2023 年 3月

サイバー攻撃の標的でもある中国

1 はじめに

1.1 本稿の目的

高度に標的化された、持続的な脅威となるサイバー攻撃は「Advanced Persistent Threat（APT）」と呼ばれる。こうした攻撃活動に関わる組織化された集団「APT グループ」は国家や政府を背景に持つことが多い。したがって、明確な意図と目的のもとに複雑且つ高度なテクニックを使用し、長期間にわたって秘密裏に特定の国／地域の標的を監視、情報を窃取する。また、APT グループは政治や治安状況とも密接に関連しており、状況が複雑な地域における APT 攻撃の被害はより深刻となる。よって、セキュリティ研究者は APT グループに命名する前にグループ間の類似性を比較、分析し、地政学的要因を踏まえながらグループの意図や動機を理解する[1]。では、隣接する国の多い中国が被る APT の状況はどうだろうか。

日本の我々が普段目にする情報は、米国を拠点とするセキュリティ企業に由来するレポートや、こうした企業の英語レポートを日本語に翻訳した情報であることが多い[2]。よって、APT グループの背後にある集団として、ロシア、北朝鮮、イラン、そして「加害者」の顔をもつ中国がよく登場するのではないだろうか。ところが、中国のセキュリティ企業がほぼ毎年のレポートのなかで「中国は世界的にみて、最も APT 攻撃の被害を受けている国だ」と主張していることはご存じだろうか。中国のセキュリティ企業が中国語で記した脅威レポートのランドスケープには、米国のセキュリティ企業が描くものとは異なった景色が浮かんでいる。言い換えれば、日本の我々が普段多く依拠している情報は、サイバー空間で観測される事象のある側面のみしか反映していないことになる。

こうしたことから本稿では、中国のセキュリティ企業や政府が発信する、中国語で書かれたリソースを基にして中国が被るサイバー攻撃の状況や、同国が抱えている問題を知り、「サイバー攻

撃の標的となる側の中国」という新たな視点を設けることによって、サイバー空間で観測される事象を別の側面からも理解することをめざす。サイバー空間で発生している趨勢をより俯瞰した立場から理解することで、日本のおかれる地政学的な立ち位置や、サイバーセキュリティに関して、今後日本がとるべき方針の一助となることを期待しているためである。

読者には、外交・安全保障に関連する担当者、企業のリスクマネージャー、中国のサイバー動向に関心を持つ個人などを想定している。攻撃に使用された手法や技術詳細をコラムに引用することは最小限にとどめた。こうした事項について参考にされたい場合は、文末脚注にリソースを掲載したため、セキュリティ企業の各レポートを参考にしていただきたい。

なお、引用／参考元の中国語文献は中国法の順守が求められる企業が作成した文献である。従って、中国共産党の思想や中国政府の意図が反映されている可能性を読者は念頭に置く必要があることを付記する。

1.2 アプローチ

中国を取り巻くサイバー空間の趨勢や中国が抱える問題を知るために、本稿は中国のセキュリティ企業によって中国語で執筆された APT グループや脅威についてのレポートを参考にしてグループの活動の動機・目的を検討した[3]。対象期間は 2016 年～2022 年に限定し、**期間Ⅰ：ハイテク化が進んだ期間（2016 年～2017 年）**、**期間Ⅱ：対中圧力が高まった期間（2018 年～2019 年）**、**期間Ⅲ：新型コロナウイルス感染症の流行以降（2020 年～2022 年）**に区別した。2015 年以前に公開されている情報は数が少ないため今回の対象範囲外とした。調査の対象とする APT グループは、中国を頻繁に攻撃、或いは中国に対して深刻な影響を与えたと中国の企業が主張する 6 つのグループ、即ち、ベトナムの「**海蓮花**」、インドの「**蔓霊花**」、台湾の「**毒雲藤**」、韓国の「**Darkhotel**」、米国の「**Longhorn**」と「**方程式**」に限定した[4]。**2 章**ではⅠ～Ⅲの各期間の傾向を理解し、**3 章**では各グループの活動の動機や目的を考察する構成とした。また、APT 集団の呼称は敢えて中国のセキュリティ企業によく使用されている名称を使用した[5]。

2 中国を標的とする攻撃の変遷

本章では、2016 から 2022 年にかけて中国において標的となった組織が変化していく様や、中国におけるサイバー脅威の変遷を理解する。繰り返しになるが、以降は中国のセキュリティ企業によって中国語で執筆された APT グループや脅威についてのレポートを情報源としている。従ってグループの活動の動機・目的については中国が主張する観点に基づいた記述が登場することを再度付記しておく。

2.1 期間Ⅰ：ハイテク化が進んだ期間（2016 年～2017 年）

2016 年は中国の今後 5 年間にわたる社会・経済戦略を示す『第 13 次五カ年計画』（「十三五」）が始動した年である。十三五期間は、中国の国力を示すために国防・科学・経済の強化、すなわち中国のハイテク化が重視された期間に相当する[6]。十三五期間開始直前の 2015 年 12 月末に中国は「戦略支援部隊」傘下にサイバー戦部隊を編成した。米国やロシアに対して遅れをとる中国の APT 研究レベルについても警鐘が鳴らされた[7]。中国独自の視点にもとづく APT 研究は十三五期間中に躍進している。また、2017 年は中国共産党にとって重要な年であった。同年 6 月には『サイバーセキュリティ法』や『国家情報法』が相次いで施行された他、10 月に中国共産党の第 19 回全国代表大会（「十九大」）が開催された。

北上する脅威とアトリビューションの外交利用に関する注目

2016 年の中国におけるサイバー攻撃は広東省（香港とマカオを除く）に最も集中し、次いで北京と沿岸部に集中したと中国のセキュリティ企業「360 数字安全集団」（以降「360」）が報じた[8]。31 省／行政区域に存在する組織・個人が 36 種類の APT グループによる攻撃の標的となり、分野別の内訳は、大学への攻撃（40%）、次いで通信・海洋・エネルギー・航空宇宙などの企業（25%）、そして外交・海洋といった政府機関（18%）であった[9]。360 は、「サイバー空間は大国の新しい戦場である」と形容し、一帯一路と軍民統合が今後の他国によるサイバー攻撃の焦点となることや、中国のインフラに対する破壊的攻撃が活発化するであろうことを推測した[10]。

2017 年になると、中国を狙う APT グループによる攻撃の被害を受けた地域が北上した（**図 1**）。同年に最も攻撃を受けたのは遼寧省と北京、次いで山東省、江蘇省、上海、浙江省となっており、前年に最も攻撃を受けた広東省を上回った。分野別にみると、2017 年に最も攻撃を受けたのは政府（50%）であり、この次に狙われたのはエネルギー分野（25%）であった[11]。

2017 年は世界で WannaCry が猛威を振るった年であった。米国は「WannaCry は北朝鮮により作成されたものである」と同国を強く批判した[12]。これに関しては 360 が「他国の APT 活動を非難することは重要な外交手段である」と評価した[13]。そしてこれ以降、中国のセキュリティ企業によるアトリビューションは増加し、より詳細な脅威分析が議論されるようになった。

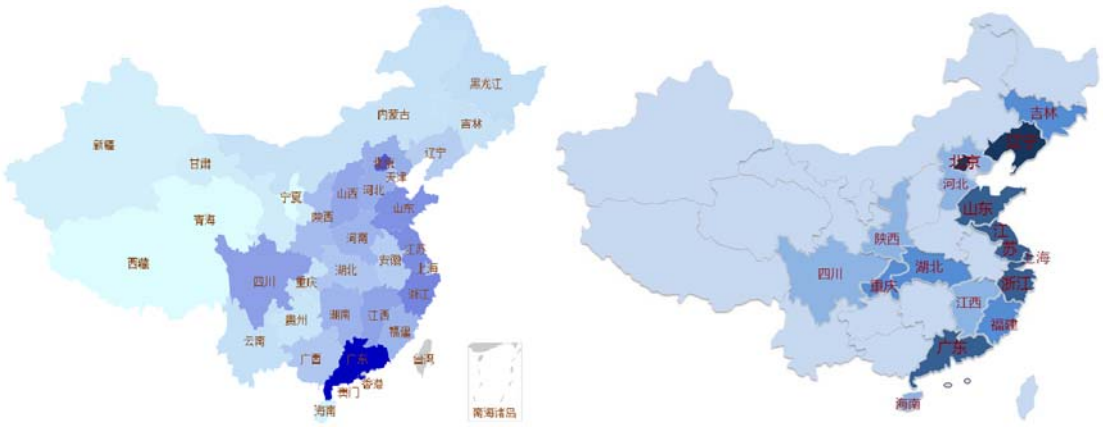

図 1 省級行政区別の攻撃分布の比較。2016 年（左）と 2017 年（右）

【出典】360『2016 年中国高級持続性脅威研究報告』P.7 および『2017 年中国高級持続性脅威研究報告』P.6

2.2 期間Ⅱ：対中圧力が高まった期間（2018 年～2019 年）

この 2 年間は、国際情勢のなかで存在感を増す中国と他国／地域との利害関係の衝突が顕著となった期間であると同時に、米国による対中圧力が強まって中国の政策に特に影響を与えた時期でもある（**3.5** で後述）。例えば 2018 年に、中国は米国から「同国との競争は米国の安全保障上の主要な懸念」という評価を受けている[14]。同年 7 月 6 日には米国が中国に対する追加関税制裁を発行しており、その同時刻に中国は米国に対して報復措置を開始した[15]。その後も双方の追加関税の

応酬が発生した。同年 8 月には、ファーウェイ（華為）など中国大手通信機器メーカーの製品は、米国政府機関での使用が禁止となり、中国はこれに反発した[16]。さらに、米国から台湾への武器売却や高官訪問といった両岸問題を巡っても中国による強い反発が発生した[17]。

APT と国家間の駆け引き

中国に対するサイバー攻撃に関しては、標的となった分野に変化が生じた。政府に対する攻撃は前年と同程度に発生したものの、金融や研究、教育分野といったエネルギーや通信以外の分野への攻撃が増加したことが中国のセキュリティ企業各社のレポートから確認できる[18]。また、中国を対象とするサイバー脅威も拡大した。2018 年から 2019 年の期間に、中国を集中的に攻撃する新たな APT グループの存在が指摘された。360 が報じた台湾系のグループとされる「毒雲藤」（**3.3.2**）や「藍宝菇」、そして、安天実験室（以降「安天」）が報じた米国のグループ「方程式」（**3.5.3**）である[19]。中国の大手 IT 企業の「騰訊」（以降「テンセント」）は、2019 年に中国を攻撃した APT グループのうちの 18%が新しく発見された組織であると報じた[20]。加えて、2018 年以降の中国に対する APT 攻撃は、従来以上により複雑かつ高度で実装に多大なコストを要する攻撃が多いことを「奇安信集団」（以降「奇安信」）および啓明星辰集団（以降「啓明」）が指摘した[21]。APT グループがゼロデイ脆弱性や攻撃モジュールをダークウェブで購入する傾向や、攻撃の達成に徹するだけでなく、残された痕跡や特徴からグループの特定を回避する工夫を凝らす傾向もこうしたうちに含まれる。APT グループが国家的背景に支援されており、豊富な資金を得ているからこそこうしたことが可能になると各社は指摘した。

APT が国家間の駆け引きに利用される傾向も顕著となった。2018 年に 360 は APT について、「国家間の駆け引きの道具であり外交意見を述べる手段である」と表現した[22]。2019 年、奇安信は北米ベンダーによるアトリビューションの悪用を批判した。『全球高級持続性威脅（APT）2019 年中報告』からは、奇安信による強い批判のメッセージ「（中国）国外のメディアや北米のセキュリティベンダーは攻撃元を中国と結論づける傾向が強く、また、中国を彷彿とする命名をすることで中国との APT グループとの関連性を強調している」を確認できる[23]。

なお、中国のセキュリティベンダーの報告書は 2019 年頃から「中国を攻撃する APT グループの脅威の一部が北米から飛来する」ことを強調するように変化していることは注目に値する[24]。2018 年以前の報告書の記述では「北米」の脅威が「明確に」中国を標的としているかについては不明瞭さが観察された[25]。米国による対中圧力の高まりが中国のセキュリティベンダーおよび中国世論に影響した可能性は排除できない。

2.3　期間Ⅲ：新型コロナウイルス感染症の流行以降（2020 年～2022 年）

2020 年 1 月 23 日、新型コロナウイルス感染症の流行により、中国は湖北省武漢を 2 か月にわたって都市を封鎖した。同年 3 月には WHO がパンデミック状態を宣言した。新型コロナウイルス感染症による影響が人・物の交流を制限し、世界経済は急速に縮小、深刻な不況に直面した[26]。同年下半期、他国が経済的な打撃に苦しむなかで中国は流行の封じ込みに成功し、生産体制を正常化して医療物資やハイテク製品の輸出を開始した。ICT 分野も大きく成長させた。主要経済諸国唯一の経済成長は、国際経済における中国の存在感を増大させたばかりでなく、中国世論の愛国主義精神にも貢献した。2020 年 12 月には「中華人民共和国国防法」の改正が採択され、サイバー空間は重大安全保障領域として規定された。

2020 年：①戦術と標的の変化

センセーショナルな「新型コロナウイルス感染症情報」をおとりとした攻撃、医療機関や 3 億人を超える在宅勤務者／在宅学習者を標的とする攻撃が影響して、中国を狙う APT グループによる攻撃は増大したと中国のセキュリティベンダー各社が報じた[27]。しかしながら、新型コロナウイルスによる特殊要因を除けば、標的となった対象は依然として政府、研究機関、国防・軍事関連組織であった。

2020 年には中国を狙う APT グループの戦術に大胆な変化が発生したことも中国のセキュリティ企業各社が報告している。台湾の APT グループ「毒雲藤」（**3.3.2**）により、中国の主要な軍事部隊が攻撃の標的となる事案が発生したことを 360 が報告した。同年の「毒雲藤」の攻撃には最終目標を直接攻撃するパターンが確認されており、軍事部隊と関与のある周辺組織を標的とする従来

の間接的な攻撃とは異なる傾向であることが指摘された[28]。原因について 360 は、「台湾海峡情勢のエスカレーション」が影響したという見解を述べた[29]。ベトナムのグループ「海蓮花」（**3.1.2**Error! Reference source not found.）は標的とする分野を拡大したことを 360、奇安信、および啓明が指摘した[30]。従来の海蓮花は、海洋関連機関に対するフィッシング攻撃を重点にしていた。2020 年にはサプライチェーン攻撃を採用し、海洋以外にも通信や石油関連の組織を標的とした。韓国のグループ「Darkhotel」（**3.4.2**）による攻撃規模は、過去に比べて大規模となった。同年初頭の Windows 7 アップデート廃止のタイミングには、同グループによる中国の商業・貿易に関連する政府機関への攻撃が発生した。3 月から 4 月にかけては、中国でよく利用される VPN クライアントの正規のアップグレード更新プロセスが Darkhotel のバックドアプログラムに置き換えられた。この攻撃は、中国の在外公館を含む政府機関や 200 以上に及ぶ組織に影響したことを 360、奇安信、安天、および啓明が報じた[31]。さらに、同グループは隔離されたネットワークまでその標的としたと奇安信および啓明が報じた[32]。

2020 年：②外交手段としてのアトリビューション

2020 年の注目に値すべきもう一つの動向は、中国政府がサイバー攻撃のアトリビューションを外交手段として積極に利用し、他国を非難する傾向に転じたことだと言えよう。

360 と奇安信は、「奇幻熊（APT28）」や「魔鼠（WellMess）」といったロシアの関与が疑われる APT グループが中国に攻撃を仕掛けていることを 2020 年の脅威レポートのなかで初めて明記した[33]。前述の 2 社の 2016 年から 2019 年の脅威レポートの中には、上記のグループが「米国や欧州の組織を攻撃している」という記述が確認できたものの、「中国の組織を攻撃している」という記述は確認できなかった。米国の APT グループ「Longhorn」（**3.5.2**）や「方程式」（**3.5.3**）による攻撃に対しては、中国政府がアトリビューションを外交手段に利用する傾向が顕著に表れた。2020 年に中国の組織へ攻撃していることが初めて明らかとなったロシアの「奇幻熊」や「魔鼠」について、中国政府はロシアを大々的に非難しなかった[34]。これに対して米国の「Longhorn」や「方程式」について、中国政府は激しく米国を非難している。2020 年 3 月の中国外交部や在外中国大使館を巻き込んだ非難は、中国の SNS やメディアに積極的に取り上げられた

[35]。もとより方程式が米国の組織であるというアトリビューションは 2017 年の段階でなされていたし、中国を攻撃の標的にしている可能性も過去に安天や 360 によって指摘されていたにも関わらず、2020 年のタイミングで大々的な非難へと発生したことになる[36]。

2021 年：コロナ禍で本格的に経済回復する中国を狙う脅威

2021 年は中国の社会・経済戦略『第 14 次五カ年計画』（「十四五」）の開幕の年であり、また、中国共産党創立 100 周年であった。同年は依然として新型コロナウイルス感染症の世界的な流行が継続した。国によっては 2020 年以上に深刻な状況が発生した。こうした状況において、2021 年の中国に対する攻撃は前年よりも増加した。360 は「コロナ禍に中国のデジタル変革とスマートシティ化が進み、都市部における攻撃対象範囲が拡大した」ことを要因の一つに挙げた[37]。啓明は「攻撃ツールが商用化されたことにより、APT 攻撃技術が実現不可能なツールから、技術可能なツールへと変化した」ことを要因に挙げが[38]。奇安信は「中国が保有する科学技術に対する西方諸国の関心の高まりと関連した情報窃取および破壊活動の過激化」を要因に挙げた[39]。各社の分析に違いはあれど、2021 年に本格的な経済回復に入り、中国共産党の掲げる社会主義現代化強国に向けて前進した中国をねらう脅威が増加したことは疑いの余地のないことであったといえる。

2021 年に攻撃の標的となったのは政治経済の中心地および沿岸地域で、広東、福建、浙江、江蘇省、北京地区の順であった。政府部門が最も多く狙われ、次いで多かったのが医療、エネルギー、科学技術研究機関であった。中国において科学技術研究所やシンクタンクが標的となるケースは 2020 年以降に増加した。高度人材の戦略拠点となる機関に侵入して中国の防衛軍事システムやイノベーション技術に関する機密情報を得ることが他国による攻撃の動機となっていると 360、奇安信、および緑盟科技が指摘した[40]。奇安信と 360 は、中国の医療分野やメディアを狙った攻撃が、南アジアや東南アジアにおける新型コロナ感染症の流行に連動して発生したと指摘した[41]。奇安信はさらに、APT グループによる不断の努力傾向、すなわち攻撃のアップグレードに巨額の資金と人材を惜しまず投じ、より高い頻度で攻撃していることも指摘した[42]。奇安信および 360 が報告に基づくと、「Darkhotel」による攻撃は 2020 年から減少し、2021 年に最も活発に中国を攻撃した APT グループは「毒云藤」、「蔓霊花」、「海蓮花」の 3 グループであった[43]。

2022 年：コロナ禍の終息と国家安全意識の高まり

2022 年に新型コロナウイルス感染症の流行関連のトピックが攻撃に使用される割合は減少した[44]。また、ゼロデイ脆弱性を悪用した中国への攻撃キャンペーンも過去 2 年間に比べて鈍化した。しかし、前年に活動の減少が報じられた「Darkhotel」が、中国の組織に対する攻撃を再開し、複数のブラウザのゼロデイ脆弱性が悪用された。

2022 年の中国に対する攻撃の特徴は二つあるといえる。一つ目は、360 が警鐘を鳴らした「龍芯（Loongson）」や「Kunpeng」に代表される中国の国産 OS や CPU および自律制御システムのサプライヤーを狙う傾向である[45]。360 の観測結果によると、ベトナムの APT グループ「海蓮花」による IoT デバイスを狙った活動は 2020 年以降に増加傾向にある。2022 年はこの傾向が特に顕著で、マイクロプロセッサが利用する MIPS や ARM のアーキテクチャを狙って中国国内の IoT デバイスを踏み台にする海蓮花の攻撃コードが発見されたと報告された[46]。海蓮花が攻撃戦略を調整し、より深刻な影響を及ぼすサイバー攻撃をこれまで以上に積極的に仕掛けていることは緑盟も指摘している[47]。海蓮花の攻撃能力の発展傾向について、「警戒が必要である」と 360 が警鐘を鳴らしたことは注目に値する[48]。

2022 年の中国に対する攻撃において特筆すべき特徴の二つ目は、2021 年に低調気味であった中国政府による「米国が中国（および世界各国）に対して行っているサイバー攻撃の常態化」に対する強い非難が、同年に発生した中国の「西北工業大学」に対するサイバー攻撃を契機に再登場したことである。これについては **3.5.4** で詳述する。

2.4　要約

2016 年当初の中国において最も顕著な脅威は、同国南部にある海洋組織をねらうベトナムの APT グループ「海蓮花」の脅威であった。しかし、中国を標的とする APT グループの全体数は年を追うごとに増加した。更に、海蓮花以外の APT グループが保有する高度な技術力と他グループが標的とする政治・経済の中心地である中国北部への攻撃が際立つようになった。代表されるのがイン

ドの「蔓霊花」、台湾の「毒雲藤」、韓国の「Darkhotel」による攻撃活動である。世界的な対中圧力が高じる趨勢の中で増加する中国への APT 攻撃に対して、中国は攻撃に対する積極的なアトリビューションとその外交利用に転じていった。新型コロナウイルス感染症の流行による経済的な打撃に他国が苦しむ中で、いち早く経済回復を見せた中国への APT 攻撃数は一層増加した。「毒雲藤」の活動が活性化し、「海蓮花」の攻撃力は警戒レベルに達した。2022 年には米国の「方程式」による大規模な攻撃が発生し、中国政府を巻き込んだ大々的な米国非難に発展した。

本章で参考・引用した情報源の多くが中国のセキュリティ企業によって中国語で執筆されたレポートに依拠している。詳細は文末脚注に記載した[49] 。

3 中国への攻撃に対して活発に活動する組織

本章では、中国に対して頻繁に攻撃あるいは深刻な影響を与えるベトナム、インド、台湾、韓国、米国の APT グループについて、中国が主張する観点に基づいて紹介する。中国が主張する観点は中国のセキュリティ企業が中国語で執筆されたレポートに依拠していることを再度付記しておく。また、国際関係に詳しくない読者を想定し、これらグループの動機・目的を理解するための説明を簡単に補足した。

3.1 ベトナム

3.1.1 中越関係

中越関係は経済面における協力と南シナ海の主権問題が特徴的である。ベトナムにとって、中国は最大の貿易相手国である[50]。その一方で、国境を接する中越双方は古くから領土問題・海洋権益を巡った対立を繰り返している。こうした経緯から、ベトナムは中国に対して強い「警戒感」と「国防意識」を有している[51]。

近年では、南シナ海諸島を「中国にとっての核心的利益」と形容して軍事拠点化を進める中国に対して、同じく領有権を主張するベトナムが激しい抗議をしている[52]。2014 年 5 月には、中国が南シナ海のパラセル諸島（中国語は「西沙群島」）近海のベトナムの排他的経済水域（EEZ）内の大陸棚で石油掘削を開始して摩擦が生じ、ベトナム世論における対中感情が悪化した[53]。以降も石油掘削問題を巡って中越は対立を続け、ベトナム国民の対中感情は悪化したままとなった[54]。2018 年 6 月には、ベトナム国会で審議されていた親中的といえる法案に反対するデモが全国に拡大した[55]。2019 年にベトナムにおける中国の投資認可額が首位になる一方で[56]、同年 7 月以降に、ベトナムの EEZ における石油・天然ガス掘削活動を巡って両国の政府船舶などが再び対峙した。社会レベルでは、同年 10 月に中国と米国の企業が共同制作した映画がベトナムの映画館で上映中止となった他、香港出身の映画スターによるベトナム慈善訪問が取り消しとなるなど、対中感情の悪化に拍車がかかった[57]。このような対中感情をベースに、コロナ禍の初期段階にあたる 2020 年 1 月末の早々にベトナム政府は中国との国境を封鎖し、航空便も停止した。対中警戒感が作用したこ

の決断は却ってベトナム国民の支持を得た。2020 年 4 月には、ベトナム漁船と中国海警船が西沙群島で衝突し、ベトナム漁船が沈没する事案が発生した[58]。

昨今におけるベトナムのサイバー能力の向上は、複数の国際機関・シンクタンクなどから高い評価を受けている。ベトナムのサイバー能力の向上という結果が、中国のセキュリティ企業に対する海蓮花の攻撃能力の発展傾向という評価と類似することは注目に値する[59]。同国では、外国の銀行口座や個人の情報をハッキングしたために、米国において実刑判決を受けたベトナム人ハッカーが、帰国直後に同国の国家サイバーセキュリティセンターで雇用された例も報告された[60]。繰り返される中国との物理的な衝突と、ベトナム国民の間で高まる対中警戒意識がベトナムのサイバー能力の底上げを後押ししている可能性が考えられる[61]。

3.1.2 海蓮花

【別名】Ocean Lotus、APT-C-00、APT-Q-31、APT32、APT-TOCS

海蓮花[62]は 2011 年頃から非常に活発に中国を攻撃している APT グループで、ベトナム政府との関連が中国内外のセキュリティ企業により指摘されている[63]。海蓮花は、英語とベトナム語に加えて中国語（簡体字）を駆使し、中国の政府、研究機関、海洋組織を標的とする集団とされる[64]。2016 年以前の海蓮花は、中国の海事建設や海運会社組織を重点的に攻撃していた。しかしその後に標的を拡大して、2017 年には中国の金融分野、2020 年初頭は医療機関、同年 3 月以降は中国の大手 IT ベンダーとその顧客である教育、通信、政府、防衛、科学研究所といった幅広い機関に標的を拡大した。海蓮花は戦術の洗練化と新技術の開発に非常に注力しているグループでもある。2016 年以前にアジアの他グループに劣ると評価された海蓮花の技術力は、2020 年の段階でアジアの他グループを超え得る攻撃力に発展しており、中国が今現在直面する最大のサイバー脅威であるとして 360、奇安信、啓明などの企業から評価された[65]。2020 年以降、海蓮花は中国国内の多数の IoT 設備を攻撃に利用し始めた[66]。これに関連して 360 および奇安信は、同グループが中国独自の CPU チップシステムに特化した攻撃ソリューションを保有しており、中国の組織は一層の警戒が必要であることを注意喚起した[67]。2021 年に海蓮花はサプライチェーン攻撃を主要な戦術化して防衛や科学研究機関を含む中国の広範囲の組織に被害を及ぼした。この際には中国でよく使用される

ソフトウェアの脆弱性が悪用されたほか、SIer や MSP を攻撃してサーバや開発端末に侵入してソフトウェアのソースコードが改変されたことを 360 および奇安信が指摘した[68]。2021 年下半期以降に南アジアの APT グループが中国の医療分野への攻撃を緩めるのに対して、海蓮花は引き続き頻繁に中国の医療分野を攻撃した。なお、海蓮花はセキュリティソフトウェアおよびセキュリティ技術者との対峙を重視する傾向が他のグループよりも強いと 360 は指摘する[69]。オープンソースで複数のプログラミング言語を使用したローダを使用して解析・調査の難易度を高める手法や、端末で異常の発見を困難にする手法へ注力する傾向が観察されているほか、2022 年には不正な DLL ファイルをロードするために有効なデジタル署名ファイルを使用する方法（中国語で「白利用方式」）が採用されたことが報告された[70]。

3.2 インド

3.2.1 中印関係

中印関係は領土問題に加えてインドにおける対中貿易赤字が特徴的である。2014 年のモディ政権発足後、中印両国は経済関係を進展させた。一方で、中国はバングラデシュ、パキスタン、ブータン、スリランカといったインド洋周辺国家との関係を深化させており、インドがこれを強く警戒している[71]。2017 年 6 月、インドとブータンの係争地「ドラクム」で中国の人民解放軍が道路建設を開始し、出動したインド軍が建設を妨害する事態が発生した。2018 年 1 月には国境係争地帯で中国軍による対立が発生し、インド側は中国による「越境」事案であると非難した。もとより存在した中国製品によるインド市場の占有とインドの対中貿易赤字化に対する不満が影響し、同年にインド世論の対中感情も悪化した[72]。他方、両政府による関係改善の努力が図られており、同年の習近平国家主席とモディ首相の武漢非公式首脳会談、2019 年の第 2 回チェンナイ非公式首脳会談で、問題の部分解決やインドが懸念する対中貿易赤字を減らすためのメカニズムの設立合意がなされた。しかし、2020 年 5 月にはインド北部の国境係争地帯「ラダック」の軍事衝突で両陣営に死者が発生して再び緊張が高まった。こうした事象が APT グループに影響を及ぼしていると安恒信息威脅情報中心（以降「安恒」）は分析した[73]。ラダック衝突は、中国製の製品や中華料理のボ

イコットが発生するなど、インド世論における反中感情にも大きく影響した[74]。その後軍事衝突は解消されたものの、ラダックでは 2022 年にもサイバー空間上の攻防が発生している[75]。

3.2.2 蔓霊花

【別名】Bitter、APT-C-08、T-APT-17、苦象

蔓霊花は強い政治的背景を持つ英語話者の集団で、中国とパキスタンの政府、軍事、電力、原子力分野に対して頻繁にサイバー攻撃を仕掛けて諜報や機密情報の窃取を行う集団であると認識されている[76]。また、中国の複数のセキュリティ企業がインド政府との関連を指摘している[77]。

360 および安恒の報告によると、2016 年 5 月～9 月に中国の外交関連部門や電力関連事業体を狙った蔓霊花による集中攻撃が発生した[78]。中国の電力関連事業体は、その後の 2018 年 10 月～12 月にも被害を受けたことがテンセントおよび安恒により報告されている[79]。2019～2020 年には、広範囲な被害がより頻繁に発生した。その際には中国政府、防衛産業、エネルギー、貿易分野の組織および、在パキスタンの中国人が蔓霊花の標的となったことを 360、奇安信、安恒が報告した[80]。安恒は 2020 年の蔓霊花（およびその他の南アジアの APT グループ）の活発化について、中印の国境紛争の影響を指摘した[81]。2020 年以降、蔓霊花は中国に対する新しい攻撃方法を採用した。中国の入札中間業者を標的としたサプライチェーン攻撃である。動機について 360 は「中国の防衛産業や政府機関などを顧客にもつ入札中間業者との需給関係を把握し、保有されている機密情報を窃取するためのもの」と分析した[82]。2021 年になると蔓霊花による攻撃は更に増加した。従来の標的に加えて、中国の医療分野を狙う攻撃が増加したことを 360、啓明、奇安信などが報告した[83]。4 月に南アジアで発生した新型コロナウイルス感染症の大流行の影響が 360 により指摘されている[84]。2022 年にも医療分野への攻撃は継続したが、同年に発生した複数の集団感染症の発生と関連するものであると 360 は指摘した[85]。なお、奇安信は「蔓霊花の技術力は他グループに劣る」と評価している。しかしながら「多様なリソースを保有し、攻撃キャンペーン中に C2 サーバを入れ替えたり、人員を増強したりすることが可能な柔軟な集団である」とも評価した[86]。

3.3 台湾

3.3.1 両岸関係

両岸関係は「祖国統一」と「台湾意識」の深い乖離が特徴的である[87]。独自性を強調する意識が台湾で高じているのに対し、中国は一貫した「一つの中国」原則のもとに台湾問題を「国家の核心的利益」と明言し、独立を抑止・阻止するために必要となる軍事能力を着々と整備している[88]。

2016 年 5 月、台湾で蔡英文政権（民進党）が発足すると、世界 5 か国が台湾と断交して中国と国交を結んだ。台湾はこの動きに反発した。同年 12 月に蔡英文台湾総統と米国のトランプ次期大統領（当時）が電話会談を行うと、中国がこの動きに強く反発した。その後の 2017 年の中国共産党十九大では「台湾同胞同化政策」が提案された。また、2019 年には中国が台湾に対して「一国二制度」を提起した。しかし、中国による前述の発言があった即日中に蔡英文台湾総統が「台湾は一国二制度を断固受け入れない」と回答している[89]。2020 年 1 月の台湾総統選で再選した蔡英文総統は、「選挙結果は『一国二制度』を拒否するものである」と発言した。中国はこれに対して、「一つの中国の原則は不変であり、台湾は中国の一部である」と牽制した。中国軍による台湾海峡を越える飛行や訓練は繰り返し発生している[90]。2019 年～2021 年 8 月期間の台湾の軍用ネットワークにおいて約 14 億件の異常が検知されたことも報告された[91]。

なお、2021 年 12 月に台湾の政府系財団の台湾民主基金会が発表した世論調査からは、72.5%の台湾人が「中国が統一を実現するために武力を行使した場合は、国家のために戦うことを望む」声が明らかとなった[92]。一方で、「台湾が独立を宣言した後に中国が攻撃してきた場合は戦うか？」という質問に対しては、「戦う」と答えた人の割合は 62.7%に減少した。26.7%は「戦わない」と答え、10.6%は無回答だった。2023 年 1 月に台湾の政治大学選挙研究センターが発表した「台湾独立・中国統一に関する意識調査」の結果によると、「中国本土との統一を望む」回答者はわずか 1.3%であった[93]。しかし、「台湾の独立を望む」回答者も 5.1%と低かった。高い水準を見せたのは「現状維持を望む」という回答（「現状維持―無期限（28.6%）」、「現状維持―後日決定（28.3%）」、「独立に向けて現状維持（25.2%）」）であった。台湾民主基金会および政治大学による二つの調査結果は、中国による台湾統一に反対する割合が台湾独立の主張より大きいことを示している。しかしながら、選挙への影響力が高いのは現状維持を望む声であり、ここには

北京とは異なる政治組織を熱望する台湾の独自意識が顕著に表れている。台湾における中国への警戒感が高まる中、2024 年 1 月 13 日に予定されている次期台湾総統選挙における影響が注目される[94]。

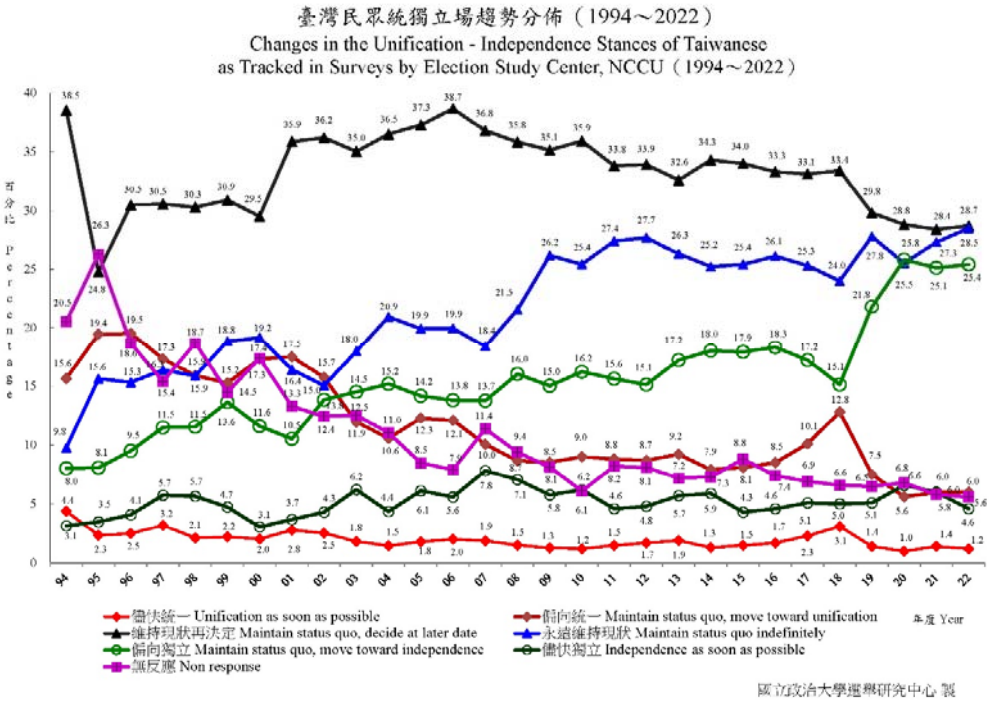

図 2 台湾独立・中国統一に関する意識調査（1994 年 12 月～2022 年 12 月）

【出典】台湾政治大学選挙センター

3.3.2 毒雲藤

【別名】APT-C-01、緑斑、APT-Q-20、窮奇、白海豚、GreenSpot、APT-TOCS

毒雲藤は「中国の防衛、政府、科学技術、教育、海事などの組織に対する情報窃盗・スパイ行為を 2007 年ころから行っている集団である」として中国のセキュリティ各社は説明している[95]。古くから中国の海洋や防衛関連の組織を標的とした攻撃活動を継続している点において、毒雲藤と

海蓮花には類似性がみられる[96]。奇安信は両者を「中国が今現在直面する最大のサイバー脅威」と評価した[97]。一方で、両者には明確な違いが存在することを安天やテンセントをはじめとする各社が指摘している[98]。毒雲藤は巧みな中国語（繁体字）を使用し、両岸関係や米中関係に深い関心を示す点である。360 は 2017 年 10 月に毒雲藤が福建省泉州市にある組織を攻撃したことを明らかにした[99]。泉州市は福建省最大の経済地区で、同年には中国の国務院が推進する「中国製造 2025」に基づく地方初のパイロット都市に指定されている[100]。泉州市は一帯一路の「海のシルクロード」の玄関口に相当する重要地域でもある[101]。その一方で、泉州市には 1949 年の中華人民共和国建国以前から台湾との間に頻繁な経済・文化交流があり、従って、泉州市を祖先のルーツとする台湾人は多い。毒雲藤による中国の船舶重工業や港湾運営会社といった複数の海事産業に対するサイバー攻撃の発生は 2018 年 5 月にも発生したことが 360 により報告されている[102]。

また、毒雲藤は海蓮花と比較すると慎重で、より中国を熟知している。毒雲藤は綿密な調査に基づいて標的を選定し、中国で話題性のあるさまざまな時事問題や関連性の高いコンテンツを的確に選択して攻撃を仕掛ける傾向があると奇安信は指摘する[103]。毒雲藤の活動は 2019 年に大幅に減少したことをテンセントが報じていたが、2020 年初頭になって中国で新型コロナウイルスの流行が拡大すると、毒雲藤は大規模なフィッシングキャンペーンを行ったことが報告された[104]。同年 6 月以降は中国の大学、研究機関や軍関係者に標的を絞り、シンクタンクや軍事雑誌記者、ヘッドハンターなどのアカウントになりすました上で、標的自ら積極的に機密情報を送信させる手法を採用したことが報告された。2021 年以降も毒雲藤は非常に活発に活動し、中国国内の有名なメールボックスサービスの精緻な偽サイトを大量に作成した。奇安信によると、毒雲藤は海蓮花に次いで 2022 年に中国を最も活発に攻撃した APT グループであった。一方で 360 は、毒雲藤が最も活発に中国を攻撃したグループであったと報じた。昨今になって強化傾向にある毒雲藤のステルス性は 360 や安恒により注目されている。従来の毒雲藤はフィッシングサイト経由で悪質な添付ファイルを配信する手法を採っていた。この手法は減少傾向にあり、代わって 2022 年は多数の通常ファイルがおとり文書に使用されたことが指摘された。例えば、標的のウェブサイトの通知や告知といった公開文書や、過去に毒雲藤による攻撃により盗まれたと考えられる文書（プロジェクト申請、政策文書、会議・フォーラム、防疫対策など）が利用されたことが報告されている[105]。

3.4 韓国

3.4.1 中韓関係

韓国国民の対中感情は必ずしも良好とは言えないものの、政府レベルにおいて中韓は経済互恵的な関係を築いてきたといえよう。2015 年には中韓自由貿易協定が発効した後に、中国は韓国にとっての最大貿易相手国、韓国は中国にとって世界第三位の貿易相手国へと発展した[106]。韓国の対中経済依存が大きくなる一方で、韓国の安全保障は米国に依存している。

北朝鮮の核実験や弾道ミサイル発射を睨み、2016 年 7 月に米韓は弾道弾迎撃ミサイルシステム（THAAD）配備の決定を発表した。しかし、米軍による朝鮮半島への THAAD 配備が中国大陸にまで影響することを嫌った中国はこの決定に猛反対して、政治情勢や国際問題に関わる韓国との対話を拒否した[107]。加えて、非公式報復の「限韓令」により韓国に経済的な打撃を与えた[108]。THAAD 問題を語るうえで中国当局が両国の関係を「小国」と「大国」と比喩すると、韓国世論の対中感情は悪化した[109]。韓国の文在寅大統領（当時）による訪中や、THAAD 問題についての中国との疎通合意といった歩み寄りにも関わらず、社会レベルでは中韓の対立が続いた[110]。2019 年には、香港の反中デモを支持する韓国人学生とこれに反対する中国人留学生が韓国の漢陽大学で対峙した。2021 年 4 月、韓国法務部が「国籍法改正案」を立法予告した際に、恩恵の対象者の 95%は中国大陸出身の華僑となることが判明すると、韓国では 30 万人以上による国籍法改正案の反対請願が大統領府に提出された[111]。さらに、同年に韓国の民間調査専門機関が実施した「韓国人の反中認識調査」世論調査には、中国に対する好感度が日本や北朝鮮より低く表れる結果となった[112]。

3.4.2 Darkhotel

【別名】黒店、APT-C-06、T-APT-02、寄生獣

Darkhotel は朝鮮半島に関連する政治的なターゲットを中心に中国を含む東アジア諸国の企業幹部を攻撃するグループである[113]。360 は Darkhotel の攻撃の特性について、中国という地理に特定されたものであり、業界は主要な焦点ではないと分析した[114]。中国の複数のセキュリティ企業

は同グループについて、高度な技術を持つ集団として評価した[115]。啓明は Darkhotel について、攻撃頻度は低いが他グループより突出した能力を有し、極めて重要な組織のみを標的とする傾向があると評価した。伏影実験室は同グループのコンポーネントを偽装する能力、水飲み場の発掘能力、脆弱性を利用する能力が非常に高いことを指摘した[116]。Darkhotel がブラウザのゼロデイ脆弱性を攻撃することを得意とすることは複数の企業が指摘している。2022 年に世界の APT グループがゼロデイ脆弱性を悪用して攻撃キャンペーンを展開する傾向が鈍化する中でも、同グループは依然としてゼロデイ脆弱性を主要な戦術としている[117]。テンセントは Darkhotel が英語と韓国語を使用して北京時間の午前 8 時～午後 4 時の時間帯で活動していること指摘しており、その他の中国のセキュリティ企業からも韓国政府との関係性を疑っている[118]。

2017 年下半期、Darkhotel は中国の標的に対する大規模攻撃キャンペーンを開始した。被害は中国北部、沿岸部と香港に集中し、海外商業取引をする中国の企業が最も影響を受けた。2018 年 4 月に発生した Windows の脆弱性を悪用した攻撃について、360 は Darkhotel によるものであると報告した[119]。香港の貿易企業や中朝貿易企業のシニアマネジメントが標的となったことをテンセントが明らかにした[120]。2019 年 9 月～11 月と 2020 年初頭にも商業や貿易に関連する中国の政府機関を狙う作戦が実行された。2020 年初には、2 種類のブラウザ（Internet Explorer と Firefox）の脆弱性が悪用され、中国の商業関連政府機関が Darkhotel による攻撃の影響を受けたことが 360 により報告された[121]。同年 3 月には、中国で広く利用されている VPN の正規のアップグレード更新プロセスが Darkhotel のバックドアプログラムに置き換えられたことで、中国の在外公館や 200 以上にわたる組織の VPN サーバがその影響を受けたことが、奇安信や 360 により確認された[122]。これらのサーバのうち 174 台は、北京や上海の政府機関のネットワークや、海外で活動する中国の外交団体の関連のネットワークに設置されていたという。新型コロナウイルス感染症の流行対策として中国で在宅勤務が実施される期間に発生したために、攻撃によるリスクが拡大したと 360 は分析した[123]。同年 5 月には、隔離されたネットワークもその標的となったことを啓明が報告した[124]。これ以降もより集中的で標的を絞ったゼロデイ攻撃が発生した。2021 年 4 月には Internet Explorer のゼロデイ脆弱性、2022 年 2 月には Firefox ブラウザのゼロデイ脆弱性が同グループにより悪用されたことが 360 により観測された他[125]、同年 3 月にはマカオの高級ホテルで標的型攻撃が発生した[126]。

3.5 米国

米国を背景とする APT グループは、他のグループと異なって中国政府が強い姿勢で非難していることが特徴といえる。中国のセキュリティ企業が北米の APT グループを非難するトーンは 2019 年頃を境に徐々に強まっているが、米国を主導に高まる対中圧力中国のセキュリティベンダーやび中国世論に影響した可能性が考えられる。

3.5.1 米中関係の変化

米中関係を本レポートで網羅することは困難であるため、ここでは中国に大きく影響したと考えられる、米国のサイバー空間の安全保障政策および関連する一部の出来事に限定して取り上げる。

2015 年 9 月、オバマ米大統領（当時）と習近平中国国家主席は首脳会談において、双方が知的財産のサイバー窃取を行わないことで合意した。しかし、米国では 2016 年以降も中国によるサイバー活動が発生したことが報告された[127]。同年 2 月の米国国防省予算要求の優先課題には中国が含まれ、『米国サイバー安全保障国家行動計画』の投資予算には 67 億米ドルが計上された（前会計年度予算から 15.5%増加）。また、2017 年に発足したトランプ政権は、米軍のサイバー作戦能力の発展を優先課題とする指針が打ち出された。同年 11 月にトランプ米大統領（当時）と習近平中国国家主席による首脳会談では 2015 年 9 月の合意事項の継続を再確認したが、同月に行われた米国議会では、継続する中国のサイバー活動に対する非難報告が発生した。2017 年から 2018 年にかけてトランプ政権が公開した『国家安全保障戦略』と『国家防衛戦略』は、「サイバー活動を拡大する修正主義勢力の中国が米国と戦略的競争関係にあること」が米国の安全保障上の懸念と明記した[128]。2018 年 1 月に米海軍の極秘情報が漏洩した直後の『年次脅威評価』は、中国軍のサイバー攻撃能力を脅威と評価した[129]。2020 会計年度の国防省予算要求におけるサイバー関連予算は前年から 10%増加した。知的財産の窃取を巡ってはさらに、2020 年 7 月に米国政府が在ヒューストン中国総領事館を閉鎖しており、その対抗措置として中国も在成都米国総領事館を閉鎖している。2020 年は 5G セキュリティに関して中国製の通信機材／サービスを排除する米国政府の指針が明確になった年でもある[130]。米国防省の『2020 年次報告書』で中国は第一位の優先事項に指定

された[131]。バイデン政権下で 7,150 億米ドルが計上された 2022 会計年度国防省予算においても中国の脅威は最優先課題と発表された[132]。米国ホワイトハウスに国家サイバー長官が新設された 2021 年、米国はマイクロソフト社メールサーバソフトウェアの脆弱性を狙ったサイバー攻撃に関して中国を非難した[133]。2023 年 3 月にバイデン政権が公開した『国家サイバーセキュリティ戦略』において、中国は「国際秩序を再構築する意図を持ち、且つ、経済・外交・軍事・技術においてこれを実現可能な唯一の国」として評価されている[134]。

2020 年から 2022 年にかけて米国のシンクタンク「Pew Research Center」が行った対中感情の世論調査の結果において、「中国に対して好意的でない意見を持つ米国人」の割合が、79%から（2020 年）82%（2022 年）に増加した[135]。この対中感情変化の調査における最も大きな変動は、2020 年に「どちらかとして好感が持てない」と回答した米国人（15%）が 2022 年には「非常に好感が持てない」と回答したこと、すなわち対中感情の更なる悪化が発生したことであった。

3.5.2 Longhorn

【別名】APT-C-39、Longhorn、The Lamberts、CIA

Longhorn[136]の存在は、ウィキリークスによって 2017 年に公開された米国中央情報局（CIA）のサイバーハッキングプロジェクト「Vault7」により明らかとなったことを、奇安信および 360 が報告している[137]。また、両企業は Longhorn について「過去に中国で観測された APT グループの中で最も洗練化された技術と最も強い攻撃力を持つ集団の一つ」と評価した。攻撃プログラムのコンパイル時間は北米の労働時間に相当し、活動スケジュールは CIA が所在する米国バージニア州の時間帯に近いと分析された。2019 年、奇安信が「Vault7 に関する情報がリークされる以前の 2012 年～2017 年の間に中国国内の組織／人物に対して発生した攻撃の痕跡に、Vault7 のプログラムと一致する技術が多数使用されていることが判明した」と発表した[138]。また、2018 年後半まで中国の航空業界は Lambert による攻撃を受けていた可能性があることも指摘した[139]。奇安信はさらに、「Lambert が使用するサイバー兵器は一から構築され、ターゲットや攻撃戦略に応じてカスタマイズされている」ことから、「米国による高度なサイバー攻撃システムが中国を重要な

標的の一つにしている証拠である」と述べた[140]。2020 年 3 月になって 360 が、「Longhorn は 2008 年 9 月～2019 年 6 月の約 11 年間にわたり、北京、広東省、浙江省などにある標的や、航空宇宙、科学研究機関、石油産業、大手インターネット企業、政府機関などに対する諜報活動を行っていた」と発表した。航空宇宙への攻撃に関しては、システム開発企業・開発者が標的となったこと、要人を含む乗客や貨物の渡航情報がリアルタイムで特定・追跡された可能性があることを報じ、情報が政治的・軍事的に利用された場合の中国にとっての危険性を問題視した[141]。そして、360 の発表から間もない 2020 年 3 月に中国政府から米国に対する強い非難へと発展した[142]。

3.5.3 方程式

【別名】Equation、APT-C-40、NSA

方程式[143]は米国国家安全保障局（NSA）を背景に持つ集団として複数の中国のセキュリティ企業が分析しており、中国政府が最も強く非難しているグループである[144]。

中国のセキュリティ企業が「方程式は NSA である」と批判する根拠は、2016 年の「Shadowbrokers（中国語では影子経紀人）」による情報流出により判明したはずの NSA のプロジェクトの技術が、情報流出が発生した 2016 年より遥か以前の 2008 年以降に発生した中国の組織の被害サンプルに多数使用されていたためである[145]。2016 年、360 はその報告書の中で「影子経紀人が開示した文書から、方程式の攻撃対象のドメインには『.cn』が最も頻繁に出現した」と報告した。この点は 2019 年に奇安信とテンセントも同様の指摘をしている[146]。2017 年の安天による報告は、2000 年から 2010 年の間に侵害された IP とドメインは主にアジア太平洋地域の 49 カ国に広がっており、中国のほかには日本、韓国、スペイン、ドイツ、インドなどが被害を受けたと報じた[147]。360 はさらに、特定のドメイン情報から「清華大学や科技大学等の中国のトップ大学が方程式の主要なターゲットである」こと、そして「中国原子力研究院などの科学研究機関や華為などの商業企業もそのターゲットに含まれている」ことを指摘し、「方程式の主要ターゲットは中国である可能性が高い」と中国の組織に注意喚起を促した[148]。方程式に対する説明のトーンに変化が発生している点も注目に値する。2016 年に 360 が「方程式は歴史上知られているすべてのサイバー攻撃グループを凌駕する、高度で洗練された技巧を持つ秘密主義の諜報集団である」という説明

は、2020 年 3 月の「Longhorn による中国への 11 年間にわたる攻撃」の発表を経て、2022 年になると批判を伴うように変化した[149]。「攻撃の洗練度と技術において歴史上のあらゆるサイバー攻撃グループを凌駕する集団」という説明に加えて、「方程式の背後にいる政府や政治家は、世界中の個人のプライバシーの権利や機密を無視して、政治的自己満足にしか関心がない」と強い批判色が確認できる[150]。360 の方程式に関する発表は、新型コロナ感染症の世界流行を受けて米国を筆頭に中国への非難が集中した 3 月のタイミングに該当する。発表から間もない 2020 年 3 月 3 日に中国の外交部は米国を「世界一のハッカー帝国」と非難し、「中国は自国の利益とサイバーセキュリティを守るために必要な措置を講じる」と牽制した[151]。もとより方程式の技術力や中国を攻撃している可能性は早い段階から指摘されていた[152]。2015 年に安天が指摘しているし、2017 年に 360 や啓明も中国のドメインや研究機関やシンクタンクが標的とされていることを警告していた[153]。その時点では中国政府による米国批判は発生しなかったのにも関わらず、2022 年 3 月になって大々的な批判に発展したのである。また、以前は「方程式」という呼称を使用していた中国の多数のセキュリティ企業が、2022 年頃から徐々に「方程式」ではなく「NSA」という米国を容易に彷彿とさせる呼称に用いるよう転じていることも注目に値する。2019 年に奇安信が北米ベンダー向けて発信した批判のメッセージ「（中国）国外のメディアや北米のセキュリティベンダーは攻撃元を中国と結論づける傾向が強く、また、中国を彷彿とする命名をすることで中国との APT グループとの関連性を強調している」を思い出させられる[154]。

3.5.4 西北工業大学事件

奇安信は 2021 年の脅威報告書の中で「中国における西洋諸国によるサイバー窃取／破壊工作活動は今後苛烈を極めるだろう」と予測した[155]。2022 年 3 月、360 が方程式に関する研究報告を公開した[156]。360 による報告は、方程式が大規模な C2 インフラや、9 種類のモジュールから成る量子システムといったサイバー資源を中国への攻撃に惜しみなく組み込んでいると指摘した[157]。また、少なくとも 2010 年から方程式が中国の組織から盗み出した膨大な重要量の影響範囲を評価することは困難であると評価した[158]。

2022 年 6 月 22 日、中国の西安市にある「西北工業大学」が海外からのサイバー攻撃の被害に遭い、公安局に通報したことを公開声明で発表した[159]。西北工業大学は中国政府の工業情報化部（MIIT）が直轄する国家重点七大学（「国防七雄」と呼ばれる）の一角で、左記の七大学の中では航空、航空宇宙、海洋工学の教育や科学研究を展開する唯一の大学に相当する。そして同年 9 月、「西北工業大学への攻撃活動は、NSA 傘下の、他国に対する大規模なサイバー攻撃活動を専門とする部隊『TAO（Office of Tailored Access Operation、コード S32）』から発生したものである」と中国の国家計算機病毒応急処理中心が断定し、その調査結果報告を複数の中国メディアが報じた[160]。

国家計算機病毒応急処理中心は、「近年に TAO が 140GB を超える高い価値のデータを中国から窃取した」こと、また、「長期間の周到な準備を経て（攻撃の）運用開始に至った」ことを指摘した[161]。例えば、インフラ構築のために NSA がフロント企業を通じて米国の通信事業者と締結した契約書は 60 件（電子文書は 170 件以上）に上ったと報告している。また、西北工業大学への攻撃には 41 種類の独自のサイバー攻撃兵器が使用され、米国国内の 13 名が直接関与したと国家計算機病毒応急処理中心は報じた[162]。国家計算機病毒応急処理中心と共に追加調査に参加した 360 は、基盤技術を任務とする TAO の S325 部隊は踏み台 49 台とプロキシサーバ 5 台からなる専用ネットワークを構築したと発表した[163]。両組織の報告は、攻撃に使用するネットワークにはファイブアイズ以外の地域に属する 17 カ国の IP アドレスが使用されたこと、踏み台の約 70%は中国周辺国、すなわち、日本や韓国にある教育機関や民間企業のうち、トラフィック量が多いサーバから慎重に選ばれていたと指摘した[164]。国家計算機病毒応急処理中心の報告には、韓国大田高等科学技術研究学院や韓国ソウル江原大学、韓国 KT 電、日本京都大学といった名前が記載されている[165]。西北工業大学の事件は米国への批判と共に多数の中国メディアで報じられた[166]。中国外交部は 2022 年 9 月 5 日の発言で「最も強力なサイバー技術を持つ国である米国は、『国益』の名の下に不法・不道徳行為を行っている」という強い非難を表明し、米国側に説明とこうした行為の即時停止を要求した[167]。

4 結語

本稿では「サイバー攻撃の標的となる側の中国」という新たな視点を設けることによって、サイバー空間で発生している趨勢をより俯瞰した立場から理解し、日本のおかれる地政学的な立ち位置や、サイバーセキュリティに関して今後日本がとるべき方針の一助となることをめざした。調査対象には**期間Ⅰ：ハイテク化が進んだ期間（2016 年～2017 年）**、**期間Ⅱ：対中圧力が高まった期間（2018 年～2019 年）**、**期間Ⅲ：新型コロナウイルス感染症の流行以降（2020 年～2022 年）**　の各期間に中国を頻繁に攻撃或いは中国に深刻な影響を与えた、ベトナム、インド、台湾、韓国、米国の 6 つの APT グループを選定した。6 グループの動機や目的を理解する上では 5 地域と中国の間にある利害関係の衝突に注目した。

期間Ⅰ：ハイテク化が進んだ期間（2016 年～2017 年）の中国における主たる脅威は、同国南部にある海洋組織をねらうベトナムの「**海蓮花**」による活動であった。これには中越間の海洋利権を巡る衝突の影響が色濃く映る。期間Ⅰから**期間Ⅱ：対中圧力が高まった期間（2018 年～2019 年）**へ移行する中で、攻撃の標的は政治・経済の中心地である中国北部へと変遷した。同時に、インドの「**蔓霊花**」、台湾の「**毒雲藤**」、韓国の「**Darkhotel**」という新しい脅威が台頭した。なお、期間Ⅱは先述の 5 地域と中国が利害関係の衝突を最も繰り返した期間でもあり、また、米国を主導する対中圧力が高まった期間に相当する。期間Ⅱ以降の中国政府は、サイバー攻撃のアトリビューションを外交に組み込んでいった。**期間Ⅲ：新型コロナウイルス感染症の流行以降（2020 年～2022 年）**には「**Longhorn**」や「**方程式**」、そして「**西北工業大学事件**」に関して、米国に対する強い外交非難が登場した。期間Ⅲは新型コロナウイルス感染症の流行を受けて、中国の医療分野もサイバー被害の対象に加わった。さらに、中国独自の ICT サプライチェーンや、デジタル強国を目指して発展する中国の IoT 機器も攻撃を受けたことで、より広範な脅威へと発展した。本稿の調査対象期間中で直近の 2022 年に最も頻繁に中国を攻撃したのは毒雲藤あるいは海蓮花であった。しかし、中国を最も震撼させたのは方程式（或いは西北工業大学事件における NSA）による攻撃であった。一方で、期間Ⅰ～期間Ⅲまでの間に着実に攻撃能力を強化する海蓮花の脅威も看過できないものであると 360 や奇安信により再評価された[168]。

中国を活発に攻撃する或いは深刻な影響を与える APT グループの背景の 5 地域のうち、韓国を除く 4 地域では政治的に、とりわけ国防において、中国に対して妥協しない姿勢が示されていた[169]。韓国は 2018 年および 2020 年国防白書に「国防においても中国との戦略的疎通の強化を維持していく」ことが明記されており、他地域との差異がみられた[170]。他 4 地域と傾向に差異がみられる点においては、Darkhotel の活動傾向にも同様のことがいえる。海蓮花、蔓霊花、毒雲藤、Longhorn や方程式の攻撃活動の活発化が、当該 4 地域の政府と中国との関係性の悪化に関連性がみられるのに対して、Darkhotel の活動は関連性が比較的弱く映った。

なお、ベトナムでは 2023 年 3 月 2 日にヴォ・ヴァン・トゥオン国家主席（国家元首に相当）が選出された。親中派として知られトゥオン国家主席の任期は 2026 年までと発表されているが、今後の中越関係や APT グループへの影響が発生する可能性も考えられる[171]。台湾でも、2024 年 1 月 13 日に次期台湾総統選挙が予定されている[172]。台湾総統の任期は連続 2 期 8 年までのため、現在 2 期目の蔡台湾総統は 24 年 5 月を以て任期満了する。今後の両岸関係やサイバー空間における変化が注目される。

中国を活発に攻撃する或いは深刻な影響を与える APT グループの背景の多くの地域において政治的には中国と対峙する姿勢が観察される一方で、経済的には中国と原則的に互恵的な関係を維持しようとする傾向が 5 地域のすべてにおいて観察された。5 地域に共通して確認された現象に関しては、世論における対中感情の悪化傾向も同様であった。筆者が特に注目したのは、韓国世論の例に示されるように 20 代の対中感情が良好でない傾向である。比較的に ICT 能力が高く、ソーシャルネットワーキングを代表とするデジタルツールに親しんだ若い世代の心理的要因がサイバー空間や対中関係に与える影響は今後注目に値する。

本稿の調査対象の 5 地域のうちで筆者が最も注目したのはベトナムである。そもそも、ベトナムの国土は米国やインドと比べると大きいとは言えず、日本と同程度の 32 万 9,241 平方キロメートルと発表されている[173]。2020 年のベトナム人口は 9,762 万人で、韓国や台湾と比較すれば多いものの、日本の人口よりは少ない[174]。2050 年のベトナム人口は日本と同程度の約 1 億人に留まるものと予想されている[175]。ベトナムの経済成長率は 2.6～2.9%と日本の 1.7%よりは高いものの、韓国の 4%および台湾 6%には及ばず、経済成長は緩やかである[176]。米中印と同等の大国では

ないにも関わらず、期間Ⅰ～Ⅲの 7 年間にわたって中国のサイバー空間に影響を与え、且つ、「中国が今現在直面する最大のサイバー脅威」、「看過できない技術力を持つグループへ発展した」と中国のセキュリティ企業に評価せしめる APT グループの「海蓮花」が誕生する土壌がベトナムには存在するということになる[177]。また、両国には軍事力の差があるはずながら、こうした事象が発生していることにも注目したい。なお、海蓮花の攻撃能力が向上した期間Ⅰ～Ⅲは、ベトナム全体のサイバー能力も同様に向上したことが観察されている。2021 年 7 月に MIC は国際電気通信連合（ITU）による「Global Cybersecurity Index 2020」の評価で世界第 25 位を取得したことを発表した。ベトナムの評価は 101 位（2017 年）から、50 位（2018 年）、25 位（2020 年）と一足飛びに上昇している[178]。ベトナムのサイバー能力の向上は別の機関からも指摘されている[179]。サイバーランキングの指標の偏りについては読み解くうえで注意が必要ではあるものの、短期間に何らかの実績を得たことが評価された形と言えよう[180]。国土、人口、経済といったベトナムが置かれるマクロ環境は、今後も経済大国としての地位を維持していくことが難しいと言われる日本にとって、ベトナムの例は大いに参考になるのではないだろうか。

そもそもベトナムでは同国の情報通信省、およびその傘下の国家サイバーセキュリティセンター（NCSC）とセキュリティオペレーションセンター（SOC）がサイバー脅威に対応している[181]。同国は日本の組織との縁も深く、2022 年にはベトナム NCSC およびベトナムの 8 大学と日系企業がサイバーセキュリティ人材育成で提携している[182]。中国を仮想敵国とするベトナムは、2022 年にベトナム情報通信省から「ベトナムのサイバー空間における挑戦に積極的に対応する」というビジョン提示されている[183]。併せて、ベトナムにおける「2020 年のセキュリティエンジニアの総数が 5 万人であるのに対して、同国国内では約 70 万人のサイバーセキュリティ人材が不足している」と情報通信省が指摘した[184]。先述のとおりベトナムは経済・人口規模ともに発展途上にあるとはいえ、現時点では日本のそれよりも規模は小さい。現在の日本では「20 万人から 40 万人のサイバーセキュリティ人材が不足している」と評価されていることを考慮すると、ベトナムでは非常に深刻なセキュリティ人材不足と大幅なセキュリティ人材需要があることになる。ベトナムと日本で不足するサイバーセキュリティ人材数の差があることについても、日本の参考となりうるのではないだろうか。そして、親中派の国家主席指導下において現在のベトナムが採用しているサイバーセキュリティ戦略や人材育成戦略に起きる変化については、今後も追加調査をしていく必要がある。

なお、今回の調査では 2016 年から 2022 年に渡る多数の中国語のリソースにあたったが、どの中国のセキュリティ企業の脅威レポートにも、攻撃者として日本は登場しなかったことは平和維持を目指す日本の姿勢が反映されていると言えよう。憲法第 9 条に「戦争放棄、戦力不保持、交戦権の否認」を掲げる日本は、必要最低限の防衛能力のみを維持しており、基本方針の専守防衛を貫いている[185]。武力衝突は今後も決して許されることではない。一方で、世界でも有数の軍事力を保有し、軍事力の現代化を推し進める中国が、5 地域の APT グループから情報窃取や絶え間ないサイバー攻撃の標的となっている事例からは、デジタル化が進んだ現代において諸外国と対等に渡り合うためには APT 攻撃に対抗する防衛手段や自国を守るための情報収集といった活動が必要不可欠と思わされざるを得ない[186]。安天による 2017 年の方程式に関する報告書は、「2000 年から 2010 年の間に侵害された IP とドメインは主にアジア太平洋地域の 49 カ国に広がっており、中国のほかには日本、韓国、スペイン、ドイツ、インドなどが被害を受けた」と述べた[187]。中国の西北工業大学事件に関する国家計算機病毒応急処理中心による報告は、7 割の踏み台が中国周辺国のサーバから選定されていたと報じ、その中には「日本京都大学」の名前が含まれていた。パートナー国家の是非に関わらず、他国は他国の利益に基づくサイバー活動を行うため、日本が図らずしてこうした活動の影響を受けることは免れないと言えよう。

以上から、日本がサイバー空間における他国の活動による影響を最小化するための能力は、日本が今後も日本の国益を守り続けるための最重要課題であると言える。日本では米国や中国同様に高度なデジタル化が推進されている。IoT 機器が多数使用され、OT が発展し、デジタルアシスタントも一般に広く利用されている。また、日本は国際社会の「優等生」で居続けようとして、自らの能力を制限することがある。国土、人口、経済といった環境を考慮すると、日本が今後も大国としての地位を維持していくことが困難になる。日本が他国の犠牲にならないために「勝ち残る」ための戦略、すなわち、日本独自の国益に沿って、本稿が取り上げた 5 地域のように「柔軟で、時にはしたたかに」諸外国と付き合ってもよいのではないだろうか。デジタル時代の日本に必要なサイバー能力を改めて評価、認識し、日本の国家戦略に導入して、計画立案そして実施していくことが重要だ。

[本調査に関する照会先]

JCIC 事務局　info@j-cic.com

文末脚注

1. はじめに

[1] Colone lF. Mejia Eric. (2014). *Act and Actor Attribution in Cyberspace A Proposed Analytic Framework*. Strategic Studies Quarterly: SSQ; Maxwell Air Force Base, 8(1), p.114-132. Retrieved from https://www.proquest.com/trade-journals/act-actor-attribution-cyberspace-proposed/docview/1516145471/se-2?accountid=14089、P.120 から P.130 を参照。

Johnson E. Durward, Schmitt N. Michael. (2021). *Responding to Proxy Cyber Operations Under International Law*. The Cyber Defense Review, 6(4), p.15-34. Retrieved from https://www.jstor.org/stable/48631304、P.17 から P.22 を参照。

Eichensehr E.Kristen. (2020). *The Law and Politics of Cyberattack Attribution*. U.C.L.A. Law Review, 67(3), p.520. Retrieved from https://search.ebscohost.com/login.aspx?direct=true&AuthType=shib&db=a9h&AN=145027191&site=ehost-live、P.527 から P.558 を参照。

また、360 脅威情報中心 (2018). 『2017 年中国高級持続性威脅（APT）研究報告』P.27 から P.28 についても参照。

https://cert.360.cn/report/detail?id=17444eedf20fed4d90c0e071b6b8a718。

[2] Ibid., note 119, 120. P.547。および、Eichensehr, E. Kristen (2017) *Public-private cybersecurity*, Texas law review, 95(3), p. 467. Retrieved from https://search.ebscohost.com/login.aspx?direct=true&AuthType=shib&db=a9h&AN=121623082&site=ehost-live&custid=s3824264、P.492 から P.493 を参照。

[3] 本稿が参照あるいは引用した情報の観測・執筆者である中国のセキュリティ企業は以下の通り。

360 数字安全集団（「360」。過去には奇虎 360 として知られる。）および 360 脅威情報中心、安天科技集団（「安天」）および安天実験室、奇安信集団（「奇安信」）および奇安信威脅情報中心、啓明星辰集団（「啓明」）、騰訊控股有限公司（「テンセント」）および騰訊安全大脳、杭州安恒信息技術股份有限公司（「安恒」）および安恒信息威脅情報中心、绿盟科技集団（「緑盟科技」）および、友盟科技集団。

なお、360 と奇安信は設立者を同じくする企業である。2005 年に「齊向東（Qi Xiangdong）」は「北京奇虎科技有限公司」（奇虎 360）を設立した。その際に、「周鴻禕（Zhou Hongyi）」は全額出資した。その後周鴻禕は共同創始者、董事長兼 CEO に就任した。2014 年に齊向東は B to B 事業を重点とする 360 企業安全集団を設立して董事長に就任した。2016 年に 360 の B to C 事業と B to B 事業が分離されたことで、360 企業安全集団が奇安信として誕生した。

なお、両名は、1998 年に周鴻禕が設立した会社「3721」からの付き合いである。2003 年に中国共産党メディアである新華社通信の通信技術局副局長であった齊向東は、3721 の総経理に就任した。同年に、3721 は中国の Yahoo！（「雅虎中国」）に買収されている（買収後に周鴻禕は雅虎中国の総裁に、齊向東は副総裁に就任した）。そして 2005 年に両名は雅虎中国を離れ、奇虎 360 の設立に至っている。

https://www.forbes.com/profile/hongyi-zhou/?sh=84e068932031
https://www.forbes.com/profile/qi-xiangdong/?sh=da63acb49772
https://www.jiemian.com/article/4711643.html
https://www.wsj.com/market-data/quotes/CN/XSHG/601360/company-people/executive-profile/88150736

[4] 本稿が主として参照あるいは引用したレポートは以下の通り。本文の各章でも別途脚注を付した。

360 脅威情報中心 (2017). 『2016 年中国高級持続性威脅（APT）研究報告』P.5 から P.7、

https://www.docin.com/p-1852251217.html および https://bbs.360.cn/thread-14837417-1-1.html、

安天 (2018). 『2017 網絡安全威脅的回顧与展望』

https://www.antiy.cn/research/notice&report/research_report/20180707.html、

360 脅威情報中心 (2018). 『2017 年中国高級持続性威脅（APT）研究報告』P.5 から P.21、

https://cert.360.cn/report/detail?id=17444eedf20fed4d90c0e071b6b8a718 および https://zhuanlan.zhihu.com/p/34039327、
啓明星辰集団 (2018). 『2017 網絡安全態勢観察報告』P.51 から P.85、
https://www.freebuf.com/articles/paper/173377.html および
https://www.venustech.com.cn/uploads/2018/08/090935329814.pdf、
奇安信威脅情報中心 (2018). 『全球高級持続性威脅（APT）2018 年中報告』https://www.secrss.com/articles/4314、
360 脅威情報中心 (2019). 『2018 年全球高級持続性威脅（APT）総結報告』P.18 から P.22、
https://ti.qianxin.com/uploads/2019/01/02/56e5630023fe905b2a8f511e24d9b84a.pdf、
騰訊安全大脳 (2019). 『2018 年高級持続性威脅（APT）研究報告』https://s.tencent.com/research/report/623.html、
奇安信威脅情報中心 (2019). 『全球高級持続性威脅（APT）2019 年中報告』P.20 から P.23、
https://ti.qianxin.com/uploads/2019/07/04/4f68090f01bcbff1921e2351732379a9.pdf、
騰訊安全大脳 (2019). 『全球高級持続性威脅（APT）2019 年上半期研究報告』https://s.tencent.com/research/report/762、
安天 (2020). 『2019 網絡安全威脅的回顧与展望』
https://www.antiy.cn/research/notice&report/research_report/2019_AnnualReport.html、
騰訊安全大脳 (2020). 『全球高級持続性威脅（APT）2019 年研究報告』https://s.tencent.com/research/report/902、
奇安信威脅情報中心 (2020). 『全球高級持続性威脅（APT）2019 年報告』https://www.secrss.com/articles/17160、
啓明星辰集団 (2020). 『網絡安全態勢観察報告（2018～2019）』P.9 から P.11 および P.113 から P.154 、
https://www.freebuf.com/articles/paper/208385.html、
奇安信威脅情報中心 (2021). 『全球高級持続性威脅（APT）2020 年報告』P.33 から P.34、
https://ti.qianxin.com/uploads/2021/01/21/3df9fce0e9abf71265f88d45188f8fec.pdf、
360 脅威情報中心 (2021). 『2020 年全球高級持続性威脅（APT）研究報告』P.10 から P.33、
https://cn-sec.com/archives/262446.html、
安天 (2021). 『2020 網絡安全威脅的回顧与展望』
https://www.antiy.cn/research/notice&report/research_report/2020_AnnualReport.html、
安恒信息威脅情報中心 (2021). 『2020 年度高級威脅態勢研究報告』P.3 から P.30、
https://ti.dbappsecurity.com.cn/blog/articles/2021/01/01/apt-report-2020/、
360 脅威情報中心 (2021). 『2021 年上半期全球高級持続性威脅（APT）研究報告』P.33 から P.46、
https://cert.360.cn/report/detail?id=6c9a1b56e4ceb84a8ab9e96044429adc。
奇安信威脅情報中心 (2022). 『全球高級持続性威脅（APT）2021 年度報告』P.33 から P.34、
https://www.qianxin.com/threat/reportdetail?report_id=151、
安天 (2022). 『2021 網絡安全威脅的回顧与展望』
https://www.antiy.cn/research/notice&report/research_report/2021_AnnualReport.html、
緑盟科技 (2022). 『2021 年度高級威脅研究報告』P.8 から P.39、https://nti.nsfocus.com/apt/report、
奇安信威脅情報中心 (2022). 『全球高級持続性威脅（APT）2022 年中報告』P.8 から P.16、
https://zhuanlan.zhihu.com/p/579118137 および https://mp.weixin.qq.com/s/w9GHtqcAbHx-E5OsQXkKPw、
360 脅威情報中心 (2023). 『2022 年全球高級持続性威脅（APT）研究報告』P.1 から P.17、
https://bbs.360.cn/thread-16076700-1-1.html および https://www.bilibili.com/read/cv21324419、
緑盟科技 (2023). 『2022 年度高級威脅研究報告』P.15 から P.32 を参照。
https://nti.nsfocus.com/apt/report。

[5] 各 APT グループの情報については、中国のセキュリティ企業各社による脅威情報（TI）プラットフォームも参考になる。
https://nti.nsfocus.com/apt/home、https://ti.dbappsecurity.com.cn/apt/map、https://apt.360.net/、
https://ti.qianxin.com/apt/?type=map、および https://redqueen.tj-un.com/IntelHome.html。

2. 中国を標的とする攻撃の変遷

[6] JCIC コメンタリー『「デジタル中国」：情報化・デジタル化を軸に中国の安全保障観を理解する』で取り上げた。
https://www.j-cic.com/pdf/report/Digital-China.pdf。

[7] 中国は 2 つの問題に危機感を持った。一つ目は、APT に関する詳細かつ専門的な研究ができる中国国内組織が限られており、米国やロシアの情報に依存していること。そして二つ目は、米国とロシア（特に前者）が公的な脅威発生情報を通じて国内企業全体のセキュリティ保護レベルを向上するのに長けており、また、こうした共有情報が他国に対する政治的影響を与えていることであった。360 脅威情報中心 (2017).『2016 年中国高級持続性威脅（APT）研究報告』P.1 から P.2 を参照。

[8] 360 脅威情報中心 (2017).『2016 年中国高級持続性威脅（APT）研究報告』P.5 から P.7 を参照。

[9] 同上。

[10] 360 脅威情報中心 (2017).『2016 年中国高級持続性威脅（APT）研究報告』P.39 および P.41 を参照。

[11] 360 脅威情報中心 (2018).『2017 年中国高級持続性威脅（APT）研究報告』P.2 から P.6 を参照。

[12] 360 脅威情報中心 (2018).『2017 年中国高級持続性威脅（APT）研究報告』の主要観点および P.29 から P.30 を参照。また、米国および英国は、WannaCry の攻撃に背後には北朝鮮が関係していると非難した。https://www.bbc.com/news/world-us-canada-42407488 も参照。

[13] 360 脅威情報中心 (2017).『2016 年中国高級持続性威脅（APT）研究報告』P.29 から P.30 を参照。

[14] Bown P. Chad. (2019). *The 2018 US-China Trade Conflict after 40 Years of Special Protection*, Peterson Institute for International Economics. Retrieved from https://www.piie.com/publications/working-papers/2018-us-china-trade-conflict-after-40-years-special-protection、P.10 から P.11 および P.19 から P.20 を参照。

[15] Ibid., P.11 から P.12 および P.19 から P.20 を参照。

[16]『米国国防権限法（*Fiscal Year 2018 National Defense Authorization Act, NDAA*）』を参照。
https://2017-2021.state.gov/fiscal-year-2018-national-defense-authorization-act-ndaa/index.html。

[17]『アジア再保証推進法（*Asia Reassurance Initiative Act of 2018, ARIA*）』は米国の国益を再保証することを目的とした法律であるものの、台湾に対する武器売却と米国政府高官の訪問が含まれており、中国はこれに対して強く反対した。
https://www.congress.gov/bill/115th-congress/senate-bill/2736/text#toc-H8D70EE453E2F41CFA3259C8F8F0FC0EE、
https://www.congress.gov/115/plaws/publ409/PLAW-115publ409.pdf、
http://j.people.com.cn/n3/2019/0103/c94474-9534377.html。

[18] 360 脅威情報中心 (2019).『2018 年全球高級持続性威脅（APT）総結報告』P.2 から P.5、啓明星辰集団 (2020).『網絡安全態勢観察報告（2018～2019）』P.9 から P.11、および騰訊安全大脳 (2019).『2018 年高級持続性威脅（APT）研究報告』を参照。

[19] 「毒雲藤」および「藍宝菇」は2018年下半期に360が公開したAPTグループ。360脅威情報中心 (2019). 『2018年全球高級持続性威脅（APT）総結報告』P.18からP.21を参照。毒雲藤の技術的な詳述は、360脅威情報中心 (2018). 『毒云藤（APT-C-01）軍政情報刺探者揭露』の第3章を参照および、安天 (2018). 『"緑斑"行動——持続多年的攻撃』のP.6からP.36も参照。「緑斑」は毒雲藤の別名である。

https://cn-sec.com/archives/262446.html 、 https://blogs.360.net/post/APT_C_01.html、https://www.ddosi.org/apt/、https://www.secrss.com/articles/5256、および https://www.antiy.com/response/20180919.html。

「方程式」は中国のセキュリティ企業から「世界で最も洗練されたサイバー攻撃グループ」と評価される集団で、2015年以降の中国で継続注視されている。方程式の技術的な詳述は、Kaspersky (2015), *EQUATION GROUP: QUESTIONS AND ANSWERS*, Retrieved from https://securelist.com/equation-the-death-star-of-malware-galaxy/68750/、P.3からP.42を参照。更に、安天による次の4編のレポートからも詳述が確認できる。

https://www.antiy.com/response/EQUATION_ANTIY_REPORT.html、
https://www.antiy.com/response/EQUATIONS/EQUATIONS.html、
https://www.antiy.com/response/Equation_part_of_the_component_analysis_of_cryptographic_techniques.html、および
https://www.antiy.cn/research/notice&report/research_report/646.html。

なお、米国国防総省の『2018 年サイバー戦略』の P.3 INTRODUCTION は、中国およびロシアと米国との間に長期的な戦略競争が発生していることが記載されており、米国の主要な戦略的敵対国である当該 2 カ国に対しては、サイバー空間で「Defend forward」していくことを宣言している。なお、「Defend forward」は悪意あるサイバー活動をその発生源で中断または停止させる活動であると説明される。

https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF。

[20] 騰訊安全大脳 (2020). 『全球高級持続性威脅（APT）2019 年研究報告』P.3 から P. 7 を参照。

https://s.tencent.com/research/report/902。

[21] 騰訊安全大脳 (2020). 『全球高級持続性威脅（APT）2019 年研究報告』P. 4、奇安信威脅情報中心 (2019). 『全球高級持続性威脅（APT）2019 年中報告』P.21 から P.22、および啓明星辰集団 (2020). 『網絡安全態勢観察報告（2018～2019）』P.211 から P.212 を参照。

[22] 360 脅威情報中心 (2019). 『2018 年全球高級持続性威脅（APT）総結報告』P.5 を参照。

[23] 奇安信威脅情報中心 (2019). 『全球高級持続性威脅（APT）2019 年中報告』P.22 から P.23 を参照。ここでは「北米のセキュリティベンダーによる、中国を彷彿とさせる命名傾向」や、「北米のセキュリティベンダーが APT グループを中国とイランに帰属させる傾向」に対する奇安信の批判姿勢を確認することができる。奇安信の批判は APT10（menuPass）の関与を結論付ける中国国外のセキュリティ研究者とメディアにも及んだ。

以下へは、奇安信側の主張を記述する：

「中国国外のセキュリティベンダーは世界の通信事業者や携帯電話ネットワークを標的とした *APT* 作戦の攻撃元を中国との関連が疑われる *APT* グループに帰属させた。そして、こうしたセキュリティベンダーに追従するメディアとセキュリティ研究者たちは、『攻撃は中国の *APT10* によるものである』と結論付けることを好んでいる。その根拠は *China Chopper Webshell* や *Poison Ivy RAT* またはその亜種の使用、制御インフラの地理（中国国内）であるが、中国は歴史的に前述の両ツールを利用した *APT* 活動の主要犠牲者の一つである。そもそも、昨今の攻撃キャンペーンでは、*APT* グループが

積極的に偽旗を導入し、他の攻撃グループの戦術やテクニックを模倣して攻撃の帰属先を隠ぺいすることが重視されている。」

北米のセキュリティ研究組織による APT10（menuPass）の説明については下記を参照。

https://attack.mitre.org/groups/G0045/、

https://unit42.paloaltonetworks.jp/unit42-menupass-returns-new-malware-new-attacks-japanese-academics-organizations/。

2018 年時点において各 APT グループが中国を攻撃する際に使用する代表的な攻撃ツールは啓明星辰集団 (2020).『網絡安全態勢観察報告（2018～2019）』P.118 を参照。

[24] 奇安信威脅情報中心 (2019).『全球高級持続性威脅（APT）2019 年中報告』P.18 から P.23、奇安信威脅情報中心 (2020).『全球高級持続性威脅（APT）2019 年報告』P.19 を参照。2018 年までには存在しなかった北米セクションと関連する APT グループの記述が登場するという変化がみられるようになった。

[25] 360 脅威情報中心 (2016).『2015 年中国高級持続性威脅（APT）研究報告』P.3 では、2013 年のスノーデン事件や Kaspersky による「方程式」の研究といった第三者に発表を根拠として、北米の APT グループ組織が中国を標的としている可能性に言及している。360 脅威情報中心 (2017).『2016 年中国高級持続性威脅（APT）研究報告』では、ロシアやイランと対峙する北米の APT グループについて言及されているものの、こうしたグループが中国を攻撃するという記述は見られない。360 脅威情報中心 (2018).『2017 年中国高級持続性威脅（APT）研究報告』では、2016 年の Shadow Brokers（中国語では「影子経紀人」）による米国 NSA のサイバー兵器や 2017 年の New York Times による CIA のサイバー兵器の存在について言及されているものの、こうしたツールが中国に対する脅威となりうるかの是非については言及されていない。ただし前述（16 を参照）のとおり、この間に方程式に対する研究の結果が安天により進められている。360 脅威情報中心 (2019).『2018 年全球高級持続性威脅（APT）総結報告』においても、セクションを設けて注意喚起されているのは東アジア、東南アジア、南アジアの脅威であった。また、「来自美国」「APT」「针对中国」といった検索キーワードによりヒットする記事は 2019 年以降のものが多い。

[26] IMF による『2020 年報告書』https://www.imf.org/external/pubs/ft/ar/2020/eng/および特設サイト『Crisis Like No Other』https://www.imf.org/external/pubs/ft/ar/2020/eng/spotlight/covid-19/を参照。

[27] 2020 年今年の旧正月に仕事再開後に在宅勤務を利用したユーザは 3 億人を超え、旧正月明けの仕事始め後 30 日以内の在宅勤務は前年比 663%増。360 脅威情報中心 (2021).『2020 年全球高級持続性威脅（APT）研究報告』P.51 から P.52、奇安信威脅情報中心 (2021).『全球高級持続性威脅（APT）2020 年報告』P.1 から P.8 を参照。啓明星辰集団 (2022).『網絡安全態勢観察報告（2020～2021）』P.46 から P.75、安天 (2021).『2020 網絡安全威脅的回顧与展望』を参照。

[28] 「毒雲藤」の従来までの戦術は、科学技術研究機関や大学、防衛産業に関連する周辺組織を標的としたもので、間接的に機密情報を窃取することを特徴としていた。360 脅威情報中心 (2021).『2020 年全球高級持続性威脅（APT）研究報告』P.52、P.61 から P.62、『毒云藤（APT-C-01）軍政情報刺探者揭露』第 3 章、奇安信威脅情報中心 (2021).『全球高級持続性威脅（APT）2020 年報告』P.17 を参照。

[29] 360 脅威情報中心 (2021).『2020 年全球高級持続性威脅（APT）研究報告』P.52、P.61 から P.62 を参照。

[30] 360 脅威情報中心 (2021)『2020 年全球高級持続性威脅（APT）研究報告』P.26 から P.29、P.59 から P.68、奇安信威脅情報中心 (2021).『全球高級持続性威脅（APT）2020 年報告』P.19 から P.20、啓明星辰集団 (2022).『網絡安全態勢観察報告（2020～2021）』

P.56 から P.57、および 360 脅威情報中心 (2015).『OceanLotus（APT-C-00）数字海洋的游猟者』P.1 から P.5 および https://blogs.360.net/post/oceanlotus-apt.html を参照。

[31] 360 脅威情報中心 (2021)『2020 年全球高級持続性威脅（APT）研究報告』P.19 から P.21、P.55、啓明星辰集団 (2022).『網絡安全態勢観察報告（2020～2021）』P.57 から P.58、奇安信威脅情報中心 (2021).『全球高級持続性威脅（APT）2020 年報告』P.16 から P.17、および安天 (2021).『2020 網絡安全威脅的回顧与展望』を参照。

[32] 啓明星辰集団 (2022).『網絡安全態勢観察報告（2020～2021）』P.57 から P.58、奇安信威脅情報中心 (2021).『全球高級持続性威脅（APT）2020 年報告』P.15 から P.16 を参照。

[33] 360 脅威情報中心 (2021)『2020 年全球高級持続性威脅（APT）研究報告』P.29 から P.32、P.74 から P.84、奇安信威脅情報中心 (2021).『全球高級持続性威脅（APT）2020 年報告』P.27 から P.28 を参照。

[34] ロシアによる中国への APT 攻撃に関して中国政府による非難は発生しなかった。その後、中国の習近平国家主席とロシアのプーチン大統領は 2022 年 2 月の北京冬季オリンピック開催前に北京で会談を行い、『中華人民共和国とロシア連邦新時代の国際関係とグローバルな持続可能開発についての共同声明』を発表した。両国は各国のサイバーセキュリティ活動を法的に規制可能な新しい行動規範や国際法を共同開発すべきと表明した。 https://www.yidaiyilu.gov.cn/xwzx/gnxw/219621.htm を参照。

[35] 中国外交部、在外中国大使館、共産党が支援するメディア各社に米国から中国に向けたサイバー攻撃を激しく非難する内容が大々的に掲載された。外交部は「米国が加害者、中国は被害者」という姿勢を強調しており、今後も自国を防衛するために必要な措置を講じると明言した。後述する方程式（APT-C-40）および Longhorn（APT-C-39）に関する批判色の強いステイトメントは以下の通り。

> 2020 年 3 月 4 日の外交部による『披露美国中央情報局 CIA 攻撃組織（Apt-c-39）対中国関鍵領域長達十一年的網絡渗透攻撃』
> http://www.xinhuanet.com/world/2020-03/03/c_1210499250.htm、https://www.360.cn/n/11563.html、
> または https://zhuanlan.zhihu.com/p/130272230 および、
> http://news.cctv.com/2020/03/04/ARTIyf5G4nbdU3zLTYLezyIQ200304.shtml、
> 2022 年 3 月 3 日の外交部による『外交部：強烈要求美国停止針対中国和全球的網絡窃密和攻撃』
> https://www.fmprc.gov.cn/wjb_673085/zzjg_673183/jks_674633/jksxwlb_674635/202203/t20220315_10651921.shtml または
> https://www.thepaper.cn/newsDetail_forward_16938094 および
> https://news.cctv.com/2022/03/03/ARTIvJxZWBh4ftn2Xl8E9XdD220303.shtml。また、http://us.china-embassy.gov.cn/eng/fyrth/202203/t20220303_10647695.htm も参照。

[36] 安天 (2015).『修改硬盤固件的木馬探索方程式（EQUATION）組織的攻撃組件』、安天 (2016).『従方程式到方程組』、安天 (2017).『方程式組織 EQUATION DRUG 平台解析』、360 脅威情報中心 (2017).『2016 年中国高級持続性威脅（APT）研究報告』P.19 から P.21 を参照。

[37] 360 脅威情報中心 (2021).『2021 年上半期全球高級持続性威脅（APT）研究報告』P.6 を参照。

[38] 啓明星辰集団 (2022).『網絡安全態勢観察報告（2020～2021）』P.101 から P.102 を参照。

[39] 奇安信威脅情報中心 (2022).『全球高級持続性威脅（APT）2021 年度報告』P.73 を参照。

[40] 奇安信威脅情報中心 (2022).『全球高級持続性威脅（APT）2021 年度報告』P.73 から P.74、360 脅威情報中心 (2021).『2021 年上半期全球高級持続性威脅（APT）研究報告』P.47 から P.54、緑盟科技 (2022).『2021 年度高級威脅研究報告』P.19 を参照。

[41] 奇安信威脅情報中心 (2022).『全球高級持続性威脅（APT）2021 年度報告』P.16、360 脅威情報中心 (2021).『2021 年上半期全球高級持続性威脅（APT）研究報告』P.9 を参照。

[42] 奇安信威脅情報中心 (2022).『全球高級持続性威脅（APT）2021 年度報告』P.5 を参照。

[43] 奇安信威脅情報中心 (2022).『全球高級持続性威脅（APT）2021 年度報告』P.8、360 脅威情報中心 (2021).『2021 年上半期全球高級持続性威脅（APT）研究報告』P.8 を参照。

[44] 360 脅威情報中心 (2023).『2022 年全球高級持続性威脅（APT）研究報告』P.58 を参照。

[45] 360 脅威情報中心 (2023).『2022 年全球高級持続性威脅（APT）研究報告』P.36 および P.66 を参照。また、奇安信威脅情報中心 (2022).『全球高級持続性威脅（APT）2022 年中報告』P.11 から P.12 および P.32 も参照。

[46] 同上。また、微歩在宣研究響応中心（2022）.『曝光！"海蓮花"組織運営的物連網僵尸網絡 Torii』も参照。MIPS と ARM は異なる企業により設計され、提供されている命令セットアーキテクチャで、マイクロプロセッサが利用する。中国の国産製品である「龍芯（Loongson）」や「Kunpeng」は MIPS 或いは ARM を利用している。

https://mp.weixin.qq.com/s?__biz=Mzg5MTc3ODY4Mw==&mid=2247496925&idx=1&sn=84124e5e3aca9f6ec49395ecaa9847bc&chksm=cfca97c9f8bd1edf9054f7aa8c837d3e940099c91571a7d95847a9f9401c8f27e05d8b4940eb&scene=178&cur_album_id=2444515725966180358#rd

[47] 緑盟科技 (2022).『2021 年度高級威脅研究報告』P.16 を参照。

[48] 360 脅威情報中心 (2023).『2022 年全球高級持続性威脅（APT）研究報告』P.66 を参照。

[49] 本章で参照した資料は、別途文末脚注が付記されている場合を除いて、文末脚注 4 に列挙したレポートを参考にした。

3．中国への攻撃に対して活発に活動する組織

[50] 中越間の貿易データについては OEC による https://oec.world/en/profile/bilateral-country/vnm/partner/chn を参照。また、米越間の貿易データについては https://oec.world/en/profile/bilateral-country/usa/partner/vnm を参照。

[51] 両国は南シナ海のパラセル諸島（中国語は「西沙群島」）やスプラトリー諸島（「南沙群島」）を巡って、古くは 1974 年と 1988 年で衝突したことがあるほか、1979 年には中越戦争で衝突している。

[52] 「国家の核心利益」について、2011 年 9 月に中国共産党が発表した白書『中国の平和的発展』には「国家の主権、安全保障、領土の保全、国家統一、中国憲法が定める国政体制と社会一般の安定、持続可能な経済・社会発展のための基本的保証など」と定義されている。中国政府は南シナ海諸島とその周辺海域に対する議論の余地のない主権を表明し、西沙諸島と南沙諸島の領有を強調した。また、ベトナムの主張を「国際連合憲章、国連海洋法条約を含む国際法に違反」と述べた。なお、国務院は 2012 年に同海域への三沙市の設立許可を公表した。

http://www.scio.gov.cn/zfbps/ndhf/2011/Document/1000032/1000032.htm、

https://www.sxjz.gov.cn/rdzt/qmgjaqjyr/xgzswd/content_328820、

http://www.gov.cn/jrzg/2012-08/10/content_2201976.htm、
http://news.cctv.com/2020/04/14/ARTIMQI4yq8hMnewGJlfzirr200414.shtml、
http://japanese.china.org.cn/politics/txt/2012-06/24/content_25720891.htm。

[53] 同月の 2014 年 5 月にはベトナムで反中デモが発生し、中国人に死傷者が発生した。https://www.nikkei.com/article/DGXNASGM15034_V10C14A5FF1000/を参照。2017 年 7 月及び 2018 年 3 月には、中国の圧力を受けたベトナム政府が、許可を与えていた南シナ海における石油掘削を中止し、ベトナム国民の不満が募った。

[54] 石油掘削問題を巡った対立では、ベトナムの航空分野に対するサイバー攻撃も発生した。2016 年にホーチミンとハノイにある空港とベトナム航空がサイバー攻撃を受け、当時の Nguyen Nhat 運輸省副相は、ベトナム航空のフライト情報を表示する画面が制御されたことを述べた。また、ベトナム民間航空局は攻撃が空港の電子チェックインシステムが中断したため手作業によるチェックイン手続きを行ったことを明らかにしている。ベトナム航空の公式ウェブサイトは「1937CN」の画像と共に南シナ海問題に関してベトナムを侮辱する言葉に差し替えられたことから、同国メディアは中国のサイバー組織が引き起こしたものであると非難した。
https://www.businessinsider.com/hackers-attacking-vietnam-airports-2016-7?op=1、
https://en.vietnamplus.vn/aviation-security-tightened-following-cyberattacks-at-airports/96917.vnp、
https://vietnamnews.vn/society/300416/chinese-hackers-attack-vns-airports-and-vietnam-airlines-website.html。

[55] ベトナム国会で審議されていた「経済特区法案」は、外国の投資家に対して最長 99 年間の土地の貸与を可能にする条項を含んでいた。３つの経済特区予定地には中国国境や南シナ海沿岸など地政学的な重要地点に位置するクアンニン、カインホア、キエンザン省が含まれており、外国企業に長期の土地使用を認めることに対する安全保障上の強い懸念が表明した。

[56] 日本貿易振興機構（JETRO）による『中国企業の投資が急増、ベトナム国内では警戒の声も　米中貿易摩擦の情勢下に見る中国企業の対外直接投資動向調査』を参照。https://www.jetro.go.jp/biz/areareports/2020/7138c3cc43a2a67e.html。

[57] ドリームワークスと上海のパールスタジオによる共同製作映画に中国の九段下線を示す地図が映り、ベトナムにおける上映が禁止された。香港出身の映画スター（ジャッキー・チェン）が九段下を支持する発言したことで、ベトナムのインターネット上の反発を受け、慈善訪問がキャンセルとなった。

[58] 2020 年 4 月は中国政府が海南省三沙市の下に「西沙区」及び「南沙区」と称する行政区の新設を公表したタイミングでもあった。

[59] ベトナムは国際電気通信連合（ITU）による『Global Cybersecurity Index（GCI）』評価で、2017 年の 101 位から 2020 年には 25 位に上昇した（日本は 2017 年 11 位、2020 年 7 位）。英国の国際戦略研究所（IISS）による『Cyber Capabilities and National Power 2021』において、ベトナムは日本と同じ「Tier 3（いくつかのカテゴリーに強みまたは潜在的な強みを持つが、その他のカテゴリーに大きな弱点を持つ国）」として評価された。ハーバードケネディスクールベルファーセンターによる『National Cyber Power Index』では、2020 年の 20 位から 2022 年には 8 位まで上昇した（日本は 9 位から 16 位に転落）。

[60] ベトナム人ハッカーの「Hieu」は外国の銀行口座や米国の個人の社会保障番号をハッキングして販売するなどの違法行為により逮捕され、米国司法当局により 45 年の実刑判決を受けた（後に 13 年に減刑された）。後に Hieu はベトナム国家サイバーセキュリティセンター（NCSC）により雇用されるに至っている。ベトナム NCSC によると、毎週平均 256 件以上のベトナムの国内システムに対する攻撃が発生しているという。
https://www.msn.com/en-us/news/world/notorious-vietnamese-hacker-turns-government-cyber-agent/ar-AAXGQat、

https://ncsc.gov.vn/intro、および https://en.vietnamplus.vn/over-265-cyber-attacks-per-week-on-vietnamese-systems/232188.vnp。

[61] ISEAS-Yusof Ishak Institute の The ASEAN Studies Centre による統計の結果、ベトナムにおける中国の経済的影響力は好意的に受け止められていない。中国を最も影響力のある経済大国と見ているベトナム人 71.9%が「中国の地域的な拡大が心配だ」と回答した。
https://www.iseas.edu.sg/wp-content/uploads/pdfs/TheStateofSEASurveyReport_2020.pdf。

3. 中国への攻撃に対して活発に活動する組織

[62] 海蓮花に関するまとまった情報は、360、安垣、奇安信の脅威情報が参考になる。
https://apt.360.net/orgDetail/1、
https://ti.dbappsecurity.com.cn/apt/dc527634-307f-11eb-9593-ac1f6b480078/overview、
https://ti.qianxin.com/apt/detail/5aa0eed8d70a3f07e3f73891?name=%E6%B5%B7%E8%8E%B2%E8%8A%B1&type=map。

[63] なお、ベトナム政府は「根拠のない情報」であるとして APT グループへの関与を否定している。
https://www.mofa.gov.vn/en/tt_baochi/nr140808202328/ns200523100607/view および、
https://www.mofa.gov.vn/en/tt_baochi/nr140808202328/ns200428160315/view。

[64] 中国のセキュリティ企業による海蓮花の詳述は以下を参照。
360 脅威情報中心 (2015).『OceanLotus（APT-C-00）数字海洋的游猟者』P.1 から P.5、
安天 (2018).『2017 網絡安全威脅的回顧与展望』、安天 (2021).『2020 網絡安全威脅的回顧与展望』、
360 脅威情報中心 (2018).『2017 年中国高級持続性威脅（APT）研究報告』P.8 から P.10、P.14、
360 脅威情報中心 (2019).『2018 年全球高級持続性威脅（APT）総結報告』P.18 から P.19、
騰訊安全大脳 (2018).『海蓮花 APT 組織最新攻撃様本分析』https://s.tencent.com/research/report/471、
騰訊安全大脳 (2018).『境外 APT"海蓮花"（OceanLotus）最新攻撃活動解析』https://s.tencent.com/research/report/490、
騰訊安全大脳 (2019).『2018 年高級持続性威脅（APT）研究報告』https://s.tencent.com/research/report/623.html、
騰訊安全大脳 (2019).『全球高級持続性威脅（APT）2019 年上半期研究報告』https://s.tencent.com/research/report/762、
騰訊安全大脳 (2019).『海蓮花組織 2019 年第一季度針対中国的攻撃活動技術揭秘』
https://s.tencent.com/research/report/715.html、
騰訊安全大脳 (2019).『"海蓮花（OceanLotus）"2019 年針対中国的攻撃活動滙総』
https://s.tencent.com/research/report/860、
奇安信威脅情報中心 (2019).『全球高級持続性威脅（APT）2019 年中報告』P.9 から P.10、
啓明星辰集団 (2020).『網絡安全態勢観察報告（2018～2019）』P.119 から P.134、
騰訊安全大脳 (2020).『全球高級持続性威脅（APT）2019 年研究報告』https://s.tencent.com/research/report/902、
奇安信威脅情報中心 (2020).『全球高級持続性威脅（APT）2019 年報告』P.9 から P.11、
360 脅威情報中心 (2021).『2020 年全球高級持続性威脅（APT）研究報告』P.26 から P.28、P.49 から P.52 から P.68、P.73 から P.77 および P.88、
360 脅威情報中心 (2021).『2021 年上半期全球高級持続性威脅（APT）研究報告』P.21 から P.22、P.35 から P.37、P.50 から P.53、
奇安信威脅情報中心 (2021).『全球高級持続性威脅（APT）2020 年報告』P.18 から P.20、
安恒信息威脅情報中心 (2021).『2020 年度高級威脅態勢研究報告』P.16 から P.17、

奇安信威脅情報中心 (2022).『全球高級持続性威脅（APT）2021 年度報告』P.6 から P.8、P.37 から P.39、P.72、
奇安信威脅情報中心 (2022).『全球高級持続性威脅（APT）2022 年中報告』P.11 から P.12、P.31 から P.32、
緑盟科技 (2022).『APT 組織情報研究年鑑』P.166、
360 脅威情報中心 (2023).『2022 年全球高級持続性威脅（APT）研究報告』P.35 から P.36、P.66、および
緑盟科技 (2023).『2022 年度高級威脅研究報告』P.16 から P.20 を参照。
なお海蓮花は、欧米のセキュリティ企業の文献には APT32 や Cobalt Kitty の名前で登場し、ベトナムの製造業、テック企業、ホスピタリティ産業に既得権益を持つ外国の民間企業や、ベトナムに対して異なる政治的見解を持つ個人、メディア、外国政府を攻撃するグループとして説明されている。https://attack.mitre.org/groups/G0050/。

[65] 360 脅威情報中心 (2015).『OceanLotus（APT-C-00）数字海洋的游猟者』P.2、啓明星辰集団 (2018).『2017 網絡安全態勢観察報告』、奇安信威脅情報中心 (2019).『全球高級持続性威脅（APT）2019 年中報告』P.9、奇安信威脅情報中心 (2021).『全球高級持続性威脅（APT）2020 年報告』P.34、奇安信威脅情報中心 (2022).『全球高級持続性威脅（APT）2021 年度報告』P.4、緑盟科技 (2023).『2022 年度高級威脅研究報告』P.20、360 脅威情報中心 (2023).『2022 年全球高級持続性威脅（APT）研究報告』P.66 を参照。

[66] 啓明星辰集団 (2022).『網絡安全態勢観察報告（2020～2021）』P.82 から P.84 参照。2020 年から 2021 年前半にかけて啓明のスレットインテリジェンスセンターにより捕獲されたデータによると、中国国内で IoT ボットのホストが分布する地域は、河南省（8.24%）、江蘇省（8.17%）、遼寧省（7.45%）、山東省（5.92%）、浙江省（5.46%）の順に多い。

[67] 360 脅威情報中心 (2023).『2022 年全球高級持続性威脅（APT）研究報告』P.35 から P.36、P.66、および奇安信威脅情報中心 (2022).『全球高級持続性威脅（APT）2022 年中報告』P.11 から P.12、P.24、P.31 から P.32。

[68] 360 脅威情報中心 (2021).『2021 年上半期全球高級持続性威脅（APT）研究報告』P.51 から P.52、360 脅威情報中心 (2023).『2022 年全球高級持続性威脅（APT）研究報告』P.35 から P.36、奇安信威脅情報中心 (2022).『全球高級持続性威脅（APT）2021 年度報告』P.6 から P.8、P.37 から P.39、P.72 を参照。

[69] 360 脅威情報中心 (2023).『2022 年全球高級持続性威脅（APT）研究報告』P.35 を参照。

[70] 文末脚注 61 および緑盟科技 (2022).『APT 組織情報研究年鑑』P.20 を参照。

[71] 中国はインド洋に面するパキスタンと密接な関係を有するほか、スリランカやバングラデシュとも関係を深化している。さらに、中国はパキスタン、バングラデシュ、ミャンマーなどのインド周辺国に武器輸出をしている。
https://www.wsws.org/en/articles/2016/11/05/bang-n05.html。
2015 年に中国が推進する一帯一路イニシアチブの基幹プロジェクト「中国・パキスタン経済回廊（中パ回廊）」の内容が公開されると、その経路にインドがパキスタンと領有権をめぐるカシミール地方が含まれることが判明した。中国が建設を支援する中パ経済回廊は「一帯一路」構想の旗艦プロジェクトで電力施設や輸送インフラなどを開発する。
http://japanese.china.org.cn/business/txt/2021-01/09/content_77097561.htm、
https://jp.reuters.com/article/idJP00093300_20210112_00220210111。
2016 年 10 月には習近平が国家主席としては約 30 年ぶりにバングラデシュを訪問し、翌月から中国企業が建設したバングラデシュのグワダル港が運用開始となった。2017 年 7 月には、スリランカのハンバントタ港の中国企業への権益貸与が合意された。

[72] インド商務省のデータによると、2015-16 年度のインド国内総輸入量の 16%が中国からの輸入を占めており、その輸入金額は、米国、UAE、サウジアラビアからの輸入金額合計よりも多く、対中貿易赤字に陥っていることを現地メディアが報じている。

https://www.firstpost.com/business/dont-fall-for-false-nationalism-india-in-no-position-to-ban-chinese-imports-3058340.html。

[73] 2017 年のドクラムでの道路建設を巡る対立では軍事衝突は発生しなかった。なお、ブータン政府が中国に対してドクラムにおける道路建設は協定違反であると非難している。

https://www.firstpost.com/india/bhutan-issues-scathing-statement-against-china-claims-beijing-violated-border-agreements-of-1988-1998-3760587.html。

2020 年 5 月に発生したインド北部の国境係争地帯「ラダック」の軍事衝突では、戦闘のため各陣営でそれぞれ 20 人以上の兵士が死亡したことがインド側により報告されている。

https://www.indiatoday.in/india/story/india-china-face-off-ladakh-lac-chinese-casualties-pla-1689714-2020-06-16、
https://www.ndtv.com/india-news/chinese-army-confirms-their-commanding-officer-was-killed-in-ladakh-face-off-during-military-level-talks-in-galwan-sources-2250280。

ラダックの軍事衝突を受けて、2020 年 6 月から 7 月にかけて複数の南アジアの ATP グループ（「白象」や「响尾蛇」）が中国を攻撃したことを安恒が報じた。安恒信息威脅情報中心 (2021).『2020 年度高級威脅態勢研究報告』P.4 を参照。

[74] 2020 年 6 月にインド当局は 59 種類のモバイルアプリの使用を禁止したが、その多くが中国企業のアプリであった。

https://pib.gov.in/PressReleasePage.aspx?PRID=1635206。

中国製電化製品のボイコットや中華料理店の利用に対するボイコットも発生した。
https://www.forbes.com/sites/meghabahree/2020/07/08/indias-anti-china-wave-sparks-uncertainty-and-fears-of-large-scale-job-losses/?sh=195b9fec1d5e、
https://www.ndtv.com/india-news/boycott-chinese-food-says-union-minister-ramdas-athwale-who-shouted-go-corona-2248312
https://www.bbc.com/news/world-asia-india-53150898、および
https://www.jetro.go.jp/biznews/2020/07/d126699885f9a315.html。

The Guardian 紙によると、2021 年 8 月のインド世論調査では、回答者の 6 割近くが「国境紛争を解決するために中国と戦争すべき」と答え、9 割以上が「中国製のアプリを禁止して、中国企業との契約を拒否することを支持する」と答えたという。

https://www.theguardian.com/world/2021/apr/29/border-dispute-casts-shadow-over-chinas-offers-of-covid-help-for-india。

[75] ラダックでは 2022 年 2 月にもインドの州給電指令所（SLDC）の 7 拠点がネットワークへの不正侵入を受けた。米国のセキュリティ企業は中国国家安全部（MSS）と繋がりのある攻撃者の犯行を指摘したが、同年 4 月に中国外交部が関与を否定した。

https://www.recordedfuture.com/continued-targeting-of-indian-power-grid-assets、
http://new.fmprc.gov.cn/web/fyrbt_673021/jzhsl_673025/202204/t20220407_10665432.shtml。

[76] 中国のセキュリティ企業による蔓霊花のまとまった情報については以下を参照。

https://apt.360.net/orgDetail/5、
https://ti.dbappsecurity.com.cn/apt/dc670d3a-307f-11eb-9593-ac1f6b480078/および
https://ti.qianxin.com/apt/detail/5acb2bd9596a10001a1a9797?name=%E8%94%93%E7%81%B5%E8%8A%B1&type=map、
蔓霊花の詳述は以下も参照。
360 脅威情報中心 (2017).『2016 年中国高級持続性威脅（APT）研究報告』P.40、
啓明星辰集団 (2018).『2017 網絡安全態勢観察報告』P.134 から P.142、

騰訊安全大脳 (2018).『蔓霊花（BITTER）APT 組織針対中国境内軍工、核能、政府等敏感機構的最新攻撃活動報告』https://s.tencent.com/research/report/615、
360 脅威情報中心 (2019).『2018 年全球高級持続性威脅（APT）総結報告』P.13 および P.27、
360 烽火実験室 (2019).『蔓霊花（APT-C-08）移動平台攻撃活動掲露』https://www.anquanke.com/post/id/195378、
騰訊安全大脳 (2019).『2018 年高級持続性威脅（APT）研究報告』https://s.tencent.com/research/report/623.html、
騰訊安全大脳 (2019).『全球高級持続性威脅（APT）2019 年上半期研究報告』https://s.tencent.com/research/report/762、
騰訊安全大脳 (2019).『印巴戦争陰影下的網絡戦―近期印巴 APT 組織攻撃活動滙総』https://s.tencent.com/research/report/799、
騰訊安全大脳 (2020).『全球高級持続性威脅（APT）2019 年研究報告』https://s.tencent.com/research/report/902、
啓明星辰集団 (2020).『網絡安全態勢観察報告（2018～2019）』P.77 から P.80、
奇安信威脅情報中心 (2021).『全球高級持続性威脅（APT）2020 年報告』P.22 から P.24 および P.34、
360 脅威情報中心 (2021).『2020 年全球高級持続性威脅（APT）研究報告』P.12 から P.15、P.37 から P.38、P.60 から P.61 および P.74、
啓明星辰集団 (2022).『網絡安全態勢観察報告（2020～2021）』P.50 から P.53、
360 脅威情報中心 (2021).『2021 年上半期全球高級持続性威脅（APT）研究報告』P.9 から P.10、P.33 から P.39、P.51 から P.53、
安恒信息威脅情報中心 (2021).『2020 年度高級威脅態勢研究報告』P.4、P.8 から P.12、
奇安信威脅情報中心 (2022).『全球高級持続性威脅（APT）2021 年度報告』P.4、P.8 から P.10、P.41 から P.44、
奇安信威脅情報中心 (2022).『全球高級持続性威脅（APT）2022 年中報告』P.32 から P.36、
緑盟科技 (2022).『2021 年度高級威脅研究報告』P.5 から P.6、P.16 から P.21、
緑盟科技 (2022).『APT 組織情報研究年鑑』P.157、および
360 脅威情報中心 (2023).『2022 年全球高級持続性威脅（APT）研究報告』P.12 から P.13 を参照。

[77] 啓明星辰集団 (2022).『網絡安全態勢観察報告（2020～2021）』P.50 から P.52 では、サイバー空間における地域間の絶え間ない攻撃と印国境沿いで発生している紛争や摩擦との関係性が指摘された他、中国以外にもパキスタンを集中的に攻撃することが指摘された。中国とパキスタンを狙う傾向については奇安信威脅情報中心 (2021).『全球高級持続性威脅（APT）2020 年報告』P.22、安恒信息威脅情報中心 (2021).『2020 年度高級威脅態勢研究報告』P.12、奇安信威脅情報中心 (2022).『全球高級持続性威脅（APT）2022 年中報告』P.41 でも指摘されている。

[78] 中国のセキュリティ企業の 360 が取得した 2016 年 11 月のサンプルから判明したことが発表された。サンプルの編集時期は 2016 年 5 月から 9 月に集中し、ネットワーク上における活動は 9 月に集中した。安恒信息威脅情報中心 (2021).『2020 年度高級威脅態勢研究報告』P.4、P.8 から P.12 を参照。https://apt.360.net/orgDetail/5 も参照。

[79] 安恒信息威脅情報中心 (2021).『2020 年度高級威脅態勢研究報告』P.4、P.8 から P.12、および騰訊安全大脳 (2018).『蔓霊花（BITTER）APT 組織針対中国境内軍工、核能、政府等敏感機構的最新攻撃活動報告』、https://s.tencent.com/research/report/615 および 360 烽火実験室 (2019).『蔓霊花（APT-C-08）移動平台攻撃活動掲露』https://www.anquanke.com/post/id/195378。

[80] 安恒信息威脅情報中心 (2021).『2020 年度高級威脅態勢研究報告』P.4、P.8 から P.12 を参照。https://apt.360.net/orgDetail/5、https://ti.dbappsecurity.com.cn/apt/dc670d3a-307f-11eb-9593-ac1f6b480078/および https://ti.qianxin.com/apt/detail/5acb2bd9596a10001a1a9797?name=%E8%94%93%E7%81%B5%E8%8A%B1&type=map も参照。

[81] 安恒信息威脅情報中心 (2021). 『2020 年度高級威脅態勢研究報告』P.4、P.8 から P.12 を参照。

[82] 360 脅威情報中心 (2021). 『2021 年上半期全球高級持続性威脅（APT）研究報告』P.10 および P.51 を参照。

[83] 同上。2021 年 2 月に蔓霊花は Windows OS のコアコンポーネント「Win32k」のゼロデイ脆弱性を悪用したことが安恒により報告された。https://nvd.nist.gov/vuln/detail/CVE-2021-1732 および https://japan.zdnet.com/article/35166328/を参照。

[84] 360 脅威情報中心 (2021). 『2021 年上半期全球高級持続性威脅（APT）研究報告』P.9 および P.33 を参照。

[85] 2022 年に蔓霊花は医療分野を標的としたが、同年には複数の集団感染症（サル痘、原因不明の小児肝炎、新型コロナウイルス亜種など）が発生している。360 脅威情報中心 (2023). 『2022 年全球高級持続性威脅（APT）研究報告』P.12 を参照。

[86] 奇安信威脅情報中心 (2022). 『全球高級持続性威脅（APT）2021 年度報告』P.4、P.8 から P.10、P.41 から P.44 および奇安信威脅情報中心 (2022). 『全球高級持続性威脅（APT）2022 年中報告』P.32 から P.36 を参照。

[87] 2020 年 1 月に台湾の蔡英文総統は、中華民国（台湾）と名乗り政府・軍隊・選挙といった国家運営機能を備える実質的な独立国であり、独立国家を宣言する必要性がないという考えを明らかにした。https://english.president.gov.tw/NEWS/5959 および https://english.president.gov.tw/NEWS/5962。

[88] 人民網による核心的利益に関する 2019 年 5 月記事は、台湾問題が中国の内政であり外国からの干渉を一切許されないことを強調した。2019 年 1 月 2 日に習近平は台湾に向けて「平和的統一を目指すこと、一方で武力行使を放棄しない」というメッセージを発信しているが、ここで強調しているのは、武力が外部勢力による干渉や少数の台湾独立分子による分裂活動であり、中国人は中国人と戦わないという姿勢であった。https://news.ltn.com.tw/news/world/breakingnews/2659618 および http://j.people.com.cn/n3/2019/0509/c94474-9576531.html。

[89] 2017 年 10 月の十九大で習近平中国国家主席が「台湾同胞と中国大陸の発展を共有する」と発言をした。以降、中国では台湾からの就学・就職促進などの優遇措置や、大陸に暮らす台湾人への「居住証」の発行といった便宜が図られた。2019 年 1 月に習近平国家主席は『台湾同胞に告げる書』の中で台湾に対して「一国二制度」を提起した。

[90] 台湾の『2019 年国防報告書』には、「台湾がインド太平洋地域における米国の重要な安全保障上のパートナー」と記載され、中国の反感をかった。

[91] 台湾の『2019 年国防報告書』は、2019 年～2021 年 8 月の期間にインターネットから切り離された台湾の軍用ネットワークで約 14 億件の異常が検知され、侵入は未然に防がれたことが報告されている。https://www.ustaiwandefense.com/taiwan-ministry-of-national-defense-reports/。

[92] 世論調査は NCCU 選挙研究センターが 8 月 10 日～15 日にかけて実施し、固定電話 874 件、携帯電話 425 件の計 1,299 件の有効回答を集めた。信頼水準は 95%、誤差は 2.72%ポイントと発表された。
https://www.taipeitimes.com/News/front/archives/2021/12/30/2003770419、
http://www.taiwandemocracy.org.tw/opencms/english/publication/journal/data/Journal0037.html。

[93] 台湾の政治大学選挙研究中心が発表した『Taiwan Independence vs. Unification with the Mainland(1994/12~2022/12)』は、https://esc.nccu.edu.tw/PageDoc/Detail?fid=7801&id=6963 を参照。

[94] 台湾選挙についての NHK 記事『どうなる台湾 総統選挙まで 1 年 候補者選びは？中国との関係は？』。https://www3.nhk.or.jp/news/special/international_news_navi/articles/qa/2023/02/09/29192.html を参照。

[95] 中国のセキュリティ企業による毒雲藤のまとまった情報については以下を参照。

https://apt.360.net/orgDetail/2、
https://ti.dbappsecurity.com.cn/apt/7510ddc2-345f-11eb-9593-ac1f6b480078/overview、
https://ti.qianxin.com/apt/detail/5acb2add596a100015e5df0f?name=%E6%AF%92%E4%BA%91%E8%97%A4&type=map。
毒雲藤の詳述は以下を参照。
安天 (2018). 『"緑斑"行動——持続多年的攻撃』https://www.antiy.com/response/20180919.html、
360 脅威情報中心 (2018).『毒雲藤（APT-C-01）軍政情報刺探者掲露』https://blogs.360.net/post/APT_C_01.html または https://www.ddosi.org/apt/あるいは https://www.secrss.com/articles/5256、
360 脅威情報中心 (2019). 『2018 年全球高級持続性威脅（APT）総結報告』P.18 から P.21、
騰訊安全大脳 (2019). 『2018 年高級持続性威脅（APT）研究報告』https://s.tencent.com/research/report/623.html、
騰訊安全大脳 (2019). 『全球高級持続性威脅（APT）2019 年上半期研究報告』https://s.tencent.com/research/report/762、
奇安信威脅情報中心 (2019). 『全球高級持続性威脅（APT）2019 年中報告』P.22 から P.23、
騰訊安全大脳 (2020). 『全球高級持続性威脅（APT）2019 年研究報告』https://s.tencent.com/research/report/902、
啓明星辰集団 (2020). 『網絡安全態勢観察報告（2018～2019）』P.9 から P.10、P.114 から P.118、
360 脅威情報中心 (2020). 『毒雲藤（APT-C-01）組織 2020 上半年針対我重要機構定向攻撃活動揭秘』
https://mp.weixin.qq.com/s?__biz=MzUyMjk4NzExMA==&mid=2247484669&idx=1&sn=c069e077e95af9f7f82969441d6731f7、
360 脅威情報中心 (2020). 『針対毒雲藤（APT-C-01）組織近期的大規模釣魚攻撃活動披露』
https://mp.weixin.qq.com/s?__biz=MzUyMjk4NzExMA==&mid=2247484690&idx=1&sn=aed7dd416e4315df3f1cbf27e746b83e、
360 脅威情報中心 (2021). 『2020 年全球高級持続性威脅（APT）研究報告』P.18 、P.60 から P.69、
奇安信威脅情報中心 (2021). 『全球高級持続性威脅（APT）2020 年報告』P.14 から P.17、P.33 から、
安恒信息威脅情報中心 (2021). 『2020 年度高級威脅態勢研究報告』P.4、P.18、P.21 から P.23、
360 脅威情報中心 (2021). 『2021 年上半期全球高級持続性威脅（APT）研究報告』P.8、P.15 から P.16、P.33 から P.39、P.53、
奇安信威脅情報中心 (2022). 『全球高級持続性威脅（APT）2021 年度報告』P.3 から P.5、P.74、
奇安信威脅情報中心 (2022). 『全球高級持続性威脅（APT）2022 年中報告』P.10 から P.12、
緑盟科技 (2022). 『2021 年度高級威脅研究報告』P.12、P.16 から P.22、
360 脅威情報中心 (2023). 『2022 年全球高級持続性威脅（APT）研究報告』P.31 から P.33、P.63 を参照。

[96] 安天 (2018). 『"緑斑"行動——持続多年的攻撃』https://www.antiy.com/response/20180919.html および 360 脅威情報中心 (2018). 『毒雲藤（APT-C-01）軍政情報刺探者掲露』https://blogs.360.net/post/APT_C_01.html、https://www.ddosi.org/apt/、https://www.secrss.com/articles/5256。

[97] 奇安信威脅情報中心 (2021). 『全球高級持続性威脅（APT）2020 年報告』P.34 を参照。

[98] 文末脚注 95 を参照。

[99] 安全内参に掲載された 360 脅威情報中心による記事『毒云藤（APT-C-01）軍政情報刺探者掲露』。https://www.secrss.com/articles/5256 を参照。

[100] 泉州市人民政府による、「中国製造 2025」パイロット都市実証計画と「泉州製造業 2025 年発展概要」の通知。今後 10 年間（2015-2025）の製造業発展にむけて、同市は中国工程院によりパイロット都市に指定された。

http://www.quanzhou.gov.cn/zfb/xxgk/zfxxgkzl/zfxxgkml/srmzfxxgkml/ghjh/201704/t20170421_439183.htm、
http://www.quanzhou.gov.cn/zfb/xxgk/zfxxgkzl/zfxxgkml/srmzfxxgkml/ghjh/201608/t20160830_361780.htm、
https://kknews.cc/news/43rgeg.html、
https://www.sohu.com/a/198709920_523140。

[101] 『大賽 | 2017 年 福建省"海峡杯"工業設計（泉州）大賽』https://www.sohu.com/a/156487318_282265。

[102] 捜狐に掲載された 360 脅威情報中心による記事『毒云藤（APT-C-01）軍政情報刺探者掲露』。https://www.sohu.com/a/256430502_354899 を参照。

[103] 例えば、2021 年には、交通規制イベント（1 月）、確定申告期（3 月）、労働節期間（5 月）をおとりにして関連当局、個人、シンクタンクを標的にした。2022 年はロシア・ウクライナ関連の話題（2 月～3 月）、確定申告（3 月）、ロケーションコードの導入（4 月）、防災（9 月）がおとりに使用された。360 脅威情報中心 (2021).『2021 年上半期全球高級持続性威脅（APT）研究報告』P.15 から P.16、P.33 から P.39、P.53、および 360 脅威情報中心 (2023).『2022 年全球高級持続性威脅（APT）研究報告』P.31 から P.33、P.63 を参照。

[104] 以下を参照。

騰訊安全大脳 (2019).『全球高級持続性威脅（APT）2019 年上半期研究報告』https://s.tencent.com/research/report/762、
360 脅威情報中心 (2020).『毒雲藤（APT-C-01）組織 2020 上半年針対我重要機構定向攻撃活動揭秘』
https://mp.weixin.qq.com/s?__biz=MzUyMjk4NzExMA==&mid=2247484669&idx=1&sn=c069e077e95af9f7f82969441d6731f7、
360 脅威情報中心 (2020).『針対毒雲藤（APT-C-01）組織近期的大規模釣魚攻撃活動披露』
https://mp.weixin.qq.com/s?__biz=MzUyMjk4NzExMA==&mid=2247484690&idx=1&sn=aed7dd416e4315df3f1cbf27e746b83e、
360 脅威情報中心 (2021).『2020 年全球高級持続性威脅（APT）研究報告』P.18 、P.60 から P.69、
奇安信威脅情報中心 (2021).『全球高級持続性威脅（APT）2020 年報告』P.14 から P.17、P.33 から、
安恒信息威脅情報中心 (2021).『2020 年度高級威脅態勢研究報告』P.4、P.18、P.21 から P.23 を参照。

[105] 360 脅威情報中心 (2023).『2022 年全球高級持続性威脅（APT）研究報告』P.31 から P.33、P.63 を参照。

[106] 在韓国中国大使館は「中国は韓国にとって最大輸出市場かつ最大輸入元であり、韓国は中国にとって世界第三位の貿易相手国である」と説明している。http://kr.china-embassy.gov.cn/chn/zhgx/sbgxx/201007/t20100728_1365476.htm。

[107] 中国政府は韓国に対して「THAAD の配備が朝鮮半島の平和と安定の維持を著しく損ねる」と非難し、中国戦略的安全保障上の利益を損なうような行為を控えるよう強く要請した。これに対して韓国政府は朝鮮半島の安全保障問題という内政への不干渉を要求した。https://cn.nytimes.com/asia-pacific/20160225/c25korea/および http://news.sina.com.cn/w/zx/2016-07-08/doc-ifxtwihp9804497.shtml。

[108] 「限韓令」は韓国企業の中国進出の抑圧や、中国人観光客の訪韓遮断、中国における韓国のエンターテイメントを規制する報復であった。中国の国家広電総局は正式な文書を発行せず、各テレビ局の関係責任者に規制内容を伝えたことを台湾メディアが報じている。江蘇衛星テレビの内部通達と思われるスクリーンショットには、「江蘇テレビ局は即時、韓国芸能人が推薦する CM を放送しない、韓国人が CM に関わっている場合は、直ちに CM を差し替えてください」と書かれた内部通達のスクリーンショットが微博に投稿されたという。

https://www.chinatimes.com/realtimenews/20161119003605-260404?chdtv。

中国共産党機関紙「人民日報」で韓国との国交断絶を「事実上」検討すべきという意見が記載されたことを NY タイムズが報じている。

https://cn.nytimes.com/asia-pacific/20170303/china-north-south-korea/zh-hant/。

中国外交部は THAAD 問題に関して強固な姿勢を貫いた。

http://sg.china-embassy.gov.cn/chn/fyrth/201703/t20170303_1795800.htm、

https://www.fmprc.gov.cn/nanhai/chn/fyrbt/201703/t20170307_8522682.htm。

[109] 中国共産党江蘇省員会が発行する雑誌『群衆』のウェブサイトにおける記事『小国"玩轉"大国的智慧』。

http://www.qunzh.com/qzxlk/jczx/2017/201708/202011/t20201104_82187.html。

[110] 中韓世論はインターネットを中心に主に文化の起源に関する対立を繰り返した。昨今になってキムチや朝鮮半島の民族衣装「ハンボック」は中国の文化であるとする説が中国のインターネットで拡がり、韓国世論は強い嫌悪感を示した。こうした中国の動向について、韓国の専門家は以下の 3 つに大別される動機が目的であると分析している (Gries & Masui, 2022)。

① 古代の朝鮮半島に存在したとされる「高句麗」が古代中国の一国家であるという主張を根拠に、朝鮮半島北部を併合するための長期的策略の一つであること。

② 双方の主張の対立の裏には、「自国」の文化認識に乖離があること。すなわち、朝鮮民族は「中華人民共和国」に住む 55 少数民族の一つであり、よって、その朝鮮民族の文化は「中国の文化」であること。

③ 新疆自治区のウイグル族の問題を抱える中国政府は、朝鮮民族が「中華人民共和国の国民」であるというアイデンティティーを確立させることで、朝鮮族の多い地区における中国共産党の支配を正当化するもの。

一般的に韓国を起源すると認知される物事を「中国起源」と主張する中国世論の傾向は 2004 年頃から確認されている。

https://repo.kinu.or.kr/bitstream/2015.oak/784/1/0000599171.pdf、

http://m.monthly.chosun.com/client/mdaily/daily_view.asp?idx=1710&Newsnumb=2017101710、および

https://thediplomat.com/2021/02/a-korean-poet-is-the-latest-example-of-chinas-cultural-imperialism/。

[111] 立法予告された『国籍法改正案』は、「外国籍の韓国永住者の子供に対して簡易に韓国国籍を取得できるようする」条項を含むものであった。改正案の恩恵の対象者の 95%が中国大陸出身の華僑となることがわかると、韓国では 30 万人以上による国籍法改正案反対請願が大統領府に提出された。韓国の国籍法改正案に対する論議が高まる中、同国の法務部が YouTube でオンライン開催した公聴会はリアルタイム視聴者が 1400 人に達するなど、多くの国民が関心を寄せる様子が見られた。公聴会の 5 人のパネルは全て賛成意見であるのに対し、YouTube チャンネルには数千件にのぼる反対意見が発生し、対照的な雰囲気となった。

https://www.youtube.com/watch?v=pditP9nyH-Q、https://www.ytn.co.kr/_ln/0103_202105281455020085、

https://biz.chosun.com/topics/law_firm/2021/05/26/NXW3NUJ2KRE45MKOQLKUOGROCQ/、および

https://www.edaily.co.kr/news/read?newsId=02168086629086312。

[112] 韓国メディアの「時事 IN」と同国の民間調査専門機関である「韓国リサーチ」が 2021 年に実施した世論調査かは顕著となったのは「日本や北朝鮮より中国が嫌い」という回答で、THAAD 配備局面以降に中国に対する好感度が日本や北朝鮮より低く出たのは初。この傾向は特に 20 代で顕著だった。

https://thediplomat.com/2021/09/anti-china-sentiment-and-south-koreas-presidential-race/、

https://www.sisain.co.kr/news/articleView.html?idxno=44821。

[113] 中国のセキュリティ企業による毒雲藤のまとまった情報については以下を参照。

https://apt.360.net/orgDetail/3、

https://ti.dbappsecurity.com.cn/apt/dc9b0d62-307f-11eb-9593-ac1f6b480078/、

https://ti.qianxin.com/apt/detail/5acb2b01596a100021a3089e?name=Darkhotel&type=map。

Darkhotel の詳述は以下を参照。

啓明星辰集団 (2018). 『2017 網絡安全態勢観察報告』P.91、

360 脅威情報中心 (2018). 『2017 年全球高級持続性威脅（APT）総結報告』P.5、

360 脅威情報中心 (2018).『APT-C-06 組織在全球範囲内首例使用"双殺"0day 漏洞(CVE-2018-8174)発起的 APT 攻撃分析及溯源』https://blogs.360.net/post/cve-2018-8174.html、

騰訊安全大脳 (2018).『DarkHotel（黒店）APT 組織針対東北亜的精確打擊行動』https://s.tencent.com/research/report/552、

騰訊安全大脳 (2019).『疑似 DarkHotelAPT 組織針対中国貿易行業高管的定向攻擊披露』

https://s.tencent.com/research/report/646、

騰訊安全大脳 (2019).『"寄生獣（DarkHotel）"針対中国外貿人士的最新攻擊活動披露』

https://s.tencent.com/research/report/741、

騰訊安全大脳 (2019). 『2018 年高級持続性威脅（APT）研究報告』https://s.tencent.com/research/report/623.html、

騰訊安全大脳 (2019). 『全球高級持続性威脅（APT）2019 年上半期研究報告』https://s.tencent.com/research/report/762、

騰訊安全大脳 (2020). 『全球高級持続性威脅（APT）2019 年研究報告』https://s.tencent.com/research/report/902、

啓明星辰集団 (2020). 『網絡安全態勢観察報告（2018～2019）』P.9 から P.10、P.113 から P.115、

啓明星辰集団 (2021). 『網絡安全態勢観察報告（2020～2021）』P.47、P.49 から P.50、P.57 から P.58、

360 脅威情報中心 (2019). 『2018 年全球高級持続性威脅（APT）総結報告』P.2 から P.5、P.22 から P.26、

360 脅威情報中心 (2021). 『2020 年全球高級持続性威脅（APT）研究報告』P.9、P.12、P.19 から P.21、P.52、P.55、P.60 から P.69、P.72、P.75、P.80、

360 脅威情報中心 (2021). 『2021 年上半期全球高級持続性威脅（APT）研究報告』P.15、P.17、P.49、

360 脅威情報中心 (2023). 『2022 年全球高級持続性威脅（APT）研究報告』P.5、P.30、P.51、

奇安信威脅情報中心 (2020). 『全球高級持続性威脅（APT）2019 年報告』P.8、

奇安信威脅情報中心 (2021). 『全球高級持続性威脅（APT）2020 年報告』P.5 から P.13 から P.17、P.35 から P.38、

奇安信威脅情報中心 (2022). 『全球高級持続性威脅（APT）2021 年度報告』P.4、P.31 から P.36、P.74、

奇安信威脅情報中心 (2022). 『全球高級持続性威脅（APT）2022 年中報告』P.27 から P.29、

安恒信息威脅情報中心 (2021). 『2020 年度高級威脅態勢研究報告』P.4、P.18、P.46、P.48 を参照。

MITRE の Darkhotel に関する脅威情報によると、Darkhotel は少なくとも 2004 年から活動していると説明されている。

https://attack.mitre.org/groups/G0012/。

[114] 360 脅威情報中心 (2021). 『2021 年上半期全球高級持続性威脅（APT）研究報告』P.49 を参照。

[115] 文末脚注 113 を参照。

[116] 緑盟科技 (2020).『APTGroup 系列——Darkhotel 之誘餌投艇递篇』http://blog.nsfocus.net/darkhotel-1-0729/。

[117] 360 脅威情報中心 (2023).『2022 年全球高級持続性威脅（APT）研究報告』P.5。

[118] 騰訊安全大脳 (2019).『疑似 DarkHotelAPT 組織針対中国貿易行業高管的定向攻撃披露』https://s.tencent.com/research/report/646 を参照。

[119] 360 脅威情報中心 (2018).『APT-C-06 組織在全球範囲内首例使用"双殺"0day 漏洞(CVE-2018-8174)発起的 APT 攻撃分析及溯源』https://blogs.360.net/post/cve-2018-8174.html。また https://japan.zdnet.com/article/35118905/および https://nvd.nist.gov/vuln/detail/CVE-2018-8174 も参照。

[120] 騰訊安全大脳 (2019).『"寄生獣（DarkHotel）"針対中国外貿人士的最新攻撃活動披露』https://s.tencent.com/research/report/741 を参照。

[121] 360 脅威情報中心 (2021).『2020 年全球高級持続性威脅（APT）研究報告』P.9、P.12、P.19 から P.21、P.52、P.55、P.60 から P.69、P.72、P.75、P.80。また、https://nvd.nist.gov/vuln/detail/CVE-2020-0674 および https://nvd.nist.gov/vuln/detail/CVE-2019-17026 も参照。

[122] 360 脅威情報中心 (2021).『2020 年全球高級持続性威脅（APT）研究報告』P.19、奇安信威脅情報中心 (2021).『全球高級持続性威脅（APT）2020 年報告』P.5 から P.13 から P.17、P.35 から P.38、また https://www.anquanke.com/post/id/202526 および https://www.zdnet.com/article/darkhotel-hackers-use-vpn-zero-day-to-compromise-chinese-government-agencies/も参照。

[123] 360 脅威情報中心 (2021).『2020 年全球高級持続性威脅（APT）研究報告』P.75 を参照。

[124] 啓明星辰集団 (2021).『網絡安全態勢観察報告（2020～2021）』P.50 を参照。

[125] 2021 年 4 月に発生した水飲み場型攻撃では、スクリプトエンジンに存在するメモリ破損の脆弱性のゼロデイ脆弱性（CVE-2021-344486）が悪用された。Darkhotel が細工した悪意あるスクリプトは、セキュリティ検知や標的の対象者以外がトリガーすることで攻撃が露見するのを避けるために、水飲み場型攻撃の際に複数の検証を行って、本当の標的をフィルタリングした上で最終的にスクリプトが実行されるように細工がなされていたことを 360 が報告した。360 脅威情報中心 (2021).『2021 年上半期全球高級持続性威脅（APT）研究報告』P.17 および https://nvd.nist.gov/vuln/detail/CVE-2021-34448 を参照。
2022 年 2 月の攻撃では、Firefox ブラウザのゼロデイ脆弱性（CVE-2022-26485、CVE-2022-26486）を利用した特定のターゲットに対する水飲み場型攻撃が観測された。360 脅威情報中心 (2023).『2022 年全球高級持続性威脅（APT）研究報告』P.5 および https://nvd.nist.gov/vuln/detail/CVE-2022-26485 および https://nvd.nist.gov/vuln/detail/CVE-2022-26486 を参照。

[126] 奇安信威脅情報中心 (2022).『全球高級持続性威脅（APT）2022 年中報告』P.27 から P.29 および https://www.trellix.com/en-us/about/newsroom/stories/research/suspected-darkhotel-apt-activity-update.html を参照。

[127] 米中経済安全保障再検討委員会による『2016 年次報告書』は、国家安全保障に関する情報から機微な経済情報、知的財産に至るまで、幅広く米国の利益を搾取し続けていることを議会に報告した。https://www.uscc.gov/annual-report/2016-annual-report-congress。

[128] https://trumpwhitehouse.archives.gov/articles/new-national-security-strategy-new-era/および https://www.defense.gov/News/Feature-Stories/Story/Article/1656414/what-is-the-national-defense-strategy/。

[129] 2018 年 1 月から 2 月にかけて米海軍の契約業者が中国政府を背景に持つとされる攻撃者によるハッキングを受け、潜水艦搭載の超音速対艦ミサイルに関する極秘情報が流出したとされる。同年 3 月に
アメリカ合衆国国家情報長官（DNI）は、ネットワーク化された部隊の妨害やインフラの破壊などのために中国軍がサイバー攻撃能力を強化していることを指摘した。

https://www.intelligence.gov/annual-threat-assessment。

[130] 米国ホワイトハウスは『5G の安全のための米国家戦略』、国防総省は『DoD 5G 戦略』を公表した。商務省は中国の華為（Huawei）に対する規制を強化した。

https://trumpwhitehouse.archives.gov/wp-content/uploads/2020/03/National-Strategy-5G-Final.pdf、
https://www.cto.mil/wp-content/uploads/2020/05/DoD_5G_Strategy_May_2020.pdf、
https://2017-2021.commerce.gov/news/press-releases/2020/08/commerce-department-further-restricts-huawei-access-us-technology-and.html。

[131] https://media.defense.gov/2020/Jul/17/2002459291/-1/-1/1/NDS-FIRST-YEAR-ACCOMPLISHMENTS-FINAL.pdf。

[132] https://www.whitehouse.gov/wp-content/uploads/2021/03/NSC-1v2.pdf および https://www.whitehouse.gov/briefing-room/statements-releases/2021/03/03/interim-national-security-strategic-guidance/。

[133] 2021 年 3 月に発生したマイクロソフト社メールサーバソフトウェアの脆弱性を狙ったサイバー攻撃について、米国ホワイトハウスは中国国家安全部（MSS）に関連する主体により実施されたものであるとして中国を非難した。

https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/19/the-united-states-joined-by-allies-and-partners-attributes-malicious-cyber-activity-and-irresponsible-state-behavior-to-the-peoples-republic-of-china/、
https://www.whitehouse.gov/briefing-room/press-briefings/2021/07/19/background-press-call-by-senior-administration-officials-on-malicious-cyber-activity-attributable-to-the-peoples-republic-of-china/。

米国国家サイバー長官は 2021 年 1 月 1 日に発効した 2021 会計年度の国防権限法に基づき創設された。

https://www.whitehouse.gov/oncd/、
https://www.hsgac.senate.gov/media/majority-media/peters-bipartisan-legislation-to-ensure-national-cyber-director-can-secure-personnel-to-help-bolster-cybersecurity-passes-senate/。

[134] https://www.whitehouse.gov/briefing-room/statements-releases/2023/03/02/fact-sheet-biden-harris-administration-announces-national-cybersecurity-strategy/および https://www.state.gov/announcing-the-release-of-the-administrations-national-cybersecurity-strategy/。

[135] 調査は米国の成人 1,897 人に対して中国に対する見方を尋ねたもので、無党派とされる米国のシンクタンク「Pew Research Center」が 2020 年 3 月および 2022 年 3 月に実施した。各調査は同一人物にインタビューを行っており、2020 年から 2022 年にかけての米国人の中国に対する態度や意見の変化を時系列で追跡することができる。

https://www.pewresearch.org/fact-tank/2022/09/28/some-americans-views-of-china-turned-more-negative-after-2020-but-others-became-more-positive/。

[136] 中国のセキュリティ企業による Longhorn の情報については以下を参照。

https://apt.360.net/orgDetail/12、

https://ti.dbappsecurity.com.cn/apt/dc8322ae-307f-11eb-9593-ac1f6b480078/、
https://ti.qianxin.com/apt/detail/5b8ca52d596a1000217094e0?name=Longhorn&type=map。
詳述は以下も参照。
360 脅威情報中心 (2018).『2017 年全球高級持続性威脅（APT）総結報告』主要観点、摘要、P.19 から P.21、P.30、
啓明星辰集団 (2018).『2017 網絡安全態勢観察報告』P.2 から P.3、
奇安信威脅情報中心 (2019).『全球高級持続性威脅（APT）2019 年中報告』P.18 から P.19、
奇安信威脅情報中心 (2020).『全球高級持続性威脅（APT）2019 年報告』P.19 から P.20、P.24、
奇安信威脅情報中心 (2021).『全球高級持続性威脅（APT）2020 年度報告』P.42 から P.43、
奇安信威脅情報中心 (2022).『全球高級持続性威脅（APT）2022 年中報告』P.26、
360 脅威情報中心 (2023).『2022 年全球高級持続性威脅（APT）研究報告』P.7、
騰訊安全大脳 (2020).『全球高級持続性威脅（APT）2019 年研究報告』https://s.tencent.com/research/report/902、
Longhorn（APT-C-39）および方程式（APT-C-40）に関する情報は、中国政府の外交部や中国共産党のメディアからも非常に批判色の強いステイトメントが発表されている。
http://news.cctv.com/2020/03/04/ARTIyf5G4nbdU3zLTYLezyIQ200304.shtml および http://www.xinhuanet.com/world/2020-03/03/c_1210499250.htm。

[137] 奇安信威脅情報中心 (2019).『美国中央情報局網絡武器庫分析与披露』は、公開報告と奇安信の内部脅威情報データに基づき攻撃チェーンの復元を試みた結果がまとめられている。
https://ti.qianxin.com/blog/articles/network-weapons-of-cia/および https://www.secrss.com/articles/14074、
360 脅威情報中心 (2020).『披露美国中央情報局 CIA 組織対中国関鍵領域長達十一年的網絡渗透攻撃』は、サイバー兵器「Vault7（中国語で「穹窿 7」）」のリークにより発覚したバックドア「Fluxwire」が、2010 年初頭の中国への攻撃に既に使用されていると指摘している。
https://apt.360.net/report/apts/96.html、https://www.360.cn/n/11563.html および https://bbs.360.cn/thread-15847087-1-1.html。英語記事については https://www.forbes.com/sites/zakdoffman/2020/03/03/new-chinese-cyber-report-just-accused-cia-of-11-year-attack-this-is-whats-behind-the-report/?sh=5339a19157e6 も参照。

[138] 奇安信威脅情報中心 (2019).『全球高級持続性威脅（APT）2019 年中報告』P.18 から P.19 を参照。奇安信はまた、Lambert が使用するサイバー兵器は一から構築され、ターゲットや攻撃戦略に応じてカスタマイズされていると分析した。奇安信威脅情報中心 (2020).『全球高級持続性威脅（APT）2019 年報告』P.20 も参照。

[139] https://ti.qianxin.com/apt/detail/5b8ca52d596a1000217094e0?name=Longhorn&type=map。

[140] 奇安信威脅情報中心 (2019).『全球高級持続性威脅（APT）2019 年中報告』P.18 から P.19 を参照。奇安信はまた、Lambert が使用するサイバー兵器は一から構築され、ターゲットや攻撃戦略に応じてカスタマイズされていると分析した。奇安信威脅情報中心 (2020).『全球高級持続性威脅（APT）2019 年報告』P.20 も参照。

[141] 航空情報技術関連サービス（中国国内外の民間航空会社向けにフライト制御をするシステム、貨物情報、決済サービス、空港の旅客ハンドリングシステム、および関連データや拡張サービス）のシステム開発企業や開発者を攻撃した。

[142] 360 によると、中国国内の航空宇宙分野の企業だけでなく、中国国外の民間航空会社 100 社も「APT-C-39（Longhorn）」の攻撃対象と公表された。中国外交部は 2020 年 03 月 04 日の会見では、中国の重要分野の組織に対する攻撃が 11 年にわたり発生しており、これが「CIA の攻撃グループ APT-C-39（Longhorn）」によるものであるとして米国の関与と責任を非難した。
2020 年 3 月 4 日の外交部による『披露美国中央情報局 CIA 攻撃組織（Apt-c-39）対中国関鍵領域長達十一年的網絡滲透攻撃』
http://www.xinhuanet.com/world/2020-03/03/c_1210499250.htm、https://www.360.cn/n/11563.html、
または https://zhuanlan.zhihu.com/p/130272230 および、http://news.cctv.com/2020/03/04/ARTIyf5G4nbdU3zLTYLezyIQ200304.shtml。

[143] 中国のセキュリティ企業による方程式の情報については以下を参照。

https://apt.360.net/orgDetail/85、
https://ti.dbappsecurity.com.cn/apt/dcb07973-307f-11eb-9593-ac1f6b480078/、
https://ti.qianxin.com/apt/detail/5b399d42596a10000ffcba7a?name=%E6%96%B9%E7%A8%8B%E5%BC%8F&type=map。
詳述は以下も参照。
安天 (2015).『方程式（EQUATION）部分組件中的加密技巧分析』
https://www.antiy.com/response/Equation_part_of_the_component_analysis_of_cryptographic_techniques.html
安天 (2016).『2015 網絡安全威脅的回顧与展望』P.2 から P.4、
および https://www.antiy.cn/research/notice&report/research_report/2015_annualReport.html、
安天 (2015).『修改硬盤固件的木馬探索方程式（EQUATION）組織的攻撃組件』
https://www.antiy.com/response/EQUATION_ANTIY_REPORT.html、
安天 (2016).『従方程式到方程組』https://www.antiy.com/response/EQUATIONS/EQUATIONS.html、
安天 (2017).『方程式組織 EQUATION DRUG 平台解析』https://www.antiy.com/response9.html、
安天 (2017).『2016 網絡安全威脅的回顧与展望』P.4、P.10 から P.12、
安天 (2018).『2017 網絡安全威脅的回顧与展望』
https://www.antiy.cn/research/notice&report/research_report/20180707.html、
360 脅威情報中心 (2017).『2016 年全球高級持続性威脅（APT）総結報告』P.25 から P.29、
啓明星辰集団 (2018).『2017 網絡安全態勢観察報告』前言、P.2 から P.3、
360 脅威情報中心 (2018).『2017 年全球高級持続性威脅（APT）総結報告』主要観点、摘要、P.19 から P.21、P.30、
奇安信威脅情報中心 (2019).『全球高級持続性威脅（APT）2019 年中報告』P.4、P.18 から P.19、
奇安信威脅情報中心 (2020).『全球高級持続性威脅（APT）2019 年報告』P.19 から P.20、P.22 から P.24、
騰訊安全大脳 (2019).『全球高級持続性威脅（APT）2019 年上半期研究報告』https://s.tencent.com/research/report/762、
騰訊安全大脳 (2020).『全球高級持続性威脅（APT）2019 年研究報告』https://s.tencent.com/research/report/902、
奇安信威脅情報中心 (2021).『全球高級持続性威脅（APT）2020 年度報告』P.35、P.42 から P.43、
奇安信威脅情報中心 (2022).『全球高級持続性威脅（APT）2022 年中報告』P.26、
啓明星辰集団 (2022).『網絡安全態勢観察報告（2020～2021）』P.9、
360 数字安全 (2022).『網絡終戦序幕：美国国安局 NSA（APT-C-40）対全球発起長達十余年無差別攻撃』
https://www.anquanke.com/post/id/268964、
360 数字安全 (2022).『Quantum（量子）攻撃系統—美国国家安全局"APT-C-40"黒客組織高端網絡攻撃武器技術分析報告（一）』https://mp.weixin.qq.com/s/27sVSUNA3aVkUDAigM3Jbg、
国家計算機病毒応急処理中心 (2022).『美国国家安全局（NSA）"酸狐狸"漏洞攻撃武器平台技術分析報告』
https://www.cverc.org.cn/head/zhaiyao/news20220629-FoxAcid.htm および https://www.cverc.org.cn/、

360 数字安全 (2022).『"験証器"（Validator）—美国国家安全局 NSA（APT-C-40）的木馬尖兵』
https://www.anquanke.com/post/id/275517、
緑盟科技 (2022).『2021 年度高級威脅研究報告』P.12、P.16 から P.22、
緑盟科技 (2022).『APT 組織情報研究年鑑』P.155、
360 脅威情報中心 (2023).『2022 年全球高級持続性威脅（APT）研究報告』P.16、P.19、
2015 年にカスペルスキーによって公開・命名された集団で、サイバー攻撃に強力な暗号化手法や難読化戦術を好むことに由来している。MITRE の情報には NSA の関連性については記載されていない。
https://attack.mitre.org/groups/G0020/。

[144] 方程式（APT-C-40）および Longhorn（APT-C-39）に関する情報は、中国政府の外交部や中国共産党のメディアからも非常に批判色の強いステイトメントが発表されている。
2020 年 3 月 4 日の外交部による『披露美国中央情報局 CIA 攻撃組織（Apt-c-39）対中国関鍵領域長達十一年的網絡滲透攻撃』
http://www.xinhuanet.com/world/2020-03/03/c_1210499250.htm、https://www.360.cn/n/11563.html、
または https://zhuanlan.zhihu.com/p/130272230 および、http://news.cctv.com/2020/03/04/ARTIyf5G4nbdU3zLTYLezyIQ200304.shtml、
2022 年 3 月 3 日の外交部による『外交部：強烈要求美国停止針対中国和全球的網絡窃密和攻撃』
https://www.fmprc.gov.cn/wjb_673085/zzjg_673183/jks_674633/jksxwlb_674635/202203/t20220315_10651921.shtml または
https://www.thepaper.cn/newsDetail_forward_16938094 および
https://news.cctv.com/2022/03/03/ARTIvJxZWBh4ftn2Xl8E9XdD220303.shtml。また、http://us.china-embassy.gov.cn/eng/fyrth/202203/t20220303_10647695.htm も参照。

[145] 2016 年に ShadowBrokers（中国では影子経紀人と記される）と名乗るハッキング集団が NSA のハッキングツールに関して情報をリークした。360 脅威情報中心 (2017).『2016 年全球高級持続性威脅（APT）総結報告』P.25 から P.29 および啓明星辰集団 (2018).『2017 網絡安全態勢観察報告』前言、P.2 から P.3、奇安信威脅情報中心 (2019).『全球高級持続性威脅（APT）2019 年中報告』P.4、P.18 から P.19 を参照。また、2017 年にウィキリークスが公開した CIA 機密文書からは、NSA が CIA のハッキングツール開発を支援しているという情報が流出した。
https://arstechnica.com/information-technology/2016/08/code-dumped-online-came-from-omnipotent-nsa-tied-hacking-group/、
https://arstechnica.com/information-technology/2016/08/group-claims-to-hack-nsa-tied-hackers-posts-exploits-as-proof/、および
https://www.washingtonpost.com/world/national-security/powerful-nsa-hacking-tools-have-been-revealed-online/2016/08/16/bce4f974-63c7-11e6-96c0-37533479f3f5_story.html。
なお、2013 年にも NSA の機密文書「NSA ANT カタログ」が流出した。作成は 2008 年ごろと推定されており、ハッキング技術・プログラムに関する幅広い記載が公開された。
https://www.eff.org/files/2014/01/06/20131230-appelbaum-nsa_ant_catalog.pdf。

[146] 奇安信威脅情報中心 (2019).『全球高級持続性威脅（APT）2019 年中報告』P.4、P.18 から P.19、騰訊安全大脳 (2019).『全球高級持続性威脅（APT）2019 年上半期研究報告』https://s.tencent.com/research/report/762、および騰訊安全大脳 (2020).『全球高級持続性威脅（APT）2019 年研究報告』https://s.tencent.com/research/report/902 を参照。奇安信は、「Defend forward のもとに米国は中国をサイバー諜報活動の重要ターゲットにしている」と警告した。

[147] 安天 (2017).『方程式組織 EQUATION DRUG 平台解析』https://www.antiy.com/response/EQUATION_DRUG/EQUATION_DRUG.html を参照。

[148] 同上。清華大学、国防技術大学、北京郵電大学、北京科技工業大学、西安電子科技大学、鄭州大学、蘭州大学などの大学のドメイン、中国原子力研究院、西北核技術研究所、杭州市経済情報化委員会、中国科学院紫山天文台などの科学機関や、華為などの商業企業のドメインが登場したと 360 は指摘した。360 脅威情報中心 (2017).『2016 年全球高級持続性威脅（APT）総結報告』P.25 から P.29 および 360 脅威情報中心 (2018).『2017 年全球高級持続性威脅（APT）総結報告』主要観点、摘要、P.19 を参照。

[149] 360 脅威情報中心 (2017).『2016 年全球高級持続性威脅（APT）総結報告』P.25 から P.29 を参照。Longhorn に関しては文末脚注 135 を参照。また、360 は 2017 年の「トランプ政権下（当時）の軍事予算増額方針により中国に対するサイバー兵器開発者の増加に繋がり得る」という警戒感を示した。360 脅威情報中心 (2018).『2017 年全球高級持続性威脅（APT）総結報告』主要観点、摘要、P.19 から P.21 を参照。テンセントは、Longhorn や方程式といった北米（およびロシアの Turla）の APT グループは IoT 機器や衛星通信を乗っ取るケースも多く、その技術力は他の組織を凌駕すると評価した。騰訊安全大脳 (2019).『全球高級持続性威脅（APT）2019 年上半期研究報告』https://s.tencent.com/research/report/762 および騰訊安全大脳 (2020).『全球高級持続性威脅（APT）2019 年研究報告』https://s.tencent.com/research/report/902。

[150] https://apt.360.net/orgDetail/85、https://www.anquanke.com/post/id/268964。

[151] 文末脚注 144 を参照。

[152] 文末脚注 143 を参照。

[153] 文末脚注 143 を参照。

[154] 奇安信威脅情報中心 (2019).『全球高級持続性威脅（APT）2019 年中報告』P.22 から P.23 を参照。ここでは「北米のセキュリティベンダーによる、中国を彷彿とさせる命名傾向」や、「北米のセキュリティベンダーが APT グループを中国とイランに帰属させる傾向」に対する奇安信の批判姿勢を確認することができる。奇安信の批判は APT10（menuPass）の関与を結論付ける中国国外のセキュリティ研究者とメディアにも及んだ。

以下へは、奇安信側の主張を記述する：

> 「中国国外のセキュリティベンダーは世界の通信事業者や携帯電話ネットワークを標的とした *APT* 作戦の攻撃元を中国との関連が疑われる *APT* グループに帰属させた。そして、こうしたセキュリティベンダーに追従するメディアとセキュリティ研究者たちは、『攻撃は中国の *APT10* によるものである』と結論付けることを好んでいる。その根拠は *China Chopper Webshell* や *Poison Ivy RAT* またはその亜種の使用、制御インフラの地理（中国国内）であるが、中国は歴史的に前述の両ツールを利用した *APT* 活動の主要犠牲者の一つである。そもそも、昨今の攻撃キャンペーンでは、*APT* グループが積極的に偽旗を導入し、他の攻撃グループの戦術やテクニックを模倣して攻撃の帰属先を隠ぺいすることが重視されている。」

北米のセキュリティ研究組織による APT10（menuPass）の説明については下記を参照。

https://attack.mitre.org/groups/G0045/、
https://unit42.paloaltonetworks.jp/unit42-menupass-returns-new-malware-new-attacks-japanese-academics-organizations/。

2018 年時点において各 APT グループが中国を攻撃する際に使用する代表的な攻撃ツールは啓明星辰集団 (2020).『網絡安全態勢観察報告（2018～2019）』P.118 を参照。

[155] 奇安信威脅情報中心 (2021).『全球高級持続性威脅（APT）2020 年報告』P.73 を参照。

[156] 360 数字安全 (2022).『網絡終戦序幕：美国国安局 NSA（APT-C-40）対全球発起長達十余年無差別攻撃』https://www.anquanke.com/post/id/268964 および 360 数字安全 (2022).『Quantum（量子）攻撃系統―美国国家安全局"APT-C-40"黒客組織高端網絡攻撃武器技術分析報告（一）』https://mp.weixin.qq.com/s/27sVSUNA3aVkUDAigM3Jbg。

[157] 360 が報じた内容によると「量子攻撃は、米国家安全保障局（NSA）が設計した、ネットワークトラフィックをハイジャック攻撃する高度な手法で、主に国家規模のネットワーク通信をターゲットに中間ハイジャックを行い、脆弱性搾取、通信操作、情報窃取といったネットワーク攻撃を実施することができる」ほか、「世界中の任意の場所の任意のインターネットユーザの通常のウェブ閲覧トラフィックを乗っ取り、ゼロデイ攻撃やバックドアプログラムをリモートで埋め込むことができる」と述べた。https://www.360kuai.com/pc/9bb4fe16fadee266c?cota=3&kuai_so=1&sign=360_57c3bbd1&refer_scene=so_1。

[158] 最新の攻撃技術が中国のほかにはロシア、パキスタン、イランに使用されたことが確認できたと 360 は述べた。範囲は多岐にわたる（政府・外交機関、通信、航空宇宙、エネルギー、原子力研究、石油・ガス、軍事、ナノテクノロジー、宗教活動家・学術関係者、マスメディア、運輸、金融機関、暗号開発企業など）。また、「QUANTUMINSERT（量子注入）」攻撃の痕跡が多数発見されたと報告されている。https://www.360kuai.com/pc/9bb4fe16fadee266c?cota=3&kuai_so=1&sign=360_57c3bbd1&refer_scene=so_1。

[159] https://www.guancha.cn/politics/2022_06_22_645884.shtml。

[160] 解析の結果、同大学へのサイバー攻撃を行ったのは、米国国家安全保障局（NSA）の情報諜報部門（コードネーム S）データ偵察部門（コードネーム S3）下に属する TAO（コードネーム S32）であると判断された。

http://www.news.cn/politics/2022-09/05/c_1128976997.htm、
https://news.cctv.com/2022/09/27/ARTI1YjUCAzciKAsNQsy1Rxd220927.shtml、https://bbs.360.cn/thread-16059907-1-1.html、
https://bbs.360.cn/thread-16063273-1-1.html、および https://www.anquanke.com/post/id/279496。
また、https://www.cverc.org.cn/head/zhaiyao/news20220905-NPU.htm および
https://www.cverc.org.cn/head/zhaiyao/news20220927-NPU2.htm も参照。
西北工業大学への攻撃に関する中国国家計算機病毒応急処理中心の特設ページは以下を参照。https://www.cverc.org.cn/。
なお、西北工業大学への攻撃の追加調査には、国家計算機病毒応急処理中心と共に 360 公司連合組成技術団体が共同調査に当たった。

[161] https://www.cverc.org.cn/head/zhaiyao/news20220905-NPU.htm および https://www.cverc.org.cn/head/zhaiyao/news20220927-NPU2.htm を参照。また、以下も参照 https://www.cverc.org.cn/。

[162] 西北工業大学への攻撃で使用したバックドアツールだけでも 14 種類にのぼるという。以下の表は西北工業大学への攻撃作戦で TAO が使用したツール。

	用途	役割	特定・命名された武器名
1	脆弱性攻撃・突破	ネットワークに侵入、中国国外の踏み台を制御、匿名ネットワークを構築する。	"剃須刀"、"孤島"、"酸狐狸"武器プラットフォーム
2	持続化・制御用	暗号化されたチャンネルを通じて制御コマンドを送信してツールを操作し、ネットワークに潜入、制御、機密の窃取を可能にする。	"二次約会"、"NOPEN"（12 種類）、"怒火噴射"、"狡詐異端犯"、"堅忍外科医生"

3	盗聴・窃取	ネットワークの運用・保守に使用するアカウントパスワードやコマンドライン操作を盗聴し、NWIT ネットワーク内の機密情報や運用・保守データを盗み出す。	“飲茶”、“敵後行動”シリーズ
4	隠蔽・証拠隠滅	痕跡の消滅、隠蔽・偽装。	“吐司面包”など

[163] https://bbs.360.cn/thread-16059907-1-1.html および https://bbs.360.cn/thread-16063273-1-1.html。

[164] https://bbs.360.cn/thread-16059907-1-1.html、https://bbs.360.cn/thread-16063273-1-1.html、https://www.cverc.org.cn/head/zhaiyao/news20220905-NPU.htm および https://www.cverc.org.cn/head/zhaiyao/news20220927-NPU2.htm。

[165] https://www.cverc.org.cn/head/zhaiyao/news20220927-NPU2.htm。

[166] 2022 年を通して多数のメディアが NSA および方程式「APT-C-40」と西北工業大学の事件を報道した。その中には政府系メディアも含まれる。

https://tv.cctv.com/2022/09/06/VIDEXZax98XVDbNxO0g6oVFU220906.shtml、
https://news.cctv.com/2022/09/06/ARTIM3saYIazLzRMR9rsKNKB220906.shtml、
https://news.cctv.com/2022/09/27/ARTI1YjUCAzciKAsNQsy1Rxd220927.shtml、
http://www.news.cn/world/2022-09/05/c_1128978360.htm。

[167] 2022 年 9 月 5 日『外交部発言人毛寧主持例行記者』https://www.mfa.gov.cn/web/wjdt_674879/fyrbt_674889/202209/t20220905_10762291.shtml、または http://www.news.cn/world/2022-09/05/c_1128978360.htm、https://www.guancha.cn/politics/2022_09_06_656766.shtml。

4. 結語

[168] 360 脅威情報中心 (2023).『2022 年全球高級持続性威脅（APT）研究報告』P.35 を参照。

[169] ベトナムは他国による南シナ海の海洋侵略に備えて海洋を優先的な防衛対象とすること、海洋経済の持続的発展が 2030～2045 年のベトナムの経済発展にとって中核的な使命であること、自国の防衛能力の構築と軍事能力の開発を望んでいると米国当局は分析した。米国 RAND 研究所は、ベトナムの『2019 年国防白書』において「南シナ海で中国による悪行が続く場合に、ベトナムは米国と防衛関係を強化していく」可能性があることを述べた。

https://media.defense.gov/2021/Dec/12/2002907686/-1/-1/1/JIPA%20-%20BURGESS%20-%20WINTER%202021.PDF、
https://www.trade.gov/country-commercial-guides/vietnam-defense-and-security-sector、
https://www.rand.org/blog/2019/12/how-to-read-vietnams-latest-defense-white-paper-a-message.html、
https://defense.info/re-shaping-defense-security/2019/12/vietnams-new-defense-whitepaper/、
http://mod.gov.vn/home。

2017 年ドクラムにおける中国人民解放軍との対峙、2020 年ラダックにおける中国人民解放軍との衝突による死者発生を経験したインドは、実行支配線における安定性と優位性の確保に主眼を置いていくことを明言した。また、曖昧化する物理的国境における軍事的不測事態に備えるためにサイバー、宇宙、情報領域で新たな脅威に対処する能力を構築すると明記した。一方、バイデン政権下の米国は、インドの規模・立地・人材・世界において果たす役割に注目し、米国の目指す安全保障を達成するために二カ国のパートナーシップ強化を目指すと明記している。

https://pib.gov.in/PressReleasePage.aspx?PRID=1884353、
https://www.state.gov/u-s-security-cooperation-with-india/、
https://www.state.gov/wp-content/uploads/2022/07/ICS_SCA_India_Public.pdf。

台湾の『2021 年国防白書』には、米中間の戦略的競争と中国の影響力行使が地域の安全保障情勢に多大な影響を与えていること、国人民解放軍による戦闘訓練と演習、台湾へのサイバー攻撃や威嚇行動が台湾海峡の重大な脅威であることが明記されている。豊富なサイバーディフェンス実務経験者を擁する台湾にとって、情報の安全は課題でありながらも機会でもあるとし、情報・電子・サイバー戦を含む能力構築を強化すると述べた。

https://www.ustaiwandefense.com/taiwan-ministry-of-national-defense-reports/。

[170] 韓国の『2018 年国防白書』および『2020 年国防白書』には中国との戦略的疎通の強化が明記されている。
https://www.mnd.go.kr/cop/pblictn/selectPublicationUser.do?siteId=mnd&componentId=14&categoryId=0&publicationSeq=835&pageIndex=3&id=mnd_020704000000、
https://www.mnd.go.kr/cop/pblictn/selectPublicationUser.do?siteId=mnd&componentId=14&categoryId=0&publicationSeq=897&pageIndex=2&id=mnd_020704000000。

[171] https://laichau.gov.vn/tin-tuc-su-kien/chuyen-de/tin-trong-nuoc/dong-chi-vo-van-thuong-duoc-bau-lam-chu-tich-nuoc.html および https://www3.nhk.or.jp/news/html/20230302/k10013996081000.html を参照。

[172] https://www3.nhk.or.jp/news/special/international_news_navi/articles/qa/2023/02/09/29192.html を参照。

[173] 外務省によるベトナム社会主義共和国基礎データ。https://www.mofa.go.jp/mofaj/area/vietnam/data.html#section1。

[174] https://www.mofa.go.jp/mofaj/area/korea/index.html および https://www.mofa.go.jp/mofaj/area/taiwan/index.html。

[175] https://www.stat.go.jp/data/sekai/pdf/2022al.pdf。

[176] 外務省の基礎データおよび World Data Bank により公開されているデータを参考にした。https://data.worldbank.org/?locations=CN-VN-JP-US-KR-IN、https://www.mofa.go.jp/mofaj/area/korea/index.html、https://www.mofa.go.jp/mofaj/area/taiwan/index.html。

[177] 奇安信威脅情報中心 (2021).『全球高級持続性威脅（APT）2020 年報告』P.34、奇安信威脅情報中心 (2022).『全球高級持続性威脅（APT）2021 年度報告』P.4、緑盟科技 (2023).『2022 年度高級威脅研究報告』P.20、360 脅威情報中心 (2023).『2022 年全球高級持続性威脅（APT）研究報告』P.66 を参照。

[178] 国際電気通信連合（ITU）による『2020 年版グローバルサイバーセキュリティ指数（GCI）』において、ベトナムは 194 カ国中 25 位の評価を得た。ASEAN 地域ではシンガポール、マレーシア、インドネシアに次ぐ 4 位であった。ベトナムは全 100 点満点中 94.59 点の総合スコアを獲得し、法的措置（20/20）、協力的措置（20/20）、技術的措置（16.31/20）、組織的措置（18.98/20）、能力開発（19.26/20）の評価を記録した。なお、2020 年版では、韓国は 4 位、日本は 7 位、インドは 10 位を記録した。
https://english.mic.gov.vn/Pages/TinTuc/147807/Vietnam-jumps-25-places-to-25th-in-ITU-s-Global-Cybersecurity-Index.html、
https://english.mic.gov.vn/Pages/TinTuc/tinchitiet.aspx?tintucid=139478。

[179] Harvard Kennedy School Belfer Center が 2020 年および 2022 年に発表した『National Cyber Power Index』において、ベトナムのサイバー能力は 20 位（2020 年）から 8 位（2022 年）に上昇した。日本は 9 位から 16 位に転落した。
https://www.belfercenter.org/publication/national-cyber-power-index-2020、

https://www.belfercenter.org/publication/national-cyber-power-index-2022。

英国の国際戦略研究所（IISS）による『Cyber Capabilities and National Power 2021』の評価では、ベトナムとインドは日本と同じ「Tier 3（いくつかのカテゴリーに強みまたは潜在的な強みを持つが、その他のカテゴリーに大きな弱点を持つ国）」として評価された。中国は「Tier2（いくつかのカテゴリーにおいて世界トップクラスの強さを持つ国）」として評価された。なお「Tier1（全項目において世界トップクラスの強さを誇る国）」の評価を得たのは米国のみであった。https://www.iiss.org/blogs/research-paper/2021/06/cyber-capabilities-national-power。

[180] JCIC コラム『ハーバード大ベルファー・センターによる国別サイバー能力ランキングの正しい読み方』https://www.j-cic.com/column/Cyber-Power-Index-2022.html を参照。

[181] https://english.mic.gov.vn/Pages/home.aspx、https://english.mic.gov.vn/Pages/TinTuc/155338/200-chuyen-gia-cong-nghe-ngan-hang-tham-gia-dien-tap-phong-thu-he-thong-truoc-tan-cong-mang.html、および https://ncsc.gov.vn/。

[182] 過去には JICA による「サイバーセキュリティに関する能力向上プロジェクト（2019 年 6 月 26 日～2021 年 11 月 25 日）」、NTT 東日本による「APT 国際共同研究のプログラム（2016 年 5 月～11 月および 2018 年 4 月～2019 年 3 月）、JPCERT/CC による「CSIRT 研修（2021 年 6 月）」などが実施されたほか、2022 年 9 月にはベトナム情報通信省（MIC）傘下の NCSC と日系企業が協力覚書を締結したほか、ハノイ市工科大学、ハノイ国家大学、自然科学大学、ベトナム国家大学、ダナン大学、ホーチミン市自然科学大学などベトナムの 8 大学と提携している。https://hybrid-technologies.co.jp/20220914_01/、https://www.jica.go.jp/project/vietnam/052/outline/index.html、https://www.jica.go.jp/project/vietnam/052/news/20210618.html、および https://journal.ntt.co.jp/article/1130。

[183] ベトナム情報通信省（MIC）によって発表された『サイバーセキュリティ戦略 2025-2030』に関する決定と通知。https://www.mic.gov.vn/mic_2020/Pages/TinTuc/154587/Xay-dung-he-thong-the-tran-an-ninh-nhan-dan-tren-khong-gian-mang.html、https://thuvienphapluat.vn/van-ban/Cong-nghe-thong-tin/Quyet-dinh-964-QD-TTg-2022-phe-duyet-Chien-luoc-An-toan-An-ninh-mang-quoc-gia-den-2025-525540.aspx。

[184] ベトナム情報通信省（MIC）は 2022 年 9 月 5 日の記事で、ベトナムのセキュリティ人材の需要が約 70 万人であると発表した。https://english.mic.gov.vn/Pages/TinTuc/tinchitiet.aspx?tintucid=154972。

[185] https://www.mod.go.jp/j/policy/agenda/kihon02.html。

[186] 台湾の『2021 年国防白書』（英語版）P.35 から P.47、および韓国の『2020 年国防白書』（英語版）P.188 から P.189、P.354 から P.355、防衛省の『令和 4 年版 防衛白書』P.2 から P.5（https://www.mod.go.jp/j/press/wp/wp2022/pdf/wp2022_JP_Full_01.pdf）を参照。

[187] 安天 (2017). 『方程式組織 EQUATION DRUG 平台解析』https://www.antiy.com/response/EQUATION_DRUG/EQUATION_DRUG.html を参照。