「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

はじめに

中国と米国―2 か国の関係は日本を含め世界中に影響を与えている。日本の経済安全保障に関する議論も、米中の関係に大きな影響を受けている。また、昨今の安全保障に関して議論するためには「デジタル化」や「サイバー空間の安全保障」の話は欠かせず、データドリブンな社会においてはこうした話はもはや土台であるともいえる。

かつて、中国がインターネットに繋がってから 20 周年目にあたる 2014 年 2 月に開催された会議の中で、習近平国家主席は「習得した情報量は国家のソフトパワーや競争力を示す重要なシンボルとなった」と述べた[1]。実際に最近の中国では、国を挙げて「情報」や「データ」を取り締まる傾向が強まっている。例えば、Log 4 Shell の脆弱性を発見して Apache[2]に報告した中国企業 AliCloud のセキュリティチームが[3]、中国の工業情報化部からネットワークセキュリティ脅威情報共有プラットフォームのパートナーとしての地位を 6 カ月間停止されたことは記憶に新しい[4]。「サイバー空間の維持」や「安全」のために、外国企業に対してだけでなく、国内企業に対しても罰金や更新停止、機能やアプリの停止といった決定が下されているのである[5]。こうしたことから、我々が現在の中国の動向や安全保障観を理解するためには中国のデジタル・情報・サイバーセキュリティに関する政策を知ることが必要不可欠と考える。

日本における中国の安全保障政策に関する先行研究は、国防の観点に基づく研究は多いものの、デジタル政策の観点における先行研究や解説は限られている。今回のコラムでは中国政府が公開しているデジタル政策に関する情報および政府系メディアの報道をもとにして、中国の安全保障観を習政権発足時から時系列で確認し、検討していく。

本稿により、特に、中国を含む海外事業に携わる、あるいは中国の政策やサイバーセキュリティ事情に関心を有する方々に新たな知見がもたらされることを期待している。

1　習近平政権発足から 2020 年までの中国の政策

1.1　2012 年　習近平による新中央指導部の誕生

2012 年 11 月、中国共産党第 18 回全国代表大会（略称「18 大」）[6]と、中央委員会全体会議が北京で開催され、中国共産党第五代中央委員会総書記および中央軍事委員会主席に習近平が就任して新中央指導部が発足した[7]。18 大報告では胡錦濤政権の総括がなされ、翌 2013 年 3 月の全国人民代表大会（略称「全人代」）を以て胡錦濤・温家宝らの前任者は引退した[8]。

当時サイバーセキュリティに関する国家戦略で活発な動きを見せていたのが米国であり、中国としては米国の動静を気にせざるを得なかった[9]。両国の呼応を示したのが**図 1** である。着任してまもない時期に開催された 18 大の報告のなかで習近平は、中国の平和（国家安全）と発展には強固な国防が必要不可欠であり[10]、2020 年までに近代化（機械化と情報化）して、多様化する脅威に備えて物理領域に加えて、サイバー空間の安全保障に注目することが必要だと指摘した［山口, 2012］。一方米国でも、科学技術による発展と情報化をめざす中国の新政権に対する警戒は強まった。

戦略名	発行機関	戦略目的
「サイバー空間に係る国際戦略」	ホワイトハウス	国際商取引を支え、国際的な安全を強化し、表現の自由とイノ ベーションを育む情報通信基盤 を国際協調の下に拡大する
「サイバー空間活動戦略」	国防総省	米国及び同盟国のサイバー空間での活動能力に対するリスクを低減すること
「国土安全保障企業のためのサイバーセキュリティ戦略」	国土安全保障省	安全で強靱なインフラであり、イノベーションと繁栄を可能にし、プライバシーと市民的自由 を保護するように設計されたサ イバー空間を目指す

中国政府の反応

米国はサイバー軍が陸海空軍と宇宙軍の作戦を支援するため総合戦闘力が強化されている。深刻かつ破壊的なサイバー攻撃を受けた場合には通常兵力で対応することも可能

中国の国家安全と発展には強固な国防が必要不可欠
中国も多様化する脅威に備えて物理領域に加えてサイバー空間の安全保障に注目することが必要

図 1 米国のサイバーセキュリティ戦略に対する中国政府による反応（NISC 資料をもとに JCIC 作成）

習近平政権発足前後の中国がおかれていたサイバー環境を、中国の情報セキュリティの問題に関して監視･対処する組織である「CNCERT」によるサイバー攻撃[11]の観測結果をもとに 2011 年から 2013 年の 3 年間に絞って確認したのが**図 2** である。中国が海外から受けたサイバー攻撃の IP アドレス所在国の割合を示している。2011 年は米国をはじめとして日本、韓国に所在する悪意のある IP アドレスが最も深刻な脅威として報告されていた［CNCERT, 2012］。2012 年になると、米国に所在する悪意のある IP アドレスが最も深刻な脅威として報告された。2013 年になると米国からの脅威が他国と比較して際立つ形となった[12]。

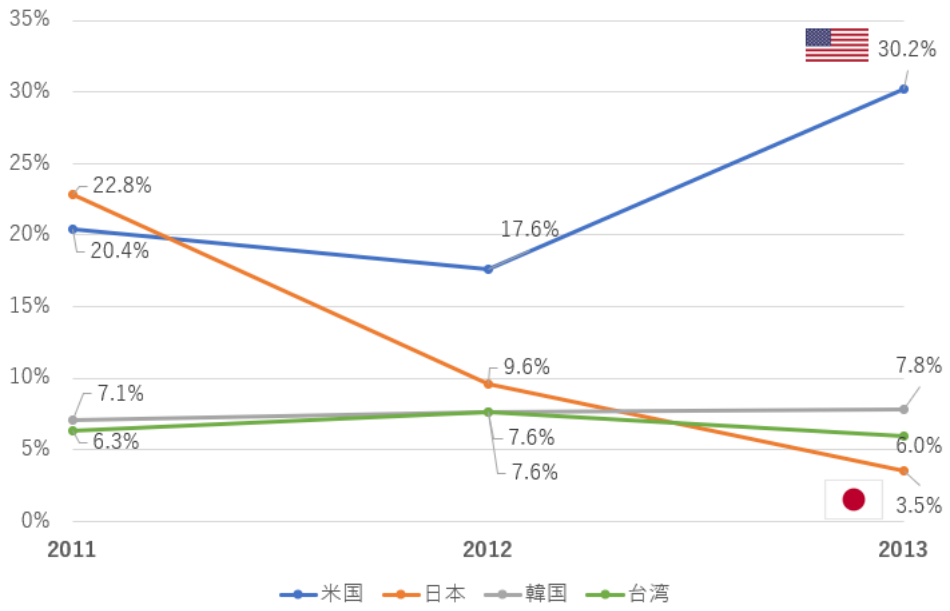

図 2 中国が海外から受けるサイバー攻撃（CNCERT 資料をもとに JCIC 作成）

1.2 「情報化」の第 12 回五か年計画期間（2011-2015）

習近平政権が発足した 2012 年は、中国の「第 12 回五か年計画（略称「125」計画）」期間[13]に該当する時期であった。125 計画の期間は内需拡大を最優先に、科学技術の革新と産業における核心的競争力の向上を重要政策目標としていた[14]。「情報化」をキーワードに掲げ、経済社会の情報化の加速およびネットワークと情報の安全保障強化が重要分野として定められていた[15]。

2013 年になると習近平は、中国を主導とした経済国家戦略である「一帯一路」構想を提唱した。一帯一路は中国から中央アジアや東南アジアを陸路や海路で経由して欧州やアフリカへと至り[16]、各地域でインフラ構築や経済発展に寄与しいく構想［Lockhart, 2017］で、各地域における中国の影響力の増大を案じた米国は難色を示した［USCC, 2016］。

翌年の 2014 年 2 月 27 日に行われた演説[17]の中で習近平は、「サイバーセキュリティと情報技術は、国家安全保障と発展、市民の労働生活といった様々な分野で国に関与している」こと、そして、「中国を強力なサイバー国家にするための努力をするべきである」ことを強調した[18]。習近平はサイバーセキュリティと情報技術を「一対の翼、二つの車輪」に例えながら、「サイバーセキュリティなくして国家安全保障はありえず、情報化なくして近代化はありえない。強いネットワーク国家を築くには、独自の技術と優れた技術、優れた情報インフラが必要である[19]」という「サイバー強国建設戦略」を打ち出した[20]。

2015 年 6 月に「中華人民共和国サイバーセキュリティに関する法案」が初めて審議され、同年 7 月に「**中国サイバーセキュリティ法（略称「CS 法」）**」の草案が一般に公開された[21]。公開された草案からは、サイバー空間における中国の主権と国家安全保障、さらに、重要インフラ運営者に対して個人情報や重要なデータを中国の領域内で保管するように要求していることがわかり、一帯一路構想

と相まって、さらに米国を警戒させることとなった。

1.3 「ハイテク化」の第 13 回五か年計画期間（2016-2020）

第 13 回五か年計画（略称「135 計画」）の全文は 2015 年 11 月 3 日に習近平によって発表され、翌年の 2016 年より始動した[22]。

図 3 の通り、習近平政権発足前から中国の GDP 成長率は下降をたどっており、2015 年は 1998 年以降で過去最低水準となる約 7%を記録していた[23]。そこで 135 計画では、社会経済発展の注力先を変更するという方針が示され、これまで中国が強みとしてきた資源と低コストの労働力を源とする「規模と速度」から、「イノベーションによる品質と経済効率の向上」へと変わった[24]。その実現にむけて人材を育成して科学技術革新を起こし、また、ベンチャー企業を創出してハイテクサービス産業の対 GDP 比を引き上げるという目標が掲げられた。さらに、サイバーセキュリティと情報技術の発展、国家サイバーセキュリティ保護システムの改善、重要な情報システムとデータ資源の保護強化、サイバー統治能力の向上も目標に加えられた。

そして、既存の産業をインターネットと融合させることにより新たなビジネス分野を開拓する「インターネット＋」[25]や、2049 年までに中国の製造業のアップグレードを図る計画の第一段階として、2025 年までに製造強国となることを目指す「中国製造 2025」といった新しい産業政策が示された[26]。

2017 年 6 月 1 日には CS 法[27]が遂に施行され、同月 28 日には組織・市民に国家情報工作への協力を求める「中国国家情報法」も施行された[28]。同年 10 月の中国共産党第 19 回全国代表大会（略称「19 大」）の中で習近平は、国家安全保障が新たな状況に直面していることに警鐘を鳴らし、「新時代の中国の特色ある社会主義思想[29]」により[30]、2035 年を節目として経済力・科学技術力の躍進、イノベーション型国家の樹立、国家統治（ガバナンス）や国防の近代化などを実現するという目標を掲げた[31]。

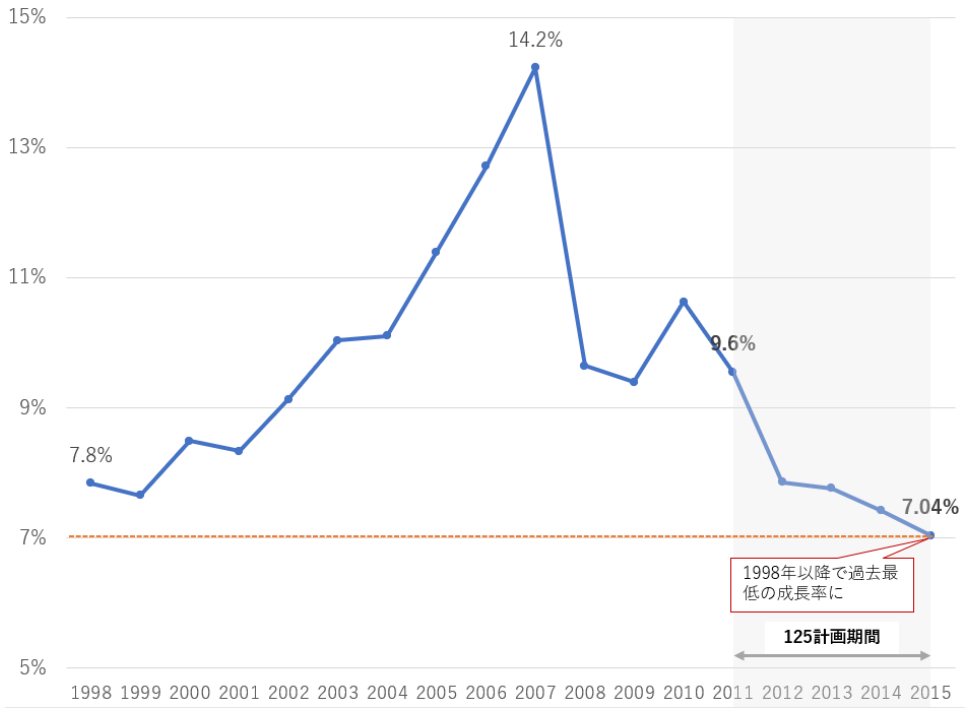

図 3　2016 年の 135 計画始動までの中国 GDP 成長率（WorldBank の GDP 成長率をもとに JCIC 作成）

2　米国の対中政策

先述のとおり、中国を警戒する米国の姿勢は、オバマ政権に続くトランプ政権下でも継続した。米国では、米国企業の知的財産を狙う中国からのサイバー攻撃が続いていた[32]。サイバー攻撃による知財侵害が米国の技術革新を弱体化させうること、そして中国で新しく施行された CS 法や国家情報法がこうした行為を助長させうることなどが懸念された[33]。2018 年 7 月に米国政府は、産業上重要な技術を含む中国からの輸入品に対して追加関税を課す対抗措置を発動した。この中には前述した中国の産業政策「中国製造 2025」に関連する品目も含まれた[34]。

米国はさらに、外国の敵対者による経済・産業スパイを含むサイバー行為に対処するための大統領令を 2019 年 5 月に発令し[35]、続いて商務省からも中国通信機器大手の華為技術（ファーウェイ・テクノロジーズ）とその関連企業 68 社を『禁輸措置対象リスト（エンティティリスト）』に追加することを発表した[36]。翌 2020 年 5 月には華為に対する制裁を更新し、規制対象の技術やソフトウェアを同社に移転すること、或いは同社から移転を受けること、を禁止する規則改正が行われた[37]。このような米国の一連の動きは、当然中国にも影響を与えた。

3　デジタル中国をめざして―2021 年以降の中国の政策

3.1　「デジタル化」の第 14 回五か年計画期間（2021-2025）

2021 年 3 月の全人代で「第 14 次回五か年計画（略称「145 計画」）と 2035 年の長期目標の策定に関する建議（「建議」）」が承認された[38]。

一つ前の 135 計画に続き 145 計画においても、イノベーションは依然として中国が発展していくための重要な駆動力となる考えが示された。但し、「国家発展戦略としての科学技術の自立自強」に示されるように、コア技術を攻防する表現が加わったのが 135 計画と 145 計画の異なる点であった。攻防とはつまり、世界の科学技術を主導する地位を確立・維持する一方で、サプライチェーンの主要な部分を国産化して国際競争力を強化・維持することを意味する。サイバーセキュリティに関しては、ネットワークの安全保護と政治的安全性を維持する能力の強化が目標に定められた。145 計画にはそのほか、国家安全システムの構築とその能力の強化や、「国家経済安全の確保」といった方針も明記されており、ハイテク技術をめぐる米国との対立の影響が垣間見える[39]。なお、前々期の 125 計画は「情報化」がキーワードであったのに対し、145 計画では「デジタル中国（デジタル経済・デジタル社会・デジタル政府により構成されるエコシステム）」のように「デジタル化」というキーワードが登場したことも特徴的といえる。**図 4** には、デジタル化やイノベーション型国家の樹立と建国 100 周年に向けて強国化をめざす中国の戦略的目標を図解した。

なお、2021 年 12 月には、習近平を指導者とする組織「中国共産党中央委員会ネットワークセキュリティ情報化弁公室（CAC）」により、145 計画期間中のデジタル発展を加速させてデジタル中国を構築するための計画（「145 国家情報化計画」）[40]が発表された。この中ではデータ資源の高度な活用

と効率化、デジタルインフラシステムの構築、5G や AI などの技術を応用するプロジェクトへの投資といった計画が明らかになった。

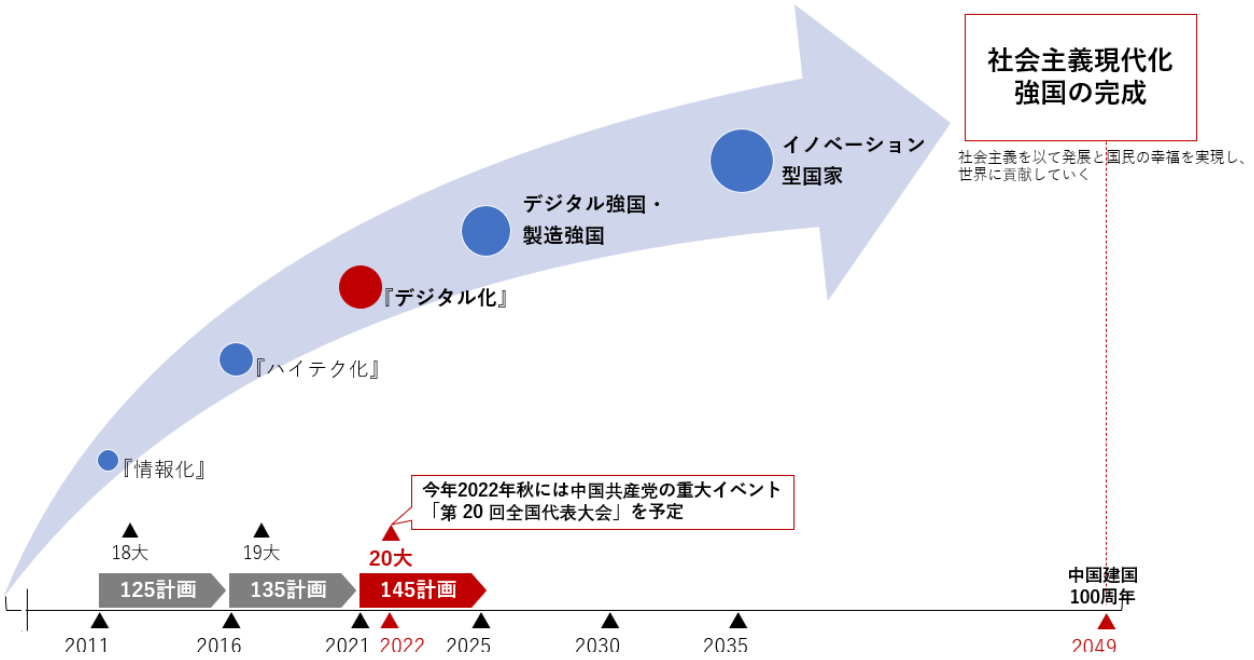

図 4 中国政府が定めている戦略的目標とマイルストーン（共産党資料をもとに JCIC 作成）

3.2 強化されるデータ管理

2021 年 7 月、中国当局により米国株式取引所に上場した配車サービスアプリ「滴滴出行（DiDi）」の CS 法および「国家安全法」違反が通告され、同アプリの即時販売停止が公表されるという出来事が発生したのは記憶に新しい[41]。中国ではその後の 2021 年 9 月に厳格なデータの輸出管理と関連主体の責任を要求する「**データセキュリティ法（略称「DS 法」）**」が施行され[42]、2021 年 11 月には「個人情報保護法（PIPL）[43]」も施行した。**図 5** に中国で試行中の国家安全保障とデータに関する 3 つの法律を図解した。

国家安全保障法には、第 59 条に国家安全保障審査監督制度にもとづく審査の実施が規定されているものの、「重要技術、ネットワーク情報技術製品およびサービス」は多々ある審査項目の 1 つに過ぎない。また、製品およびサービスにより取得・分析・使用するデータについては特段規定されてはいない。また一方で、CS 法の第 35 条に規定される審査は「ネットワーク」に範囲が限定されている。こうした状況を受けて、DS 法の第 24 条では、国家安全保障にもとづく「データ」の審査が規定されている。DS 法の下では、国家安全保障に影響を与える、或いは与えるおそれのあるデータ処理活動に対して国家安全保障審査を実施することが定められており、同時に、データ処理サービスの提供者には行政許可を取得することが要求されている。そして、個人情報に焦点をおく PIPL には、重要情報インフラ運営者に該当する場合や、規定量を超える個人情報を処理する場合の国内データ保存義務や、国家安全と公共利益を脅かす個人情報処理活動従事者への禁止措置、そして、中国に差別

的措置をとる国家・地域への類似対抗措置が規定されている。

整理すると、中国の国民や組織に対して国家安全に関する義務の遵守を求める土台が国家安全法であり、サイバー空間における主権やネットワークの安全・管理を保護するのが CS 法、データ処理活動に関する安全・管理を担うのが DS 法、個人情報の安全・管理を担うのが PIPL となる。

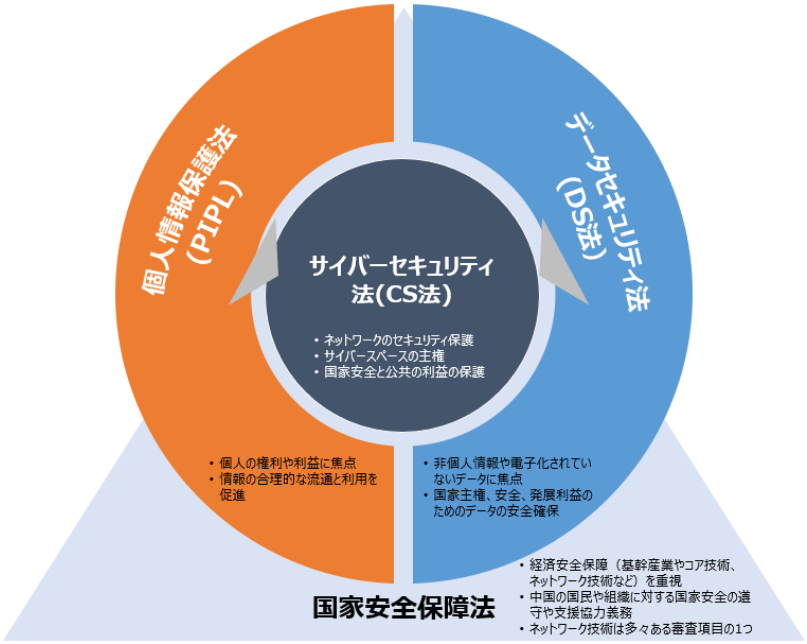

図 5 国家安全保障法とデータに関連する 3 つの法律（中国政府資料をもとに JCIC 作成）

おわりに

中国は国内にあるデータの管理を一層強化する傾向にある。

中国にとってデータは資源、すなわち国家として保護するべき対象であり、サイバー空間における主権、公共の利益や国家安全を保護するための国家政策の中心に据えられるべき重要事項なのである。「『データ＝資源』であり、保護するべき対象であり、方針や戦略の中心に据えるべき」というデジタルガバナンスの考え方は、日本企業についてもいえることなのではないだろうか。

2021 年 7 月に米国と NATO 諸国からサイバー攻撃への関与を名指し非難された中国は[44]、先日閉幕を迎えた冬季北京オリンピックの専用アプリ「MY2022」による個人データの取り扱いをめぐっても批判を受けており[45]、欧米諸国との対立は多岐に渡る。2022 年 2 月 5 日にはロシアとともに共同声明を出して、ロシアとサイバーセキュリティ領域で協力を深めていく計画を明らかにした[46]。米国や欧州諸国などとの火種を抱えるロシアと中国の協力計画は日本のみならず世界の注目を集めることが予想される。

いまや中国の動向抜きに世界のサイバーセキュリティを考えることは難しい。中国のデジタル・情報・サイバーセキュリティに関する政策の動向について今後も注視していくことが必要だ。

【注釈】

[1] 「習近平主持召開中央網絡安全和信息化領導小組第一次会議」『中国共産党新聞網』，2014 年 2 月 27 日（http://cpc.people.com.cn/n/2014/0227/c64094-24486402.html）。

[2] Apache は世界で広く使用されている Web サーバーソフトウェア。Apache ソフトウェア財団による支援のもと、開発者のオープンコミュニティによって開発・保守されている。

[3] AliCloud は中国の電子商取引企業である Alibaba 集団の関連会社で、クラウドサービスを展開している企業。

[4] AliCloud は中国政府の工業情報化部のサイバーセキュリティ脅威情報共有プラットフォームのパートナーパートナーであったが、2021 年 12 月 21 日に「ネットワーク製品のセキュリティ脆弱性管理に関する規定『網絡産品安全漏洞管理規定』」違反を理由に、上記パートナーとしてしての地位を 6 ヶ月間の停止されることになった。AliClooud は Log4Shell 脆弱性を発見した後に Apache に報告をしていたが、中国当局に報告しなかったことがネットワークセキュリティ脅威と脆弱性管理の実施を効果的に支援していないと判断されたためである。より詳細については以下を参照。

中国人民政府「工業和信息化部国家互連網信息弁公室公安部　関于印発網絡産品安全漏洞管理規定的通知」（工信部連網安[2021] 66 号），2021 年 7 月 12 日（http://www.gov.cn/zhengce/zhengceku/2021-07/14/content_5624965.htm），

中国工業和信息化部「関于阿帕奇 Log4j2 組件重大安全漏洞的網絡安全風険提示」，2021 年 12 月 17 日（https://wap.miit.gov.cn/xwdt/gxdt/sjdt/art/2021/art_7587d13959e24aeb86887f7ef60d50d3.html），

「阿里雲被暫停工信部網絡安全威脅信息共享平台合作単位」『21 財経』，2021 年 12 月 22 日（https://m.21jingji.com/timestream/html/%7BU9Pjf0FaKEU=%7D）。

[5] 中国共産党中央委員会ネットワークセキュリティ情報化弁公室により、2021 年国家的サイバー犯罪の取締り成果が発表されている。より詳細については以下を参照。

中国人民共和国国家互連網信息弁公室（CAC）「2021 年全国網絡執法取得顕著成效」，2022 年 01 月 27 日（http://www.cac.gov.cn/2022-01/27/c_1644887128880847.htm）。

[6] 全国代表大会（「全大会」）は 5 年に 1 度のみ開催される中国の最高意思決定機関で、2 千人以上の中国共産党議員のみにより構成されている。一方、全人代は毎年 3 月に開会されている立法府で、中国共産党の指導下に置かれている。なお、全人代の下には行政府である「国務院」と、司法府である「最高人民法院」・「最高人民検察院」、そして「国家中央軍事委員会」が置かれている。より詳細については以下を参照。

「中国共産党第十八回全国代表大会」『人民網日本語版』（http://j.people.com.cn/94474/204190/206190/），

「【戦略】中国の『第 13 次 5 カ年計画（2016～2020 年）』、設定された社会・環境の定量目標」『Sustainable Japan』，2016 年 3 月 23 日（https://sustainablejapan.jp/2016/03/23/chinas-13th-five-year-plan）。

[7] 「習近平氏が総書記に新中央指導部が発足」『人民網日本語版』，2012 年 11 月 15 日（http://j.people.com.cn/94474/8021004.html）。

[8] 「胡錦濤主席と習近平総書記が党大会代表と面会し、重要談話を発表」『人民網日本語版』，2012 年 11 月 19 日

(http://j.people.com.cn/94474/8022470.html)。

[9] 2011 年頃の欧米諸国では国家利益や国家安全保障上の目標を達成するために、サイバー空間で効果的に作戦を展開するためのサイバーセキュリティ戦略が策定されており、米国では 2011 年 5 月ホワイトハウスから「サイバー空間に係る国際戦略」、同年 7 月国防省から「米国サイバー空間上の作戦のための国防総省戦略」が公表されていた。より詳細については [NISC, 2015]を参照。

[10] 「中国共産党第１８回全国代表大会以降、習近平主席と中央軍事委員会が推進する強軍興軍の記録」『新華網日本語版』, 2016 年 3 月 3 日
(http://jp.xinhuanet.com/2016-03/03/c_135151134.htm)。

[11] ここでいうサイバー攻撃には、IP アドレスからみたトロイの木馬、ボット制御サーバーが含まれる。

[12] 2011 年、中国国外の IP アドレス 約 47,000 件がトロイの木馬やボットネットのコントロールサーバーとして中国国内のホストのコントロールに関与しており、コントロールされた中国国内ホストの数は 2010 年の約 500 万件から約 890 万件へと大幅の増加傾向を示していた。なお、当時のコントロールサーバーの IP 数は、日本（22.8%）、米国（20.4%）が上位を占めていた。2012 年に中国国内のホストのコントロールに関与したコントロールサーバーは米国（17.6%）が首位を占め、日本（9.6%）、台湾（7.6%）が続いた。2013 年には、米国（30.2%）で首位、韓国（7.8%）、中国香港（7.7%）、日本（3.5%）と米国が群を抜く結果になった。より詳細については [CNCERT, 2013]および [CNCERT, 2014]を参照。

[13] 中国では今後 5 年間の社会・経済に関する国家戦略が定められており、「五か年計画」と呼ばれている。

[14] 中国人民政府「国民経済和社会発展第十二個五年規画綱要（全文）」, 2011 年 03 月 16 日
(http://www.gov.cn/2011lh/content_1825838.htm)。

[15] 125 計画には「安全」というフレーズが 30 回登場し、「強国」というフレーズは 6 回登場した。

[16] 「『一帯一路』版図が発表　初めて海上シルクロード南ルートを明示」『中国網日本語版』, 2015 年 4 月 14 日
(http://japanese.china.org.cn/business/txt/2015-04/14/content_35317683.htm)。

[17] 2014 年 2 月 27 日に行われた習近平による演説は通称「重要講話」と呼ばれている。

[18] 中国共産党新聞網に掲載された記事「中国をサイバー強国にするために努力する」の原文では「网络强国」と記されており、「ネットワーク強国」や「インターネット強国」と訳すこともできるが、ここでは「サイバー強国」の訳を使用している。「努力把我国建設成為網絡強国」『中国共産党新聞網』, 2014 年 2 月 27 日
(http://cpc.people.com.cn/xuexi/n/2015/0720/c397563-27331860.html)。

[19] 2014 年 2 月 27 日に実施されたサイバーセキュリティと情報化に関する中央指導グループ第 1 回会合における習近平重要演説。中国人民共和国国家互連網信息弁公室（CAC）「中央網絡安全和信息化領導小組第一次会議召開 習近平発表重要講話」, 2014 年 2 月 27 日
(http://www.cac.gov.cn/2014-02/27/c_133148354.htm)。

[20] 中国人民共和国国家互連網信息弁公室（CAC）「凝芯聚力推進新時代網絡強国建設」
(http://www.cac.gov.cn/gzzt/ztzl/zt/xsdwlqgjs/A0920010807index_1.htm)。

[21] 全人代ウェブサイトに掲載された当時の「サイバーセキュリティ法案」。中国人大网全国人民代表大会「網絡安全法（草案）全文」, 2015 年 7 月 6 日
(http://www.npc.gov.cn/npc/c1481/201507/82ce4cb5549c4f56be8a6744cf2b3273.shtml)。

[22] 第 13 回五カ年計画のなかには「安全」というフレーズは 157 回登場し、125 計画にはなかった「サイバーセキュリティ」というフレーズが 7 回登場した。「強国」は 27 回登場した。中央人民政府「中华人民共和国国民经济和社会发展第十三个五年规划纲要」，2016 年 3 月 17 日 (http://www.gov.cn/xinwen/2016-03/17/content_5054992.htm)。

[23] 「GDP Growth (annual %) - China」，The WorldBank ウェブサイト，(https://data.worldbank.org/indicator/NY.GDP.MKTP.KD.ZG?end=2020&locations=CN&start=2011)。

[24] 「関于『中共中央関于制定国民経済和社会発展第十三個五年規画的建議』的説明」，中共中央宣伝部宣伝舆情研究中心の学習強国ウェブサイトによる第 13 回五カ年計画の策定提案に関する説明，2015 年 11 月 3 日 (https://www.xuexi.cn/bfe5ee170d1bbaf3f7f1c0c0e08b4105/e43e220633a65f9b6d8b53712cba9caa.html)。

[25] 「『互聯網＋（インターネットプラス)』で変わる 中国のライフスタイル 2017」，独立行政法人日本貿易振興機構（JETRO）による資料，2017 年 3 月，(https://www.jetro.go.jp/ext_images/_Reports/02/2017/7854a5ba68a23e2d/reportchina2017.pdf)。

[26] 「中国政府が『中国製造 2025』発表、製造強国を実現」，JETRO 知的財産ニュース，2015 年 5 月 21 日 (https://www.jetro.go.jp/world/asia/cn/ip/ipnews/2015/gov/d0100319c70eadaf.html)。

[27] 「中華人民共和国網絡安全法　中華人民共和国ネットワーク安全法」，JETRO 掲載資料の大地法律事務所仮訳，(https://www.jetro.go.jp/ext_images/world/asia/cn/law/pdf/others_005.pdf)。

[28] CS 法と国家情報法の施行に対して諸外国は、中国政府が一帯一路に関連する中国の組織や個人に対して情報提供義務を課す可能性があることを懸念した。

[29] 「新時代の中国の特色ある社会主義思想」は「習近平思想」とも呼ばれる。

[30] 習近平思想は一帯一路建設の推進とともに、中国共産党規約にも取り込まれた。詳細については以下を参照。「中国共産党第 19 回全国代表大会」『新華網日本語版』，2017 年 10 月 28 日 (http://jp.xinhuanet.com/2017-10/28/c_136711568.htm)，「受権発布：中国共産党章程」『人民網』，2017 年 10 月 28 日 (http://politics.people.com.cn/n1/2017/1028/c1001-29614278.html)，「『習近平による新時代の中国の特色ある社会主義思想』が党規約に」『人民網日本語版』，2017 年 10 月 24 日 (http://j.people.com.cn/n3/2017/1024/c94474-9284198.html)。

[31] 「系列重要講話数据庫」『人民網』，習近平重要講話の特設サイト，(http://jhsjk.people.cn/)。

[32] "US authorities name Chinese firms involved in hacks," *The Hill*, October 8, 2015 (https://thehill.com/policy/cybersecurity/256330-us-authorities-name-chinese-firms-involved-in-military-hacks), "United States Steel Corporation Announces Action On Section 337 Case [Press Release] ," *United States Steel Corporation*, February 15 2017 (https://uss.mediaroom.com/index.php?s=32722&item=137111)。

[33] "President Trump Announces Strong Actions to Address China's Unfair Trade," *The Office of the U.S. Trade Representative (USTR)*, March 22, 2018 (https//ustr.gov/about-us/policy-offices/press-office/press-releases/2018/march/president-trump-announces-strong),

"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," *The Office of the U.S. Trade Representative (USTR)*, March 22, 2018 (https://ustr.gov/sites/default/files/Section%20301%20FINAL.PDF).

[34] "Issues Tariffs on Chinese Products in Response to Unfair Trade Practices," *The Office of the U.S. Trade Representative (USTR)*, June 15, 2018 (https://ustr.gov/about-us/policy-offices/press-office/press-releases/2018/june/ustr-issues-tariffs-chinese-products),
「米政府が対中追加関税賦課を開始、中国政府も対抗」, JETRO 知的財産ニュース, 2018 年 07 月 09 日 (https://www.jetro.go.jp/biznews/2018/07/85c573de8367caa8.html)。

[35] "Securing the Information and Communications Technology and Services Supply Chain," A Presidential Document by the Executive Office of the President, *Federal Register*, May 17 2019 (https://www.federalregister.gov/documents/2019/05/17/2019-10538/securing-the-information-and-communications-technology-and-services-supply-chain).

[36] "Addition of Entities to the Entity List," A Rule by the Industry and Security Bureau, *Federal Register*, May 21 2019 (https://www.federalregister.gov/documents/2019/05/21/2019-10616/addition-of-entities-to-the-entity-list).

[37] "Export Administration Regulations: Amendments to General Prohibition Three (Foreign-Produced Direct Product Rule) and the Entity List," A Rule by the Industry and Security Bureau, *Federal Register*, May 19 2020 (https://www.federalregister.gov/documents/2020/05/19/2020-10856/export-administration-regulations-amendments-to-general-prohibition-three-foreign-produced-direct),
さらに 2020 年 7 月には、米国の姿勢に同調した英国が、英国の 5G ネットワークから華為社を排除すると公表した。
より詳細については以下参照。
"Huawei to be removed from UK 5G networks by 2027," *Gov.UK*, July 14 2020, (https://www.gov.uk/government/news/huawei-to-be-removed-from-uk-5g-networks-by-2027),
"Summary of the NCSC analysis of May 2020 US sanction," *National Cyber Security Centre (NCSC)*, July 14, 2020 (https://www.ncsc.gov.uk/report/summary-of-ncsc-analysis-of-us-may-2020-sanction).

[38] 第 14 回五カ年計画と併せて、2035 年の長期目標の策定に関する提案が公開された。中央人民政府「中華人民共和国国民経済和社会発展第十四個五年規画和 2035 年遠景目標鋼要」, 2021 年 3 月 13 日 (http://www.gov.cn/xinwen/2021-03/13/content_5592681.htm),
なお、「2035 年遠景目標鋼要」は戦略目標と重点分野に関する文書で、全人代に先駆けて 2020 年 10 月に実施された共産党五中全会で承認された。より詳細については以下を参照。
「中国の次期 5 カ年規画、科学技術の自立強化を国家発展戦略の柱に位置付け、国家経済安全保障も強化」, JETRO ビジネス短信, 2020 年 11 月 06 (https://www.jetro.go.jp/biznews/2020/11/b00e379433496a5a.html)。

[39] 145 計画には「安全」というフレーズが 180 回登場し、前期計画よりからさらに増加している。「強国」は 37

回、「サイバーセキュリティ」は 14 回登場した。

[40] 中国人民共和国国家互連網信息弁公室（CAC）「中央網絡安全和信息化委員会印発『“十四五”国家信息化規画』」，145 計画期間の CAC による情報化計画，2021 年 12 月 27 日
(http://www.cac.gov.cn/2021-12/27/c_1642205312337636.htm)，
[田中, 2020]「当面のマクロ経済政策」，財務省財務総合政策研究所中国研究会，2020 年 12 月 24 日
(https://www.mof.go.jp/pri/research/conference/china_research_conference/2020/china_202002-1.pdf)。

[41] 網絡安全審査弁公室「網絡安全審査弁公室関于対“滴滴出行”啓動網絡安全審査的公告」，配車サービスアプリ「滴滴出行（DiDi）」のサイバーセキュリティ審査に関する通知，2021 年 7 月 2 日
(http://www.cac.gov.cn/2021-07/02/c_1626811521011934.htm)，
中国人民共和国国家互連網信息弁公室（CAC）「関于下架“滴滴出行”App 的通報」，CAC による配車サービスアプリ「滴滴出行（DiDi）」の削除に関する通知，2021 年 7 月 4 日
(http://www.cac.gov.cn/2021-07/04/c_1627016782176163.htm)。

[42] 中国人大网全国人民代表大会「中華人民共和国数据安全法」，2021 年 6 月 10 日
(http://www.npc.gov.cn/npc/c30834/202106/7c9af12f51334a73b56d7938f99a788a.shtml)。

[43] 中国人大网全国人民代表大会「中華人民共和国個人情報保護法」，2021 年 8 月 20 日
(http://www.npc.gov.cn/npc/c30834/202108/a8c4e3672c74491a80b53a172bb753fe.shtml)，
なお、同法前後のタイミングで LinkedIn や Yahoo が中国でのサービス提供の終了を決定しているように、外国企業への影響の大きさが窺える。中国におけるサービス提供の終了については以下を参照。
“China: Sunset of Localized Version of LinkedIn and Launch of New InJobs App Later This Year,” *LinkedIn Official Blog*, October 14, 2021
(https://blog.linkedin.com/2021/october/14/china-sunset-of-localized-version-of-linkedin-and-launch-of-new-injobs-app)，
「雅虎 Yahoo：11 月 1 日起在中国大陸停止産产品及服務」『テンセントニュース』，2021 年 11 月 2 日
(https://new.qq.com/omn/20211102/20211102A06Z1X00.html)。

[44] The White House, “The United States, Joined by Allies and Partners, Attributes Malicious Cyber Activity and Irresponsible State Behavior to the People’s Republic of China,” July 19 2021
(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/)，
また、米国に呼応する形で NATO も中国によるサイバー行為を批判した。
NATO, ”Statement by the North Atlantic Council in solidarity with those affected by recent malicious cyber activities including the Microsoft Exchange Server compromise,” July 19 2021
(https://www.nato.int/cps/en/natohq/news_185863.htm).

[45] カナダのトロント大学 CitizenLab が冬季北京オリンピック専用アプリ「MY2022」に関する分析レポート[Knockel, 2022]を公開した。これに関する記者からの質問に対して在カナダ中国大使館が反論をしている。詳細については以下を参照。

中華人民共和国駐加拿大使館「駐加拿大使館発言人答記者問」，2022 年 1 月 18 日（http://ca.china-embassy.org/chn/xw/202201/t20220119_10630233.htm）。

[46] 推進“一帯一路”建設工作領導小組弁公室「中華人民共和国和俄羅斯連邦関于新時代国際関係和全球可持継発展的連合声明（全文）」，2022 年 2 月 5 日（https://www.yidaiyilu.gov.cn/xwzx/gnxw/219621.htm）。

【閲覧日について】

インターネットリソースは、別途注記したものを除き、すべて 2022 年 3 月 20 日に最終閲覧した。

引用文献

CNCERT. (2012 年 5 月 23 日). 2011 年中国互連網網絡安全報告. 参照日: 2022 年 3 月 20 日, 参照先: 国家互連網応急中心（CNCERT）: https://www.cert.org.cn/publish/main/46/2012/20120523085533341215471/20120523085533341215471_.html

CNCERT. (2013 年 7 月 10 日). 2012 年中国互連網網絡安全报告. 参照日: 2022 年 3 月 20 日, 参照先: 国家互連網応急中心（CNCERT）: https://www.cert.org.cn/publish/main/46/2013/20130709131057230104032/20130709131057230104032_.html

CNCERT. (2014 年 6 月 3 日). 2013 年中国互連網網絡安全报告. 参照日: 2022 年 3 月 20 日, 参照先: 国家互連網応急中心（CNCERT）: https://www.cert.org.cn/publish/main/46/2014/20140603151551324380013/20140603151551324380013_.html

KnockelJeffrey. (2022). Cross-Country Exposure Analysis of the MY2022 Olympics App. University of Tronto. Tronto: CitizenLab. 参照日: 2022 年 3 月 20 日, 参照先: https://citizenlab.ca/2022/01/cross-country-exposure-analysis-my2022-olympics-app/

LockhartBruceAnna. (2017 年 6 月 26 日). China’s $900 billion New Silk Road. What you need to know. 参照日: 2022 年 3 月 20 日, 参照先: World Economic Forum: https://www.weforum.org/agenda/2017/06/china-new-silk-road-explainer/

NISC. (2015 年 2 月 10 日). NISC による資料 4「新・サイバーセキュリティ戦略について」. 参照日: 2022 年 3 月 20 日, 参照先: 内閣サイバーセキュリティセンター（NISC）: https://www.nisc.go.jp/conference/cs/dai01/pdf/01shiryou04.pdf

USCC. (2016). CHAPTER 3 CHINA AND THE WORLD SECTION 1: BELT AND ROAD INITIATIVE. Washington, DC: U.S.-China Economic and Security Review Commission（USCC）. 参照日: 2022 年 3 月 20 日, 参照先: https://www.uscc.gov/sites/default/files/2019-09/Chapter%203%20Section%201-%20Belt%20and%20Road%20Initative_0.pdf

山口信治. (2012 年 12 月 11 日). ブリーフィング・メモ　中国共産党第 18 全国代表大会と習近平政権の

始動. 参照日: 2021 年 12 月 17 日, 参照先: 防衛研究所:
http://www.nids.mod.go.jp/publication/briefing/pdf/2012/briefing_171.pdf
田中修. (2020). 当面のマクロ経済政策. 中国研究会. 東京: 財務省財務総合政策研究所. 参照日: 2022 年 3 月 20 日, 参照先:
https://www.mof.go.jp/pri/research/conference/china_research_conference/2020/china_202002-1.pdf