サイバー空間における米中対立と安全保障：国際貿易への影響

大澤　淳

US-China Struggle in Cyber Domain and National Security : Implication for International Trade

Jun OSAWA

はしがき

デジタル社会が進展する中で、社会経済活動のネット依存が高まり、それと比例して国家が関与するサイバー攻撃の脅威も増大している。このうち、中国が関与するサイバー攻撃は、「情報窃取型」の特徴を持ち、米国など先端技術を持つ企業から情報を窃取し、米中の対立の焦点の一つとなっている。このようなサイバー攻撃は、産業競争力、ひいては国の競争力にどのような影響を与えるのか。サイバー攻撃は、安全保障上どのような脅威と捉えることができるのか、本章では、そのような問題意識から論述を行った。

本章では、第１節で、サイバー攻撃の様相を明らかにし、国家が関与するサイバー攻撃の特徴を分類する。第２節では、中国による情報窃取型のサイバー攻撃の現状と攻撃グループの目的、そこから導き出される中国の技術戦略とサイバー攻撃との関連性を論述する。さらに、サイバー攻撃によって、知的財産やビジネス秘密が盗まれた事例の検討を通じて、サイバー攻撃による産業競争力の強制移転の現実を描く。第３節では、中国のサイバー攻撃に対する米国の政策対応について概観し、サイバー空間における米中の対立の最近の様相を明らかにする。最後に、このような技術移転が国際貿易に与える影響について、考察を行う。

第１節　サイバー攻撃の様相

1. サイバー攻撃の類型

デジタル・トランスフォーメーションにより、社会・経済活動のデジタル化が進展し、近年インターネットへの社会の依存度が高まっている。それと比例する形で、サイバー攻撃の脅威も増大している。サイバー空間では、国家が関与したとみられるサイバー攻撃が、この15年で急速に増加し、またその被害も深刻化している[1]。このようなサイバー攻撃の中には、民間では防ぐことができない攻撃も出現しており、物理的な武力攻撃と同様の人的・物的損害を引き起こしかねないサイバー攻撃も発生している。

このような国家が関与するサイバー攻撃は、2007年にバルト三国のエストニアで発生した政府・金融機関への機能妨害型のサイバー攻撃以降目立つようになった。サイバー攻撃を類型別に見ると、次の第１表のように整理することができる。

---

[1] Jun Osawa（2017）pp. 114-115.

第１表　サイバー攻撃の類型

情報窃取型：	標的型攻撃（ウィルス付きメール、水飲み場攻撃）などにより、特定の政府機関、企業、団体、個人のネットワーク、PC に侵入し、機密情報、営業情報、特許、知的財産などを窃取する攻撃。
機能妨害型：	DDoS 攻撃等の手法により、ネットワークの許容量を超える飽和通信要求によって、サーバー、ネットワークを麻痺させる攻撃。
機能破壊型：	標的型攻撃などにより、特定の政府機関、企業、団体、個人のネットワークに侵入し、システム破壊・改ざんを行う攻撃。ネットワーク内のデータ消去・改ざんを目的とするものと、制御系システムを標的として物理的破壊を目的とするものがある。
金銭目的型：	標的型攻撃、脆弱性利用などにより、特定の政府機関、銀行、企業、個人のネットワークに侵入し、不正な送金を行い、または PC 内のデータを暗号化し、解読に身代金を要求する攻撃。
情報操作型：	代理主体（Proxy）等を用いて真の発信者を隠匿したうえで、SNS 等に偽ニュースを流布させることにより、対象国（主に民主主義国）における世論操作を目的とした攻撃。選挙結果に影響を与えることを企図している攻撃も見られる。
軍事的サイバー攻撃（ハイブリッド型）：	軍事攻撃と一体的に行われる機能妨害・機能破壊を目的とした攻撃。電子戦の一環として C4I を標的とするものと、軍事行動に影響を与える重要インフラを標的としたものがある。

（資料）各種公開情報より著者作成

2007 年から 2015 年ごろまでの国家が関与する攻撃は、エストニアの事例のような相手国内の混乱の誘発を狙い、重要インフラの制御系システムの麻痺・破壊を目的とする「機能妨害型」／「機能破壊型」サイバー攻撃や、政策決定者や防衛産業など特定の企業・組織・個人から機密情報や知的財産を窃取することを目的とした「情報窃取型」サイバー攻撃が主流であった。

2015 年頃からは、新しい攻撃の様相として、サプライチェーン経由等で企業のネットワーク内に侵入し、データを人質に身代金を要求する「金銭目的型（ランサムウェア型）」サイバー攻撃や、相手国内の情報操作や影響工作を目的として、ディスインフォメーションの流布やサイバー攻撃で窃取した機密情報の暴露などを行う「情報操作型」サイバー攻撃が新たに見られるようになっている。

2. 安全保障上の懸念されるサイバー攻撃と懸念国

国際法上は、「サイバー空間で行われる国家のサイバー活動の内、国家による平時のサイバー諜報は、それ自体は国際法に違反しない（タリンマニュアル 2.0 規則 32）」[2] と整理されており、軍事機関が行う無線通信傍受[3] と同様に、インターネット空間では平時から国家がサイバー手法を用いて情報収集を行うことが認められてきた。また、サイバー空間において、「国家は国際法の規則に従う限り、自国の領域外で自由にサイバー行動をとることができる（タリンマニュアル 2.0 規則 3）」[4] と認識されており、他国の主権侵害や、干渉、武力行使の禁止といった国際法上の禁忌事項に反しない限りにおいて、国家は他国の領域でも自由に行動をすることが国際法上認められている。

しかし近年西側先進国の間で、国家が関与するサイバー攻撃に関して、急速に安全保障上の懸念が高まっている。その理由は大きく次の 3 点に分けられる。

第 1 は、一部の国家が関与して行われている「情報窃取型」サイバー攻撃によって、安全保障上重要な先進技術や企業競争力に直結する重要技術が盗まれ、国家の産業競争力が失われる懸念が生じていること、である。一部の国家は、他国の国家機関を標的とした政策情報の窃取だけでなく、他国の民間企業を標的とした情報窃取を行っている。それにより、窃取した軍事技術を戦闘機などの自国の兵器開発に利用する事例[5] や、窃取した西側民間企業の技術を自国の企業に渡して自国の産業競争力を高める事例[6] が見られるようになっている。

第 2 は、一部の国家が関与して行われている「機能妨害型」／「機能破壊型」サイバー攻撃が、他国の政府や重要インフラ、メディアなどに行われ、攻撃を受けた国において、市民生活が混乱する事例[7] が増加していることである。

第 3 は、「情報操作型」サイバー攻撃を用いて、民主主義プロセスへの干渉を試みる事例が増加していることである。2016 年の米国大統領選挙では、ロシアによる情報操作型のサイバー攻撃が行われ、選挙結果に影響を

---

[2] 中谷他（2018）32-33 ページ

[3] 国際電気通信連合憲章では、第 48 条で「構成国は、軍用無線設備について、完全な自由を保有する」と定められており、軍事機関による通信傍受が国際法上認められている。

[4] 中谷他（2018）7 ページ

[5] 米国の第 5 世代戦闘機 F-22 や F-35 の技術情報がサイバー攻撃によって中国に流出し、中国人解放空軍の J-31 戦闘機に用いられた事例がある。

[6] 中国の人民解放軍と密接な関係にあるサイバー攻撃グループ APT1 は、米国の原子力、太陽光、鉄鋼、非鉄金属企業から技術を窃取したことが知られている。

[7] 例えば、2007 年エストニア、2008 年リトアニア、2013 年韓国、2015 年ウクライナ、等でこのようなサイバー攻撃が発生した。

与えた。同様の干渉は、2016年の英国のブレクジットを問う国民投票、2017年のフランス大統領選挙やドイツの総選挙でも観測されている。

このような安全保障上の懸念の高まりを受け、米国は2018年9月に公表した『国家サイバー戦略』において、「ロシア、中国、イラン、北朝鮮」の4カ国を安全保障上の懸念国と認定し、「サイバーという道具を用いて、我々の経済と民主主義を弱体化させ、知的財産を奪い、我々の民主主義のプロセスに争いのタネを蒔いている」敵対国であると規定した[8]。

米国が懸念国と認定した「ロシア、中国、北朝鮮、イラン」の4カ国は、既存の国際ルールを逸脱したサイバー攻撃を積極的に行っており、安全保障上の脅威となっている。これらの4カ国が関与したと指摘されているサイバー攻撃の特徴は、次の第2表のよう整理することができる。

ロシアは、①周辺国に対する「機能妨害型」／「機能破壊型」サイバー攻撃、②軍事行動に伴う「ハイブリッド戦」、③「情報操作型」サイバー攻撃による民主主義国プロセスへの干渉、が特徴である。

中国は、「情報窃取型」を特徴としている。相手国の政府や政府機関が持つ「政策情報」の窃取に加え、中国の国防技術や科学技術の発展に資する「知財情報」の窃取、中国企業をビジネス上有利にする「企業秘密」の窃取を行っている。加えて、最近ではアジア地域を中心に、ロシアと同様の「情報操作型」攻撃による民主主義プロセスへの干渉も行っている。

北朝鮮は、韓国や米国に対する「機能妨害型」／「機能破壊型」サイバー攻撃に加え、直近では、経済制裁による外貨不足を補うため、「金銭目的型」のサイバー攻撃に従事している。

イランは、主に米国やスンニ派の湾岸諸国に向けられた「機能破壊型」を行っているのが特徴である。

第2表　サイバー攻撃の類型と懸念国

情報窃取型：	中国（技術、政策情報）、ロシア（政策情報）
機能妨害型：	ロシア、北朝鮮
機能破壊型：	ロシア、北朝鮮、イラン
金銭目的型：	北朝鮮
情報操作型：	ロシア、中国
軍事的サイバー攻撃（ハイブリッド型）：	ロシア

（資料）各種公開資料より著者作成

[8] US Department of Defense, “Department of Defense Cyber Strategy 2018 Summary”, Sep. 2018. https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF.

これらのサイバー懸念国のうち、中国は先進国の民間企業、研究所、大学などへの情報窃取型サイバー攻撃を多数実施している。このようなサイバー攻撃は、既存の国際法・ルールから逸脱しているのみならず、攻撃による結果として、先進国の保有する技術の不公正な強制移転をもたらし、先進国の技術優位を脅かしている。この問題は、安全保障上の問題のみならず、自由貿易体制の大きな脅威となっている。後節で詳述するが、このような不公正な手段で入手した技術を用いて、途上国向けの製品を中国企業が製造して輸出している事例も発生しており、自由で公正なルールに基づく自由貿易体制の信頼を揺るがすことになりかねない。

日本でも、中国からの情報窃取型のサイバー攻撃が、2016年以降増加しいていると分析[9]されており、少なくとも10以上の中国関連の攻撃グループが日本を攻撃していると指摘されている。特に防衛、航空・宇宙、ハイテク、医薬など先端産業の知財や企業秘密が狙われており、経済安全保障上もこのようなサイバー攻撃は、日本の産業基盤に対する脅威となっている[10]。

第2節　産業競争力を奪う中国による情報窃取型サイバー攻撃

1. 中国製造2025と中国による情報窃取型サイバー攻撃

「中国製造2025」[11]は、中国国務院が2015年5月に発表した10カ年の産業政策であり、中長期の産業育成戦略が定められている。この文章では、戦略目標として、以下の3段階を経て、中華人民共和国建国の100周年となる2049年までに「製造強国」としての地歩を確立する、としている。その段階は、①2025年までに第一段

[9] FireEye, “APT10（MenuPass Group）: New Tools, Global Campaign Latest Manifestation of Longstanding Threat”, April 6, 2017. https://www.fireeye.com/blog/threat-research/2017/04/apt10_menupass_grou.html.

[10] 内閣官房経済安全保障法制準備室「経済安全保障法制に関する有識者会議」資料、2021年（令和3年）11月26日。

[11] 原典は中国国務院のホームページに掲載された「国务院关于印发《中国制造2025》的通知」（2015年5月8日）であるが、米中間の対立の焦点となったことから、現在は掲載されていない。日本語訳については、科学技術振興機構の日本語訳を参照。https://www.jst.go.jp/crds/pdf/2015/FU/CN20150725.pdf

階の製造強国への仲間入り、② 2035 年までに第二段階のイノベーション牽引国である製造強国の中位レベルの達成、③ 2049 年までに第三段階の大半の分野での産業競争優位を確立する「製造強国」の地位確立、を達成するとなっている。

「中国製造 2025」の序文では、国際競争力のある製造業こそが、中国の国力を増大させ、国家安全保障を確かにし、世界の強国として中華民族が復興するために、欠かせない、と述べられている。

「製造強国」の実現に向けて、具体的に 10 の重点産業育成分野が定められている。それらは、①次世代情報技術、②新エネ自動車、③航空・宇宙、④海洋工学（ハイテク船舶）、⑤先進鉄道、⑥ロボット・工作機械、⑦電力設備、⑧新素材、⑨バイオ医薬・医療機器、⑩農業機械、である。

これらの重点産業分野を育成する手法として、自主的な技術開発だけでなく、先進技術を持つ外資の積極誘致による技術移転の促進を掲げているのも特徴である。次世代情報技術や新材料、バイオ医薬などの外国企業を誘致し、中国国内の開発拠点設立を促す、としている。また、中国企業のグローバルな進出を促進し、海外での合併・買収や株式投資を促進するとも述べられており、投資を用いた外国技術の取り込みを行うことが示されている。

当然のことながら、「中国製造 2025」の本文には、違法な手段で技術を移転し、自国の産業競争力を強化するとは一言も書かれていない。しかしながら、次に見ていくように、サイバー空間においては、「中国製造 2025」の重点分野に掲げられた企業に対する、情報窃取型のサイバー攻撃が発生している。

中国を攻撃の発信源とする情報窃取型サイバー攻撃は、主に先進国の知的財産を狙って行われており、中国の国家の関与が疑われている。これらの攻撃は、先に述べた中国の中長期的な科学技術政策「中国製造 2025」と密接な関係性がみられる。中国のサイバー攻撃者がターゲットとしているのは、①次世代情報技術、②新エネ自動車、③航空・宇宙、④海洋工学、⑤新素材、⑥電力設備、といった産業であり、これらの産業群は、「中国製造 2025」で重点育成分野として定められた項目と一致している。

具体的な事例として、航空・宇宙分野の技術窃取を狙ったとみられるサイバー攻撃が 2021 年 4 月に発覚[12]している。同年 4 月 20 日、警視庁は、中国共産党員の男を私電磁的記録不正作出・同供用の疑いで書類送検した。この男は、日本国内でレンタルサーバーを借りていたが、その目的は中国のサイバー攻撃グループ「Tick」に、サイバー攻撃に利用する中継サーバーとして使用させるためであった。この男が契約したレンタルサーバーは、宇宙航空研究開発機構（Japan Aerospace Exploration Agency：JAXA）をはじめ三菱電機や IHI、大学など、防衛・航空宇宙関連の約 200 の企業や研究機関へ行われたサイバー攻撃で、マルウェアに指示を出すために用いられていた。この攻撃グループ「Tick」は、我が国以外でも、アメリカ航空宇宙局（National Aeronautics and Space Administration：NASA）やドイツ航空宇宙センター（Deutsches Zentrum für Luft-und Raumfahrt： DLR）などの宇宙関連の研究機関を標的とする攻撃を行っていた。

警察庁は別の中国人留学生の男も事情聴取しているが、この留学生は中国人民解放軍の関係者から指示を受け、日本製セキュリティソフトの購入やサーバーの契約などの協力をしていたことが明らかになっている[13]。松本警察庁長官は 4 月 22 日の記者会見で、「Tick の背景組織として、山東省青島市を拠点とする中国人民解放軍戦略支援部隊ネットワークシステム部第 61419 部隊が関与している可能性が高いと結論付けた」と述べている[14]。

先進技術を有する日本企業を標的として、知的財産や特許を狙った情報窃取型のサイバー攻撃には、この「Tick」以外に 10 を超える中国の攻撃グループが活動していることが分かっている。

2. 先進技術を狙う中国のサイバー攻撃グループ[15]

2012 年 10 月 25 日、アメリカのニューヨーク・タイムズ紙は、中国の温家宝首相（当時）の一族が 27 億ドルの資産を蓄財してきたと報じた[16]。一見してサイバーと何ら関係ないと思われるこの報道は、その後のサイバー空間における米中の熾烈な対立の発火点となった。

報道の直後から、中国人民解放軍と関係あるサイバー攻撃グループ「APT1」が、ニューヨーク・タイムズ紙のネットワークに対する必要なサイバー攻撃を開始し、記事を執筆した同紙上海支局の Barboza 支局長と同紙のインド南アジア支局の Yardley 支局長のメールを

---

[12] 国家公安委員会、国家公安委員会委員長会見要旨、2021 年（令和 3 年）4 月 22 日。
https://www.npsc.go.jp/pressconf_2021/04_22.htm

[13] Ibid. 国家公安委員会委員長会見要旨。

[14] Ibid. 国家公安委員会委員長会見要旨。

[15] このような特定の標的に対してサイバー攻撃を行うグループをサイバーセキュリティ業界では、（Advanced Persistent Threat: APT）と読んでおり、APT ○○というかたちで番号を振って区分けしている

[16] David Barboza, “Billions in Hidden Riches for Family of Chinese Leader”, New York Times, October 25, 2012.

ハッキングしたのである[17]。ニューヨーク・タイムズ紙に対するサイバー攻撃は、2013年1月に発覚したが、この攻撃の調査を担当した米セキュリティ会社Mandiant社の分析によって、米国の幅広い産業界を標的とした、中国人民解放軍によるサイバー攻撃作戦の全貌が明らかになった。

Mandiant社が発表した報告書[18]によれば、ニューヨーク・タイムズ紙を攻撃した「APT1」は、中国上海に拠点を置く、人民解放軍（PLA）総参謀部第三部第二局（当時）傘下の第61398部隊であり、この攻撃グループは2006年以降7年以上の長期にわたって、米国のメディアだけでなく、幅広い産業を標的としたサイバー攻撃を行っていた。標的となった産業は、情報、運輸、ハイテク、金融、法律事務所、エンジニアリング、メディア、食糧・農業、宇宙、衛星通信、化学、エネルギー、医療、など広範囲に渡っていた。

この「APT1」による知的財産およびビジネス秘密の情報窃取型サイバー攻撃が明らかになって以降、中国の国家機関が関与するサイバー攻撃に対して、米国は攻撃者を特定し、司法訴追を含むあらゆる政策を動員して、強い対抗措置を取り始めている。中国の国家機関による米国民間企業へのサイバー攻撃では、米国政府への攻撃で使われているのと同じサイバー攻撃技術が用いられている。国家機関が開発した最先端（state-of-the-art）のサイバー攻撃ツールを、民間企業への攻撃に使われたのでは防ぎようがない。米国の強い憤りの背景には、そのような中国のサイバー攻撃のやり方が「不公正＝アンフェア」という判断がある。

米司法当局は2014年5月、攻撃グループ「APT1」の実行犯として、人民解放軍61398部隊に所属する将兵5名を訴追した[19]。訴追状によれば、人民解放軍の将兵は、2006年から2014年にかけて、米国のWestinghouse Electric社（原子炉）、SolarWorld社（太陽光発電）、US Steel社（鉄鋼）、Allegheny Technologies社（特殊金属）、Alcoa社（アルミ）などに情報を窃取する目的で侵入し、情報を窃取した。これらの攻撃実行犯は、コンピュータへの不正侵入の罪だけでなく、経済スパイおよび企業秘密窃取の罪で訴追されている。

「APT1」は、主に米国を標的とする中国のサイバー攻撃グループであったが、中国のサイバー攻撃の標的は米国にとどまらない。先進国の技術を狙う同様な攻撃グループに「APT10」が知られている。この攻撃グループは、クラウドサービスなどを提供するサプライヤーを標的として攻撃し、その顧客である政府機関・企業の機微情報・知的財産の窃取を行っていた。「APT10」は、政府機関のみならず、製薬、鉱業、エネルギー、金属、エンジニアリング、工業生産、技術産業、小売など多岐にわたる産業を標的として「情報窃取型」サイバー攻撃を繰り返していた。

2017年4月、英大手防衛産業のBAEとコンサルティング大手のPWCは、英国政府の国家サイバーセキュリティセンター（National Cyber Security Center：NCSC）の協力を得て、「APT10」のサイバー攻撃に関する報告書を公表した[20]。同報告書では、APT10が行なっているサイバー活動を「Operation Cloud Hopper」の名付けた上で、APT10が中国に拠点を置く大規模なサイバー攻撃集団であり、2016年頃から新しい攻撃技術を用いて作戦を実施したと分析している。その新しい手法とは、世界中のマネージドITサービスプロバイダ（Managed Service Provider：MSP）を標的としてサイバー攻撃を行い、MSPの顧客企業に対する前例のない大規模なアクセス権を得て企業ネットワークに侵入を計るものであった。特に標的となった国は、日本、インド、米国、英国、カナダ、オーストラリア、タイ、ブラジル、南アフリカ、韓国、スイス、フランス、ノルウェー、フィンランド、スゥェーデンであり、とくに日本では多数のAPT10による攻撃が観測されていた。

米国は英国などの同盟国とともにこの「APT10」の攻撃者に対するアトリビューション（帰属性解決）を実施し[21]、中国の国家安全部と関係がある攻撃者2名を具体的に特定した。米司法省は、2018年12月、サイバー攻撃によって、45以上の企業の技術情報を窃取したとして、中国人二名（朱华（Zhu Hua）、张士龙（Zhang

---

[17] Nicole Perlroth, “Hackers in China Attacked The Times for Last 4 Months”, New York Times, January 30, 2013.

[18] Madiant, “APT1: Exposing One of China’s Cyber Espionage Units”, (2013.2).

[19] US Department of Justice, “U.S. Charges Five Chinese Military Hackers For Cyber Espionage Against U.S. Corporations And A Labor Organization For Commercial Advantage”, May 19, 2014. https://www.justice.gov/usao-wdpa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and

[20] PWC/BAE, ”Operation Cloud Hopper: Exposing a systematic hacking operation with an unprecedented web of global victims”, April, 2017. https://www.pwc.co.uk/cyber-security/pdf/cloud-hopper-report-final-v4.pdf

[21] UK Government, “UK and allies reveal global scale of Chinese cyber campaign”, December 20, 2018. https://www.gov.uk/government/news/uk-and-allies-reveal-global-scale-of-chinese-cyber-campaign

Shilong)）を訴追したと発表した[22]。中国天津のテクノロジー企業の社員であったこの2名は、国家安全部天津支局と協力して、2006年から2018年にかけて、少なくとも十二カ国の多岐にわたる企業から情報を窃取していたことが訴追状から明らかになっている[23]。2名が標的としていた個別企業の名前は開示されていないが、航空、宇宙・衛星、製造機械、製薬、石油ガス探査、通信、半導体、海洋工学、といった産業を標的としていた。

APT1やAPT10のように先進国の先端産業を攻撃対象とする中国のサイバー攻撃グループは、サイバーセキュリティの関係者で知られているだけでも数十におよび、主なものでも次の第3表にあげた十数グループが知られている。サイバー攻撃は、投資制限条項や様々な政策による外国企業に対する技術移転の強制、最先端技術を有する外国企業の買収による技術の獲得と並んで、ビジネス秘密や知的財産を窃取し外国企業から技術を獲得する重要な手段となっている。

第3表　中国のサイバー攻撃グループと攻撃対象

攻撃グループ（所属）	攻撃対象
APT1	政府機関、先端産業全般
APT4	航空宇宙、防衛産業
APT9	宇宙、農業、建設、エネルギー、医療、ハイテク、メディア、交通
APT10（国家安全部）	政府機関、シンクタンク、防衛産業、宇宙、医療、メディア
APT12（人民解放軍）	防衛関連企業（特に衛星、暗号技術）、メディア
LODEINFO（APT10の可能性）	政府系機関、主要メディア、シンクタンク
APT15	商社、エネルギー、金融、防衛産業、外交当局、ウィグル族関連
APT16	政府機関、ハイテク関連、メディア、金融関連
APT17	政府機関、防衛産業、航空産業、IT企業、法律事務所
Tick（PLA 61419部隊）	政府機関、防衛関連組織、通信、電機、重工業（造船関連）、ハイテク関連、化学、メディア
Dragon Ok	大学・学術機関（科学技術）、ハイテク、製造業
APT41/ Winnti	ハイテク関連製造業、化学、電子商取引、投資ファンド、エレクトロニクス、テレコム、オンラインゲーム
Black Tec（別名PLEAD）	メディア、建設、エンジニアリング、電機、金融
Tonto （PLA）	自動車産業

（資料）各種公開情報より著者作成

3. 情報窃取型サイバー攻撃による産業競争力への影響事例

このような中国のサイバー攻撃を放置した場合、企業の産業競争力にどのような影響が出るのであろうか。具体的にいくつかの事例を基に検討していきたい。

カナダにかつてNortelという通信機器大手の会社があった。同社は、現在のインターネット時代に不可欠なネットワーク制御機器に強みを持つ優良企業であり、次世代無線通信技術の4G, 5Gを開発していた。しかし、安価な競合製品の登場などから2009年に経営破綻した。優良企業が急に破綻した大きな原因となったのが、中国からのサイバー攻撃であった。

「中国による広範なサイバー攻撃が企業崩壊の一因なにった」とメディアのインタビューで、Nortel社上級システムセキュリティ顧問たったブライアン・シールズは、答えている[24]。中国のサイバー攻撃グループは、2000年から数年にわたって、同社の技術マニュアルや調査研究リポート、事業計画書、従業員の電子メールなどを含む文書を盗んでいたことが明らかになっている。Nortelが経営破綻した後、同社の移動体通信技術は、競合のHuaweiへと伝播していった。Huaweiは、Nortelの破綻後、5Gの開発に従事していた同社の技術者20名を雇用している[25]。現在、「フェーウェイ・フェロー」の称号を与えられた童文と朱佩英は、ともにNortelでワイヤレス技術研究に長年携わったのち、2009年にHuaweiに入社し、同社の5G開発の中心人材となっている。

米国の事例では、APT1のサイバー攻撃を受けた東芝の子会社で原子力関連企業Westinghouse Electric社やドイツ企業の子会社で太陽光発電パネル製造のSolarWorld社がある。

---

[22] US Department of Justice, “Two Chinese Hackers Associated With the Ministry of State Security Charged with Global Computer Intrusion Campaigns Targeting Intellectual Property and Confidential Business Information”, December 20, 2018. https://www.justice.gov/opa/pr/two-chinese-hackers-associated-ministry-state-security-charged-global-computer-int rusion

[23] ニューヨーク州南地区裁判所「アメリカ合衆国対朱および張」訴追状 https://www.justice.gov/opa/press-release/file/1121706/download

[24] “Nortel collapse linked to Chinese hackers”, CBC News, February 15, 2012.

[25] Natalie Obiko Pearson, “Did a Chinese Hack Kill Canada’s Greatest Tech Company?”, Bloomberg Businessweek, July 1, 2020. https://www.bloomberg.com/news/features/2020-07-01/did-china-steal-canada-s-edge-in-5g-from-nortel

Westinghouse Electric は 2006 年に東芝に買収されたが、2010 年代には世界で最先端の第 3 世代加圧水型軽水炉 AP1000 を主力商品とし、この分野で最も競争力のある企業であった。この AP1000 は、2008 年から中国に輸出され、同社と中国国家核電技術公司の間で技術開発協力協定が締結された。

中国のサイバー攻撃グループ APT1 は、この直後の 2010 年から 2011 年にかけて Westinghouse Electric 社にサイバー攻撃を行い、AP1000 に関する技術情報を窃取した。先に述べたように、米国司法当局は中国人民解放軍の将兵 5 人を起訴しているが、起訴状の中で、原子炉に関する独占的で機密性の高い技術と設計仕様が盗まれ、これにより（中国の）競合他社が設計のための開発にかかる研究開発費を圧縮できた、と告発している。サイバー攻撃後、AP1000 の技術は中国に渡り、競合製品として中国製の CAP1400（2017 年型式認可）が登場した。競合製品により、Westinghouse Electric 社の中国および途上国でのビジネスがうまくいかなくなり、同社は 2017 年原子炉建設事業の赤字が原因でチャプター 11 に基づく破産保護を申請し倒産している。

SolarWorld 社も Westinghouse Electric 社と同様に、2017 年にチャプター 11 を申請して倒産した企業である。SolarWorld 社も太陽光発電設備の製造では、当時世界的に有数な競争優位を持つ企業であった。中国のサイバー攻撃グループ APT1 は、2012 年頃から SolarWorld 社にサイバー攻撃を実施し、中国の太陽光発電設備製造企業に有利となる企業秘密を窃取していた[26]。サイバー攻撃によって盗まれたものは、同社の製品の設計図だけでなく、製品価格や米国の規制を回避して市場に参入する方法など多岐にわたっており、結果として、安い中国製の競合製品が大量に米国市場に流れこむこととなった。

このように、中国による国家が関与する情報窃取型サイバー攻撃によって、米国の多くの企業が知的財産および設計情報を盗まれ、米国市場のみならず世界の市場での競争力を失う事例が 2010 年代後半に多く見られるようになった。

第 3 節　サイバー空間における米中の対立と国際貿易への影響

1. 中国のサイバー攻撃への複合抑止政策：積極的サイバー防御

中国の国家機関が関与するサイバー攻撃に対して、米国は攻撃者の行動を抑止する柔軟抑止戦略（Flexible Deterrence Option：FDO）の一環として積極的サイバー防御（Active Cyber Defense：ACD）を実施している。ACD は、誰が攻撃を行っているのかをアトリビューション（帰属性の解決）に基づいて特定し、外交的圧力、司法訴追、経済制裁、サイバー反撃を含むあらゆる政策を動員して攻撃側の負荷を増大させ、攻撃に対抗措置を取る政策である。

第 2 節で検討した APT1 によるサイバー攻撃に対しては、2013 年 2 月にセキュリティ企業によるレポートという形で、中国人民解放軍の関与を名指しし、さらに、2014 年 5 月には、米司法当局が人民解放軍の将兵 5 名を攻撃の実行犯として訴追した。さらに外交面では、2015 年 9 月の米中首脳会談で、当時のオバマ大統領がこの問題を習近平国家主席に提起し、オバマ大統領は共同記者会見で「米中両国は経済的なサイバー情報窃取を行わず、支援しないと合意した」[27] と発表した。

米中首脳会談後、中国から米国企業へのサイバー攻撃は著しく減少した。しかし、その効果は 1 年半ほどしか続かず、第 2 節で見たように、APT10 のようなのサイバー攻撃が発生したため、米国政府は司法訴追を含むより厳しい措置に移行している。

2016 年 7 月、中国人民解放軍の将校と結託して米国の防衛産業からサイバー攻撃で情報窃取をしていたとして、中国籍の男に懲役 46 ヶ月、罰金 1 万ドルの判決。2017 年 11 月、金融、エンジニアリング企業からサイバー攻撃で情報窃取をしていたとして、中国広東省にある広州博御信息技術有限公司の経営陣ら中国人 3 名を起訴。2018 年 10 月、航空機のジェットエンジン技術に関わる企業秘密を窃取していたとして、中国国家安全部江蘇省庁の高官 2 名と中国人ハッカー 5 名を起訴。2018 年 11 月、DRAM 製造に関わる企業秘密を窃取したとして、産業スパイ活動の罪で福建省晋華集成電路とその関係者を訴追。2019 年 5 月、米大手保険会社 Anthem から米国人の個人情報 7800 万件をサイバー攻撃で窃取し

[26] Shane Harris, “Exclusive: Inside the FBI’s Fight Against Chinese Cyber-Espionage”, Foreign Policy, May 27, 2014. https://foreignpolicy.com/2014/05/27/exclusive-inside-the-fbis-fight-against-chinese-cyber-espionage/

[27] 発表原文は以下の通り。“We’ve agreed that neither the U.S. or the Chinese government will conduct or knowingly support cyber-enabled theft of intellectual property, including trade secrets or other confidential business information for commercial advantage.” White House Press Release, September 25, 2015.

たとして、中国人2名を訴追。2020年2月、米国人の大量の信用情報をサイバー攻撃で窃取したとして、中国人民解放軍第五十四研究所に所属していた4名の中国人を訴追。2020年3月、中国人2名を暗号通貨のマネーロンダリングの罪で起訴。2020年7月、世界中の企業などを標的にして、知的財産及びビジネス秘密を十年以上にわたりサイバー窃取していたとして、中国国家安全部に関係する2名の中国人ハッカーを訴追。2020年9月、米企業など世界100社以上の企業から情報を盗んだとして、中国人5名を訴追。2021年7月、米司法省は、潜水艦などの軍事技術や自動運転といった最先端技術などに関する情報を狙い、世界各国でサイバー攻撃を行ったとして、国家安全部傘下の中国人4人を起訴。

以上のように、米国の中国に対する対応は、2018年前後を境として大変厳しいものとなっている。

2. 米中対立の国際貿易への影響

これまで見てきたような情報窃取型サイバー攻撃による知的財産やビジネス秘密の窃取は、中国の技術獲得の中核に据えられているとの分析がある[28]。そのため、米国政府は、中国が自国の5カ年計画の重点分野に沿ってサイバー窃取を行っているとの疑いを深めている[29]。

知的財産を狙った情報窃取型サイバー攻撃は、結果的に中国の技術力を強化し、中国の産業競争力を押し上げ、中長期的には国家間の力関係に重大な影響を及ぼす。マイケル・ピルズベリーは、著書『The Hundred-Year Marathon』の中で、中国の長期的な戦略目標は、アメリカから覇権国の地位を奪い、中国中心の世界秩序を確立することであると分析しており、「国際市場への拡大を図る中国だがルールに従うつもりなどない」と警告している[30]。薬師寺泰蔵が、著書『テクノヘゲモニー』で述べている[31]ように、技術は模倣によって国から国へと伝播するのが歴史の常ではあるが、中国の場合は、明らかにルールを逸脱していると言えよう。

米国通商代表部（United States Trade Representative：USTR）は、2018年3月に中国の技術移転政策に関する調査報告書[32]を公表した。同報告書でUSTRは、中国政府を名指しで非難し、中国の長期的技術優位獲得戦略である「中国製造2025」の戦略目標に沿って、中国政府が、①投資制限条項や様々な政策を用いて米国企業に対して技術移転を強制、②中国政府の産業計画に掲載された最先端技術を有する米国企業を買収して技術を獲得、③戦略目標に沿って米国企業にサイバー攻撃を実施し、ビジネス秘密や知的財産を窃取、と指摘している。

USTRの報告書を受けて、当時のトランプ大統領は、対中政策のメモを発表し、通商法301条に基づき、中国の不公正な貿易に対して、関税、WTOへの提訴、米国への投資制限からなる強い対抗措置を取ると表明した[33]。

2019年度国防権限法案（H.R.5515, 2018年8月1日上院通過、8月13日大統領署名成立）では、ハイテク分野、通信技術分野における中国政府への強い警戒感が表明されている。第889節で政府機関に対し、中国通信機器大手「中興通訊」（ZTE）や「華為技術」（ファーウェイ）等の製品を用いた調達を禁止。さらに、両者等の機器を用いている企業体との契約も禁止した。その理由として、中国製ネットワーク機器の利用によって、サイバー攻撃の入り口とも言える、不正アクセスが急増したことを挙げている。

これまで見てきたように、米国政府は2018年以降、中国による民間企業へのサイバー攻撃に対して、非常に厳しい対応をとるようになってきている。これらのサイバー手段を用いた情報窃取は、強制技術移転によって、中国の技術力を強化し、中国の国力を増大させる。中長期的には、国家間の力関係に重大な影響を及ぼし、中国を覇権国として押し上げるのではないかとの危機感がある。

今後米国は、そのような技術の不公正な移転を、輸出管理や安全保障目的のための投資管理といった側面だけでなく、積極的サイバー防御で抑止していくと分析される。

さらに、サイバー攻撃など不正な手段によって入手し

---

[28] 例えば、以下を参照。Hannas, Mulvenon and Puglisi（2013）.

[29] Gina Chon & Charles Clover ‘US spooks scour China’s 5-year plan for hacking clues’（Financial Times, November 25, 2015）
http://www.ft.com/intl/cms/s/0/40dc895a-92c6-11e5-94e6-c5413829caa5.html

[30] Pillsbury（2015）, 邦訳266ページ。

[31] 薬師寺泰蔵（1989）。

[32] USTR, “FINDINGS OF THE INVESTIGATION INTO CHINA’S ACTS, POLICIES, AND PRACTICES RELATED TO TECHNOLOGY TRANSFER, INTELLECTUAL PROPERTY, AND INNOVATION UNDER SECTION 301 OF THE TRADE ACT OF 1974”, March 22, 2018. https://ustr.gov/sites/default/files/Section%20301%20FINAL.PDF

[33] The White House, “Presidential Memorandum on the Actions by the United States Related to the Section 301 Investigation”, March 22, 2018. https://www.whitehouse.gov/presidential-actions/presidential-memorandum-actions-united-states-related-section-301-investigation/

た技術による中国製品は、公正な競争による貿易品と認められなくなる可能性もある。実際に、2020年1月の日米欧三局貿易大臣会合共同声明では、「強制技術移転について、（中略）、不公正な慣行は市場原理に基づいた国際貿易システムと不整合であり、成長と土台を損なう」と表明し、「有害な強制技術移転政策および措置を止めるための効果的な方法に対するコミットメントについて議論した」としており、今後サイバー攻撃の防止も含めて、国際ルールの議論が進むと思われる。

参考文献

大澤淳（2020），「米中サイバー戦争の様相とその行方」川島真・森聡編『UP plus アフターコロナ時代の米中関係と世界秩序』東京大学出版会。

大澤淳（2020），「デジタル覇権を巡る米中対立の様相」安全保障防衛機情報センター『CISTEC ジャーナル』第187号。

大澤淳（2021），「産業競争力を奪うサイバー攻撃の脅威」産経新聞社『正論』2021年7月号。

大澤淳（2021），「中国とデジタル覇権の夢」慶應義塾『三田評論』2021年8、9月号。

中谷和宏，河野桂子，黒崎将広（2018），『サイバー攻撃の国際法：タリンマニュアル2.0の解説』信山社。

薬師寺泰蔵（1989），『テクノヘゲモニー』中央公論社。

Bernner, J.（2011），America the Vulnerable：Inside the New Threat Matrix of Digital Espionage, Crime, and Warfare, Penguin Books, London.

Hannas, W., Mulvenon, J. and Puglisi, A.(2013), Chinese Industrial Espionage, Routledge, London.

Lindsay, J.R., Cheung, T.M. and Reverson D.R.(2015), China and Cybersecurity：Espionage, Strategy, and Politics in the Digital Domain, Oxford University Press, New York.

Osawa, J.(2017), “The Escalation of State Sponsored Cyberattack and National Cyber Security Affairs：Is Strategic Cyber Deterrence the Key to Solving the Problem?”, Asia-Pacific Review, vol.24, No.2：113–131.

Osawa, J.(2021), “The Cyber Threat Landscape and Japan’s Policy Challenges”, International Centre for Defence and Security, Report：So Far, Yet So Close Japanese and Estonian Cybersecurity Policy Perspectives and Cooperation, International Center for Defense and Security（Estonia）.

Pillsbury, M.（2015），The Hundred-Year Marathon, Henry Holt and Company, New York.（野中香方子訳，（2015）『China 2049』日経BP。）

Sanger, D.E.(2018), The Perfect Weapon, War, Sabotage, and Fear in the Cyber Age, Crown, New York.

Spalding, R.(2019), Stealth War：How China Took Over while America’s Elite Slept. Portfolio/Penguin.