環太平洋地域文化研究　№.３：187-189（2022）

書評

ジム・スキアット
『シャドウ・ウォー ―中国・ロシアのハイブリッド戦争最前線―』

志田　淳二郎*

The Shadow War: Inside Russia's and China's Secret Operations to Defeat America

Junjiro SHIDA*

2017年12月，ドナルド・トランプ政権が『国家安全保障戦略』を公表して以降，米国，中国，ロシアの間の大国間競争に強い関心が寄せられている。今日の大国間競争とは，19世紀にみられたような，軍事力を実際に用いた戦争を基調とするものを意味せず，「重要インフラへのサイバー攻撃から，宇宙資産を脅かすことや，国内の分裂に拍車をかけるための情報活動さらには本格的な侵略すれすれの領土獲得までを行う」影のなかで行われる戦争，すなわち，「シャドウ・ウォー」の形態をとっている（16頁）。

『シャドウ・ウォー』（小金輝彦訳，原書房，2020年３月）の著者ジム・スキアットは，CNNのジャーナリストである。本書は，著者による膨大な取材に基づくエピソードの数々を紹介し，「西側諸国に敵対する国々が，武力戦争で勝つことは難しくても，勝利へつながる別の道があることに気づいたときに何が起きるか」（17頁）という大きな問いを，読者に投げかけている。本書は日本の読者にとっての良著である。

第１章「シャドウ・ウォーの渦中で」では，ロシア政府が関与した，英国でのロシア人元スパイ暗殺計画が取り上げられている。2006年11月，FSB（露連邦保安庁）の元職員でロシアの反体制活動家アレクサンドル・リトビネンコがロンドン市内の飲食店で放射性物質ポロニウム210を盛られ，死亡した。18年３月には，ソールズベリーでGRU（露軍参謀本部情報総局）の元スパイ，セルゲイ・スクリパリ大佐と娘ユリアが神経剤ノビチョクによる暗殺未遂事件に遭遇した。著者の情報提供者によれば，暗殺を指示したのはウラジミール・プーチン大統領であり，ロシアは「海外におけるロシアの暴力的行為に国境はない」と西側にメッセージを発信した，と著者は指摘する（６頁）。

第２章「最初の一撃」は，ロシアからのエストニアに対するサイバー攻撃（2007年）を取り上げる。首都タリンの赤軍兵士像の撤去・移転をめぐるロシア系住民の暴動と並行して行われたサイバー攻撃により，エストニアの政府，銀行，メディア等がロシア発のサイバー攻撃の被害に見舞われた。その後，エストニアはサイバー・セキュリティー能力を向上させ，「サイバー衛生」を国民に徹底することで，サイバー上の脅威に対抗した。翻って，米国は，エストニアの事例から得られる教訓を得ず，16年の米大統領選へのロシアの干渉の前兆を見逃してしまったと著者は酷評する（49頁）。

第３章「機密を盗みだす」は，中国人ビジネスマン，スー・ビンによる米国の機密情報窃取の事例を取り上げている。北米で軍用機産業の取引先と良好な関係を構築したスーは，狙いを定めた企業のコンピュータ・ファイルを特定し，その情報を中国本土の仲間に伝え，彼らが標的となる企業のコンピュータ・システムに不正侵入し，ファイルを窃取する。スーのチームは窃取したファイルを，中国内で関心を示す相手に売りつける。スーは，2009年から５年間，この活動を繰り返し，F-35，F-22ステルス戦闘機，C-17軍用輸送機に関する膨大な機密情報を窃取し，米中間の軍用機の技術力の差を縮めるのに一役買った。著者は，中国がこうした米政府および民間部門の機密や知的所有権を数十年にわたって窃取し続けており，米国側が中国側に課す様々な制裁措置では，中国の行動を変えることはできていないことを教訓とするべきと説く（72-73頁）。

* 名桜大学国際学群准教授　〒905-8585　沖縄県名護市為又1220-1　Associate Professor, Faculty of International Studies, Meio University, 1220-1 Biimata, Nago, Okinawa 905-8585 Japan

第４章「リトル・グリーンメン」は，章タイトルから想像されるエピソード，すなわち，2014年の２月末に迷彩服に何の記章もつけていない武装集団「リトル･グリーンメン」がクリミアに突如出現し，半島がウクライナからロシアへ編入された一連の事件ではなく，同年７月17日に親露派支配地域のウクライナ東部で発生したマレーシア航空17便の撃墜事件のエピソードから始まる。事件発生直後，OSCE（欧州安全保障協力機構）ウクライナ特別監視団スタッフが現場へ向かったが，そこにも「リトル・グリーンメン」が立ちはだかり，OSCEの調査活動を３ヵ月にもわたり妨害した。西側がロシアによる犯行と非難している同事件により，西側は対露認識を硬化させることになるが，ウクライナ危機の何年も前から，再三にわたり発せられてきたロシアの意図を見逃し（例えば，2007年のプーチンのミュンヘン演説），西側のルールに従ってロシアは行動するとみていた西側の対露認識の甘さを著者は鋭く指摘する（122頁）。

第５章「不沈空母」では，2012年以降，中国が着手している南シナ海の礁の埋め立てと恒久的な軍事拠点化に関する記述が続く。第４章の事例とは異なり，中国は直接的な武力衝突を伴わずに，南シナ海の国境線を引き直した。ウクライナ問題についてのロシアと同様，中国の同地域における領土的野心は何十年もの間，中国側から発せられてきたが，これを見落とし，あるいは，軽視してきた米国側の対応に著者は批判的である（159頁）。

第６章「宇宙での戦争」は，著者のカリフォルニア州ヴァンデンバーグ空軍基地にある統合宇宙運用センターへの訪問記録から始まる。同センターでは，「宇宙オペレーター」が宇宙ごみのみならず，複雑な軌道を描きながら地球を周回する衛星を監視していた。というのも，中国の衛星攻撃ミサイルの発射実験（2007年）による宇宙ごみの大量発生が，米国の宇宙資産への脅威と認識されたことは知られているが，14年に発射されたロシアの衛星攻撃兵器「コスモス2499」，機動性･駆動力に富む衛星「ルーチ」，ロボットアームで対象物をつかんでは離すことができる「キッドナッパー衛星」，中国の「試練７号」等への監視活動が軍事作戦のみならず日常生活を宇宙資産に依存している米国にとり，喫緊の課題となっているからだ。「危険にさらされていない宇宙資産などひとつもない」（183頁）という著者のインタビュー相手の一人，第50宇宙航空団司令官デイヴィッド・バック中将の言葉は，宇宙が中露のシャドウ・ウォーの新しく危険な前線であることの証左である。著者は，官民一体となって宇宙資産のレジリエンスを強化する必要性を唱えている（207-208頁）。

第７章「選挙へのハッキング」では，著者と米国のインテリジェンス関係者のインタビューを基に，2016年の米大統領選へのロシアの干渉のエピソードが再現されている。15年９月と11月，民主党全国委員会のコンピュータがロシアからサイバー攻撃を相次いで受けた。やがて，ロシアのハッカー集団は，ヒラリー・クリントンの大統領選挙対策本部長だったジョン･ポデスタにスピアフィッシング･メールを送り，これをポデスタが開封してしまい，クリントン陣営側の何万通ものメールがロシアに流出し，その後，流出したメールをウィキリークスが1000通程度ずつ小出しに，大統領選挙の日まで公表し続け，その結果，何が起きたかは我々が知っている通りである。著者は，この事例が米国に敵対する国々にとっての選挙干渉の実験になったと指摘し，やや具体性に欠けるが，米国がそれに対抗する力を備える必要性を訴えている（243頁）。

第８章「潜水艦戦争」では，著者が北極海で行われた米海軍の実弾射撃演習（ICEX2018）への参加記録を軸に，米露中の潜水艦競争の話題が進む。近年，気候変動の影響により，北極海の氷が溶け，北極は不毛地帯から石油資源獲得，商業用の新航路，さらには，米露両国の心理的・空間的距離感が縮小した戦略空間となっている。ロシアは，自らの主権領域と見なしている北極からバルト海，黒海，大西洋に至るまで潜水艦の活動範囲を拡大している。また，ロシアは，ステルス性に富む新型の攻撃型潜水艦―第955号計画「ボレイ」級核潜水艦，第885号計画「ヤーセン」級潜水艦―を建造・配備しており，さらに，従来の弾道ミサイルを搭載する攻撃型潜水艦を，より小型で数千フィート下の海底に到達可能な深海潜水艦を搭載できるように改良している。こうしたロシアの小型の深海潜水艦は，北大西洋の海底に敷設された海底ケーブルの観察・移動・切断等の工作活動に従事でき，有事の際のNATO（北大西洋条約機構）の作戦遂行に甚大な影響を与えることができる。中国も驚異的なスピードで潜水艦を建造しており，英国IISS（国際戦略研究所）のデータによれば，2030年までに，軍艦･潜水艦合わせて，中国（260隻）が米国（199隻）を追い越すと予想されている。著者は，米海軍が，監視能力・機動力・ステルス性に富む潜水艦に改良していくこと，旧式艦に固執するのではなく，次世代兵器システムの開発に投資すべきと説く（279頁）。

終章にあたる第９章「シャドウ・ウォーに勝つ」では，米国が中露の仕掛けるシャドウ・ウォーに対抗し，勝利するための解決策として，米国が中露側の動機を見過ごすことなく正確に把握すること，中露が米国側の意図を誤認しないよう明確なレッドラインを設定すること，サイバー・宇宙領域におけるレジリエンスや米国主導の同盟システムの強化等，多岐にわたる詳細な提言がなされている。

本書は，米中露の大国間競争の時代に生きる日本の読者にとって必読の書であり，出版のタイミングも時宜に適っている。エストニアのサイバー攻撃やウクライナ危機を経て，日本の防衛当局の間で，サイバー戦やハイブリッド戦への関心が高まっており，宇宙，サイバー，電

磁波をめぐる安全保障論議も本格化しつつある。また，米国に対し中国が度々しかけている機密情報窃取活動の在り様は，日本における経済安全保障という概念の普及にも一役買っている。もとより，尖閣諸島をめぐり，中国が「力による現状変更」をしかけてくることを懸念している日本にとっては，南シナ海情勢や，米中露の間の潜水艦競争について，海洋安全保障の観点から多くのことを学ばなければならない。

大国間競争の時代にあって，米中露は，しのぎを削っているわけだが，直接的に軍事力を行使する形で対抗されているわけではなく，まさに，「影のなかで」展開していることから，その実態がなかなか掴みにくいのが実情だ。本書を手にとることで，米国が中露発のシャドウ・ウォーに，どのように向き合っているかのみならず，宇宙安全保障，経済安全保障，海洋安全保障等の課題を抱えている日本にとっても，有益な視座を得ることが可能だ。

最後に以下を付言しておきたい。本書・邦訳版のサブタイトルには，「中国・ロシアのハイブリッド戦争最前線」とあるが，これはミスリーディングな文言である。第一に，「ハイブリッド戦争」という用語については，ウクライナ危機以降，米欧の安全保障専門家の間で，頻繁に使用されるようになったが，「どういった現象をハイブリッド戦争と表現するか」という問題について，学術的に決着がついていない。第二に，本書の終章にあたる第９章をのぞく全８章のうち，すべての事例が「ハイブリッド戦争」に該当するかといえば，そうではない。むしろ，ほとんどが，「ハイブリッド戦争」という言葉を用いるまでもない現象だ。第６章や第８章の事例は，宇宙兵器や潜水艦分野での米中露の間の軍拡競争であり，第１章，第３章，第７章の事例は，サイバー・セキュリティーという用語を用いれば事足りる。そもそも，筆者も，これらの事例を説明する際に，「ハイブリッド戦争」という概念を用いていない。

以上のことを踏まえれば，本書のサブタイトルには，「ハイブリッド戦争」の用語を挿入するのではなく，原文サブタイトルのまま「米国を打ち負かす中露の秘密作戦の内幕」にとどめるべきだったのではないだろうかと評者は考える。