画の立案や管理、指揮などを任せた。

第四に、保険としての通常戦力である。米国とイスラエルには、スタックスネットによるCN攻撃が失敗した場合の保険として通常戦力があった。これは、イランの核武装化を遅らせるための措置として、最初は空爆が検討されていたことにより示されている[39)]。強力な国家は作戦の失敗という戦略的リスクを管理するのに優れている。匿名性の消失や標的ミスなどの緊急事態において、強力な国家はさらなる措置を講じるための資源と力をより多く保持している。

このように、スタックスネットによるCN攻撃が成功するためには、綿密な計画と多大な資源が必要だった。CN攻撃は組織的基盤と資源的余裕とを要し、これらは強力な国家にしかない。よって、CN攻撃が単独で通常戦力におけるバランス・オブ・パワーを均一化することはなく、依然として強力な国家が有利であると言える。

3　攻撃優位性

次に、スタックスネットの事例における攻撃優位性の有無を三つの視点から分析する。

第一に、匿名性の重視である。スタックスネットが立案された当初、開発者らはイランが遠心分離機の故障の原因として部品不良などを疑うことを期待していた[40)]。イランがカーン博士から遠心分離機の設計図を購入していた事実を考慮すれば、機械的故障はもっともらしかった。しかし、その可能性が高かったとしても、攻撃元を特定されないようにしておく必要があった。当時のオバマ（Barack Obama）大統領は、付随的な損害と報復を恐れ、スタックスネットは「非帰属可能」でなければならないと強調していた[41)]。その結果、あまりにも大きな損害を与えるとイランが攻撃されていることに気付いてしまうのではないかと心配し、スタックスネットによる被害の規模が制限された。

第二に、標的の複雑さである。ナタンツの核施設は技術的にも組織的にも非常に複雑だった。技術面においては、周辺機器の多様性が証拠として挙げられる。イランは、密輸ネットワークを通して違法にウラン濃縮のための機械や部品を調達していた[42]。具体的には、ドイツやトルコなどの企業から周波数変換器を入手していたことが分かっている。しかし、スタックスネットはフィンランド製またはイラン製の周辺機器を探すようにのみプログラミングされていた。つまり、スタックスネットが一部では発動されなかったかもしれないのである。組織面においては、ナタンツほどの大規模な核施設であれば、業務を円滑に進めるための文書化されていない慣行が数多くあることが予想される[43]。このような複雑さは、攻撃側が標的を完全に理解するのを妨げるだけでなく、防御側にとって有利に働く。

第三に、ウィルス対策研究者たちの存在である。スタックスネットの存在は、2010年6月にミンスクのコンピュータ・セキュリティ会社ウィルス・ブロック・アーダのウィルス対策研究者であるセルゲイ・ウラーセン（Sergey Ulasen）氏により発見された[44]。翌7月にそのことをセキュリティ・フォーラムに投稿すると、数日のうちにシマンテックやマカフィーなど世界中のウィルス対策企業がスタックスネットの研究を始め、次々と解読の結果を発表した。よって、イランは対敵情報活動を部分的に外部に委託することができた。しかし、米国とイスラエルは作戦を止めなければならなくなった。このように、ウィルス対策研究者たちの存在は防御側のコストを引き下げ、攻撃側のコストを引き上げるのである[45]。

概括すると、スタックスネットによるCN攻撃の成果は、攻撃側が匿名性を維持しようとし、標的が非常に複雑であり、ウィルス対策研究者たちがコンピュータ・ワームを解読したため、限定された。したがって、サイバー戦争は攻撃側に優位性を与えるものではないと言える。

4　匿名性

続いて、スタックスネットの事例における匿名性の有無を三つの視点から分析する。

第一に、手段および動機である。まず、手段として、スタックスネットは極めて精巧であった。毎年発見される1,200万件を超えるマルウェアのうち、ゼロデイ脆弱性を悪用しているのは僅か12件ほどである[46]。このようなマルウェアの開発には、それなりのスキルが必要になる。スタックスネットの解析に携わった

ウィルス対策企業 ESET の研究者であるビュロー（Pierre Bureau）氏によると、高性能なコンピュータ・ワームを開発できるということは、攻撃側が豊富な資源を持っていることを示している[47]。したがって、ナタンツに対する CN 攻撃は単独犯のハッカーやテロ集団が主犯格ではないことが分かった。次に、動機の有無が判断材料となった。高度なサイバー技術と多大な資源を有する国家のうち、ロシアと中国は説得力のある動機に欠けた[48]。一方で、米国には手段も動機も十分にあった。付随的損害を抑えつつイランの核武装化を遅らせたかった米国にとって、CN 攻撃はうってつけだったのである。ジャリーリー（Saeed Jalili）元イラン国家安全保障最高評議会書記は、スタックスネットによる CN 攻撃は米国とイスラエルが仕掛けたものであるという認識を示している[49]。つまり、スタックスネットは手段と動機があった米国に帰属され、最終的に匿名性は失われた。

第二に、作戦の規模である。スタックスネットは、開発に約 3 年、攻撃に約 1 年を要したとされている[50]。通算 4 年間も続いた作戦には、戦略家や技術者に加え、資金調達などを担当する管理者、そして監督者と、多くの人員が必要であった。しかし、人間が増えると人為的ミスが起こる可能性も高まる[51]。多数のアクションが複雑に入り組んでいるサイバー作戦ならば、操作上の誤りはなおさら多くなる。人員の増加に伴うもう一つの難点が、機密情報の潜在的な流出源が増えるということである。スタックスネットの攻撃元を暴いた記事でも、米国国家安全保障会議や作戦の関係者による証言が複数取り上げられていた[52]。よって、作戦の規模が大きいと、匿名性が失われる可能性が高まると言える。それに対して、作戦の規模が小さいと、匿名性が失われる可能性はより低くなると考えられる。

第三に、サイバーセキュリティ専門家たちの存在である。オバマ大統領が望んでいたように、スタックスネットを「非帰属可能」にしておくのは容易ではなかった[53]。2010年 7 月以降、コンピュータ・ワームの正体が明らかになるにつれて、サイバーセキュリティ専門家たちがその生みの親をめぐり議論するようになった。やがて、発見から 2 年後に、オバマ大統領がナタンツの核施設に対する攻撃を密かに命じていたことが報道され、スタックスネットの攻撃元が発覚した[54]。しかし、これはスタックスネットがイランの核武装化を遅らせて、世界中の注目を集めたからであるとも言える。つまり、スタックスネットが「世界初のデジタル兵器（訳は引用者による）」でなければ、サイバーセキュリティ専門家たちもここまで綿密な調査をしたか否かは知りえない[55]。

このように、スタックスネットの事例においては、手段と動機との保持、大規

模な作戦に伴う人為的ミスや情報流出、そしてサイバーセキュリティ専門家たちの探求により、攻撃側の匿名性が失われた。CN 攻撃の作戦や被害が大きければ大きいほど、人為的ミスが増えたり、事件の調査により多くの労力が費やされる。逆に、作戦や被害が小さければ小さいほど、関係者も減り、攻撃元の特定に対する関心も低くなる。よって、匿名性が保たれるか否かは、作戦および被害の規模に従属的であると言える。

5　サイバー抑止の無効性

最後に、スタックスネットの事例におけるサイバー抑止の無効性を三つの視点から分析する。

第一に、エスカレーションに対する恐怖である。米国はイランの核武装化を遅らせたかったが、新たな紛争の火付け役になることや、すでに関わっていた戦争をエスカレートさせるのは避けたいと考えていた[56]。なぜならば、当時の米国はイランの国境付近で二つの戦争の当事者だったからである。まず、アフガニスタンでは2001年から米国およびその同盟国とタリバンとの間で戦いが続いていた。そして、イラクでも2003年から続いていたイラク戦争が終盤に差し掛かっていた。スタックスネットによる CN 攻撃が検討されていた2008年には、当時のブッシュ（George W. Bush）大統領がイラクから8,000人もの戦闘部隊を撤退させることを発表していた[57]。よって、米国はイランを攻撃することによって地域情勢を悪化させないように注意していたと考えられる。

第二に、報復に対する恐怖である。中東での戦争に加えて、当時はヒズボラの活動も盛んだった。ヒズボラは、欧米やイスラエルに抵抗することでイランと親密な関係を保ち、多大な支援を受けていた。また、2008年 1 月には、ヒズボラにより米国大使館の車両が爆破された[58]。2001年 9 月の同時多発テロ事件がまだ記憶に鮮明だったことから、当時の米国はヒズボラの行動にも敏感になっていたと考えられる。

第三に、CN 攻撃を使用した理由である。初めに提案されていた空爆には大きなリスクがあったため、米国の戦略家は代案を模索しなければならなかった。その結果、CN 攻撃が採用された。これには三つの理由がある[59]。まず、CN 攻撃は通常戦力を用いた攻撃よりも隠密に展開することができた。次に、イランの核武装化を遅らせることができた。最後に、外交的解決のために時間を稼ぐことができた。つまり、CN 攻撃は通常戦力による本格的な戦争を回避しながらも目的

を果たすことができる魅力的な方法であったため、実行されたと考えられる。

このように、スタックスネットによるCN攻撃は、結果として空爆を防いだ。しかし、実際には、イランは反撃をしている。2012年8月、サウジアラムコのコンピュータが「シャムーン」というマルウェアに感染した[60]。シャムーンは、サウジアラムコが所有するコンピュータから全てのデータを消去し、燃えている米国旗の画像に置き換えた。このシャムーンのコードには、同年5月にイランの石油会社を攻撃したマルウェアと同じく「ワイパー」という装置が埋め込まれていた。よって、シャムーンの攻撃元はイランであることが推測された。このように、イランによる米国への敵意を示すCN攻撃はあった。

概括すると、スタックスネットの事例においては、サイバー抑止の無効性は限定的に認められたと言える。米国側のエスカレーションと報復とに対する恐怖が働き、CN攻撃の使用により空爆という過剰な軍事行動は免れたが、イランから報復らしき行動はあった。つまり、空爆やイランからの核攻撃の可能性に対する抑止は成功したが、イランからのサイバー攻撃に対する抑止は失敗に終わった。結論として、サイバー抑止の効果の有無は定義によって変わると言える。

6　問いの考察

本節では、事例研究と仮説の検証を踏まえて、研究の問いを考察する。

まず、サイバー戦争に関する四つの主要な命題をスタックスネットの事例と照らし合わせて、改めて検証する。第一に、非対称性である。CN攻撃は、開発に必要なコストが低く、標的までの距離を短縮するため、通常戦力におけるバランス・オブ・パワーを均一化するとされてきた。しかし、スタックスネットの事例において米国がCN攻撃を成功させることができたのは、十分な組織的基盤と多大な資源を保持していたからである。したがって、サイバー戦争が通常戦力における勢力関係を変化させることはなく、依然として大国が有利であると言える。

第二に、攻撃優位性である。サイバー戦争では、攻撃に要する時間が短縮され、CN防御のコストが高いため、攻撃側が優位であるとされてきた。だが、スタックスネットの事例においては、米国が匿名性を維持しようとし、標的が非常に複雑であり、ウィルス対策研究者たちがコンピュータ・ワームを解読したため、CN攻撃の成果は限定された。よって、サイバー戦争は攻撃側に優位性を与えるものではないと言える。

第三に、匿名性である。攻撃元の特定が難しいサイバー戦争では、攻撃側が報

復を恐れないことに加え、攻撃元の誤った特定やエスカレーションが戦争を増加させるとされてきた。しかし、スタックスネットの事例においては、手段と動機との保持、大規模な作戦に伴う人為的ミスや情報流出、そしてサイバーセキュリティ専門家たちの探求により、攻撃側の匿名性は維持されなかった。つまり、CN 攻撃では、作戦や被害が大きければ大きいほど、人為的ミスが増えたり、調査により多くの労力が費やされる。逆に、作戦や被害が小さければ小さいほど、関係者も減り、攻撃元の特定に対する関心も低くなる。したがって、匿名性が保たれるか否かは、作戦および被害の規模に従属的であると言える。

第四に、サイバー抑止の無効性である。匿名性、攻撃優位性、そして軍備管理協定を締結する難しさにより、サイバー抑止は無効であるとされてきた。だが、スタックスネットの事例においては、エスカレーションと報復に対する恐怖が働き、CN 攻撃の使用が空爆という過剰な軍事行動を防いだ一方で、イランによる報復らしき行動もあった。つまり、イランからのサイバー攻撃に対する抑止は失敗したが、空爆やイランからの核攻撃の可能性に対する抑止は効いた。したがって、サイバー抑止は定義によって機能しているか否かの判断が異なると言える。

次に、研究の問いを考察する。事例研究の結果、サイバー戦争における非対称性と攻撃優位性はともに否定された。一方、匿名性とサイバー抑止の無効性については限定的に認められた。よって、「サイバー戦争の革命性は条件付きで50％である」と判断される。

おわりに

結論として、サイバー戦争に関する四つの主要な命題のうち二つが限定的に立証された。理由としては、以下 4 点が挙げられる。第一に、CN 攻撃に必要な組織的基盤と資源的余裕は強力な国家にしかないため、非対称性が否定された。第二に、攻撃側による匿名性の重視や研究者たちの存在により、攻撃優位性が否定された。第三に、作戦および被害の規模によって人為的ミスが起こる確率や攻撃元の特定への関心の度合いが変化するため、匿名性の維持が限定的にしか認められなかった。第四に、サイバー抑止の無効性も定義によって判断が異なるため、限定的にしか認められなかった。このように、「サイバー戦争の革命性は条件付きで50％である」と判断された。

それでは、この主張は何を意味するのか。まず、理論的含意を考える。本研究

では、サイバー抑止の効果の有無は定義によって変わることが判明した。だが、そもそもサイバー空間において従来の抑止理論が適用できるのかという疑問が残る。抑止理論は「信憑性のある報復能力を維持することにより敵の攻撃を防ぐことができる（訳は引用者による）」と主張するが、サイバー空間では主体の特定が比較的困難である[61]。また、攻撃の規模が大小様々である。DDoS 攻撃などの小規模なものは気軽に使用でき、それに対する抑止は難しいと考えられる。よって、抑止に関しては、サイバー空間に特有の性質を踏まえて新たな理論を打ち出す必要があるかもしれない。

次に、政策的含意を考える。サイバー技術が戦車や核兵器のような戦略的重要性を持つ可能性は低い。よって、各国はサイバー技術を通常戦力に対する補助的な兵器として国家安全保障戦略に組み込むべきである。例えば、「総当たり攻撃」（brute force attack）や「先制の一撃」（opening salvo）としての使用が想定できる。総当たり攻撃は、暗号化されたデータを解読するために使用できる攻撃であり、目的は諜報などである[62]。一方、先制の一撃は相手の機先を制して行う攻撃であり、相手が対応に追われている間に通常戦力を用いてさらに打撃を与えるために使われる。このように、サイバー技術に補助的な役割を付すことで、国家は効率的に戦争を遂行できるだろう。

最後に、今後の研究課題に触れる。ここでは、主に二つの問題を取り上げる。第一に、サイバー戦争の革命性に関する事例研究を増やすことである。本研究を通して、サイバー戦争は匿名性とサイバー抑止の無効性に焦点を当てた場合に革命的となる可能性があることが判明した。ただし、事例研究を柱とした本研究も、一つの事例しか扱っていない。サイバー戦争の革命性を正確に判断するためには、適切な事象を用いてさらに検証を進める必要がある。第二に、サイバー空間における国際的な規範の構築に向けた研究である。今も、自由民主主義的な欧米諸国と権威主義的な中国やロシアとの間でインターネットなどの規制をめぐり主張が対立している。例えば、中国とロシアは、2015年にサイバーセキュリティに関する取り決めを交わし、「内部の政治的または社会経済的な状況を不安定化させたり、公序良俗に反したり、内政に干渉する（訳は引用者による）」ようなサイバー攻撃をお互いに加えないと誓約した[63]。一方で、米国や日本を含む27カ国は2019年にサイバー空間における公平または不公平な行動を構成する要素を定めるサイバーセキュリティ協定に合意した。同協定には、中国とロシアに対する非難と捉えられる文言もあった[64]。このように、サイバー空間に適用される共通の国際法

はない。国際社会経済のサイバー空間への依存が進むにつれて、この法的規範の欠如を改善するための研究はより重要となる。

1） “The Sony Pictures Hack, Explained,” The Washington Post, December 19, 2014.
2） AP News, *UN Probing 35 North Korean Cyberattacks in 17 Countries*, August 13, 2019, https://apnews.com/ece1c6b122224bd9ac5e4cbd0c1e1d80 (accessed December 14, 2019).
3）「デジタル防衛へG7主導　外相宣言を採択、中ロ念頭に」『日本経済新聞』2019年4月6日。
4）「「スパイ部品」官民で排除　車や防衛、業種ごとに指針・検証」『日本経済新聞』2019年4月7日。
5） 伊東寛『サイバー戦争論―ナショナルセキュリティの現在』原書房、2016年、21頁。
6） 同上、27-33頁。
7） United States Department of Defense, *Summary of the 2018 National Defense Strategy*, January 2019, https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf (accessed September 21, 2019).
8） Richard A. Clarke and Robert K. Knake, *Cyber War: The Next Threat to National Security and What to Do about It* (New York: Harper-Collins Publishers, 2010), 6.
9） 伊東『サイバー戦争論』41頁。
10） Ronald Deibert, “Cyber-Security,” *The Routledge Handbook of Security Studies*, 2nd ed., ed. Myriam D. Cavelty and Victor Mauer (Abingdon: Routledge, 2017), 178.
11） ボットネットとは、マルウェアに感染したことで外部の者が遠隔操作で制御できるようになったコンピュータのネットワークである。Kaspersky, *What Is a Botnet?*, https://usa.kaspersky.com/resource-center/threats/botnet-attacks (accessed February 13, 2020).
12） DDoS攻撃とは、過剰なアクセスやデータを送付することによりウェブサイトやオンライン・サービスを使用不可にするサービス拒否攻撃（denial-of-service attack、DoS攻撃）を複数のコンピュータから大量に行うことを指す。DDoS攻撃を受けると、ネットワーク機器に大きな負荷がかかるため、ウェブサイトを閲覧できなくなったり、通信の遅延が発生する。Norton, *What Is a Distributed Denial of Service Attack (DDoS) and What Can You Do About Them?*, https://us.norton.com/internetsecurity-emerging-threats-what-is-a-ddos-attack-30sectech-by-norton.html (accessed February 13, 2020). NTTコミュニケーションズ「DDoS攻撃とは？」https://www.ntt.com/business/services/network/internet-connect/ocn-business/bocn/knowledge/archive_18.html、2020年2月13日アクセス。
13） Adam P. Liff, “Cyberwar: A New ‘Absolute Weapon’? The Proliferation of Cyberwarfare Capabilities and Interstate War,” *Journal of Strategic Studies* 35, no. 3

(June 2012): 401–428.

14） Lucas Kello, “The Meaning of the Cyber Revolution: Perils to Theory and Statecraft,” *International Security* 38, no. 2 (Fall 2013): 7–40.

15） コンピュータ・ワームとは、人間による介入なしに自分を複製し、コンピュータからコンピュータへと自分のコピーを拡散するマルウェアの一種である。Norton, *What Is a Computer Worm, and How Does It Work?*, https://us.norton.com/internetsecurity-malware-what-is-a-computer-worm.html (accessed February 13, 2020).

16） Liff, “Cyberwar,” 409.

17） Robert Jervis, “Cooperation Under the Security Dilemma,” *World Politics* 30, no. 2 (January 1978): 187.

18） Charles L. Glaser and Chaim Kaufmann, “What Is the Offense-Defense Balance and Can We Measure It?” *International Security* 22, no. 4 (Spring 1998): 49–50.

19） Liff, “Cyberwar,” 412–413.

20） Lawrence Freedman and Srinath Raghavan, “Coercion,” *Security Studies: An Introduction*, 3rd ed., ed. Paul D. Williams and Matt McDonald (Abingdon: Routledge, 2018), 193, 196–197.

21） Liff, “Cyberwar,” 417–422.

22） United Nations Security Council, *Resolution 1803*, March 2008, https://www.iaea.org/sites/default/files/unsc_res1803-2008.pdf (accessed October 12, 2019).

23） 原子炉や核爆弾の動力源としてウランを活用するには、自然形から処理しなければならない。ウランには、ウラン238とウラン235（以下 U-235）という二つの同位体が含まれている。これらのうち、動力源を生成するために必要なのは核分裂をさせることができる U-235である。したがって、ウランを処理して U-235の濃度を上げる必要がある。このためには、重量の僅かな違いを利用する遠心分離機が用いられる。遠心分離機の中心にある回転子は長軸を中心に高速で回転し、二つの同位体を分離する強力な遠心力を生成する。ただし、一つの遠心分離機では十分な濃縮度を達成できないため、多数の遠心分離機が並行して稼働される。つまり、一組目の遠心分離機の出力がさらなる濃縮のために別の遠心分離機のセットに供給されるのである。このプロセスは、望ましい濃度が達成されるまで繰り返される。Federation of American Scientists, *How a Centrifuge Works*, https://fas.org/issues/nonproliferation-counterproliferation/nuclear-fuel-cycle/uranium-enrichment-gas-centrifuge-technology/centrifuge-works/ (accessed February 13, 2020).

24） 産業用制御システムとは、産業プロセスの管理と制御を目的とする様々な情報技術（以下 IT）や IT システムを総称する言葉である。例えば、監視制御システムや分散制御システムなどである；カスペルスキー・デイリー「ICS とは？保護の手段は？」2017年11月14日、https://blog.kaspersky.co.jp/what-is-ics/18596/、2020年 2 月13日アクセス。

25） David Sanger, *Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power* (New York: Crown, 2012), 194–196.

26） ツールキットとは、攻撃を行うために脆弱性を確認するツールや攻撃そのものを実行するツールを一つにまとめたものである。サイバーセキュリティ.com「エクスプロイトとは？マルウェアとの違いから考える防止・対策方法」2019年４月19日、https://cybersecurity-jp.com/security-measures/25320、2019年２月15日アクセス。

27） 周波数変換器とは、遠心分離機に内蔵されている回転子の回転速度を制御する機器である。Eric A. Croddy, Jeffrey A. Larsen and James J. Wirtz eds., *Weapons of Mass Destruction: An Encyclopedia of Worldwide Policy, Technology, and History*, 2nd vol. (Santa Barbara: ABC-CLIO, Inc., 2005), 118–119.

28） Institute for Science and International Security, *Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant?*, December 2010, 4, http://isis-online.org/uploads/isis-reports/documents/stuxnet_FEP_22Dec2010.pdf (accessed October 12, 2019).

29） Symantec, *W32.Stuxnet Dossier*, February 2011, https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf (accessed October 12, 2019).

30） 中間者攻撃とは、攻撃者が二者間の通信に割り込み、それぞれになりすまして通信内容の改ざんなどを行う攻撃である。これにより、攻撃者は他者に向けられたデータや送信されないはずであったデータを当事者に気づかれることなく傍受・送受信できる。VERACODE, *Man in the Middle (MITM) Attack*, https://www.veracode.com/security/man-middle-attack (accessed February 13, 2020).

31） ISIS, *Did Stuxnet Take Out 1,000 Centrifuges*, 1.

32） Jon R. Lindsay, "Stuxnet and the Limits of Cyber Warfare," *Security Studies* 22, no. 3 (August 2013): 385.

33） "U.S., Israel Developed Flame Computer Virus to Slow Iranian Nuclear Efforts, Officials Say," The Washington Post, June 19, 2012.

34） ゼロデイ脆弱性とは、ソフトウェア・セキュリティー上の欠陥の一種である。具体的には、ソフトウェアの生産者は欠陥の存在を認知してはいるが、その欠陥を修正するための対策がない状態を指す。攻撃者は、この脆弱性を利用しゼロデイ攻撃を実行することができる。Norton, *Zero-Day Vulnerability: What It Is, and How It Works*, https://us.norton.com/internetsecurity-emerging-threats-how-do-zeroday-vulnerabilities-work-30sectech.html (accessed February 13, 2020); Lukas Milevski, "Stuxnet and Strategy: A Special Operation in Cyberspace?" *Joint Force Quarterly* 63 (October 2011): 65.

35） Norton, *Zero-Day Vulnerability* (accessed February 13, 2020).

36） Sanger, *Confront and Conceal*, 197–198.

37） Der Spiegel, *Mossad's Miracle Weapon: Stuxnet Virus Opens New Era of Cyber War*,

August 8, 2011, https://www.spiegel.de/international/world/mossad-s-miracle-weapon-stuxnet-virus-opens-new-era-of-cyber-war-a-778912.html (accessed October 14, 2019).

38） Lindsay, "Stuxnet," 387.

39） Sanger, *Confront and Conceal*, 190.

40） Ibid., 188.

41） Ibid., 202.

42） ISIS, *Did Stuxnet Take Out 1,000 Centrifuges*, 6.

43） Lindsay, "Stuxnet," 393.

44） WIRED, *How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History*, July 11, 2011, https://www.wired.com/2011/07/how-digital-detectives-deciphered-stuxnet/ (accessed November 9, 2019).

45） Lindsay, "Stuxnet," 394.

46） WIRED, *How Digital Detectives Deciphered Stuxnet* (accessed November 2, 2019).

47） Pierre-Marc Bureau, *Win32/Stuxnet Signed Binaries*, July 19, 2010, https://www.welivesecurity.com/2010/07/19/win32stuxnet-signed-binaries/ (accessed November 9, 2019).

48） Lindsay, "Stuxnet," 400.

49） Der Spiegel, *Iran's Chief Nuclear Negotiator 'We Have to Be Constantly on Guard'*, January 18, 2011, https://www.spiegel.de/international/world/iran-s-chief-nuclear-negotiator-we-have-to-be-constantly-on-guard-a-739945.html (accessed November 9, 2019).

50） Der Spiegel, *Mossad's Miracle Weapon* (accessed October 14, 2019); Symantec, *W32.Stuxnet Dossier* (accessed October 12, 2019).

51） Lindsay, "Stuxnet," 399.

52） "Obama Order Sped Up Wave of Cyberattacks against Iran," The New York Times, June 1, 2012.

53） Sanger, *Confront and Conceal*, 202.

54） "Obama Order Sped Up Wave of Cyberattacks against Iran," The New York Times, June 1, 2012.

55） WIRED, *An Unprecedented Look at Stuxnet, the World's First Digital Weapon*, November 3, 2014, https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/ (accessed December 10, 2019).

56） Lindsay, "Stuxnet," 398.

57） "Bush Announces Withdrawal of 8,000 Troops from Iraq," The Guardian, September 9, 2008.

58） Stratfor, *Lebanon: Hezbollah and the Jan. 15 Bombing*, January 15, 2008, https://worldview.stratfor.com/article/lebanon-hezbollah-and-jan-15-bombing (accessed November 27, 2019).

59) Lindsay, "Stuxnet," 397-401.

60) "In Cyberattack on Saudi Firm, U.S. Sees Iran Firing Back," The New York Times, October 23, 2012.

61) Rhea Siers, "Cybersecurity," *Security Studies: An Introduction*, 3rd ed., ed. Paul D. Williams and Matt McDonald (Abingdon: Routledge, 2018), 560.

62) Kaspersky, *What's a Brute Force Attack?*, https://www.kaspersky.com/resource-center/definitions/brute-force-attack (accessed January 16, 2020).

63) "Russia and China Pledge Not to Hack Each Other," The Washington Post, May 8, 2015.

64) CNN, *27 Countries Sign Cybersecurity Pledge with Digs at China and Russia*, September 23, 2019, https://edition.cnn.com/2019/09/23/politics/united-nations-cyber-condemns-russia-china/index.html (accessed February 13, 2020).