サイバーセキュリティ国家戦略

―サイバー強国を目指す中国のシナリオ―

The National Strategy for Cybersecurity: China's Scenario to Become a Cyber Powerhouse

周　　橋

ZHOU Qiao

愛知大学国際コミュニケーション学部　非常勤講師

Faculty of International Communication, Aichi University

E-mail: zhouqiao513@hotmail.co.jp

要旨：

本論文は「サイバー強国」を国家の目標としている中国の「国家サイバーセキュリティ戦略」を体系的に研究したものである。中国政府により公表された『国家サイバー空間セキュリティ戦略』を解読し、その形成のプロセスを明らかにしたのみならず、その戦略を貫く基本理念を整理した。さらに、それらの基本理念に基づき、「サイバーセキュリティ」の名目により中国政府が実践している様々な施策を概観し、中国の「国家サイバーセキュリティ戦略」は内政の安定に重きを置いたものであるという結論に至った。

Abstract:

This paper is a systematic study of China's National Cybersecurity Strategy, which aims to set China as a "Cyber Powerhouse." It deciphers the National Cyberspace Security Strategy published by the Chinese government and not only clarifies the process of its formation, but also describes the basic principles that run through the strategy. Furthermore, based on those basic principles, it reviews the various measures implemented by the Chinese government in the guise of "cyber security" and concludes that China's National Cyber Security Strategy heavily focuses on internal political stability.

Ⅰ．はじめに

2017年に実施された世界経済フォーラム（WEF）の「世界の主要リスクに関する意識調査」では、気候異常、自然災害、大量移民、テロ攻撃に次いで「サイバー攻撃」が5位にランクインし（World Economic Forum 2017）、サイバー攻撃が世界中の人々に広く認識されるようになっていることがわかる。1990年代以降、インターネットの台頭を核とするIT革命は、人類の社会生活の隅々のあらゆる方面にまで浸透し、その結果、サイバー空間の影響は現実の社会にまで及んでいる。サイバー空間の重要な特徴は、情報空間と現実世界が交差していることであり、そのためサイバー攻撃の影響は決してサイバー空間にとどまらず、人々の日常生活や依存する社会環境・インフラ等にまで波及し、被害範囲の拡大に繋がる恐れがある。

サイバー空間の出現とその発展により、世界各国の安全保障政策は大きな変革を余儀なくされているが、同時に各国のサイバーセキュリティ対応は多くの困難にも直面している。クラウドコンピューティング、IoT（モノのインターネット）、ビッグデータ、仮想通貨、ChatGPTなど、サイバー空間の基盤となるインターネット技術は常に急速に進化しており、こうした新しい技術には、新しいセキュリティの脆弱性や新しい形のサイバー攻撃がつきものである。特に複雑なのは、主権国家の政府、軍隊、企業、団体、国際機関、NGO、NPO、個人、様々な利益団体、テロリスト、ハッカーなど、サイバー空間に依存し活動するステークホルダーが多様であり、その全員がサイバー攻撃の被害者となり得るうえに、加害者またはサイバー攻撃の実行者にもなり得ることである。ある国におけるサイバーセキュリティには、国家的な対策に加えて、その国のすべての関連組織、市民社会、教育機関の協力と援助が必要であることは言うまでもない。このように、サイバーガバナンスは、当然ながら国家の内部管理にとっても、重要かつ全く新しい領域となっている。

国家がサイバー攻撃の発動者となることもあるため、世界各国はそれぞれのセキュリティ部署、情報機関、軍のサイバー部門などの機能を強化しなければならず、国家の意思決定のためにサイバー空間を通じて質の高い情報および関連する情報を取得することの重要性が著しく高まっている。また、国内外からのサイバー攻撃の脅威を認識しながらも、さまざまな理由でそれを防ぐことができないが故に国家の安全保障のために先制してサイバー攻撃を行うことを選択することもあり得る。このパラドクスは、攻撃と防御あるいは抑圧の境界線が明確に定義されていないサイバー空間においては、特に注意すべきものとなっている。ブキャナン（B. Buchanan）が指摘するように、「防衛を目的とした侵入」（defensive-minded intrusion）やいわゆる「積極的防御」（active defense）の名の下に国家が行うサイバー攻撃やその他サイバー関連の活動は、しばしばその行動が正当化されたり、

またそうする動機が与えられたりする傾向が強く見られる（Buchanan 2017）。

サイバー空間における安全保障問題は複雑であり、各国はサイバーセキュリティの問題に対処するために、サイバー空間を管理する法律や規制、一連の具体的な政策などを含む国家戦略や基本制度を策定する必要がある。国家サイバーセキュリティ戦略や関連政策の策定において、各国政府はサイバー空間における自国利益の最大化を積極的に追求している。グローバル化したサイバー情報空間は今や各国が情報社会にアクセスするための共通の場となったため、国家はそれぞれ自らのサイバーセキュリティを定義しながら、その境地を拡大し、自国の安全保障を追求することに尽力する。その結果として、サイバー空間のグローバル・ガバナンスと国家による独自のサイバーセキュリティへの過剰な追求の間に緊張感がもたらされている。

「国家サイバーセキュリティ戦略」とは、サイバーセキュリティの分野における各国の国家的な要領・計画である。多くの場合、該当する国家の計画を達成するための主要なアプローチや基本的な道筋の説明が含まれており、サイバー外交のような宣言を伴うことも多い。 21世紀の最初の10年間にサイバー犯罪やサイバー攻撃などのサイバーセキュリティの問題が急速にクローズアップされるに従い、各国政府は独自の対応を展開した。2011年頃までに少なくとも20カ国がサイバーセキュリティに関する国家戦略を策定・公表し、2017年頃にはこのような国家戦略を持つ国は80カ国近くにまで急増した（小宮山・土屋 2018）。

現在、世界で唯一の「サイバー犯罪に関する条約」（通称「ブダペスト条約」[1)]）の批准国はわずかで、アジア太平洋地域では日本、オーストラリア、スリランカの 3 カ国しか批准していない（須田 2015）。サイバー空間の安全保障に関する国際社会の議論は、国連総会第一委員会が設置した政府専門家会合（国連サイバーGGE、Group of Governmental Experts）で一部協議が行われているが、拘束力のある合意には至っていない。また、一部の国家間でもサイバーセキュリティに関する議論が行われており、例えば、サイバー空間に関する国際会議（GCCS：Global Conference on Cyberspace）などもあるが、まだ普遍的かつ代表的とはなっていない。サイバー空間が事実上の無政府状態である以上、主権国家から次々と発表された国家サイバーセキュリティ戦略は、将来的にサイバー空間におけるグローバル・ガバナンスを実現するための重要な基盤となるため、当然ながら特に注目

1）「サイバー犯罪に関する条約」（Cyber-crime Convention）とは、2001年11月にブダペストで EU 加盟国26カ国と米国、カナダ、日本、南アフリカなど30カ国が署名した国際条約である。2003年1月23日に EU がストラスブールで「サイバー犯罪に関する条約の追加議定書：コンピュータシステムを通じて行われる人種差別的および排外主義的性質の行為の犯罪化について」（Additional Protocol to the Convention on Cybercrime, Concerning the Racist and Xenophobic Nature Criminalization of Acts of a Racist and Xenophobic Nature Committed through Computer Systems）を採択した。

されるべきであろう。

2016年12月27日、中国政府は「国家網絡空間安全戦略」(「国家サイバー空間セキュリティ戦略」[2])を発表し、2017年3月1日には「網絡空間国際合作戦略」(「サイバー空間に関する国際協力戦略」[3])が発表された。特に「国家網絡空間安全戦略」は、サイバー空間の発展と安全保障に関する中国の立場と主張を示し、サイバー空間における国家主権、安全や発展の利益を守ることを基本目標として宣言するとともに、今後一定期間のサイバー安全保障分野における中国の戦略課題を定めている。インターネット利用者の数が世界トップであることから、「インターネット大国」と言われる中国は、さらに「インターネット強国」を目指している。その中国のインターネット政策とサイバー安全保障に関する国家戦略を定め、インターネット強国に向かうシナリオを描いた前述の2つの基本文書は、直ちに国内外の学界の注目が集まり、中国国内のサイバー管制において主導的役割を果たすとともに、サイバー空間に関わる国際関係にも大きな影響を与えることは予想に難くない。中国の国家サイバーセキュリティ戦略をめぐる学術研究は、これまで簡単な紹介のレベルにとどまっていたことから、本稿では、この国家戦略とそれに関連する中国国内の諸問題や対応について、より体系的で深い考察を行うことを意図している。

Ⅱ．先行研究、問題意識、キーワード

世界各国のサイバー安全保障に関する国家戦略についての学術研究には一定の蓄積がある。2013年、欧州安全保障協力機構（OSCE）は、各国にサイバー空間とサイバー戦争に関する立場の公表や、サイバー空間における相互信頼と理解の発展に努めることを求める決定を行った（OSCE 2013)。また、欧州連合サイバーセキュリティ機関（ENISA：The European Union Agency for Cybersecurity）と北大西洋条約機構サイバー防衛協力センター（NATO CCDCOE：NATO Cooperative Cyber Defense Centre of Excellence）は、各国の戦略的意図の透明性を促進することを目的に、世界各国のサイバー安全保障に関する戦略文書を広く収集した。その結果、国家戦略に関する文書や情報のカタログが纏められ、研究者が国家戦略の策定に関する一般的な背景を探ったり、国をまたいだ比較研究をしたりする際に役立つだろう。北大西洋条約機構サイバー防衛協力センターは、「国家サイバーセキュリティ戦略策定のためのガイド」を公開し、各国の国家戦略の策定における理念、視点や対応されるべき問題などについて示唆を与えている（NATO CCDCOE 2013)。

2）「中央網絡安全和信息化領導小組」（サイバー安全保障と情報化に関する中央指導グループ）の承認を得て、「国家互聯網信息弁公室」（国家インターネット情報弁公室）により公表された。

3）「中央網絡安全和信息化領導小組」の承認を得て、外交部と「国家互聯網信息弁公室」により共同で公表された。

1，先行研究の概観

諸国のサイバー安全保障にかかる国家戦略についての研究には以下のような蓄積がある。英語圏に目を向けてみると、ルイフ（E. Luiijf）らは、諸国のサイバーセキュリティ戦略に相当する19の文書を調査し、具体性、測定可能性、達成可能性、現実性、適時性という5つの尺度で評価することを提案した（Luiijf, Besseling, and De Graaf 2013）。アズミ（R. Azmi）らは、世界54カ国のサイバーセキュリティ戦略を分析し、これらの戦略がサイバー空間における国益を守るためだけのものではなく、サイバー空間における技術革新が将来的に自国にもたらすはずの権利や利益を確保しようとする強い意思を反映していると指摘している（Azmi, Tibben, and Win 2016 ）。ミン（K. Min）らは、米国、EUや日本の国家サイバーセキュリティ戦略を分析し、政府と民間企業に期待される役割の割合がそれぞれであることを明らかにし、インフラ保護をはじめとするサイバーセキュリティの分野において、政府と民間企業の役割を明確に区分することは非常に困難であることを指摘している（Min, Chai and Han 2015）。

日本人学者小宮山功一郎と土屋大洋は、主要8カ国（国連安保理常任理事国、日本、オーストラリア、ドイツ）のサイバーセキュリティ戦略の関連文書を精査し、その内容の多様性を指摘し、各国の関連文書は「国家サイバーセキュリティ戦略」または「情報セキュリティ戦略」と呼ばれ、名称だけでなくそれぞれの国における法的位置づけやその実施を担当する政府機関も異なっていると指摘した（小宮山・土屋 2018）。「サイバーセキュリティ」、「サイバー空間」、「重要インフラ」といった概念やカテゴリーの具体的な定義には各国間で微妙な違いがあるものの、世界のサイバーセキュリティの厳しい現状に対する認識は、各国間でほぼ一致していることがわかる。

小宮山と土屋は、各国のサイバーセキュリティ戦略がどのような目的で策定され、その結果、政府がどのような問題に取り組み、具体的にどのような施策を推進し、国内外に対してどのように発信してきたのかを問うた。そして、これらの問いに対する答えを理解することで、サイバーセキュリティ問題にかかる主要国それぞれの立場や基本姿勢を明らかにした。攻撃的なサイバー能力の獲得を明示的に望んでいるのか、サイバーセキュリティ技術を用いた情報分析を行う機関を有しているかなど、戦略文書の内容に基づいて、各国のサイバーセキュリティ戦略を4つのタイプに分類し、戦略立案者のビジョンや意図の違いを探り、その上で策定・公表することの意味を明らかにしようとした（小宮山・土屋 2018）。

1つ目は「政府内調整」型で、政府内の組織や連携を明確にして、サイバーセキュリティ危機への対応力を向上させることを目指す。例えば、オーストラリアでは、これまで分断されていた各機関の機能をサイバーセキュリティセンターに集約し、政府内にコンピュータ緊急対応チーム（CSIRT：Computer Security Incident Response Team）を新設した。

2つ目は「国内政治」型であり、民間企業、学術研究機関、中央・地方政府の責任など、政府と国民の役割と責任を明確化することである。例えば、フランスは様々な関係者の情報共有や共通認識を重視している。また、中国は国内のインターネットガバナンスや統制を重視している。既存の国家安全保障戦略と比較すると、サイバー空間のセキュリティ戦略は、政府以外のアクターの役割を重視していることが特徴的である。3つ目は「政策宣言」型で、すなわち国際社会に対する自国の立場、理念方針などを表明するものである。主要8カ国のサイバーセキュリティ戦略はいずれもこうした性格を持っているが、ロシアは基本的に国内問題を扱わず、外務省の国際交渉指針を詳細に確認している点でより典型的である。サイバー空間には明確な管理者、あるいは自国の立場をアピールできる明確なオーディエンスが存在しないため、各国がサイバー空間における国益を最大化する目標と手段を国内外に明示する必要がある。これは、危機が発生した際の過剰反応を防止することにもつながる。4つ目は「懲罰的抑止」型で、他国によるサイバー攻撃が発生した場合の報復の原則を明示し、そのための攻撃的サイバー能力の強化の必要性、ないし他国によるサイバー攻撃が行われる可能性がある前に先制攻撃を辞さないことなど明確に文書化、あるいは暗示的に示すものである。言うまでもなく、上記の4つのタイプは相互排他的ではなく、各国のサイバーセキュリティ戦略によっては、上記の4つのタイプが混在し、それぞれの側面に対する比重が異なるため、4つのタイプというより4つの理念型、モデルと言えるだとう。

中国人学者朱莉欣と韓暁陽は、中国政府が公表した「網絡空間安全国家戦略」を、策定の背景、戦略目標、原則、戦略任務などの方面から体系的に解読し、米国の2011年「サイバー空間国際戦略」やロシアの「ロシア連邦情報安全ドクトリン」(2016年12月改訂版)の関連内容と比較し、中国のサイバーセキュリティ国家戦略の最も特徴的なポイントを指摘している。すなわち、サイバー空間での発展を図りながらサイバーセキュリティを強調し、サイバー領域における国家主権を守りながら平和的共有の実現を推進することであるとした（朱・韓 2017)。朱莉欣と韓暁陽は、中国、米国、ロシアのサイバーセキュリティ戦略には同様の見解といくつかの相違点の両方があると論じている。サイバー空間がもたらす機会と課題に向き合うという点で、3カ国の認識には多くの共通点があり、例えば、インターネットが情報へのアクセスをより迅速かつ容易にし、関連産業の繁栄を促進し、社会運営や国家機関の透明性・民主化を高めたことを認めている。また、サイバー犯罪やサイバー攻撃の頻発は、国防を脅かすだけでなく、世界の平和に新たな課題を突きつけたという点においても近い認識を共有している。他方で、以下のような相違点も指摘された。米国は、サイバー空間における「抑止力」に執着しており、また、いわゆる知的財産権問題を強調し、自国のサイバーインフラに対する脅威の排除を特に重要視している。中国はサイバー空間における軍拡競争に反対しており、米国のサイバー抑止戦略は安全保障

をもたらさないばかりか、むしろ逆効果であり他国をも危うくすると考えている。また、中国とロシアは、サイバー空間における国家主権の原則を重視し、サイバー空間からの外部干渉を強く警戒しているという。

3カ国の戦略は、サイバー犯罪対策における国際協力、インターネット技術の開発、サイバーセキュリティの確保、国際的ルールの確立といった戦略目標をともに含んでいるが、それぞれの表述には明確な違いがある。例えば、サイバー空間における協力関係については、米露ともに戦略的パートナーシップの構築を目指し、特に米国は「同盟国との協力関係の構築」を重視しているのに対し、中国は「人類の運命共同体」という説話のもと、サイバー空間における共存について論じている。サイバー空間における各国の共同利益を訴える中国の目標は、多国間での共益的・国際的なインターネットガバナンスシステムの構築であり、これはサイバー空間の安全保障という問題に関して、非同盟・反覇権という中国の長年の外交政策の自然な延長線上にある。また、米中ともにサイバー空間における国際法などのルール作りの必要性を提起しているが、米国は既存の国際法の領域で優位に立っているため、それをサイバー空間に適用することに重きを置いている。そのためサイバー空間からの敵対行為に対しては（同盟国への責務も含めて）報復（retaliation）や先制（preemption）することができると主張し、サイバー空間における抑止に注力している。他方、中国は既存の国際法では情報空間における国家間紛争を充分に抑制できないどころか、自国の利益実現の妨げにさえなると考えている。そして、そのビジョンに沿うかたちでサイバー空間における国内の法制度や基準を徐々に確立させてきており、また国際法の新たな規範についてのコンセンサスを国外から得られるよう働きかけている。

張彬、彭書貞らは、米国、英国、日本、韓国、欧州連合などの国や国際機関が発表した「データガバナンスに関する国家戦略」のレビューを通じて、各国の戦略の共通点をまとめ、その多くが政府の責任、公共理念、法的保護に基づいていることを明らかにしている。また、それぞれのサイバーセキュリティ政策には、重要インフラ、政府と企業の協力、国際協力、個人のプライバシー保護などが含まれていることも指摘した。著者らによると、中国の現行のサイバーセキュリティ戦略は、重要インフラ保護、特殊人材育成、サイバー技術革新、国際協力などをカバーしており、これらは概ね世界各国のサイバーセキュリティ戦略の一般的傾向と一致している。サイバーセキュリティ規制の面では、中国は政府主導で、ハイテクデジタル技術のセキュリティ管理を重視しており、また、最新技術を使ってセキュリティ分野の産業化を促進する点では、国際社会の主流とも一致している。しかし、国家のサイバー安全保障を推進するための政府と企業の協力という点では、政府は依然として綿密な計画を立て、インターネット企業が積極的な役割を果たすよう指導する必要があり、それによってあらゆる分野・セクターでサイバー空間のセキュリティレベルを高められる（張 et al. 2019）。

蔡翠紅は、中国と米国のサイバーセキュリティ戦略を比較研究し、両国の競争を浮き彫りにした。中国と米国はともに経済・社会の発展においてサイバーインフラへの依存度が高いため、サイバー空間戦略の内部目標には類似性があるが、サイバー空間におけるそれぞれの中核利益に関する定義が異なるため、両国の戦略では特に外的目標に大きな違いがある。米国のサイバーセキュリティ戦略は「強さによる安全保障」であり、中国の国家戦略は「管制・ガバナンスによる安全保障」である。米国は先制攻撃を示唆しつつ、抑止を特徴とするサイバー空間戦略を構築しようと、統制、抑止、介入、協力を交互に繰り返しているが、中国は対外的には協力、内部的には発展と安全保障をともに重視するサイバー空間戦略を採用しているという（蔡 2019）。

2，本稿の問題意識

上記の文献を概観すると、その多くが複数の国のサイバーセキュリティ戦略を比較し、各国の関連戦略や政策の類似点と相違点を示していることがわかる。これらの研究は、各国のサイバーセキュリティ戦略の意図や方向性、さらには世界のサイバー安全保障における基本的な傾向を明らかにし、効果的な国際協力メカニズムを模索し、サイバー空間のグローバル・ガバナンスを推進する上で大きな価値を持つ。先行研究では、各国のサイバー空間に対する認識の違いが、多かれ少なかれ、サイバーセキュリティに関するそれぞれの国家戦略の目標や方向性に影響を与えていることが示されている（Lindstrom 2012）。これらの文献はいずれも本稿の筆者にとって重要な示唆を与えてくれるものである。ただし、一国のサイバーセキュリティ戦略、特にその形成の背景や経緯、国内の政治体制や国家安全保障に関する言説における位置づけなどについての洞察を欠いている点において限界はある。これに対し、本稿の問題意識は、第一に、サイバーセキュリティに関する中国の国家戦略が徐々に形成されていく過程を整理し、それによってサイバーセキュリティとサイバー空間のガバナンスに関する中国の基本的な理念、意識や認識を明らかにすることである。第二に、中国の「国家安全保障全体構想」におけるサイバーセキュリティ戦略の位置づけを明らかにすること、そして中国の「国家網絡空間安全戦略」に期待されている効果などを明らかにすることである。第三に、中国政府がそのサイバーセキュリティ戦略の目標、すなわち「サイバー強国」の構築を達成するための重要なシナリオ、あるいはどのような具体的施策やアプローチをとっているかなどを明らかにし、そして、これらすべての行動や実践を支える最も基本的な原則を明らかにすることである。

3，キーワードの説明

以上のような問題意識に基づき、また論理的な表述のために、ここでは本文に使われるいくつかのキーワードを説明する。

「サイバー空間」（cyberspace）とは、主にコンピュータとそれらを相互に接続するネットワーク装置で構成され、また、その中で交換・蓄積される情報のあふれる空間である。Cyberspace という用語は、1980年代の SF（例えば、ウィリアム・ギブスンの1982年の短編小説「バーニング・クローム」）で初めて登場し、その後、インターネットの発展とともに一般化した（Mihalache 2002: 293–301）。サイバー空間は、インターネット、コンピュータシステム、自動化システム、様々なデジタル機器とそれらがホストするアプリケーション、サービス、データなどで構成される空間であり、現在に至ってはほとんどすべての社会機能をサポートし、無数のデジタルプラットフォームをホストしているという点で複合的である。「サイバー空間」をより深く理解するには、隠喩的な想像力が必要であると論じる学者もいる（東 2011）。サイバー空間に関する定義は複数あり、例えば、米国政府はサイバー空間を世界規模での電子的な情報交換とコミュニケーションのためのインフラとして捉えており（White House 2009）、カナダ政府はサイバー空間を相互に接続された情報技術のネットワークとそこに含まれる情報によって作られる電子世界と捉えている（Government of Canada Publications 2010）。D. ベッツと T. スティーブンス（D. Betz & T. Stevens）は、すべての定義を二つのパターンに分類している。すなわち、インフラを含むものと、そうでないものである。前者は具象的かつ物理的なものとして理解されるものに対し、後者は抽象的でバーチャルなものとして理解される（Betz and Stevens 2017）。本稿では、サイバー空間を、様々なインフラやデバイス、エンドポイント、さらには仮想世界と現実世界が交錯する空間も含めたものとして定義する。

「国家サイバーセキュリティ戦略」（National Strategy for Cyberspace Security）とは、主に主権国家によるサイバー空間の安全保障に関する国家計画を指す（Azmi et al. 2016）。通常、一定期間内にサイバーセキュリティの目標を達成するために、いくつか特定のタスクと目標を設定することを目的としている。ほとんどの場合、サイバーセキュリティと言われると、その国の全体的な国家安全保障戦略とも密接に関連しているか、あるいは国家安全保障戦略のサイバー空間領域における直接的な応用である。各国のサイバーセキュリティ戦略の焦点は様々であるが、基本的にはいずれも情報セキュリティ、インフラストラクチャ・セキュリティ、技術セキュリティといった側面を含み、自国のネットワーク情報システムまたは蓄積・伝送された情報資源への侵入・破壊から保護し、サイバー空間の秩序を維持し、ネットワーク情報資源、ネットワークインフラの基本セキュリティとネットワーク利用者のプライバシーなどを含む全体目標を掲げている。

プロセス（process）：何かの生成、発展、継続的な変化、ある結果的な状態に達する前の通過状態を指す。本稿では、この言葉を、サイバーセキュリティの国家戦略を形成するための、その背景、道筋、さまざまな段階を含むものを指すものとして使用する。その「プロセス」を整理することで、中国のサイバーセキュリティ国家戦略の形成と進化の各

段階で生じた政策の転換や調整について考察することができると思われる。

「理念」（ideal）：サイバーセキュリティ国家戦略に反映される基本的な概念、認識、論理、価値、あるいは思想的な命題を指す。それぞれの理念を正確に理解することで、各国のサイバーセキュリティ戦略の異なる傾向を把握し、その結果、各国の関連する政策や行動を説明することができる。

「実践」（practice）とは、主にサイバーセキュリティに関する国家戦略を着実に実施する際に国家が採用する様々な実践的な取り組みや行動を指す。これらの実践や行動は国内政治体制下のサイバー統制・コントロールに関係しているのみならず、国際関係や外交の領域においても及ぶことである。

「サイバー強国」：中国の国家目標の一つであり、「インターネット強国」もいう。2018年4月、「全国網絡信息安全和信息化工作会議」（サイバー安全保障と情報化に関する全国会議）において、習近平氏が正式に打ち出したスローガンで、その内容はサイバー関係のインフラ建設、情報通信産業の新たな展開や、サイバー情報セキュリティなどを含んでいる。ネットワークの規模やインターネット利用者数で世界最大級のインターネット大国である中国は、サイバー領域におけるコア技術やインフラの後進性により、世界の情報化ランキングで70位と出遅れている。また、サイバー関連のキーテクノロジーが西側諸国によりますます制限されるなか、サイバーセキュリティについても深刻な課題を抱えている。さらに都市部と農村部、地域間の「デジタルデバイド」も顕著である。ある意味では、中国の「国家サイバーセキュリティ戦略」は、以上の諸問題を解決し、「サイバー強国」へ邁進せんとするシナリオとも言える。

上記の先行研究を踏まえ、本稿では、中国のサイバー安全保障に関する国家戦略を、プロセス、理念のコンセプト、実践という3つの基本的な次元で、体系的にかつ深く分析・考察することを目的とする。

Ⅲ．サイバーセキュリティ国家戦略の形成プロセス

中国のサイバーセキュリティ国家戦略は、時代とともに進化し、時代のさまざまなニーズ、社会的背景や国際情勢の変化に応じて徐々に進化してきた。醸成、蓄積のもとで次第に形成される長いプロセスを経てきたとも言える。概観すると、その形成過程には次のような段階がある。

1．第1段階（1980年～1985年）

1980年代初頭は新興のコンピュータ産業が重視された時期である。インターネットが勃興する以前の1980年代、コンピュータや集積電子回路などの技術は新興産業として、

中国政府に重視された。1982年10月、国務院は「計算機与大規模集成電路領導小組」（コンピュータと大規模集積回路に関する指導グループ）を設置し、対応する産業政策を策定した。1984年、国務院は「電子振興領導小組」（エレクトロニクス活性化指導グループ）を設置し、エレクトロニクスや関連事業に対する集中的・統一的指導を強化した。この段階では、新技術の開発に重点が置かれ、産業の進歩を促進するための政策が策定・実施されたことが特徴である。

2，第２段階（1986年～2002年）

続く21世紀初頭までは国家の情報化発展を推進する段階である。1986年２月、国家経済情報システムを強化するため、中国政府は「国家経済信息中心」（国家経済情報センター）と「国家経済信息管理領導小組」（国家経済情報管理指導グループ）を設立した。1990年代に入ると、「情報スーパーハイウェイ」（初期のインターネット）を核とした米国の情報技術革命に呼応して、中国も国家的な情報化の動きを活発化させていった。1993年12月、国務院は「国家経済信息化聯席会議」（国家経済情報化連合会議）を設置し、国家情報化の発展に関係する諸部署を統括・調整し、連動する作業のメカニズムを構築した。1994年４月20日に中国が国際インターネットへの接続を果たした後、「国家経済信息化聯席会議」を元に国務院は1999年12月、「国家信息化工作領導小組」（全国情報化指導グループ）を設立し、信息産業部（情報産業省）が具体的な事務を担うようになった。この時期にIT産業の重要性に対する認識がさらに強まったことは明らかである。

2001年８月、中国政府は国務院総理をトップとする「国家信息化領導小組」（「国家情報化指導グループ」）を改編し、その下に「国務院信息化工作弁公室」（国務院情報化事務室）を設置した。「国家信息化領導小組」は国家情報化発展戦略の策定、主要なイニシアティブの提案、国家情報化プロセスの調整、党・政府・軍を横断した国家情報化事情の指導強化などを担っている。同時に、「国家信息化専門家諮問委員会」も設置され、情報化の発展に関する重大な問題について、「国家信息化領導小組」に助言することになった。それ以降、「国家信息化領導小組」―「国務院信息化工作弁公室」―「国家信息化専門家諮問委員会」の間に安定した交流のメカニズムが形成された。この時期の特徴は、国家の経済建設のため、情報サービスの提供や保障に重点が置かれ、IT産業の発展を促進するための計画や取り組みが徐々に導入されたことである。この時期以前は、情報の機密性などの要求はあったものの、基本的には技術的な運用レベルであり、サイバーセキュリティはまだ世界的にも重要な課題とはなっていなかった。

3，第３段階（2003年～2013年）

この時期になると政府はサイバーセキュリティ問題を扱う専門機関を設置し、サイバー

セキュリティ国家戦略が構想され始めた。21世紀の最初の10年以降、世界的な情報通信技術の革新とともに、中国でもサイバーセキュリティ問題がますます顕著になってきた。2003年、中国政府は新たに「国家信息化領導小組」を新設し、その下に「国家網絡与信息安全協調小組」（国家インターネットと情報セキュリティ調整グループ」を設置し、インターネット・情報セキュリティの新しい状況に対応することとなった。サイバーセキュリティは国の議題となり、国家の情報化戦略とのバランスをとる必要があった。サイバーセキュリティ問題が初めて専門の国家機関によって対応されたことを考えると（汪2014）、2003年を第3段階の始まりと見なすことができる。この時期には、サイバー空間に対する認識が大きく変化し、サイバーセキュリティに対する理解も、技術的な領域に限定されていた以前のフェーズを超越した。

2003年8月に公表された「国家信息化領導小組関於加強信息安全保障工作的意見」（情報セキュリティの強化に関する国家情報化指導グループの意見」と2006年3月に公表された「2006–2020国家信息化発展戦略」（国家情報化発展戦略2006–2020）は、国家の情報セキュリティ戦略の全体的指導思想として、積極的防御、総合的予防、情報セキュリティの保障能力の強力などを明確に規定する重要な文書である。そのため、一部の学者は、当時の国家情報セキュリティ戦略のモデルは「積極的防御」型であり、情報の安全保障、情報ガバナンス、情報対抗の能力などのレベルを総合的に高め、情報セキュリティに対する脅威や課題に積極的に対処し、国家の総合的な安全と発展の利益を全面的に守ることを意図していると指摘した（惠2012a）。ここで言う「情報の安全保障」とは、情報資源と情報システムの保護と防御、各種重要情報システムの侵入検知能力、事故対応能力、侵入による被害を受けた後の迅速な復旧能力などの向上である。また、いわゆる「情報ガバナンス」とは、情報コンテンツを管理し、サイバー空間における情報の発信を法律に基づいて規制し、サイバー犯罪や望ましくないコンテンツの発信に対抗し、社会安全保障上の危険を排除することである。さらに、いわゆる「情報対抗」とは、サイバー覇権やサイバーテロの脅威に対処し、サイバー情報空間の抑止力や反撃力を強化することである。この3つの方面でともに進展を果たすべく、国の情報セキュリティ戦略が実行されることになる。

ところが、行政改革の結果、国の情報管理体制は大きく変化し、サイバーセキュリティの調整と情報化発展のバランスをどうとるかという課題を避けて通れなくなった。2008年7月、「国務院信息化工作弁公室」の職責は、新設された工業和信息化部（工業・情報化省）に移管され、「信息化推進司」（情報化推進部）が担当することになった。

「国家信息化専門家諮問委員会」は、2009年と20011年に国家情報化管理システムの体制やメカニズムに関する研究プロジェクトを2回展開した。2012年11月に提出した研究報告書では、情報化時代における国家情報化管理システムの改善が急務であると指摘し、情報化と情報技術革命が経済、政治、社会の各分野に浸透していることを強く強調し、情

報化が経済と社会の変革・転換を促進し、持続可能な発展を実現させ、国の総合競争力を強化する強い推進力になっていると訴えた。政治分野では、情報技術が従来の政治的生態を変え、民主と法制の発展を促し、経済分野では、情報技術が伝統産業の変革を促すとともに新しい経済形態を生み出し、社会分野では、情報技術が社会構造に変革をもたらし、人々の生活様式を変え、文化分野では、情報技術が文化の内容や伝播に劇的な変化を与え、文化事業の発展を大いに促進し、また、軍事分野では情報技術の文脈での軍事闘争能力が国防軍の発展における重要な要因になり、情報化を背景とした軍事力が国防の最重要課題となっている。科学技術分野では、現代の情報技術の水準が一国の科学技術全体の進歩の重要な指標となっている。これらの論説はある意味では、国家サイバーセキュリティ戦略の策定における背景情報や根拠を提供している。これらの分野を分析した上で、報告書は情報技術を管理する体制やメカニズムについて、解決すべき問題があると指摘した。例えば、管理機関の権限が弱いため、国の全体像を把握することが難しく、工業・情報化省だけで党、全国人民代表大会、政府、中国人民政治協商会議、高検、高裁などの機関・組織・部門のデジタル政務の建設などを統括、調整や企画することも困難であり、また、開発・改革、科学技術、公安、財政、金融、機密、暗号化などの分野と連携し、具体的な政策をめぐって調整することも障壁となっている。つまり、トップレベルの指導メカニズムや権限がないため、国家の情報化発展やサイバーセキュリティに関わる全体的・戦略的な問題で突破口を開くことが難しいとしたのである。報告書は、情報化の発展と情報システムのセキュリティに関する国家戦略・計画の策定を明確に提案し、国家が重要な情報技術や情報システムの開発、技術研究開発などを組織・調整することを提案している。

ほぼ同時に、学術界でもサイバーセキュリティの国家戦略に関する問題が議論されるようになった。惠志斌は、中国のサイバーセキュリティ戦略を、その時代背景、現実的価値、思想的起源、システム構成などの観点から理論化しようと試み、この戦略を実現するための道筋を論じている（惠 2012b）。著者は、情報セキュリティ戦略を「新国家安全観」のビジョンの下に位置づけている。従来の国家安全保障の理念は、主権独立、領土保全、政治的安定を核とした軍事・政治領域を重視するハイ・ポリティクスな傾向にあったが、サイバー時代の「新国家安全観」の理念は、政治安全保障、軍事安全保障、社会安全保障、経済安全保障、文化安全保障、情報セキュリティなど様々な分野を含み、中でもサイバー空間における情報セキュリティの重要性はますます顕著で、包括的な国家安全保障構造の基本的な基礎となっている。その結果、サイバー情報セキュリティは国家中核戦略のレベルにまで昇格し、総合的な国家安全戦略の高嶺の花となった。沈逸の分析によれば、サイバーセキュリティの国家戦略には、「実力によるセキュリティ」と「ガバナンスによるセキュリティ」という異なる選択肢がある（沈2013）。前者は国家の実力と能力を重視し、特定の領域における絶対的な優位性や支配力を追求する傾向にあるが、後者はサイ

バー空間の安全性と安定性を全体として捉え、実力の異なる国々がサイバー空間における安全性の脅威から守られ、全体の安定を保つガバナンスにより、サイバー空間およびその発展の恩恵を全ての当事国が享受できるようにするというものである。前者の典型である米国とは対照的に、中国は自国の社会変革の状況や国際関係の環境全体から後者を選択した。したがって、中国のサイバー空間における中核的な関心は、国家の安全を守り社会の秩序を維持するために、サイバー環境の安定とサイバー活動の制御可能性を確保することにある。

この時期の情報セキュリティに関する国家戦略をめぐる中国の考え方はその実、米国をはじめとする西側のサイバー大国の様々な動きを強く意識しており、例えば、欧米諸国は、サイバーセキュリティに関する独自の戦略を発表し（惠 2012b、2013）、米国の場合、2011年 5 月、オバマ政権により「サイバー空間国際戦略：繁栄、安全や開放的な世界の構築」（International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World）が発表され、「ネットワーク化が進む世界でいかに繁栄を築き、安全を促進し、開放性を守るか」という米国の価値観を詳しく述べ、全世界のインターネットの発展、ガバナンス、セキュリティ等のルールを設定し、主導権を掌握する強い動機を示し、また、外交、軍事、サイバーセキュリティ問題を統合する意図も反映されていた（White House 2011）。それらに呼応するように、2011年 9 月、中国は「中国的和平発展」（中国の平和的発展）白書を発表し、相互信頼、相互利益、平等、協力という「新安全観」を提唱し、包括的、共通、協力的な安全保障の実現を目指したいと述べた。白書に描かれた国家安全保障戦略の枠組には、サイバーセキュリティ戦略が値する位置づけも示された。しかし、米国、EU をはじめとする先進国や国際機関がサイバーセキュリティの分野で既に策定している戦略、政策、法規の整合性や綿密さと比較すると、当時中国のサイバーセキュリティ管理体制はまだ体系的で権威あるものとは言い難く、サイバーセキュリティに関する中長期の国家戦略をさらに明確にする必要があった。

丁度この時期にサイバーセキュリティに関わる重要な出来事がいくつも起きたことは指摘しておく必要がある。まず、2009年末から2010年初頭にかけての Google 事件（Google 中国撤退騒動）を契機に、中国は、サイバーセキュリティ問題が譲歩できないイデオロギー対立とサイバー空間のグローバル・ガバナンスの言説をめぐる争いを含んでいることを強く認識するようになった。米国をはじめとする西側先進国はインターネットガバナンスの言説を支配し、インターネットはオープンで、シェアできて、またボーダレスであると標榜し、「サイバーフリーダム」の立場から中国のサイバー管制・ガバナンスを非難し、中国に圧力をかけ、その国の威信や名誉に深刻な打撃を与えている（周 2020）。中国は、国内外の環境に対応できるサイバーセキュリティ・ガバナンスに関する基本的な表述・言説を打ち出す必要に迫られた。

次に、2010年11月よりStuxnetを用いたイラン核施設へのサイバー攻撃を契機に、中国を含む世界各国は、国内のサイバーインフラが常に他国から悪意のある攻撃を受け、国民生活に大きなダメージを受ける危険性があることを認識するようになった。かつては主に経済的動機に駆られた悪意ある個人やグループによる目の上のたん瘤程度だったサイバー攻撃は、実世界の、さらには重要インフラに対して打撃を与えうる国家主導のサイバー攻撃へと驚異の次元が繰り上がった。刺激を受けた中国でも速やかな一連の安全体制の構築およびそのための高度な技術力の向上が急務となった。

三つ目は、2013年6月のスノーデン事件により、米国家安全保障局（NSA）がプリズム計画を密かに実施し、中国を含む多くの国の重要部門、政治家、一般のインターネットユーザーに対して長期的かつ大規模な盗聴活動を実施していたことが明らかになった。これにより、中国は米国や西側諸国によるサイバー空間における情報監視やスパイ活動、エスピオナージの脅威に常に晒されているという事実に目覚めた。

さらに、この時期の中国は前例のないレベルのサイバー攻撃を記録した。2012年、「反共ハッカー」と呼ばれる海外グループが、中国の党・政府機関や社会組織のウェブサイトを持続的に攻撃し、90以上の部門のウェブサイト142件が改ざんされた（孟 2014）。2013年、中国のインターネットユーザー数は6億人を超え、うちモバイルネットユーザー数は4億6,100万人と、ユーザー規模、ブロードバンド数、ドメイン名登録数などの指標では世界トップクラスに位置するが、中国は依然サイバー強国とは言えない状況であった。そのサイバーセキュリティの程度は低く、米国や西側のサイバー強国に比べ、中国社会のサイバーセキュリティに対する意識も弱く、技術や予防能力も明らかに不十分である。関連データによると、2013年1月から2月にかけて、中国国内の約190万台以上のホストPCを制御する国外のトロイの木馬またはボットネット制御サーバーは6747台で、そのうち米国にある制御サーバーは2194台であり、中国国内の128万7000台のホストPCを制御していた。その間、中国チベットネット、中国ネットの英語版企業支社、人民日報オンラインでは、メールシステムにバックドアが埋め込まれ、ウェブサイトが改ざんされたり国外からDDoS攻撃を含むサイバー攻撃を受けたりした。2013年11月時点で、中国国内のウイルスに感染した端末数は約250万台、改ざんされたウェブサイト数は7,146（うち政府サイトが546）であり、バックドアが埋め込まれたウェブサイトの数は22,672件（うち政府系ウェブサイトは266件）で、また、特定のウェブサイトを模倣したページ数は1,835件だった（孟 2014）。

要するに、中国にとってサイバーセキュリティ国家戦略をどのように構築し、サイバーセキュリティ分野での受動性を完全に改善するためにどのような重要な取り組みができるかは、国家安全保障体制のトップレベルが対応すべき緊急課題となっていることは明らかである。

4，第４段階（2014年～）

この期間に、中国のサイバーセキュリティ国家戦略が形成され、そして改善が繰り返されている。2014年２月27日、新たに設立された「中央網絡安全和信息化領導小組」(「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」の初会合が北京で開催され、「中央網絡安全和信息化領導小組工作規則」（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の工作規程)、「中央網絡安全和信息化領導小組弁公室工作細則」（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事務局の工作細則」)、「中央網絡安全和信息化領導小組 2014年の重要計画」など重要な文書が審議・承認された。習近平氏はこの会議の演説で、「サイバーセキュリティなくして国家安全なし」、「情報化なくして現代化なし」と指摘した。この発言はその後、サイバーセキュリティと情報化に関する国家戦略の策定において、「発展」と「安全」を両立させ、両方を考慮し推進するという基本原則を強調することとなった。 つまり、中国は近代的な強国になることを目指す一方で、サイバー強国も目指している。したがって、新たに設立された「中央網絡安全和信息化領導小組」が、サイバーセキュリティと情報化の発展のため、国家戦略を策定・実施し、サイバーセキュリティを保障する国の能力を絶えず強化・向上させ、社会全体の情報化レベルを引き上げるという基本責任を負うようになったのは当然のことである。

「中央網絡安全和信息化領導小組」の設立は、中国のサイバーセキュリティと情報化のプロセスが全体として調整され、推進されることを示すものである。これまでと異なり、「中央網絡安全和信息化領導小組」のトップは、国務院総理ではなく、党総書記となり、情報化にとどまらず、サイバーセキュリティも最重要の位置づけにされ、中国の最高指導・調整機関であることが明確になった（汪 2014)。これまで、中国の最高レベルに設置された３つの組織、すなわち「全面深化改革領導小組」（改革全面深化指導グループ)、「国家安全委員会」、そしてこの「中央網絡安全和信息化領導小組」は、いずれの管轄も国家戦略全般に関わり、最高の指導体制で計画・調整する必要があるため、すべて党総書記がトップに立ち、国務院総理が第一副首席に就任している。今回の「中央網絡安全和信息化領導小組」の新設は、もともと2012年の「国家情報化専門家諮問委員会」による提案、つまり「ダブルスパン方式」の実施によるものであり、党の中央委員会と国務院の両方に属する新組織として、最高の権威性を確保したのである。

胡錦涛氏は中国共産党第18回全国代表大会の報告で「海洋、宇宙、サイバー空間の安全保障に大きな注意を払い、……情報化された状況下で局地戦に勝つ能力を中核として、多様な軍事任務を遂行する能力を高める」ことを明確に提言した。その次に、習近平氏は中国共産党の第19回全国代表大会報告でも、インターネットコンテンツの建設を強化し、総合的なサイバーガバナンスシステムを構築し、サイバー空間の公序良俗を維持するだけでなく、技術革新を通じて「科学技術強国、品質強国、宇宙開発の強国、サイバー強国、

交通強国、デジタル中国、スマート社会」などの構築を強力に支援することを提案した。さらに「軍事のAI化発展を速め、サイバー情報システムに基づく共同作戦の実施能力、全領域作戦を行う能力を向上」することを宣言した。2018年4月20日から21日にかけて、「全国網絡安全和信息化工作会議」（サイバーセキュリティと情報化に関する全国会議）が北京で開かれ、習近平氏の演説では、サイバー強国を建設するという戦略思想が強く強調された。その5年後、さらに中国共産党第20回全国代表大会報告では、「新世代の情報技術の構築」、「モノのインターネットの発展の加速」、「デジタル経済の発展の加速、デジタル経済と実体経済の深い統合の促進」、「経済、主要インフラ、金融、インターネット、データ、生物、資源、核、宇宙、海などのセキュリティシステムの構築」などがより具体的な目標となった。また、強力な戦略的抑止能力を構築し、新しい分野・領域の戦闘部隊の比率を高め、無人AI戦闘部隊の開発を加速し、サイバー情報システムを構築・利用するとも明言した。

以上のように、サイバーセキュリティ国家戦略の策定を指導する中国指導部の方針には、高い連続性があることがわかる。2014年から現在に至るまで、中国はサイバーセキュリティの分野において、2016年に採択され2017年6月から施行された「中華人民共和国インターネット安全法」、2021年6月に採択され同年9月から施行された「中華人民共和国データセキュリティ法」、2021年8月に採択され同年11月から実施される「中華人民共和国個人情報保護法」など、サイバー情報社会の実態に対応した法令の制度整備をさらに強化するなど、一連の大きな進展を急速に遂げてきた。いうまでもなく、2016年、2017年に相次いだ「国家網絡空間安全戦略」と「国家網絡空間国際合作戦略」の公表もその流れの中に位置づけられるべきである。

Ⅳ．テキストの解読：「国家網絡空間安全戦略」の基本理念

世界各国のサイバーセキュリティ戦略に関する学者らの国別比較研究は、通常、各国の個別の特徴を強調する傾向があるが、諸国のサイバーセキュリティ戦略の全体性を軽視しがちであり、その戦略の根底的な論理や基本理念への追究に欠けることが多い。このような観点から、本節では、中国の「国家網絡空間安全戦略」の本文を深く読み解き、その論理を明らかにしたうえで、その基本的な考え方や理念を整理してまとめることを意図している。

1．「国家網絡空間安全戦略」の要点

「国家網絡空間安全戦略」は、序章と4つのセクションから構成されている。

序章では、サイバーセキュリティ国家戦略を策定する必要性と目的について論説してい

る。その必要性は、サイバー空間の安全保障が全人類共通の利益、世界の平和と発展、各国の安全保障に関わる問題であるだけでなく、中国が確立した国家目標、すなわちあらゆる方面で豊かな社会を築くための重要な保障であることにある。その目的は、サイバー空間の発展と安全に関する中国政府の立場を明確にさせ、国家のサイバーセキュリティの取り組みを導き、サイバー空間における中国の主権、安全、発展の利益を保護することである。この国家戦略の策定は、同時に、世界のサイバーガバナンスシステムの変革を推進する習近平氏の思想と「サイバー空間運命共同体」[4)]の構築という理念の実現であることに注目すべきである。さらに、サイバーセキュリティ国家戦略の策定は、サイバー空間における国家主権の意義を強調し、この分野における発言権を争う機会でもある（胡 et al. 2018）。

第一セクションは「機会と課題」であり、中国が直面する主要な機会と深刻な課題について包括的に分析し、サイバー空間の現状に対する中国の基本認識を表明している。機会については、サイバー空間が人々の生産と生活のあり方を変え、人間社会の発展過程に深い影響を与えたと論じている。「サイバー空間は情報発信の新しいチャンネル、生産と生活の新しい空間、経済発展の新しいエンジン、文化繁栄の新しい担い手、社会統治の新しいプラットフォーム」という表現は、主に国内の国民を対象としたもので、平易で理解しやすい表現である。注目すべきは、国家統治システムの近代化と統治能力を促進するネットワークの役割が強調され、政府情報のオープンな共有、政府の意思決定の科学化、民主化、法による支配、市民の社会管理への参加チャンネルの開放を促進すると主張している点である。同時に、サイバー空間はコミュニケーションと協力の新しい結節点であり、国家主権の「新しいフロンティア」でもあるとし、このような表現は国際社会に対するものである。中国政府は、サイバー空間における情報、資本、技術、人材などの流れのグローバル化により、世界が真の地球村になったと認識しているが、同時に国家主権もサイバー空間にまで拡大解釈し、サイバー空間における主権は国家主権の重要な一部となっていると訴えている。

課題については、政治的安全を危うくするサイバー侵入、経済的安全を脅かすサイバー工作やエスピオナージ、文化的安全を侵食する有害情報、社会的安全を損なうサイバーテ

4）2015年12月16日、第2回世界インターネット大会の開会式での基調講演で、習近平氏は世界のサイバーガバナンス体制の変革を進めるための「4つの原則」と、サイバースペースにおける人類運命共同体の構築に向けた「5つの提案」を打ち出した。4つの原則とは、サイバー主権の尊重、平和と安全の維持、開放と協力の促進、良好な秩序の構築である。5つの提案とは、相互の接続を促進するためにグローバル的なサイバーインフラの建設を加速すること、交流と相互評価を促進するためにオンライン文化交流・共有のプラットフォームを構築すること、共同繁栄を促進するためにIT経済の革新的発展を促進すること、秩序ある発展を促進するためにサイバーセキュリティを保護すること、公平と正義を促進するためにサイバーガバナンスシステムを構築することである。

ロ・攻撃や違法犯罪、サイバー空間での国際競争の激化など、サイバーセキュリティの現状はますます深刻になっている。特に、インターネットを利用した他国への内政干渉、大規模なサイバー監視や情報窃盗などの行為は、国家の政治的安全やユーザーの情報セキュリティを著しく脅かし、インターネットを利用した暴力的テロ活動の扇動、計画、組織化、実行などは国民の生命・財産の安全や社会秩序を直接脅かし、サイバー空間におけるコンピュータウイルスなどの拡散、詐欺、ハッカー攻撃、知的財産権の侵害及び個人情報の濫用・悪用などの不正行為は、国家、企業、個人の利益を著しく損ねている。また、欧米各国によるサイバー抑止戦略の強化とサイバー空間の軍拡競争の激化は、国際平和にも挑戦している。全体的な結論としては、機会と課題は共存しているが、機会は課題を上回っている。したがって、中国政府はサイバーセキュリティを維持しながら、サイバー空間が提供する発展の可能性を最大限に活用しなければならないと主張している。

第 2 セッションの「目的」では、サイバーセキュリティ国家戦略の目的は、「総体国家安全観」（国家安全保障全体構想）に導かれ、国内と国際、発展と安全といった二つ局面を統合し、サイバー空間の平和、安全、開放、協力、秩序を推進すると宣言している。国家主権、安全保障、発展の利益を守り、サイバー強国を構築することが全体的な目的である。

サイバー強国という全体目標は、さらに 5 つの小目標により構成されている。第 1 は平和：情報技術の悪用を抑制し、サイバー空間の軍拡競争など国際平和を脅かす活動に反対し、サイバー空間での紛争を防止する。第 2 は安全：サイバーセキュリティのリスクを制御し、国家のサイバーセキュリティを保障するシステムを改善・完成させ、安全で制御可能なコア技術・設備を所持し、インターネットと情報システムの安定的かつ信頼できる運用を実現し、サイバーセキュリティ人材の需要を満たし、社会全体のサイバーセキュリティに対する意識、基本的な保護スキル、インターネット利用に対する自信を向上させる。第 3 は開放性：情報技術の標準、政策、市場がオープンかつ透明性が高く、情報が円滑に輸送され、デジタルデバイドが解消され、各国、特に途上国が機会と成果を共有し、サイバー空間の統治に公正に参加できる。第 4 は協力：各国は技術の交流、サイバーテロやサイバー犯罪の撲滅、多国間で民主的かつ透明な国際インターネットガバナンスシステムの改善と完成、ウィンウィンの協力による「サイバー運命共同体」の形成などの分野で緊密に協力する。そして、第 5 の小目標に秩序あること：情報、参加、表現、監督の権利など、サイバー空間における市民の正当な権利と利益が保護され、サイバー空間における個人のプライバシーが守られ、人権が尊重される。また、秩序があるとは、法律に従ってサイバー空間を管理すること、すなわち、国内外の法制度、サイバー空間における行動の基準や規範が徐々に確立され、法律による効果的なガバナンスが実現されることである。

これら 5 つの目標は兼ねて、個人（インターネット利用者）と社会、そして国家と国際

的なレベルを考慮している。これら目標の設定と明確化は、中国の戦略が、発展と安全、国内と国際、市民の権益と公共利益のバランスを維持することなどに尽力する意思があることを示している。

第三セッションの「原則」において、中国は世界のインターネットガバナンスシステムの変革を提唱し、それを積極的に推進し、共同でサイバー空間の平和と安全を維持し、そのためにサイバーセキュリティに関する 4 つの原則を打ち出している。まず、サイバー空間の主権を尊重し、各国が独立してサイバー発展の道、サイバー管理のモード、サイバー公共政策などを選択し、国際ガバナンスへ平等に参加する権利を尊重する。各国は、自国の国情に応じ、国際的な経験に基づき、サイバー空間に関する法令を策定し、自国の情報システムおよびサイバー活動を自国内で管理し、国家の安全および利益を脅かす国内ネット上の有害情報の流布を防止、処罰するために、法律に基づき必要な措置をとる権利を有する。いかなる国も、サイバー覇権に関与したり、インターネットを利用して他国の内政に干渉したり、他国の国家安全保障を危うくするサイバー活動に関与、容認、支援したりしない。第二に、サイバー空間を平和的に利用し、『国連憲章』の武力行使または武力行使の威嚇を行わないという原則を順守し、情報技術が国際的な安全と平和に反する目的で利用されることを防止し、共同でサイバー空間における軍拡競争に抵抗し、サイバー空間における紛争を防止すべきである。また、国家の安全保障を口実に、他国のインターネットや情報システムをコントロールし、他国のデータを収集・窃取し、他国の安全保障を犠牲にして自国の絶対安全を求めることには反対である。第三に、法によるサイバー空間のガバナンスを行い、サイバー空間における法の支配を推進する。法に従ってインターネットを運営、アクセスし、秩序正しくサイバー空間の情報の自由な流れを守り、個人のプライバシーを守り、知的財産権を保護すべきである。第四に、サイバーセキュリティと発展を兼ねて調整し、セキュリティにより発展を確保し、また、発展によりセキュリティを促進する。

第 4 セッションの「戦略的任務」では、サイバー空間の主権を断固として守る、国家の安全を断固として守る、重要な情報インフラを守る、サイバー文化の建設を強化する、サイバーテロや違法犯罪を退治する、サイバーガバナンス体制を改善する、サイバーセキュリティの基盤を固める、保護の能力を強化する、サイバー空間における国際協力を強化するという 9 項目を挙げている。以下は、上記のタスクの一部である。

これらのタスクは、それぞれ詳細かつ具体的に記述されている。第 3 項目の「重要情報インフラの保護」を例にとると、まず「国家重要情報インフラ」の定義について、公共通信、放送、テレビなどを提供する基本的な情報ネットワークのほか、エネルギー、金融、交通、教育、科学研究、水利、工業製造、医療衛生、社会保障、公共事業などの領域およびその他の国家機関の重要情報システム、重要なインターネット運営システム（アプリ

ケーション）なども含まれるが、これらに限定されるものではない。サイバーインフラの定義は国によって異なり、中国には独自の特殊な定義がある。例えば、水力発電所や防災用堤防などの「水利施設」が含まれているのは、中国の伝統的な政治文化（治水）の影響によるものである。重要情報インフラとその重要データは国家の安定や国民の生活に関わっており、あらゆる必要な措置によって保護する必要がある（周＆汪 2013）ため、中国では検索サービスを提供する百度やネットビジネスを展開するアリババなど、一部のIT 企業の重要情報システムも保護対象と見なされている。公的機関から、従来の「重厚長大」産業[5]、個人情報や国民生活に影響を与えるインフラまで、すべてが含まれており、各国の定義を加味した上でも中国の定義はより広く一般化されたものである。次に、識別、保護、検出、早期警戒、対応、処置など様々な側面に及ぶ「重要情報インフラ保護制度」の構築と実施と重要情報インフラの保護を政府、企業、社会全体の共同責任として認識し、所轄官庁、事業単位や組織に対し、法律、規制、基準に従って重要情報インフラのセキュリティを守るために必要な措置を講じることを求める。さらに、政府、産業界、企業間でサイバーセキュリティ情報を秩序正しく共有する仕組みを構築すること、サイバーセキュリティの審査制度を構築し実施することなども求めている。

「国家網絡空間安全戦略」が掲げる 9 つの「戦略的任務」のうち、最初の 8 つは主に国内向けであり、サイバー空間主権の根本を守り、これをベースにサイバー空間の国内統制を実現することが戦略の核心である。明らかに、中国が想定するサイバーセキュリティ国家戦略の内的目的は、外的目的よりもはるかに重要である。内部的には、重要な情報インフラと重要なシステムのセキュリティを維持し、サイバー技術力を向上させ、サイバー空間における国益を守り、社会の安全と安定を促進するサイバーセキュリティの役割を重視し、サイバー情報の自由な流れによる社会的・政治的安定などの問題に焦点を当てることである（薄 2015）。

「国家網絡空間安全戦略」と「網絡空間国際合作戦略」は、それぞれ国内と国際の異なる次元を対象としているが、前者で提示された 9 番目の「戦略的任務」、すなわち「サイバー空間における国際協力の強化」が両者をつなぐ役割を担っている。この戦略タスクの目的は、サイバー主権の相互尊重を前提に国際的な対話と協力を強化し、サイバー空間におけるグローバルガバナンスシステムの変革を促進することである。もちろん、これは国内向けの 8 つの戦略的任務を国際レベルから支援するためでもある。サイバー空間の国家主権を標榜する一方で、サイバー技術は国境を越えるものであり、サイバー空間は国境を越えた情報発信やグローバルな共有といった特徴を持つことを認識し、したがって、すべ

5）鉄鋼、造船、石油化学、紡績、自動車などの「重厚長大産業」に対して、コンピュータ、自動的事務システム、情報機械などの「軽薄短小産業」があり、その製品の大きさや重さは対照的である。

ての国に受け入れられるサイバー空間に関する普遍的な国際ルールの策定を推進する必要があるため、政策・法律、技術革新、基準・規範、緊急対応、重要情報インフラ保護など様々な関連分野における国際協力を継続的に深めていく必要がある。すなわち、公正で合理的かつ民主的なグローバル・サイバー・ガバナンスシステムの構築に、自らの能力に応じて参画していくことが必要である。

2,「国家網絡空間安全戦略」を貫く基本理念

以上、「国家網絡空間安全戦略」の要点を簡潔にまとめたが、そこから以下のように、中国がサイバーガバナンスとサイバーセキュリティについて常に堅持し、特に重視してきた基本理念のいくつかを分析することができる。これらの理念は、中国がサイバー領域において追求する価値観であり、そこから中国がサイバー経済の発展を内部的に促進し、セキュリティの名のもとに統制を強化し、外部的なグローバル・ガバナンスで積極的なイニシアティブを発揮するといった行動の基本的な根拠を洞察することができる。

第一は、サイバー空間における国家主権の理念である。「国家網絡空間安全戦略」と「網絡空間国際合作戦略」はいずれも、中国が最も強く主張している「主権」の原則を重視している。「サイバー空間における主権の不可侵」とは、中国がサイバー空間の発展や管理のモデルを正当に選択し、その公共政策を独自に決定することを意味する。サイバー空間は伝統的な意味での「国家領土」とは異なるが、陸、海、空、宇宙と並ぶ「第 5 の空間」であり、『国連憲章』が定めた主権平等の原則は依然として適用されるべきであるとしている。したがって、サイバー空間における主権は従来の国家主権の自然な延長であり、平和的発展および今日の世界平和の保護と促進のための基本理念でもある。この理念に基づき、中国は国内のサイバー活動を管理し、国家の情報施設と情報資源の安全を守り、経済、行政、科学技術、法律、外交、軍事などあらゆる手段を講じて、インターネットを利用した国家主権を損なう行為に対抗してきた。また、中国は国外勢力がインターネットを利用して内政に干渉することに対する警戒を明確に表明し、国内の安定や国家の安全を維持するために必要な場合には、法律に従ってサイバー空間の利用を制限することの必要性を主張する。この姿勢はインターネットにおける「表現の自由」を主張するアメリカを中心とする欧米の立場（小宮山＆土屋2018）とは全く対照的であるため、国外からは批判の的となっている。しかし、グーグル事件の結果が示すように、この理念に関してはたとえ大きな経済的損失につながる恐れがあるとしても、妥協することはない。

サイバー空間における国家主権の主張は、中国の「サイバー空間観」が一部の欧米人学者が提唱する「グローバル・コモンズ」論とは異なることを示す。1996年、J. バルロー（J. P. Barlow）は「サイバー空間の独立宣言」（A Declaration of the Independence of Cyberspace）を提唱し、サイバー空間には主権が存在しない「心の新しい家」であるとし

た（Barlow 1996）。この見解は、後にヒラリー米国務長官によって「サイバーフリーダム宣言」として政治的に援用された。サイバー空間における覇権的な立場を維持するために、欧米のサイバー強国はサイバー空間を公海や宇宙空間と同様のグローバル・コモンズとみなし、どの国にも支配されておらず国家主権を主張できないとしている。しかし中国は、サイバー空間の越境的な性質は、サイバー空間に国家主権が存在しないという主張の根拠にはなり得ないと考えている。

中国がこの理念に固執するのは、それが多くの国、特に発展途上国の利益につながるという事実よりも、中国の社会的現実に基づくものである。中国社会は移行期にあり、政権の安定と国家安全が最大の関心事になっている。中国のネット世論には実際に欧米イデオロギーの影響拡大の痕跡が散見されることから（劉＆黄 2012）、政府はインターネットを使って欧米イデオロギーを宣伝したり、反中国勢力の中国に対するオンライン活動やそれを扇動したり、インターネットを使って中国の社会体制やイデオロギーを中傷したりするなどの動きに対して非常に敏感で、彼らを国家の安全に対する脅威であると見なし、これらは国家崩壊につながりかねない「カラー革命」の最初の兆候であると考えている。中国のサイバーセキュリティ国家戦略は、対外的にも対内的にも、この点への警戒感を強く反映している。

第二に、発展と安全保障を両立させる理念が特徴的である。サイバー空間における国家主権に加え、中国はサイバー空間の発展と安全保障上の利益も重視している。中国はすでに機会が課題を上回るという分析結論に達しており、論理的には、発展と安全の関係は発展が先であるべきであると、すなわち、「発展をもって安全を促進し、安全は発展を保障する」サイバー強国への道である（朱＆韓 2017）。中国はサイバーセキュリティを発展の観点から捉えており、セキュリティ問題で自らを閉ざすことはない。つまり、サイバー空間においては国家中心的な方向性（state-centric orientation）を追求しており、インターネットを利用して国家建設と発展を促進しつつ、その負の影響を最小限に抑えるというアプローチをとっている（Swaine 2013）。中国はインターネットと情報技術革命がもたらす機会を明確に理解し、それを国全体の発展の新たな原動力として捉えている。「国家網絡空間安全戦略」に確認された戦略的任務の 1 つは、サイバーセキュリティの基盤を固めることである。その焦点は企業を主軸に、革新的な技術によって経済・社会の発展を推進するための資源と努力を統括・調整し、サイバー経済を発展させる「インターネット＋」を実行することである。これは、産業基盤を固めるために、経済だけでなく、情報技術やサイバーセキュリティ企業も高いレベルで発展させることを意味する。国家情報化の発展なくして、サイバーセキュリティの保障は困難、というわけである。中国の公式見解では、情報化の発展は近代化を意味し、そのためには改革開放を堅持しなければならない。そして、サイバーセキュリティは国家の安全保障を意味し、発展と安全のバランスを統合して

計画する必要があることを強調している。

第三には、サイバー空間を管理するという理念である。これは法によるサイバー空間の統制を包括的に推進するための政府のさまざまなイニシアティブに反映されている。情報雑多のサイバー空間に対し、明確な法律法規なくしては、ガバナンスは極めて困難と言わざるを得ない。2023年3月16日、中国は「新時代的中国網絡法治建設」（新時代の中国サイバー法治の構築）という白書[6)]を発表した。白書では、サイバーガバナンスのための法整備、すなわち、法に従ってインターネットを管理・運営し、またアクセス・利用に関する政府の長年にわたるサイバー法制を構築する努力を包括的に述べ、サイバー空間が無法地帯にならないように維持してきた歩みを記録もした。サイバー空間は極めて複雑な「社会」であるため、法による空間の統治も社会全体の包括的なガバナンスと同様に、綿密な法制度の構築と改善を必要とする。例えば、法的規範の確立に加え、行政監督、業界の自主規制、技術的セーフガード、公衆の監督、社会組織の管理、社会教育などあらゆる手段を動員し、それらを互いに組み合わせ、包括的なサイバー空間のガバナンスシステムを形成する必要がある。

中国では、サイバー空間を管理する諸法規の主な責任は政府当局にあり、政府当局・関連部署は公共の利益と国家の安全を守る観点から業務を管理・維持するが、同時にIT企業も公的監督の下で業界の自主規制を行い、それぞれが運営・管理するプラットフォームで公開・発信される情報に対しても責任を負わなければならない。サイバー空間の構造的なガバナンスやデータのセキュリティを重視する欧米諸国とは対照的に、中国はサイバーインフラの安全や「情報のセキュリティ」を特に重視している。すなわち、サイバー空間における自由な情報の流れを保護し、インターネット利用者のプライバシーを守り、関連する知的財産権の保護にも力を入れる一方で、そうした自由を享受し、権利を行使する組織や個人は、法律を厳格に遵守し、オンラインでの言動に責任を持つことを強く求めている。中国のサイバー管制は言論の自由を制限すると批判する西側諸国に対して、中国はこのような批判を受けつけず、情報の自由な流通と国家安全保障といった公共利益との間で適切なバランスを取る必要性を強調し続けている。

第四に、「積極的防衛」という理念である。サイバー空間が国家主権の新たなフロンティアとして捉えられる中、サイバーセキュリティのため、保護能力を継続的に強化・向上させる必要があるのは言うまでもない。中国は、国際的な地位に見合った、サイバー強国レベルの技術的能力を構築し、サイバー侵入を適時に検知し防御する能力を開発する必要があると考えている。各国の戦略において、サイバー攻撃能力を明言する国も増えてき

6）国務院新聞弁公室が公式に発表したものである。紙面の都合上、中国のサイバー法制については別稿で取り上げる予定である。

ているが、中国の国家戦略では明確に言及されておらず、その防衛的な姿勢が伺える。他方では、サイバー攻撃のような現実の脅威に対応するため、中国も自国の防衛能力を強化しなければならず、その結果、抑止力や反撃能力の向上にも取り組み始めている。

サイバー中核技術が西側に握られ、重要な情報インフラも欧米に制限されていることが、中国のサイバーセキュリティの弱点とされ、大国間ゲームの激化の流れの中で、中国ではサイバー情報・データに関するセキュリティアラームが繰り返し鳴らされ、また攻撃にも面してきた。中国が重視する国内のサイバー空間コントロールは、国内で使用されるインターネット関連のチップ機器、OS、アプリケーションソフトウェアの大半が米国企業の製品であるため、最初からほとんど安全とは言えなかった。そこで、サイバー情報セキュリティの先端技術や基幹産業の育成を支援することが、国家戦略の主要な検討事項として盛り込まれている。

第五に、平和、共有、ウィンウィンな協力によるサイバー空間運命共同体のコンセプトである。サイバーセキュリティ問題は、世界すべての国が直面する共通の脅威であり、国際協力によって予防・対処する必要がある。中国は、すべての国がサイバー空間を平和的に使用し、情報技術が国際の平和、安全、安定に反する目的に使用されることを防止すべきであると提唱し、国際的協力のもとで軍拡競争に抵抗し、サイバー空間での紛争を防止することを希望する。中国は、ウィンウィンな協力関係による「サイバー空間運命共同体」の形成を望み、サイバー空間の利益の共有、平和利用、共通ガバナンスを積極的に推進することを提唱している。

「国家網絡空間安全戦略」は国内のインターネット政治に焦点を当て作成されたが、中国政府はサイバー空間における国際協力について、特に国際社会を対象として「網絡空間国際合作戦略」を別に作成した[7)]。中国の目標は、サイバー空間のグローバル・バナンスにおいて国家間の対等な関係を追求し、サイバー主権という理念に導かれながら、欧米諸国との対等な地位を求めることである。中国は、国の規模、強弱、富や貧困にかかわらず、すべての国、特にグローバル・サウスが、サイバー空間のグローバル・バナンスに公平に参加し、サイバー空間の発展によってもたらされる機会と成果を共有できるようにすべきであると提唱している。

Ⅴ.「国家網絡空間安全戦略」に導かれた取り組みの実践

「国家網絡空間安全戦略」の目標は、そのために設定された戦略的タスクの遂行を通じて達成される必要があり、これらのタスクを一つずつ実施・完了するためには、より多く

7）紙面の都合上、中国の「網絡空間国際合作戦略」については別稿で取り上げる予定である。

のサブタスクや具体的なイニシアティブに分解する必要がある。サイバーセキュリティ国家戦略の目的を達成し、サイバー空間における様々な現実的・潜在的脅威に対処するために、政府は経済、行政、科学技術、法律、外交、軍事などあらゆる手段を講じることを表明している。もちろん、国家戦略が導入される前から実施されていた具体的な取り組みもあり、関連する実践が事実上、サイバーの安全保障に関する国家戦略の裏付けとなっていることを示している。また、国家戦略が出来た後に、その任務として徐々に実践され始めているイニシアティブも多くある。サイバーセキュリティ国家戦略が空言化していないのは、こうした取り組みや実践のおかげであると言えよう。その多種多様な取り組みを一つ一つ整理するのは大変な作業だが、以下のように重要かつ継続的な実践活動とその成果をまとめることができる

1，サイバー統制に関する法律法規体系の強化

2015年7月1日、第12期全国人民代表大会常務委員会第15回会議で採択された「中華人民共和国国家安全法」第25条は、「国家は、インターネット及び情報セキュリティ保障システムを構築し、インターネット及び情報セキュリティの保護能力を高め、インターネット及び情報技術の革新的研究開発及び応用を強化し、インターネット及び情報のコア技術・重要インフラ・重要分野の情報システムおよびデータを安全かつ制御可能にする。同時にインターネットの管理を強化し、法律に基づいてサイバー攻撃、サイバー侵入、サイバー窃盗、および違法・有害情報の流布などのサイバー犯罪を防止、阻止、処罰し、国家のサイバー空間における主権、安全と発展の利益を保護する」と定めている。「サイバー主権」という概念が法律で正式に導入されたのはこれが初めてで、国家主権と不可分なものとされている。その後、2016年11月7日に第12期全国人民代表大会常務委員会第24回会議で「中華人民共和国法インターネット安全法」が採択され、サイバー主権と国家の安全保障を守ることが立法目的として明示された。わずか1ヵ月後、中国政府は「国家網絡空間安全戦略」を発表し、「インターネット安全法」とサイバーセキュリティ国家戦略が密接な関係にあることを示し、前者は後者の法的バックボーンとしての役割を担っているとした。

2023年3月に公表された白書「新時代の中国サイバー法治の構築」は、中国のサイバー法整備がゼロからスタートし、次第に体系化した歩みを概説した。中国がインターネットに接続されていた1994年から1999年の期間には、関連法規は主にインフラのセキュリティ、すなわちコンピュータシステムやそのネットワークのセキュリティに焦点を当てていた。2000年から2011年にかけて、コンピュータネットワークが普及し、コンピュータユーザーが増え、インターネット情報サービスが急速に発展すると、関連法規は徐々にインターネットサービスの管理とコンテンツの管理に重点を置くようになった。2012年、

中国がモバイルネットワークの時代に入ると、関連法規は、ネットワーク情報サービス、情報開発、サイバーセキュリティなど、総合的なサイバー統制に及ぶ傾向を見せ始めた。現在までに中国は、140以上の関連法、行政法規、部門別法規、地方法規を導入し、コンテンツの開発と管理、サイバーセキュリティと情報化など専門化した法規をバックボーンとするサイバー法体系を形成し、それら法律・法規の全体性、相乗性、適時性を継続的に高めてきた。

「インターネット安全法」を中心に形成されたサイバー法体系は、国家サイバー情報部門がサイバーセキュリティと関連する監督における統括などの役割や、インターネット上の実名、情報公開、情報発信、データ保存に関する運営企業の法的責任などを明確にし、通信プライバシー権、表現の自由、知的財産権を強化するとともに、サイバー空間における名誉権と個人情報に関する権利などの法的権利や利益の保護を強化している。例えば、2019年以降、中国は合計322万件のモバイルインターネットアプリケーションのテストを完成し、約3000件の違法・非適合アプリケーションを通報または取り下げさせた。こうした取り締まりにより、個人情報に関する違法・非正規な収集・利用やユーザーの個人情報権侵害などが強く抑制された。

2，ファイアウォールの構築

サイバー空間における情報セキュリティを監視・管理する基本的な技術手段や安全対策として、中国は1990年代からいわゆる「グレート・ファイアウォール」の建設を徐々に強化してきた。セキュリティへの考慮に基づいて、ファイアウォール技術は事実上「イントラネット」と「パブリックネットワーク」の間に障壁とブロックを形成することにより、イントラネットユーザーの情報とデータ伝送のセキュリティを保護し、起こりうるサイバー攻撃やイントラネットへの侵入・盗難などを防止する。

サイバーセキュリティ問題の複雑化に伴い、中国でも公安関連の技術・設備の改新が続いており、ファイアウォールに関連するインターネットセキュリティ技術も著しく発展している。インターネットを通じて国家権力を転覆させ、国家の安全を損なうあらゆる行為に対抗する目的で、中国はファイアウォール技術を使って、国外からの有害な情報を選別、遮断、傍受し、「中国のインターネット」と「国際インターネット」の間に差異を作り出してきた。中国がこの技術を使ってネット情報の検閲、選別、遮断などを行っていることに対して、米国を中心とする欧米諸国は、ネット情報の自由な流れを損なうことや表現の自由が侵害されるとして中国を批判し続けているが、中国は主権国家が国内のインターネットを統制するための正当な措置であり、当然の正当性を持っていると考えている。国外からのサイバー攻撃や有害情報、さらにはネット世論を操作して国家安全を脅かすカラー革命を引き起こす可能性もあることから、中国の国内インターネット統制は、

Google 事件や香港暴動の経験を踏まえ、簡単にファイアウォールを放棄することはないだろう。また、この問題をめぐる攻防は続き、「ファイアウォール」と「ウォール」を克服する技術の両方が、相互作用的に発展していくことが予測される。こうした中国政府の努力が相互性を強める情報のハイウェイの発展の前に無力なのではないか（Healy 2007）、またはこのような排他的な政策が実は国内のインターネット関連技術や産業の発展を間接的に助長しているのか（Quan 2022）、議論が分かれるところである。

国家全体を包み込むファイアウォールの設置は、いわば国家主権に基づくサイバー空間の「境界線」や「国境」を敷くことを意味しており、米国政府はこの点において徐々に認識を改め、サイバー空間における自国のインフラに対して国家主権に基づく保護を行使しており、その現実主義的姿勢を反映している（塩原 2015）。

3，「浄網」行動（クリーンネット・キャンペーン）

2013年以降、中国はほぼ毎年「ネット掃除」と言われるようなキャンペーンを開催している。「浄網2013」（クリーンネット2013）は、「全国『掃黄打非』工作小組弁公室」（国家ポルノ・違法撲滅作業グループ事務局）が展開する特別キャンペーンである。「掃黄打非」（ポルノや違法との闘い）とは、文化市場の管理および国家の文化的安全や秩序を維持するために使われている作業用語で、様々なポルノ関係の書籍・オーディオ・ビデオ製品、違法な出版物やわいせつ情報などを排除することを指す。加えて、憲法に違反して社会の安定を損なうもの、国家の安全を脅かすもの、国家分裂を扇動するものや海賊版などあらゆる違法出版物と戦うことも意味する。サイバーセキュリティの観点からみれば、「浄網」は同時にサイバー空間の情報コンテンツを包括的に検閲するプロセスでもある。

2014年以降、「浄網」作業の多くは、「全国『掃黄打非』工作小組弁公室」、「国家互聯網信息弁公室」、工業・情報化部、公安部などの政府機関が共同で企画・実施するようになった。キャンペーンの基本的な内容は、国内インターネット上のわいせつ・ポルノ情報を全面的に削除し、それらを制作、複製、出版、販売、配布する企業や人員を法律に基づいて対処し、必要に応じて刑事責任を追及することである。違法なウェブサイトを閉鎖または禁止し、行政許可を取り消すことに加え、IT 企業も主な責任を負うことが求められている。例えば、ネットワークサービス企業には自己点検を要求し、自ら有害な情報やリンクを浄化し、情報セキュリティ管理システムを厳格に実施し、コンテンツの審査とゲートキーピングを改善し、猥褻情報の拡散防止の技術措置を採用することが挙げられる。「インターネット安全法」およびその他の関連法律に違反した場合、企業の法定代理人または責任者は法律上の責任を負う。監督を怠り、わいせつ・ポルノ情報を生産・流布し、社会的に悪影響を与えた場合、関連業界監督部門、行政許可認可または申請部門の責任者は法律および規律に従って責任を負う。

近年、「浄網」キャンペーンはしばしば他のサイバー犯罪、例えばオンライン詐欺、オンライン賭博、偽情報、個人情報の違法窃盗、公序良俗に反する各種の映像・情報、世論強要、ネット水軍[8)]、麻薬・銃器の違法取引、爆発物などの対策にまで拡大されてきた。政府は、現在も進行中の浄化活動を通じて、サイバー空間の秩序および情報の流通を基本的に掌握しようと努めている。この過程では、もちろん海外サイトからのわいせつ・暴力的な情報、民族分裂やカラー革命を助長するような情報もブロックし、抑制してきた。

中国政府にとって「浄網」は、サイバー空間における国家主権の行使であり、サイバーセキュリティ国家戦略や「インターネット安全法」の具体的実施でもある。したがって、こうしたキャンペーンは、常にその年のサイバーイベント記録の一つに選ばれる。しかし、それらが表現の自由を危うくし、人権問題を伴うものとして批判される。サイバー空間で得られる複雑な情報を取捨選択することは実に難しく、中国と他国のイデオロギー対立もあって、この問題はさらに複雑になっている。

4，「中国国家網絡安全宣伝周」（中国国家サイバーセキュリティ啓蒙週間）

「サイバーセキュリティを構築し、サイバー文明を共有する」ために、「中央網絡安全和信息化領導小組弁公室」（サイバーセキュリティ・情報化中央指導グループ事務局）は、2014年11月下旬、金融、通信、電子政務、電子商取引などの分野・業界を中心に、一般向けに第1回「中国国家サイバーセキュリティ啓発週間」を開催した。例えば、「党・政府機関のウェブサイトの統一ロゴキャンペーン」、「サイバーセキュリティ知識クイズ」、「サイバーセキュリティ専門家へのインタビュー」、「サイバーセキュリティ講演会」、「身近なサイバーセキュリティを感じ取る公開体験展示」など、国民の関心が高い話題について一連の広報活動や啓発が相次いで行われた。ちょうど2014年は「中央網絡安全和信息化領導小組」が設立され、サイバーセキュリティが国の重要な戦略課題に格上げされた最初の年でもあった。

以来、2022年まで9回にわたり、「中国全国サイバーセキュリティ啓発週間」は年1回開催されている。そこでは毎回異なるテーマを設定し、そのテーマに沿ったさまざまな活動が展開されている。例えば、2015年6月に開催された第2回では、金融デー、通信デー、政務デー、科学技術デー、法治デー、青少年デーなど複数のテーマ・デーが設定され、公開体験展示、青少年サイバーセキュリティ知識コンテスト、全国サイバーセキュリティ広報作品コンテストなどの活動に加え、サイバー犯罪対策に関する講演、電子認証サービス

8）網絡水軍（ネット水軍）とは、インターネット上の「サクラ」行為、あるいはその行為を行っている組織である。だれかに雇われた多数の人びとが、ネット上で特定のコメントや発言にフォローアップし世論を誘導する投稿などは、中国国内のインターネットにおいて問題を引き起こしてきた。

応用に関するセミナー、金融サイバーセキュリティ知識に関する講演、国民のサイバーセキュリティ意識の現状に関する調査報告書の公表など、実践的な活動が行われた。

2016年の第3回以降、毎年9月に開催されることがほぼ決められている。第3回と第4回のテーマは「人民のためのサイバーセキュリティ、人民によるサイバーセキュリティ」で、期間中はサイバーセキュリティ業界のリーディングカンパニーである「騰迅安全」（Tencent Security）が多くの企業と手を組み、さまざまなサイバーセキュリティ技術を紹介した。同時に、「中国信息安全評測中心」（中国情報セキュリティ評価センター）とテンセント（騰迅、Tencent Holdings Ltd.）は、国家情報セキュリティ防衛システムの構築、情報セキュリティ技術フォーラムの開催と専門家育成、ユーザーセキュリティと「浄網」業務、情報セキュリティ業界標準の策定など、多くの分野で包括的協力関係を確立していった。これらの活動はすべて、サイバーセキュリティ国家戦略の具体的な実施と言える。また、第3回啓発週間に開催された「サイバーセキュリティ技術サミット」では、米国、ロシア、フィンランド、韓国などから業界人や専門家を招いたことも特筆に値する。

2018年の第5回、2019年の第6回では、より専門性の高い「サイバーセキュリティEXPO」が開催された。特に第6回では、「インターネット安全法」ならびにデータセキュリティ管理および個人情報保護に関する法律、法規、基準の実施に焦点を当て、新聞、ラジオ局、テレビ局、ウェブサイトなどの広報チャンネルだけでなく、展示、フォーラム、知識・技能コンテスト、公益広告など、さまざまな方法を通じて企業、メディア、社会団体および一般市民を動員し、幅広い参加を実現した。2022年9月に開催された第9回では、「サイバーセキュリティサミットフォーラム」など通常のプログラムに加え、軍におけるサイバーセキュリティをテーマに取り上げ、軍営におけるサイバー文明の構築、軍人のサイバーリテラシー向上、軍のサイバーセキュリティに対する防御線の構築、軍関連のサイバー環境の改善などの活動を行った。

「中国国家網絡安全宣伝周」は毎年、各都市でリレー形式をとって開催され、中国におけるサイバーセキュリティに関する公衆教育の最も重要なプラットフォームとなり、誰もがサイバーセキュリティの主体であるという雰囲気の形成を促進している。

5，「インターネット＋」行動計画

インターネット技術は国家経済発展と社会情報化の加速や国防・軍事情報化において重要な役割を果たしている。優れた産業発展モデルの確立も中国の情報化発展の目標の一つであるため、2015年から中国は「インターネット＋」行動計画を強力に推進し、クラウドコンピューティング、ビッグデータ、モノのインターネット（IoT）、モバイルインターネットを様々な伝統産業と融合させ、新しい産業モデルや情報化社会の発展を推進している。

「インターネット＋」とはすなわち「インターネット＋伝統産業」のことで、伝統産業がインターネットのプラットフォームを活用し、インターネットを伝統産業と深く融合させ、新たな発展機会を生み出すことである。「インターネット＋」は、伝統産業のアップグレードと変革を助け、すべての社会・経済の主体を若返らせ、急速に発展する情報社会に適応することを可能にする。さらに、インターネットは社会資源の配分において最適化と統合の役割を果たすと考えられており、経済社会のあらゆる分野にネットワーク技術を統合することで、社会全体のイノベーション力を高めることができる。「インターネット＋」のコンセプトは、もともと伝統的な企業をインターネットの力を借りてアップグレードすることを目的としていたが、それだけに留まらず、無数の中小企業がインターネットを導入するようになった結果「全民創業」（普遍的な起業）が促進され、ネット起業のプロジェクトが急増している。

2012年11月に開催された「第5回モバイルインターネットEXPO」で、ネットビジネスの経営陣が「インターネット＋」のコンセプトを初めて紹介し、大きな反響に及んだ。2014年11月、李克強氏は第1回「世界互聯網大会」で、インターネットは大衆創業・創新の新しい道具であり、中国経済をレベルアップさせる新しいエンジンであると指摘した。2015年3月、全国人民代表大会の代表馬化騰氏は、中国の経済・社会の革新と発展を促進する原動力として「インターネット＋」にかかわる建言書を提出したが、この年の3月5日の第12期全国人民代表大会第3回会議で、李克強氏は政府業務報告で初めて「インターネット＋」行動計画を提案し、モバイルインターネット、クラウドコンピューティング、ビッグデータ、モノのインターネットなどを現代製造業と融合させ、電子商取引の推進、工業インターネットやネット（ITFIN）などの健全な発展を図った。2015年7月4日、国務院は「『インターネット＋』行動の積極的推進に関する指導意見」を発表し、「インターネット＋」行動の全体目標として、2018年までに、インターネットと経済社会の各分野との融合を深め、インターネットを利用した新ビジネスを経済成長の新たなエンジンとし、また、公共サービスを提供する重要な手段とし、ネット経済と実体経済との相乗効果と相互作用の発展モデルを形成させることなどを提案した。同時に、起業とイノベーション、共同製造、現代農業、スマートエネルギー、インクルーシブな金融、国民向けサービス、物流、電子商取引、交通、グリーンエコロジー、人工知能など、合わせて11の重要分野で「インターネット＋」での相乗効果を目指すアクションが定義されている。

その直後、工業・情報化部は国務院の指導を受け、工業・情報化部の行動計画（2015–2018）を発表し、2018年までにデジタル化、ネットワーク化、そしてインテリジェンスのレベルを大幅に向上させ、ハイエンドな設備の現地化率を大幅に高め、重点産業のスマート工場を多数建設し、インテリジェント製造のパイロット実証プロジェクトを200項目育成し、重点産業における「工業インターネット」の初期応用を実現させるなどを企画

した。また、今後数年間でインフラを大幅に改善し、ブロードバンド、ユビキタス、セキュアな次世代国家情報インフラを構築し、「インターネット＋」へのサポート能力を全面的に強化しようとしている。同計画では、光ファイバーネットワークが完備された都市を多数完成させること、都市と村落を4G ネットワークで完全にカバーすること、行政村の80％以上に光ファイバーアクセスを実現させること、中央直轄の主要都市と省都でブロードバンドユーザーに平均30Mbps のアクセスレートを確保させることなどを求めている。高性能コンピュータ、大容量記憶装置、ネットワーク通信機器、セキュリティ・保護製品、インテリジェント端末、集積回路、フラットパネルディスプレイ、ソフトウェア、情報技術サービスなどの分野で大きな飛躍があり、独自のイノベーション能力を持つ国際的な有力企業が多数出現することが期待されている。

2015年12月、第 2 回「世界互聯網大会」で「インターネット＋フォーラム」が開催され、「中国互聯網発展基金会」と百度（Baidu）、アリババ（*Alibaba* Group Holding Limited）、テンセントなどの大手 IT 企業が共同で「中国インターネット＋同盟」を設立した。2016年、教育部と国家語言文字工作委員会が発表した「中国語言生活状況報告（2016年）」において、「インターネット＋」という言葉が流行語のトップ10の 1 つとして挙げられた。2020年 5 月22日、李克強氏はさらに政府業務報告で「インターネット＋」を総合的に推進し、中国のデジタル経済における新たな優位性の形成を促進することを明言した。

中国の「インターネット＋」行動計画とその結果をどう評価するかは難しい。しかし、より確かなこととしては、例えば、既存の社会・経済構造、地縁関係と文化の構造、権力・言説の構造などが絶えず形を変えており、その結果中国社会が急速に変化していることである。「インターネット＋」政務サービスは、政府の作業手順や行政組織を変えつつあり、「インターネット＋」社会管理は、サイバーガバナンスの文脈において国内政治における重みを増している。2019年以降のコロナ危機は、さらにオンライン教育、オンラインオフィス、オンライン医療、オンライン政務などの推進剤となった。「インターネット＋」構想の影響で、中国はインターネットマインドを持つ新世代を形成しつつある。ただし、「インターネット＋」は試行錯誤の過程であり、発展の過程で多くの疑問が生じることは言うまでもない。例えば、金融業がオンライン企業に取って代わられるかどうか、あるいはどの程度取って代わられるかは、真剣に検討しなければならない問題の一つである。

6，「中国互聯網大会」と「世界互聯網大会」

中国はインターネットを新たなハイテク情報技術産業として捉え、支持し、業界団体組織という形で国家情報化・サイバー空間発展戦略を推進するなど、IT 産業政策の面に注

力してきた。「中国互聯網協会」（中国インターネット協会）は2001年5月25日、国内のIT企業（インターネット事業者、ネットサービスプロバイダー、ネット機器メーカー、システム開発者など）と科学研究機関、教育機関、社会団体など70社以上が自主的に結成した非営利団体である。その目的は、IT業界の交流と協力のプラットフォームを構築し、インターネットの応用と普及、インターネットによる公共の福祉を促進し、業界に自主規制を行わせ、会員、業界のみならず、ネットユーザー、政府にも対してサービスとサポートを提供することである。民間組織ではあるが、工業・情報化部、国家互聯網信息弁公室、国家発展改革委員会、文化部、教育部などの政府部門の支援を受けており、政府、社会、学術、企業の橋渡し役として重要な役割を担っている。

2002年11月25日から27日にかけて、「中国互聯網協会」は初めて「中国互聯網大会」（中国インターネット会議）を開催した。それ以来年1回、2022年までに計21回開催され、今や中国のIT業界では最も有名な業界会議となっている。会議ごとにテーマが異なり、例えば、2003年第2回のテーマは「インターネットの透視、e時代に向けて」[9]、2016年第15回のテーマは「繁栄するインターネット経済、インターネット強国へ」で、2022年の第21回のテーマは「デジタル経済の発展とデジタル文明の推進」であった。「中国互聯網大会」の主なテーマは、国家の情報化やIT産業の発展を大義名分とすることが常だが、サイバーセキュリティや個人情報・データの保護なども含まれる。例えば、2019年第18回では、5G[10]、IPv6[11]、人工知能、金融技術、オンライン教育、サイバーセキュリティとガバナンス、知的財産保護、オンライン詐欺対策、個人情報保護、ウェブサイト開発などのサブテーマで30ものサブフォーラムが設けられていた。2019年はインターネット誕生50周年であり、中国が国際インターネットにアクセスするようになって25周年でもあったことから、同会議では「中国のインターネットアクセス25周年」をテーマにした特別展示が開催された。

「中国互聯網大会」は主に国内の業界会議であるが、これと対になる「世界互聯網大会」（世界インターネット会議、World Internet Conference、略称WIC）もあり、こちらは国内外からの来場者に開放されている。「世界互聯網大会」国際組織は、2022年7月12日に正式に設立され、北京を拠点に中国で登録された国際組織である。世界移動通信システム協会（GSMA）、中国国家計算機網絡応急技術処理協調中心（中国国家コンピュータネットワーク緊急対応技術調整センター）、中国互聯網絡信息中心（中国インターネット情報セ

9） e時代とは電子時代であり、eはelectronicの略称である。
10）5Gとは Fifth Generation Mobile Communication Technology の略で、「第5世代移動通信技術」のことである。
11）IPv6は Internet Protocol Version 6の略で、ネットワークアドレスのリソース不足の問題を解決するためのものである。

ンター)、アリババ、深セン騰訊コンピュータシステム有限公司、浙江之江実験室など 6 単位が主導し、グローバルな議論の共有のプラットフォームを構築し、国際社会が情報化時代のデジタル化、ネットワーク化、インテリジェンス化の流れに対応し、安全保障上の課題を共に解決し、発展の利益を共に求め、サイバー空間における国際交流と協力を深め、サイバー空間における運命共同体を構築することを目的とする。中国政府が支援し、IT 企業、業界団体、関連国際機関、個人の専門家や学者が自主的に結成したこの国際組織とその活動は、中国が世界インターネットの発展とサイバーガバナンスに積極的に参加するためのイニシアティブであり、ある意味で中国のサイバーセキュリティ国家戦略第 9 項の戦略的な課題の具体化である。

2014年に浙江省烏鎮で第 1 回「世界互聯網大会」が開催され、その後、年次会議である「烏鎮サミット」(World Internet Conference Wuzhen Summit、略称 WIC Wuzhen Summit) が 9 年連続で開催されてきた。毎回80以上の国や地域から1,000人以上の代表が参加している。「烏鎮サミット」には毎回テーマがあり、第 1 回は「互聯互通、共享共治」(インターネットを通じて交流しあい、サイバー空間を共有しともにガバナンスに参加する) であったが、2015年第 2 回烏鎮サミットは「互聯互通、共享共治―サイバー空間における運命共同体を共に築く」(Connectivity - Shared Governance - Building a Community of Destiny in Cyberspace) をテーマに掲げていた。その後は毎回「サイバー空間における運命共同体を共に築く」という副題がつけられ、「世界互聯網大会」の恒久テーマとなっている。このことからも、サイバー空間のグローバル・ガバナンスに対する中国の「解決策」が、基本的には全当事者の合意形成、共有ガバナンスの追求、デジタル分野での協力の継続的深化、サイバー空間における運命共同体の構築に向けられたものであることが伺える。

「烏鎮サミット」は、しばしばオンラインとオフラインのセッションを組み合わせて開催され、世界のサイバー空間の発展に関する焦点となる話題が当てられた。各セッションでは、国際的なサイバーガバナンス、オンラインメディア、国境を越えた電子商取引、サイバーセキュリティ、サイバーテロとの戦い、サイバーと持続可能な発展、オンラインの的財産保護、技術革新など、さまざまなテーマでサブフォーラムや対話が開催されてきた。毎回、サミットは程度の差こそあれ何らかの成果を上げており、例えば2015年の第 2 セッションでは「ハイレベル専門家諮問委員会」が設立され、「烏鎮イニシアティブ」「インターネット金融発展報告」「『インターネット＋貧困緩和』の共同イニシアティブ」「『デジタルシルクロード』建設に関する宣言」などが発表された。2016年の第 3 回では、情報技術、情報インフラ、サイバーセキュリティ、インターネット金融などの分野をカバーする 6 つの機能エリアからなる「インターネットライト博覧会」を立ち上げた。2017年の第 4 回では「中国互聯網発展報告2017」と「世界互聯網発展報告2017」を発表し、中国と海外の大手 IT 企業の最先端技術成果も集中的に発表した。2017年以降、「世界互

聯網大会」青書は継続的に発表され、重要な研究成果として、徐々に各国から広く注目されるようになった。2020年の第7回サミットでは、「サイバー空間における運命共同体を共に築くための行動イニシアティブ」を発表し、国際社会に20のイニシアティブを提示し、デジタル、ネットワーク、インテリジェント発展の機会を捉え、サイバー空間リスクの課題に積極的に取り組むための共同努力を呼びかけ、グローバル・ガバナンスにおける中国の使命感を示した。さらに、2021年の第8回サミットでは、「サイバー空間で運命共同体を共に築く」実践事例集を収集し、「2021年サイバー空間で運命共同体を共に築く事例集」をリリースした。

2019年の第6回サミットにおいて、サイバー主権の概念と原則を明確に定義し、関連する実践プロセスを体系的に説明した成果文書『サイバー主権：理論と実践』を発表したことは特筆に値する。この文書では、サイバー主権はサイバー空間における国家主権の自然な延長であり、その意味は独立、平等、管轄、防衛などの権利を含むと明言している。その後、2020年-2021年の第7回、第8回では、国連憲章で定められた主権平等の原則をサイバー空間に適用することを提唱し、その適用における各国の具体的な原則と実践を述べた『サイバー主権：理論と実践』の2.0版と3.0版が相次ぎ発表され、さらに国際法におけるサイバー主権の属性を詳しく説明し、サイバー主権に基づくより包括的な国際協力の枠組みを提案している。

「世界互聯網大会」は、中国自身のイニシアティブにより構築されたグローバルなサイバーの共有やガバナンスのプラットフォームであると同時に、国際協力の推進に関するサイバーセキュリティ国家戦略の規定を具体的に実施するものである。また、国際的なサイバー空間に関する舞台で発言権を得ようとする中国の努力と試みでもある。

7，関連調査報告書のタイムリーな公開

1997年11月、中国互聯網絡信息中心（CNNIC）は、第1回「中国互聯網絡発展状況統計報告」（中国におけるインターネットの発展状況に関する統計報告）を発表し、以来、半年ごとに定期的に報告を発表する慣例を形成してきた。2023年3月2日、CNNICの第51回統計報告発表では、2022年12月時点で中国のインターネットユーザー数が10億6700万人に達し、前の年より3549万人増加し、インターネット普及率は75.6％に達したことが明らかとなった。「中国互聯網絡発展状況統計報告」は中国におけるインターネットの発展データに関する最も権威ある報告書であり、中国政府の年次統計報告書に掲載されるだけでなく、国連や国際電気通信連合でも採用される調査データを提供している。

中国互聯網協会が主催し（後にCNNICと共同作成）、2003年から毎年1巻ずつ公刊してきた『中国互聯網発展報告』は、現在までに20巻連続で刊行されており、中国のインターネットビジネス発展の軌跡と成果を詳細に記録し、国内外に中国インターネットの全

体像を体系的に理解させることに貢献している。最近発表された『中国互聯網発展報告(2022)』によると、2021年末時点のデータとして、中国は142万5000の5G基地局を完成・開設し、世界最大の5Gネットワークを構築した。また、中国は情報技術分野で3万以上のPCT国際特許を出願し、その数は世界の3分の1を占めた。中国の「5G＋産業用インターネット」は1,800のプロジェクトが建設中で、鉄鋼や電力など国民経済の主要産業の多くをカバーしている。中国のデジタル経済は45兆5千億元に達し、総額で世界第2位となった。中国のサイバーセキュリティ産業とサイバーセキュリティサービス市場は急速に発展し、産業規模は約20025億元、成長率は15.8％となった。

こうした報告書の順次作成と公表はサイバーセキュリティの領域でも見られる。2001年8月、中国は工業・情報化部の指導のもと、主にサイバーセキュリティの監視、早期警戒、処理に従事する国家計算機網絡応急技術処理協調中心（国家コンピュータネットワーク緊急対応技術調整センター、CNCERT、CNCERT/CCとも呼ばれる）を設立した。2004年以来、同センターは毎年、受信、監視、処理したサイバー攻撃やセキュリティ脅威などの情報に基づいて「CNCERT網絡安全工作報告」を作成、発表している。2008年には、通信業界の関連部門からのデータをまとめた上で、「中国互聯網網絡安全報告」（中国インターネットサイバーセキュリティ報告書）と改称した。その後、工業・情報化部通信保障局およびセキュリティ緊急対応専門家グループの指導のもと、2010年から毎年『互聯網網絡安全態勢総述』報告書（インターネットネットワークセキュリティ状況概要報告）を作成・公開しており、国内外から注目されている。中国のインターネット産業に関する情報は、同国の他の分野や産業に比べて比較的透明性が高く、さまざまな研究報告や成果文書をタイムリーに公開することで、国の情報化、サイバー空間の発展、さらにはセキュリティに関する国家戦略の国民理解と協力に役立っている。

これらは、中国がサイバーセキュリティ国家戦略を実施するために行ってきた比較的明白な取り組みの一部に過ぎない。実際には、これ以外にも多くの具体的な実践がある。例えば、eID技術[12)]を利用してサイバー空間における本人認証の問題を解決することは、信用社会の確立を促進し、サイバー空間における個人のプライバシーを保護する際に役立つ。また、『未成年者網絡保護条例』(「サイバー空間における未成年者の保護に関する条例」[13)]の立法プロセスが促進され、サイバー空間における未成年者の正当な権利と利益を保護し、未成年者がサイバー空間で被害を受けることを防ぐ。サイバーセキュリティ人材プロジェクトを実施してその分野の学術研究を強化し、国家サイバーセキュリティのサ

12）eIDとは、電子IDカード識別のことで、eID技術は電子ID識別技術とも呼ばれる。中国では、「公安部公民網絡身分識別システム」が応用されている。

13）2022年3月、国家互聯網信息弁公室は「サイバースペースにおける未成年者の保護に関する条例（意見募集案)」について、さらなる意見募集・パブリックコメントの告知を行った。

ポート体制を向上させるなどである。

VI. 終わりに

中国のサイバーセキュリティ国家戦略の形成過程、基本理念および様々な具体的実践を整理したことで、2014年は中国が国際インターネットにアクセスしてから20周年という年とも重なり、非常に重要な時点であることが分かった。2014年 4 月15日、習近平氏は中央国家安全委員会第 1 回会議で、「国家安全保障全体構想」を初めて表明した。すなわち、内部安全と外部安全を両立させ、内部の安全保障は発展、変革、安定を追求し、平和な中国を築くことを目指し、外部の安全保障は平和、協力、互恵的関係を追求し、調和のとれた世界を築くことを目指すことである。また、伝統的安全保障と非伝統的安全保障をともに含めて、政治、国土、軍事、経済、文化、社会、科学技術、情報、エコロジー、資源、核の安全保障などを一体化委し、完全な国家安全保障システムに統合する。さらに、発展と安全は両立し、安全のために発展を犠牲にすることも、発展のために安全を犠牲にすることもないというものであった。同年、中央網絡安全和信息化領導小組の第 1 回会議では、「サイバー強国」の建設が初めて国家戦略目標として掲げられた。

その後、2015年に採択された「中華人民共和国国家安全法」では、「国家安全保障全体構想」を核心とするだけでなく、同法第25条では「サイバー・情報セキュリティ保障システムの構築とサイバー・情報セキュリティ保護能力の強化」に関して明確な規定が設けられている。これは、サイバーセキュリティ国家戦略と国家安全保障全般との間に深い相関関係があり、サイバーセキュリティが中国の国家安全保障全般において重要な位置を占め、国家安全保障全体構想と高度に統合されていることを裏付けるものである。同法第14条に基づき、中国は毎年 4 月15日を「全民国家安全教育日」と定め、毎年この日になると、サイバーセキュリティに関する国民教育といった内容のイベントが催されるようになっている。

当然のことながら、2016–2017年に中国が「国家網絡空間安全戦略」と「網絡空間国際合作戦略」を策定したのは、こうした国内政治の大きな動きの中でのサイバー空間分野における「国家安全保障全体構想」の実施と実践のためである。その目的は、サイバー空間の安全保障と発展における中国の国益が最大化されることである。中国のみならず、世界各国の国家安全保障におけるサイバーセキュリティの重要性は著しく高まっており、今日の世界における国際関係やグローバル・ガバナンスの方向性に影響を与える最重要課題の一つとなっている（孟 2014）。

中国のサイバーセキュリティ国家戦略は、政府のサイバー安全保障に対する考え方や目標、サイバー安全保障に対する脅威とそれに対処するために必要な資源、政策、メカニズ

ムに関する基本的判断など、含蓄に富んでいる。中国のサイバーセキュリティに関する理念は、基本的に「国家安全保障全体構想」をサイバー空間の分野に援用したものである。サイバーセキュリティから得られる利益とそれに対する脅威についての基本的判断も、主に国益を守り、国家全体の発展目標とその道筋を確保する必要性に基づいている。中国のサイバーセキュリティ国家戦略が活用できる資源は情報技術および関連資源のほか、より広い意味での自然資源、人的資源、経済資源、社会資源、軍事資源を指している。

現在の中国政府にとって、発展と安全保障は最も重要な課題であるため、国内では情報流通の規制と管理を含むサイバー管理を強化し、社会と政治の安定を確保するためにあらゆる努力を行っている。外部では、サイバー空間の国家主権を強化し、サイバー攻撃をはじめとした外からの影響を抑止するためにあらゆる努力を行っている。中国は、サイバー空間における競争力を徐々に高めながら、そこにおける国際的なグローバル・ガバナンスに積極的に参加し、国際協力によってサイバー空間の平和と発展を目指すと謳っている。

また、中国のサイバーセキュリティ国家戦略の体系的な研究を通じて、いくつかの問題があることもわかった。例えば、サイバーセキュリティ対策と空間の開放性のバランスをどうとるか、情報の自由な流れや新しい情報技術の進歩を妨げずに公序良俗に反し国家の安全を脅かす情報を排除できるかなどである。国家安全の定義が広すぎると、サイバー空間における情報の選別や判断が厳しくなるおそれがある。米国や民主主義制度を誇る欧米諸国も同様な問題に直面しているが、これらの面で中国は絶えず国内外からの圧力に晒されていることもまた事実である。

つまり、中国は世界の主要国と同様に、サイバー空間の安全保障に関する国家戦略文書を策定し、適時公表することで、関連する問題に対する自らの立場、理念、姿勢、関心領域、主張を国際社会にオープンしているが、それらすべてがただの国内外へのプロパガンダではない。そのサイバーセキュリティ国家戦略の分析を通してこそ、サイバー空間の安全保障をめぐる中国社会の国内政治論理と政策実践を深く理解することができるだけでなく、中国の国際サイバー空間ガバナンスへの参加と自らの立場に基づく貢献の可能性も理解できる。中国を含む世界の主要国により、透明性の高いサイバーセキュリティ国家戦略が策定・公表され続けることが、サイバー空間におけるグローバル・ガバナンスのさらなる発展に寄与することは間違いないだろう。

参考文献

薄澄宇 2015 『網絡安全與中美關系』、中共中央黨校2015年度博士論文
蔡翠紅 2019 「中美網絡空間戰略比較：目標、手段與模式」、『當代世界與社會主義』2019年第 1 期
胡麗、齊愛民、何金海 2018 「國家網絡空間主權戰略（學者建議稿）」、『河北法學』2018年第 6 期
劉勃然、黃鳳誌 2012 「網絡空間國際政治權力博弈問題探析」、『社會主義研究』2012年第 3 期

孟威 2014 「網絡安全：國家戰略與國際治理」、『當代世界』2014年第 2 期
沈逸 2013 「以實力保安全，還是以治理謀安全？ ——兩種網絡安全戰略與中國的戰略選擇」、『外交評論』2013年第 3 期
汪玉凱2014 「中央網絡安全和信息化領導小組的由來及其影響」、『信息安全與通信保密』2014年第 3 期
惠志斌 2012a 「新安全觀下中國網絡信息安全戰略的理論構建」、『國際觀察』2012年第 2 期
—— 2012b 「我國國家網絡空間安全戰略的理論建構與實現路徑」、『中國軟科學』2012年第 5 期
—— 2013 『全球網絡空間信息安全戰略研究』、中國出版集團／上海世界圖書出版公司
張彬、彭書楨、金知燁、隋雨佳、谷寧 2019 「『大智物雲』時代數據治理國家戰略比較分析—數據開放、網絡安全保障與個人隱私保護」、『電子政務 E-GOVERNMENT』2019年第 6 期
朱莉欣、韓曉陽 2017 「基於機遇和挑戰，謀略發展和安全——比較中解讀《國家網絡空間安全戰略》」、『信息安全與通信保密』2017年第 2 期
周琪、汪曉風 2013 「網絡安全與中美新型大國關系」、『當代世界』2013年第11期
小宮山功一朗・土屋大洋 2018 「サイバーセキュリティ戦略の国際比較—目的と対象範囲に基づく四類型—」、『グローバル・ガバナンス』、2018巻 4 号
塩原俊彦 2015 「サイバー空間と国家主権」、『境界研究』No. 5 (2015) pp. 29–56
周橋 2020 「中国におけるインターネットの発展と Google 中国撤退騒動をめぐる米中間の摩擦」、*ICCS Journal of Modern Chinese Studies* Vol. 13, No. 1: 12–34
須田祐子 2015 「サイバーセキュリティの国際政治—サイバー空間の安全をめぐる対立と協調—」、『国際政治』第179号
東浩紀 2011 『サイバー空間はなぜそう呼ばれるか』、河出書房新社
Adrian Mihalache, A. (2002). “The Cyber Space-Time Continuum: Meaning and Metaphor.” *The Information Society: An International Journal*, Vol. 18, No. 4: 293–301
Azmi, R., Tibben, W., and Win, K, T. (2016). “Motives behind Cyber Security Strategy Development: A Literature Review of National Cyber Security Strategy.” *Australasian Conference on Information Systems 2016, Wollongong* https://www.researchgate.net/publication/308470260_Motives_behind_Cyber_Security_Strategy_Development_A_Literature_Review_of_National_Cyber_Security_Strategy
Betz, D, J, and Stevens, T. (2017). *Cyberspace and the State: Toward a Strategy for Cyber-Power*. Routledge
Buchanan, B. (2017). *The Cybersecurity Dilemma: Network Intrusions, Trust and Fear in the International System*. Hurst & Co Publishers Ltd
European Union Agency for Cybersecurity. (n.d.). *National Cyber Security Strategies (NCSSs) Map* https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map
Government of Canada Publications. (2010). “Canada’s Cyber Security Strategy: For a Stronger and More Prospective Canada”. https://publications.gc.ca/site/archivee-archived.html?url=https://publications.gc.ca/collections/collection_2010/sp-ps/PS4−102−2010-eng.pdf
Gustav Lindstrom, G. (2012). “Meeting the Cyber Security Challenge.” *GCSP Geneva Papers Research Series No 7*
Healy, S. (2007). “The Great Firewall of China.” *Social Education*. Vol. 71, No. 3: 158−163
John Perry Barlow, J, P. (1996). “A Declaration of the Independence of Cyberspace.” *EFF* https://www.eff.org/cyberspace-independence
Luiijf, E., Besseling, K., and De Graaf, P. (2013). “Nineteen National Cyber Security Strategies.” *International Journal of Critical Infrastructures*. Vol. 9, No. 1−2: 3−31
Michael D. Swaine, M, D. (2013) “Chinese Views on Cybersecurity in Foreign Relations.” *China Leadership Monitor*, No. 42
Min, K., Chai, S., and Han, M. (2015). “An International Comparative Study on Cyber Security Strategy.” *International Journal of Security and Its Applications*, Vol. 9, No. 2: 13–20
NATO CCDCOE. (2013). “National Cyber Security Strategy Guidelines.” https://ccdcoe.org/library/publications/national-cyber-security-strategy-guidelines/
OSCE. (2013). “Decision No.1106 Initial Set of OSCE Confidence-Building Measures to Reduce the Risks of

Conflict Stemming from the Use of Information and Communication Technologies."
http://www.osce.org/pc/109168

Quan, E. (2022). "Censorship Sensing: The Capabilities and Implications of China's Great Firewall Under Xi Jinping." *Sigma: Journal of Political and International Studies*. Vol. 39, No. 4: 19–31.

The White House. (2009) *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure*. US Government Printing Office

—— (2011). *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World*. National Security Archive
https://nsarchive.gwu.edu/document/20843-04

World Economic Forum. (2017). *The Global Risks Report 2017 12th Edition*. World Economic Forum