論文

オリンピック・ゲームズ作戦に見る「匿名性の破れ」

後　藤　信　介
小樽市役所

本稿は 2019 年 3 月に Web 出版された『IIET 通信第 52 号』（東京国際大学国際交流研究所紀要、https://www.tiu.ac.jp/iiet/page03.htm）に掲載された後藤信介氏による論文で、当時としては斬新な視点から書かれた論文です。この論文は、後藤氏が放送大学大学院博士後期課程に在籍中に纏められたものであり、３年を経過した今日、改めて拝読してみると、さらに重要な、喫緊のテーマを論じたものとなりました。

今般のロシアによるウクライナ侵攻に関して、世界の情報通信にかかわる深刻な問題を、後藤氏が３年前から分析していたことを、ここに改めて知ることになりました。ロシアによるウクライナ侵犯の今後は、世界がどのような形に収まっていくのか、この事件後の世界の通信事情はどのように変化するのか、本論文は私たちに戦慄をもって向き直ることを要請しているように思えます。まさに世界は危機に満ちているのです。（塩尻和子）

はじめに――サイバー・パワー

2018 年 7 月 27 日には、日本においても閣議決定を経て「サイバーセキュリティ戦略」が変更されたが、「AI、IoT、ロボティクス、3D プリンター、AR/VR など、サイバー空間における知見や技術・サービスが社会に定着し…サイバー空間と実空間の一体化が進展している。[1]」との認識が明示されている。サイバー空間と実空間の一体化が進む中、2016 年、エストニアのタリンにおいて、北大西洋条約機構（NATO: North Atlantic Treaty Organization）のサイバー防衛センター（CCDCOE: Cooperative Cyber Defence Centre of Excellence）が第 8 回サイバー紛争国際会議（CyCon: The International Conference on Cyber Conflict）を開催した。この年、CyCon がスポットライトを当てたのは「サイバー・パワー」であった。会議の成果として刊行された論文集には 18 の論文が掲載されている[2]。サイバー空間と実空間との一体化の進展に伴い、サイバー・パワーも論理的要素や物理的なネットワークのみならず、人的要素にも影響を与えるものとして捉えられており、サイバー・パワーという概念の射程は広い[3]。サイバー・パワーについてはこれまで様々な分析枠組みが提示されてきたが[4]、ソフト・パワーやスマート・パワーを国際関係の分析概念として提唱してきたジョ

セフ・S・ナイ・ジュニア（Joseph S. Nye, Jr.）も、サイバー・パワーに関する研究を著している[5]。ジョセフ・ナイはサイバー・パワーの分析においても、ハード・パワーとソフト・パワーの両面を持つものとして捉えつつ、DoS（denial of service）攻撃や SCADA（Supervisory Control and Data Acquisition）に障害を引き起こすことについては、ハード・パワーに分類している[6]。

アメリカ政府は 2006 年から、イランのナタンズにあるウラン濃縮施設に対してサイバー攻撃を行う「オリンピック・ゲームズ作戦」の計画に着手したことが知られているが、実際にその作戦において用いられたマルウェアは、一般的に「スタックスネット（Stuxnet)」として知られている。スタックスネットが一般に認知されるようになったのは 2010 年のことであるが、それ以降、多くのサイバー・インシデントが発生してきているにもかかわらず、ハード・パワーの代表的存在として今もなお言及され続けており、2016 年の CyCon の論文集においても表 1 のような文脈において言及されている。

表 1　2016CyCon 論文集におけるスタックスネットへの言及

対象限定的な物理損壊に至る高度な設計
- 物理的損壊に至る重要インフラへの攻撃 - ナタンズの遠心分離機の回転数を操作して、物理的な結果をもたらした攻撃 - シーメンス社製のプログラマブル・ロジック・コンロトーラー（PLC）のプログラムを書き換え、モーターを安全ではない範囲の回転数にする攻撃 - アメリカとイスラエルが主体だとされているオリンピック・ゲームズ作戦で用いられたマルウェアであり、ネットワークのエア・ギャップを越えるよう設計され、産業制御システムに秘密裏に障害を起こす攻撃 - 高度で、コストがかかり、多年にわたる侵入作戦 - ゼロデイ脆弱性を 4 つ利用した、高度に洗練されたコンピュータ・ネットワーク攻撃作戦 - あらかじめ定められた標的にのみ攻撃する精密誘導兵器 - 多くの様々な要素に関する詳細な情報と、専門知識を備えた高い資質を備えたチームを必要とする攻撃
政治的な目的達成のための手段
- 外国への介入のような政治的な道具として用いられるサイバー能力 - イランの核の野望を諦めさせる手段としての攻撃 - アトリビューション問題を利用し、目的を達成した秘密作戦であり、関係の否認という点で、証明責任が伴う強制的なパワー（coercive power）の行使とは異なる「力ずく」(brute force) - 1）核の脅威を減らし、計画を遅延させる、2）産業制御システム分野の重要インフラ防護が改善され、サイバー脅威を減少させる、というイスラエルの戦略的目標に合致

する作戦 - 1,000機のイランの遠心分離機を機能不全にしたが、この時期の濃縮量は増えており、イランの核開発計画を阻止するという点では失敗と言えるが、開発を遅らせ、イスラエルによる空爆をそらすという点では成功とも言え、戦略的な政治的目標について議論されてきた攻撃 - イランのサイバー能力を強化させる結果 - イランによるサイバー能力の構築を加速させ、アメリカとイランとの間のサイバー軍備競争を招いた攻撃 - 勝利と敗北を評価するサイバー戦略を持ち合わせていなかったためにアメリカが取ったリスクある攻撃

（出典）Pissanidis, Rõigas and Veenendaal (2016)より筆者作成

第一に、対象限定的な物理損壊に至る高度な設計に関して言えば、スタックスネットは、精密誘導兵器と言われるように、シーメンス社の PLC に限って回転数を変化させるよう設計されていた。PLC により制御されていたのは、ウラン濃縮のために用いられていた高速で回転する遠心分離機であることが推定され、イラン中部に位置するナタンズにあるウラン濃縮施設が攻撃対象であったとされている。技術的な高度さの説明として用いられるのがゼロデイ脆弱性、つまり、一般的には世に認知されておらず、システムの製作企業も対処していないシステム上の瑕疵の複数使用という点であり、システムの欠陥についての熟知が不可欠である。国家の重要インフラであるウラン濃縮施設で用いられているシステムや機器の構成を正確に把握していなければ、こうした設計は不可能であり、機器構成の把握から、侵入から回転数の変化に至るまでの多くの機能の統合に至るまで、多くの人員が関与した攻撃であったことが推測されるのである。

第二に、政治的な目的達成のための手段という観点では、イランの核開発計画に対する介入という形を取っているものの、秘密作戦として実行され、攻撃後しばらくアメリカ政府は自らの攻撃であると積極的に公言しなかった。この攻撃は、イランの核開発推進の意図を挫くものとはならず、ナタンズにおけるウラン濃縮量は増加した。イランの核開発に対しては影響を与えなかったが、イランによるサイバー能力開発の推進といった事態を招き、スタックスネット使用後における、イランによるアメリカに対するサイバー攻撃の増加という結果に至っている。マルウェアは、アメリカとイスラエルが共同で開発したものであり、核開発の後退や重要インフラ防護の雰囲気の醸成といった、イスラエルの政治的目的との合致という点からは評価されている。

このように、サイバー・パワーの中でもハード・パワーの代表例として政治的な目的達成手段としてスタックスネットは分析される。バートランド・ラッセル (Bertrand Russell) は、1938 年刊行の著書『権力論　新たな社会分析』において、パワーを「意図した効果の創出」と定義した[7]。ラッセルの述べたパワー観においては、意図した効果がいかなるもので

あったか、そしてそれを創出できかたできなかったのかによってパワーは評価されるという側面を持つ。スタックスネットの評価が成功であるのか失敗であるのかの評価が分かれるのは、アメリカ政府が意図した効果をどのように設定するのかという研究上の観点の違いに起因する。

この論文では、スタックスネットを用いたオリンピック・ゲームズ作戦を、アメリカによる軍事施設以外の他国の重要インフラへのサイバー攻撃として捉え、この作戦の特徴を把握するため、1982 年に旧ソ連のガス・パイプラインをロジック・ボムで攻撃した事例とを比較する。イランのウラン濃縮施設をマルウェア「スタックスネット」で攻撃したオリンピック・ゲームズ作戦は 2006 年に着手されたものであるが、両事例の間には 24 年の差があり、一方はロナルド・レーガン（Ronald Reagan）政権下で発案・実行された作戦であり、もう一方はジョージ・W・ブッシュ（George W. Bush）政権下で発案され、バラク・オバマ（Barack Obama）政権下で実行された作戦であるという、政権の違いもある。また、コンピュータ・ネットワークの黎明期と、ユーザーが爆発的に増加したワールド・ワイド・ウェブの成熟期という違いがあり、サイバー空間のあり方が大きく様変わりしていることは否めない。アメリカ政府による軍事施設ではない他国へのサイバー攻撃の事例として把握されている事例は少なく、事例が限定されている点も否めない。しかし、このような研究上の限界があるものの、両事例の過程を比較することで、オリンピック・ゲームズ作戦の特徴である「匿名性の破れ」が指摘できる。以下、旧ソ連ガス・パイプラインへの攻撃とイランのウラン濃縮施設への攻撃、それぞれの過程を第 1 節と第 2 節で見る。その上で、第 3 節で両作戦を比較し、共通点、相違点について考察する。

１　旧ソ連ガス・パイプラインへの攻撃

（1）背景

東西冷戦がデタントの時期にあった 1981 年 1 月 20 日、アメリカではレーガンが第 40 代大統領に就任した。レーガン大統領はソ連の構造を破壊する意志を持っていたことが知られている[8]が、レーガン政権下の 1987 年にホワイトハウスがまとめた「アメリカ合衆国国家安全保障戦略」においても、アメリカの国益につながる方策のひとつとして、「ソ連の過剰な軍事支出と世界的な冒険主義を挫くため、ソ連を国内経済の欠点に直面させる[9]」ことが挙げられている。

1982 年 9 月 21 日に中央情報局長官（DCI: The Director of Central Intelligence）の名で作成された特別国家情報評価（SNIE: Special National Intelligence Estimate)「ソ連ガス・パイプライン概観[10]」において述べられているように、アメリカは、ソ連がシベリアから西ヨーロッパへ天然ガスが輸出し、外貨を獲得しようと目指していることを把握していた。目下建設中のパイプラインを含め、1990 年代までにさらなる敷設が検討されてい

ることがレポートには記されており、シベリア-西ヨーロッパ・パイプラインはソ連経済によって有用な収入源であるとアメリカ政府は認識していた。

ソ連は、インフラを支える科学技術の全てを自国で開発しておらず、アメリカから輸入した製品や技術がソ連経済にとって重要であったことは、1974 年にランド研究所（RAND Corporation）のチャールズ・ウォルフ・ジュニア（Charles Wolf, Jr.）がまとめた「ソ連とアメリカとの技術交流　包括レポート[11]」に記されている。同年である 1974 年にホワイトハウスにより発出された国家安全保障決議覚書（National Security Decision Memorandum）247 号は「アメリカの共産主義国家へのコンピュータの輸出政策[12]」と題されており、コンピュータ技術や製品、プログラムの輸出や技術移転は制限されることが明確に述べられている。

1980 年代初頭は、サイバー空間を構成する技術はまだ黎明期にあった。1969 年に、世界初となるパケット通信に基づくコンピュータ・ネットワークとして誕生した高等研究計画局ネットワーク（ARPANET: Advanced Research Projects Agency Network）は、現在のインターネットの母体とされているが、1980 年代までに数百程度のホストと接続されていたのみである。また、1977 年にアップル社からパーソナル・コンピュータである Apple II が発売され、フロッピー・ディスクを介して感染を拡大する初のコンピュータ・ウィルスとされる「エルク・クローナー」が登場したのは 1982 年のことである。

（2）フェアウェル文書とトロイの木馬

1981 年 7 月 21 日、第 7 回先進国首脳会議がカナダのオタワで開催された。会議で採択された宣言では東西経済関係に触れられており、「政治的、経済的な利益と危険の複雑なバランスが東西関係には存在する[13]」と述べられている。このサミットの開催中、フランスのフランソワ・ミッテラン（François Mitterrand）大統領から、アメリカのレーガン大統領へ「フェアウェル文書」と呼ばれる文書が渡された[14]。

元ソ連国家保安委員会（КГБ: Комитет государственной безопасности СССР）のヴラジーミル・ヴェートラフ（Владимир Ветров）大佐は、フランスの国土監視局（DST: Direction de la Surveillance du Terriroire）に所属し、コードネームを「フェアウェル」と名乗っていた。彼はＫＧＢでは、西側からソ連へ技術移転する経路である「ライン X」を通じてソ連にもたらされた科学技術や製品を評価する職に就いていた技術者であった。フェアウェルとなったヴェートラフ大佐は、フランスにソ連の内情を記した多くの文書を提供しており、それが「フェアウェル文書」と呼ばれている。その文書の中には、西側で暮らしライン X にたずさわる職員の氏名や、ソ連が今後西側から輸入を検討している技術や製品のリストがあった。ソ連がアメリカの技術を求めて規制をかいくぐり技術移転を進めていたことは既知であったが、具体的な購買リストが、この時、レーガン大統領の元に渡ったのである。

この文書は、ジョージ・H・W・ブッシュ（George H. W. Bush）副大統領を通じて、中央情報局（CIA: Central Intelligence Agency）にもたらされた。当時、アメリカ国家安全保障会議（NSC: United States National Security Council）において国際経済担当スタッフであったガス・ワイス（Gus Weiss）も文書の利用を許された[15]。ガス・ワイスは科学技術の知識を備えており、アメリカ航空宇宙局（NASA: National Aeronautics and Space Administration）からメダルを授与されたこともあり、また、アメリカのゼネラル・エレクトリック社とフランスのスネクマ社とが共同で出資して民間航空機のエンジンであるCFM56の開発に当たった際、その推進役としての功績が称えられ、フランスからレジオンドヌール勲章も授与されたこともある[16]。1982年1月、彼はウィリアム・ケーシー（William Casey）CIA長官に会い、フェアウェル文書に記された製品をライン X を通じて購入させ、ソ連に着いてすぐのうちは正常に稼働するが、しばらくすると不具合が起きるようにしてはどうか、と提案し、ケーシーCIA長官は承諾した。偽装工作がほどこされたコンピュータ・チップがソ連の軍事機器に用いられ、欠陥のあるタービンがガス・パイプラインに組み込まれるなどといったことが想定されていた。すでに、アメリカ国防総省から、ステルス航空機や宇宙防衛、戦術航空機については誤った情報を与えてソ連を混乱させる手法を取っており、ソ連はスペース・シャトルの設計においてはNASAからの情報は用いないようになっていたという[17]。ケーシーCIA長官からレーガン大統領へ計画が伝えられると、大統領からも承諾を得ることができ、計画は実行に移されることとなった。

それから数か月後には偽装工作がほどこされた製品が輸出されたという[18]。ソ連はシベリア-西ヨーロッパ間のガス・パイプラインの敷設を進めており、バルブや圧縮装置、貯蔵施設をコンピュータによって制御する技術を求めていた。アメリカはソ連に対してソフトウェアの輸出を規制しており、ソ連はカナダの企業へ接近した。その際、アメリカはカナダの協力者の助力により、トロイの木馬を仕込んだソフトウェアをソ連に握らせることに成功した。そのソフトウェアは、一定の間は順調に稼働するが、パイプラインの継ぎ目や溶接が耐えることのできない程度にまで圧力を上げるよう仕組まれていた[19]。

後日、ホワイトハウスに、赤外線衛星がシベリアで3キロトン規模と推定される爆発を観測したという情報が入った。北アメリカ航空宇宙防衛司令部（NORAD: North American Aerospace Defense Command）はロケットの発射か小規模の核爆発を疑ったものの、核実験監視衛星は核爆発を感知していなかった。このとき、ガス・ワイスはこの事態が心配には及ばないことをNSCメンバーに語ったとされている[20]。

1982年のこの計画から14年後の1996年、ガス・ワイスはCIAが刊行している『インテリジェンス研究』に「フェアウェル文書」と題した記事を投稿し、作戦の存在はインテリジェンス・コミュニティ内部においては共有されていた。しかし、一般に広く刊行物の中で公表されたのは、計画から22年後の2004年、元アメリカ合衆国空軍長官であったトーマス・C・リード（Thomas C. Reed）が記した『深淵にて』においてであった。

２　イランのウラン濃縮施設への攻撃

（１）背景

2002 年 8 月、イランの反体制派組織モジャーヘディーネ・ハルグの政治部門であるイラン国民抵抗評議会が会見において、イラン中部に位置するナタンズに核燃料の製造施設が建設されていることを明らかにした[21]。この事態を受けて、EU3（イギリス、フランス、ドイツ）がイランと交渉し、2003 年にはテヘラン合意が締結され、2004 年にはパリ合意が締結された。しかし、2005 年、イランは合意に反して、六フッ化ウランの製造を開始した。これにより、2006 年、国際原子力機関（IAEA: International Atomic Energy Agency）は国連安全保障理事会にイラン核開発問題を付託して、同年、EU3 にロシア、中国、そしてアメリカが加わり、P5+1（国連安全保障理事会常任理事国 5 か国とドイツ）がイランとの交渉に当たることとなった。交渉による決着には至らず、同年、国連安保理決議が採択され、イランに対してウラン濃縮の停止が要求されたものの、イランは平和利用であるとの姿勢を崩さず濃縮作業は停止されなかった。

このウラン濃縮作業を担う施設では、ドイツのシーメンス社製の産業工程制御システム（PLC: Programable Logic Controller）であるシマティック S7 シリーズが使用されていた。このシステムが発売されたのは 1995 年であったが、シマティック S7 シリーズはイランの石油、天然ガス、石油化学、鉱業、そして核開発といった様々な分野で工場等の施設内で作業工程を制御するために用いられていたことが指摘されている[22]。後にナタンズのウラン濃縮施設攻撃に用いられるマルウェアには、2000 年と 2001 年に作製された PLC への侵入機能や、2003 年に作製された Step7.DLL を偽のものに置換する機能が用いられており、PLC への攻撃ツールは 2000 年代にはすでに段階的に作製されてきていた[23]。

アメリカでは、1999 年、ワシントン州ベリンハムで、SCADA の誤操作が原因となりガソリン・パイプラインが爆発する事故が起こっており、また、2003 年には、オハイオ州のオークハーバーにあるデービス・ベッセ原子力発電所のシステムに SQL スラマーというマルウェアが感染し、安全管理や作業工程監視を担っていた SCADA システムを数時間にわたって停止させたという事例が発生している。産業工程を制御するシステムは、作業のオートメーション化に伴い、広く、エネルギーや原子力を扱う重要インフラで利用されていたが、マルウェア感染や爆発といった事態をアメリカは経験していた[24]。

2003 年には、リビアのムアンマル・アル＝カッザーフィー（mu‘ammar al-qaḍḍāfī）が核放棄を宣言し、IAEA の査察団の受け入れを許していた。その際、保有していたウラン濃縮施設の機器がアメリカに運び込まれ、テネシー州にあるオークリッジ国立研究所に保管されていた。リビアが保有していたウラン濃縮のための遠心分離機は、パキスタンの核科学者アブドゥル・カディール・カーン（Abdul Qadeer Khan）によるものであった。イランのナタンズで稼働しているものと類似の遠心分離機をアメリカは研究することが可能であった

[25]。

（2）オリンピック・ゲームズ作戦

2006 年、ホワイトハウスでは、対イラン政策として、交渉と経済制裁、そして軍事行動が議論の俎上に載っていた[26]。イランの核開発計画に対処する時間を生み出すアイディアとして、ブッシュ大統領、コンドリーザ・ライス（Condoleezza Rice）国務長官、そしてスティーブン・ハドリー（Stephen Hadley）国家安全保障問題担当大統領補佐官に提案されたのが「オリンピック・ゲームズ作戦」であり、提案者は、当時、アメリカ戦略軍（USSTRATCOM: United States Strategic Command）の司令官であったジェームズ・カートライトらであった[27]。2003 年 10 月 30 日に発出された「情報作戦ロードマップ」では、情報作戦のあり方を 6 つの能力、つまり 1）コンピュータ・ネットワーク防衛、2）コンピュータ・ネットワーク攻撃、3）電子戦、4）心理作戦、5）作戦保全、6）軍事的偽り、から成るものと整理されており、コンピュータ・ネットワーク攻撃を担うのは USSTRATCOM であると明言されている[28]。このロードマップには、2003 年から 2006 年までのタイムラインが示され、2004 年にはコンピュータ・ネットワーク攻撃の兵器化が目標として設定されており[29]、カートライトは、2004 年 7 月に USSTRATCOM 司令官代理を務め、同年 9 月 1 日に司令官の任に就いており、彼は後にアメリカサイバー軍（USCYBERCOM: United States Cyber Command）となる小隊を指揮下に置いていたのである。

カートライトの提案から 8 か月で最初の計画が立案され、初めに「ビーコン」と呼ばれる偵察用のソフトウェアが作製された。このビーコンは、ナタンズのコンピュータ・システムに侵入し、稼働状況や遠心分離機の制御方法を知るためのものであった。そして、NSA 本部にウラン濃縮施設の構造や通常の稼働リズムを送信する機能を備えていた[30]。スタックスネットには開発段階によって複数のバージョンが存在するのだが、最初のものとされるスタックスネット 0.5 は 2005 年に通信するサーバが登録され、2007 年にはすでにマルウェア検知リストに載っていた。スタックスネット 0.5 は、濃縮プロセスが定常状態に達するまで待機し、周辺機器のスナップショットを作成するといった機能を持ち合わせ、その上で、遠心分離機のバルブを開閉し、また待機状態へ戻る、といった周期的な機能を備えていた[31]。このバージョンは 2009 年 7 月に感染が停止している。オリンピック・ゲームズ作戦を承認し、マルウェアの開発を進めてきたブッシュ大統領は、2009 年 1 月 20 日に退任しており、ブッシュ大統領が使用したのは、このバルブ開閉を攻撃手法とするバージョンであった。

作戦はオバマ大統領に継承された。2009 年から 2010 年にかけて、3 つのバージョンのスタックスネットが作製されている[32]。それぞれのバージョンの作製日は、バージョン 1.001 は 2009 年 6 月 22 日、バージョン 1.100 は 2010 年 3 月 1 日、バージョン 1.101 は 2010 年 4 月 14 日である。バージョン 0.5 ではバルブの開閉を攻撃手法としていたのに対し、バージョン 1.x シリーズに共通するのは、遠心分離機の回転数の変化が攻撃手法とされていた点

である。1.x シリーズは、イランにある重工業やエネルギー、産業オートメーションに関連する 5 つの企業（フーラード社、ベフパジューフ社、ネダー社、コントロール・ゴスタル・ジャーヘド社、カラーイェ電機）に初期感染し、そこから感染が拡大した[33]。

スタックスネットは、ネットワークが繋がっていれば OS を探し、探し当てた OS がウィンドウズ社製の汎用 OS であれば自己複製をする。それだけでなく、USB メモリを介しても感染を拡大する。2000 年代にはウィンドウズ社製の OS は広く普及しており、産業工程制御のためにも、独自の OS ではなく、こうした汎用 OS が用いられることがあった。

スタックスネットは、このように非常に広範に感染するよう設計されていたが、実際の攻撃段階になると、システムや機器を限定し、条件に合致しなければ攻撃をしない。条件に合致すると、モニターには正常稼働時の状況を表示させながら、その裏では遠心分離機の回転数を変化させ、ウラン濃縮工程に不具合を生じさせる[34]。2009 年から 2010 年までの間、IAEA によるレポート「イラン・イスラーム共和国における核兵器不拡散条約保障措置協定及び安全保障理事会決議関連条項の履行」においては、攻撃対象とされたナタンズのウラン濃縮施設において、放射性物質の漏出や、施設内での爆発や核分裂などの重大インシデントは報告されていない[35]。

2010 年 6 月、イランの顧客からコンピュータの不具合の報告を受け、調査に当たっていたベラルーシのコンピュータ・セキュリティ企業、ヴィルス・ブロク・アダ社は「Trojan-Spy.0485 と Malware-Cryptor.Win32.Inject.gen.2 の報告」と題したレポートをウェブ上に公開した[36]。このレポートによると、新種のマルウェアの発見は 2010 年 6 月 17 日であったとされている。2010 年 7 月には、マイクロソフト社やカスペルスキー・ラボ社、シマンテック社、トレンド・マイクロ社、マカフィー社らが次々とマルウェアに関する情報を公開した。2010 年 12 月に、アメリカのシンクタンクである科学国際安全保障研究所（ISIS: Institute for Science and International Security）は、スタックスネットの攻撃対象をナタンズのウラン濃縮施設であるとするレポートを出している[37]。

しかし、2010 年 6 月から 2012 年 6 月までの約 2 年間は、技術的なレポートが公開されても、攻撃・開発主体が判明することはなかった。攻撃・開発主体についてメディアで取り上げられたとしても、マルウェアで用いられていた文字列を痕跡として、そこからイスラエルが攻撃・開発主体ではないか、と論を展開するものもあったが、攻撃・開発主体は匿名性を保持していた。

2012 年 6 月 1 日、ニューヨーク・タイムズ紙のデービッド・サンガー（David Sanger）ワシントン支局長による記事が掲載された。その記事は、同年 6 月 5 日に出版予定の『直面と隠匿　オバマの秘密戦争とアメリカのパワーの驚くべき利用』から抜粋された文章であったが、そこには、スタックスネットと呼ばれているマルウェアは、ブッシュ大統領時代に着手された「オリンピック・ゲームズ作戦」において作製されたものであったことが記されていた[38]。

オリンピック・ゲームズ作戦の提案者のひとりであったカートライトは、2007 年に統合

参謀本部（JCS: Joint Chiefs of Staff）の副議長という要職を務め、2011 年に退役していた。彼は、2012 年 1 月から同年 6 月にかけて、メディア関係者へ情報を提供していた。そのひとりがニューヨーク・タイムズ氏のサンガー記者であった。2012 年 11 月、アメリカ連邦捜査局（FBI: Federal Bureau of Investigation）の捜査官が『直面と隠匿』からの引用をカートライトに見せたところ、カートライトは捜査官に、自分は情報源ではなく、機密情報をメディア関係者へ提供していない、と供述した。しかし、2016 年 10 月、裁判においてカートライトは、2012 年 11 月の捜査官への供述が虚偽であったことを認め、合衆国法典第 18 編「犯罪及び刑事手続」第 1001 条第 a 項第 2 節「連邦捜査官への虚偽の供述」の罪を受け入れた[39]。判決言い渡しが 2017 年 1 月 31 日に予定されていたが、2017 年 1 月 17 日、オバマ大統領はカートライトに恩赦を与えた[40]。

３　事例比較――旧ソ連ガス・パイプライン攻撃とイランのウラン濃縮施設攻撃

第１節で旧ソ連バス・パイプラインへの攻撃、第２節でイランのウラン濃縮施設への攻撃の事例を見てきた。両事例とも、アメリカが軍事施設以外の重要インフラ施設をサイバー的手法により攻撃した事例である。両作戦を比較したものが、表２である。

表２　ガス・パイプライン攻撃とウラン濃縮施設攻撃との比較

比較項目	ガス・パイプライン攻撃	ウラン濃縮施設攻撃
計画開始年	1981 年	2006 年
対象国	旧ソ連	イラン
事前情報	ガス・パイプライン建設の把握 フェアウェル文書	ウラン濃縮施設建設の把握 リビアから類似機器接収
計画発案者	ガス・ワイス NSC スタッフ	ジェームズ・カートライト STRATCOM 司令官ら
承諾	レーガン大統領、ケーシーCIA 長官	ブッシュ大統領、ライス国務長官、ハドリー国家安全保障問題担当大統領補佐官 （オバマ大統領へ継承）
攻撃手法	順調に稼働後、不具合	汎用 OS と USB で感染、偵察、偽装画面表示（、バルブ開閉)、遠心分離機の回転数の周期的変更
攻撃結果	ガス・パイプラインの爆発	放射性物質の漏出や爆発に至らない遠心分離機の障害
攻撃結果の確認	赤外線衛星	IAEA レポート
第三者による報告	-	2010 年、ベラルーシのエンジニ

		アによるレポート公表
メディア等の反応	－	コンピュータ・セキュリティ企業、シンクタンク、新聞記者、研究者など
作戦の公表	2004 年、トーマス・C・リード『深淵にて』	2012 年、デービッド・サンガー『直面と隠匿』
作戦の公表に対する政府の対応	－	2012 年、FBI による捜査 2016 年、恩赦

まず、共通点から挙げる。アメリカは攻撃対象国と対立関係にあり、看過できないインフラ建設の情報を得ている。また、1981 年においては、東西冷戦のデタントの時期、ソ連と既存の兵器で戦火を交えることは核戦争の危機を再燃させることを意味しており、2006 年においては、イランは強硬な態度を崩さないがテロとの戦いを続けるアメリカにイランと交戦する選択肢よりも別の選択肢を欲していた。こうした状況において、科学に関わり、コンピュータを利用した作戦を立案し、ホワイトハウスにおいて大統領にまで届く提案をできる人物の存在も指摘できる。両作戦とも、発案者が発した情報に基づき、一般に向けた書籍で作戦の存在が公表されている。

これらの共通点がありながら、一般への公表までの期間に大きな隔たりがある。旧ソ連ガス・パイプライン攻撃の場合、1981 年の作戦計画立案から、2004 年の書籍刊行まで 23 年が経っている。一方、イランのウラン濃縮施設攻撃の場合、2006 年の作戦計画立案から、2012 年の書籍刊行まで 6 年しか経っていない。

この差は、アメリカ政府関係者が作戦の存在の公表に意義を見出しているか否かによるものと言える。旧ソ連ガス・パイプライン攻撃は、第一義的にパイプラインへ打撃を与えることが目的とされ、その副次的効果としてソ連にアメリカから輸入した製品や技術に対する不信感を抱かせることが期待されたと言える。パイプラインに爆発が起こった時点で目的が達成されており、それ以上、意味を見出すには至らなかった。インテリジェンス機関内部での情報共有もソ連崩壊後の 1996 年であり、すでに過去となった冷戦時代を回顧する一部として作戦は公表されるに至った。イランのウラン濃縮施設攻撃は異なる。第一義的にウラン濃縮施設へ障害を起こすことが目的とされ、その副次的効果としてイランに、何者かによって重要なインフラ施設の機器構成まで詳細に把握されており、ピンポイントでサイバー攻撃の標的とされている恐怖を抱かせることが期待されたと言える。しかし、ウラン濃縮施設に障害が発生しただけでは目的は達成されておらず、さらなる政治的な意味を見出したからこそ、主体の公表という段階に移ったのではないか。つまり、旧ソ連ガス・パイプライン攻撃とイランのウラン濃縮施設攻撃との間には、匿名性に見出した意味が異なると言える。

サイバー攻撃の特徴とされる匿名性は、アトリビューション問題としても知られるが、攻

撃の存在は攻撃結果が生じるために認識されるものの、攻撃主体の特定や攻撃の責任の所在を確定させることが困難なことを言う。ハード・パワーとして用いられるサイバー・パワーの場合、物理的な不具合や損壊は起こるが、それを誰の行為によるものなのかが不明である状態と言える。イランのウラン濃縮施設攻撃では、主体の謎に、攻撃手法の高度さと核関連施設が標的とされたという危険度も相まってメディアを通じて話題となり、サイバー攻撃は人類に大きな影響を与えかねないという恐怖が一般に広まった。これがサイバー・パワーにおけるハード・パワーの典型例として現在も語られ続けるスタックスネットの姿である。

匿名性を保持したままでも、このように一般化された恐怖を広める効果があった。秘密作戦であれば名乗り出る必要は無いにもかかわらず、2012 年に、アメリカとイスラエルが共同でこの作戦の主体であることが明らかにされたのはなぜだろうか。「抑止態勢の確立は外国からの際限のない攻撃の波を打ち消す一助になるであろう。[41]」オリンピック・ゲームズ作戦に関する新聞報道の情報源となったカートライトが、2011 年に語った言葉である。カートライトは、そこにあるかどうかわからないものは怖がらせることができないとして、サイバー攻撃能力について公に語り、能力を養成し、他国からのサイバー攻撃に対しては自衛権を発動するという強力なシグナルを相手国に送ることが重要であると、サイバー攻撃に対する抑止について述べている[42]。メディアに対する情報提供に、こうしたカートライト個人の信念の影響は少なくないであろう。

サイバー空間における抑止については、オリンピック・ゲームズ作戦が計画立案された 2006 年に JCS 議長名で発出された「サイバー空間作戦のための国家軍事戦略」に色濃く描かれている[43]。この文書は、サイバー空間におけるアメリカの軍事的優越性（military superiority）を確かにすることを目的にまとめられ、国防総省は、アメリカの利益に対する脅威を打ち負かし、説得し、抑止するために、全範囲の軍事作戦をサイバー空間において、また、サイバー空間を通して実行する、としている。サイバー空間における攻撃能力は、アメリカ及び敵国に、主導権を獲得し、維持する機会を与える、という認識も示されており、サイバー攻撃能力の保有は、アメリカに軍事的優越性を与えるものであり、抑止態勢においては実際に攻撃能力を保有し、それを使用する意志があるという信憑性を向上させることで抑止の効果が得られる。こうした国家軍事戦略のもと、USSTRATCOM 司令官としてカートライトはサイバー部隊を率いていたのである。オリンピック・ゲームズ作戦の「匿名性の破れ」は、サイバー攻撃能力を公にすることに、「抑止態勢の構築」という軍事的な意味を持つと見出したカートライトの思想によると言えよう。重要インフラにも攻撃を加えるだけの能力と意志を、他でもなくアメリカは有している、というメッセージを世界に対して発する機会としたのである。

おわりに

以上、アメリカによる外国のインフラへのサイバー攻撃として、旧ソ連ガス・パイプライン攻撃と、イランのウラン濃縮施設攻撃という 2 つの事例を比較した。両事例に共通していたのは、1）アメリカは攻撃対象国と対立関係にあり、2）看過できないインフラ建設の情報を得ており、3）交戦する選択肢よりも別の選択肢を欲しており、4）コンピュータを利用した作戦を立案でき、5）ホワイトハウスにおいて大統領にまで届く提案をできる人物がいる、という点であった。公表までの時間の差異は、匿名のままでは得られない意義、つまり、抑止態勢の構築の一助という意義が、公表することによって得られると判断されたためであると言えよう。サイバー空間における軍事的優越性の確保を目指し、国家間におけるサイバー軍備拡張競争を進め、そのひとつの到達点がオリンピック・ゲームズ作戦であった。パワーには「意図した結果の創出」という側面があるが、オリンピック・ゲームズ作戦においては、「意図した結果」の設定の仕方によって研究者間の評価が揺れていた。アメリカは、「サイバー軍備の拡張」と「対イラン政策」とが交差する 2006 年という時点において、国家軍事戦略に基づき、サイバー空間における軍事的優越性を敵国に知らしめるものとして作戦を立案した、と解釈するのであれば、作戦は成功であったと評価することができよう。

（ごとう　しんすけ　　放送大学大学院　博士後期課程）

---

1 「サイバーセキュリティ戦略」2018, p. 4.

2 N. Pissanidis, H. Rõigas and M. Veenendaal eds., *2016 8th International Conference on Cyber Conflict: Cyber Power*, NATO CCD COE Publications, 2016.

3 Haaster, Jelle van, “Assessing Cyber Power,” N. Pissanidis, H. Rõigas and M. Veenendaal eds., *2016 8th International Conference on Cyber Conflict: Cyber Power*, NATO CCD COE Publications, 2016, pp. 7-21.

4 Franklin D. Kramer. Stuart H. Starr and Larry K. Wentz eds., *Cyberpower and National Security*, National Defense University Press, 2009.; David J. Betz and Tim Stevens, *Cyberspace and the State: Towards a Strategy for Cyber-Power*, Routledge, 2011.

5 Joseph S. Nye, Jr., “Cyber Power,” Belfer Center for Science and International Affairs, 2010.

6 Ibid., p. 7.

7 Bertrand Russell, *Power: A New Social Analysis*, W. W. Norton, 1938, p. 35.

8 Peter Schweizer, *Victory: The Reagan Administration’s Secret Strategy that Hastened the Collapse of the Soviet Union*, Atlantic Monthly Press, 1994.

9 The White House, “National Security Strategy of the United States,” 1987, p. 4.

10 Director of Central Intelligence, “The Soviet Gas Pipeline in Perspective: Special

National Intelligence Estimate," 1982.

[11] Charles Wolf. Jr., "U. S. Technology Exchange with the Soviet Union: A Summary Report," National Technical Information Service, 1974.

[12] The White House, "National Security Decision Memorandum 247: U. S. Policy on the Export of Computers to Communist Countries," 1974.

[13] "Declaration of the Ottawa Summit," 1981.

[14] Gus W. Weiss, "Duping the Soviets: The Farewell Dossier," *Studies in Intelligence*, Vol. 39, No. 5, 1996, p. 124.

[15] Ibid., p. 124.

[16] Sergei Kostin and Eric Raynaud, trans. by Catherine Cauvin-Higgins, *Farewell: The Greatest Spy Story of the Twentieth Century*, 2011, p. 282.

[17] Gus W. Weiss (1996), p. 125.

[18] Thomas C. Reed, At the Abyss: An Insider's History of the Cold War, Presidio Press, 2005, p. 268.

[19] Ibid., p. 269.

[20] Ibid., p. 269.

[21] Arms Control Association, "Timeline of Nuclear Diplomacy With Iran," 2019.

[22] Kim Zetter, *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon*, Crown Publishers, 2014, pp. 310-311.

[23] Ibid., p. 310.

[24] George Loukas, *Cyber-Physical Attacks: A Growing Invisible Threat*, Butterworth-Heinemann, 2015, pp. 23-27.

[25] David E. Sanger, *Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power*, Broadway Paperbacks, 2012, p.197.

[26] 後藤信介「対イラン・サイバー攻撃計画とホワイトハウス　政策決定から見た「オリンピック・ゲームズ作戦」の多層性」東京国際大学国際交流研究所『IIET 通信』第 50 号, 2017, p. 13.

[27] Sanger (2012), p. 191.

[28] Department of Defense, "Information Operations Roadmap," 2003, p. 6.

[29] Ibid., p. 69.

[30] Sanger (2012), p. 193.

[31] Geoff McDonald, Liam O Murchu, Stephen Doherty, Eric Chien, "Stuxnet 0.5: The Missing Link," Symantec Security Response, 2013, pp. 9-12.

[32] Ibid., p. 2.

[33] Nicolas Falliere, Liam O Murchu and Eric Chien, "W32.Stuxnet Dossier," Symantec Security Response, 2011, pp. 8-10.; GReAT, "Stuxnet: Zero victims: The identity of the companies targeted by the first known cyber-weapon," SecureList, 2014.

[34] Falliere, Murchu and Chien (2011), pp. 33-42.

[35] IAEA, “Implementation of the NPT Safeguards Agreement and relevant provisions of Security Council resolutions 1737(2006), 1747(2007), 1803(2008) and 1835(2008) in the Islamic Republic of Iran.” 2009-2010.

[36] Oleg Kupreev and Sergey Ulasen, “Trojan-Spy.0485 And Malware-Cryptor.Win32.Inject.gen.2 Review,” VirusBlokAda, 2010.; Eugene Kaspersky, “The Man Who Found Stuxnet – Sergey Ulasen in the Spotlight,” 2011.

[37] David Albright, Paul Brannan and Christina Walrond, “Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant? Preliminary Assessment.” ISIS Reports, 2010.

[38] David E. Sanger, “Obama Order Sped Up Wave of Cyberattacks Against Iran,” The New York Times, 2012.

[39] 後藤信介「アメリカの対イラン・サイバー攻撃作戦と情報漏洩　ジェームズ・カートライト裁判に見る」SYNODOS, 2017.

[40] Charlie Savage, “Obama Pardons James Cartwright, General Who Lied to F.B.I. in Leak Case,” The New York Times, 2017.

[41] Andrea Shalal-Esa, “Ex-U.S. general urges frank talk on cyber weapons,” Reuters, 2011.

[42] Ibid.

[43] Chairman of the Joint Chiefs of Staff, “The National Military Strategy for Cyberspace Operation,” 2006.