博士論文 2020 年度

サイバーセキュリティのグローバル・ガバナンス

慶應義塾大学大学院政策・メディア研究科

小宮山功一朗

主　論　文　要　旨

No.1

報告番号	甲　乙　第　　号	氏　名	小宮山 功一朗

主 論 文 題 目：

サイバーセキュリティのグローバル・ガバナンス

（内容の要旨）

サイバー空間はその誕生以来、支配者が存在しなかった。経済活動、政治活動、軍事活動の多くがサイバー空間で繰り広げられる時代となり、サイバー空間をアナーキーのまま放置するリスクが高まっている。この空間を統治するメカニズムが希求されている。本論文はまだ見ぬ統治のメカニズムの前提として、現代のサイバー空間を、「情報拡散国家」と「情報支配国家」と「グローバルテックカンパニー」の 3 アクターによる、より多くのデータにアクセスするための競争というモデルを通して分析する。サイバー空間に統治のシステムが成立するためには、秩序の前提となる共通の価値が必要である。3 アクターは自らの立場を有利にする共通の価値観を、サイバー空間に敷衍しようとしている。情報拡散国家は民主主義的なサイバー空間を、情報支配国家は国家主権が確保されるサイバー空間を、グローバルテックカンパニーはグローバリゼーションが担保されるサイバー空間を作り上げようとしている。3 アクターの競争は、「民主主義」「国家主権」「グローバリゼーション」という 3 つの価値のコンペティションという側面を持つ。「グローバルで民主主義的に運営され、なおかつ国家の主権が認められるサイバー空間」は成立しないとすれば、サイバー空間の統治は、その有るべき姿について 3 つの価値のいずれか 2 つを選択するところから始められなければならないのである。この状況は、とりわけ情報拡散国家に厳しい選択を迫る。情報拡散国家はサイバー空間における民主主義を放棄できない。したがって、グローバルなサイバー空間、国家主権が確保されるサイバー空間のどちらかを諦めなければならない。本論文を通して検討するサイバーセキュリティ確保のための国際的な合意、セキュリティインシデント対応のための組織の現状は、グローバルテックカンパニーの急速な台頭と、サイバー空間におけるグローバリゼーションの後退を示唆している。

キーワード：サイバーセキュリティ，グローバル・ガバナンス，グローバリゼーション，国家主権, CSIRT

Thesis Abstract

No.

Registration Number:	□ "KOU" □ "OTSU" No. *Office use only	Name:	KOMIYAMA, Koichiro

Title of Thesis:

Global governance in the Cyberspace

Summary of Thesis:

Since its birth, Cyberspace has never had a dominant power structure. However, in an era where economic, political, military and intelligence activities are conducted in Cyberspace, the risk of leaving it in a state of anarchy is increasing. There is a clear and growing need for a mechanism to govern this space. In exploring the development of governance mechanisms, this paper begins from the premise that in modern Cyberspace, three actors namely "info-diffusion states", "info-control states" and "global tech companies" contests with each other to obtain access to the physical and logical terrain of accessing data. A system of power alone does not bring it. Common values are fundamental prerequisite and each of these three actors are working to spread a common set of values for their advantage in Cyberspace. Info-diffusion states are trying to create a democratic cyberspace, info-control states are looking to ensure state sovereignty, and global tech companies are seeking to make it flat and global. The competition between these types of actors embody the competition of three values: "democracy", "sovereignty of the state" and "globalization". This possess a trilemma where any approach to the governance of Cyberspace can only embody one or two of these fundamental values. This trilemma poses a difficult decision especially for Info-diffusion states, as they are not allowed to abandon the value of democracy in Cyberspace. Therefore, there must be a compromise on either the conceptualization of a global Cyberspace or moving toward a cyberspace where national sovereignty is secured. Through the assessment of international agreements and the status of organizations that respond to security incidents, this paper demonstrates that these circumstances have resulted in a retreat of globalization in Cyberspace.

Keyword: Cyber Security, Global Governance, Globalization, CSIRT, state sovereignty

目次

図表目次

第 1 章　序

第 1 節　アナーキー・イン・ザ・サイバースペース

今日のサイバー空間は、単に人々の日々のコミュニケーション手段以上の役割を果たしている。それは、電気や水道やガスなどのインフラの神経であり、あらゆる経済活動の土台であり、軍事活動の新領域であることに議論の余地はないだろう。

歴史を振り返れば、国際関係の変容を迫る技術は、絶え間なく生み出されてきた。火薬、飛行機、潜水艦、ミサイルと核兵器、宇宙技術は、その一例である。情報を伝達する技術に限定しても、アルファベット、活版印刷、腕木通信、電信、テレビなどを挙げることができる。これら既存の技術革新と我々の目の前にあるサイバー空間には、大きな違いが存在している。

まず、サイバー空間は情報の双方向のやり取りを前提としている。テレビなどの放送局から一方的に情報が提供されるモデルと異なり、サイバー空間においてコンテンツを提供しているのはユーザ自身である。そして、サイバー空間はまたたく間に我々の生活の一部となった。インターネットが実用化されてから、僅か 30 年で世界を席巻した。多くの未来学者や情報学者はこのサイバー空間の特質に着目し、市民同士が相互に情報を交換する機会を増やし、情報の自由な流通がもたらされ、情報格差が是正され、やがて「世界にバラ色の民主主義社会をもたらす」と予測した。

サイバー空間の重要性が広く理解されるに連れ、そのセキュリティ、つまりサイバーセキュリティは複雑な社会問題となっていった[1]。サイバーセキュリティの確保は容易

[1] 世界経済フォーラムが主導する世界的な重大リスクに関する調査の結果を例にとれば、サイバー攻撃は異常気象、自然災害、大規模不随意移民、テロリストによる攻撃につぐ 5 番目に大きなリスクとされている（World Economic Forum 2017）。

でない。たびたび指摘される要因は、以下のようなものである。

第一に、サイバー空間の土台ともいえるインターネット技術が、現在も急速に進歩しているということである。クラウドサービスやIoT（モノのインターネット）[2]やブロックチェーンを用いた暗号通貨、量子暗号などの技術は、新たな攻撃手法や新たな脆弱性を生み出す。

第二に、サイバーセキュリティ対策とサイバー空間の開放性の適切なバランスが求められることである。自由な情報の流通を阻害することなく、技術革新を妨げることなく、公序良俗に反する情報だけを、インターネット上からとりのぞくことは難しい。とりわけ民主主義体制の国においては、サイバーセキュリティ対策は開放性や自由な情報の流通と安全性の両面へのバランスの取れた配慮が求められる。

第三に、インターネットやサイバー空間の多様な利害関係者（ステークホルダー）の存在が挙げられる。サイバーセキュリティを確保するためには国内の関係組織、民間事業者、教育機関などの連携が不可欠である。意見の集約、合意形成は容易ではない。

第四に、国家自身がサイバー攻撃の実行者となっている事実がある。2014年11月に発覚したソニー・ピクチャーズエンタテイメント社へのサイバー攻撃による社内メールの暴露事案、2015年6月に政府職員約2150万人の個人情報が漏えいした米国人事管理局へのサイバー攻撃、そして2016年2月にバングラデシュ中央銀行がサイバー攻撃を受けて約8100万米ドルの不正送金の被害にあった事案などは、すべて国家による関与が疑われている[3]。インテリジェンス機関、軍隊のサイバー担当部門の機能強化が進められ、インテリジェンス活動における情報技術の重要性が高まった。国家は近隣諸国

---

[2] 従来インターネットに接続されるのはパソコンやスマートフォンといった情報機器に限定されていたのに対し、例えば冷蔵庫や炊飯器などの生活家電や車などあらゆる「モノ」が接続されインターネットを構成している現状をInternet of Things（IoTまたはモノのインターネットなどとも）と表現する。

[3] 他に国家の関与が強く疑われるサイバー攻撃は、2007年から2019年までで少なくとも32件確認されている（Tikk et al. 2019）。

からのサイバー攻撃の脅威を感じながら、単に防御に専念するのではなく、自らの安全を確保するために攻撃を行うようになったのである[4]。

このような背景をふまえ、サイバー空間の統治と管理の仕組みを模索する議論は、発展の途上にある。既存の研究に繰り返し指摘されるように、現在のサイバー空間には、中央管理の仕組み、サイバー戦争の定義（河野 2015）、秩序や弱者救済の仕組み（Buchanan 2017）、ルールのエンフォーサー（Raymond 2016）が存在しない。そしてサイバーセキュリティのガバナンスを目指す様々な議論の場が確立していない[5]。「傘ではなくパッチワーク」（Choucri, Madnick, & Ferwerda 2014）、「レジームコンプレックス」（Nye 2014）と表現されるように、議論の場が乱立し重複している。

現代のリアリストの多くが国際関係の基本的前提をそう捉えるのと同様に、本論文では、国際関係の視点から見るサイバー空間は、国家より上位の権威や権力、つまりは君主や支配者を持たないアナーキーであると捉える[6]。経済活動、政治活動、軍事活動の多くがサイバー空間で繰り広げられる時代となり、サイバー空間をアナーキーのまま放置するリスクが高まっている。この空間を手懐けるメカニズムが希求されている。

---

[4] ベン・ブキャナン（Ben Buchanan）は攻撃と防御の境界が明確にできないサイバー空間において国家は「防御指向の侵入行為（defensive-minded intrusion）」あるいは「積極的防御（Active Defense）」などの攻撃活動を行う強いインセンティブを持つことを論じている（Buchanan 2017）。

[5] 2019 年に NGO によって実施された、150 以上の政府・インターネット企業・技術コミュニティ・市民社会・学術研究機関そして国際機関へのインタビュー調査の結果を引用する。まず回答者の 95%が、インターネットをめぐる国境を超えた法制度の問題が向こう 3 年でより先鋭化すると予想した。回答者の 79%は国際的な調整の不足を自覚している。その一方で、問題に対処する組織や議論の場が存在していると考えるのは 15%にとどまった（the Secretariat of the Internet & Jurisdiction Policy Network 2019: 2）。統一された議論の場は不在である。

[6] 土山（2014: 44）によればアナーキーには 2 つの意味があるという。1 つめは支配者が不在の状態。国際社会においては国家より上位の権威や権力、つまり中央政府のない状態である。もう 1 つは混沌、無法、無秩序状態のことである。本論文においては前者を意味する。

第２節　より多くのデータにアクセスする力

アナーキーなサイバー空間を統治する手段を模索する作業を始める前に、サイバー空間における力、言い換えればサイバーパワーについて触れておかねばならない。国際政治の研究において繰り返し論じられてきたことだが、「パワーの意味は多義的で、その定義も一様ではない」（土山 2014: 384）、そしてパワーに単一の定義はできない。「定義は必ずその人の利益と価値観を反映する」（Nye 2010: 2）からである。

サイバーパワーは、これまでの代表的な研究では「サイバー空間を利用して、他の作戦空間における優位な立場を作り出したり出来事への影響を与える能力」（Nye 2010: 4）や「あらゆる情報を使いこなす能力の集合」（Kramer et al. 2009: 559）などと定義されてきた。前者は、サイバー空間の部分を宇宙や深海に置き換えてもそのまま通用しそうな汎用的な定義である。逆に言えばサイバー空間の特質を捉えていると言い難い。後者は情報を保持するだけでなく、活用することの重要性を捉える定義である。しかし、情報を使いこなす能力は、保持するデータの量に比例する。例えば、動画配信サービスのネットフリックス（Netflix）社がユーザを引きつけるのは動画のおすすめアルゴリズムの精度という情報を使いこなす能力の高さゆえとされてきた。ところが近年の研究で明らかになったのは、精度の高い推薦のアルゴリズムの開発には大量のコンテンツとユーザが生みだすデータが不可欠ということである（Hindman 2018: Chapter 3）。情報を使いこなす能力と同等かそれ以上に情報にアクセスできることが重要である。

以上を踏まえて、本論文ではサイバーパワーを「より多くのデータにアクセスする力」と定義する。サイバーパワーを持つアクターは、多くのデータにアクセスすることができ、そのデータを用いて情報を使いこなす能力を高め、他者の行動に影響を与える。

「この世界が情報を燃料に走っていることを、今の私たちは知っている。情報は血液であり、ガソリンであり、生命力でもある」（グリック 2013: 13）と表現されるように、

情報が価値を生む世界に我々は生きている。その世界で、個人が、企業が、そして政府が、日々生成される大量のデータへのアクセス権を巡る争奪戦を行っている。データは人（ヒト）を呼び、データは金（カネ）を呼び、データはさらなるデータを呼ぶ。こうしてサイバー空間において、データが少数の者の手に独占されていく。

より多くのデータにアクセスする力を得るための手段は大きく 3 つに分けることが可能である。1 つ目は、技術やテクノロジーを用いる方法である。サイバー攻撃によってデータを盗んだり、通信の経路上で強制的に監視を行ったりする。2 つ目は経済に頼る方法である。多くの企業が、地図や E メールやスケジュール管理などの便利なサービスを無償で提供する対価として、ユーザのデータを受け取るという経済活動を通じてデータを得ている。3 つ目は共通の価値観によって実現するデータへのアクセスである。価値観は常識や正義と言い換えても良い[7]。新型コロナウィルス（COVID-19）感染症の世界的流行は、個人が自らの位置情報を広く共有することが社会の利益になるという新たな価値観を生み出した[8]。このような新たな常識はデータへのアクセス権を巡る争奪戦を大きく変える可能性を持つ。

サイバーパワーの移ろいを論じるために、我々は技術や経済だけでなく、国際社会が

---

[7] 国際政治学者の高坂正堯は国家間の関係を力の体系、利益の体系、価値の体系という 3 つのレベルの複合物として捉えた（高坂 1966: 260）。平和の実現にはその 3 つのレベルでそれぞれ複雑に絡み合った国家関係を検討する必要があるという主張である。サイバーパワー、すなわちより多くのデータにアクセスする力もまた、技術によって、経済によって、共通の価値観によってもたらされる。技術を力と読み替えれば力の体系、利益の体系、価値の体系という 3 つのレベルでのデータにアクセスする競争が進行しているとも言える。

[8] 新型コロナウィルス（COVID-19）感染のコントロールを目的として、ウイルス感染者に接触した可能性のある人物を特定する仕組み（コンタクトトレーシング）の技術開発が行われている。位置情報を国が所有するデータベースに登録するという方式やグーグル社とアップル社のように Bluetooth 通信を使用した、個人情報を収集しない、よりプライバシーに配慮した方式などがある。これまで第三者に位置情報を提供することを拒否していた者も含め、より多くの人が受け入れるのはどの方式か、経過を見守りたい。

どのような価値を共有していくかに注意を払う必要がある[9]。サイバー空間における価値の体系を、言い換えればそれぞれのアクターが実現しようとしているサイバー空間の姿を描き出さずに、サイバー空間の秩序を語ることはできないのである[10]。

第３節　先行研究の課題

ここで改めて先行研究の課題そして本論文の学術的貢献について述べたい。サイバーセキュリティのガバナンスは、つまりいかにサイバー空間に秩序をもたらすかという社会的関心事項は、主にインターネットガバナンス論、そして安全保障論・国際関係論の2つのエリアで検討されてきた。

第１項 インターネットガバナンス論におけるサイバー空間

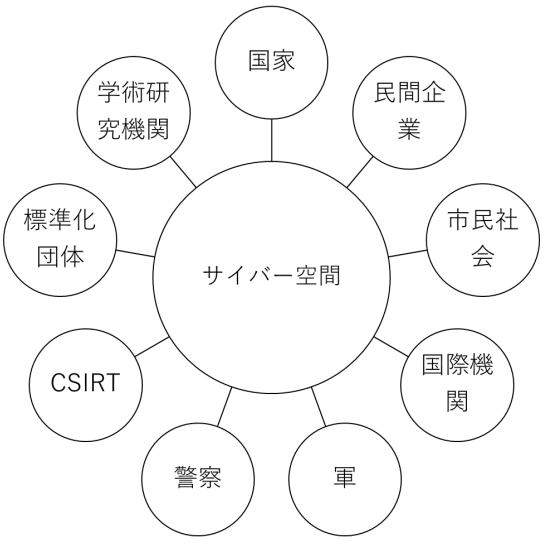
インターネットガバナンス論は文字どおり、インターネットをいかに統治していくかを検討する学問である。純粋な学問というよりは実務の中に見いだされた現象の理論化の性格が強い。インターネットガバナンスを論じる際に、その中には「インターネット資源管理」、「標準の策定」、「サイバーセキュリティガバナンス」、「相互接続に関する合意形成」、「情報仲介の政策的役割」、「システム化された知的財産保護」という6つのサブアジェンダがあるというのが、この分野の泰斗である米国の研究者ローラ・ディナル

---

[9] ガバナンスの前提としての「価値の体系」は現代の国際政治学にも引き継がれている。篠田英朗は「国際秩序の探求とは、まずもって国際社会を構成する原則あるいは価値規範の探求から始められなければならないのである」（篠田 2007: iv）と表現し、細谷雄一は「国際社会を構成している諸国間で、はたしてどの程度価値が共有されているかによって、国際秩序の安定性も異なる」（細谷 2012: 22）とし、表現を変えつつも、基本的な考え方が踏襲されていることを窺わせる。

[10] 高坂はまたこうも言っている。「しかし、共通の価値体系が育ちさえすれば、それで秩序ができるわけではない。やはり権力による強制がなくてはならない。正確に言えば、権力による強制の支えがなければ共通の価値体系も育たない」（高坂 1966: 1654）。力の体系と価値の体系は相互に補完する関係にある。

ディス（Laura Denardis）の分析である（Denardis 2015）。インターネットの統治方法を検討するプロセスの一部分として、インターネットにおけるサイバーセキュリティをいかに確保するかという研究が行われてきた。インターネットガバナンスの文脈でサイバーセキュリティが論じられる場合に、そこに一種の暗黙の前提がある。それは問題を「官・民・市民社会の対等な参加」で解決するという前提である。マルチステークホルダリズムとよばれるインターネット管理の原則である。次に示す、図表 1-1 はマルチステークホルダリズムを重視した際の、サイバー空間のガバナンスのイメージ図になる。



図表 1-1 インターネットガバナンス論におけるサイバー空間のイメージ

官・民・市民社会の対等な参加という一面的には受け入れられやすい構造であるが、これには 2 つの批判を加えることができる。1 つめは多様なアクターによるガバナンスが、科学技術分野などの先端領域では難しいことである。サイバー空間という現在も変容を続ける世界の統治の仕組みを、市民社会と軍隊と大手 IT 企業が同じ量の知識を持って議論することは難しい。派生する問題は、多様なアクターの分散されたパワーの集合が、結局の所、既存の力関係（パワーダイナミクス）を強化してしまうという点であ

る[11]。つまり、多様なアクターによるサイバー空間のガバナンスの議論は、結局のところ、強者をさらに強くし、弱者をさらに弱くする。

2 つめの批判はサイバーセキュリティとインターネットガバナンスの違いである。サイバー空間は言論活動のプラットフォームであるだけでなく、あらゆる生活の土台となっている。サイバー空間になにかトラブルが起きれば、その影響で多くの人間の生命や安全が損なわれる。ここで我々は「人間は自由だけを希求するわけではない」（Kagan 2019b）ことに自覚的でなくてはならない。インターネットガバナンス論は身体の安全、家族の安全、民族の安全、宗教の安全は言論の自由と同等に重要であることに正面から向き合ってこなかったという批判は成立する。サイバーセキュリティはインターネットガバナンスに内包される 1 つのサブアジェンダではない。セキュリティが確保されて初めて相互に接続する必要性が生まれるのである。

インターネットガバナンス論におけるマルチステークホルダリズムは、特に冷戦崩壊後のリベラルな国際秩序が求められた時代にマッチしていた。リベラルな秩序が維持されるにはいくつかの前提が必要となる。強者（大国）が抑制的な行動を取ることもその一つである。米国の国際政治学者ジョン・アイケンベリー（John Ikenberry）は「現代の秩序の維持を担う、米国には抑制戦略に携わるユニークな能力がある」（Ikenberry 2001: 271）と主張した。アイケンベリーの見立ては、サイバー空間において明確に裏切られた。一例を示せば、米国のインテリジェンス機関や軍隊は、サイバー空間においてその支配的な立場を利用して、大規模なサーベイランス活動を行っていた。後述するスノーデン事件により、2013 年にその事実が公になった。サイバー空間をめぐるリベラルな

[11] Carr（2015: 3）は、マルチステークホルダーガバナンスの特に技術分野のガバナンスへの適性を認めつつも、根源的な問題点として多様なアクターの分散されたパワーの集合が、結局の所、既存の力関係を強化してしまうことをあげた。具体的に言えば富めるものがさらに富む構造であるという指摘である。この構造によって米国と米国のプライベートセクターは利益を甘受していると Carr は言う。

秩序はそこで一度終止符を打たれた。サイバー空間の管理の政治性が改めて認識され、インターネット冷戦（Mueller 2013）、デジタル冷戦（Kleinwachter 2013）、インターネットのヤルタ体制（Klimburg 2013）など、大国間のパワーゲームを連想させるキーワードを使ってサイバー空間が論じられるようになった。以来、インターネットガバナンスの研究者らは理論の再構築を続けているが、その出口は見えていない。

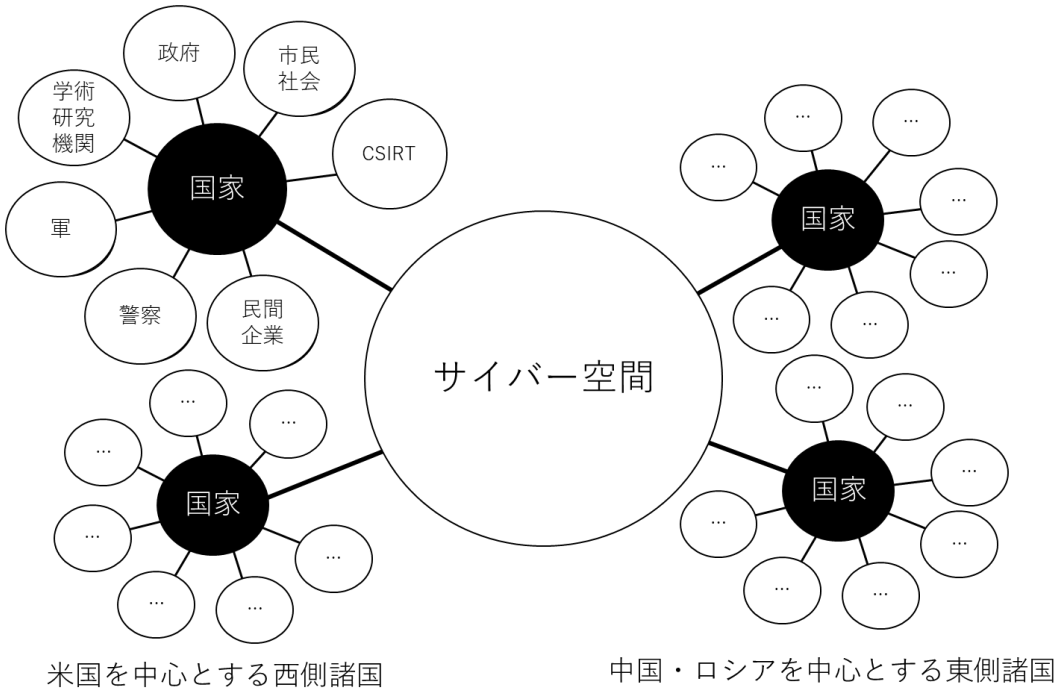
第２項 国際関係論におけるサイバー空間

サイバー空間におけるリベラルな秩序が損なわれる以前から、国際関係論や安全保障論におけるサイバー空間の研究は、国際機関や政府組織の戦略・能力・責任の分析に多くの時間を費やしてきた[12]。サイバー空間は陸・海・空・宇宙に続く「第 5 の戦闘空間」であると言われることも多い。既存の戦闘空間を支配してきた論理を振り返り、応用するのは自然な流れである。研究者たちは程度の差こそあれ、「国際的なパワーの源泉は武力であり、政府が武力行使の唯一のエージェント」（Lewis 2018: 2）と捉えた。そしてサイバー空間のガバナンスを論ずるために、核兵器の不拡散、生物化学兵器の制限、炭素排出量規制などに用いられた論理を応用しようと試みた。それらの研究者にとってサイバー空間とは以下の図表 1-2 に示すとおり、西側諸国と東側諸国がしのぎを削る新たな舞台である。核技術開発、宇宙技術開発で行われた東西の競争と対立がサイバー空間という新たな場で起きているのである[13]。

---

[12] 安全保障は、「国家間の競争の時代が終わり、非国家主体に目を向ける必要があるテロリズムの時代に入った」という言説は勢いを失っているようである。例えば、2018 年の米国の国家防衛戦略は「国家間の戦略競争が米国の安全保障の最重要課題であり、テロリズムではない」と国家間の対立こそが最大の安全保障課題だとした。（U.S. DoD 2018: 1）。

[13] これを、例えば川口（2019）はサイバー空間がユートピアから国家中心の競争の場へと変容していると表現する。



図表　1 -2 国際関係論におけるサイバー空間のイメージ

このような国家を中心とした見方の中でも特に広く支持されるのが、サイバー空間の覇権を巡り米国と中国が争っているという、米中対立の構図である（Triolo et al. 2020; 佐橋 2020）。米中のデカップリング（分断）と呼ばれる現象の大きな一角を、情報技術を巡る対立が占めている。AI 技術開発、半導体製造、5G などの新世代通信規格などの分野で米中は激しい競争を行っている。米中対立論者にとっては、5G 通信のための製品で、中国製を選択するか、欧州製を選択するかは米国の陣営に加わるか、中国の陣営に加わるかの「踏み絵」と解釈される。

もちろん、世界を単純な二項対立で捉えられないという主張も少なくない。例えば、国際戦略家として知られるパラグ・カンナ（Parag Khanna）は、欧州連合（EU）と米国と中国を現代の 3 つの帝国と捉え、現在の世界をそれらの三つ巴と捉えた。カンナによればサイバー空間というネットワークもまた帝国が影響力を行使する場である。そして「現在、世界の力のバランスを支える比較的同程度の政治の中心地は、ワシントン、ブ

リュッセル、北京」だと言う。(カンナ 2009: 20)。同様にサイバー空間を三つ巴と捉える研究としては、横澤誠の「デジタル・エコノミーの地政学」があげられる。横澤は現代のサイバー空間での力学を米中欧の大三角形対立と日米欧の少三角形の 2 つで分析した（横澤 2019)。

米中対立の構図も EU-米国-中国の三つ巴という捉え方も、国家以外のアクターの働きを考慮していないという点で共通している。サイバー空間はそのほとんどが民間企業の所有するインフラの集合である。近年話題になっている GAFA（グーグル社、アマゾン社、フェイスブック社、アップル社というシリコンバレーのグローバルテックカンパニーの総称）を持ち出すまでもなく、企業の力が部分的に国家を超えるということが珍しくない。例えば、米国の 3 社（グーグル社、フェイスブック社、マイクロソフト社）と中国の 1 社（テンセント社）が 10 億人以上のユーザを獲得している（シュワブ 2019)。世界で最も先進的なサイバー攻撃能力を持つと言われる米国家安全保障局（NSA）は、米国ユタ州に約 12 エクサバイトを保存する巨大なデータセンターを持っているが、グーグル社はそれを遥かに超える規模のデータセンターを世界に複数所有している（シュナイアー 2016)。各国政府はネットワークを「セキュアにする」という名目で検閲を行っているが、それらの検閲を可能にする技術開発は民間企業の仕事である（Deibert 2013）[14]。インターネットの通信を相互にやり取りするインターネット・サービス・プロバイダーの中でもティア 1（Tier1）と呼ばれる大手企業は 15 社しかなく、そのうち 8 つは米国企業[15]である。インテリジェンス機関といえども、

[14] チュニジアではウェブセンス社の技術が、ミャンマーではフォーティネット社の技術が、サウジアラビア、オマーン、UAE などではスマートフィルター社の技術が使用されている。より一般的な製品を開発しているブルーコート社の Web 検閲システムはアフガニスタン、バーレーン、ミャンマー、中国、エジプト、インド、インドネシア、イラク、ケニア、クウェート、レバノン、マレーシア、ナイジェリア、カタール、ロシア、サウジアラビア、シンガポール、韓国、シリア、タイ、トルコ、ベネズエラといった国でも使用されていることが確認されている。

[15] AT&T 社、CenturyLink 社、Verizon 社など。

これらの企業の協力なしに大規模な情報収集活動をすることは、容易でない。

サイバー空間は物理的・地理的制約が少なく、行動の単位としての国家の有効性は減少している[16]。代わりに力をつけているのは、ここに紹介したグローバルテックカンパニーである。サイバー空間をいわゆる冷戦の構図を用いて分析すると、民間企業の持つ力が死角となる[17]。

異なる 2 つの分野の先行研究を振り返るなかで、本論文において克服すべき課題が見いだされる。まず、サイバー空間における価値が論じられてこなかったことである。すでに指摘したとおり、統治のメカニズムは力だけでなく、共通の価値観や世界観を要する。

そしてグローバルテックカンパニーの力を正しく評価し、その戦略が国家とまったく同一なのか違うのかを精査する必要がある。戦略が違うのであれば、そしてグローバルテックカンパニーに国家と肩を並べる力があるのであれば、それはサイバー空間のガバナンスの大きな決定要素になるからだ。

さらに「多様なアクター」「パワーの分散」というサイバーセキュリティに固有の現象への過剰なフォーカスから距離をおきたい。サイバー攻撃や防御能力は非国家主体やときに個人であっても保有できるものである。その点において、多様なアクターというのは真実であろう。個別のアクターの動きを正確に捉えることの重要性は言うまでもないが、ガバナンスを考える上ではある程度のディテールを犠牲にしても、その空間を支

---

16 田所昌幸はこれを世界の脱領域化と表現する。インターネットなどのテクノロジーが情報の流れを媒介し、世界が脱領域化された現代では、国境で区切られた領土を排他的に支配することに由来する国家の能力が後退するという（田所 2020: 75）。

17 インターネットガバナンスの研究者ミルトン・ミュラー（Milton Mueller）は国家間の競争のみを分析する姿勢を、次のように鋭く批判した。「（インターネットをアメリカ政府が支配しているという考え方に賛同できない。なぜならば）サイバー空間においては独自の利害に基づいた、独自の統治の機構があり、それらは特定の政府の利害と一致しない。もし、我々がインターネットガバナンスをめぐる軋轢を、何れの国家がライバル国家より力を持つかという視点で捉えるならば、我々の精神は 17 世紀の産業主義から大きく前進したと言えない。」（Mueller 2017: 19）

配する法則に目を向けなくてはならない。

第４節　リサーチクエスチョンと用語の定義

第１項 リサーチクエスチョン

複数の国際関係論やグローバル・ガバナンス論の研究者たちは効果的な統治の仕組みという課題に「政府・国家に代わって問題の解決に当たる主体とは何か。それはどのように実践されるのか」という問いを立てて分析を試みてきた。しかしながら多くの場合、「国家主体だけでなく非国家主体の役割が拡大しており、両者が共同する新たな主体が必要」という既視感のある解にとどまってしまう。これはサイバー空間に限らず、温暖化や地域安全保障などの分野で繰り返された、「主体の増設と争点領域の拡張というお馴染みの理論枠組み」（南山 2015）であり、実社会に貢献していると言い難い。サイバーセキュリティ・ガバナンスを一歩前に進めるためには新たな問いが必要である。

そのためには既に第 1 章第 2 節で述べたサイバー空間における価値の体系に迫ることが必要となろう。サイバー空間における価値の体系を、言い換えればそれぞれのアクターが力の行使を通して実現しようとしているサイバー空間の姿を描き出さずに、サイバー空間の秩序を語ることはできない。「サイバー空間の秩序の土台となる共通の価値観とはなにか」という問いを核となるリサーチクエスチョンとして設定する。これは「誰がどのようなサイバー空間を実現しようとしているか」と換言することもできる。

ここからいくつかの派生するリサーチクエスチョンが浮かび上がる。まずは共通の価値観そのものへの理解を深めるための問いが必要である。共通の価値観は 1 つなのか、複数あるとすればそれらはどのように相互作用するのか、サイバー空間の誕生から現在まで普遍的なものか、などの問いである。そのためには既存のサイバー空間に関する国際的な合意のテキストや国家のサイバーセキュリティ戦略などの分析が必要となる。さ

らに、サイバーパワーを得ようとするアクターが誰であるか、アクター同士の関係がどのように変化しているかも重要である。サイバー空間に乱立するレジームを整理し、その中でも特にサイバーセキュリティのガバナンスにおける重要なアクターであるCSIRT（Computer Security Incident Response Team）とよばれるレジームの変化を考察したい。

これらのリサーチクエスチョンに対する本論文の結論を先取りすれば以下のとおりになる。サイバー空間の統治や管理をめぐる言説の分析から、サイバー空間において「民主主義」と「国家主権」と「グローバリゼーション」の 3 つが共通の利益であり、共通の価値として認識されている。ところが、この 3 つの価値はトリレンマの関係にある。つまり 3 つの価値のうちいずれか 2 つを確保したサイバー空間は実現できるが、「グローバルで民主主義的に運営され、なおかつ国家の主権が認められるサイバー空間」は実現できない。

現代のサイバー空間におけるアクターに目を転じると、「情報拡散国家」と「情報支配国家」と「プライベートテックカンパニー」という 3 グループが生存競争を行っていると考えられる。3 アクターはそれぞれに、サイバー空間でより多くのデータにアクセスするための競争を行っている。

その競争に勝つため、情報拡散国家は民主主義的なサイバー空間を、情報支配国家は国家主権が確保されるサイバー空間を、グローバルテックカンパニーはグローバリゼーションが担保されるサイバー空間を作り上げようとしている。このトリレンマは情報拡散国家に最も厳しい選択を迫る。情報拡散国家はサイバー空間における民主主義を捨てられない。したがって、グローバルなサイバー空間、国家主権が確保されるサイバー空間のどちらかを諦めなければならないのである。

第２項 用語の定義

本論文において「情報拡散国家」という言葉を使った場合、それは国家や社会内における情報の共有や拡散に高い価値を置き、それが民主主義の発展を促すことを積極的に認める国家を意味する。G7 に加盟する先進自由主義、民主主義国家群、より具体的には米国、英国、フランス、ドイツ、イタリア、カナダ、日本などがこれに当てはまる。情報拡散国家は、民主主義を効率的かつ公正に推進するためにデータへのアクセスを求める。民主主義の前提は主権者である国民の間での情報の共有である。正しい情報を共有していなければ、例えば選挙のような主権の行使も正しく行われないことになる。そして、現代のようにインターネット、さらにはソーシャル・メディアが普及した社会では、情報は単に分散的に共有されるだけではなく、積極的に拡散される側面がある。一方向に情報を共有する従来のメディアとは違い、多くの人が情報を自ら発信できるようになった側面を踏まえ、ここでは「拡散」という言葉を使いたい。こうした社会では、情報を拡散することが善とされている。しかし、そこには誤情報の入る余地があったり、意図的に偽情報を拡散させようとする勢力に脆弱であったりするという側面があることは否めない。また、本論文では米国の巨大テックカンパニーは国家とは別の戦略を持つアクターと捉える。例えば、グーグル社、アマゾン社、マイクロソフト社は「情報拡散国家」に含まない。

「情報支配国家」とは、情報拡散国家とは異なり、国家や社会内における情報の共有や拡散を重視せず、むしろ国家や社会の安定を重視する故に、情報は為政者が限定的に保有し、効率的な支配を目指す国家である。具体的には中国、ロシアや中東諸国に代表される、国家による情報支配の重要性が高い国家群を指す。権威主義体制がとられるこ

との多いこれらの国々の為政者は[18]、情報拡散国家のように情報を共有したり拡散させたりすることに価値を見いだしていない。ゆえに国家や政府によるサイバー空間の管理の必要性を正当化しやすいという特徴がある。

「グローバルテックカンパニー」は、特定の国家や社会に収まらず、グローバルな市場において利益を追求し、特に情報技術を駆使する企業群のことである。本論文では、個々のグローバルテックカンパニーの本社の所在地や起業地がどこであるかはあえて問わない。無論、米国を発祥とする企業と中国を発祥とする企業では、それぞれに適用される法律も違えば、企業文化も大きく異なるだろう。しかし、グローバルテックカンパニーはおしなべて、利益追求のために顧客に関するデータを徹底的に収集し、それを利益に転換しようとする点で共通の特性を持っている。そして、グローバルテックカンパニーはある程度の影響力を持つようになると、自社の出身国の政府を含む各国の政府の規制に抵抗しようとする姿勢を見せる。そして、できるだけ国家の色を廃し、顧客の利益を代表するという立場を見せながら、自社の利益を追求する傾向がある。

「サイバー空間」という言葉もまた、定義が定まっていない（Maurer & Morgus 2014; Stevens & Betz 2013; 塩原 2015）。北大西洋条約機構（NATO）は電磁スペクトラムも、スイスはアプリケーションや電子商取引もサイバー空間の一部であるという立場をとっている。日本の経済産業省が提唱するサイバーフィジカルフレームワークのように製品の供給路までを射程に置く定義もある。日本の慶應義塾大学がサイバー文明研究センターを設置したのは、サイバー空間の中に科学技術を駆使して作り上げられた高度な文明社会が見いだせるという含意があるようである（村井 2019: 66）。また逆にサイバー空間とは電子的なデータの集合「のみ」であり、その土台となる物理的なインフラはサ

[18] 情報支配国家は権威主義体制をとる国が多いが、全体主義体制や建前上の民主主義体制をとる国もあり、政治体制のみを情報支配国家の基準にすることは困難である。そもそもある国が、民主主義体制なのか、権威主義体制なのか、全体主義体制なのか断定することは難しい。リンス（1995）はむしろ体制が明確でない国のほうが多いとしている。

イバー空間に含まれないという国際標準化機構（ISO）のような少数派の定義もある。ロシアのようにそもそもサイバー空間という語を使わず、情報空間という言葉でほぼ同じ意味を表現する国もある（佐々木 2012: 1）。

これらのサイバー空間の議論からわかるのは、サイバー空間は議論の主体の都合により伸び縮みする言葉であるということである。同じプレーヤーが異なる議論の場で異なるサイバー空間の定義を使い分けることもある。仮に一番狭い定義を採用し、サイバー空間にデータや人と人とのコミュニケーションが含まれないとする。その場合、サイバー空間のセキュリティとはインターネットなどの様々な通信インフラのセキュリティを確保するための手段であり、サイバー空間上でのテロリストのやりとりや不正送金や迷惑メールなどはスコープを外れることになる。後述するサイバー空間における国家主権の問題を持ち出すまでもなく、サイバー空間という言葉の定義そのものが、きわめて影響範囲の広い政治問題である。

移ろいの激しい情報通信技術の性質を考えれば、サイバー空間の定義は、労多くして得るものが少ない作業と言わざるをえない[19]。本論文は実効的な秩序およびそれを目指すための議論は必ずしも厳密な定義を必要としないという基本的な立場をとる。その上で研究を進めるにあたって先行研究（土屋 2018a）に倣い、サイバー空間とは「通信端末＋通信回線（有線・無線）＋記憶装置＋データ」であると定義する。しかし、今後この定義が拡張される可能性を念頭に置く。

「サイバーパワー」という言葉が定義しづらいのは、サイバー空間そのものに曖昧さが残っていることを考えれば自明のことである。Nye（2010: 4）は「サイバー空間を利用して、他の作戦空間における優位な立場を作り出したり出来事への影響を与える能力」

[19] 例えば国際社会は「テロリズム」の問題をこれまで 200 年以上してきたが議論、未だに統一された定義はない（U.S. Department of Justice Federal Bureau of Investigation 1998: i）。

とサイバー空間におけるパワーを定義した[20]。この定義の解釈の難しさは優位な立場という言葉の曖昧さにある。第 1 章第 2 節で論じたとおり、本論文ではサイバーパワーとは「より多くのデータにアクセスする力」と定義する。

第５節　論文の構成

本論文の構成は以下のとおりである。

ここまで本章では、問題の背景、サイバー空間の秩序の土台となる共通の価値観とはなにかというリサーチクエスチョン、先行研究の課題とそれを克服する本論文のアプローチを示してきた。また「情報拡散国家」、「情報支配国家」、「サイバーパワー」といった本論文を通した議論に必須の概念を定義した。

第２章「サイバー空間における情報拡散国家の苦悩」では情報拡散国家の戦略を紐解き、同時にロドリックの世界経済の政治的トリレンマの原理を応用したサイバー空間のトリレンマという本論文を貫く分析の枠組みを提示する。サイバー空間においては、民主主義と国家主権とグローバリゼーションを推進しているのが、それぞれ情報拡散国家、情報支配国家、グローバルテックカンパニーと捉えられる。そして現在のサイバー空間をその 3 つのアクターによる争いとみなすことができる。情報拡散国家はサイバー空間において、グローバリゼーションと民主主義を一貫して追求してきた。一時、インターネットと民主主義の蜜月と呼べる期間があったが、国家として国民の安全の確保を図る必要があり、情報拡散国家は国家主権の確保に舵を切った。その選択がサイバー空間におけるグローバリゼーションもしくは民主主義のいずれかを

[20] これが「パワーに単一の定義はできない。定義は必ずその人の利益と価値観を反映する」と、前置きした上での定義であることは留意しておきたい（Nye 2010: 2）。また持永らは、サイバー空間を支配するためのパワーは技術、産業／政策、数（データ、市場、利用者数）の関係から導かれるという枠組みを提示した（持永 et al. 2018; 3620）。

諦める覚悟を伴うことを指摘する。

第 3 章「情報支配国家」では情報支配国家の戦略を検討する。中国、ロシア、北朝鮮の３カ国をとりあげ、サイバーセキュリティ・ガバナンスに関連する動きを整理する。導き出されるのは、サイバー空間に起こっているのが自由を希求する情報拡散国家と統治を望む情報支配国家という単純な対決ではないということである。情報支配国家にカテゴライズした中国とロシアと北朝鮮の間には大きな違いがある。中国はグローバルなインターネットを求めており、ロシアはそれを求めていない。その違いを意識せずに既存の国際安全保障の視点から中国とロシアを「中露」と一括にできない。そして、どの国も細部で様々な性格と異なる行動をとるため、「強いサイバー国家」「弱いサイバー国家」「自由を保つサイバー国家」「自由を嫌うサイバー国家」という分類ができないということを主張していく。多くの情報支配国家でも少なくとも建前上、自由なインターネットが希求されている。しかし、同時に「安全なインターネット」が望まれている。身体の安全、家族の安全、民族の安全、宗教の安全の重要性を我々は恣意的に小さくとらえていなかったか、という問題を提起する。

第４章「グローバルテックカンパニー」ではサイバー空間トリレンマ理論における 3 つ目のアクターである、グローバルテックカンパニーの戦略を論じる。法、規範、市場、アーキテクチャのすべてにおいて、国家を凌ぐ強い影響力を持つグローバルテックカンパニーの力を描く。グローバルテックカンパニーの力の源泉は、数十億人のユーザが日々生成するデータに自由にアクセスできる点にある。そして現在のサイバー空間のガバナンスを支えるのは、政府の行動が後手に回る状況を様々な創意工夫で対応してきたグローバルテックカンパニーの貢献が大きい。しかし、グローバルテックカンパニーは自らが、国家の代役はできないことを自覚すべきである。グローバルテックカンパニーには技術と大量のデータと資金が存在するが、それを大規模に行使する民主的な正当性も、ガバナンスも中立性も確保されていない。したがって第４章では、グローバルテッ

クカンパニーが新たな国際秩序を作る可能性は低いとし、今後情報拡散国家もしくは情報支配国家のいずれか、もしくはその両方を支える役割を担うものと結論づける。

第５章「合意を巡る戦い」では文字どおり、情報拡散国家、情報支配国家、グローバルテックカンパニーの３つのグループによる、合意を巡る戦いを描く。派生するリサーチクエスチョン「共通の価値観は１つなのか、複数あるとすればそれらはどのように相互作用するのか、サイバー空間の誕生から現在まで普遍的なものか」という問いに答えるために既存のサイバー空間に関する国際的な合意のテキストや国家のサイバーセキュリティ戦略などの分析を行う。ここでの合意とは国家サイバーセキュリティ戦略や国際条約や規範などの総称である。既存の国際合意のテキスト分析からは、①3 つのグループのいずれかの内部での合意、つまりはグループ内合意、②複数のグループ間での合意、つまりグループ間合意、③そして議論の場が持つ格式に支えられる国連のもとでの合意の 3 つに分けることができそうである。GCSC（Global Commission on the Stability of Cyberspace）という後述する国際委員会における規範の議論への参与観察からは、合意の文章が明示的に語らない、裏の狙いを解き明かすことを試みた。合意形成が、必ずしも世界平和を目指した高尚な活動ではなく、各参加者の安全保障や経済的反映を得るための手段であることを示す。

第６章「インシデント対応コミュニティの発展」では情報拡散国家、情報支配国家、グローバルテックカンパニーの争いにおいて CSIRT というセキュリティ対策組織が果たす役割を取り上げる。サブリサーチクエスチョンの「サイバーパワーを得ようとするアクターが誰であるか、アクター同士の関係がどのように変化しているか」に迫るための手段として、サイバー空間に乱立するレジームを整理し、その中でも特にサイバーセキュリティのガバナンスにおける重要なアクターである CSIRT とよばれるレジームの変化を考察したい。サイバーセキュリティガバナンスにおけるレジームのうち、目的に「被害者救済と復旧」を掲げ、かつ機能として「インシデント対応能力」を備え、かつ

文化として「互恵主義」を信条とするのが CSIRT である。サイバーセキュリティの非ゼロ和ゲーム化を指摘し、CSIRT 自身の「被害者救済と復旧」という目的と互恵主義の文化が共に揺らいでいることを解き明かした。CSIRT コミュニティは自らの目的を再定義することが求められている。

第 7 章ではこれらの議論をまとめる。

第２章　サイバー空間における情報拡散国家の苦悩

第１節　グローバリゼーション、民主主義、国家主権

サイバー空間の急速な発展、そして 2010 年代から顕在化した安全保障問題化は、サイバー空間を巡るアクターの勢力図を現在進行形で塗り替えている。サイバー空間の大きな割合を占めるインターネットは人々のコミュニケーションの手段であるだけでなく、電気・水道・ガスなどのインフラの神経系であり、あらゆる経済活動を支える装置であり、軍事活動の新領域である。また近年の民主国家におけるサイバー攻撃による選挙干渉、フェイクニュースの問題などは統治の正当性への疑問を喚起し、メディアへの信頼を損なった。

歴史を振り返れば様々なパワーバランスを変える技術が繰り返し発明されてきた。火薬、飛行機、潜水艦、長距離弾道ミサイルと核兵器、宇宙技術などが代表である。サイバー空間が既存の発明と違うのは、それが特定の政治体制においてより強い力を生み出すことである。インターネットソーシャルメディア、大規模データ収集、AI の活用は情報拡散国家にとって扱いづらい反面、情報支配国家にとっては便利な道具になっているという懸念が生まれている（Kagan 2019b: 13）。

懸念の一部はすでに現実化している。情報拡散国家の土台、民主主義の根幹である公正な選挙は、サイバーセキュリティ上の脅威に晒されている。2015 年の米大統領選挙、2017 年のフランス大統領選挙、2017 年のウクライナの国民投票、これらはすべて外国のインテリジェンス機関による情報操作が行われたという報道がある。情報操作が本当に行われていたとして、どの程度結果に影響をもたらしたのか、それは極めて評価が難

しい問題である。しかし、いずれの場合も、選挙において敗北した側だけでなく、一般市民にも選挙成果の正当性への疑問が残るだろう。公正な選挙の実施という一点をみるだけでも、民主主義とサイバー空間は相性が悪いという言説が説得力を増している。

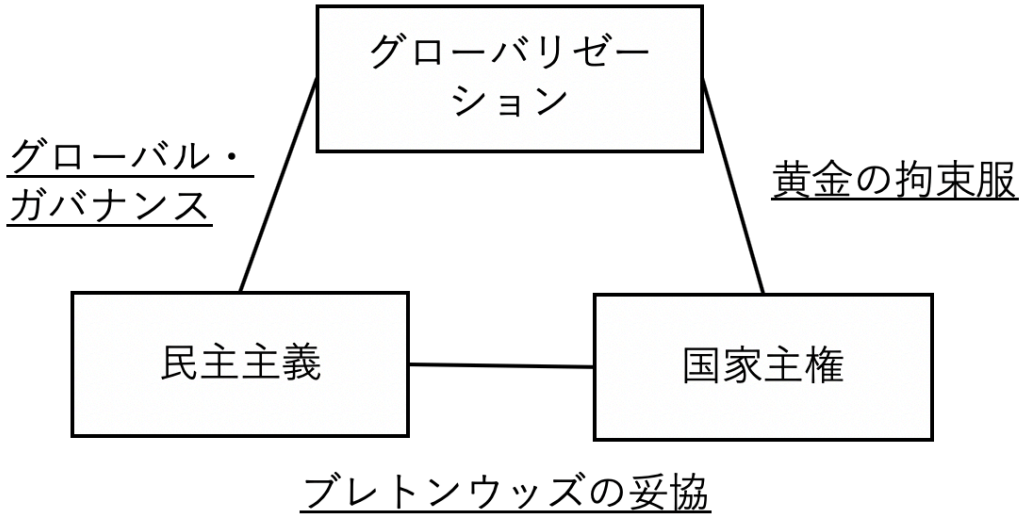
現在のサイバー空間をとりまく国際情勢を眺めたとき、日本を含めた情報拡散国家は「こんなはずではなかった」と思いに駆られるのではないか。サイバー空間はグローバルに人々を相互に結びつけ、経済やアイデアを交換する手段となり、情報の普及が世界に遍く民主主義をもたらすはずではなかったのか。情報拡散国家はどこでボタンを掛け違えたのだろうか。

この疑問に対して、本論文はまず情報拡散国家がサイバー空間にグローバリゼーション、民主主義、サイバー空間における国家主権の 3 つの目標を同時に追求していることを指摘する。詳しくは後述するが、国際経済の分野の研究では、この 3 つが併存できないことがすでに指摘されている。情報拡散国家が、達成不能なことを自覚した上で、目標として掲げ続けるという戦略であるのか、あるいは達成不能なことに無自覚であるかは定かでないが、これをサイバーセキュリティのトリレンマとして解説し、3 つのいずれかを捨てる必要性があるという問題提起を試みる。

第２節　本章における分析の枠組み

トルコ出身の国際経済学者であるダニ・ロドリック（Dani Rodrik）は世界経済の政治的トリレンマの原理（Fundamental Political Trilemma）を提唱した。ロドリックは市場万能論に支えられた新自由主義の下で世界経済のグローバリゼーションが進んでおり、多くの先進国が経済のグローバリゼーションと民主主義政治（democratic politics）と国家主権の確保（nation state）を目標として掲げている現状を描いた上で、「我々は民主主義と、国家の自立と、経済のグローバリゼーションの 3 つを同時に達成することはで

きない」（Rodrik 2012: 181）という命題を提示する。そしてロドリックは世界経済の各アクターは 3 つの目標のうちの 2 つを選ぶことを迫られていると主張する。



図表 2-1 世界経済の政治的トリレンマの原理

選択肢とは上の図表 2-1 に示されるとおりである。①グローバリゼーションと民主主義政治を選び、国家主権を捨て、グローバル・ガバナンスを模索する道、②民主主義政治と国家主権を選び、グローバリゼーションを諦め、ブレトンウッズの妥協（Bretton Woods compromise）を取る道、③グローバリゼーションと国家主権を選び、民主主義政治を捨て、金色の拘束着（Golden Straitjacket）を取る道である（Rodrik 2012: 201）。

3 つの選択肢を示した上で、ロドリック自身は世界経済のあり方について、②のブレトンウッズの妥協を取る道を推した。世界経済を運営するアクターとしての国家主権の役割を軽視することはできず、民主主義はその国家運営の土台である。であれば相対的にグローバリゼーションの優先度を下げざるをえない。民主主義国家の体制に負の影響を与えない程度に、グローバリゼーションを制限するのが現実的というロドリックの主

張である[21]。

ロドリックの世界経済の政治的トリレンマの原理は、サイバーセキュリティのグローバル・ガバナンスにおいても当てはまることを本論文は論証していく。サイバー空間はそのグローバルな性質が当初から重要な価値であった。その空間において民主的なガバナンスを模索する議論が活発に行われてきた。またサイバー空間の拡大が民主主義を推進することが期待されていた。さらに近年になって、国家安全保障への配慮から、サイバー空間がグローバル・コモンズではなく、国家の主権が及ぶ対象であるという理解が情報拡散国家にも広がっている[22]。

グローバリゼーションと民主主義と国家主権という並び立たない 3 つの目標を掲げているのが、現在の情報拡散国家の姿である。このことが、情報拡散国家の政策に不透明性と混乱をもたらし、その主張の一貫性を毀損してきた。特に既存の東西対決の構図で、情報拡散国家と情報支配国家とが正対した場合に、民主主義の実現を求めない情報支配国家の主張に説得力を与えることとなった。情報拡散国家が、この状況を打開するためには、まず矛盾を認識し、グローバリゼーションと民主主義と国家主権の 3 つのうちのいずれかを諦めるための議論を始めなければならない。

本章の構成は以下のとおりである。サイバー空間において、情報拡散国家が、「グローバリゼーション」と「民主主義」と「国家主権」という 3 つの目標をどのように追求してきたかを第３節、第４節、第５節でそれぞれ論じていく。それを受けて第６節では

---

[21] 正村公彦は、「20 世紀を動かしたものは産業主義、民主主義、国民国家」（正村 1993: 23-25）と主張した。産業主義をグローバリゼーションに読み替えれば、3 つの価値観の重要性をいち早く指摘していたと言える。しかしながら、ロドリックの研究において 3 つの並立がないというトリレンマの存在という重要な発展があり、本論文ではロドリックの理論を応用する。

[22] ロドリックの理論を用いてサイバーセキュリティやサイバー空間のガバナンスを解読するという着想は林（2020）でも言及された。林は「西欧先進諸国」と「中国・ロシア等の国々」の間の衝突にこの理論を用いているのに対し、本論文はより広くグローバルテックカンパニーを主たるアクターに据える点に相違がある。

ロドリックの世界経済の政治的トリレンマの原理をサイバー空間に当てはめると、そこにどのような世界が広がるのかを 3 つのシナリオにそって概説し、それぞれのシナリオの実現可能性を添える。第 7 節ではこれらの議論を総括し、ロドリックの理論を応用した、サイバー空間のトリレンマ理論の有効性を論じる。

第 3 節　グローバルなサイバー空間

第 1 項 グローバルなサイバー空間という言説の形成

サイバー空間はいずれの国家による干渉も受けないグローバルな空間であるべきという言説はインターネットが発明されたサイバー空間の黎明期から、繰り返し見られた。サイバー空間がグローバルな空間であるという認識が強固な理由は、1 つにインターネットの技術的特性がある。そしてもう 1 つの理由をインターネットが育まれた米国西海岸の時代と場所の空気に求められる。それらを受けて、本節の最後では、グローバルなサイバー空間への期待は急速に薄れつつあり、サイバー空間の分断が起こっていることを説明する。

インターネットの起源を米国防省の研究所による、ミサイル攻撃に耐えうる情報通信ネットワークを目指した研究とするか、大学などに所属する研究者によるグローバルな

草の根ネットワーク構築とするかという点は未だ一致した見解をみることはない[23]。その起源の時点でミサイル攻撃からの防衛を狙ったネットワークの実現という意図を完全に否定できない。一方で、世界中に普及する過程において学術研究機関や民間企業がこれを先頭に立って進めたことに疑いの余地は少ない。

実態として通信ネットワークとしてのインターネットはグローバルである。これはインターネット以前の国際通信の手段である電話と比較すると明らかである。電話も世界中を結ぶネットワークであり、インターネット以前から地球の裏側にいる誰かと音声通話が可能であった。本論文の文脈では電話は、しかし、グローバルではなく、インターナショナルなネットワークであった。国際電話は国際電気通信連合（ITU）という国際機関によって管理がなされている。ITU は国連の専門機関であり、重大な決定は、原則として加盟する主権国家に委ねられる。電話番号の体系を例にとろう。ITU の決定に基づき、各国に国番号が割り振られ、その範囲内で各国政府の独自管理が許容されている。我々が国際電話をかける際に、国番号以下の番号体系が国によってバラバラであるように感じるのはそのためである。対してインターネットは世界中で一意の番号体系（アドレス体系）が用いられている。国毎に分断されることはなく、世界中に同じ IP アドレスを持つコンピュータが重複しないように、グローバルな管理がなされている。IP アドレスは一例であり、ドメイン名や AS（Autonomous System）番号とよばれる国をまたが

[23] インターネットの起源となる ARPANET プロジェクトに自ら関与したイアン・ピーター（Ian Peter）は、ARPANET はメインフレームコンピュータの接続のみが目的であったと証言する。ゴシップが得意なコラムニストによって、核戦争への備えというストーリーが後付されたという主張である。（Kettemann et al. 2019: 76）。他方で、インターネットプロトコルの開発に資金を提供した国防省の狙いは、核戦争が起きても機能するネットワークではなく、現場の兵士一人ひとりがシステムや物理的な媒体の違いによらず通信できる状態の実現であったという説もある（Mueller 2017: 8）。つまり、インターネットの起源に、軍事的な利用への期待は少なからずあったが、それは核戦争への備えとは直接的に関係なかった。なお、コンピュータ同士の接続を目指した ARPANET はほぼ 100%電子メールのやり取りに用いられた。ネットワーク技術は当初からコンピュータ同士ではなく、人と人を繋いだ（ばるぼら 2005: 18）。

る相互接続に必要なリソース（資源）もまた国家や国際機関の手を借りることなく、グローバルな技術者のつながりに拠ったコミュニティによって管理されている。このようにインターネットは技術的にグローバルな性質をもっている。

そのインターネットの上に実現するサイバー空間がグローバルな性質を持つというのは、インターネット創設者やその支持者たちの政治的スタンスと無縁ではない。1996年、ビル・クリントン（Bill Clinton）政権における通信品位法の成立の後、電子フロンティア財団の創立者でもあるジョン・ペリー・バーロウ（John Perry Barlow）は、有名なサイバー空間独立宣言を公開した。

> 私は宣言する。我々が創り出しつつあるグローバルな社会空間は、あなたたちが課そうとしている圧政から、本来、独立したものである。あなたたちは我々を統治するなんらの道義的権利も持たないし、我々を恐怖させるに足る如何なる強制の手段も持たないのだ（Barlow 1996; 高野 2007）。

バーロウはサイバー空間を単一のグローバルな仮想空間と捉え、インターネットにおける表現の自由を最上級の価値と捉え、そこに国家の主権は存在しないと断言した。バーロウの独立宣言は 1990 年代のサイバー空間において奇異ではなかった。サイバー空間には米国西海岸に由来する「カリフォルニア・イデオロギー」が色濃く存在した[24]。東浩紀によれば、カリフォルニア・イデオロギーとは「新右翼と新左翼、ヤッピー的起業精神とヒッピー的反体制意識、市場資本主義と共同体主義という本来ならば対立するはずの政治的契機を、『新しい情報テクノロジーが社会的解放をもたらす可能性への深い信仰』により止揚するものである」（東 2015: 889–95）。本来なら相容れない 2 つの

[24] これを土屋は技術者文化（ギーク文化）と政府官僚や企業人のスーツ文化と軍人のユニフォーム文化との軋轢と表現した（土屋 2013: 1）。

グループはサイバー空間のグローバル性を高めるという作業の共犯者となった。市場資本主義者（ヤッピー）はグローバルな市場を、共同体主義者（ヒッピー）は世界市民を夢見たからである。

多くの情報拡散国家は、サイバー空間のグローバル性を追認した。それは情報拡散国家が示す戦略文書や国連はじめとする国際会議の発言にも現れている。

- 「サイバー空間とはグローバルに相互接続されたデジタル情報コミュニケーションのインフラ」（米国）（United States of America 2009: III）
- 「サイバー空間は相互接続された情報技術ネットワークであり、17 億人が相互に繋がり、アイデアやサービスや友情を生むグローバル・コモンズ」（カナダ）（Canada 2010: 2）
- 「世界中に相互接続された自動的なデジタルデータの処理装置によって構成されるコミュニケーション空間」（フランス）（France 2011: 21）
- 「サイバー空間は『国境を意識することなく自由にアイディアを議論でき、そこで生まれた知的創造物やイノベーションにより、無限の価値を産むフロンティア』である人工の空間」（日本）（内閣サイバーセキュリティセンター 2015: 5）

と一様にそのグローバルな性質、言い換えれば一国の意思だけでは好きにコントロールできない側面に言及している。

加藤（2015: 12）は、サイバーという空間を、政治機構としての国家は戦闘空間と捉え、軍事機構としての国家は無秩序ととらえ、非国家主体はグローバル・コモンズと捉えるとサイバー空間の捉え方が主体によって異なるという考えを示したが、塩原が指摘するように「2005 年の米国の『国家防衛戦略』では、宇宙、公海、空域、サイバー空間をグローバル・コモンズとみなしており、一国だけの境界設定を主張していたわけではなかった」（塩原 2015: 32）ことからも、複数の解釈が並行していると言うより、同一の主体がその認識を改めてきたという説明がより有力である。

個々の国家がそれぞれにグローバルなサイバー空間を打ち出すだけでなく、それを国際的な合意に昇華する努力も行われた。例えば、2000 年 7 月に開かれた G8 の九州・沖縄サミットでは「グローバルな情報社会に関する沖縄憲章」が打ち出された（外務省 2000）。グローバルな情報社会の実現のため、デジタル・オポチュニティ作業部会（ドット・フォース）の設置などが憲章に謳われた（土屋 2013: 3）。

これらの事実が示すのは少なくとも 2010 年前後まで、サイバー空間はグローバルな空間であるべきであるという認識が情報拡散国家に行き渡っていたという事実である。前掲のカナダのように、明示的にサイバー空間はグローバル・コモンズ[25]であると明言していた民主国家も少なくない。ドメイン名管理の国際組織 ICANN（Internet Corporation for Assigned Names and Numbers）が 2013 年に「1 つの世界、1 つのインターネット（One World. One Internet.）」というスローガンを掲げたのはそれを端的に象徴している（ICANN 2013）。しかし、この認識は徐々に希薄になり、サイバー空間におけるグローバリズムは難しい局面を迎えている。次項以降で論じていく。

第 2 項 米国への不信

サイバー空間はグローバルな場という情報拡散国家の認識は徐々に薄れ、その主張が弱まりつつある。これを定量的に証明することは難しい。ここでは、サイバー空間の歴史を振り返ると 2010 年から 2013 年までの間に、情報拡散国家の中での相互不信が生まれる、より具体的には米国への不信を招く「事件」が起きている[26]ことを通して、グ

---

[25] 土屋（2013: 6）によれば「グローバル・コモンズとは、「一国がコントロールはできないが、すべての国が依拠する領域や区域」のこと」。

[26] インターネットガバナンスのライフサイクルを研究した西岡（2007）は、それが 4 つのフェーズに分けられることを示した。第一フェーズ（誕生期）=IETF および ISOC、第二フェーズ（成長期）は ICANN、第三フェーズ（安定期）は WSIS および IGF、第四フェーズ（再生期）は WCIT およびネットムンディアルにその典型を見いだせるという主張である。本論文でグローバル化への諦めが起きた時期は、西岡の言う第四フェーズのタイミングとほぼ一致する。

ローバル化という目標が説得力を失っていったことを主張していく。

1 つ目の契機は 2010 年である。米国においてサイバー軍（CYBERCOM）が公式に発足した。さらに米国がイランの核処理施設をサイバー兵器によって攻撃したいわゆるスタックスネット事件が公に知られることとなった[27]。国家がサイバー攻撃能力を有していることを否定することが難しくなった。攻撃対象となったイランのみならず、世界中にサイバー空間が軍事行動の舞台となることを印象づけた。同時にサイバーセキュリティは、犯罪者とそれに立ち向かう正義の市民という図式が崩れた。

2 つ目は 2012 年 12 月に開催された国連の専門機関である国際電気通信連合（ITU）の会合での民主主義陣営の敗北である。この会合は国際電気通信規則（ITR）という、国際通信における各国政府に対する拘束力のある規則の改定を目的とした。ロシア、中国、イラン、アラブ諸国などの国々は安全保障上の配慮などを理由に、サイバー空間に規制を行う規則に盛り込もうとした。米国、EU 諸国、日本などはサイバー空間上を流れる情報について国家が干渉すべきでないという立場からこれに反対した。EU 諸国・日本も概ねセキュリティ対策を推し進める必要性を規則に盛り込むことの妥当性を認めて、妥協案を探っていたが、あくまで自由でオープンなインターネットを追求する米国はそれを許さなかったようである[28]。その結果、一国一票方式の投票による採決で新規則は承認された。サイバー空間をめぐり、米国、EU 諸国、日本の連合が白日の下に敗北したことは、情報拡散国家の集積的な影響力の低下を国際社会に見せつけたといえる。

---

[27] 蛇足だが、スタックスネットはグローバルなサイバー空間のセキュリティを維持するために技術者として業務に勤しんでいた筆者をして、国際関係を学ぶことを決意させたきっかけである。日頃、相互の信頼に基づいて情報交換をする関係だった米国の技術者たちは、スタックスネットについて一様に口を閉ざした。

[28] ITU の会合（WCIT）における情報拡散国家陣営（米国・EU 諸国・日本）の間に生じた歪については、当然ながら ITU が公表する公式文書からは確認できない。当時、総務省総務審議官として交渉を率いた田中栄一の著作を頼った（田中 2014）。

3 つ目は 2013 年 6 月に公になったスノーデン事件である。元契約職員であるエドワード・スノーデン（Edward Snowden）が持ち出した文書で、NSA を中心とするインテリジェンス機関がドイツやフランスや日本などの友好国に対しても、情報収集活動を行っていることが明らかになった。この一件は、米国の製品とサービスへの信頼を傷つけた。米情報技術・イノベーション財団は 3 年間の売上減額を 220 億から 350 億ドルと見積もった。フォレスターリサーチ社は 3 年間の売上減は 1800 億ドルと推計している（Staten 2013）。スノーデン事件以降、米国を経由するアジア地域・アフリカ地域・ラテンアメリカ地域からの通信が減少したという説もある（Deibert 2013）。シスコ社の CEO であるジョン・チェンバース（John Chambers）は「（NSA のハッキング行為は）業界の信頼を蝕み、テクノロジー企業が世界に向けて製品を売る能力をそこなう」と自国のインテリジェンス機関を非難した（Lau 2014）。このように経済への負の影響は甚大であったが、それ以上にサイバー空間における言論の自由、グローバルなどのビジョンを庇護してきた米政府への信頼が損なわれ、米政府がリーダーシップを失ったことは、金銭に換算することのできない大きなダメージであったと捉えることができる[29]。

第 3 項 グローバル化の後退

一連の事件を受けて、グローバルなサイバー空間への期待は薄れていった。米国の「デジタル植民地主義」あるいは「ミリタリーデジタル複合体」の解体を望む声が、情報支配国家からではなく、基本的な価値観を共有するヨーロッパの情報拡散国家から上がりはじめた（Nocetti 2015: 128）。直接的にはスノーデン事件が契機と考えられるが、ブラジルやロシアだけでなく民主主義国家のドイツでさえも、自国内にデータ

[29] ここでは米政府がリーダーシップを失った理由を、一連の諸外国の信頼を損なう行動に求めた。もう 1 つ、仮説として検討すべきは、当時のオバマ政権の「世界の警察官の地位を返上する」という外交政策の中で、米国の立場を縮小しリーダーシップをあえて明け渡すという決定がなされたという可能性である。さらなる研究を要する。

を囲い込むことを検討するようになる（Birnbaum 2013）。ドイツのアンゲラ・メルケル（Angela Merkel）首相は「ヨーロッパのインターネット」の創設を呼びかけ、その問題意識は、ヨーロッパのプライバシー重視の伝統と合流し、2016 年に制定された EU 一般データ保護規則（General Data Protection Regulation: GDPR）へと繋がっていく。

米国政府と中国通信機器企業との摩擦が表面化したのも 2010 年代前半のことである。2012 年 9 月に米下院の公聴会がファーウェイ社と ZTE 社[30]から聞き取りを行った。グローバル化から保護主義への意識転換が起こっていたと言えるのではないか。

国際政治学者のジョセフ・ナイ（Joseph Nye）は早くも 2010 年にサイバー空間を公共財、グローバル・コモンズとみなすことに疑問を呈している（Nye 2010: 15）。ナイによればサイバー空間の一部は明確に国家の主権の及ぶ対象であり、「不完全なコモンズ」「難解な共同所有物」がせいぜいである。2013 年に国際法の専門家であるスコット・シャッケルフォード（Scott Shackelford）はサイバー空間を「共有リソースプール（common pool resources）」と表現した（Shackelford 2013: 1289）。これらの主張に共通するのは、つまりサイバー空間はグローバル・コモンズではなく、一方で、ドメスティックな公共財でもないという点である。国際関係論、国際法の両分野でサイバー空間という新たな分野を整理する努力が行われているが、そこに決定的な解はない[31]。

ここまでの議論をまとめると、ポイントは 2 点ある。サイバー空間はその誕生以来、グローバルな空間であるという理解が情報拡散国家の政府レベルでも市民レベルでも

---

[30] ZTE 社は中国深セン市に本拠を置く、通信機器企業である。上海証券取引所などに上場した公開企業である。

[31] 現在も、サイバー空間におけるグローバリゼーションを強化しようという運動はいくつかある。代表的なものとしては 2019 年 1 月に、ダボス会議で安倍総理大臣が提唱した「データフリーフロー with トラスト（DFFT）」という考え方や、一部の研究者が提案する国際データ機構の設置などである（経済産業省 2019, Bailey 2019）。しかし、それらの一部のグローバル化維持の動きに勢いはなく、現時点ではグローバル化が後退していると主張するものである。

幅広く共有されていたこと。そしておそらく 2010 年から数年の間に、その期待が失われてしまったことである。以来、サイバー空間はアントニオ・グテーレス（Antonio Guterres）国連事務総長の言うところの「信頼欠乏症」（中満 2019）に苦しんでいる。

第 4 節　民主主義

第 1 項 サイバー空間の民主主義についての 2 つの視座

民主主義は、効果的なガバナンスをもたらし、国家全体の幸福の最大化を実現する手段として、一定の効用を果たしてきた。米国をはじめとする西側民主主義国家の経済的成功がその何よりの証拠である。英国の元首相ウィンストン・チャーチル（Winston Churchill）が「実際のところ、民主主義は最悪の政治形態と言うことができる。これまでに試みられてきた民主主義以外のあらゆる政治形態を除けば、だが」と言ったように、民主主義が最高の政治形態であることへの懐疑は綿々とあった。近年、ロシアやトルコで民主主義が形骸化し、ハンガリーやアルゼンチンでポピュリズムが台頭した。中国やインドやシンガポールなどの非民主主義国家の経済的成功もあり、欧州と米国に住む「民主主義が確保された場に住むことが不可欠」と考える人の比率は全体の 3 分の 2 から 3 分の 1 まで減少したという（Khanna 2017: 3）。これらの民主主義への逆風はサイバー空間に、そのガバナンスにどのような影響をもたらしているのだろうか。

サイバー空間における民主主義を語るために、2 つの異なる視座からの整理を行う。1 つ目の視座はサイバー空間の統治のシステムとしての民主主義である。これはインターネットガバナンスという学問の領域で繰り返し検討されてきたことを要約し、サイバー空間とインターネットがどのように統治されているのかの概要を示し、そこに民主主義の原則が現在も生きていることを主張する。要すれば、サイバー空間における民主主義の議論である。

2 つ目の視座はサイバー空間によって実世界に民主主義がより広がるという期待である。本来政治的にニュートラルであるはずのサイバー空間の技術に、特定の政治体制を推進することが期待された背景を説明する。こちらは要すれば、サイバー空間がもたらす民主主義の議論である。両者の解説を通して、情報拡散国家が、サイバー空間における民主主義と、サイバー空間がもたらす民主主義の両者に期待し、それを実現しようとしていたことを論じる。

第２項 サイバー空間における民主主義

インターネットがこの世に誕生してから、政府と民間企業と市民社会は、インターネットを統治し、管理する方策について議論を積み重ねてきた。いわゆるインターネットガバナンスである。インターネットはいかにデザインされるべきかという問いへの答えとインターネットがどう使われるべきかという問いへの答えを同時に探る議論[32]であり、論点やプロセスが複雑である。

現在のインターネットガバナンスの基本的なスタンスであるマルチステークホルダリズムは、サイバー空間における民主主義の発露ともとらえられる考え方である。マルチステークホルダリズムはサイバー空間の政策決定のプロセスにおいて、官民市民社会の同じ立場での参加を求める[33]。そしてサイバー空間における重要な決定は、政府と民間企業と市民社会の代表者が参加した場で議論されるべき[34]であると説いてきた。実際に毎年秋に国連が主催するインターネットガバナンスフォーラムなどでは、様々な関係

---

[32] これを Maurer（2017）はインターネットのガバナンス（Governance of the Internet）とインターネット上のガバナンス（Governance on the Internet）と表現した。

[33] イコールフッティング（equal footing）の原則と呼ばれている。

[34] Mueller（2018: 3）は「本質的にマルチステークホルダリズムという言葉が表すのは、様々なステークホルダーの存在ではなく、非国家主体の優位性である」と見抜いた。政府はマルチステークホルダーな機構の外側で法律や制度を作ることができる。さらに民間企業は製品やサービスを通じて、自らの価値を社会に反映できる。したがってマルチステークホルダリズムの一番の受益者は市民社会と括られるグループである。

者が集って議論を行い、その様子はインターネット技術を使って、リアルタイムで世界中に配信されている。原則的には、誰もが政策決定のプロセスをつぶさに知ることでき、意見を出して参加できるのである。

インターネットとサイバー空間のガバナンスにマルチステークホルダリズムという原則が、現在でも根強く残る理由はいくつか考えられる。なかでも、初期インターネットの管理者、そして利用者の多くが先進民主主義国の出身者であったことは大きかった。米国の、特に西海岸のリベラルな風土がインターネットガバナンスに持ち込まれた[35]。

第３項 サイバー空間がもたらす民主主義

サイバー空間は情報をあまねく市民に広め、情報格差を緩和し、この世にバラ色の民主主義をもたらすと考えられていた時期があった。この期待にはそれなりの根拠がある。

1 つ目は民主主義の特質からして、サイバー空間は良質な民主主義をもたらすという論理である（横江 2008: 3–4）。ロバート・ダール（Robert Dahl）は、「大きな規模のデモクラシー」には 6 つの要素が必要であるとし、その 1 つに「多様な情報源」を挙げている（Dahl 2005: 193）。同じくバーナード・クリック（Bernard Crick）は「近代デモクラシー」の 11 の要件の 1 つとして「情報の普及」をあげた（Crick 2002: 91）。サイバー空間の情報を世界中に、大量に、一瞬で、双方向にやり取りするという性質は、「多様な情報源」を確保し、「情報の普及」をもたらすと考えられていた。「インターネットは人々をエンパワーする。エンパワーされた人々が「創発的なアクティビズム」を展開し、国際政治の中で発言力を持つ」（土屋 2007: 170–75）ことが期待されたのである。

2 つ目に、体制に不都合な情報を隠すことで正当性を維持していた情報支配国家は、相対的に不利になると考えられていた。この捉え方が最高潮に達したのは、2010 年か

---

[35] フランスのマクロン大統領は「現代のサイバー空間の管理モデルはカリフォルニアモデルと中国モデルであり、両者がせめぎ合っている。しかし、正解はそのどちらでもない」と、現在の体制に占めるカリフォルニアモデルの存在を指摘する（Macron 2018）。

ら 2012 年のことである。中東において「アラブの春」と呼ばれる一連の民主化の波が起こった。チュニジア、エジプト、リビアなど複数の国で、ソーシャルメディア上の投稿がきっかけとなり独裁体制や権威主義体制をとる政権が転覆した[36]。

3 つ目はサイバー空間が生まれた時代背景に求めることができる。東西冷戦の終わりとインターネットの始まりは、歴史年表ではほぼ同時期のことである。当時、冷戦終結によって民主主義体制の勝利が確定するという見方に説得力があった（Bremmer 2010; Fukuyama 1993）。実際に 1989 年にポーランドが民主化し、その後 10 年の間に 16 の国が民主化した（Hunt 2019）。サイバー空間を抜きにしても、世界は民主化に向かっていると信じられていたのである。

第 4 項 サイバー空間と民主主義の関係の変化

これまで論じてきたとおり、サイバー空間は民主主義的に管理されるべきであり、サイバー空間の拡大は世界に民主主義を広げるという見方が大勢であった[37]。それがピークに達した 2010 年代前半以降、両者には疑問が呈されている[38]。

情報支配国家はサイバー空間を上手に使いこなし、市民の監視や言論の統制を、極め

---

[36] アラブの春とその当時のインターネット上での統制については山本達也の 2 つの研究を参照した（山本 2005, 2006）。

[37] サイバー空間がむしろ民主主義を阻害する可能性を指摘したものとしてはサスティーン（2003）が代表的である。民主制度は、広範な共通体験と多様な話題や考え方への思いがけない接触を必要とするが、サイバー空間は自分と違う意見に触れる機会が少ない場であるというのが、根拠の 1 つとしてあげられた。

[38] サイバー空間への疑念として代表的なものは例えば以下のようなものがある。「かつて世間一般の通念（Conventional wisdom）とか市民社会をエンパワーし、集合を助けるとおもわれていたプラットフォームは社会の病という認識に変わりつつある（Deibert 2019: 25）」。あるいは、東浩紀のインタビューでの以下の発言。「10 年前と今とでもっとも違う点は、『ネットを使うと新しい時代が作れる』という希望の有無だと思います。僕はその希望はもうないと思っている（村上 2019）」。

て低コストで実施しているという指摘[39]がされるようになった。民主主義を助けるどころか、「パノプティコンの高度な現代版ではないかという疑い」（神里 2015: 29）が生まれたのである。また本章の冒頭に触れたように、民主主義にとって重要な公正な選挙は、サイバー空間によってより直接的に脅かされている。

かつてマイクロソフトの研究所でデジタルデバイドに関する研究を行った、ミシガン大学の外山健太郎は、インターネットを構成する技術もこれまでの技術革新と同様に、技術自体に体制を変える力はなく、力を持っているものが使えばその力を増幅させるだけの存在ということを主張している[40]。クリストファー・アータートン（Christopher Atterton）はインターネットが議論の場として活用できるか、政治のどの部分で利用できるのかについて研究を行った（Arterton 1988: 620）。双方向の情報の流通は、市民が情報を知らされるばかりでなく、思考を操作され、誘導される危険をはらんでいることを 1988 年に予言したアータートンの指摘は、30 年を経た今も鮮やかである。サイバー空間やインターネットという場が世界にバラ色の民主主義をもたらすというのは、テクノロジー万能論の延長にある、根拠のない期待であった[41]。

---

[39] フランシス・フクヤマの「文明の終わり」に描かれた自由民主主義の定着に当初から懐疑的な立場をとった研究者の一人が、ネオコンとして知られるロバート・ケーガン（Robert Kagan）である。ケーガンは自由民主主義が広がったのは、思想の優越ではなく、武力を含めた力を民主主義国家が有していたからと主張した。ケーガンの主張は一貫しており、2019 年になってサイバー空間を上手に活用した権威主義の再興を論じている。

[40] Toyama（2015: 247）はこれを増幅の法則（The Law of Amplification）と名付けた。

[41] ここでは明示的に論じていないが、2016 年の米国大統領選挙を機に、サイバー空間の動向とはまったく独立した動きとして、民主主義そのものが危機に晒されているという見方が支持を得ている。例えば、Levitsky&Ziblatt（2018）は民主的な選挙を経た指導者が、自らの権力を用いて民主主義を静かに破壊する現象を、民主主義の歴史とともに紐解いた。また、インターネットを通じた政治活動の失敗を宇野（2020: 14）は次のように分析する。「今日において明白なのはソーシャルメディアによる『動員の革命』とはポピュリズムの一形態に過ぎないということだ。その動員力はテレビのそれよりも弱い。しかし、よりアクティブで熱狂的な参加者がそこには集う。（中略）それはテレビのそれよりも、より短期で、そして熱量の高い分冷めやすく、思慮を欠いたポピュリズムに過ぎなかったのだ。」

第５節　国家主権

第１項 サイバー空間における国家主権とは

ここまで論じてきたように、情報拡散国家は伝統的にサイバー空間をグローバルな空間ととらえ、民主的な統治を好ましいと判断し、その実現に向けて直接的、間接的に支援を行ってきた。これは裏を返せば、サイバー空間における主権の確保は最重要課題ではなかったということを意味する。しかし、様々な事情から、情報拡散国家もまたサイバー空間における自国の主権確保に乗り出していることを、本節で論ずる。

先立って本論文における国家主権という言葉の意味するところを明らかにしておきたい。国家主権という言葉について、スティーブン・クラズナー（Stephen D. Krasner）はその意味の曖昧さを指摘し、少なくとも 1）相互依存的主権: 国境の内部及び国境を超える諸活動を管理する政府の能力、2）国内的主権: ある政体における権力の構造、3）ウェストファリア主権: 国内の権力構造の、外的影響力からの事実上の独立、4）国際法的主権: 国際法に認められる主権の 4 つに分けて考えるべきとしている（クラズナー 2001: 47）。例えば、台湾は実態としてウェストファリア主権を確保しているが、国際法的主権を持っていない。EU 加盟国はウェストファリア主権をもたない。1990 年代のアフリカ諸国は国際法的に主権を認められても、相互依存的主権や国内的主権を持たなかったとクラズナーは言う。

この整理に従えば、サイバー空間における国家主権とはいったいどれに該当するのであろうか。国際法の観点でいえば、2013 年と 2015 年の国連政府専門家会合では国連憲章に規定される国家の「固有の権利」（inherent right）を含む国際法がサイバー空間に

適用されることで合意している。そして「サイバー空間に主権原則が適用される[42]」と確認された[43]ものの、そこには情報拡散国家と情報支配国家のスタンスの違いがあることが指摘されている。河野によれば、米国はサイバー空間における主権を領域主権の延長で捉えているが、中国にとっての主権とは、政府がインターネットを規制する権利のことである（China Institute of Contemporary International Relations et al. 2019; 河野 2015: 26–27）。情報拡散国家はサイバー空間における主権の存在を認めるが、その主権は領域主権の延長であり、表現の自由を支持する観点から政府の介入を抑えることが常に念頭にあった（八塚 2017: 3）。また国連憲章には内政不干渉の原則があるが、そこに選挙システムへの干渉が含まれるか合意はない（Hunt 2019）。つまり情報拡散国家において「サイバー空間に国家の主権が認められる」という理解は、通信インフラが物理的に存在する国に対して、通信インフラへの国家主権が及ぶという意味であり、国家がサイバー空間を分割し、それぞれに対してウェストファリア主権が及ぶわけではないという主張と、今のところ捉えることができる。そして、この主権の解釈は、インフラを自国内に多く抱える国家にとって有利なものであり、そうでない国にとってインフラを自国に抱え込むモチベーションとなる。

サイバー空間における国家主権の概念が大事なのは、これが、どのような行為を（領域）主権の侵害とみなすかの土台となるからである（Schmitt & Vihul 2017）。陸海空などの従来の空間においては、軍艦・軍用機等による領域侵犯や侵略行為などが主権侵害

---

[42] 2015 年の国連政府専門家会合のレポートでは「国家は自国領土内にある ICT 危機の管轄権を有する（パラグラフ 28（a））」と明示的に管轄権が認められたが、主権については、複数の解釈の余地がある記述となっている。したがって「サイバー空間に主権原則が適用される」とはみなせないという分析もある。

[43] 宇宙空間は 1984 年発効の月協定 11 条で「月および全ての天体（天然資源）は人類の共有財産であり、国家主権の主張、使用、占拠などによっても国家の占有物とならない」と明文化された。サイバー空間に主権が認められるという政府専門家会合の合意は条約・協定などのハードローではないとはいえ、コモンズであることが明文化されている月との比較において国家主権が及ぶことはよりあからさまに認められていると言える（鈴木 2011: 264）。

とみなされてきた。サイバー空間におけるいかなる行為が主権の侵害とみなされるのか、主権の定義と合わせて、国際社会に共通理解は形成されていない。また英国のように、あえて「現在の国際法においてサイバー空間における主権の侵害が禁じられているかというと、そうでもない」として、自らの取りうる選択肢を減らさないものもいる[44]。

第２項 情報拡散国家がインターネットを規制する権利を求める背景

少なくとも領域的主権が認められそうなサイバー空間であるが、情報拡散国家はそこからさらに「自国のインターネット」をより明示的にコントロールする「ウェストファリア主権」を希求しているように見える。

一例としてフランスをみていく。2018 年 11 月、パリで開かれたインターネットガバナンスフォーラムでスピーチを行ったフランスのエマニュエル・マクロン（Emmanuel Macron）大統領は苛立ちを隠さなかった。「サイバーセキュリティ対策は不十分である。サイバー空間には規制が必要である」（Macron 2018）という趣旨の発言が、中国でも、ロシアでもなく、フランスの元首から発せられたことに会場からは戸惑いの声があがった（遠山 2019）。会場にいた、多くの参加者はインターネットガバナンスフォーラムの参加者であり、これまでチュニスアジェンダを庇護してきた立場の者であったことを考えれば[45]、このスピーチが不評だったのは頷ける。ここでは、サイバーセキュリティの視点からマクロン発言をあえて擁護する論を展開し、それを通して情報拡散国家がグローバリゼーションや民主主義をある程度犠牲にしても、ウェストファリア主権を手にし、

---

44 サイバー空間における国家主権の侵害は国際法で禁じられているか、という点について西側諸国でも意見が分かれている。オランダ、フランスなどは、主権の尊重は国際的な法的義務の一環であるという立場である。対する英国は主権の尊重は国際法の基本原理ではあるものの、義務ではないという立場である（The Attorney General Jeremy Wright 2018）。

45 チュニスアジェンダは国連などの支援で開催された 2005 年の世界情報社会サミットの合意文書である。この中ではインターネットのガバナンスについて「政府、プライベートセクター、市民社会がそれぞれの役割を果たす」と明記されている（WSIS 2005: para 34; Maurer 2017）。

サイバー空間を規制する必要性を認めていることを主張したい。マクロンの発言の背景には少なくとも 3 つの大きな要因がある。

1 つ目はフランスのインターネットガバナンスへの長年の不満である。フランスは ICANN と米国の持つ ICANN への影響力に長年疑問を呈し続ける、数少ない情報拡散国家であった。2014 年にワインを巡る.wine というトップレベルドメイン名の利用をめぐり、フランス政府と ICANN が衝突したという経緯もある。

2 つ目にフランスはサイバー空間のセキュリティが、市民の生命に直結するということを肌で知る国である。2015 年パリ同時多発テロは、テロリスト同士がガールフレンドの携帯電話を借りて、あるいはオンラインゲームのチャット機能を使ってコミュニケーションを取っていたことが後に明らかになった。死者 130 名、負傷者 300 名以上を出したことについて、インテリジェンス機関や治安機関に対する非難の声が高まり、市民のプライバシーを重視するフランス伝統の気風は弱まった。

3 つ目にマクロン自身が大統領に選出される経緯をあげたい。2017 年 4 月に行われた大統領選挙の第 1 回投票で本命と言われていたマクロンは 24%の得票率で首位に立った。世間を驚かせたのは民族主義的スタンスで知られる国民戦線のマリーヌ・ル・ペン（Marine Le Pen）が 21%と下馬評以上に支持を得たことである。勝利の行方が見えないなか、決選投票までの期間に、マクロン陣営のメールが流出し、匿名掲示板やウィキリークス（Wikileaks）を使って拡散され、それを対立候補陣営がさらに広めようとした。決選投票ではマクロンが 66%の得票を獲得し、圧勝したが、この件がマクロンに与えたインパクトは想像に難くない[46]。

このような事件が再発するのを防ぐために、治安の維持と政治の安定を実現するため

[46] 選挙後の 2018 年 8 月にフランス外務省と国防省の共同チームが作成した、大統領選挙にまつわる情報操作についてのレポート（Vilmer et al. 2018）が公開され、その中では極めて直接的な表現で、ロシア政府による選挙干渉を非難している。

に、フランスは、そして情報拡散国家は表現の自由を一定程度犠牲にする必要がある[47]というのがマクロンの主張である。それは現代のサイバー空間の実態をふまえた、現実的な提案であるとも言える。

これまでであれば、サイバー空間に対して規制を求めるのは中国やロシアなどの情報支配国家であり、それに対して情報拡散国家が言論の自由を根拠に反論を行った。しかし、サイバー空間の拡大によって引き起こされた、主権を巡る対立は権威主義の非民主主義国家とリベラルな自由を愛する国家の戦いというだけではとらえきれなくなっている。それはまた、「歴史を持つコスモポリタン思想を持つ国家と国家の主権に確証を持てない歴史の浅い国家の争いという側面も持つ」（Nocetti 2015: 129）と先行研究にも指摘されている。ここまで見てきたフランスの例は、グローバリゼーションや民主主義は国内における不幸な出来事、例えば、大規模なテロなどで一夜にして後退することを物語っている。

第6節　待ち受ける3つのシナリオ

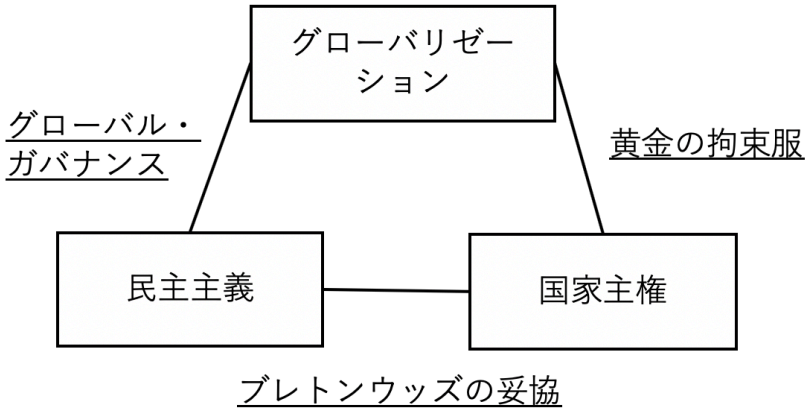
第1項 世界経済の政治的トリレンマの原理はサイバー空間にどう表現されるか

ここまで情報拡散国家が、サイバー空間におけるグローバリゼーションと民主主義と国家主権を並行して求めてきたことを論じてきた。ここで再び分析の土台となるロドリ

---

[47] 表現の自由の維持と、政治の安定のジレンマは繰り返し議論されてきたテーマである。オーストリアのサイバーセキュリティ研究者アレックス・クリンバーグ（Alexander Klimburg）らによれば国家のサイバーセキュリティは5つのジレンマを抱えている。経済の発展と国家安全保障の向上、インフラの近代化と重要インフラの防護、民間セクターと公共セクター、データの保護と情報の共有、表現の自由と政治の安定の5つである。そして伝統的に民主主義国は表現の自由に重きをおいてきた（Hathaway & Klimburg 2012: 34）。

ックの世界経済の政治的トリレンマの原理を振り返る。ロドリックによれば、現在多くの民主主義国家が実現しようとしているグローバリゼーション、民主主義、国家主権の3つの目標は並立しえない。図表 2-2 に示すように、どれかを捨て、グローバル・ガバナンス、黄金の拘束服、ブレトンウッズの妥協のいずれかのシナリオを選ぶことを迫られている。それぞれがサイバー空間にどのような変化をもたらすかを、考察する。



図表 2-2 世界経済の政治的トリレンマの原理（再掲）

第2項 グローバル・ガバナンス（国家主権を捨てたサイバー空間）

サイバー空間における国家主権を手放し、グローバルな民主主義体制を打ち立てることは理論上可能である。具体的な形態としてはサイバー空間における国家の権限を、ICANN などの民主主義の原則が生きるインターネット管理団体に移すという形が想定される。インターネット初期の頃から、ドメイン名や IP アドレスの管理などについては実際にこの形態がとられていた。そしてすでに論じてきたように、インターネットが普及してから、2010 年代前半まで、情報拡散国家が無意識に思い描いていたサイバー空間のあるべき姿は、このグローバル・ガバナンスの追求であった。

このシナリオの勝者、つまりこのシナリオによってより多くのデータにアクセスすることが可能になるのは、情報拡散国家とグローバルテックカンパニーである。情報拡散

国家の一般市民はグローバルなサイバー空間とその運営へのなんらかの形での参加を保証される。他方で、サイバー空間において国家よりも力を持つ組織をどう統制するのかという新たな問題も浮上する。サイバー空間はおそらく「一般市民が自由に扱える技術ではない。その専門性は、時として排他的な集団を形成し、その集団が共有する利益を増進することにつながる。このような専門家集団は、リスクのある科学技術であっても、そのリスクを軽視し、科学技術の発展を進め、それを応用して産業として勧めていく傾向を持つ」（鈴木 2015）という専門家システムと呼ばれる新たなリスクに配慮しなければならない。

仮に専門家システムの問題を超克できたとしても、サイバー空間が国家安全保障と密接に結びつく時代に、このシナリオの実現可能性には懐疑的にならざるをえない。もともとサイバーセキュリティは「安全保障という一般にグローバル・ガバナンスがもっとも当てはまらないと考えられている分野」（渡辺・土山 2001: 13）の一部分である。安全保障は国家の専管事項であり、国家が関与しないという選択が許されるとは考えがたい。仮に、多くの国家がサイバー空間の統治を手放すという決定をした場合、世界政治における政府なき（良き）ガバナンスという、極めて大きな問題をサイバー空間にもたらす。それが「グローバル・デモクラシーを促進するのか、あるいは国境を超えてさらなる無秩序を招来するのか」（南山 2015: 93）、誰にもわからない。グローバル・デモクラシーの実現には 100 年単位の時間がかかるとされている。多くの国際関係論の専門家は、近い将来においては無秩序を招く可能性の方が高いという判断をするだろう。

一方で、サイバー空間におけるグローバル・ガバナンスは決して荒唐無稽な考え方でもない。繰り返しになるが、これは少なくとも、インターネットやサイバー空間の創成期において信じられていた統治の形態である。そしてこの後の第４章で詳しく論じるとおり、サイバー空間に強い影響力を持つグローバルテックカンパニーが自らの利益を最大化しようと考えた場合に、個別の国家による規制を取り払い、グローバルに均一なサ

ービスを提供するのが理にかなっているからである。

第３項 黄金の拘束服（民主主義を捨てたサイバー空間）

国際的なやり取りのコストを低下させるために民主主義を規制するというシナリオであり、現実的に現在の中国がとっている政策である。西側諸国から国家による監視や、市場の閉鎖性を繰り返し非難される中国であるが、実際に中国国民からインターネットが不便という声はなく、表面的に様々なオンラインサービスの充実度は多くの西側諸国を凌いでいる。

このシナリオがとられた場合、サイバー空間にグローバリゼーションと国家主権が同時に確保される。予想されるのは、国連のようなマルチラテラルな国際機関の下にサイバー空間にかかわる重要な決定や、セキュリティの確保、資源管理を所管する新たな組織を作ることである。

このシナリオの勝者は情報支配国家およびグローバルテックカンパニーである。グローバルテックカンパニーとユーザは封建的な関係で結ばれている。「企業が封建領主さながらに一方的に優位に立ち、ルールはいつ変更されるかわからない」（シュナイアー 2016: 333）からである。いわゆるウェブ（World Wide Web）を発明したティム・バーナーズ=リー（Tim Berners-Lee）は、政府と企業の両方の行動を制限し、情報化時代の企業に権利だけでなく責任を課すべきと、サイバー空間版のマグナ・カルタの必要性を説いている（フランス通信社 2014）。バーナーズ=リーはテックカンパニーの利潤追求がグローバリゼーションを推進しても、民主主義を力づけないという構造を問題視しているのである[48]。

---

[48] バーナーズ=リーのサイバー空間版のマグナ・カルタという発想は、コントラクトフォーザウェブ（Contract for the Web）として 2019 年に正式公開された。国家、企業、市民に対してそれぞれ 3 つの規範を提示した。このうち、企業については以下の 3 点を求めた。①インターネットを誰もが利用し、アクセスできるように保つこと、②オンラインの

現在のグローバルテックカンパニーの力は強大である。米国の 3 社（グーグル社、フェイスブック社、マイクロソフト社）と中国の 1 社（テンセント社）が 10 億人以上のユーザを獲得している（シュワブ 2019, 11）。GAFA と総称されるグーグル社、アマゾン社、フェイスブック社、アップル社の合計売上は 70 兆円を超え、日本の税収 60 兆円を凌ぐ。国連大学の推計によるとグローバル企業全体の法人税の徴収逃れ額は年 5000 億ドル（約 56 兆円）に上る（菊地 2019）。

テックカンパニーは世界中のユーザに便利なサービスを提供している。しかし、民主主義や判断の透明性は彼らの優先課題ではない。サイバー空間の利便性が向上するが、そこに民主主義によるオーバーサイトはない。これは多くの情報拡散国家にとって、特に米国にとって[49]、受け入れがたいシナリオであろう。

第 4 項 ブレトンウッズの妥協（グローバリゼーションを捨てたサイバー空間）

ブレトンウッズの妥協とは、グローバリゼーションを規制し、個々の国における民主的正当性を固めることである。ロドリックはトリレンマを提示した上で、国際経済についてブレトンウッズ体制期のように、グローバルな市場経済を「再度」国民国家の統制下に置くことが最も妥当という指摘をしている（西川 2017: 40）。現代社会におけるブレトンウッズの妥協の実例としては国際金融体制があげられる。各国は通貨の発行を含

トラストを確立できるようプライバシーと個人情報を尊重し保護すること、③人類の最良をサポートし、最悪を克服する技術を開発すること、である（contractfortheweb.org 2019）。

[49] 代表的な論としては「21 世紀のアメリカは何を目標とすべきなのだろうか。我々は、『世界のすべての国が民主主義国になる』ために創造的に、根気よく、懸命に行動しないといけない」というイアン・ブレマー（Ian Bremmer）の発言をあげたい。ブレマーはさらに「選挙の実施を求めるだけでは不十分だ。アメリカ政府は、法の支配、言論の自由、宗教の自由、集会の自由、そして人権の尊重を推進するために、こういった手段すべてを使っていくべきだ」（イアン・ブレマー 2015: 198）と米国の価値観を強く打ち出すことを主張する。

め、その多くを統制している。一方で国境を超えた経済活動もまた行われている。

サイバー空間はブレトンウッズの妥協を受け入れられるだろうか。言うまでもなく、インターネットはグローバルなインフラである[50]。2008 年から 2014 年までの間に無料音声通話サービス「スカイプ（Skype）」を利用した通話は 5 倍になり、2005 年から 2012 年までの間に国境を超えた通信の量は 18 倍になった（Manyika et al. 2014: ii-iv）。しかし、普遍であったはずのエンドツーエンドの接続性は 15 年以上前にファイヤーウォールと NAT というセキュリティ対策などを目的とした技術によって絶滅した。さらにインターネット上をとびかう情報への国家の監督権が認められるべきという言説が指示を得るようになってきた。ここに個別の国毎に、国家単位での規制が行われる、インターネットの分断が起きるのである[51]。

このシナリオの勝者は、再び意思決定の中枢を握る情報拡散国家と情報支配国家といえる。情報拡散国家は国家毎に異なる制度と両立しうる範囲内に、グローバル化のレベルを制限する。データは国境の内側に蓄えられ、サイバー空間の相互接続性は損なわれ、利便性は下がるだろう。それはグローバルな市場から最大限の利益を得たいグローバルテックカンパニーの思惑とも背反する。

第 7 節　まとめ: サイバー空間のトリレンマ理論

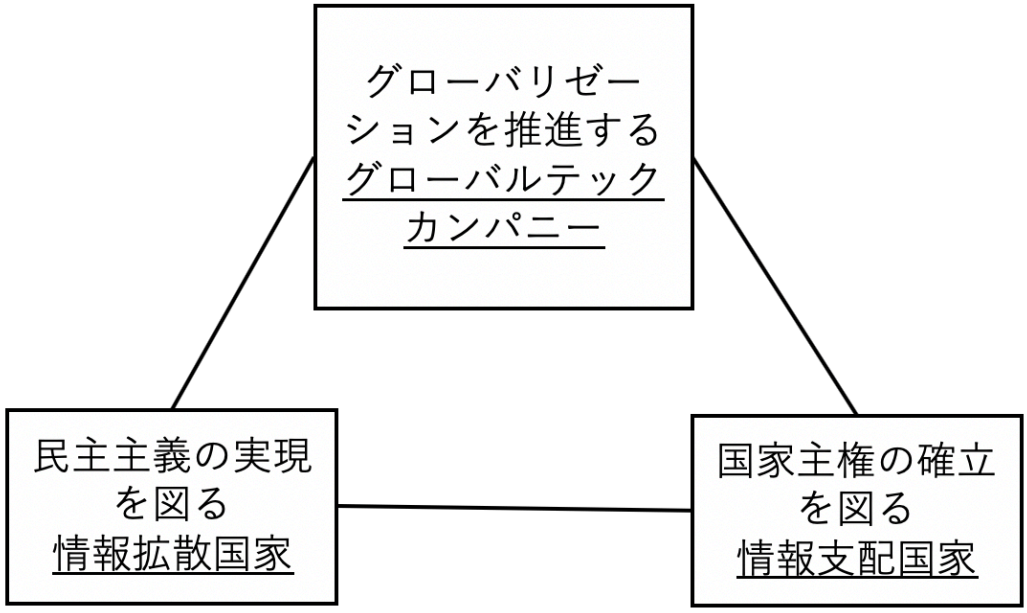
ロドリックの世界経済の政治的トリレンマの原理を応用して、現在のサイバー空間の

---

[50] インターネットが、あるいはサイバー空間がグローバルであるというのはどのような状態か。本論文では Hill（2012）に従い、「ある Web サイトが中国にいてもチリにいても同じように見えること。どんな場所にいても、どんなコンピュータを使っていても、どんなユーザがみても同じ経験を得る状態」とする。

[51] インターネットの分断を研究した Mueller（2017: 18-19）は大規模な分断は起こらないと結論づけた。その理由として、グローバルなインターネットのネットワーク効果、経済的な利益は現在も強く、まだ強くなり続けていることなどを挙げた。

ガバナンス、そしてサイバーセキュリティのガバナンスを説明できることがわかった。そしてサイバー空間においては、民主主義と国家主権とグローバリゼーションを推進しているのが、それぞれ情報拡散国家、情報支配国家、グローバルテックカンパニーと捉えると、図表 2-3 に示したとおり、本論文全体を通じて骨格となるサイバー空間のトリレンマの構図が浮かび上がってくる。これを今後、本論文ではサイバー空間のトリレンマ理論と呼ぶ。



図表 2-3 サイバー空間のトリレンマ

情報拡散国家はサイバー空間において、グローバリゼーションと民主主義を一貫して追求してきた。その背景にはサイバー空間とインターネットの創成期において米国という国が一貫して主導的な立場にあったことがあげられる。一時、インターネットと民主主義の蜜月と呼べる期間があったことは疑いの余地があまりない。しかし、本章第５節第２項のフランスの例からも明らかなように、国家として国民の安全の確保を図る必要が増し、そこに国家主権を確立するという新たな目標が加えられた。社会の安全と自由

な情報の流通を両立することが困難になってきているのである（土屋 2015b: xiv）。情報拡散国家は国家主権の確保に舵を切ったが、そのことによりサイバー空間におけるグローバリゼーションもしくは民主主義を諦める覚悟をしているか、言い換えればトリレンマを理解しているかは定かでない。

情報拡散国家が、この矛盾した状況を打開するためには、グローバリゼーションと民主主義と国家主権の 3 つのうちのいずれかを諦めるための議論を始めなければならない。第 6 節の分析によれば、グローバル・ガバナンスの道は険しく、黄金の拘束服のシナリオは現代の覇権国家である米国の戦略に反する。したがって現時点で情報拡散国家にとれる次善の策とはブレトンウッズの妥協、つまりグローバルなインターネットを民主的な国民国家の統制下に飼いならすという道である。

情報拡散国家がサイバー空間におけるグローバリゼーションを捨て、国家主権を重視しだすことに「こんなはずではなかった」という感情を抱いていることを本章の冒頭に述べた。その変節は、インターネットにおいては誰もが対等で、生活と自由と幸せを追求する場であるべきというリベラルな価値観を損なった。自らをサイバーリバタリアンと呼び、2013 年に米国インテリジェンス機関による大規模なサーベイランス活動の存在をリークした米国家安全保障局（NSA）の元契約職員エドワード・スノーデンはこう言う。「インターネットは誰もが対等で、生活と自由と幸せを追求する場だった。そしてその考え方はアメリカの建国の意図、そして合衆国憲法と相似している。国とインターネットに裏切られ、私は考えを変えた」（Snowden 2019: 11:17）と。情報拡散国家を容易ならざる立場に追い込むもう 1 つの理由は、「こんなはずではなかった」「裏切られた」という負の感情である。それは様々なきっかけで爆発する。現代に残るリベラルなインターネット観の残滓が、情報拡散国家の足かせになっている。

次章以降では、情報支配国家とグローバルテックカンパニーの戦略について目を向けていく。

第３章　情報支配国家

第１節　はじめに

第２章では情報拡散国家が、サイバー空間におけるグローバリゼーションと民主主義と国家主権を並行して求めてきたことを論じてきた。そしてロドリックの世界経済の政治的トリレンマの原理を応用し、サイバー空間のトリレンマ理論を提起した。ポイントはサイバー空間にグローバリゼーションと民主主義と国家主権の 3 つが共存しないことである。つまり情報拡散国家から発せられるサイバー空間をめぐる発言は、大いなる矛盾をはらんでいる。ここに新たな疑問が浮上する。それはサイバー空間が古典的な国際政治でいうアナーキー状態であると仮定して、本論文の主張どおり、情報拡散国家の立場が悪くなっているとするならば、相対的に情報支配国家が力を得ているのかというものである。第 1 章第 4 節第 2 項の繰り返しとなるが、情報支配国家とは中国、ロシアや中東諸国に代表される、国家による情報支配の重要性が高い国家群を指す。権威主義体制がとられることの多いこれらの国々では、サイバー空間における情報の自由な流通よりも、治安の維持や政治の安定が優先される。ゆえに国家や政府によるサイバー空間の管理の必要性を正当化されやすいという特徴がある。本章では現代のサイバー空間において個別の情報支配国家の戦略を紐解く。

本章の構成は以下のとおりである。まず第２節では中国、第３節ではロシアという二大情報支配国家に固有の戦略について、主に 2017 年以降の政策決定を中心に振り返っていく。第４節では北朝鮮の戦略を解説する。第５節でこれらの議論を総括する。

分析対象として中国とロシアと北朝鮮の 3 カ国をとりあげたのは、3 つの国が情報支配国家というグループの中で特別な位置付けにあると考えるからである。まず中国は自

国内に情報通信産業が発展し、サイバー空間のグローバリゼーションによる経済的恩恵を十分に受けているという特異な情報支配国家である。次にロシアは建前としては憲法に民主主義が謳われており、グローバリゼーションと民主主義の 2 つのいずれを取るかの決断を迫られている。さらにロシアからはかつての超大国が、新技術によって力を削がれた場合の戦略を汲み取っていきたい。最後に北朝鮮であるが、これはグローバリゼーションも民主主義も価値をもたない、ごく一部の特権グループによる国家運営が行われている国のサイバー空間における戦略のケーススタディと考えることができる。3 カ国ともに日本に近接し、日本の安全保障環境に大きな影響を与える重要な国であることも付け加える。

情報支配国家はサイバー空間をうまく活用し、その力を蓄えているが、それでも全体的に強い安全保障上の脅威を感じている。サイバー空間における米国の影響力は圧倒的である。その一例として、米軍と米インテリジェンス機関が持つサイバー攻撃能力の洗練度があげられる。世界で最初のサイバー軍をたちあげ、サイバー攻撃のノウハウを蓄積してきた米軍は、近年その攻撃能力を隠すことなく、むしろ抑止効果を期待し、その存在をアピールしていると言っても差し支えない状況である。また米国は同盟国にも同調を呼びかけている。情報支配国家が脅威を感じないと考えるのは不自然である。

逆に、多くの情報支配国家が情報拡散国家との比較において有利なのは、多国間議論における味方の多さとその論理の整合性である。第２章第３節第２項「米国への不信」ですでに論じたとおり、国連のような国家が一国一票で議決を行う場においては、情報支配国家の論理は数の多い途上国の支援を得やすい。もともとサイバーセキュリティ政策を決定する上での、大きな変数は国内政治の安定度である。サイバーセキュリティのガバナンスを巡る対立は権威主義、全体主義国家、非民主主義国家の連合とリベラルな自由を愛する国家の戦いというだけではとらえきれない。それはまた、「歴史を持つコスモポリタン思想を持つ国家と国家の主権に確証を持てない歴史の浅い国家の争いと

いう側面も持つ」（Nocetti 2015: 129）。情報支配国家と多くの発展途上国家は後者であり、政策の親和性は必然的に高くなる。情報支配国家は味方が多いのである。

そして論理の整合性というのは、第２章第２節「本章における**エラー! 参照元が見つかりません。**」で論じたとおりであるが、現代の情報拡散国家はサイバー空間にグローバリゼーション、民主主義、サイバー空間における国家主権の 3 つの目標を同時に追求している。国際経済学の研究では、この 3 つが併存できないことがすでに指摘されている。しかし、情報支配国家はサイバー空間が民主主義の原則に従って管理されることを望んではおらず、3 つが併存しないことについてなんら問題がないのである。今後数年にわたって情報拡散国家は、これまで自らが展開してきた、「サイバー空間はグローバルな公共財であり、国家の主権が認められない」という言説を撤回しなければならない。つまりサイバー空間は国家の主権が及ぶ領域であると説いて回らなくてはならない。市民社会からの反発は大きいだろう。情報支配国家はこのような、負債を背負っていない。情報支配国家の主張は論理整合性が高い。

第２節　中国

第 1 項 サイバー大国中国

GDP 世界第 2 位を誇る経済大国中国はサイバー大国でもある。2011 年の広告代理店による調査では世界トップ 50 の Web サイトのうち 8 つが中国企業によるものである[52]。別の調査では訪問者数の世界トップ 20 のウェブサイトのうち、7 つが中国企業によって所有・運用されているとされた。移動通信の新規格 5G 関連技術、AI、量子コンピ

[52] 調査の内容については Grumbach の研究を参照した（Grumbach 2013）。元となったイギリス資本の広告代理店オグルヴィの調査結果は現在 Web 上に存在せず、確認が取れなかった。なお 8 つの中国企業は以下のとおり。括弧内は順位。バイドゥ（5）、QQ（8）、タオバオ（13）、Sina.com（17）、163.com（28）、Soso（29）、微博（31）、Sohu（43）。

ューティングなどの国際関係に影響を与える新技術分野への投資も活発に行われている。中国の GDP は毎年 7%近い成長をしている。それを支えるのはデジタル経済とよばれる、デジタル技術を活用したビジネスである。GDP に占めるデジタル経済の割合はおよそ 26.6%（2015 年）から 32.28%（2017 年）まで急増した（Sui & Guan 2018: 252）。

一般に中国の製品は安価で、調達までの時間が早い。西側の企業が利用者のプライバシーへの配慮から採用しない技術も用いるため、情報のコントロールという観点で優れている部分もある。中国製品の泣き所は、製品に中国政府と情報を共有するスパイプログラムが埋め込まれているなどのセキュリティ上の懸念である。しかし、今後も中国製品の採用は止まらないだろう。中国製品を使うことによる情報漏えいの確たる証拠が公の場に示されることはなく、中国の情報活動の危険性について問われたマレーシアの首相マハティール・ビン・モハマド（Mahathir bin Mohamad）が「マレーシアにスパイの対象となるような情報があるだろうか?」と強がったことからも分かるように、セキュリティ確保の重要性は時と場合によって異なるからである。

第２項 政府の動き

習近平体制はサイバー空間における強国を目指すという姿勢[53]を鮮明に打ち出している。サイバー空間での影響力拡大は、中国経済の発展と強固に結びついており、経済の発展は中国共産党による統治の正当性の土台である。近年の中国は半導体部品などの国産化を強力に推進し、技術的な自給率を高めている。また移動通信の新規格 5G 関連技術、AI、量子コンピューティングなどの新技術分野への助成も活発に行われている。

---

[53] 一帯一路は 2013 年に国家主席となった習近平が、2014 年 11 月のアジア太平洋経済協力（APEC）首脳会議でアピールした。西安交通大学の李長久教授がとなえた「東穏 北強南下 西進」という戦略が元になっているという説がある。「東を安定化する、北を強化する、南下する、西に前進する」という意味でシルクロード経済ベルト（SREB）や一帯一路イニシアティブの狙いに近い（塩原 2019: 169）。

デジタルシルクロードと呼ばれる情報通信技術を用いた中国の影響圏拡大政策は、一帯一路政策の重要なコンポーネントでもある。これは IT 企業（アリババ社、テンセント社、バイドゥ社、ファーウェイ社）と通信事業者（チャイナ・モバイル社、チャイナ・テレコム社、チャイナ・ユニコム社）が一帯一路の対象国の市場で成功することを国が支援する狙いもある（Triolo et al. 2020: 1）。中国の支援で、多くの途上国に海底ケーブル、地上ケーブル、5G 通信インフラ、データセンターなどがもたらされている。

中国のサイバーセキュリティ政策を研究した朱紅穎は、中国におけるサイバーセキュリティの指導機構の変容が 3 つのステージに分けられると指摘した。1986 年から 2011 年までは工業情報化部などの中央省庁がサイバーセキュリティ政策をリードした。その後、2011 年から 2014 年までは国務院が指導し、2014 年から現在に至るまでは中国共産党中央が直接指導する体制となっている。つまりサイバーセキュリティを所管する組織がよりハイレベルになっている（朱 2018: 40–41）。この過程を通じて特に 2014 年以降、サイバー政策と文書が発行される頻度が増している。

現在の中国のサイバーセキュリティに関する戦略策定の中心となるのは中央網絡安全和信息化委員会（Cyberspace Administration of China、以後 CAC）である。CAC の前身は、2011 年 5 月に国務院の中に成立した国家互聯網信息弁公室である。その後 2014 年に中国共産党の中央網絡安全和信息化領導小組という組織に改組され、2018 年 3 月に現在の形に落ち着いた。領導小組の議長は習近平国家主席であり、副議長が李国強首相および劉雲山中央書記処書記の 2 名という体制からも、中国におけるサイバーセキュリティ政策の重要度の高さを推し量ることができる。CAC は中国共産党中央委員会直属機関であり、実質的な政策決定権を持つ。

中国政府は 2014 年から毎年、浙江省烏鎮で世界インターネット大会（World Internet

Conference）という国際会議を開催している[54]。世界中のサイバー関連分野のリーダーを招聘し、中国の戦略を世界に普及するための会議である。この会議の運営も CAC が行っている。

中国サイバーセキュリティ法（網絡安全法）は国際的な注目を集めた。EU における一般データ保護規則と同様のデータのローカライゼーションを図る条項が含まれたからである。2017 年 6 月に施行された同法によって、VPN サービス[55]利用が規制され、掲示板や SNS などへの投稿の管理が強化され、中国国外でのサイバーセキュリティ競技活動（ハッキングコンテスト）への参加制限[56]が始まり、また CAC に法を執行するための権限が与えられた。一方で、中国政府が策定した戦略は数多く[57]、法律も日本のように厳格に運用されるとは限らない[58]。したがって国としての中国の戦略を関連の法制度のみから理解することは難しい。

第３項 サイバー空間におけるマルチラテラリズム

では、中国はサイバー空間で何を実現しようとしているのだろうか。他の情報支配国家と異なり、中国はサイバー空間の支配者となりえる。そして意識的か、無意識的か中

---

[54] 世界インターネット大会の模様は実際に出席した者の参加記に頼った（前村 2018; 土屋 2018b）。

[55] VPN とは通信の暗号化技術、またはそれを提供するサービスを指す。中国においては政府の検閲によりアクセスできない Web サイトなどにアクセスするために日常的に VPN サービスが使用されていた。2016 年以降取り締まりが強化された。

[56] 未修正の脆弱性情報を、みだらに公開したり、国外のセキュリティイベントに提供したりしてはならないという通知である。この通知はサイバーセキュリティ法とは別。关于规范促进网络安全竞赛活动的通知（2018/9/7）。

[57] 確認できただけで「サイバー空間国際協力戦略」、「情報通信ネットワークおよび情報セキュリティ計画（2016-2020 年）」、「工業制御システム情報セキュリティ行動計画（2018-2020 年）」、「ビッグデータ産業発展計画（2016-2020 年）」、「クラウドコンピューティング発展三年行動計画（2017-2019 年）」、「新世代の人工智能発展計画」、「工業電子商務発展三年行動計画」 などがある。

[58] 民主主義国家において一般的に認められる三権分立（立法、行政、司法の独立）が認められず、中国共産党がそれらを領導（命令的指導）する政治的地位にあるからである。

国はサイバー空間における自国の立場を主張すると同時に、サイバー空間全体のあるべき姿を繰り返し発信している。あるべき姿とは、つまり中国のサイバーガバナンスの原則とは「サイバー空間における国家主権に立脚した多国間共存」である。

2015 年に世界インターネット大会で登壇した習近平主席はサイバー空間を通じて全人類が「未来を共有する運命共同体」という趣旨の発言をした（Xi 2015）。以来、運命共同体は流行語となり（Cuihong 2018: 655）、サイバー空間のグローバル・ガバナンスを求める機運が高まっていった。中国政府は公式文書でサイバー空間が民主的で、マルチラテラルであり、透明性が高いガバナンスの仕組みを持つべきであると繰り返し主張する[59]。

中国政府が「民主的でマルチラテラルなサイバー空間」を求めるという点には補足説明を要する。本来、マルチラテラリズムとは、本来 3 カ国あるいはそれ以上の国が協調関係の維持を指す（Ruggie 1992）。しかし、中国政府がサイバー空間における発言でマルチラテラリズムという言葉を使った場合、それはマルチステークホルダリズムへのアンチテーゼであり、世界中の国々がより平等な決定権を持つガバナンスを模索する動きの一貫である。マルチステークホルダリズムに支えられる現在のインターネットのガバナンスに対する中国の不信感は強い[60]。

中国はマルチステークホルダーという建前の裏で、サイバー空間において米国の実効的な支配が成立していると考えている。マルチラテラリズムは米国が独占するサイバー空間のための処方箋である。そのためにサイバー空間に国家の主権が認められ、国家の代表者が集うマルチラテラルな議論の場でサイバー空間の統治が行われるべきという

---

[59] 2017 年に中国外交部が公表したサイバー空間における国際協力戦略という名の文書（Ministry of Foreign Affairs - the People's Republic of China 2017）には以下の記載がある。“China advocates building a multilateral, democratic and transparent global cyberspace governance system through the equal participation and joint decision-making of the international community.”

[60] 例えば世界 2 位のインターネット人口を抱える中国の国内に DNS のルートサーバを設置するべきであるという中国の主張は今も実現していない。

論理である。

現在の国際社会において、最も認知されたマルチラテラルな議論の場は国連であろう。ゆえに中国はサイバー空間のガバナンスの議論における国連の役割の重要性を、事ある毎に強調してきた。それは単に自国が安全保障理事会の常任理事国であるだけでなく、国連が最も平等に加盟国を扱う場であるからである。

第４項 戦略の矛盾

サイバー空間にグローバルリゼーションと民主主義と国家主権の 3 つが併存しないこと、それ故に多くの情報拡散国家がサイバー空間のガバナンスについて矛盾を抱えていることをすでに第２章で述べた。対して中国の「民主的なサイバー空間」という言説は一般市民ではなくすべての主権国家の均等な参加を確保しようとする点においてデモクラティックであることを前節で述べた。中国が抱える矛盾は、米国を批判し、デモクラティックなサイバー空間ガバナンスの仕組みを目指しているが、国内においてはまったく別のルールを用いてサイバー空間をコントロールする点である。中国国内では検閲システムが導入され、グーグル社やフェイスブック社のサービスは使用できない。もともと中国政府は、サイバー空間における監視活動に相当量の資源を投入してきたが、2008 年のグローバル金融危機とその後の 2011 年の「アラブの春」を受けて[61]、そのさらなる強化に踏み切ったと言われる（フリードバーグ 2018: 15）。この監視活動については、国家や共産党への批判が主な検閲の対象と捉えられてきたが、実際のところ体制に批判的な発言よりも、集団行動をよびかける、大衆を扇動する発言が最も中国当局が神経を尖らせる点であるようだ（King, Pan, & Roberts 2013: 326）。

米国のヘリテージ財団のディーン・チェン（Dean Cheng）は、こうした中国の情報を

61 「中国共産党がネット空間の統制に乗り出したきっかけは 2003 年の SARS（重症急性呼吸器症候群）が流行して社会的危機が起きたこと」（益尾 2019: 162）という分析もあり、大規模監視の契機は定まっていない。

めぐる活動を「情報ドミナンス（information dominance）」の構築と呼ぶ（Cheng 2016）。情報ドミナンスとはすなわち、「情報の収集、伝達、分析、評価、諜報を敵国よりも速く、正確に実施し、そのうえで、友好国、敵国、第三者の認識や評価を形成し影響を与えること」（八塚 2017）である。

前述のとおり、情報支配国家の中で中国は特殊なポジションにいる。中国政府がサイバー空間のコントロールを求める一方で、多くの中国企業がグローバルに営利活動を行っているという点である。デジタル経済などとよばれる産業の拡大と「サイバー空間における国家主権に立脚した多国間共存」はときに相反する[62]。中国政府は難しい舵取りを迫られている。

第５項 グローバル企業と中国政府

サイバー空間のガバナンスをめぐる中国の立場が難しいのは、他の情報支配国家と同様に国家主権の確保が必要であるのと同時に、サイバー空間のグローバリゼーションもまた中国の発展に欠かせないということである。中国の複数の企業が、オンライン決済やクラウドサービスや通信機器の製造などの分野でグローバルなビジネスを行っている。米中対立の激化は 5G に関する政府調達について、中国企業を排除するという決定をもたらした。問題の背景にあるのは、中国政府もしくは中国共産党と中国企業の関係が不透明であることである。

欧米からの批判に対して中国の通信企業ファーウェイ・テクノロジーズ社（以後、ファーウェイ社）は一貫して自社と中国政府との関係は特別なものでないと弁明してきた。例えば、ファーウェイ社幹部は、同社が日本の経済や雇用に好影響を与えていることを

---

62 「中国製造 2025」に基づいた半導体産業の振興策が象徴的である。中国における急ピッチな半導体関連部品の国内自給率上昇を狙った一連の政策は、部品を海外に頼らず、コストが高くても国内生産のノウハウを蓄積するために巨額の投資を行っている。その規模は一説に 18 兆円である（湯之上 2019: 183）。

強調する[63]。また同社の任正非 CEO はインタビューにこう答えている。

> 我々は欧米に進出すると共産主義から来た企業と思われる。だからこそ現地の法律を守らなければ生き残ることはできなかった。逆に中国に戻ると資本主義と言われる。双方向から睨まれているだけに、規範に乗った行動を取らないと自ら危ない橋を渡ることになる（浜田 2019）。

中国内外の両方から敵視されるというファーウェイ社 CEO の発言には根拠がある。一般にはあまり知られていないが、ファーウェイ社と中国政府の関係はこれまで一貫して良好とは言い難かった。国営企業として発展した同じ通信機器を開発、販売する ZTE 社とは対照的である。中国の改革開放 40 周年記念大会の際に、改革開放に貢献した 100 人が表彰されたがファーウェイ社の CEO の名は無く、また政府が指名した AI 国家戦略に協力する 5 大企業にもファーウェイは含まれないという（遠藤 2019）。中国政府にとっては改革開放の模範的モデルではないものの、製造輸出のトップランナーであり、対外的な中国企業の顔として消極的に支援する対象である。ファーウェイ社と中国政府の関係は、西側研究者がいうような、単純な支配、被支配の関係で言い表すことが難しい。

一方で、ファーウェイ社が、自社と政府の関係について問われた際に、たびたび用いる「ファーウェイ社は株式非公開企業だが、持株会を通じて従業員が下部を持ち合う企業である（政府が所有する企業ではない）」という説明は不正確である。ファーウェイ社の株式は持株会社が 100%を保有する。そして、その持株会社の株式は 1%を創業者

---

[63] 2019 年に中国の北京で開催された会議で、ファーウェイ社の幹部は以下のように述べた。「ハイエンド向け携帯電話端末「P30」の部品 1600 点のうち半分以上は日本製であり、ファーウェイ社は日本の GDP に 700 億以上貢献している。また日本で雇用を 4 万人創出している」（言論 NPO 2019: 49）。

任正非が保有し、残り 99%を工会委員会（Trade Union Committee）という構成もガバナンスのメカニズムも明らかにされていない組織が保有する。工会委員会と共産党との関係性など多くの謎が残っている（Bolding & Clarke 2019）。また中国企業は反産業スパイ法に基づき、①従業員が 3 名以上の党員がいる場合、社内当組織を結成しなくてはならない、②定款に企業の党活動への協力を規定すること、③インテリジェンス活動への協力を隠すことなどが義務付けられる。ファーウェイ社内には 300 以上の共産党支部がある。「（中国企業を）純粋な商業利益を追求するアクターとしてみなすことができないのは明白」という分析にも頷かざるをええない（Cave et al. 2019: 4–7）。

以上は決して中国政府とファーウェイ社に限った話ではない。メッセージングソフト WeChat などを開発するテンセント社には 89 の、E コマース企業アリババ社には 200 の党支部が存在するという。欧米政府は、共産党が民間部門への影響力を持っている以上、中国企業は国から離れた独立した存在ではありえないと考える。そしてその上で中国に対し経済政策と官民の関係の構造改革を求めているのである（ウィリアムズ 2019: 71–74）。中国政府と中国のグローバルテックカンパニーの対立は顕在化していない。実態を外部から窺い知ることは困難である。ここでは、中国は巨大な市場であるが、それでも有限であることを指摘するにとどめたい。中国のグローバルテックカンパニーは近い将来、国内でのユーザ数拡大を望めなくなり、国外市場開拓に取り組むことになる。中国のグローバルテックカンパニーの収益に占める海外の割合が増えるにつれて、中国政府の声の重要性は失われていくだろう。

第３節　ロシア

サイバー空間の登場前後で、最も国際的な影響力が減少したのがロシアである。現在のロシアは米国と並び称される超大国ではない。それは 2016 年での、プーチン大統領

自身の「米国は、偉大な国だ。恐らく今日、唯一の超大国だろう。我々は、それを理解している」（President of Russia 2016）という発言からも明らかである。米国とソ連（ロシア）という二極構造の終焉にはサイバー空間や情報通信技術の進歩と普及が大きく影響している。

第 1 項 パワーを失うロシア

国際政治学におけるパワーの概念は依然として万人に受け入れられる明確な定義がない。それでもパワーの重要な要素として、国土の広さがあることは広く認識されている。「最も広大な領土を保有する国家こそが最大の人口と最も豊富な資源や生産物に恵まれ、最大の富と力をもち、自己充足度も高かったから」（神谷 2009: 30）である。国際政治の歴史の長い期間にわたって、大きい国が強い国である時代が続いていた。冷戦の終結は軍事力を背景にした影響力の行使を一層困難にし、ナイがソフト・パワーやスマート・パワーの概念を提唱したことからも分かるとおり、パワーの概念における国土・軍事力・経済力の重要性は相対化されてきた。陸海空の伝統的な安全保障の領域において、そして宇宙空間において圧倒的であったロシアの影響力はサイバー空間に見られない。サイバー空間という情報通信ネットワークの支配という文脈において、国土の広さはアドバンテージにならない。ズビグニュー・ブレジンスキー（Zbigniew Brzezinski）にならって、超大国を「軍事、経済、科学技術、文化において突出した力を持つ国」と定義すれば、ロシアはサイバー空間を支配する科学技術、デジタル経済の掌握の両面において顕著な成功を収めていない、大国もしくは中規模国とも捉えられる。

データと海底ケーブルの状況からロシアの実態にもう少し迫ってみたい。図表 3-1 は簡易なサイバーインフラの地政図である。円はそれぞれが特定の国を表している。円の大きさは各国に保管されるデータの量を表す。そして円を結ぶ先の太さは接続する海

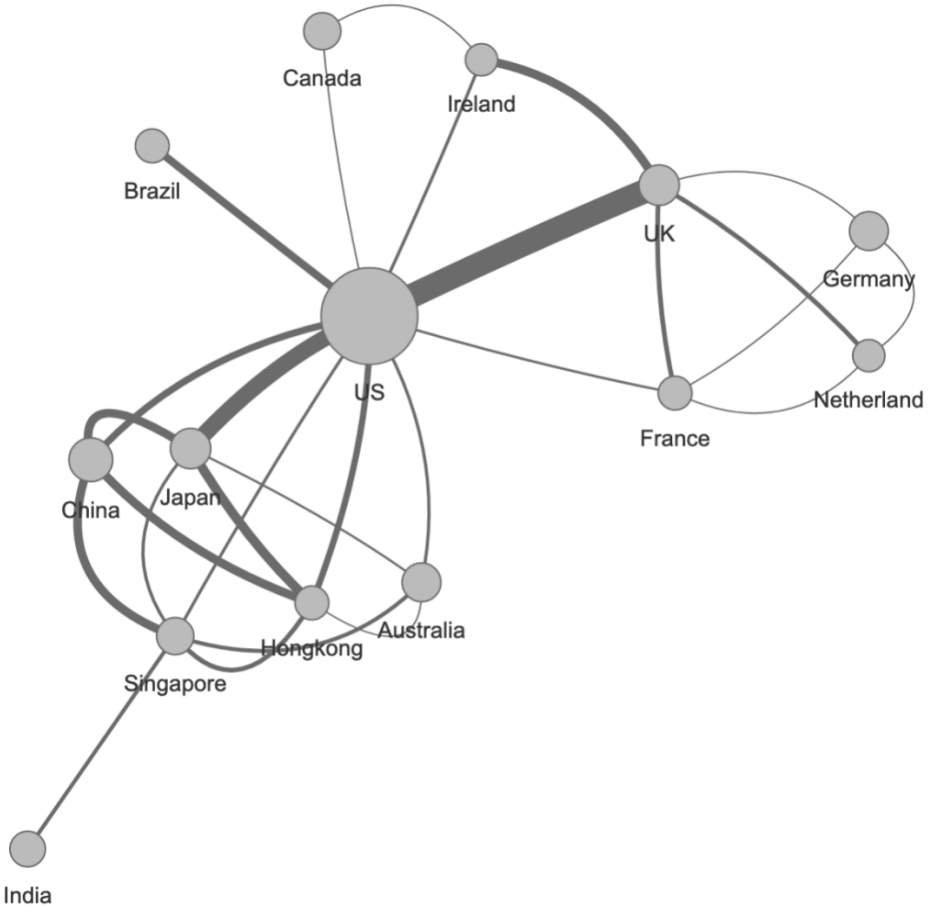
底ケーブルの物理的な本数[64]である。ここから明らかになるのは、まず、世界の上位 14 カ国でおよそ世界のデータ総量の 90%を保持するという事実である。次に、気づくのは米国内に保存されるデータの多さである。世界のデータのおよそ 40%が米国内に保存されているとみられる。全体の数値の大部分は、全体を構成するうちの一部の要素が生み出しているというパレートの法則（80:20 の法則とも）はデータの流通においてもみられる。一部の国へのデータの独占・寡占は進み、特に米国への集中が顕著である。

ケーブルの数に目を転じると、インターネットのネットワークトポロジー同様、サイバーインフラについても、米国を中心としたスター型ネットワークとなっていることが確認できる。サイバー空間における力が「より多くのデータにアクセスする力」だという本論文の前提に基づけば、図の中で円が大きく、多くの国とつながっている国が強い力を持つ。米国の優位はここでも明らかである。

サイバーインフラは伝統的地政学に描かれた構図と矛盾する点があるということも言えそうである。つまりシンガポール、オランダ、アイルランドはサイバーインフラについて上位 14 カ国に含まれる。サイバー分野以外の力に対して、サイバー空間で力がある国である。対して、伝統的安全保障分野での大国にもかかわらず、サイバー空間における力が極めて弱いのがロシアと言える。ロシアは保有するデータ量、他国との接続において極めて不利な立場にある。ロシアがサイバー大国となるためには、より多くのデータを集め、より多くの国と接続を持つ必要がある。前者は中国における動画サービスや E コマースのように、世界中で利用されるようなサービスの開発などが有効だ。後者は地理的な制約が大きいが、それでもロシア領土の北岸や東岸から諸外国へと接続される海底ケーブルが実現されれば、構図に変化をもたらすであろう。いずれも一朝一夕に実現するようなものではない。

---

[64] 海底ケーブルマップ（https://www.submarinecablemap.com/）から本数を目視確認するという手法をとっている。描画には vis.js とよばれる描画ライブラリを用いた。ソースコードは付録第 2 節に収録した。



図表 3-1 データのストックとフローにみる国際関係

サイバーインフラの地政図に基づく分析では、改めてロシアの厳しい立場を確認できた。ロシアは国際政治の舞台における超大国の役回りを終え、生き残りのための戦略を模索している。

第２項 鎖国へと向かうロシア

ユーラシア大陸を横切る鉄道網において、中国と東ヨーロッパが標準軌とよばれるレールの間隔を用いているのに対して、ロシア（旧ソ連諸国）ではそれよりも広い広軌が採用されている。規格が違うためにロシア国内を列車でそのまま通り抜けることはでき

ない。ロシア国境周辺で、貨物の積み換えなどの作業を強いられる。鉄道輸送の効率性を追求するのであれば、当然標準軌を採用すべきであったロシアが広軌を採用したのは、外部からロシアへの侵略を困難にするためであったと言われている（Buchanan 2017: 1991; Jervis 1978: 195）。現代のロシアのサイバー空間における戦略は、この鉄道網敷設の際の戦略を彷彿とさせるものである。

ロシアは欧米以上に自国へのサイバー攻撃を深刻なリスクとして捉えている。ロシア当局の報告によれば「国家機関のサイトに対するサイバーアタックの回数は増大傾向にあり、2015 年は 1,440 万回、2016 年には 5,250 万回前後に上り、1 年間に 3 倍になったことになる。ここ数年のハッカー攻撃による世界の損失は（中略）世界の GDP の 0.4 から 1.5（％）に相当するだけでなく，増大する傾向にある」（藤巻 2018: 10）という。GDP の 1.5%という数字はその内容を精査する必要があるが、ロシア政府にとってサイバー空間のリスクは決して軽んじられるものではないということが、この推計から言える。

EU 圏内のデータの域外移転に制限をかけた GDPR よりも早く、ロシアは 2014 年からデータのロシア国内での保存・保管をよびかけている（Henni 2014; Maynes 2014）。さらに 2019 年 4 月には海外の DNS ルートサーバをバックアップし、海外とのインターネットが遮断された際にもロシア国内のインターネット（Runet）が機能し続けることを狙ったネット主権法がロシア上院の委員会で承認され（TASS 2019）、その後 5 月にはプーチン大統領が署名して法律が成立した（Hodge & Ilyushina 2019）。

ロシアの政策に詳しい国際政治学者ジュリアン・ノセッティ（Julien Nocetti）は、近年のロシアの戦略を次のように紐解く。ロシアは国家主権と内政不干渉がサイバー空間にも生きると信じている。サイバー空間を構成する機器が置かれている地理的位置に基づいて、仮想の国境線がひくことができるというものである。サイバー空間にグローバルさと民主主義と国家主権の 3 つを求めて苦しむ情報拡散国家、グローバルさと国家主

権を効率的に追求し影響力を増す中国に対して、ロシアはグローバリゼーションを求めていない。そこにロシアの論理の強靭さと現実の経済活動における脆弱さの両面が現れている。

ここで注意が必要なのは、ロシアは情報拡散国家とそれらの国から生まれたテックカンパニーを同一視していないという事実である。ロシアは長年にわたり、インターネットを米国が支配していると非難してきた。例えば、2014 年 4 月にはプーチン大統領自ら、インターネットを「CIA のプロジェクト[65]」と形容し、米国への不信感を明らかにした。一方で、ロシアは米国を批判しても、民間企業や市民社会の発言力が強いインターネットガバナンスを正面から批判することを避けてきた[66]。前掲のノセッティの言葉を借りれば、それが「マルクス主義の色濃い発言が多いインドとの大きな違いである」（Nocetti 2015: 121）。また、メドベージェフ大統領（Dmirtry Medvedev: 肩書は当時のもの）はアップル社やツイッター社を訪問した様子を大々的に宣伝し、むしろテックカンパニーとの協力関係を深めようと努力してきたと見ることもできる（佐藤 2010）。

筆者は 2009 年にベトナムでアジア太平洋経済協力会議（APEC）が主催するサイバーセキュリティに関する国際会議に出席した。あるセッションでロシアの政府職員が、現在のサイバー空間における米国の特権的な地位を批判し、国際社会が共同で統治していく仕組みの必要性を熱弁していた。ひとしきりの米国批判を終えたあと、「質問などあればメールで連絡ください」と彼の資料の最後のページに連絡先が書かれていた。それは米国のマイクロソフト社が管理するホットメール（Hotmail）という無料メールサー

---

[65] 「CIA のプロジェクト」という発言は、インターネットが米国によるグローバルなスパイ活動のために運営されているという意味と考えられる。

[66] ただし、メドベージェフ政権において副首相を務めたドミトリー・ロゴージンが 2013 年に「Twitter や Facebook は米国の政治キャンペーンの一部」と非難したり、2019 年 9 月に実施されたロシアの統一地方選挙のタイミングにおいて、ロシア側が主にグーグル社とフェイスブック社に対して情報操作を非難したりするなどの、本論の主張に沿わない事象も確認されている。

ビスのアドレスであった。米国を批判する政府の活動自体が米国のインフラやサービスに支えられている、現在のロシアの苦しい姿を象徴している。

第４節　北朝鮮

2017 年 5 月にワナクライというコンピュータウイルスの被害が世界中に広がった。ワナクライは感染後にコンピュータ上のファイルを暗号化し、使用不能にした上で、ファイルを復号するための身代金としてビットコインの送金を求めた。斬新な手法であり注目をあつめた。2018 年 6 月に米政府がこの件および関連するサイバー攻撃への関与を理由に、北朝鮮系企業と従業員の北朝鮮人を訴追した[67]。北朝鮮発のサイバー攻撃に対して厳しい目が向けられている。

北朝鮮に限らずサイバー攻撃能力能力に関しては、それを秘匿するために様々な努力が行われており、明らかにすることは難しい。本節では、それを理解するための第一歩として、背景となる北朝鮮の情報通信技術全般について 1980 年代からの発展の経緯を振り返る。情報通信技術の発展は必ずしもサイバー攻撃能力に直結するわけではない。しかし、国内に情報通信技術が皆無であれば、サイバー攻撃能力が生まれる余地はない。情報通信技術をサイバー攻撃能力が生まれる「土壌」としてとらえることができるはずである。

本節は、北朝鮮地域研究の文脈で、これまであまり論じられてこなかった情報通信技

[67] 2018 年 6 月 8 日に承認され、同年 9 月 7 日に公表された起訴状によれば、ワナクライ、バングラデシュ中央銀行の外貨口座からの不正送金、ソニー・ピクチャーズエンタテインメント社へのハッキングおよびその他は朝鮮エクスポジョイントベンチャー社の中国大連にある拠点から準備されたという。

術の発展に向き合うものである[68]。結論を先取りすれば、特に 2 代目指導者金正日は、必ずしも核ミサイル技術開発のためだけに情報通信技術政策を進めたわけではなかった。半導体からソフトウェアまでフルセットでまかなえる国家を目指した。社会システムを維持したまま、経済発展を成し遂げた中国を手本とした。そして、その試みはいびつな成功をおさめた。試験的な生産で技術を蓄積し、国内に通信インフラを張り巡らせ、大量の優秀な人材を確保した。一方で、経済に貢献する産業の創造に失敗した。その結果、もたらされたのは技術者の余剰である。技術者の余剰はサイバーセキュリティ・ガバナンスの障害となりうる。

まず第 1 項では情報通信技術大国となろうとした 1980 年代からの北朝鮮の歩みを紹介する。そしてハードウェア製造大国からソフトウェア開発大国へと政策目標が密かに修正されていたことを指摘する。またネットワークの分野では、大きく対象を光ファイバーケーブルネットワーク構築とインターネットと携帯電話の 3 つにわけ、国際政治に振り回された発展の経緯を描く。

第２項では、北朝鮮のこれからを考察する。まず金正日が果たした大きな役割を明らかにする。その上で、現指導者金正恩時代の戦略について①言論統制の緩和、②海外拡散、③中国との関係強化の 3 点に絞って、論じていく。

第 1 項 北朝鮮の情報通信

北朝鮮の情報通信技術への取り組み

北朝鮮は情報通信技術を活用して、経済的あるいは軍事的な大国の地位を目指した。1970 年代からの北朝鮮の情報通信技術政策は、その土台となるコンピュータとネットワークを自国にもたらすことを、目的として始まった。

---

[68] 情報通信技術とほぼ同時期に進められた CNC 化（工業製品の生産をコンピュータ制御する技術）についてはすでに優れた考察がある。ここではこれまであまり語られてこなかった情報通信技術のみを研究の対象を限定した。

北朝鮮の情報通信技術への取り組みは、1984 年の金日成の旧ソ連および東欧諸国歴訪の前後から見られる。金日成は東欧における情報技術の発展を目の当たりにした。その翌年から留学生を旧ソ連および東欧に送り出し、技術の習得にあたらせた。

1987 年には第 3 次 7 カ年人民経済発展計画が策定され、「産業の電算化」が政策の柱となった。ここでいう電算化とは工場や農場において、情報通信技術を用いて生活インフラを合理化することである。

第 3 次 7 カ年人民経済発展計画を実現するための作業プランとして、翌 1988 年に第 1 次科学技術発展 3 カ年計画が策定された。この計画には大規模集積化（LSI）回路や高度な半導体生産の工業化、経済主要部門のコンピュータ化が目標として掲げられた。

1991 年には第 2 次科学技術発展計画が実施された。第 2 次計画においては LSI 生産の工業化、あらゆる分野のオートメーション化が引き続き盛り込まれるとともに、超小型コンピュータの生産と開発が掲げられた。

このように朝鮮労働党が承認する文書で情報通信技術が言及されるのは 1980 年代後半になってからである。しかし、それ以前から、下地となる取り組みは始まっていた。以下では、半導体製造、ソフトウェア開発、情報通信ネットワークの構築という 3 つの分野に分け、歩みを追っていく。

半導体立国への夢

日本において半導体は「産業の米」と呼ばれ、経済成長を支えた重要な産業である。韓国、中国そして台湾も同様に半導体生産を国策として進めた。北朝鮮もある時期、半導体立国を夢見た。

1979 年に国連開発計画（UNDP）が平壌での活動を開始し、北朝鮮は他の開発途上国と同様に国連の支援を受けることが可能となった。このとき、北朝鮮は集積回路（IC）工場の設置を要請した。IC 工場と関連処理施設を建設し、半導体技術者を育成するという大掛かりなプロジェクトであった。対共産圏輸出統制委員会（COCOM）違反の可能性

などを勘案した西側諸国が入札を躊躇したこともあり、インド政府と関係が強い企業が落札した。1986 年の冬に、インドの企業が建設した工場が引き渡される。

先行研究には、この工場において実際に小規模の IC 生産に成功した事実が残されている。しかし、半導体生産は生産にはこぎつけたものの、経済的な利益を生み出さずに終わった。UNDP のプロジェクト報告書には英語が苦手な北朝鮮技術者がインド人技術者とコミュニケーションに課題を抱えていたこと、そして電力供給が不安定という状況下で安定した生産が難しかった点が挙げられているという[69]。

理由はそれだけではないだろう。半導体生産には安定した電力供給と共に、洗浄などの工程で必要な水の供給が欠かせない。北朝鮮には「旅人に一椀の飯は提供できても、一杯の水は提供できない」ということわざがある（真勢 1989: 82）。これが示すのは水の確保に苦労してきた共通経験である。

加えて、半導体ビジネスは一国内で完結することはない。設備および原材料を海外調達する必要があり、生産した半導体を一括大量消費する市場が不可欠だ。北朝鮮の半導体生産は技術としては成功したのかもしれないが、ビジネスとしては失敗であった。

地理的・環境的な制約から半導体ビジネスが難しい、という事実がいつ認識されたのかは定かでない。2001 年 1 月に金正日は中国上海の浦東地区を視察した。その際に現地で半導体製造を行う日本の電子機器メーカーを訪問した。その時点では自国での半導体ビジネスを諦めていなかったのだろう。その 5 年後の 2006 年 4 月に最高人民会議第 11 期 4 次会議で「科学技術大国」という長期的ビジョンが掲げられる。「国全体をカバーする情報ネットワークとプログラミング技術の強化をすすめ、もって北朝鮮をソフトウェア開発大国にする」というソフトウェア開発に注力する方針が示された。この文書

---

[69] UNDP によるプロジェクト完了報告書は機密指定されており、閲覧ができない。少量の IC 生産に成功したなどの記述は、機密指定以前に報告書を取得した Mansourov の研究などから得た（Mansourov 2005）。Mansourov はロシア人ながら、平壌市内の大学を卒業し、現在米国のシンクタンクで北朝鮮研究を行うという、珍しい経歴の持ち主である。

は、前述の科学技術発展 3 カ年計画と違い、半導体製造への強い期待は読み取れない。2001 年から 2006 年までのどこかで半導体製造ビジネスを諦めるという方針変更が静かに行われたと見られる。

ソフトウェア開発大国への道

半導体製造により外貨を稼ぐという計画はソフトウェア開発大国を目指すという計画に、静かに置き換えられていたことを前節の最後で触れた。次なる目標はソフトウェア開発産業での成功であった。

この分野で成功した国としてインドの名前が挙がることが多い。特に有名なのはインドにおけるオフショアソフトウェア開発だ。インドは英語が公用語の 1 つであり、優秀な情報通信技術者の労働力を安く確保できることで有名となった。米企業のオフショア開発受注をきっかけに、インドは一大ソフトウェア開発地になった。インドのソフトウェア産業の GDP 貢献率は 2014 年時点で 8%を超え、国の基幹となる産業である（中田 2014）。

情報技術産業の中でソフトウェア開発は敷居が低い。ハードウェア製造と違い、工場などの大規模設備、原材料の輸入、在庫管理などの必要がない。誤解を恐れずに単純化すれば、少数の優秀なプログラマーが確保できればビジネスを始められる。北朝鮮はインドの成功をモデルに、日本・中国・韓国などの近隣諸国から受託をうける「ニアショアソフトウェア開発拠点」となることを目指した。それを支えたのは朝鮮総連や日本にいる北朝鮮とのつながりを持つ人々であった。

国産ソフトウェア開発と受託開発

1986 年 7 月に平壌プログラムセンター（PIC。別名は平壌情報センター）が設立された（Mansourov 2005; ウラジミール 2003）。同時期に情報技術局という行政機関も設けられ、北朝鮮のソフトウェア技術への取り組みが始まる。

PIC は朝鮮語ワープロソフト、朝鮮語入力支援ソフトなどの Windows 上で動くソフ

トウェアを開発した。設立初期の PIC のパンフレットには「北朝鮮国内でもっともコンピュータを保有する組織」との記述がある。日本を始めとする近隣諸国からパソコンやソフトウェアを調達し、平壌に送るサプライヤーであり、徐々にソフトウェア開発にも携わるようになっていった可能性がある。

創業 2 年目の 1988 年に PIC のトップが来日し、日本の営業所開設の視察を行い、徐々に日本市場を相手にしたソフトウェア開発ビジネスを拡大する。1993 年には出版関連、ホテル予約管理、港湾でのコンテナ管理、保険管理などのソフトウェア受託開発を行い、1993 年単年で 20 万米ドルを売り上げたという。当時 PIC にソフトウェア開発を委託した企業には日本の自動車会社の名も挙がっている。

UNDP は PIC に対して「北朝鮮国内産業マネジメントのための IT 活用、産業自動化」を目的に総額 69 万米ドルの支援を行っていた。先行研究はこの時期に北朝鮮の国内産業にその成果がもたらされた形跡はないことを指摘し、PIC は開発受託を得て外貨を獲得することに専念していたと指摘する（Mansourov 2005: 80）。

PIC に遅れること 2 年、1988 年に、前述の第 1 次科学技術発展 3 カ年計画に呼応する形で、朝鮮コンピュータセンター（KCC）が設立された。KCC の設置は 1990 年に金正日自らが命令した。1996 年に内閣の省級機関に公式に昇格され、現在に至るまで KCC は一貫して労働党指導部が公認する情報技術分野の重要なプレーヤーとして活動している。

KCC は「Red Star OS」とよばれる独自の Linux ベースのオペレーティングシステムを開発したことで有名である。また囲碁ソフトウェア、将棋ソフトウェアの開発を行っていた。1998 年に日本で開催された世界的な囲碁プログラム競技大会で優勝するなど、世界トップクラスの技術を擁していた。

2000 年 6 月に韓国大統領の金大中と金正日の南北首脳会談が行われ、韓国からの膨大な経済援助が約束されたのを機に、南北の間に融和ムードが広がった。この頃の北朝

鮮には韓国から様々な形態の支援が行われた。2000 年 3 月、KCC が韓国のサムスン電子と合弁で「朝鮮コンピュータ・三星ソフトウェア共同協力開発センター」を中国北京に設立したのもその一環であろう（サンウ 2001）。共同開発センターでは携帯電話用のソフトウェア開発などを行っていたとされている。

セキュリティソフト

北朝鮮企業が開発したソフトウェアの中には、暗号化ソフト、ウイルス検知ソフトなどのサイバーセキュリティ分野の製品も含まれる。この分野のソフトウェア開発に必要な知識は、自らがサイバー攻撃を実施する場合に必要となる知識と共通部分が多く、北朝鮮のサイバー攻撃能力能力を理解する上で重要である。

北朝鮮との関係が深いオランダ人ビジネスマンが書き残すところによれば、遅くとも 2006 年には光明 IT センターという KCC の関連組織が創設されたという（Tija 2006）。光明 IT センターはネットワークとセキュリティに特化し、ウイルス検知ソフト、データ暗号化、データ復旧、指紋認証ソフトウェアの開発を行っていた。また STS（STS Tech-Service）社という会社も類似の分野のソフトウェア開発に携わっていた。光明 IT センターと STS の両社が関与したとされる、「北朝鮮国産」と謳われるウイルス検知ソフトを解析した専門家によれば、大手ウイルス検知ソフトに無断改造をほどこしたものであり、国産技術とは言い難いものであったという（Lechtik & Kajiloti 2018）。

北朝鮮におけるソフトウェア開発[70]の道のりから明らかなのは、純粋にアルゴリズムの巧拙を競う分野における、北朝鮮技術者のプログラミング能力の高さである。2000 年代の半ば、北朝鮮の将棋ソフトと囲碁ソフトは世界最高峰の水準にあったことがそれを証明している。一方で、ソフトウェアもまた海外市場での成功には至らなかった。

---

[70] 2003 年 6 月、最高人民会議常任委員会の政令で「コンピュータソフトウェア保護法」が制定され、2004 年 6 月に「ソフトウェア産業法」が制定されたという記録が残っている。本章執筆時点でその内容について記した資料がなく、今後朝鮮語を解する研究者によって明らかにされることを期待する。

翻弄されたネットワーク化計画

近年平壌を訪れた外国人の報告を読むと、携帯電話の普及に関しての驚きの声が多く見られる。携帯電話が使えず、インターネットへの接続ができないというイメージは根強いのであろう。本節では携帯電話が平壌だけでなく多くの地方都市まで普及している現在の状況がいかにもたらされたのか、そしてインターネット接続可能な国内ネットワークを持ちながらも鎖国状態を続ける北朝鮮の実態を明らかにしていく。

都市を結ぶ光ファイバーケーブルと電話

前述の第 1 次科学技術発展 3 カ年計画（1998 年）は情報技術に関して、国をあげた取り組みのスタートとなった文書である。その中には「KCC を中心としたコンピュータ・ネットワーク構築」という通信ネットワークの構築も目標として掲げられていた。

1990 年 8 月、UNDP の支援をうけ、平壌と主要 3 都市を結ぶ光ファイバーケーブルの敷設が完了した。北朝鮮は UNDP に対して光ファイバーケーブルの敷設だけでなく、その製造を自国で行える環境を要請した。要請は認められ、2 年後に平壌ファイバーオプティックケーブル工場が完成し、ケーブルの国産体制が整う。その後、北朝鮮の光ファイバーケーブル網はそのエリアを広げていく。1995 年 9 月に咸興市が、1998 年 2 月に新義州市が、2000 年 3 月に北平壌地方の主要都市が、2001 年に南浦が、それぞれ平壌と光ファイバーケーブルで結ばれた。2000 年代の早い時期に、50 以上の主要な市と郡に光ファイバーケーブルが通ったと専門家は見る。

全国を張り巡らす光ファイバーケーブル敷設が行われている最中の 1993 年 8 月、金正日は国家情報通信会議に対し「テレコミュニケーションの近代化に全速力で取り組め」という書簡を送る。1994 年から 1998 年にかけては、飢饉水害により多くの人命がうばわれた「苦難の行軍」と呼ばれる時期でもある。「他の公共事業がすべて一時中断を余儀なくされるなかで光ファイバー網の建設はつづけられた」と後に北朝鮮の官僚が振り返っており、この事業の優先度の高さがうかがえる。

この光ファイバーケーブルが企業や家庭へと固定電話回線としてさらにネットワークを広げていった。北朝鮮が国際電気通信連合（ITU）に報告したところによれば、電話加入回線総数は 1998 年の時点で 110 万回線を数えた（ウラジミール 2003）。

国内の電話網構築に付随して、国際電話の導入についても簡単にふれておきたい。1993 年 3 月の核拡散防止条約からの脱退宣言、5 月のノドンミサイル発射などをへて、北朝鮮と国際社会の関係は厳しさを増していた。ところが翌 1994 年 6 月にジミー・カーター（Jimmy Carter）元米大統領と金日成の会談が実施され、10 月に米朝枠組み合意が成立し、米朝間の緊張が急速に緩和する。1995 年 1 月に米国務省は自国の通信事業者に対して北朝鮮へのサービス提供を許可する。この許可が枠組み合意の範疇であったか定かではないが、政府のお墨付きを得た AT&T 社は 1995 年 4 月に商用長距離サービスの北朝鮮への提供を開始した。北朝鮮への国際電話が可能となった。

北朝鮮に国際電話がもたらされるプロセスからは、国を超えたネットワーク同士の接続は国際政治情勢に大きく左右されことがあらためて浮かび上がる。

インターネット

北朝鮮のインターネットは鎖国状態であることで有名である。しかし、国内に閉じたネットワーク「光明」があり、研究機関や政府機関が広報したい情報が掲載されている。1994 年には金策工業総合大学がオーストラリアとのネットワーク接続に成功している。1996 年には朝鮮中央通信のウェブサイトが立ち上がる。1995 年には北朝鮮と海外を結ぶ光ケーブルが北朝鮮とタイの合弁会社によって、羅先経済貿易特区と中国琿春市を結んだ。技術面に関して言えば、1990 年代なかばにいわゆる「インターネット」の技術はすでに北朝鮮国内で確立されたと見られる。以来、現在に至るまで、北朝鮮技術者は自国内のネットワークを、海外と接続する指導者からの命令を待っている。

この鎖国状態は国内統治の観点から必要であったものであろうが、2000 年代に入り情報通信技術の完全遮断は難しくなっていく。瀋陽にある北朝鮮資本のホテルあるいは

その周辺には北朝鮮がコントロールするネットワーク・サーバが設置され、日本の鎖国時代の出島に似た役割を果たしたと見られる。電子メールサービスなどがこの拠点で運営された[71]。

携帯電話ネットワーク

北朝鮮では闇市場での取引や外国のテレビやラジオの視聴はもともと厳しく統制されていた。その統制が 1990 年代半ばの飢饉を契機に緩んだ。忠誠心の低下から市民が相互に密告をすることも減った。2000 年以降、静かな開放（Kretchun & Kim 2012）とよばれる、市民同士が相互に繋がり、海外との障壁が低くなる状況が続いている。その主役は市民が持つ携帯電話である。

2001 年 1 月、金正日は中国上海の浦東地区の視察から帰国する。そして科学教育部に対して、「IT 革命と平壌エリアでの携帯電話ネットワーク構築を翌 2002 年 4 月の金日成 90 年期までに」と指示する。翌 2002 年にタイの企業との合弁会社が携帯電話サービスを提供開始する。これは第 2 世代携帯システム（2G）とよばれる信号をデジタル方式で伝えるネットワークである。デジタル方式には GSM が選択された。理由の 1 つは韓国で使われている CDMA との互換性をあえて持たせたくなかったからだといわれている[72]。もう 1 つは米国の対敵通商法（U.S. Trading with the Enemy Act）とワッセナー協約の結果、CDMA ネットワークの北朝鮮への輸出が禁じられていたことが挙げられる（Mansourov 2011: 18）。2002 年に開始した携帯電話サービスは市民に幅広く使われたわけではないが、2004 年 5 月にサービスが停止される。2004 年 4 月に起きた列車爆

---

71 「インターネット接続は中国にあるインターネット接続事業者に国際電話でダイヤルアップ接続を行うものであり、極めて高額だった。したがって衛星携帯電話を購入することが流行した」（2000 年代はじめに平壌に駐在した、ある ASEAN 加盟国の外交官に対する筆者インタビューより。2018 年 8 月に実施）。

72 2002 年 6 月には南北の政府関係者と通信事業者が集まり会議が行われた。1 つの議題は北朝鮮における携帯電話通信の通信方式であった。同時期に北朝鮮との交渉にあたった韓国人技術者によれば南北での通信方式統一というシナリオが検討された（Park 2015）。

破事件で携帯電話が起爆装置で使われたことが契機と見られている[73]。

その後、2008 年にエジプトのオラスコム社[74]と朝鮮通信会社とが 75%対 25%の比率で出資し、高麗リンク社という政府が正式に認める 3G 携帯電話ネットワークを設置した。中国における 3G 携帯サービスの提供とほぼ同時期であり、中朝間での技術協力があったことが示唆されている。オラスコム社が 2012 年に公開したデータによれば契約数は 100 万超、北朝鮮の全人口のおよそ 5%である。

そして遅くとも 2015 年にはスターネットワーク社という新たな携帯電話会社がサービス提供を始めている。現在の北朝鮮国内では同社とオラスコムが競合している。脱北者への聞き取り調査[75]では、7 割程度が亡命前に携帯電話を所有している。携帯電話は急速に生活に浸透していった。特に若い世代の間では携帯電話を持つことが一種のステータスであるという。携帯電話からの国際電話やインターネットアクセスは不可能であり、市民はもっぱらショートメッセージサービス（SMS）を使って家族や友人や同僚とやり取りをしている。

2015 年に行われた脱北者、北朝鮮への旅行者に対するアンケート調査によれば、体制による通信への検閲は金正恩政権に入ってますます厳しさを増してきている。国内に流通する「違法コンテンツ」に対応するために、2013 年後半に北朝鮮は国内の正規携

---

[73] 列車爆破事件で起爆に携帯電話が用いられたことは複数の研究で指摘されている（Mansourov 2011; 山口 2013; 石丸 & リ 2012）。一方で、北朝鮮から亡命した外交官の手記では、「龍川駅爆発事件は、本当に金正日が考えていたような暗殺事件だったのか。それともつねに暗殺の恐怖に怯えていた金正日をなだめるための、国家安全保衛部のこじつけだったのだろうか」とそもそも暗殺事件であったという前提から疑問視している（太 2019: 3772）。真相は依然として不明である。

[74] オラスコム社のトップは何回か訪朝しており、金正日および張成沢と並んで写る写真も残されている（Mansourov 2011: 18）を参照。

[75] Kretchun らは 2015 年に実施された 350 人の亡命者、難民、旅行者へのアンケート調査と 2016 年 5 月と 6 月に実施された 35 回のインタビューをもとにして北朝鮮における市民のインターネット利用の姿を記している（Kretchun, Lee, & Tuohy 2015）。

帯電話やタブレット端末のオペレーティングシステムを更新し、署名システム[76]を導入した。このシステムを導入した端末では、政府が認めたアプリケーションのみが稼働し、政府が認めたファイルのみ閲覧可能である。

インターネットの切断によるネットを経由したコンテンツの流入防止、署名システムによる不正コンテンツの利用制限、そして昔ながらの当局の監視の 3 つの取り組みにより、北朝鮮国内への情報流入は引き続き厳しくコントロールされている。

北朝鮮のネットワーク化の歩みを振り返ると、ネットワークの接続は強く国際政治に左右されるということを改めて感じる。米朝枠組み合意の後の突然の国際音声通話サービス開始がその代表的な例である。ネットワーク化は国内政治の着実な成果の積み重ねだけでは実現しない。

情報通信技術人材育成

新たな技術にはそれを推進する人材が必要である。金正日は 1999 年を「科学の年」と呼び、「強盛大国となるための 3 本柱が思想と銃（軍事力）、科学技術」とした。北朝鮮におけるイデオロギーの基盤となる主体思想と、独立の生命線である軍事力、その 2 つとならべられる程に科学技術が重要という指導者の言葉を市民に浸透させるため、教育が拡充される。

まず高等教育機関での情報通信技術教育が強化される。原則としてインターネットにアクセスできず、パソコンが手に入りにくく、そしてパソコンの所持にすら届け出が必要な北朝鮮国内においては、他の国のように自習でプログラミング技術を身につけることが不可能だからである（石丸 & リ 2012）。

1997 年に金策工業総合大学内にコンピュータ情報センターが設けられ、翌 1998 年には中学、高校の課程でコンピュータ教育が開始される。さらに 1999 年には金日成総

[76] 2017 年にドイツで開催されたサイバーセキュリティカンファレンスで、署名システムの詳細が発表されている。その映像が YouTube で視聴可能である（Grunow & Schiess 2017）。

合大学内に単科大学コンピュータ科学大学[77]が設立された。金日成総合大学は朝鮮労働党幹部への登竜門である。この権威ある総合大学に単科大学が設置されたのはこのときが初めてであり、コンピュータ教育への強い意志の現れとみることもできる。同年に金策工業総合大学・平壌電子計算機大学内にプログラミング学科が設立された。2001 年には万景台学生少年宮殿など平壌市の 4 つの施設にコンピュータ秀才養成班が設置され、より若い世代への英才教育が施された。

英才教育といえば、秀才大学の別名を持つとされる美林大学がある。1980 年台に旧ソ連との関係が好転した時期に、北朝鮮は電子戦の将校を養成する機関を設立する計画について、ソ連に支援を依頼した。1984 年ソ連国防部、フルンゼ軍事大学の支援の下、美林大学（1984 年当時は美林講習所、金一軍事大学、自動化大学と呼び方が変わったが、本節では美林大学で統一する）が開かれた（Kim 2014; ウラジミール 2003; 山口 2013: 212）。

美林大学は情報戦の指揮官を養成するための 5 年制大学である。2007 年に韓国に亡命したジャン・セユル（Jang Se-yul）によれば毎年 5000 名を超える応募者の中から 100 名が選抜され、様々なオペレーティングシステム、プログラミング言語について理解を深める。純粋な情報技術以外にサイバー戦争シミュレーションなどいくつかの専攻にわかれている。

情報通信技術者は高給が約束され、平壌の中心部に居住を許されるなどの特典もあった。加えて、北朝鮮では情報通信技術分野の入試では、出身成分とよばれる社会階級を不問とされた。「出身成分が良くない」若い秀才にとって、技術者への道は魅力的に映ったであろう。

これまで見てきた他の分野との比較において、人材育成は順調に進められたと見られ

[77] 単科大学とは、日本における学部に相当する。したがって金日成総合大学内にコンピュータサイエンス学部が設置されたと表現しても実態とそう乖離していないと考えられる。

る。当局は情報通信技術分野の技術者を必要とし、優秀な若者は新しい分野に果敢に挑戦したからである。急速な人材育成には弊害もある。次項で改めて論じたい。

第２項 金正日が残したものと金正恩に残された課題

金正日の残したもの

前項まで、北朝鮮における情報通信技術の萌芽の過程を振り返ってきた。本項ではその流れを、指導者金正日の関与という側面から改めて振り返る。そして、今後の北朝鮮の情報通信政策、あるいはサイバーセキュリティ政策ひいてはサイバー攻撃に関する決定を左右すると思われるいくつかの点について、推論を試みる

金正日自身の情報技術への関心を裏付ける逸話は多い[78]。指導者がコンピュータに強い関心を示していたことが、北朝鮮の情報通信関連の政策の主たる推進力であったと主張するつもりはない。ただ金正日自身が情報通信の分野において大きな意思決定者であったことは認めざるをえない。

前項で述べたとおり、IC 工場の設置、光ファイバーケーブルネットワークの建設などの長く将来を見据えた取り組みは、金日成の後継者として金正日が台頭していった時期に始まった。80 年代の北朝鮮は衣食住の供給すら十分とは言えない状態である。そのような状況下、金正日は来るべき情報化時代を見越していた。既に述べたとおり、光ファイバー敷設などの事業が、苦難の行軍（韓国統一省は 1995～1997 年の間に少なくとも毎年 7～8 万人が死亡と推定する）の最中も継続されことがその証左である。

別の例を示そう。金正日は、中国各地の情報技術産業を視察している。合計して 4 回行われた視察の対象は半導体製造業、電話交換機製造業、ソフトウェア研究所、光ファイバーケーブル企業、軍事衛星通信を含む通信機器製造業、テレビなどの家電製造、金

[78] 有名なものとしては、マデレーン・オルブライト（Madeleine Albright）国務長官が平壌で金正日と会談した際にメールアドレスを尋ねられたというものや、金正日の執務室に常にアップル社製のコンピュータが置かれていたという逸話がある。

融分野ソフトウェア開発、SIM カードを含むスマートカード製造などなど多岐にわたる。そして、例えば金正日が中国の家電製造業を訪れた後には、北朝鮮で中朝合弁のテレビ工場が建設されるなど、具体的な成果をともなっている[79]。金正日は死去する約半年前の 2011 年 5 月にも中国南東部の IT 企業や家電企業を訪問している。死の直前まで、北朝鮮の情報技術分野での発展に強い関心を持ち続けた。

北朝鮮市民の間では、「偉大なる首領」などと呼ばれる金日成との比較において金正日の評価が低い。様々な理由の 1 つに挙げられるのは、金正日が銅像やモニュメントなどの公共事業に熱心で、市民の生活の向上に直結する政策に無関心というものである。本章で示してきた、将来を見据えた情報通信技術分野への投資はその好例といえる。

2011 年 12 月の金正日の葬儀にあたり「金正日氏の革命遺産」として①核と衛星、②新世紀の産業革命、③民族の精神力、が示された。情報通信技術分野においては大量の優秀なソフトウェア技術者、全国を結ぶネットワークが金正日の遺産である。

金正恩に残された課題

2012 年 4 月、金日成生誕 100 周年祝賀閲兵式において金正恩は演説を行った。指導者の座について、初めての公の場でのスピーチである。そこで金正恩は「1 にも 2 にも 3 にも軍隊をあらゆる面から強化していかねばならない」と軍最重視の方針が変わらないことをアピールした（平岩 2013）。軍のサイバー防衛能力、サイバー攻撃能力能力を高めことが主要な課題であることは疑いようがない。ここでは情報通信技術分野での課題について、若干の未来予測を含めて論じてみたい。

言論統制の緩和

北朝鮮の体制維持のために、国内言論の統制の必要性は高い。しかし、一定の自由化

[79] 金正恩も 2018 年 3 月に極秘裏に北京を訪問し、習近平との会談の翌日、中国のシリコンバレーとも呼ばれる中関村に立ち寄った。見学先は中国科学院の成果発表の展示会である。金正日が「(自らが) 見たいものを見ようとした」のに対して、金正恩は「(中国が) 見せたいものを見た」と分析できる。

は経済に貢献し、国の発展に欠かせない。第 1 項で述べた、北朝鮮発の囲碁ソフトウェアの聚落がそれを雄弁に物語る。ライバルはネットワークを介してクラウド技術を活用し、膨大な機械学習を行うことで性能アップを図ったが、北朝鮮はその流れに取り残された（河 2017）。

開放への具体的な動きも見える。携帯電話サービスを外資企業に提供させたことはすでに述べた。さらに北朝鮮国内では中国、韓国などの資本を受け入れた経済開発区が 2016 年までに 26 カ所設置されたが、ここでは法律で「国際通信」が保障されている。経済発展にネットワーク化が欠かせないことを認め、部分的に許可を始めている。中国やベトナムなどの社会主義国は言論コントロール緩和と経済発展を両立させた。それらの国をお手本にした緩和が行われる可能性は高い。現在の論点は「いつ」「どのように」その許可が拡大するかという点である。

情報通信技術の海外拡散

度重なる核・ミサイル発射実験を受け、北朝鮮に対する国連や有志国による経済制裁は厳しさを増している。この影響は当然ながら情報通信技術分野にも及ぶ。2017 年 2 月、国連安保理北朝鮮制裁委員会専門家パネルはあるマレーシア企業群を北朝鮮偵察総局のフロント企業と結論づけた。2018 年 1 月、中朝合弁の IT 企業が中国政府によって会社登記を抹消された。専門家パネルの元委員は経済制裁の網羅性の低さを指摘するが（古川 2017a）、それらの活動の成果で、北朝鮮の情報通信技術産業の海外拠点は大っぴらな活動をするのが難しくなってきているという見方も可能である。

経済制裁の影響を回避するため、北朝鮮は個人の「出稼ぎ」を推奨している。欧州安全保障協力機構（OSCE）の報告によれば、推定 5 万人以上の北朝鮮労働者が欧州を中心に 16 か国で働いており、年間 12 億ドル～23 億ドル（約 1210 億円～2320 億円）を

北朝鮮に送金しているとされる（小野 2017）[80]。

先述のように 1990 年代後半から情報通信技術に関する教育をうけた人材の余剰プールが北朝鮮国内に存在する。それらの人材を海外に送り、現地で仕事をさせるという手段が経済制裁などにより、困難となっている。これは個人をしてサイバー犯罪による金銭詐取に駆り立て[81]、国家全体を経済目的のサイバー攻撃に向かわせる、無視できない要素である。

中国との関係強化と依存脱却

金正恩時代に入った後、とりわけ北朝鮮と中国のパイプ役であった金正恩の叔父でもある有力者張成沢が粛清されてから、中朝関係は冷え込んでいた。2017 年 12 月、中国の汪洋政治局常務委員は日本の国会議員との懇談で「中国にとって（北）朝鮮はかつて血で固めた友誼を結ぶ国だった。今はそうではなく、対立する関係になっている」と表現した。「度重なる核実験に中国は面子を完全につぶされた」（中澤 2018）という見方もあれば、「中国と北朝鮮の関係が悪化しているというよりは、北朝鮮が中国に依存しすぎた状態を是正しつつある」（武貞 2014）という見方もある。

その状況が 2018 年に入って一変する。金正恩の初北京訪問に始まり、すでに 3 回の中朝首脳会談が実施されている。サイバー分野での協力が始まる可能性がある。1 つの見どころは、2021 年に予定される中朝条約の更新である。中朝条約は 1961 年に締結され、20 年毎に自動的に更新され、現在までに 2 度更新されている。自動参戦条項（どちらかが攻撃されて戦争状態に陥った場合、他方は軍事援助を行う）が含まれており、中朝の同盟関係の土台である。2001 年の条約更新時にはサイバーセキュリティについ

[80] 送金額は情報通信技術分野の労働者に限らない。例えば、朝鮮日報は「世界 40 カ国に 5 万人の労働者を派遣、年間 3 億ドル近くを稼ぐ」としている（山口 2013）。数字に乖離が大きく、参考値として理解いただきたい。

[81] 活動を制限された技術者の一部は、Freelancer.com や Guru.com といったクラウドソーシングサービスを使って自らの身分を明かすことなく、技術をお金に変えているという。Berger et al.（2018: 2）を参照。

ての問題意識が高まっておらず、サイバー攻撃に関して自動参戦条項をどう解釈するかなどの議論はなかっただろう。この 10 数年の間に、複数の国や NATO などが集団安全保障の発動のトリガーにサイバー攻撃が含まれるという見解を示している。中朝条約更新のプロセスを通じて、中朝の軍当局の間で、サイバー攻撃とサイバー防御に関する中朝協力案が検討されるのではないだろうか。

矛盾するようだが、金正恩にとって、中朝関係の強化と並んで重要なのは、中国だけに依存する立場に自らを追い込まないことだ。2012 年 9 月にはイランと北朝鮮の間で科学技術に関する協定が結ばれた（Torbati 2012）。2017 年後半にはロシアを経由したインターネットとの接続を開始した。今後も北朝鮮は同様により多くの国との協力を拡大していくであろう。

金正日は 2013 年に「これまでの戦争が弾丸と石油によるものだとすれば、これからの戦争は情報によるものになる」と司令官たちに語ったとされる（Sanger 2018）。韓国インテリジェンス機関は金正恩がサイバー能力を「魔法の兵器（A Magic Weapon）」と捉えていると報告した（Sang-ho 2014）。指導者がサイバー攻撃とサイバー防御能力が重大な問題と捉えていることを示す発言や事実は他にもある。問題はそのサイバー課題の中で北朝鮮がどれに優先的にとりかかるかという点にある。そのいくつかの手がかりは、本章で提示したとおり、北朝鮮の情報通信技術の萌芽の過程から導かれる。

主にネットワークの閉鎖性から情報技術からは程遠いイメージがある北朝鮮だが、2 節で述べてきたように、国内での半導体製造、ソフトウェア開発、光ファイバーケーブル敷設などの事業に 1980 年台から着実に取り組んできたことがわかる。

そしてこれまで論じてきたとおり、北朝鮮の情報通信技術者は諸外国に拠点を拡大するインセンティブがある。国際的な経済制裁が効果を発揮するためには、日本や中国などの近隣諸国の一層の努力が必要である。

第５節　まとめ

3 つの国を情報支配国家の代表として論じてきた。この情報支配国家にカテゴライズした中国とロシアの間には極めて大きな違いがあることも明らかになった。中国は民主主義を捨て、ロシアはグローバリゼーションを捨てている。その違いを意識せずに既存の国際安全保障の視点から中国とロシアを「中露」と一括にし、不可分の印象を与えるのはミスリーディングである[82]。両者は、サイバー空間における国家主権の確保に共通の利益を見出しているが、その他の政策において、特に産業政策において立場が大きく異なる。北朝鮮については、民主主義とグローバリゼーションの両方を捨てている。それほど、国際的に孤立し、情報統制に重きをおく国であっても、携帯電話が使われ、インターネットが使われるという事実からは、サイバー空間の広がりを止めることは不可能であるといえる。

本章では、情報支配国家には「サイバー空間における情報の自由な流通よりも、治安の維持や政治の安定が優先される。ゆえに国家や政府によるサイバー空間の管理の必要性を正当化されやすい」という共通点があるとした。このような傾向は情報支配国家だけでなく、昨今の情報拡散国家においても見られる。情報支配国家と情報拡散国家の立場の違いはサイバー空間の成熟と共に薄れていっている可能性があり、本論文が十分に明らかにできなかった課題である。

本章の冒頭に「サイバー空間が古典的な国際政治でいうアナーキー状態であると仮定して、本論文の主張どおり、情報拡散国家の立場が悪くなっているとするならば、相対的に情報支配国家が力を得ているのか」という問いを示した。ここまで情報支配国家の

---

[82] サイバーセキュリティに限らず国家戦略全般について、廣瀬（2018: 2260）は「中露関係については、『蜜月は偽装されたものであり、その賞味期限はいつまでか』ということを常に考える必要がある」と警告する。

戦略と実態を検討した結果、中国以外の情報支配国家はサイバーパワーを得ていないと言える。第 2 章の情報拡散国家の実態と合わせると、情報拡散国家と情報支配国家は共にその影響力を弱めている。その力は誰の手に移ったのか。この答えに迫るため、次章ではサイバー空間におけるグローバルテックカンパニーの台頭を分析する。

第４章　グローバルテックカンパニー

第１節　はじめに

「政府だけでも、プライベートセクターだけでも国家の防衛をすることはできない。サイバーセキュリティは政府とプライベートセクターに課せられた共通のミッションである。両者はパートナーとして手に手を取り合っていくことになるだろう。」2015 年に米国の民間のサイバー防護を司る政府機関を訪問した、当時のバラク・オバマ（Barack Obama）米大統領はそう述べた（Richmond 2015）。オバマの言葉を待つまでもなく、サイバーセキュリティに関する官民連携の必要性が叫ばれて久しい。

インターネットを語る上で、それが概ね民間企業が所有・管理する空間であることは強調しておかないといけない。海底ケーブル、データセンターなどのインフラがあって初めて我々は「インターネットを使う」ことができる。サイバー空間の安全保障において、この民間企業の戦略は解明されていると言い難い。多くの研究は民間企業が所有・管理する事実に言及するものの、それらの企業が不特定多数の利益のために右から左にデータを受け渡す、対価に応じて平等にサービスを提供する存在としてとらえている。実際のところサイバー空間における民間企業の役割は決定的であり、その行動を支える指針は単に経済的な合理性と決めつけることはできない。

民間企業の中でも本論文がグローバルテックカンパニーと呼ぶ一群の企業が持つ力はとりわけ強い。世界中にユーザを抱え、データを保有し、近年では自社専用のデータセンターや海底ケーブルなどのインフラを持つ。政党のソーシャルメディア上での選挙運動、国家元首のソーシャルメディアを使った外交の生殺与奪権を握っているのもグローバルテックカンパニーである。グローバルテックカンパニーが望めば、それらの情報

をより多くの人に届けることも、その逆も容易い。

前章まで、情報拡散国家と情報支配国家の陣営がサイバー空間においていかなる戦略をとっているかを論じてきた。伝統的安全保障の視座からのサイバー空間の研究では、情報拡散国家を拠点とするテックカンパニーは情報拡散国家と協調し、情報支配国家を拠点とするテックカンパニーを情報支配国家と協調しているという見方が今も根強い。果たしてファーウェイ社は中国政府のエージェントなのであろうか。マイクロソフト社は米国政府のエージェントなのだろうか。本章はこの単純化した構造に挑戦するものである。

第２節　グローバルテックカンパニーと国家の間の緊張

第１項 グローバルテックカンパニーとは

はじめに、グローバルテックカンパニーという言葉が、何をさすのか明らかにしておきたい。本論文におけるグローバルテックカンパニーとは、世界の多数の国において経済活動を行い、かつ情報通信技術分野で競争力を持つ企業のことである。具体的にはGAFA と通称される、グーグル社、アップル社、フェイスブック社、アマゾン社や BATH と通称されるバイドゥ社、アリババ社、テンセント社、ファーウェイ社などを指す。他にもマイクロソフト社やインテル社などはグローバルテックカンパニーといえる。グローバルテックカンパニーの条件の１つは「世界の多数の国において経済活動を行う」ということであるが、これは具体的に収益の一定の割合を海外市場に頼っている状態を指す。国外収益が多い企業は、特定の政府との間に特別な関係をあえて築かず、自らの技術的優位をより多くの国の市場で示すことが理にかなった戦略となる。

国際政治のアクターとしての企業を含む非政府主体の役割は既存の研究でどのように論じられてきたのか、ここで簡単に振り返りたい。国際関係論を振り返れば、多国籍

企業が持つ大きな力という事象に新規性はない。エドワード・サイード（Edward Said）は一握りの多国籍企業に支配されるマスメディアを批判し（サイード 1998)、ジョン・ブレイトワイト（John Braithwaite）とピーター・ドラホス（Peter Drahos）はマイクロソフト社やモトローラー社などの政策コミュニティとの近接化を指摘した（Braithwaite & Drahos 2000: 491)。スーザン・ストレンジ（Susan Strange）が著書『国家の退場』で書いたような、巨大超国家企業のトップこそが現代の君主であり、国家はその役割を徐々に失っていくという姿はサイバー空間で現実になっているように見える（ストレンジ 2011)。それらを踏まえると、グローバル・ガバナンスのアクターの１つとして「多国籍企業」のステータスは揺るがないものになっているという論には説得力がある（Davis Cross 2013)。

ジョセフ・ナイはそもそもサイバー空間では政府が影響力を独占しておらず、政府は力の分散と呼ばれる現象に戸惑っているとした。その上でナイはサイバー空間のアクターを「政府」「組織や密な構造のネットワーク」「個人や緩い構造のネットワーク」に 3 分類した。政府以外の役割は早い時期から指摘されていたのである（Nye 2010: 2:10)。サイバー空間において多国籍企業が政府に代わって何らかの役割を果たすという点において既存の研究は大まかに一致していると言える。したがって本章におけるリサーチクエスチョンは、「グローバルテックカンパニーはサイバー空間のガバナンスにどのような力を持つか。その力は何に由来するか」とし、グローバルテックカンパニーの影響力を理解することを目指す。

第２項 本章における分析の枠組み

本章では分析の枠組みとしてパセティックドットセオリー（Lessig 1998: 661; レッシグ 2007: 170-177,475-483）を用いる。ハーバード大学のローレンス・レッシグ（Lawrence Lessig）は、レッシグはサイバー空間についての、「どんな政府もインター

ネットの富なしには生き残れないけれど、どんな政府もインターネット上で起こることをコントロールできない」という言説を批判し、人の行動への影響力を法（Law）、規範（Norm）、市場（Market）、アーキテクチャ（Architecture）の 4 つであるとした。例えば、飲酒運転の規制であれば、人々の価値観や道徳心に訴えかけるのが「規範」による規制、道路交通法による罰則が「法律」による規制、罰金を高額に上げるのが「市場」による規制とされる。「アーキテクチャ」とは自動車にアルコールの検知機能を設置し、そもそも飲酒している場合にはエンジンがかからないようにするというようなプラットフォームを予め設定しておくということ（神保 et al. 2011: 10）である[83]。

今日のインターネットを形作った技術者コミュニティの中には「私達は王様、大統領、投票を拒否します。大まかな合意と動作するコード（プログラム）を信じます」（Hoffman & Harris 2006）という信念が今でも共有されている。インターネットは正しく書かれたコードで機能するかもしれない。しかし、サイバー空間はそう簡単ではない。統治には法や規範や市場、そしてアーキテクチャの力が求められるはずである。

つまり、ここではサイバー空間における人々の行動について、グローバルテックカンパニーがどのような法と規範と市場とアーキテクチャを作り出し、それをコントロールしていくかを確認していくことで、「グローバルテックカンパニーはサイバー空間のガバナンスにどのような力を持つか」というリサーチクエスチョンの答えに近づくことができるはずである。

第 3 節　グローバルテックカンパニーと法、規範、市場、

[83] 法と規範は共に社会における望ましい行動を文書化したものである。両者は混同されがちである。2 つの違いはレッシグによれば、制裁のメカニズムと根拠である。「法は『これをするな、さもないと・・・』という罰則の脅しである。規範は期待されるふるまいの集合である」（ローレンス・レッシグ 2007: 437）。

アーキテクチャ

第 1 項 法

サイバー空間における法は、少なくとも立法、司法、執行の 3 つの観点でグローバルテックカンパニーの関与を必要としている。グローバルテックカンパニーの「国際的な法の支配に占める役割は主権国家と似通っている」（Cohen 2017: 51）という指摘があるが、似ているどころではなく、部分的に国家を超える大きな役割を果たしているというのが本節の主張である。

法の執行

法の執行から見ていこう。法の執行は国家安全保障の担保、外交、徴税などと並び政府の典型的役割とされてきた。しかし、以下に示すとおり、サイバー空間における法の執行において、国家よりもグローバルテックカンパニーが有効かつ広範囲に影響を及ぼすケースが見て取れる。具体例としてボットネット停止（テークダウン）とサイバー攻撃のアトリビューションの 2 例を示す

ボットネットテークダウン

ボットとはコンピュータウイルスの一種である。ボットは感染したコンピュータにおいて目に見える破壊活動を行わない。感染後はオーナー[84]からの指示を待ち、例えばスパムメールを送信するという指示が下ればそれに従う。同じ種類のボットに感染した一連のコンピュータをボットネットと呼ぶ。2016 年 10 月に Mirai と呼ばれるボットネットが一斉に DDOS 攻撃を行い、米国のネットワークサービスなどを混乱に陥れたが、これには世界中で数十万のボットが、コンピュータの所有者が知らぬ間に、参加させられていた。

---

[84] ボットに対して司令を出すもの。ハーダーなどとも呼ばれる。

ボットネットは大規模なものになると 100 万台の規模に膨れ上がる。これを止めるには、感染したコンピュータからひとつひとつボットプログラムを駆除するよりも、感染したボットとオーナーとの通信のメカニズムを解析し、オーナーが新たな指示を出せないように、オーナーが所有するIPアドレスやドメイン名を乗っ取るのが有効である。このような一網打尽に行う対策のことを、ボットネットテークダウン（Botnet Takedown）とよぶ。

ボットネットテークダウンを初めて大規模に行うことに成功したのは、どの国の法執行機関でもなく、マイクロソフト社である。2010 年に同社はウェールダック（Waledac）ボットネットという世界中にスパムを送信していたボットネットに目をつけ、同ボットネットを管理する正体不明の個人に対する民事訴訟を起こした。数カ月後に、米国の裁判所は同ボットネットのオーナーが所有する IP アドレスをマイクロソフト社に移転する命令を下した。まもなくして、管理者との通信が不能になりボットネットは崩壊した。

サイバー空間に起こる多くの衝突は、既存の法律が制定された時点では、想定もされてないような状況で発生する。ボットネット問題を例にとれば、「ボットネット取締法」などは存在しない。したがって、ボットネットの急所[85]を特定するという技術力と、その急所を既存のどの法律に基づいてどのような訴えを起こすかという点に、創造性が求められる[86]。その創造性を発揮するのが、法執行機関でなく、グローバルテックカンパニーであることがある。2013 年にマイクロソフト社と米国連邦捜査局（FBI）が共同作戦でシタデル（Citadel）と呼ばれるボットネットテークダウンを実施した。これは連邦捜査局にとって初めてのケースだが、マイクロソフト社にとっては 7 度目のケースであった。共同作戦を銘打っていても、経験豊富なマイクロソフト社からノウハウの移転があったと考えるのが自然である。ボットネットのテークダウンの例からは、「民間がテ

[85] ボットネットを例にとれば、オーナーが所有するIPアドレスやドメイン名は、後から変更ができない急所である。
[86] マイクロソフト社は商標権の侵害などを理由にIPアドレスの移転を求めた。

ークダウンオペレーションの遂行の大部分を担った」（Eichensehr 2017: 482）と言うことができる。

国家が関与するサイバー攻撃のアトリビューション

法の執行において、当然ながら罰を与える対象が特定されていなければならない。サイバー攻撃の実行者を特定する「アトリビューション」とよばれる作業において、国家はグローバルテックカンパニーの情報を必要としている[87]。

2013 年 2 月に米国のサイバーセキュリティ企業であるマンディアント社が APT1 と呼ばれる中国のハッカー集団と人民解放軍 61398 部隊との関係を主張する報告書をリリースし、大きな話題となった（Mandiant 2013）。それ以前から、高度なサイバー攻撃の背後に、軍やインテリジェンス機関の関与が噂されることは珍しくなかった。しかし、一企業が、具体的な根拠をもとに、人民解放軍の特定の部隊とサイバー攻撃とを結びつけたことは驚きをもって受け止められた。

そして、この報告書は米政府をして、中国によるサイバー技術を用いた経済スパイ活動への対策を強化する契機となった。当時のアッシュ・カーター（Ash Carter）国防長官は「国防省は政府内のパートナーシップそして、ファイヤーアイ社、クラウドストライク社、HP 社などのプライベートセクターの研究者の力をかりている」（U.S. DoD. 2015）と語り、グローバルテックカンパニーの力が攻撃元の特定に貢献していることを認めた[88]。

---

87 アトリビューションの作業の実態については、付録第一節「アトリビューションについて小論」を参照のこと。

88 グローバルテックカンパニーのアトリビューションの能力が、米政府を大いに助けているという本節の主張は、米政府内にアトリビューション能力が無かった、もしくは民間と比べて劣っていたということを意味しない。筆者のマンディアント社幹部へのインタビュー（2016 年）によれば同社が APT1 の報告書を公開するにあたっては、綿密に当局との調整を行ったという。また複数のインテリジェンス機関から、マンディアント社が報告書を公開したことについて「自分たちのカードを場に晒すことなく、中国にプレッシャーをかけることができてよかった」という趣旨の感謝の言葉を受け取ったという。

高度なサイバー攻撃について、攻撃者の素性を明らかにし、圧力をかけることは多くの国が抑止効果を期待して行っている[89]。2013 年のマンディアント社の報告書を皮切りに、多くのグローバルテックカンパニーが、サイバー攻撃と他国の政府の関係を告発してきた。

現在、この状況は変化しつつある。2016 年 12 月に米国政府がロシアのサイバー攻撃を非難する報告書を公開した。政府が攻撃者の素性を対外的に公表し、圧力をかける最初のケースとなった（DHS & FBI 2016）。以後、アトリビューションの作業を、政府が自ら行うことが主流になってきている。日本においてもワナクライというウイルスの感染について、政府が初めて公式に「わが国として事案の背後に北朝鮮の関与があったと承知」と北朝鮮を非難した（外務省 2017）。また 2018 年には APT10 とよばれる攻撃グループが中国を拠点としていると非難声明を出した（外務省 2018）。政府はアトリビューションを自ら行うだけの能力を身につけている[90]。しかし、この流れもボットネットテークダウンと同様に、グローバルテックカンパニーが敷いたレールを政府が走っているとみなすこともできる。

立法

次にサイバー空間における立法のプロセスにおける、グローバルテックカンパニーの役割を確認していく。サイバー空間における法の支配をめぐる状況は、現在のところ国連憲章を含む既存の国際法がサイバー空間にも適用されるという、大まかな合意がなさ

---

[89] その作業自体を、パブリックアトリビューションやネームアンドシェーム（Name and Shame）と呼ぶことが多い。

[90] ワナクライを北朝鮮のサイバー攻撃によるものと非難した米国ホワイトハウスのトム・ボサート（Tom Bossert）大統領補佐官は次のように述べている。「我々は、マイクロソフトなどが、先週、北朝鮮のハッカーの行動を妨害するために、（当局の指示を得ずに）、自らのイニシアティブで行動したことを高く評価する」（The White House 2017）。実際、マイクロソフト社の 2017 年 12 月 19 日の公式発表で、ブラッド・スミス（Brad Smith）最高法務責任者は「北朝鮮のハッカー集団が使用していたウイルスの駆除やアカウントの閉鎖などの対応をした」としている（Smith 2017）。タイミングがまったく同じであり、当局の指示でなかったにせよ、両者の間で連携が取られていたものと想像する。

れている（United Nations 2015a）。そして国家が主導して新たな国際法を作ろうという動きは見えない。新たな空間に新たな国際条約を、そしてそのガバナンスのために新たな国際機関設置をよびかけているのは一部のグローバルテックカンパニーである[91]。

2017 年 11 月にマイクロソフト社の最高法務責任者であるブラッド・スミスは高まるサイバー戦争から社会と市民を守るための、サイバー版ジュネーブ条約を設けることとサイバー版の赤十字社を設けることを提案した。赤十字社は戦争や天災（自然災害）時における傷病者救護活動を中心とした人道支援団体である。スイス人実業家アンリ・デュナン（Henri Dunant）の提唱により創立された。スミスはサイバー空間にも同様の人道保護のメカニズムが必要という主張を行った。学術研究の世界では、サイバー版の赤十字社、サイバー版の国際原子力機関（IAEA）やサイバー版の世界保健機関（WHO）やサイバー版の疾病予防センター（CDC）の必要性を主張する動きはそれ以前から存在していた。スミスとマイクロソフト社の発想が飛び抜けて斬新だったということではない。しかし、彼らにはそのアイデアを実現に移すだけの、資金力とブレインパワーがある。

サイバー版ジュネーブ条約をもうける動きは、2018 年のパリ平和フォーラムにおいて、パリ・コール（Paris Call）として部分的に結実した（France Diplomatie 2018）。同文書はサイバー空間における衛生の確保、選挙システムの保護、知的財産権の尊重などを確認するもので、2018 年の時点で 400 以上の国や団体や企業が賛同している[92]。

サイバー版の赤十字社を設ける動きとの関連は明らかでないが、2019 年 10 月にサイバー平和インスティチュート（Cyber Peace Institute）という組織が正式に発足した。

---

91 国際機関設置を設ける声はグローバルテックカンパニー以外にも拡大している。中谷和宏は「国連サイバー・セキュリティー機関」の必要性を訴える（中谷 2019: 4）。また、後述するサイバー空間安定化委員会は、「独立したマルチステークホルダーなサイバー空間の安定化のための機関が必要である」と主張している（Global Commission on the Stability of Cyberspace 2019）。

92 パリ・コール（Paris Call）の解説は次章に譲る。

同組織はスイスのジュネーブに本部を置く NGO である。特定のサイバー攻撃が発生した際のサイバーボランティアフォースの設置、説明責任や透明性の確保、そしてロビー活動の 3 つを主な活動の内容として説明している。マイクロソフト社やヒューレット財団が団体の活動に賛同し、資金を提供している。

司法

2018 年夏、フェイスブック社はミャンマー軍幹部数名のアカウントを停止した。ミャンマーのイスラム教徒少数民族ロヒンギャに対する迫害問題に関して国連人権理事会が設置した国際調査団が、軍幹部のフェイスブックへの投稿が迫害を助長していると非難の声を強めているなかでの出来事だった。

フェイスブック社は各国における国内法と自社のプラットフォーム上を行き交う情報との整合性に配慮してきた。捜査当局との調整に当たる各国の法制度を熟知したチームを持つ。ミャンマーでの出来事は、しかし、同社の責任がもはや各国国内法の執行をサポートするだけでないことを示唆している。ミャンマー政府が是とする広報活動も、より広い視野から問題があるときにはプラットフォーム上から削除する必要がある。同社の法務部は各国の捜査当局からの依頼に答える前に、市民的及び政治的権利に関する国際規約の第 19 条「干渉されることなく意見を持つ権利。公の秩序・道徳の保護と表現の自由」との整合性を確認するとしている。グローバルテックカンパニーのコンプライアンスは単に国内法を遵守するだけでは不十分という指摘がなされる状況になっている。

同じく 2018 年夏、グーグル社はプロジェクトメイブンへの参加をとりやめた。プロジェクトメイブンはドローンなどからの画像の自動処理を研究するプロジェクトであった。約 4000 人のグーグル社員が、この技術が軍隊のサーベイランス活動に流用され、最終的に人命に影響することを懸念して、プロジェクト中止の嘆願書に署名した。同プロジェクトを取り仕切るのは米国防省であり、プロジェクトは当然ながら米国内法にお

いては適法である。この件を契機に打ち立てられたグーグル社における AI 研究の原則は、国際法と人権への配慮を明示的に謳った。

以上、フェイスブック社とグーグル社の事例が示すとおり、グローバルテックカンパニーは、消極的ながらも、国際法への関心を強め、国際法を自ら解釈し、新たな国際法の制定を追求せざるをえない立場に追い込まれている（Deeks 2019）。フェイスブック社の創業者マーク・ザッカーバーグ（Mark Zuckerberg）は「フェイスブック最高裁」と通称される、同社の意思決定機関の設置を発表した。フェイスブック最高裁は 2020 年に活動を始める予定である。20 人から 40 人程度の有識者による諮問委員会であり、同社から独立し、同社の経営決定に拘束力のある決定を下すという。フェイスブック社のこの動きからは、グローバルテックカンパニーが一種の司法機能を内部に備えつつあることを指摘できる。

第２項 規範

レッシグのパセティックドットセオリーにおける規範とは、人々の価値観や道徳心に訴えかけ、社会にある程度共有される期待される振る舞いを規定するものである。サイバー空間において国家の行動の、人々の行動の規範が必要であることは立場の違いを乗り越えて共通の理解がある。政府はその動きをリードし、サイバー空間における国家の振る舞いについての規範を模索してきた。2015 年の国連政府専門家会合の報告書では 11 の規範が盛り込まれた（United Nations 2015a: 7–8）。この点について、複数の国家が合意にたどり着けたのはこの 2015 年が最後になる。以後、様々なサイバー空間の規範が提案されてきたが、それは複数のグローバルテックカンパニーの貢献の成果である。グローバルテックカンパニーは現代のノームファクトリー（規範の工場）といって差し支えない。

規範	賛同者	成立年
テックアコード（Cybersecurity Tech Accord）	マイクロソフト中心とする民間企業	2018
パリ・コール（Paris Call）	フランス政府、マイクロソフト他	2018
チャーター・オブ・トラスト（Charter of Trust）	シーメンス社（ドイツ）他	2018
GCSC 規範	サイバー空間安定化委員会	2017-2019
クライストチャーチコール	ニュージーランド政府、マイクロソフト他	2019

図表　4 -1 2015 年以降に提案された規範[93]

本章前半で触れたパリ・コール、別の章で細かく分析する GCSC 規範をのぞいた、3 つの規範の概要は以下のとおりである。

テックアコードはマイクロソフト社、フェイスブック社、ノキア社、シスコ社、デル社、シマンテック社、日立製作所など 34 社が賛同している。この規範の重要な点は「政府が仕掛けるサイバー攻撃は支援せず、自分たちの製品やサービスの改ざんあるいは悪用を防止する」という文言にあらわれるとおり、国家によるサイバー攻撃やサイバースパイ活動の増加を受けて、企業の中立性を保つための、線引きをしようとしている点にある。

チャーター・オブ・トラストはシーメンス社、エアバス社、ドイツテレコム社といったヨーロッパの企業が初期の賛同メンバーとして名を連ねた。日系企業では 2019 年に三菱重工社、2020 年に NTT がこれに加わった。製品の安全性を保つ、サプライチェーンを保護するなど 10 の宣言の中には「自由貿易協定の中にサイバーセキュリティ関連製品を含める」など市場のグローバル化を企図する点に特色がある。

93 それぞれの規範の内容について、依るべき文書は以下のとおりとなる。テックアコード（Cybersecurity Tech Accord 2018）、パリ・コール（France Diplomatie 2018）、チャーター・オブ・トラスト（Siemens AG 2018）、GCSC 規範（Global Commission on the Stability of Cyberspace 2017, 2018a, 2018b）、クライストチャーチコール（フランス大統領府 2019）。

クライストチャーチコールはオンライン上にあるテロリズムや暴力を誘発しかねないコンテンツへの対策について努力することを政府と民間企業が共に宣言したものである[94]。グーグル社、フェイスブック社、アマゾン社、マイクロソフト社、ツイッター社、デイリーモーション社などの主要なグローバルテックカンパニーが賛同者に名を連ねている。ニューヨーク大学教授のスコット・ギャロウェイはフェイスブック社とグーグル社のオンライン上での言論規制の姿勢について以下のように批判している。「現在のメディアはフェイスブックとグーグルに独占されている。気がかりなのは、それら 2 社の『我々をメディアと呼ばないでくれ。我々はプラットフォームだ』というスタンスだ。社会的責任を回避するこの姿勢によって、権威主義者やヘイト活動家がフェイクニュースを巧みに発信できるようになった」（スコット・ギャロウェイ 2018: 3002）。クライストチャーチコールはギャロウェイの指摘する責任回避を牽制する動きでもあった[95]。

これらの規範の賛同者、そしてその内容からはグローバルテックカンパニーの関与無しに規範が形成されるのは難しいと言える。クライストチャーチコールに顕著であるが、例えばオンライン上にあるテロリズムや暴力を誘発しかねないコンテンツへの対策という文書の目標を実現できるのは、基本的にグローバルテックカンパニーのみであるからである。クライストチャーチコールはたしかに多くの国家が賛同し、名を連ねている。

---

[94] 言うまでもなくクライストチャーチコールという合意形成の契機となったのは、クライストチャーチの 2 つのモスクでの銃乱射事件である。この事件では、ツイッター上で扇動され、掲示板システム（8chan）でアナウンスされ、ソーシャルメディア（Facebook）上で生中継され、その模様が動画サイト（YouTube）やニュースサイト（Reddit）などで繰り返し配信された。「世界最初のインターネットネイティブの銃乱射事件」である（Roose 2019）。

[95] クライストチャーチコールが、グローバルテックカンパニーにより大きな責任を認めさせようとした文書であることは、当時のニュージーランド首相の「（オンラインプラットフォームは）郵便配達員や単なるメッセンジャーではない。出版社である。利益だけを手にし、責任をとらないというのはゆるされない」という発言にも明確である（Novak 2019）。

それは、政府がお墨付きを与え、実際の作業をグローバルテックカンパニーが行うという既存の民営化（Privatization）の延長にある現象と捉えるのは難しい。なぜならば 2015 年以降、グローバルテックカンパニーが中心となり提案されてきた規範は国家の行動を制限し、グローバルなビジネスの土壌を育てる活動とも理解できるからである。

本項で示した、チャーター・オブ・トラストにおける自由貿易の推進を図る条項が好例である。「安全保障上の配慮」という大まかな説明で、海外製品排除の動きが見える市場に対する、グローバルテックカンパニーの反撃ともとれる。

第 3 項 市場

グローバルテックカンパニーの市場における、経済的な力は圧倒的である。まず GAFA の合計売上は 70 兆円以上と言われる。これは世界 3 位の経済大国である日本の税収 60 兆円を凌ぐ（菊地 2019）。BATH の一角である中国のアリババ社のビジョンは「米国、中国、欧州、日本に次ぐ世界第 5 位のアリババ経済圏を構築すること」である。2016 年における流通総額の実績は 60 兆円、これを 2020 年に 110 兆円までに成長させることを目標としている（田中 2017: 22）。

グローバルテックカンパニーはこれまでの花形産業との比較において、国家に富をもたらさない。企業が雇用を生み、中間層が豊かになり、国の経済が成長するという図式は現代のグローバルテックカンパニーにはことごとく当てはまらない。まず IT 産業においては雇用が生まれにくい。むしろ技術によって人が行っていたことをロボットやコンピュータに行わせるところに、産業の情報化の狙いがある。膨大な売上からの税収についても、様々な節税の手法が用いられていることに、税務当局の不満は募っている。国連大学の推計によるとグローバル企業全体の法人税の徴収逃れ額は年 5000 億ドル（約 56 兆円）に上るという。労働者への課税ではなく、プラットフォームの活動の拠点、つまりユーザが存在する位置に基づいて課税するなどの、新たな徴税の仕組みが検

討されつつある（シュワブ 2019: 14）。

さらにグローバルテックカンパニーが主導する仮想通貨により、マネーの流れが金融当局の手を離れる可能性もある。2019 年 6 月、フェイスブック社などがリードするリブラ協会は 2020 年から独自の仮想通貨リブラの運用を開始すると発表した（Libra Association 2019）。リブラはブロックチェーン技術を用いる点でビットコインなどの仮想通貨と似ている。大きな違いはリブラリザーブとよばれる法定通貨のリザーブを通して価値の安定性を保つ点にある。フェイスブック社だけでなく、ライドシェアサービスのウーバー社や音楽再生サービスのスポティファイ社などのテックカンパニーが賛同したことから、複数のオンラインサービスにおける共通の決済手段となることへの期待が高まった。

リブラは G20 や G7 の財務当局会合では冷淡な評価を受けた。執筆時点では G7 のステーブルコインに関する作業部会の成果文書（財務省 2019）などではマネー・ロンダリング対策の不十分さや、国家の持つ通貨主権への懸念が表明されている。フェイスブック社はこれらの懸念の声に応える形で、運用開始時期の延期を示唆している。

市場にあたえるグローバルテックカンパニーの力は、既存の制度との軋轢、政府との緊張などにより常に移ろっている。一方で、グローバルテックカンパニーは技術を持ち、データを保有している。新たなイノベーションはグローバルテックカンパニーから生まれる。その動きは早く、政府が規制を加えようとしても追いつけない状況が続いていることを指摘して、この項を終えたい。

第 4 項 アーキテクチャ

レッシグは特にアーキテクチャこそがサイバー空間を支配するとしている。グローバルテックカンパニーはサイバー空間のアーキテクチャをどのように作り上げ、そしてどのように変えていっているのだろうか。

第 1 章第 3 節第 2 項で述べたことの繰り返しになるが、サイバー空間はそのほとんどが民間企業の所有するインフラの集合である。米国のインテリジェンス機関と軍隊の通信のおよそ 9 割が民間の所有するインフラを使ってやり取りされる（Segal 2017; 67）。例えば、米国の 3 社（グーグル社、フェイスブック社、マイクロソフト社）と中国の 1 社（テンセント社）が 10 億人以上のユーザを獲得している。世界で最も先進的な能力を持つと言われる NSA は、米国ユタ州に約 12 エクサバイトを保存する巨大なデータセンターを持っていると言われるが、グーグル社はそれを遥かに超える規模のデータセンターを世界に複数所有している。各国政府はネットワークを「セキュアにする」という名目で検閲を行っているが、それらの検閲を可能にする技術開発は民間企業の仕事である[96]。インターネットの通信を相互にやり取りするインターネット・サービス・プロバイダーの中でも Tier1 と呼ばれる大手企業は 16 社しかなく、そのうち 6 つは米国企業である。海底ケーブルの敷設主体も、通信会社からグーグル、アマゾン、マイクロソフトなどに変わりつつある（大野 2018: 290）。インテリジェンス機関といえども、これらの企業の協力なしに大規模な情報収集活動をすることは、容易でない。21 世紀のグローバルテックカンパニーやサイバーセキュリティ企業は、20 世紀のロッキード・マーティン社、ボーイング社、レイセオン社などの防衛産業に相当する。

インターネットが生まれた頃、想定されていたのはノードが分散し、それぞれのノードが自律性を持ち、複数の経路でつながるネットワークであった。ところがインターネ

[96] 例えば北朝鮮の携帯電話事業は高麗リンク社によって提供されている。同社はエジプトのホスニ・ムバラクの長期政権化で業績を伸ばした通信会社オラスコム社が 75%を出資するエジプト系の企業である。イランでは 2009 年のグリーン革命に対する政府の弾圧をきっかけに、エリクソンや当時のノキア・シーメンス・ネットワークスなどの西側諸国が同国における移動通信事業から撤退し、その穴をファーウェイが埋めた。サイバー空間を巡って、国家と特定の民間企業との間に「特殊な共犯関係」が生まれつつあるとみることができる。

ットやサイバー空間は分散ではなく集約に向かっている。何事も集約して管理するほうが効率がよいのである。過去 10 年の、自らがインフラを用意する状態から、クラウドコンピューティングへの移行の流れは、今後も続くだろう。数えるほどのグローバルテックカンパニーによって多くの人のデータが握られている状態が生まれた[97]。できるだけ多くのデータにアクセスし、安全を確保したいグループとインターネットの分散性を維持したいグループの対立には埋めがたい溝がある。

インターネットやサイバー空間のアーキテクチャが市民に情報をもたらし、力を与えるという期待が大きかったことはすでに述べた。しかし、グーグル社の CEO を務めたエリック・シュミット（Eric Schmidt）らは「国家と市民はともにコネクティビティから力を得るが、どのようにして力を得るかは両者で異なる。民衆が、コネクティビティを通してアクセスできるようになったもの（情報やデータなど）から力を得ているのに対し、国家はゲートキーパー（門番）としての立場から力を得ている」（コーエン 2014: 126）と主張した。つまりインターネットが力を与えるのは市民だけではない、国家にもゲートキーパーとしての力が与えられるという指摘である。シュミットらの指摘の前半部は正しい。通信インフラを持つもの、集約されたデータにアクセスできるゲートキーパーは極めて効率的に情報を支配できる。シュミットらの指摘の後半部、その支配者を国家とする点は大いに疑問が残る。つまりこれまで見たとおり、そのゲートキーパーの位置を占めるのは国家ではなく、グローバルテックカンパニーであるからだ。グローバルテックカンパニーの構造上の強さは、数十億人のユーザが日々生成するデータのゲートキーパーであることに集約される。

---

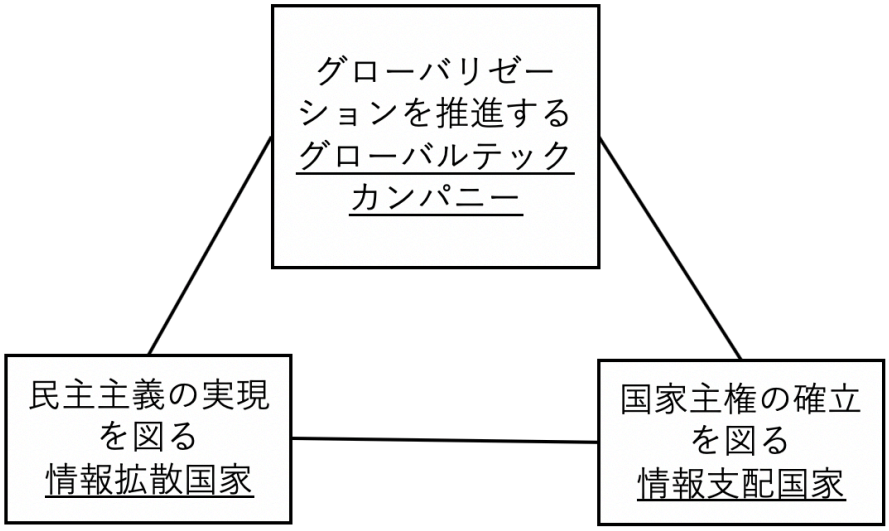
[97] コンテンツデリバリーネットワークとよばれる Web の負荷分散と高可用性確保のための技術も、分散から集約へ向かう動きの好例である。アカマイ社という米国の企業は世界中の Web の通信のおよそ 30%をコントロールする（小川 2014）。

第４節　グローバルテックカンパニーの戦略

第１項 情報拡散国家をとるか、情報支配国家をとるか

ここで再び、図表 4-2 に示すサイバー空間のトリレンマ理論を確認し、グローバルテックカンパニーの戦略を確認する。グローバルなサイバー空間、民主主義、国家主権の３つは共存しない。グローバルテックカンパニーはこれまでもそしてこれからも、グローバルなサイバー空間を追求していくであろう。先進国の国民の中では、グローバリゼーションを否定するかのような動きが広がっている。イギリスの国民は国民投票で EU 離脱を選択し、アメリカ国民は不法移民の国外追放や外国製品に対する関税引き上げを唱えていた候補者を大統領に選んだ。グローバルテックカンパニーは市民社会と共にグローバリゼーションの宣教者の役割を担っていると言える[98]。

[98] 例えば 2017 年 1 月、米国において 7 つのイスラム国家の国民の米国への渡航を制限する大統領令が署名された際に、これに真っ先に反対の声をあげたのはアマゾン社やマイクロソフト社などのグローバルテックカンパニーであった（Brad & Ann Browne 2019: 172）。



図表 4-2 サイバー空間のトリレンマ（再掲）

グローバルテックカンパニーは今後、情報拡散国家と手を取り合いグローバル・ガバナンスの実現を目指すのか。それとも情報支配国家と手を取り合って、情報化社会に黄金の拘束服を仕立てるのか。その点を解き明かすために、グローバルテックカンパニーを中心に据えた場合の情報拡散国家と情報支配国家との関係を整理していく。

第２項 グローバルテックカンパニーと情報支配国家

グローバルテックカンパニーと情報支配国家の関係は複雑である。グローバルテックカンパニーの中でも特にソーシャルメディアサービスは市民社会をエンパワーし、集合を助けると思われていた。ソーシャルメディアによってリベラルな民主主義が世界にあまねく広がると期待されていた。しかし、昨今では、ソーシャルメディアには「これこそが権威主義を最も効果的に実現する手段ではないか」という疑念の目がむけられ、「社会の病（society's ills）」として批判されている（Deibert 2019: 25）。批判の対象となるのはソーシャルメディアの構造である。ソーシャルメディアのビジネスモデルはユーザの

行動の解析を必要とする。ソーシャルメディアの運営者は、ユーザの行動を解析し、最適な広告を表示し、それによって広告主からの報酬を受け取っている。ユーザは明示的に、あるいは非明示的に、ソーシャルメディア運営者からの監視を快く受け入れ、その代わりに無料で利便性のあるサービスを使用している。ユーザがサービスを無料もしくは安価で利用するかわりに、サービス提供者が行動に基づいて最適化された広告を提示し広告料収益を得る構造を「サーベイランス資本主義」と呼ぶ研究者もいる。

グーグル社と中国政府との関係の移ろいはグローバルテックカンパニーと情報支配国家の関係の典型として興味深い。シリコンバレーで創業し、自由でオープンなインターネットを標榜するグーグル社は創業以来、情報支配国家と距離を置こうとしていた。しかし、膨大なインターネット人口とそれが生み出すデータを持つ中国市場の魅力に抗えず、中国市場向けのサービスを提供していた。2010 年に起きた、オーロラ作戦とよばれる高度で大規模なサイバー攻撃により、同社の中国オフィスから大量の情報が盗まれていたことが発覚した。同社は中国市場からの撤退を決め、中国内の拠点を大幅に縮小した。基本的な価値観が異なっていても、サイバー攻撃によって知的財産を危機に晒しても、グーグル社は中国市場をあきらめていない。2018 年にはドラゴンフライ（Dragonfly）とよばれる社内プロジェクトは中国内で使える検索エンジンを開発していることがリークされ、1400 人の従業員がこれに反対する署名運動に賛同した。

サーベイランス資本主義はより多くのユーザに対して、より多くの広告を届けることを求める。中国、インド、インドネシアなどの大規模な市場を、政治的なスタンスの違いだけで諦めるわけにはいかない。中国で 2016 年に成立した網絡安全法は、データを中国の領土外に保存することについて制限を加える内容であった。サイバーセキュリティの研究者はこれにより、グローバルテックカンパニーが中国市場から緩やかに離れると予想した。米国に本拠を置くグローバルテックカンパニーは、自国政府が中国の経済政策、政府と民間企業の関係の構造改革を求めていることを理解しているはずであり、

自国政府との関係維持を望むグローバルテックカンパニーが中国政府と接近するはずがないという言説がみられた。この予想は大きく外れ、テックカンパニーは中国市場にさらに投資を行った。アップル社は 2018 年に同社のクラウドサービスの中国人ユーザ専用のサーバを貴州省に設け、グーグル社の中国向け検索エンジン開発もこの時期に行われた。「アップルはアメリカ国内では 5 万人しか雇っていないけれども、中国で 50 万人分もの仕事を増やしている」（佐々木俊尚 2013: 288）ということからも分かるとおり、中国なしにグローバルなビジネスが成立しない企業は製造業を中心に多く存在する。結果、多くのグローバルテックカンパニーが中国政府の望む規制をクリアした上で、中国でのビジネス拡大に懸命に努力をした。グローバルテックカンパニーはグローバリゼーションという価値観の敷衍を抑制し、情報支配国家の市場に参入するという戦略をとっている。

米国に本拠を置くグローバルテックカンパニーは、米国政府の手先ではない。グローバルテックカンパニーは自らの成長が、米国以外の市場に大きく依存していることを理解している。2017 年時点で、米国のテックカンパニーの収益の 6 割は米国外からもたらされる（Segal 2017: 68）[99]。2013 年に NSA の元契約職員エドワード・スノーデンは米国インテリジェンス機関による大規模なサーベイランス活動の存在を明らかにしたが、そこで同時に明らかになったのは米国政府と米国に本社を置くグローバルテックカンパニーとのせめぎ合いである。例えば、NSA はヤフー社に対して PRISM プログラムに協力しなければ 1 日当たり 25 万ドルの罰金を科すと通知した（Timberg 2014）。NSA はさらにプログラムに協力しないグーグル社およびヤフー社にしびれを切らし、上位の通信会社レベル 3 社の協力を密かに得ていた（Perlroth & Markoff 2013）。暗号ソフトの

[99] 2015 年冬、筆者はフェイスブック社の本社を訪問した。その際に社員用カフェテリアの至るところに、世界地図の下に「Facebook ユーザの 6 割は非英語圏」というスローガンが書かれたポスターが掲出されるのを目にした。社員に対して米国外市場の重要性をアピールする狙いがあったと想像する。

開発販売をしている RSA セキュリティ社に対しては、必要に応じて当局が復号できるような弱い乱数生成アルゴリズムを暗号ライブラリの標準に設定するよう求め、その対価を支払った（Menn 2013）。グローバルテックカンパニーは米政府のサーベイランスに対抗して、より高度な暗号を用いるようになっており、FBI ですら押収した電子デバイスに含まれる暗号化された情報を復号するのに苦心している[100]。米政府はグローバルテックカンパニーの協力を得るために、なだめたり、脅したり、金を払ったりしている。少なくとも、「国家安全保障上の理由で」という但し書きがつけば、企業が政府に無条件に協力するという環境ではない。

では、中国に本社を置くグローバルテックカンパニーはどうだろう。西側の政府も、研究者も「共産党が民間部門への影響力を持っている以上、中国企業は国から離れた独立した存在ではありえないという懸念に突き動かされている」（ウィリアムズ 2019: 71）ようである。前の段落で米国政府と米国のグローバルテックカンパニーの間の緊張を指摘したが、同様の緊張は中国にもあると考えるのが自然である。中国のグローバルテックカンパニーが中国政府および中国共産党の手先でないという主張はすでに第３章第２節第５項で行った。ここでは改めて収益の構造への読者の着目を促したい。

中国は巨大な市場であるが、それでも有限である。中国のグローバルテックカンパニーは早晩、国内での市場拡大を望めなくなり、国外市場開拓に取り組むことになる。アリババの「米国、中国、欧州、日本に次ぐ世界第 5 位のアリババ経済圏を構築」（田中 2017: 22）という目標からは、すでに中国外での競争を予期しているようにも思える。中国のグローバルテックカンパニーの収益に占める海外の割合が増えるにつれて、中国政府の声の重要性が失われていくだろう。

そしてインターネットやサイバー空間は集約に向かっている。何事も集約して管理す

[100] 2017 年 3 月、当時のジェームズ・コーミー（James Comey）FBI 長官の発言によれば「FBI は 2016 年の第 4 四半期におよそ 2,000 台の電子デバイスを受け取り、1,200 台についてはデータにアクセスできなかった」（C-SPAN.org 2017）。

るほうが効率がよい。良いサービスが、多くのユーザを惹きつける[101]。多くのユーザは多くのデータをもたらす。多くのデータはさらによいサービスを生み出す。このサイクルが繰り返された結果、少数のグローバルテックカンパニーによって多くの人のデータが握られている状態が生まれている。米中両国を股にかけ活躍する台湾生まれのベンチャーキャピタリストであるリー・カイフー（Lee, Kai-Fu）が予測する、「今後もデータの寡占が進み、米国と中国の少数の企業によって独占され、残りの多くはスクラップを拾う」（Lee 2018: 169）という未来は絵空事ではない。

第３項 グローバルテックカンパニーそのもののガバナンス

ここで改めてグローバルテックカンパニーそのものについて検討したい。グローバルテックカンパニーは言うまでもなく営利企業であり、その収益の最大化を追求する組織である。これまで見てきたとおり、現在のサイバー空間のガバナンスを支えるのは、政府の対処が遅れている状況のもとで、様々な創意工夫で対応してきた、グローバルテックカンパニーの貢献が大きい。たとえばマイクロソフト社は「デジタル平和」というスローガンを掲げ、その実現のために多くのリソースを投入している。これは短期的にマイクロソフト社の利益にはなりえない。自社の利益と公共の利益は両立しないことが多い。それが衝突した場合、グローバルテックカンパニーは自社の経済的利益よりも公共の利益を度々優先してきたのである。

例えば、マイクロソフト社の幹部の手記では、ワナクライというウイルス感染が世界中に広がった際の、マイクロソフト社内部の議論が開陳されている。ワナクライは Windows の脆弱性を悪用するウイルスであり、感染を予防するには修正プログラムをインストールすることが必要であった。マイクロソフトは修正プログラムを公開済みで

101 グローバルテックカンパニーが保有するデータはネットワーク効果による独占や寡占が働きやすい（大木 2018）。

あり、顧客に対してただしにインストールして被害を予防するように呼びかけた。問題となったのは、サポート期間が切れて、修正プログラムが提供されていない古いバージョンの Windows である。サポート期間が終わった Windows XP というバージョンのための修正プログラムを提供すべきか否か、マイクロソフト社の幹部は自社の利益よりも公共の利益を優先し、修正プログラムを提供した（Smith & Ann Browne 2019: 64-69）。

そのことを踏まえた上で、研究者として筆者は、グローバルテックカンパニーは今後も公共の利益を実現する組織であり続けられるかという、疑問を呈さなければならない。グローバルテックカンパニーはサイバー空間において、法、規範、市場、アーキテクチャのすべてにおいて、国家を凌ぐ強い影響力を持つ。グローバルテックカンパニーは果たして、国家の代わりとなれるのだろうか。

情報化が国家の役割を変えるという指摘は様々な研究者によってなされてきた。国際政治学者の土屋大洋はインターネットにエンパワーされた人々が「創発的なアクティビズム」を展開し、国際政治の中で発言力を持つが故に、暴力装置としての国家の役割は相対的に小さくなると主張した。そして「プラットフォームとしての国家にかわるのはインテル、マイクロソフト、ヤフー、グーグル、アマゾンといった米国の企業かもしれない」とグローバルテックカンパニーによるガバナンスの可能性を指摘している（土屋 2007: 170–75）。国家がプラットフォームに取って代わられるという土屋の論を「場」という形で言い表したのが佐々木俊尚である。「権力は、国民国家から奪い取られるのです。国家の権威は消滅し、最終的には国という形そのものでさえも無くなっていくかもしれません。すべては〈場〉に吸収され、〈場〉こそが国家に代わる権力になっていく」。そして「超国籍企業が国民国家を終わらせる」という（佐々木俊尚 2013: 2095, 2100）。はたまた、パラグ・カンナは「究極的には、影響力を持つのは技術上の優位に立つ者であり、国家ではない。」と断言している。「インターネットはすでにデジタル主権と封建制度の兆候を見せており、そこに存在する競争関係は政治的な地理と一致しな

い」（パラグ・カンナ 2017: 148）という言葉を現在のサイバー空間になぞらえると、そこには物理的な制約を離れた新しい秩序の出現を想定せざるをえない。

グローバルテックカンパニーは果たして、国家の代わりとなれるのだろうか。その可能性は極めて低いと主張したい。サイバー空間はいろいろな意味で、支配者不在の無秩序な世界という、国際関係論の古典的仮説が現実化したものともいえる。インターネットの誕生から 30 年以上の歴史を振り返ると、「仮想世界は既存の世界秩序を覆したり、組み替えたりすることはないが、現実世界でのあらゆる動きを複雑にしていく」（コーエン&シュミット 2014: 398）というのがより正確な解釈ではないだろうか[102]。

グローバルテックカンパニーに国家の代役が務まらない理由は、それらの企業自身に 1）民主的な正当性、2）透明性[103]、3）プライバシーへの配慮、4）中立性が備わっていないからである。多くの情報支配国家はこれらのいくつかを欠いているが、それでもなおグローバルテックカンパニーよりは「まし」である。グローバルテックカンパニーとユーザは一方的な関係で結ばれている。「企業が封建領主さながらに一方的に優位に立ち、ルールはいつ変更されるかわからない」（シュナイアー 2016: 333）のである。

イギリスの政治家トニー・ベン（Tony Benn）は民主主義政治を解説する本の中で、権力を理解するためには、権力者に対して以下の質問をなげかけることをすすめた（Benn & Mullin 1981）。

---

102 コーエンらはサイバー空間と現実空間の同一性を根底においている。もう 1 つの指摘は「一般に国家が仮想世界でもつ力が、現実世界での力に釣り合うまでには、まだ時間がかかる。このことは一部の新しい主体や、正当に評価されていない主体にとっては、チャンスとなる」というものであり、これは現在サイバー空間において積極的な動きを見せるシンガポール政府、エストニア政府、リトアニア政府などの動きを的確に解説している。

103 ヤフー社、グーグル社、マイクロソフト社などが透明性レポートという報告書を定期的に発行し、自らと政府や法執行機関などとの関係について透明性確保を図っている。逆説的ではあるが、そのような報告書が求められるほどに彼らの活動が不透明だという告白と捉えることもできる。

- いかなる権力を持っているか。（What power have you got?）
- その権力をどこから得たか。（Where did you get it from?）
- 誰のためにその権力を行使するのか。（In whose interests do you exercise it?）
- 誰に対する説明責任を負っているのか。（To whom are you accountable?）
- その権力を剥奪するにはどうすればよいか。（how can we get rid of you?）

ベンによれば、特に最後の質問が重要で、これが満たされないのは民主主義が確保されたシステムとは言えないという。グローバルテックカンパニーはユーザから集められたデータと技術力を持って、現代のサイバー空間に極めて大きな影響力を持っている。何者かがグローバルテックカンパニーの権力を剥奪するには、そのサービスをボイコットすればよい。しかし、現実にグローバルテックカンパニーが提供する、オンラインサービス無しに日常生活を送るのは困難である[104]。ボイコットという選択はときに社会的に大きな不利益を生む。サイバー空間はグローバルテックカンパニーの権力を剥奪することは難しいという状況にまで追い込まれている。

グローバルテックカンパニーに国家の代役が務まらないとすれば、情報拡散国家と手を取り合いグローバル・ガバナンスの実現を目指すのか、それとも情報支配国家と手を取り合って、情報化社会に黄金の拘束服を仕立てるのかの二者択一を迫られる。現在のグローバルテックカンパニーのサーベイランス資本主義とユーザとの封建的な関係は情報支配国家との親和性が高いとみられる。しかし、長期的には、より多くのデータを持つのが、情報拡散国家陣営なのか、情報支配国家陣営なのかによってグローバルテックカンパニーが判断を行うことになる。

---

[104] 3 週間にわたり GAFA のサービスの利用断ちの実験を行った新聞記者は、生産性が 3 分の 1 になり、仕事に支障をきたしたとまとめた（日本経済新聞データエコノミー取材班 2019: 642-695）。

第５節　まとめ

本章ではグローバルテックカンパニーはサイバー空間のガバナンスにどのような力を持つか、その力は何に由来するか、という問いを立てた。そしてその答えを得るために、レッシグのパセティックドットセオリーを用いて、法、規範、市場、アーキテクチャのすべてにおいて、国家を凌ぐ強い影響力を持つグローバルテックカンパニーの力を描いてきた。特にアーキテクチャの項で述べたとおり、グローバルテックカンパニーの力の源泉は、数十億人のユーザが日々生成するデータに自由にアクセスできる点にある。

現在のサイバー空間のガバナンスを支えるのは、政府の行動が無い中を様々な創意工夫で対応してきたグローバルテックカンパニーの貢献が大きい。しかし、一般論として経済的な利益と公共の利益は両立しない。グローバルテックカンパニーは経済的利益よりも公共の利益を度々優先してきた。それはここ数十年の行動パターンにすぎず、より市場の寡占化が進み、競争が激しくなる前に、グローバルテックカンパニーは自らの役目を問い直し、国家の代役はできないことを自覚すべきである。グローバルテックカンパニーには技術と大量のデータと資金が存在するが、それを大規模に行使する民主的な正当性も、ガバナンスも中立性も確保されていない。

したがって本章の結論としては、グローバルテックカンパニーが新たな国際秩序を作る可能性は低いと結論づけ、今後情報拡散国家もしくは情報支配国家のいずれかを支える役割を担うものと予想する。他方で、グローバルテックカンパニーがガバナンス上の課題を克服した場合、サイバー空間を契機に、いわゆるウェストファリア国家像を見直さなければならない。国家に認められていた主権のいくつかがグローバルテックカンパニーによって剥奪されれば、国家の基本コンセプトが揺らぐからである。

第５章　合意を巡る戦い

第１節　はじめに

ここまで本論文では、サイバー空間における、情報拡散国家と情報支配国家とグローバルテックカンパニーの３つのアクターに分類し、その動向を個別に考察してきた。情報拡散国家と情報支配国家とグローバルテックカンパニーはそれぞれにグローバルなサイバー空間、民主主義、国家主権を追求しているが、その主張が国際社会においてどう衝突しているか、合意を巡る戦いを描きだすのが本章の狙いである。

サイバー空間の安定、そしてサイバーセキュリティの確保を目指して、実に多くのサイバー空間をめぐる合意がなされてきた。その一部はすでに前章までに述べてきた。それら合意は特定の職能グループの中での明文化されていないものから、国際法に近いものまで数多くある。ガイドライン、規範、国際的な共同宣言、戦略文書、これらを本章では大きく「合意」とひとくくりにする。

サイバー空間は決して無法地帯ではない。国際人権法があり、国際電気通信に関する法があり、宇宙や海などの空間に固有の法があり、国際人道法（戦時国際法）があり、これらが多くのサイバー空間での活動に影響を与えている。合意をめぐる戦いは、これらの既存の法体系が明らかにしていない点を検討し、関係者間での理解を平準化するプロセスであるとも言える。

サイバーセキュリティのグローバル・ガバナンスの考える上で、合意の最小単位は各国家なり、企業の内部での合意であろう。具体的には各国が策定するサイバーセキュリティ戦略に着目する。サイバーセキュリティ戦略は国民に対してサイバー空間のあるべき姿を示す合意文書であり、対外的には自国の姿勢を示すメッセージである。次にそれ

らの個別のアクターを超えて、国際的になされた合意が数多くある。例えば、情報拡散国家と情報支配国家とグローバルテックカンパニーのグループの内部での合意（グループ内合意）、そしてグループを超える合意（グループ間合意）である。

合意を研究することは、サイバー空間の現在を理解することにつながる。これまでサイバー犯罪条約や国連政府専門家会合など個別の合意を対象にして優れた分析が行われてきた（Henriksen 2019; Ziolkowski 2013; 須田 2015）。しかし、多くの場合、これらの分析は個別の国際合意、あるいは複数の国際合意の比較分析にとどまる。本章を通して描きたいのは、より複合的な合意を巡る戦いの様相である。ヒントとなったのはジンハン・ゼン（Jinghan Zeng）らの中国のサイバー政策研究である（Zeng, Stevens, & Chen 2017）。ゼンらは、中国は一貫してインターネットにおける国家主権を主張しているが、政府の中国国内への説明を分析すると、国家主権の構成要素を政府が国内向けと、国外向けで使い分けていることを指摘した。国際政治研究において再三指摘されてきた、内政と外交の連関という事象はサイバー空間においても存在すると考えられる。またサイバー空間をめぐる合意はしばしば研究者の目に届かない密室で行われる。最終的な合意文書だけを頼りに、合意に至るまでのプロセスを紐解くことは難しい作業である。しかし、その密室での議論の中にこそ、サイバー空間のガバナンスを巡る利害の衝突があらわれるはずである。合意はその衝突にきれいな装飾を施したものである。

これらの問題を克服するため、本章では以下のようにサイバー空間の合意を論じていきたい。まず第２節では主要国家のサイバーセキュリティ戦略を国家と国民の間の合意ととらえ、主要８カ国のサイバーセキュリティ戦略を分析していく。各国の国内向けの言説を収集していく。次に第３節ではおよそ 20 の国際的な合意文書を分析し、国際社会の論点や国内向け言説との違いを明らかにしていく。最後に第４節ではサイバー空間安定化委員会（GCSC）における規範形成のプロセスを通して、合意に埋め込まれた参加者の安全保障上の、あるいは経済上の利益を得るためのエゴイスティックな主張を明ら

かにしていく。後述するが筆者は 2017 年から 2019 年まで行われた GCSC の活動に直接参加する機会を得た。つまり第４節は参与観察の手法を用いて、密室の議論の様子をできるだけ読者に与えるのが目的である。第５節では国家サイバーセキュリティ戦略、国際合意、なかでも GCSC という特定の合意プロセスの 3 つの分析から得られた情報を総合して考察を行う。

第２節　主要国家のサイバーセキュリティ戦略

第 1 項 分析の対象

サイバーセキュリティ戦略はその国におけるサイバーセキュリティ対策の重要な要素である[105]。サイバーセキュリティ戦略の定義については現在も検討が行われているが、ここでは「一定の期間にわたって特定の国家の目標を達成するために作成される、情報通信インフラに存在する情報・非情報資産の保護のための計画、もしくは方法論[106]」と定義する。2011 年には少なくとも 20 の国がサイバーセキュリティ戦略を策定し、公開していたが、2017 年にはその数が少なくとも 78 カ国と増加している。

多くの政府がサイバーセキュリティ戦略と呼ばれる文書を策定している一方で、その内容が極めて多様である。国家サイバー戦略ポリシー、情報セキュリティ戦略など文書の名前が異なるだけでなく、策定の時期、その文書の国内における位置づけ、取りまとめを行った政府機関などが大きく異なっている。なぜそれらは必要なのか。それによって各国政府はどのような合意をし、課題を解決し、いかなる読者に、どのようなメッセ

105 本節は小宮山、土屋（2018）を一部改変し利用した。
106 リーザ・アズミ（Riza Azmi）らにおけるサイバーセキュリティ戦略の定義、すなわち「a careful plan or method of protection both informational and non-informational assets through the ICT infrastructure for achieving a particular national goals usually over a long period of time」を参考にした（Azmi et al. 2016）。

ージを届けようとしているのであろうか。サイバーセキュリティ戦略から主要国のスタンスを明らかにしていきたい。

分析の対象は国連安全保障理事会常任理事国 5 カ国（米国、英国、フランス、ロシア、中国）、それに日本とドイツとオーストラリアを加えた 8 カ国に限定した。2015 年後半から 2017 年前半までの関連文書と分析対象国が過去に策定したサイバーセキュリティ戦略を分析対象とし、それらの国のサイバー空間に関する認識の差異、政策転換などの変化を明らかにすることを試みた。対象としたサイバーセキュリティ戦略は以下の図表５-1 のとおりである。

本節の流れは以下のとおりである。まず第２項で主要 8 カ国のサイバーセキュリティ戦略の内容の質的な差異を見出す作業を通じて、サイバーセキュリティ戦略の多様性が生まれる背景を考察する。つづく第３項ではサイバーセキュリティ戦略をその内容をもとに 4 つの類型に分けることを試みる。それぞれの類型に応じたサイバーセキュリティ戦略策定者の狙いを考察するための視座を提供する。第４項でそれら議論をまとめる。

グループ	国名	文書名（成立もしくは公開年）
情報拡散国家	米国	“Cyberspace Policy Review”（2009）[107] “International Strategy for Cyberspace”（2011）[108] “Executive Order - Improving Critical Infrastructure Cybersecurity”（2013）[109] “The Department of Defense Cyber Strategy”（2015）[110]

[107] Government of United States, “Cyberspace Policy Review,” https://www.dhs.gov/publication/2009-cyberspace-policy-review （2019 年 12 月 3 日確認）

[108] The White House, “International Strategy for Cyberspace - Prosperity, Security, and Openness in a Networked World -,” https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf （2019 年 12 月 3 日確認）

[109] The White House, “Executive Order - Improving Critical Infrastructure Cybersecurity,” https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity （2019 年 12 月 3 日確認）

[110] The Department of Defense, “The Department of Defense Cyber Strategy,”

	英国	“National Cyber Security Strategy 2016-2021”（2016）[111] “The UK Cyber Security Strategy Protecting and Promoting the UK in a Digital World”（2011）[112]
	フランス	“French National Digital Security Strategy”（2015）[113]
	日本	『サイバーセキュリティ戦略』（2015）[114] 『サイバーセキュリティ国際連携取組方針』（2013）[115] 『重要インフラの情報セキュリティ対策に係る第 4 次行動計画』（2017）[116]
	ドイツ	“Cyber Security Strategy for Germany”（2011）[117]
	オーストラリア	“Australia's Cyber Security Strategy”（2016）[118]

https://archive.defense.gov/home/features/2015/0415_cyber-strategy/final_2015_dod_cyber_strategy_for_web.pdf （2019 年 12 月 3 日確認）

111 Government of United Kingdom, “National Cyber Security Strategy 2016-2021,” https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf （2019 年 12 月 3 日確認）

112 Government of United Kingdom, “The UK Cyber Security Strategy Protecting and promoting the UK in a digital world,” https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/UK_NCSS.pdf （2019 年 12 月 3 日確認）

113 National Cybersecurity Agency of France, “French National Digital Security Strategy,” http://www.ssi.gouv.fr/uploads/2015/10/strategie_nationale_securite_numerique_en.pdf （2019 年 12 月 3 日確認）

114 内閣サイバーセキュリティセンター『サイバーセキュリティ戦略』 http://www.nisc.go.jp/active/kihon/pdf/cs-senryaku.pdf （2019 年 12 月 3 日確認）

115 内閣サイバーセキュリティセンター『サイバーセキュリティ国際連携取組方針 ～j-initiative for Cybersecurity～』 https://www.nisc.go.jp/active/kihon/pdf/InternationalStrategyonCybersecurityCooperation_j.pdf （2019 年 12 月 3 日確認）

116 サイバーセキュリティ戦略本部『重要インフラの情報セキュリティ対策に係る第 4 次行動計画』 https://www.nisc.go.jp/active/infra/pdf/infra_rt4.pdf （2019 年 12 月 3 日確認）

117 The German Federal Office for Information Security, “Cyber Security Strategy for Germany,” https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/cyber-security-strategy-for-germany （2019 年 12 月 3 日確認）

118 Australian Government, “Australia's Cyber Security Strategy: Enabling Innovation, Growth & Prosperity,” https://cybersecuritystrategy.homeaffairs.gov.au/AssetLibrary/dist/assets/images/PMC-Cyber-Strategy.pdf （2019 年 12 月 3 日確認）

情報支配国家	ロシア	“Basic Principle for State Policy of the Russian Federation” （2013）[119]
	中国	国家互聯網信息弁公室『国家網絡空間安全戦略』（2016）[120] 中華人民共和国政府『網絡空間国際合作戦略』（2017）[121]

図表 5-1 分析対象としたサイバーセキュリティ戦略

サイバーセキュリティ戦略の分析はこれまでも様々なアプローチで試みられてきた。リーザ・アズミ（Riza Azmi）らは 54 カ国のサイバーセキュリティ戦略の調査を通じてサイバーセキュリティ戦略が現在のサイバー空間における自国の保護だけを目的としておらず、技術革新が進行中のサイバー空間における将来の権益確保のための法的ツールとしての側面を持つと結論づけた（Azmi, Tibben, & Than Win 2016）。また、キョンシク・ミン（Kyoung-Sik Min）らは米国、欧州、日本のサイバーセキュリティ戦略について政府の役割と民間事業者の役割の多寡の観点から分析を行い、サイバーセキュリティの分野における官民の役割の分担の難しさを指摘する（Min, Chai, & Han 2015）。エリック・ルイーフ（Eric Luiijf）らは 2003 年の 19 のサイバーセキュリティ戦略を対象とした研究においてサイバーセキュリティ戦略を具体性、測定可能性、達成可能性、現実性、適時性の 5 つの尺度で評価するアプローチを提案した（Luiijf, Besseling, & Graaf 2013）。

本節とこれらの先行研究の違いは、次項で提示する 4 つの分類に基づき、各国の思惑を再整理した上で、各国がそれらを作成・公表する意義を検討することにある。サイバ

119 Government of Russia, “Basic Principle for State Policy of the Russian Federation in the Field of International Information Security to 2020,” https://ccdcoe.org/sites/default/files/strategy/RU_state-policy.pdf （2019 年 12 月 3 日現在、同文書を公開する Web サイト無し。本論文では 2017 年 9 月時点で確認できた文書に基づき記述した。なお英訳作成者は不明）

120 国家互聯網信息弁公室『国家網絡空間安全戦略』http://www.cac.gov.cn/2016-12/27/c_1120195926.htm （2019 年 12 月 3 日確認）

121 中華人民共和国政府『網絡空間国際合作戦略』http://news.xinhuanet.com/2017-03/01/c_1120552767.htm （2019 年 12 月 3 日確認）

ーセキュリティ戦略はなぜ必要なのか、言い換えれば、なぜ、誰に向けて発信されるのかを分析対象とする点にある。

そのため、それぞれの戦略文書について特に以下の点を確認した。基本情報として収集したのは、成立または公開の時期、文書の有効期限、所管する省庁、関連する戦略文書や法律などの国内文書体系法との関係における文書の位置付けである。次に、各国の現状認識に着目した。例えば、サイバーセキュリティおよびサイバー空間といった言葉の定義、重要インフラの定義、サイバー空間に関する現状の認識などである。サイバーセキュリティ戦略そのものの内容については、戦略策定の目的、目的達成のための特徴的な施策、施策実施のための予算措置の有無などに着目した。合わせて国家によるサイバー攻撃能力の準備、サイバーセキュリティ技術を活用したインテリジェンス活動についても記述を収集した。

第２項 サイバーセキュリティ戦略の比較

サイバー空間のあるべき姿の相違

一般的にサイバー空間におけるセキュリティの確保を目的とするのがサイバーセキュリティ戦略であるが、サイバー空間のあるべき姿について主要国の中に意見の相違があることを指摘しなければならない。例を挙げれば、日本政府のサイバーセキュリティ戦略は自国の施策を示す前に、まず現在のサイバー空間について「情報の自由な流通の確保」「法の支配」「開放性」「自律性」「多様な主体の連携」という 5 つの基本原則が国境を超えて確保されるべきであると掲げている。同様の記述は中国とロシアを含めた多くの国で見られる。

逆に中国とロシアの戦略にのみ見られたのが内政干渉への警戒感を示す記述である。ロシアは「国際情報セキュリティに関する 4 つの主要な脅威」の 1 つとして「主権国家の内政への干渉、公的秩序の破壊」などを明記している。中国はサイバーセキュリティ

戦略の目的として「サイバー空間における平和、安全、開放、合作、秩序」を掲げており開放性を否定しているわけではない。一方で、同文書後半に「ネットワークを利用した他国の内政への干渉、政治制度への攻撃、社会的動乱の扇動（後略）」をサイバー空間の脅威として挙げて、やはり内政への干渉への警戒感を示している。ただし内政干渉の具体的事例についてサイバーセキュリティ戦略には記述されていない。これまでの議論を振り返れば、国内の治安維持の必要性からサイバー空間の利用に制限を行っている中国とロシアは、「言論の自由」を理由に規制の撤廃を求める西側諸国の主張を横槍と捉えていると解釈すべきであろう。

ロシアにおいては、情報セキュリティとサイバーセキュリティの言葉は明確に使い分けられている。サイバーセキュリティはソフトウェアやハードウェアなどのシステムそのもののセキュリティを意味し、情報セキュリティはその上でやりとりされる情報の中身（コンテンツ）も含めた保護を意味する。「ネットワークやシステムのセキュリティだけでなくコンテンツのセキュリティも国家により管理しないと、国家の安全を担保できない」（佐々木孝博 2013: 10）との考え方から、今後もロシアはコンテンツの規制に前向きな姿勢を持ち続けるであろう。

サイバー攻撃能力の保持・使用

政府・軍隊がサイバー攻撃を行う能力を保持することについて各国のサイバーセキュリティ戦略はどのような記述をしているのだろうか[122]。分析対象の中で最も直接的にサイバー攻撃能力に触れているのは「攻撃的サイバー能力について世界のリーダーの地位を目指す」という英国、そして「抑止のためにサイバー攻撃能力を使用する」とするオーストラリアのサイバーセキュリティ戦略である。

---

122 各国のサイバーセキュリティ戦略に、サイバー攻撃能力について言及されるケースが増えてきたが、中国、ロシアについてはサイバー攻撃能力についてサイバーセキュリティ戦略の中で触れることを避けている。ロシアについては佐々木の前掲論文が、そして中国については横山の報告書に詳しい（横山 2016）。

サイバー攻撃能力に言及するのはこの 2 カ国が初めてではない。振り返れば米国、ロシア、イスラエルを始めとするいくつかの「サイバー先進国」が、密かに、サイバー攻撃能力を高め、サイバー兵器開発を行っているという推測は複数の専門家によってなされていた[123]。しかしながらサイバー攻撃能力について政府がその存在を対外的に認めることはなかった。

2010 年に転機が訪れる[124]。まず米国においてサイバー軍が公式に発足した。さらに米国がイランの核処理施設をサイバー兵器によって攻撃したいわゆるスタックスネット事件[125]が公に知られることとなった。サイバー攻撃能力を有していることを否定することが難しくなったのである。

そのような状況下、2011 年 3 月に公表された米国の『サイバー空間に関する国際戦略』はサイバー攻撃能力について「(米国は) サイバー空間での自衛の権利を保持する」という表現ではあったものの、「サイバー空間での敵対的行為に対して軍事力の使用も辞さない」という姿勢を明らかにした。それから約 4 年後の 2015 年 4 月に公表された『国防総省サイバーセキュリティ戦略』は、イスラム国がサイバー空間を活用し、人員のリクルート活動を行っていることなどを引き合いに、国防総省におけるサイバーセキ

---

123 2007 年 4 月にエストニア政府が同国を解放した旧ソ連軍兵士の像を首都タリン市郊外に移設しようとしたことをきっかけとして、エストニアのコンピュータ・ネットワーク及び銀行などの重要インフラに対し、サイバー攻撃が行われた。2 週間以上に渡って断続的に銀行や電子政府サービスが利用できないという自体が発生した。この事件は多くの耳目を集め、その経緯からエストニア政府は攻撃をロシアによるものと非難したが、現在に至るまでロシア政府が関与したという確かな証拠は確認されていない。

124 アダム・シーガル（Adam Segal）は、2012 年 6 月から 2013 年 6 月がサイバー空間をめぐる戦いの「イヤー・ゼロ（Year Zero）」だとしている（Segal 2016）。ジェイソン・ヒーリー（Jason Healey）はサイバー空間の歴史を自覚期（1990 年~1997 年）、発展期（1998 年~2002 年）そして軍事化期（2002 年~現在）という 3 つに分類し、サイバー空間の軍事化は 2002 年から本格化しているとしている（Healey 2013）。ここではサイバーセキュリティ戦略の記述に依って 2010 年という立場を取るが、それ以前からサイバー空間での軍事作戦の準備が進められてきたという見解を否定するものではない。

125 スタックスネットはコンピュータウイルスの名前でもある。イランのナタンツにあるウラン濃縮施設で使用されている遠心分離機を破壊するために極めて高度なサイバー攻撃作戦が実施された（Zetter 2014）。

ュリティ対処能力強化の正当性と重要性を強調した。この中でサイバー攻撃能力について「(大統領からの命令あらば)、国防総省はサイバー作戦を用いて、敵方の指揮通信ネットワーク、軍事関連の重要インフラ、および兵器使用能力を混乱させる能力を持つべきであり、そのための準備を進める」とある。2011 年の国際戦略との比較においてサイバー攻撃実施の可能性がより具体的に記述されている。

2010 年以前、公に言及される機会がなかった国家のサイバー攻撃能力は、2011 年以降、段階的にその「保持」が表現の手段を変えて明言されるようになった。冒頭で紹介した 2016 年に公開されたオーストラリアと英国のサイバーセキュリティ戦略には「保持」からさらに一歩進んでサイバー攻撃能力の「使用」を強く想起させるものとなっている。今後これに倣って、他の国がサイバー攻撃能力についてアピールすることが予想される。

パートナーシップ政策の相違

分析の対象とした 8 カ国中、フランスとドイツを除く 6 カ国がサイバーセキュリティについて自国が重視する国際機関や会議体を列挙している。6 カ国のすべてが名指しで重要としているのが国連である。とりわけ総会決議によって招集される国連政府専門家会合（GGE）[126]については法の支配を議論する場として期待が高いことがわかった。中国は「国連の主導を支持し、各方面が普遍的に受け入れられる、サイバー空間国際規

[126] サイバーセキュリティの専門家の間では「サイバーGGE」あるいは単に「政府専門家会合」と呼ばれているが、正式な名称は「国際安全保障の文脈における情報とテレコミュニケーションの開発（Developments in the Field of Information and Telecommunications in the Context of International Security）に関する国連政府専門家会合」である。国家のサイバー空間における攻撃を規制するために、国連憲章を含む既存の国際法がサイバー空間に適用されるのか否か、新しいルールや国際法を打ち立てるべきかなどについて議論が行われてきた。2004 年から執筆時点までで 5 回招集されている。2016-2017 年会合は日本を含む 25 カ国が参加し、既存国際法がいかにサイバー空間に適用されるかについて意見が対立し、合意文書を残すこと無く解散した。執筆時点で第 6 回会合（会期 2019-2020 年）の開催が決定している（United Nations 2018）。これまでの GGE 報告書に含まれる提言を前進させるための議論を行い、2021 年第 76 回国連総会に報告書を提出することが求められている。議長はブラジルのパトリオッタ軍縮代表部大使に決定した。

範、サイバー空間国際反テロ公約の制定を推進し、サイバー犯罪を打撃する司法協力メカニズムを整備する」と国連によるサイバー空間のガバナンスを明確に望んでいる。ロシアと中国は 2011 年に「情報セキュリティに関する国際行動規範」[127]という文書を提案し、サイバー空間国際規範の国連総会での議論を求めた。両国らの提案した規範は国家による情報空間での主権管轄（国家によるサイバー空間における主権と領土の保全）、サイバー兵器や関連技術の規制、サイバー空間における資源の公平な配分などを認めるという内容であった。とりわけ「主権国家は情報空間の管理に同等の権利と責任を有する」という原則は、現在のサイバー空間に大きな影響力を持つ米国[128]および国内に大規模な情報通信産業事業者を有する西側先進国にとっては受け入れがたいものであったと考えられる。ロシアと中国は 2015 年にも同様の提案を行っているが、いずれも総会で議論されることはなかった。

国連に次いで重要と考えられるのが、6 カ国の戦略で重要性が指摘される G20 である。G7 に言及した国が 3 カ国であったことを考えると、東西の主要国が集う G20 の交渉の場としての価値が広く認められていると考えられる。2017 年 3 月に開催された G20 財務大臣・中央銀行総裁会議の成果文書に「情報通信技術（ICT）の悪意のある利用は、各国及び国際金融システムにとって極めて重要である金融サービスを混乱させ、セキュリティと信頼を損ない、金融安定を脅かしうる」（財務省 2017）とあることからも、G20

---

127 情報セキュリティに関する国際行動規範は 2011 年に中国、ロシア、タジキスタン、ウズベキスタンの 4 カ国によって共同提案されたが、事務総長はこの提案を総会の議案に追加しなかった。その後 2015 年には前述 4 カ国にキルギスタンとカザフスタンが加わり 6 カ国の共同提案という形で再度提案されたが、またしても不調に終わった。情報通信技術、ネットワーク技術を「敵対的行為や侵略行為」あるいは「国際平和と安全保障の妨げとなる行為、情報兵器や関連技術の拡散」を目的として利用することを禁ずるという提案である。

128 インターネットにおける重要な資源（IP アドレスやドメイン名）については IANA（Internet Assigned Numbers Authority）という組織が管理を担っている。この IANA 機能を監督する権限は歴史的な経緯から米国商務省が持っていた。2016 年からこの IANA 機能の監督権限はマルチステークホルダーコミュニティに移管されている。米国政府の直接的影響力は弱まる。

の枠組みの中で継続して議論が行われている。

多様な重要インフラの定義

重要インフラの保護の重要性については疑問の余地がないものの、保護する対象となる産業分野に国毎の考え方の違いが現れる。例えば、日本は「情報通信、金融、航空、鉄道、電力、ガス、政府・行政サービス（地方公共団体を含む）、医療、水道、物流、化学、クレジット及び石油の 13 分野」を重要インフラとして定義している。多くの国で金融は重要インフラとして名前が挙がるが、クレジットを重要インフラとして指定しているのは日本だけである[129]。それに対して中国における重要インフラの定義[130]は「公共通信、テレビ放送の伝送等サービスのインフラ情報ネットワーク、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、公共事業等の国家機関の重要情報システム、重要なインターネットアプリケーションシステム等（これらを含み、これらに限らない）」である。水利が重要インフラに含まれるのは、治水が伝統的な政治課題であった中国らしいといえる。ドイツは食糧産業を重要インフラに含めているという特色がある。食糧、クレジット、治水などを重要インフラと定義する背景にはそれぞれの産業分野が各国固有の事情からサイバーセキュリティ対策の重要性が特に高いことがある。

重要インフラ保護政策の課題の 1 つとしてセキュリティ問題が発生した際の生活への影響が大きいクラウドホスティングサービス、電子メールサービス、チャットサービス、ニュースなどを提供する新興の IT 企業が重要インフラに指定されていない点が挙げられる。英国と中国の戦略からこの課題解決への努力がみられる。英国のサイバーセ

---

129 日本以外の国ではクレジットにおける金融取引は金融分野に含まれているが、日本では経済産業省の所轄とされているので、クレジットが別立てになっている。

130 中国における重要インフラ保護の対象となる産業分野については前掲の『国家網絡空間安全戦略』に加えて 2016 年に成立した『網絡安全法（いわゆるサイバーセキュリティ法）』内の記述を参考にしている。

キュリティ戦略では、政府が直接関与し、重要ネットワーク企業（Critical Network Infrastructure、以後 CNI）を重点的に防衛するとした。CNI の例として「大量の個人情報を保有する企業、メディアなど攻撃者に狙われやすい企業、オンライン小売企業など」があるという。中国も重要インフラに「重要なインターネットアプリケーションシステム」を含めた。検索サービスを提供する百度（バイドゥ）、オンラインマーケットサービスを提供するアリババ・グループなどの企業が保護の対象となる可能性がある。公的機関、重厚長大産業の保護を優先してきた重要インフラ保護政策が、個人情報保護や国民生活への影響度を元に再考されていく潮流が各国のサイバーセキュリティ戦略から読み取れた。

マーケット・アプローチへの期待と失望

サイバーセキュリティ戦略に民間事業者の役割に関する記述は多くなかったが、官民連携（Public-Private Partnership）については、基本的な価値観や安全保障上の課題を共有する英国とオーストラリアのサイバーセキュリティ戦略が対照的な方針をとっていることがわかった。

オーストラリアは首相と民間企業トップとの年次会合実施などを通じて官民の連携を強化するだけでなく、民間主導サイバーセキュリティ成長センター（Industry-led Cyber Security Growth Centre、2015 年設立）に 3000 万豪ドル（約 27 億円）以上を出資し、国内サイバーセキュリティ産業の拡充を目指す。国内サイバーセキュリティ市場の活性化がオーストラリア全体の対策推進に寄与するというマーケット・アプローチの考え方をとっている。

英国は過去のサイバーセキュリティ戦略でマーケット・アプローチを重視していた。2016 年版の英国のサイバーセキュリティ戦略は 2011 年から 2015 年の 5 年間に 8 億 6 千万ポンド（約 1259 億円）を投じた過去のサイバーセキュリティ戦略の元での施策を振り返って、「英国のサイバーセキュリティ産業を活性化し、その結果として国全体の

セキュリティ能力の向上をはかるマーケット・アプローチは充分な成果を出すことができなかった」と結論づける。その上で政府、特にインテリジェンス機関がより直接的に関与する必要があることを強調する。

政策ツールとしての自由度の高さ

本節を通じて、各国のサイバーセキュリティ戦略は極めて自由度の高い政策ツールであることが確認された。どの国のサイバーセキュリティ戦略も法律ではないため立法府における検討を経ていない。「自国が望むサイバー空間のありかたを国際社会に対して明らかにすることを目的とした宣言政策型」の記述が含まれることはすべてのサイバーセキュリティ戦略に共通して見られたが、それ以外の共通項を見出すことはできなかった。

まず戦略を策定した省庁、あるいは公布を行っている省庁が多様である。大まかには以下の 3 つのパターンに分けて考えることができる。第一に、ホワイトハウス（米国）、首相府（オーストラリア）のように国家元首を直接に補佐する組織が主となるパターンである。第二に、国家サイバーセキュリティセンター（英国）、内閣サイバーセキュリティセンター（日本）のようにサイバーセキュリティに関する各省間の政策の集約を担う組織が主となって策定、公布するパターンである。第三に、外務省（ロシア）、連邦情報技術安全局（ドイツ）などのような個別の省庁が公布するパターンである。背景にはサイバーセキュリティが、外交・防衛・警察・司法・通信・経済・科学技術政策などに幅広く影響を及ぼす分野であることが考えられる。

サイバーセキュリティ戦略の政府文書体系における位置づけも異なる。フランス、英国のサイバーセキュリティ戦略はそれぞれフランスが「防衛と国家安全保障白書」、英国が「英国家安全保障戦略（2015）」をサイバーセキュリティ戦略の上位文書として位置付けている。他方でドイツ、ロシアなどのサイバーセキュリティ戦略は位置付けを示唆する記述がなく、文書の重要性が不明瞭である。さらに中国の『サイバー空間国際合

作戦略』、日本の『サイバーセキュリティ国際連携取組方針』のようにサイバーセキュリティ戦略全体における国際戦略に限定したいわばサイバーセキュリティ政策の下位文書も存在する。真の戦略把握の観点からはサイバーセキュリティ戦略という名前の単一の文書にとらわれず、安全保障戦略、防衛白書、国際連携の指針そして関連法規までを視野に入れた「サイバーセキュリティ戦略文書群」として分析することが必要である。

本節でこれまで述べてきたサイバーセキュリティ戦略の自由度の高さは、同時にそこに記述された政策が実際に履行されるかの予測を困難にさせる。多くのサイバーセキュリティ戦略は戦略自体の有効期限が決められておらず、個別の政策についていつまでにそれを達成するかのタイムラインが示されない。予算措置まで記述されることは稀である[131]。他方で、サイバーセキュリティ戦略は各国の政府が目指す姿を、制約を無視して、表現するためのツールとして重要なものであるともいえる。

第３項 四類型による分析

8 カ国のサイバーセキュリティ戦略の調査から質的な差異を踏まえた上で、サイバーセキュリティ戦略の多様性を生み出す要因の 1 つとして、想定される文書の読者に着目し政府内調整型、国内政治型、宣言政策型、懲罰抑止型の 4 つの類型に分類することを試みた。それぞれ以下に解説する。

政府内における組織の役割を明確化するための「政府内調整型」

本来国内外に向けてサイバーセキュリティ政策を打ち出すことがサイバーセキュリティ戦略の本来の役割であるところ、政府内での役割分担に言及するものがこれにあたる。外務省における取り組み、外務省の国際交渉の指針を細かく記述したロシアのサイバーセキュリティ戦略が代表的なものとして挙げられる。

---

131 オーストラリアと英国のサイバーセキュリティ戦略においては一部、記述された政策の実施に必要な予算の確保を約束している。

各政府機関に分散したサイバーセキュリティ対応能力をサイバーセキュリティセンターに集約・統合することを打ち出したオーストラリアのサイバーセキュリティ戦略、2020 年の東京オリンピック・パラリンピック競技大会に向けオリンピック・パラリンピック CSIRT を政府内に新設することを打ち出した日本のサイバーセキュリティ戦略、有事の際には内務省長官が率いる危機管理対応チームに報告を行う国家サイバーレスポンスセンターを連邦情報技術局の下に設置し情報の集約と分析をはかるとしたドイツのサイバーセキュリティ戦略も同様に「政府内調整型」の代表例である。

政府内での各組織の役割が不明確な部分を、対外的にサイバーセキュリティ戦略の形で公開することにより規定していく狙いがある。

自国内における官民の役割の明確化などを目的とした「国内政治型」

自国内の民間企業、学術研究機関、地方政府などの役割分担に言及するものがこれにあたる。大学含む高等教育機関や、民間業界団体によるサイバーセキュリティ情報共有の強化を打ち出したフランスのサイバーセキュリティ戦略が代表的なものとして挙げられる。

国内の様々な利害関係者に対して指針を示し、重点課題への協力を求める狙いがあると考えられる。サイバー空間を構成する要素の多くは民間事業者が所有あるいは管理していることから、そのセキュリティ対策についても民間に役割と責任を与えるという考え方は論理的である。既存分野の安全保障戦略との対比において、政府以外の役割が重要なサイバー空間の特徴がサイバーセキュリティ戦略に現れているともいえる。

自国が望むサイバー空間のありかたを国際社会に対して明らかにすることを目的とした「宣言政策型」

自国のサイバー空間に対しての基本的な原則を主として国外に向けて示すことを目的とするものがこれにあたる。今回分析対象としたすべての戦略に宣言政策型の記述がある。特にロシアのサイバーセキュリティ戦略は全体として「国内政治型」の記述がほ

とんどない、最も典型的な「宣言政策型」といえる。

サイバーセキュリティ戦略の多くが「宣言政策型」の記述を多く含む理由の 1 つとしては、サイバー空間に明示的な管理者が存在せず、自国の立場を直接的に訴える相手がいないことが挙げられる。国家は自国の利益を最大化するサイバー空間のあり方について国内外に理解を促していくことが必要なのであろう。

「宣言政策型」戦略はサイバー空間における信頼醸成の観点からも重要である。信頼醸成とは透明性を相互に確保し、危機発生時の過激化（エスカレーション）を防ぐための手段である。キューバミサイル危機に際して、当時のソ連と米国の指導者を結ぶホットラインが設置されたことなどが信頼醸成措置の例として挙げられる。この分野の議論をリードする欧州安全保障協力機構は 2013 年に「欧州安全保障協力機構 1106 号 サイバー空間における信頼醸成のための初期セット」（OSCE 2013）を全会一致で決定した。この決定の中ではサイバー空間やサイバー戦争に関する各国のスタンスを公開し、相互理解をすすめることが求められている。このような地域安全保障機構からの要求を受け、今後も多くのサイバーセキュリティ戦略が「宣言政策型」の側面をもつことが予想される。

報復サイバー攻撃の存在を明らかにする「懲罰抑止型」

「宣言政策型」の派生として「懲罰抑止型」を 4 つ目の類型として指摘したい。他国からのサイバー攻撃の増加を背景に、サイバー攻撃能力の強化や先制攻撃を受けた際の報復措置について記述するサイバーセキュリティ戦略である。「攻撃的サイバー能力について世界のリーダーの地位を目指す」という英国や「抑止のためにサイバー攻撃能力を使用する」とするオーストラリアのサイバーセキュリティ戦略がこれにあたる。サイバーセキュリティ戦略において明確にサイバー攻撃能力を保持することを認め、それを

使用する可能性に言及したのは英国のサイバーセキュリティ戦略が初めてである[132]。

「抑止とは恐怖を通じて相手を思いとどまらせること」（ナイ&ウェルチ 2013: 174）だとすれば、今後サイバーセキュリティ戦略にはさらなる抑止効果を得るためにより強いメッセージが並ぶ可能性がある。英国と、それに続いたオーストラリアのサイバーセキュリティ戦略が他国にどのような影響をもたらすのかは継続的な検証を要する。

ここまでで見てきたサイバーセキュリティ戦略はその多くが、上記 4 類型の複数の型にあてはまるものであった。各サイバーセキュリティ戦略について、記述に占める「政府内調整型」「国内政治型」「宣言政策型」「懲罰抑止型」それぞれの割合を調査することによって、その性質を定量的に評価できる。

第 4 項 国家サイバーセキュリティ戦略の価値

サイバーセキュリティ戦略はなぜ策定されるのか。それによって各国政府はどのような課題を解決しようと試みているのであろうか。

本節では想定読者という糸口からそれらが 4 つに分類されることを示した。つまり、政府内を意識した「政府内調整型」、政府と民間を合わせた国内関係者を意識した「国内政治型」、一国を超えて国際社会を意識した「宣言政策型」、そして、潜在敵国を意識した「懲罰抑止型」である。それらは対象範囲に広さという点では、政府内調整型＜国内政治型＜懲罰抑止型＜宣言政策型、であるともいえるだろう。

---

132 例えば前掲の米国 Cyberspace Policy Review では能動的サイバー防御（Active Defense）能力の強化が謳われていた。米国防総省のサイバーセキュリティ戦略もサイバー攻撃能力強化の必要性を訴えている。したがってサイバー攻撃能力の使用を仄めかすことは 2016 年より前にも存在した。しかし、能動的サイバー防御とサイバー攻撃能力では周辺国に与える印象が異なり、「サイバー攻撃能力世界一を目指す」という直接的なメッセージの周囲への影響も加味して、ここでは英国のサイバーセキュリティ戦略が初めての「懲罰抑止型」というスタンスをとった。

しかし、同じ「サイバーセキュリティ戦略」あるいは同様の表現で提示される文書において、想定されている読者が違うということは何を意味するのだろうか。国際条約に基づいた各国における国内措置のための法整備などとは違い、サイバーセキュリティ戦略では必ず盛り込むべき内容が固定されているわけではない。法律や条約ではないため、立法府の承認を得る必要性もない。サイバーセキュリティ戦略は、その名のもとに国内外に対して自国政府の主張を比較的自由に表現できる手段になっている。

それぞれの読者層が示すのは、どこまで政府ないし国内において調整が済んでいるか、そして、被害の範囲・深刻度が関係しているといえる。つまり、サイバーセキュリティをめぐる問題が深刻度を増しているにもかかわらず、政府内での意識統一ができていないため、それを促す手段してサイバーセキュリティ戦略が使われる場合、それは政府内調整型にならざるをえない。

政府内での調整がある程度済んでいるものの、国内における民間との調整が十分でない場合には、それを促す国内調整型になる。重要インフラの多くは民間事業者が保有するものである。本節で取り上げた多くの国は情報拡散国家（リベラル民主主義国家）であり、そうした国では平時から軍が直接的に民間事業者を防衛するという体制を取りにくい。そのため、いかにして民間の意識を高め、設備やシステムの防衛のためにコストを負担させるかという点が政策課題になる。利益追求を求められる企業にとって、サイバーセキュリティはコストとしてしか認識されない。そうではなく、より大きな被害を防止するための投資だと認識させることが重要になる。そうした認識変化を促すためにサイバーセキュリティ戦略が使われることもある。

また、すでに多くのサイバー犯罪、サイバーエスピオナージ（スパイ活動）、サイバー攻撃の被害に遭っている国は、その抑制・抑止が政策上、重要な課題になっている。具体的な攻撃者ないし攻撃国が見えている場合には、そうしたアクターに対しど

のような対応を取るかを明確にするために懲罰抑止型が用いられることになるだろう。

しかし、そうした具体的な被害が多くないものの、潜在的なそれが予期されており、それに備えることを目的としてサイバーセキュリティ戦略が使われる場合には宣言政策型になるだろう。

つまり、その国のサイバーセキュリティ戦略がどの型になっているかを分析することで、その国のサイバーセキュリティの状況、そして課題が見えてくることになる。それは当然ながら、その国が置かれている状況が変われば、サイバーセキュリティ戦略の内容が変わるということを意味する。

第３節　サイバー空間に関する国際合意

第１項 はじめに

前節までの主要国の戦略の分析を通して、サイバー空間における個別のアクターの戦略や関心に迫ってきた。本節では、個別のアクターではなく、すでにあるサイバー空間をめぐる国際的な合意について分析を試みる。

１つの国がコントロールできる枠を超えた社会的な課題について、国際社会は合意を条約という形で文書化してきた。例を挙げれば、1945 年に調印された国連憲章には大戦を防ぐという大義が、市民的及び政治的権利に関する国際規約（ICCPR）には個人の市民的・政治的権利を尊重し確保するという大義があった。多くの国家がその大義の価値を認め、細部には様々な不満を抱えつつも、条約に批准してきた。既存の条約がたびたび反故にされたことを、殊更にとりあげ、その価値が無いと論ずるのは一面的な批評である。条約は国際社会における国家の望ましい振る舞いを決める。したがって条約は、ある分野における、国家の行動の予測可能性を高める。予測可能性は国際社会に安定を

もたらしてきた。サイバー空間を統治する国際法体系を望む声は強まっている。

サイバー空間を統治する国際法体系の実現は大きく 2 つの異なるアプローチが考えられる。1 つめはサイバー問題を扱う新たな条約を打ち立てることである。新たな条約の必要性や効果は広く理解されている。問題はサイバー空間の歴史が浅く、主要国家間に条約やグローバルな行動指針の土台となる現状認識にも乖離があることである。例えば、国際社会は、我々が面している問題が「サイバーセキュリティ」なのか「情報セキュリティ」なのか合意できない。条約を検討するにあたり、その名前は「情報セキュリティ条約」なのか「サイバーセキュリティ条約」なのかという点だけをとっても、リベラルな情報拡散国家と情報支配国家の間には埋めがたい溝がある。溝が、単に修辞上の問題ではない、根本的なサイバー空間に対する国家のリスク評価に起因するからである。

もう 1 つのアプローチは既存の国際法をもってサイバー空間を統治するというものである。例えば、国連憲章の第 1 章の第 2 条第 4 項は「すべての加盟国は、その国際関係において、武力による威嚇又は武力の行使を、いかなる国の領土保全又は政治的独立に対するものも、また、国際連合の目的と両立しない他のいかなる方法によるものも慎まなければならない」としている（国連広報センター 2019）。国際憲章は、一部の例外を除いて、武力行使を禁じている。であるならば、武力行使にサイバー攻撃が含まれるという追加の合意ができれば、サイバー攻撃を抑制できるはずである。どのようなサイバー攻撃を国連憲章が定める武力行使とみなされるのかはタリン・マニュアルにおいても大きな論点であった。検討は現在も継続している。何れにせよ以上の状況から、近い将来、単一の国際的合意によりサイバー空間が統治される可能性は低いということが言えそうである。

そこで本節では、複数の国際的な合意に注目する。現代のサイバー空間を支配する単一のルールは存在しない。多様なアクターが議論を行い、様々なアイデアが提案され、一部は効力を持ち出している。議論の場は拡散を続け、全体的な流れが見失われつつあ

る。拡散し続ける議論における、既存の合意の内容を概覧し、国際社会がどこまで合意しているのかを明らかにするというのが、本節が挑む課題である。

本節で分析の対象とする合意の定義は HorenBeeck（2019: 11）に従った。すなわち①達成目標が明確で、②国際的に賛同を得ていて[133]、③特定のグループへの約束や推奨事項を含むものという 3 つの条件を満たすものである。サイバー空間の合意については文書化されていないもの、文書化されていても公表されていないものが一定数存在することもわかった。ここでは一般公開されている合意のみを扱う。また、様々な会議の共同声明などは、もちろん国際的な賛同を得ているが、達成目標が不明確なものが少なくない。したがってそのようなものは本項において合意として扱っていない。

以下の図表 5-2 はそれらを満たす国際合意である。

カテゴリ	合意の名称	主体	成立年
グループ内合意	Charlevoix commitment on defending Democracy from foreign threats	G7	2018
	テックアコード（Cybersecurity Tech Accord）	マイクロソフト中心とする民間企業	2018
	Recommendations for Human Rights Based Approaches to Cyber security	フリーダムオンラインコーリション	2015
	Agreement on cooperation in the field of ensuring the international information security（エカテリンブルグ合意）	上海協力機構	2009
	Convention on Cyber Security and Personal Data Protection	アフリカ連合	2014[134]
	Convention on Combating Information Technology Offences	アラブ連盟	2010

[133] 国際的に合意を得ているというのは、3 カ国以上で認知されていることを条件にした。したがって、例えば 2015 年の米中合意のように 2 国間（バイラテラル）合意は、本論文において、国際合意に含まれない。

[134] Convention on Cyber Security and Personal Protection は条約であり、2014 年に採択され、その後徐々に締約国を増やしている。ここでは初出の時期を成立年として用いた。

	サイバー犯罪条約[135]	欧州評議会	2004
	EAC Framework for Cyberlaws	東アフリカ共同体	2008
	西アフリカ指令（Directive C/DIR. 1/08/11）	西アフリカ諸国経済共同体	2011
	NIS 指令（NIS Directive）	欧州連合	2016
	Cyber Defence Pledge	NATO	2016
	Joint Communication: Resilience, Deterrence and Defence: Building strong cybersecurity for the EU	欧州連合	2017
	Mutually Agreed Norms for Routing Security	MANRS	2014
グループ間合意	パリ・コール（Paris Call）	フランス政府、マイクロソフト他	2018
	チャーター・オブ・トラスト（Charter of Trust）	シーメンス社（ドイツ）他	
	GCSC 規範	GCSC	2017-2019
	アンタルヤサミットコミュニケ	G20	2015
	クライストチャーチコール	ニュージーランド政府、マイクロソフト他	2019
国連での合意[136]	政府専門家会合報告書（2015 consensus report of the UNGGE）	政府専門家会合	2015

図表　5-2 既存の国際合意

第２項 合意の主体

ここでは合意の主体に着目して 3 つに分類していく。1 つはグループ内合意である。

---

135 サイバー犯罪条約は主に中国やロシアから「欧州という地域における合意であり、グローバルな合意ではない」という批判を受けていた。2019 年秋、ロシアは国連の第 3 委員会において、国連においてサイバー犯罪条約相当の条約に向けた議論を開始することを提案した。欧米諸国や日本が反対票を投じたが、賛成 88 票、反対 58 票、棄権 34 票でこの提案は可決した（United Nations 2019）。今後、実際に条約に向けた議論が開始されるのか、本論執筆時点では見通しは不透明である。

136 国連においては政府専門家会合（GGE）の他に、「サイバーセキュリティに関するオープンエンデッドワーキンググループ（OEWG）」という会議も行われている。OEWG は第 73 回の総会決議に基づき、国連に加盟するすべての国が参加可能な会議である（メンデレー A/RES/73/27）。20 数カ国に限定している GGE と違い、国連での交渉プロセスをより包括的にする狙いがある。市民社会や企業からの意見陳述の機会を設けるなどよりオープンな議論を標榜する。2020 年の 75 回総会に報告書を提出する。議長はスイスのラウバー国連軍縮部常駐代表が務める。

本論文の第２章にも示したとおり、サイバーセキュリティのガバナンスの主たるアクターは情報拡散国家、情報支配国家、グローバルテックカンパニーの 3 者であるという前提に立ち、この 3 つのグループのいずれかの内部での合意をグループ内合意とした。例えば、G7 の成果文書は情報拡散国家の間での合意であり、上海協力機構における合意は情報支配国家の間での合意であり、テックアコードはグローバルテックカンパニーの間での合意である。グループ内合意は、立場の似通ったものの間での合意であり、比較的合意に達するのが容易である。

2 つめはグループ間合意である。情報拡散国家、情報支配国家、グローバルテックカンパニーの 3 者のうち 2 つ以上が合意しているものを指す。G20 のアンタルヤサミットコミュニケは G20 の参加国（ロシア、中国、サウジアラビア、トルコ）も議論に関与しており、これは情報拡散国家と情報支配国家という 2 つのグループにまたがる合意といえる。パリ・コールは現時点で唯一の情報拡散国家、情報支配国家、グローバルテックカンパニーすべてが賛同者として名を連ねるものである。

グループ間合意はグループ内合意よりも実現するのが難しい。サイバー空間に、法の支配や、ルールの支配をもたらそうとするのであればグループ間合意を、特に 3 つのグループすべてが参加する合意を目指すべきであろう。

最後に 3 つ目は国連の下での合意である。サイバー空間のガバナンスに国連がどこまで関与すべきかは、現時点でも不明瞭である。しかし、サイバー空間のセキュリティに関して言えば、国連への期待の声は高まっている。陸海空宇宙のセキュリティについて国連には安全保障理事会という議論の場がある。同様にサイバー空間の安全保障についても国連がより中心的な役割を果たすべきという声は、情報支配国家や途上国から根強い。アントニオ・グテーレス（Antonio Guterres）国連事務総長が諮問委員会を設置した

のもそのような期待の声を受けてのものだった[137]。

現時点で国連の下での明確な合意としては 2015 年の政府専門家会合の報告が挙げられる（United Nations 2015a）。これは形式としては情報拡散国家と情報支配国家の間での合意にすぎないが、以降今日に至るまで重要なマイルストーンとして、繰り返し参照されてきた。本論文では国連での合意を、グループ間合意に含まれるとはいえ、より影響力の大きい合意とみなす。ただし国連でのサイバー空間に関する議論は様々なレベルで行われている。格別に影響力が大きいのは安全保障理事会や第一委員会という安全保障を論じる場での議論である。ITU などの専門機関、UNIDIR などの研究機関はこれに該当しない。

第 3 項 合意内容の考察

これらの国際合意は相互に何を確認しているのだろうか。それらを比較して眺めると国際的合意の要所を 4 つ指摘できる。

罰則のない合意

サイバー空間における合意を、拘束力を持つか否かで、分類することは難しい。合意文書に文書自体が拘束力を持つ（Binding）と書かれていたとしても、実際の内容について自発的な（voluntary）取り組みを求めているなどのケースがある（OSCE 2013）。それでは合意を守らなかった場合になんらかのペナルティが課されるのか。本節でとりあげた合意はいずれも罰則がなく、合意の当事者間における協力を促すものであった。

しかし、この点をして、これらの合意が無意味であると捉えるのは正しくない。罰則

[137] 正式名称は、国連事務総長のためのデジタル協力に関するハイレベルパネル（Secretary-General’s High-level Panel on Digital Cooperation）である。事務総長の諮問に応じて 2018 年春に招集された。共同議長がジャック・マーとメリンダ・ゲイツであることが話題を呼んだ。サイバーセキュリティに限らず、デジタル全般についての賢人会議である。2019 年に報告書を事務総長に提出した。

がなくとも、一部の合意は政治的な拘束力を生んでいる。

マルチステークホルダーへの態度

サイバーセキュリティを確保し、サイバー空間を統治することが重要であるが、果たしてその責務を負うのは誰なのか。ほぼすべての合意において、それは「官民市民社会含むすべての利害関係者」としている。いわゆるマルチステークホルダリズムが、多くのサイバーセキュリティの合意に共有されていることが確認できた。分析対象の合意の中で、西アフリカ指令、上海協力機構の 2 つのみがマルチステークホルダーに言及しない。サイバーセキュリティ対策は政府の責任であり、政府が主導するということを間接的に訴えている。

サイバー空間への国際法の適用

サイバー空間に既存の国際法がどのように適応されるかは、特に情報拡散国家と情報支配国家の間の立場の違いが明確な点である。国際合意を時系列に沿って振り返れば、2015 年を境に議論の内容が変わったことがわかる。

2015 年より前における、情報支配国家の基本的な立場は、サイバー空間は新たな空間であり、新しい法・制度が必要というものであった。また情報拡散国家においても、サイバー空間は国家の主権の及ばないコモンズという考え方が残っており、既存の国際法をサイバー空間に適用することについて足並みが乱れていた。この不明瞭さを解消したのが 2015 年の国連政府専門家会合での議論であり、その報告書である。政府専門家会合でサイバー空間への既存の国際法の適用が確認された。しかし、それ以降も不透明さが残っている。その理由は主に 2 つ指摘できる。

1 つめの理由は「既存の国際法のサイバー空間への適用」という言葉は極めて高度な解釈の能力を必要とする、曖昧な言葉であることだ。国家の権利や責任はサイバー空間にそのまま「キャリーオーバー」されるのか否か、専門家の間でも意見がわかれた（Buchanan 2017: 2507–8）。

2 つめの理由は、国家はある国際法の適用を受け入れた上で、個別のケースについて適用が除外されることを主張することが度々ある。例えば、米国はキューバに位置するグアンタナモ湾収容キャンプでの収容者の取扱について国際社会から非難を受けた。被拘束者の権利を保証する「市民的及び政治的権利に関する国際規約」の締約国である米国がそれを犯しているという非難である。しかし、グアンタナモの米軍施設はキューバの法も、米国の方も及ばない治外法権であり、したがって同国際規約が適用されないという主張を行った。詭弁にも聞こえるが、これは法を背景とした主張としては一定の説得力を持つ。

どの国際法が、どのようなケースで適用されるのか、国際社会は引き続き議論による相互理解を深めていく必要がある。サイバー空間のガバナンスをめぐる争点は、サイバー空間への国際法の適用ではなく、どの国際法がどのように適用されるかに移った。この移り変わりを反映している例として興味深いのはパリ・コールである。2018 年に多くの情報拡散国家と情報支配国家とグローバルテックカンパニーが賛同したこの合意では国連憲章と国際人道法がサイバー空間に適用されることが明記された。

人権

サイバー空間における表現の自由を含む人権の確保は、それぞれの国際合意の中で扱いが大きく分かれるポイントである。アフリカ連合はサイバー空間における人権確保を目的に掲げ、上海協力機構は「基本的な人権・市民権と自由を確保する手段としての情報セキュリティ」と、やはり人権への配慮を見せる。また EU や国連での合意も同様にサイバー空間の発展が、既存の人権を侵すことへの牽制の文章が入る。一方で、グローバルテックカンパニーが推進する 3 つの合意（テックアコード、GCSC、チャーター・オブ・トラスト）は人権に言及しない。人権という軸からは、国民を代表する主権国家とグローバルテックカンパニーの間に溝があると表現することもできる。つまりグローバ

ルテックカンパニーがこれまで人権に対して概ね冷淡であり[138]、それと比較すると、情報支配国家と情報拡散国家の二者は、少なくとも見かけ上は、スタンスが一致している。

コンテンツ制限

サイバー空間の上で我々がやり取りする情報の流通を制限することは、最低限に留めるべきというスタンスは多くの国際合意に共通している。では、どういう場合に表現の自由を毀損しても検閲や制限を加えるべきなのだろう。児童ポルノ、人種差別の 2 つは複数の合意に共通のインターネット上から駆逐すべき対象である。この 2 つを排除することについて国際社会に議論の余地はあまりない。

グローバルテックカンパニーのルールを形成する力は今後ますます強まると考えられるが、彼らが真にサイバー空間の統治者となるのであれば、人権やコンテンツ制限といった商業的利益を産まない社会課題に対して、主権国家を超える説得力のある策を示すことが求められる。その意味においてライツコン（RightsCon）のような、グローバルテックカンパニーが一同に会し、ICT と人権を論ずる場の動きが、今後のサイバーセキュリティガバナンスにおいて極めて重要になっていく。

第 4 節　サイバー空間安定化委員会

第 5 章第 2 節「主要国家のサイバーセキュリティ戦略」と第 3 節「サイバー空間に関

---

138 グローバルテックカンパニーが、自らのビジネスと基本的人権の確保の両立を目指すように変化しているのは重要な変化である。グーグル社の「邪悪になるな（Don’t be evil.）」はその背景に人権やその他社会の良識を保護する責任を従業員に植え付けるものとも言える。加えて、マイクロソフト社の幹部はテクノロジー業界には世界の変革に責任を持つという態度、強大な力を扱っているが故の倫理教育の重要性を訴える（Brad & Ann Browne 2019: 206）。旧東ドイツで秘密警察が政治活動を弾圧した例を引き合いに、国家が基本的人権の抑圧をする場合に、テックカンパニーはそれに立ち向かわなければいけないという。それは、テックカンパニーが国家による基本的人権の侵害から市民を守るという構図を意識したものである。

する国際合意」を通して、様々なアクターによるサイバー空間をめぐる戦略を合意の内容からさかのぼって検討してきた。この分析手法はしかし、完成した料理から、調理に使われた材料を推察するような作業である。誤った解釈をする可能性を排除できない。ここでは、サイバー空間における規範や国際合意の 1 つであるサイバー空間安定化委員会（GCSC）の活動に参加し、参与観察を行うことにより、合意の形成過程についてミクロの分析を加えていく。

第 1 項 体制と資金

GCSC の活動の目的は、Web サイトによると「国際サイバーセキュリティについて官民の枠をこえた議論を行い、セキュアで安定したサイバー空間のためのルールづくりを補佐すること」である。委員会は議長の元エストニア外相マリーナ・カリュランド（Marina Kaljurand）がリードした。そして 2 人の共同副議長すなわち元米国国土安全保障省長官マイク・チャートフ（Michael Chertoff）と元インド国家安全保障副アドバイザーのラタ・レディ（Latha Reddy）が、カリュランドを支えた。委員はサイバーセキュリティの分野に深い知見を持つ個人を地域、人種などのバランスを考慮して選ばれた。議長と共同副議長を含めて 30 名弱の委員が名を連ねた。その顔ぶれは以下のとおりである（2019 年 9 月時点）。

氏名	**主たる経歴**
マリーナ・カリュランド（議長）	元エストニア外相
マイク・チャートフ（共同副議長）	元米国国土安全保障省長官
ラタ・レディ（共同副議長）	元インド国家安全保障副アドバイザー
アイザック・ベンーイズラエル	テルアビブ大学教授
アブドゥル・ハキーム・アリオリ	OIC-CERT
アンリエッテ・ エスターハイゼン	Association for Progressive Communications
イリヤ・サチコフ	Group-IB 社

ウーリ・ローゼンタール	元オランダ外相、元 GCCS 特使
ウルフギャング・クラインワッター	Net Mundial 発起人
エリナ・ノール	アジア太平洋安全保障研究センター准教授、元 ISIS マレーシア
オラフ・コルマン	ISOC[139]理事
カール・ビルド	元スウェーデン首相
クリス・ペインター	前米国務省サイバーセキュリティ調整官
クー・ブーン・フイ	元シンガポール内務省副大臣、元インターポール総裁
サミール・サラン	インドシンクタンク ORF 代表
ジョセフ・ナイ	ハーバード大学名誉教授
ジム・ルイス	戦略国際問題研究所、CSIS
ジェフ・モス	デフコン創始者
ジェーン・ホール・ルッテ	元米国国土安全保障省副長官、元国連平和構築部門副局長
シャオドン・リー	清華大学教授、元 CNNIC 副 CEO
スコット・チャーニー	マイクロソフト社
張力	中国現代国際関係研究院
土屋大洋	慶應義塾大学教授
ナイジェル・インクスター	国際戦略研究所、IISS
バージリオ・アルメイダ	ミナス・ジェライス連邦大学教授
ビル・ウッドコック	パケットクリアリングハウス社
フレドリック・ドーゼ	パリ第 8 大学教授
マリエッテ・シャーケ	欧州議会議員、2017 年ケニア総選挙 EU 監視団代表

図表　5 -3 GCSC、委員の顔ぶれ

委員の出自は大まかに政府、学者、民間企業の 3 つに分けられる。サイバー空間の規範という比較的狭い議論を行う委員会であることを考えると、委員の社会的ポジションがハイレベルであると言える。

139 インターネット関連の標準・教育・方針について検討するための国際非営利団体。トップレベルドメイン（.org）のドメイン名使用料が主たる資金源である。

委員に対して会議参加のための直接費用は支給されるものの、給与などは支払われない。いわゆるプロボノである。特定の国家との関連が深くなることを避けるため、委員は国の公職との兼務ができないとされた。3 年の期間中、議長のカリュランドを含め 2 名が公職につき、委員の職を辞した[140]。

委員を支えるスタッフ（事務局）は基本的にオランダとアメリカのシンクタンクが共同で請け負った。ハーグ戦略研究所のアレクサンダー・クリンバーグとイーストウエストインスティチュートのブルース・マッコーネルは事務方の代表として、活動を主導し、議論を支えた。

GCSC は委員会によるトップダウンアプローチとリサーチアドバイザリグループによるボトムダウンアプローチの両輪で成り立つとされた。リサーチアドバイザリグループの役割は①委員会からの諮問に答えてレポートを作成すること、②情報共有、キャパビル、多様な関係者を巻き込んでコミュニティを作ること、③コミュニティからの声を委員会に吸い上げることとされた。ショーン・カナック（国際戦略研究所）がリーダーを務め、それを 4 人のそれぞれ国際安全保障、インターネットガバナンス、国際法、セキュリティ技術に明るい補佐が支えた。筆者はこのセキュリティ技術分野の補佐として、GCSC の活動全般に参加した。その経験を元に以降、参与観察の結果を記していく。

多くの政府や国際機関がこの委員会の活動を直接的、間接的に支援した。フランス、ハンガリー、フィンランド、米国、スイス、メキシコ、オーストラリア、ポーランド、エストニア、ノルウェー、英国、ニュージーランド、カナダ、ドイツ、ケニア、インド、日本、国連（軍縮部、軍縮研究所）、欧州安全保障協力機構（OSCE）、欧州連合（EU）、

---

140 2017 年 10 月に委員のシギリッド・ケーグ（国連開発計画）がオランダの貿易開発協力大臣となり、GCSC 委員職を辞した。2019 年 3 月 GCSC 議長のカリュランドはエストニア議会のメンバーとなり、委員職を辞した。チャートフとレディの共同議長体制となった。カリュランドは 2019 年 7 月より欧州議会議員を務める。斎藤ウィリアム浩幸（コンサルティング会社）は 2017 年 4 月から 2018 年 1 月まで委員を務めたが、自己都合で辞任した。

ICANN、FIRST、APNIC などが担当者を派遣し、コメントを寄せた。シンガポールとオランダについては、後に述べるように、支援という域を越えて、委員会に不可欠な存在であった。

ある運動の性質を理解する上で、資金源は重要なポイントである。GCSC の場合、まずオランダの外務省が資金を提供し、事務局の運営や委員のリクルート活動が始まった。2017 年 4 月の正式発足までにマイクロソフト、ISOC などがスポンサーとなった。また後に米国の営利企業アフィリアスやシンガポールのサイバーセキュリティ庁がスポンサーとして加わった。これらのスポンサーは委員会に参加し、発言を許された。

第 2 項 活動内容

GCSC は 2019 年末に最終報告書を完成して解散する、時限付きのプロジェクトである。活動の目的は「セキュアで安定したサイバー空間のためのルールづくりを補佐する」であったが、その目的を達成するために、国際社会に広く受け入れられる規範を作ることが主要な活動となった。規範の案は年 2 回の全委員会合、複数回開催された小規模会合、およびメーリングリストで議論された。

委員の議論を経て合意に至った規範を、GCSC は対外的に 3 回にわけて発表してきた。

まず 1 つ目は 2017 年 11 月にインドのニューデリーでの委員会のあとに公開された、インターネットのパブリックコア保護を呼びかける規範である。この規範は、DNS ルートサーバ、海底ケーブル、認証局など一度機能が失われるとその影響が広範囲に及ぶものを「インターネットのパブリックコア」と定義し、その上で、国家及び非国家主体はインターネットのパブリックコアの可用性と整合性を損なう行動をとってはならないとした（Global Commission on the Stability of Cyberspace 2017: 1）。

2 つ目の規範は 2018 年 5 月のスロバキアのブラチスラヴァでの委員会で決定され公開された、選挙および投票システムへの攻撃禁止を呼びかける規範である。国家及び非

国家主体は選挙、国民投票を支える技術インフラへの攻撃や攻撃の支援を行ってはならないとした。（Global Commission on the Stability of Cyberspace 2018a: 1）。

3つ目の成果物はシンガポール規範パッケージと通称される6つの規範のセットである（Global Commission on the Stability of Cyberspace 2018b）。2018年11月のシンガポールでの委員会の議論および有識者への公聴会を経て公開された。ここで提案された規範は以下の図表 5-4のとおりである。

番号	タイトル	概要
1	リリース前の製品へのタンパリングの禁止	国家あるいは非国家アクターは、製品やサービスの機能を損なうような、幅広い利用を阻害するための脆弱性を挿入してはならない。
2	一般消費者が利用するデバイスへの細工禁止	国家あるいは非国家アクターは、一般の個人が利用する電子デバイス、計算リソース、ストレージ、ネットワークリソースにアクセスしたり、それを徴発もしくは徴用したりすべきでない。
3	脆弱性エクイティプロセスの策定義務	国家あるいは非国家アクターは、①非公然の脆弱性情報や②自らが見つけた情報システムや技術の不具合を、どの様な基準でいつ公開するかのプロセスを定めるべきである。プロセスは透明性が確保され、ネットワークセキュリティとレジリエンス、ユーザとユーザが保有するデータのセキュリティ、法執行機関や安全保障上の利用形態、外交や商業活動における位置づけが記載されるべきである。原則として（脆弱性情報を）一般公開する側が優先されるべきである。
4	深刻な脆弱性の修正義務	サイバー空間の安定性に影響を与えうる重要な製品の開発者、製作者はセキュリティ対策を優先し、深刻な脆弱性を修正せずに放置すべきでない。
5	防衛の土台となる基本的なサイバー衛生確保	政府は基本的なサイバー衛生防衛を求め法令を定めるべきである。サイバー衛生対策はすべてのユーザへのユニバーサルで信頼に足る対策、技術情報やベストプラクティスの提供、それら活動への適切な監視を伴うべきである。
6	非国家アクターによるサイバー攻撃作戦禁止	国家は非国家アクターによるサイバー攻撃作戦を禁止すべきである。国家がそれらを許すと、国際法に基づいて国家の責任が問われる可能性がある。国家は国内と国外において非国家アクターによるサイバー攻撃作戦を防ぐための行動をとらなければならない。

図表 5-4 GCSCのシンガポール規範パッケージ

インターネットのパブリックコア保護を呼びかける規範はオランダ、シンガポール、ケニア、エストニアなどが採択している[141]。

第３項 過程の考察

前項までの GCSC の体制および活動内容は、公開されている資料などを元に記述した。本項では、そのような公開資料とヒアリングや参与観察を組み合わせて、GCSC の成果を分析する。分析の視点は 2 つある。まず本項（第３項）があつかう規範の過程に着目するもの。そして第４項が扱う規範の文章そのものに着目するものである。

なぜ GCSC が生まれたのか、GGE の破綻

そもそも GCSC という議論の場は誰が何のために作り出したものなのだろうか。GCSC の起源をたどっていくと、その源流は正式発足の 1 年以上前、2016 年 1 月にミュンヘン安全保障会議のために集まった関係者の間での議論まで遡ることができる[142]。

当時、西側諸国のサイバー外交サークルは大きな懸念を共有していた。国連の政府専門家会合（GGE）[143]の見通しの不安である。国連でのサイバー空間の規範の議論は、2014 年から 2015 年に行われた政府専門家会合で 1 つの頂点を迎えた。そこではサイバー空間への既存国際法の適用が確認され、重要インフラへのサイバー攻撃禁止、ナショナル CERT への攻撃禁止などの規範が合意され、信頼醸成や能力開発に国家が一致して取り組むことで合意がなされた。政府専門家会合によるレポートは、その後 2015 年秋の国連総会に図られ、これを推進することが満場一致で採択された（United Nations 2015a）。

---

141 正確にはオランダ、シンガポール、ケニア、エストニアはインターネットのパブリックコア保護を呼びかける規範を「採択（Adopt）」している。Adopt が実際に意味するところは不明瞭さが残る。

142 GCSC 関係者に対して筆者が実施した匿名のインタビューによる。

143 GGE については脚注 127 を参照のこと。

2014 年から 2015 年に行われた政府専門家会合は大きな成果をあげた。

その成果を引き継ぎ、どの国際法がいかにサイバー空間に適用されるかを主たる争点として、2016 年から 2017 年に政府専門家会合が再度招集された（United Nations 2015b）。しかし、会議が始まった 2016 年当初から、合意の積み上げが難しいという観測が関係者の中にはあった。理由はいくつかある。参加国の一部に国連憲章などの基本的な法体系への理解が不十分なものがいたこと[144]、特定の国がサイバー空間に自衛権を認めることに慎重であったこと、複数の国が国際人道法のサイバー空間への適用に慎重であったことなどが指摘されている（Henriksen 2019: 3–4）。加えて、米国は様々なチャネルを通して、政府専門家会合でさらなる規範の議論をするつもりがないというスタンスを明確に打ち出していたからである。

このような状況を踏まえて、2016 年の当初から 2016-2017 年の政府専門家会合が合意を積み重ねられないと仮定し、次善の策が検討されていた。GCSC はまさにその 1 つである。2016 年 1 月にミュンヘン安全保障会議では米国、オランダやエストニアの関係者があつまり、「サイバー空間の規範を検討するマルチステークホルダーの議論の場」作りがはじまった。その後、議長や事務局などの顔ぶれがきまり、2017 年 1 月にミュンヘン安全保障会議の脇で GCSC の発足がアナウンスされた。2017 年 4 月に正式発足までの間に議長と事務局による委員のリクルーティング作業がはじまる。

委員の選定の重要性

GCSC にとって委員の選定は死活的に重要な作業である。当然であるがサイバー空間の規範を論じるだけの専門性を持つ人物が求められる。加えて、委員の顔ぶれを眺めたときに、その委員会の成果物に有る種の説得力が生まれるような人選が必要である。政府専門家会合のように国連決議で招集されるわけでなく、パリ・コール（France Diplomatie 2018）のように大国の大統領が強力に推進するものでもない。拠り所となる

144 筆者が 2017 年 9 月に行った EU 加盟国の外交官へのインタビューによる。

組織のない、独立したプロセスとしてのGCSCの権威は議長はじめとする委員の個人的資質に大きく左右されるからである。

GCSCの委員はその属性によって3分類できることは既に述べた。まず最大派閥はそれぞれの国において官僚、閣僚としてサイバーセキュリティ政策担当したものである。議長と2人の共同議長の3名がすべてこれに当てはまる。次のグループは民間企業である。世界最大のハッカーカンファレンスであるデフコンの創始者であるジェフ・モス（Jeff Moss）、パケットクリアリングハウス社のビル・ウッドコック（Bill Woodcock）など米国のテックカンパニーが多い。最後のグループは学術研究機関と市民社会を代表する委員である。

議長の力量

GCSCの過程の観察において強調したいのは、議長の重要性である。議長と2人の共同副議長は閣僚経験者で、国際法などの分野の教育を受けている人物である。彼らにとって主たる関心は国際安全保障であり、サイバーセキュリティというのは安全保障確保のための数ある論点の1つにすぎない。しかし、議長と共同議長は規範の議論に必要とあらば技術的に細かい議論にも自ら参加した。議論に参加できるだけの専門知識を有していた。カリュランドは2007年に発生したロシアからとみられるエストニア政府などへの大規模DDoS攻撃発生した際に、駐露エストニア大使として外交交渉を率いた人物である。またエストニアの政府代表として国連の政府専門家会合にも参加した。副議長のチャートフは元米国国土安全保障省の長官であり、米国における重要インフラのサイバーセキュリティ確保に努めた経験を持つ。

単に社会的な地位の高い人物をトップに据える会議体は多いが、GCSCにおいては委員が実際にサイバー空間の規範の議論にどれだけ貢献するかが重要視されたといえる。

参加者の偏り

GCSCは少なくとも世界中の様々な立場の識者の意見を取り込もうと努力した。委員

の前で専門家が発表をする公聴会は合計 4 回開催された。委員会の開催場所が特定地域に集中しないような配慮がなされた[145]。あらゆる国、地域からの異なる意見に対してオープンであるというイメージを得ようとした。

ただし実態として、途上国の意見を代弁できる委員は数少なく、欧米先進国に共有されるサイバー空間像が議論の土台となっていた。特に西側諸国にとっての安全保障上の懸念国である中国およびロシアからの積極的な参加はみられなかった。ロシアについて言えば、議長がエストニア人であり、発足時にロシア人委員がいなかった[146]ことからも、GCSC の活動との隔たりが大きい。中国は発足当初から国家安全部の下のシンクタンクである現代国際関係研究院の張が参加した。しかし、張が積極的に議論に参加することは少なかった。中国のサイバー空間に大きな影響力を持つグローバルテックカンパニー（例えばバイドゥ社、アリババ社、テンセント社、ファーウェイ社）などは不参加である。つまり委員会においてロシア政府や中国政府の利害を代弁する意思を持つものはいなかったし、中国企業に発言の機会は与えられなかった。

以上が GCSC の議論を内側から観察して得られた、過程としての特徴である。

第 4 項 合意内容の考察

合意の拡大が重要

GCSC の活動の目的はサイバー空間の規範を提案することであった。本項では結果として GCSC が世に問うた規範の内容、つまり委員の合意の内容を分析の対象とする。

まず成果の規範の多くは、白紙からドラフトされたわけではないということを指摘し

---

145 委員会の主要な会合開催場所はタリン（エストニア）、ニューデリー（インド）、ブラチスラヴァ（スロバキア）、シンガポール、ジュネーブ（スイス）、神戸（日本）、アジスアベバ（エチオピア）。

146 Group-IB 社というロシアのサイバーセキュリティ企業の CEO サチコフが、2017 年秋から委員に名を連ねたが、積極的に議論に参加したとは言い難い。

たい。GCSC の規範にはその元となる先行した取り組みがある。例えば、2 回目の委員会（デリー、2017 年 11 月）では「インターネットのパブリックコアへの攻撃を禁止する」規範で合意に至った。このインターネットのパブリックコアの概念は、オランダ人研究者のデニス・ブローダーズ（Dennis Broeders）が 2015 年に提唱したものである（Broeders 2015, 2017）。つまり 2015 年の国連政府専門家会合の報告書で禁じられた重要インフラへのサイバー攻撃について、より具体的に重要インフラとしてパブリックコアが含まれるというスタンスを示したところに、GCSC というプロセスの付加価値が認められるのである。

選挙および投票システムへの攻撃禁止を呼びかける規範を例に取る。GCSC は選挙および投票システムへの攻撃禁止を謳う規範を公開したが、その根拠として当時メディアなどで大きく取り上げられ、問題視されていた米大統領選挙に対するロシアの影響工作の存在は無関係である。この規範はあくまで、国連憲章で加盟国が他の加盟国の内政への干渉を禁ずる、いわゆる内政不干渉の原則をサイバー空間に拡大しようという試み[147]である。選挙および投票システムにサイバー攻撃が行われた場合、政治の独立性が侵されると多くの委員は判断した。

サイバー空間はたしかに歴史の浅い新規の空間であるが、その空間を支配するルールは、既存の国際社会の合意と照らして整合性があることが好ましい。この観点から GCSC の会合においては国連憲章やジュネーブ条約や国際人道法が度々俎上に上った。GCSC の規範が、強く既存の国際社会の合意の存在を意識したことは、それらを無視したまったく斬新な規範は、説得力がなく、現実に履行される可能性が低いことを意味する。

GCSC は合意を一から生み出すのではなく、既存の合意を拡大するという戦略を意識

147 選挙システムへのサイバー攻撃についてはタリン・マニュアルにおいても検討が行われ国際法、特に戦時国際法の専門家は「白よりのグレーゾーン」という判断をした。GCSC の功績は、選挙および投票システムへの攻撃禁止と明言したこと、つまりタリン・マニュアル判断から一歩踏み込んだことである。

的に採用した。そのためその過程にあっては既存の枠組み（会議や国際組織や有志グループ）[148]との意見交換を重視し、それらの枠組みの主要メンバーを GCSC の委員にするという手法がとられた。

曖昧すぎても、緻密すぎてもよくない

規範の議論が難しいのは、記述が曖昧すぎると行動の指針をもたらさず、一方で、記述が詳細すぎると、解釈のための余白がなく、国際的な合意が難しくなることにある。加えて、すでにサイバー空間においては、複数の国が軍事活動もしくは情報活動と呼ばれる行為をすでに行っている。それらのすでに行われている、現在行われている活動を禁止する規範を提案することは容易いが、軍やインテリジェンス機関が GCSC の規範の公表をもって、それらの活動を見直す可能性は低い。委員はサイバー空間のあるべき姿を示しつつも、サイバー空間の安定性を脅かしている軍やインテリジェンス機関からの反発を受けないラインを探した。

この好例は「インターネットのパブリックコアへの攻撃を禁止する」規範である。実はこの規範の文章をよく読むと、パブリックコアの可用性と整合性を損なう攻撃が禁止されていることがわかる。パブリックコアへのあらゆる攻撃を禁じているわけではないのである。なぜこのような表現が必要なのか。なぜあらゆる攻撃を禁ずるという規範にしないのか。その答えは、すでに海底ケーブルやデータセンターなどのパブリックコアにおいて大規模サーベイランスが行われているからである。現在行われている大規模サーベイランスは機密性を損なう行為と整理し、機密性までは致し方がないが、可用性と整合性は損なわないという最低限度の合意を、（このケースにおいては軍やインテリジ

[148] GCSC が明示的に協力した既存の枠組みという表現が具体的に示しているのは例えば以下のとおりである。Global Commission on Internet Governance （ビルド委員会）、Global Conference on Cyber Space （ロンドンプロセス）、NETmundial Initiative、World Summit on the Information Society（WSIS）、OSCE、Charter of Trust、テックアコード、Hague Program for Cyber Norms、米カーネギー平和財団における金融システム保護規範、UNIDIR。GCSC はこれらの枠組みの主導者の声を取り入れようとした。

ェンス機関から）得ようとしているのである。リリース前の製品へのタンパリングの禁止の規範も同様である。裏を返せばGCSCの規範は間接的にリリース後の製品への細工は禁じていない。同様に間接的に、大規模サーベイランスを禁じていない。

サイバー空間での武力行使の定義、サイバー兵器の定義は抑止、拡散防止の観点で必須であると当初考えられたが、サイバー空間で活動を行っているとみられる国の委員から「定義が明確になると、（軍事）オペレーションの幅が狭まるという懸念が政権トップレベルにある」と反対の声があがり、その後検討されることはなかった。

GCSCでの合意は、現在、進行している軍事活動もしくは情報活動、主要国が縛られたくないと考えているポイントに慎重に避けながら、しかし、文章としてその他多くの関係者に行動の指針を与えるものでなくてはならない。一言で言えば、「緻密な曖昧さ」が求められる。

規範から見える利益調整

規範づくりは世界平和を目指した高尚な活動ではなく、各参加者の安全保障や経済的反映を得るための手段であるという見方ができる。

選挙および投票システムへの攻撃禁止を呼びかける規範を例にとる。そもそも選挙への攻撃は地域的な課題である。身代金ウイルス、重要インフラのセキュリティなどは問題となる事象が世界中で確認されているが、選挙へのサイバー攻撃が確認されている国は少なく、そして、世界には選挙や国民投票が存在しない、あるいは存在しても形式上の意味しかない国が多く存在する。そんな中でGCSCが特定の国において重要な選挙および投票システムのサイバーセキュリティ確保を早い段階で取り扱ったことに、GCSCの活動の優先度が現れている。高坂（1966: 2035）の「国際連合は人びとが権力政治を離れて、平和について語り合う友愛的なフォーラムではない。そこでは激しい応酬がなされ、利害計算の上にたった抜け目のない取引が行われている」という言葉は、GCSCにも大いにあてはまる。

以上のとおり、本節では GCSC というサイバー空間の規範形成のプロセスへの参与観察を通じて得た情報を、過程と合意内容の 2 つの側面から考察した。限定的な対象に対して、ミクロの視点で向き合うことにより、委員会内部での議長や委員のパワーバランス、緻密な曖昧さが求められる合意内容などの発見があった。

第 5 節　まとめ

本章ではサイバー空間をめぐる合意を分析した。

各国のサイバーセキュリティ戦略という合意を見直すことで、政府はサイバーセキュリティ戦略を作成・公表するという手段を通じて、国内外の利害調整や国際社会に向けた意見表明を行っていることが明らかになった。加えて、昨今、サイバーセキュリティ戦略がサイバー攻撃を抑止するためのメッセージを発する手段として使われていることが明らかになった。

自由度の高さ故にサイバーセキュリティ戦略には各国の利益追求のための意思が直接的に記述される。しかし、サイバーセキュリティ戦略には国家の取り組みがもれなく記述されるわけではない。例えば、アトリビューション問題はグローバル・ガバナンスの観点から重要な研究課題であり、多くの国にとっては根本的政策課題であるが、これを解決する具体案を示すサイバーセキュリティ戦略はなかった。このような各国の恣意的な取捨選択が行われている点を踏まえることが、サイバーセキュリティ戦略を通じて政策への理解を深める際に不可欠である。そして各国の政策を調査する際の資料としての有用性は今後も変わることはないと考えられる。

サイバー空間に関する国際合意の分析からは、合意の主体の峻別が重要であることが導き出された。サイバーセキュリティのガバナンスの主たるアクターは情報拡散国家、情報支配国家、グローバルテックカンパニーの 3 者である。既存の国際合意は①3 つの

グループのいずれかの内部での合意、つまりはグループ内合意②複数のグループ間での合意、つまりグループ間合意③そして議論の場が持つ権威に支えられる国連のもとでの合意の 3 つに分けることができる。

そして合意には繰り返し登場するキーエレメントがある。マルチステークホルダリズム、サイバー空間への国際法の適用、サイバー空間における人権確保、違法有害コンテンツの制限の 4 つで大きく国際合意がスタンスを違えることが明らかになった。グローバルテックカンパニーのルールを形成する力は今後ますます強まると考えられる。

GCSC への参与観察からは、合意の文章が明示的に語らない、裏の狙いを解き明かすことを試みた。分析対象の事例が少なく、偏りがあるという問題点は今後の課題として残るが、それでも合意形成が、必ずしも世界平和を目指した高尚な活動ではなく、各参加者の安全保障や経済的反映を得るための手段であることを示せたと考える。

本章の議論を通して、合意形成のメカニズムの多様さ、合意の強制力の不透明さが浮かび上がってきた。サイバー空間においては、国際的な合意が存在するか、否かの議論はあまり意味を持たない。重要なのは、ある合意についてそれが強い合意なのか、弱い合意なのかの見極めである。

強い合意は、既存の国際法などで合意された現代社会に共通の価値観（表現の自由や内政不干渉）に支えられている。単純に自国や自企業の利益を追求するだけでは、国際的な合意は得られないのである。そして強い合意は一朝一夕に実現しない。既存の合意を少しずつ拡張していく営みが求められている。

第６章　インシデント対応コミュニティの発展

第１節　はじめに

これまで一貫して情報拡散国家と情報支配国家とグローバルテックカンパニーによるサイバーセキュリティのガバナンスについて検討してきた。情報拡散国家と情報支配国家とグローバルテックカンパニーのそれぞれの役割や戦略について、より具体的なイメージが描けるようになったはずである。本章では、サイバーセキュリティのガバナンスが情報拡散国家と情報支配国家とグローバルテックカンパニーの協調もしくは対立によって規定されるとして、この３者以外のサイバーセキュリティガバナンスのアクターの役割が今後どのように変わるかという問題に取り組む。

３者以外のアクターは数多く存在する。まず国際機関があげられる。国連、ASEAN、アフリカ連合、米州機構、イスラム協力機構などの国際機関はこれまでサイバーセキュリティの分野における自らの役割を模索してきた。初期のインターネット自体が大学を結ぶネットワークとして利用されていたことから、サイバー空間において大学や研究機関などアカデミアの影響力は伝統的に強かった。その力は今後も維持されるのだろうか。ISO、ITU や IETF などの標準化団体はその役割を維持できるだろうか、それとも今後はグローバルテックカンパニーが作るデファクト標準が世界を形成するのだろうか。電子フロンティア財団のような、市民社会を代弁し、市民の権利を守る活動は今後より一般的に支持されるようになるだろうか。あるいは、これらの役割は分割され、情報拡散国家と情報支配国家とグローバルテックカンパニーの中に吸収されるのだろうか。

ここではサイバーセキュリティのトリレンマが、情報拡散国家と情報支配国家とグローバルテックカンパニー以外にどのように作用するかを、インシデント対応組織「CSIRT

（Computer Security Incident Response Team）」のケーススタディを通じて分析する[149]。

CSIRT が国際的に注目されるようになった直接の契機は、2015 年の国連政府専門家会合の報告書で、サイバー空間における国家の責任ある振る舞いに関する規範が示されたことである。この中では「他国の CSIRT に対するサイバー攻撃を行わない。自国の CSIRT に他国へのサイバー攻撃に関与させない」という項目が含まれた（United Nations 2015b: paras. 13-k）。報告書はその後国連総会で承認され、現在の国際社会において CSIRT はある種のステータスを得ているといえる[150]。

ここで問題になるのは、CSIRT への攻撃を禁ずる規範が存在するにもかかわらず、肝心の CSIRT について共通認識が希薄なことである。CSIRT を正しく理解する作業なしに、今後のサイバーセキュリティガバナンスにおける CSIRT の役割を論ずることはできない。これまで様々な CSIRT の定義が積み重ねられてきたが、それらは 30 年の歴史を持つ CSIRT コミュニティのその時点でのスナップショットである。ある程度の普遍性を持つ CSIRT の概念化が必要ではないだろうか。ここでは、CSIRT とは何かという繰り返された問いに対する答えとして、定義ではなく概念を提示することを試みた。

本章の構成は以下のとおりである。第２節では CSIRT に関しての分析を試みた先行研究の問題として CSIRT の定義の曖昧さを指摘し、定義ではなく概念を提示することの学術的、社会的意義を説明する。そして目的、機能、文化という 3 つのレンズによって成

---

[149] CSIRT はたびたび CERT（Computer Emergency Response Team）とも表現される。両者の意味するところは同じであり、本論文では CSIRT に統一する。なお"CERT"は日本や米国を含むいくつかの国で米カーネギーメロン大学のソフトウェア工学研究所によって商標登録されている。新たな CSIRT を作り、その名称に CERT の語を使用したい場合には同研究所の許諾が必要である。また CSIRT は設置される組織の種類によって政府 CSIRT、ナショナル CSIRT、組織内 CSIRT などの細分化が行われるが、本章で単に CSIRT と言った場合はそれらすべてを含む。

[150] 2014-2015 年の国連政府専門家会合は、事務総長によって選ばれた 25 カ国が集い、サイバー空間の安定のための方策を議論する場であった。この会合の報告書では国家の責任ある振る舞いに関する規範が示された。「他国の CSIRT に対するサイバー攻撃を行わない。自国の CSIRT に他国へのサイバー攻撃に関与させない」という項目はその 1 つである。なお、報告書では CSIRT ではなく、CERT と表記されている。

り立つ本章の分析の枠組みを提示する。第３節ではサイバーセキュリティガバナンスにおける様々なレジームを目的によって分類し、CSIRT などのインシデント対応を目的とするレジームの誕生の過程を描く。第４節では CSIRT の機能としてのインシデント対応能力に焦点をあて、国際協力と科学的知識の必要性がこの能力の支柱であることを示す。あわせて CSIRT のコミュニティの拡大とレジーム化の過程を描く。第５節では文化の観点から、CSIRT に見られる互恵主義の文化を考察し、目的と機能と文化の 3 つのレンズで CSIRT を概念化できることを主張する。第６節ではサイバーセキュリティのガバナンスの環境変化にともない、この国際的な技術者ネットワークの有効性が失われつつあることを指摘する。第７節でこれらの議論をとりまとめる。

第２節　問題の所在と分析の枠組み

第 1 項 先行研究と問題の所在

世界で最初の CSIRT が誕生して 30 年が経った。世界に数多くの CSIRT が存在し、それらが相互に情報を交換するプラットフォームとして CSIRT コミュニティが存在する。CSIRT コミュニティはサイバーインシデントへの対応、セキュリティ対策の強化などの分野において重要な役割を果たしている。

これまでの CSIRT に関する研究成果は 2 つに大別できる。

1 つは CSIRT 自らが自身の役割を定義し、そのあるべき姿を示すものである。特に 1998 年に世界で最初の CSIRT である"CERT/CC"の創立者らによって記された CSIRT ハンドブックはその代表例である（West Brown et al. 2003）。FIRST（Forum of Incident Response and Security Teams）という世界最大の CSIRT 団体と、日本シーサート協議会という日本最大の CSIRT 団体は、共に現代の CSIRT に求められる役割を文書で提示している（FIRST 2017; 日本シーサート協議会 2011）。それらの共通点は、前提とする読

者を CSIRT あるいは今後 CSIRT を設置する組織と設定し、いかに単一の CSIRT を運営するかについて、技術や運用面を中心に描かれることである。学術的な研究というよりは現場の技術者のマニュアルとしての色彩が強い。

他方で、CSIRT が国際関係論や安全保障論の研究者から注目されるようになったのは 2014 年前後である。Bradshaw（2015）、Skierka et al.（2015）などに代表される研究は、CSIRT コミュニティの外側からインタビューなどを通じて分析することを試みた。想定される読者である政策決定者に対して「CSIRT とは何か」という問いへの答えを提示するものであった。

これら 2 つの異なるアプローチの研究は、前者がいわば CSIRT のコミュニティ内部にいるものによって描かれる自画像であり、後者が外側から描かれた像である。その両者において、CSIRT は繰り返し定義され、また再定義されてきた。図表 6-1 は、これまでの研究における CSIRT とは何かという問いへの答えをまとめたものである。現実世界に既に存在する組織とのアナロジーを用いるアプローチや、CSIRT に期待される役割の最大公約数を網羅しようとするアプローチなどがとられた。しかし、通説が定まっているとは言い難い。

定義の多様さ自体が CSIRT を理解する上での重要な鍵となる。CSIRT はセキュリティインシデントの解決を目指した現場の技術者の内的な問題意識から出発している。最初から組織が満たすべき要件が存在せず、自らの有り様を後知恵で定義してきた。定義の賞味期限が短いのも、特徴である。サイバーセキュリティの脅威が日々変化を遂げるのに伴い、CSIRT の果たすべき役割も変化するためである。それに加えて、これまでの CSIRT を定義する試みは、その時点で存在する CSIRT を名乗る組織を内包するため、包容力のある定義を追求した。これらを乗り越え、より普遍的な CSIRT とは何かという問いへの答えを求めて、本論文は CSIRT の概念化を試みる。

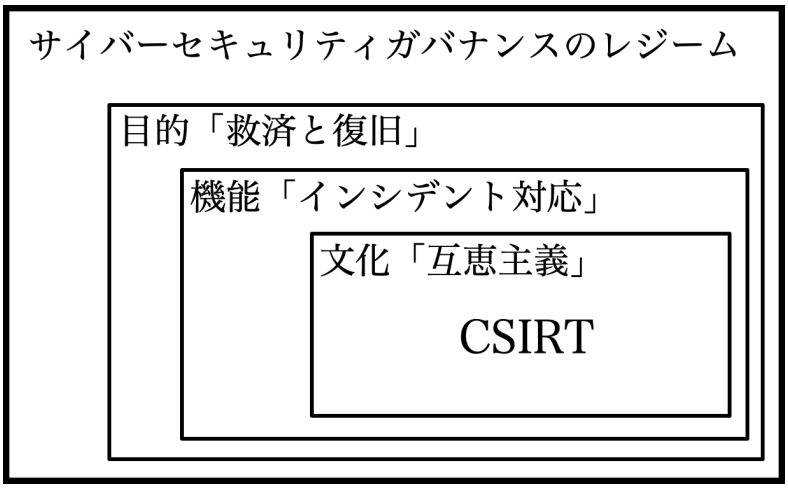
CSIRT とは何か
コンピュータセキュリティにかかるインシデントに対処するための組織の総称。インシデント関連情報、脆弱性情報、攻撃予兆情報を常に収集、分析し、対応方針や手順の策定などの活動をする（日本シーサート協議会 2007）。
インターネットにおける消防署（ENISA 2016）。
組織内の情報セキュリティ問題を専門に扱う、インシデント対応チーム（一般社団法人 JPCERT コーディネーションセンター 2008）。
独立した技術者のネットワークであり、コンピュータセキュリティインシデントへの対応・解決策の調整および通知、情報の交換、インシデントの被害予防を助ける活動を行うもの（Internet Governance Forum 2014）
保険や建築基準法の監査人や法執行機関の捜査員に似た存在（Klimburg & Zylberberg 2015）。
広くインターネットコミュニティのために、自らの技能と知識を用いてインシデントの防止、検知、対応を行う専門家集団（Bradshaw 2015）。
非中央集権の自主管理されたコミュニティの模範（Tanczer, Brass, & Carr 2018）。

図表 6-1 先行研究における「CSIRT」

第２項 本章における分析の枠組み

CSIRT という捉えにくいコミュニティを概念として捕捉するために、ここではサイバーセキュリティガバナンスに乱立するレジームを母集団のデータとして用いる。そして個々のレジームについてその目的と、機能と、文化という 3 つのレンズを通して整理することによって、他のレジームとは異なる CSIRT の概念を抽出できるはずである。

結論を先取りすれば、サイバーセキュリティガバナンスにおけるレジームのうち、目的に「被害者救済と復旧」を掲げ、かつ機能として「インシデント対応能力」を備え、かつ文化として「互恵主義」を信条とするのが CSIRT であるというのが本章の主張である。それは図表 6-2 に示した関係で表すことができる。



図表 6-2 目的と機能と文化の 3 つのレンズ

第３節　救済と復旧という目的

第 1 項 乱立するレジーム

「レジームとは、特定の領域における原則や規範やルールや意思決定の手続きであり、ゲームのルールを決め、アクターの期待を形作るものである」（山本 2008）。国際関係論の研究者は、国家の枠を超えて政策調整をする試みを統治のシステムとして理論化してきた[151]。同分野の研究者は、サイバー空間のガバナンスを巡る混沌とした現状をそれぞれ「レジームの複合体」（Nye 2014）、「傘ではなくパッチワーク」（Choucri et al. 2014: 34）などと表現し、乱立するレジームの整理による実効性のあるガバナンスを模索した。両者に共通するのは、現在の官民市民社会の自主協力は一時的な策でしかなく、将来的には統一されたグローバル組織あるいは制度が必要と主張することである。その担い手

151 一例として核不拡散に関わるレジームがある。核兵器は、様々なアプローチで開発・所持・使用の規制が試みられてきた。1957 年に国際原子力機関が国連に設置され、1963 年に部分的核実験禁止条約ができ、1968 年に不拡散条約が成立した。昨今の核保有国の増加により、その有効性に疑問の声があがることもある。しかし、少なくとも、広島と長崎への原爆投下以降、地球上で核兵器は使用されていない。その功績は、部分的にせよ、核不拡散レジームに帰する。

の１つとしてCSIRTを捉えようとしている。図表 6-3はそれらのレジームを主たる目的という第一のレンズで整理したものである。

サイバーセキュリティのガバナンスは現在形成の途上にあり、レジーム、あるいはレジームの卵は互いに緩やかに連携しながら、しかし、それぞれの分野毎に活動している。サイバー空間の重要性が増すに連れ、それまでインターネットやサイバー空間とはあまり縁が無いと思われていたレジームがサイバーセキュリティを課題と捉えるようになり、今後もアクターは増えていくだろう。

この中で、本章が特に着目するのは、サイバー空間における被害者の救済と復旧を目的としたインシデント対応グループである。このグループを理解するためには、インターネットやサイバー空間に被害者の救済と復旧を支える仕組みが存在しなかった30年前まで遡る必要がある。

グループ	組織、会議体、ルールの例	主たる目的
インターネットガバナンス	ICANN、IANA、インターネットソサイエティ（ISOC）	インターネットの統治と管理
人権	市民的及び政治的権利に関する国際規約、フリーダムオンライン連合	サイバー空間における人権確保
テレコム	国際電気通信連合（ITU）	テレコムの管理
貿易	世界貿易機構（WTO）、ワッセナー・アレンジメント	公正な貿易確保、兵器輸出管理
法の執行	欧州評議会サイバー犯罪条約、インターポール、警察	サイバー攻撃者の検挙・訴追
国際法	サイバーGGE、国連総会、タリン・マニュアル	サイバー空間における法の支配の確立
規範	サイバー空間安定化に関するグローバル委員会（GCSC）、ASEANリージョナルフォーラム（ARF）、欧州安全保障協力機構（OSCE）、テックアコード、信頼憲章	サイバー空間における期待される振舞いの設定
キャパシティビルディング	サイバー専門性に関するグローバルフォーラム（GFCE）、世界銀行	サイバー空間における格差の是正

標準化	IEEE、ISO、IETF、W3C	サイバー空間を支える技術の標準化
インシデント対応	CSIRT、警察	サイバー空間における被害者の救済と復旧
市民団体	電子フロンティア財団、プライバシーインターナショナル	サイバー空間における市民の権利保護
軍	NATO、各国軍隊	サイバー空間におけるパワーの行使
情報活動	ファイブアイズ、各国インテリジェンス機関	サイバー空間を利用した情報活動

図表 6-3 レジームと主たる目的

第２項 インターネット黎明期のインシデントと CSIRT の誕生

世界で最初の CSIRT が発足したのは今から約 30 年前の 1988 年 11 月 17 日のことである。インターネットおよびサイバー空間は「元々『善意の研究者のネットワーク』として誕生したので、設計段階からセキュリティに配慮する（security-by-design）という発想は薄く、圧倒的に攻撃者優位の構造」になっていた（林 2016）。その構造的な弱点を詳らかに明らかにしたのがモリス・ワームである。1988 年に、米国の大学院生ロバート・モリス（Robert T. Morris）がネットワークのセキュリティを調査する目的でメールサーバソフトウェアの脆弱性を利用して、自動増殖を行うプログラムを作成し公開した。当時、約 60,000 台のネットワークに接続していたサーバのうち、10%がまたたく間に機能を失った。このとき、問題を解決するための修正プログラムはすでに準備されていたが、多くのネットワーク管理者の手に行き渡らせるメカニズムが不在であった。このインシデントの 6 日後に国防省や研究機関などが集められた会議でインシデント[152]情報を共有する組織の必要性、日頃からセキュリティ関連情報を提供する組織の必要

[152] インシデントとは「情報および制御システムの運用におけるセキュリティ上の問題として捉えられる事象」である。人的・物的被害を伴う事象は事故であり、なんらかの法律や制度に反する行為は犯罪とされる。それらとの比較において、社会的な深刻度が低いものという見方もある。

性が確認され、15 日後に CERT/CC が設立された[153]。

この当時 CSIRT が解決しようとした問題は、セキュリティ問題について相談できる窓口の不在、情報の流通の仕組みの不在、情報の散逸である。リスク共有手段の欠如と言い換えることもできる。既存の電話網や電信網であれば、電話会社などが自社のネットワーク内においてその役割を一手に担ってきた。ところが、インターネットは、自律・分散・協調を原則とするネットワークのネットワークであり、中心となる管理者が存在しなかった。このインターネットの特質が、セキュリティインシデントや事故への対処のための新たなレジームを求めたとも言える。

最初の CSIRT である CERT/CC が米国に設立された。その後、欧米やアジアを中心に CERT/CC を原型とした CSIRT が作られた。オランダの研究者ネットワークの CSIRT である SURFnet が 1992 年に設置され、ドイツの学術関連組織が DFN-CERT を 1993 年に設置した。オーストラリアのクイーンズランド大学に拠点を持つ AusCERT も 2003 年にオーストラリア研究者ネットワークによって設置された。1990 年代後半になると政府の支援を受けた CSIRT が日本・韓国・シンガポールなどアジア太平洋地域に立ち上がる。CERT/CC 設立から程なくして、CSIRT という組織の有効性は米国以外でも認められたことからも、国際的な救済と復旧を目的とするレジームは時代の要請だったといえる

153 現在との比較において牧歌的なイメージの根強い 1980 年代のコンピュータ・ネットワークであるが、当時からすでに高度なサイバー攻撃は存在していた。よく知られているものとして 1986 年にローレンスリバモア国立研究所の研究者が軍事機密を狙ったとみられる海外からの攻撃の痕跡を発見し、米国内外で様々な協力を得ようと奔走していた一件がある。事件の顛末は 1989 年に出版されてベストセラーとなった（Stoll 1989）。CSIRT は高度なサイバー攻撃に対応するために作られたわけではない。モリス・ワームのように大規模にネットワーク全体に被害を及ぼすインシデントに対して作られた。このことは後に説明する CSIRT コミュニティの文化に影響を与えた。

[154]。

CSIRT がインシデント対応を目的とする唯一のレジームでなかったという点は注意が必要である。当時から警察や軍隊などの中に被害者の救済や自国や自組織におけるインシデントからの復旧を図るための機能は存在した。CERT/CC 設立を決めた会議が米国防省の旗振りで行われたことなどからもそのことは裏付けられている。

第一のレンズ「救済と復旧」を通して見えるのは、1998 年に誕生した CSIRT がサイバー空間における被害者の救済と復旧を目的としたこと、しかし、同様の目的を持ったレジームが他にもあったことである。したがって、第一のレンズだけでは CSIRT だけを捕捉する概念が成立しないことを意味する。

第 4 節　インシデント対応の機能

第 1 項 CSIRT の機能の確立とレジーム化

被害者救済と復旧を目的に始まった CSIRT コミュニティには、それを実現するためのインシデント対応能力が求められる。起こっているインシデントをありのままに理解し、有効な対策を実施する「インシデントハンドリング」が CSIRT の提供する基本的なサー

154 この頃の CSIRT は国と一線を画すことに配慮した。日本で最初の CSIRT である JPCERT/CC の創立者の 1 人である、山口英は 1996 年のインタビューで以下のように述べた。「この中立性をなんとか保ちたいために、発足が遅れてしまったんです。国に任せてしまうと、どこかで管理される恐れもあるし、営利目的ではメドがたたない。かといって学術の人間が片手間にできる活動ではない。（中略）組織の性格としては、警察ではなく、あくまで消防署で、救助と防災が中心。出資段階では通産省に公的資金として負担してもらうけれど、将来的には、産学官の共同組織にし、サービスなどの整備を含め 2-3 年で独立採算を取れる形態にする予定です」（森健 1996: 173）。

ビスとして定着していった[155]。インシデント対応の機能については「国際協力の必要性」と「科学的知識の必要性」という 2 つの重要な論点があり、これが他のレジームと CSIRT の大きな違いとなっている。

インターネットの地理的制約が少ないという特性ゆえに、インシデント対応には国際協力が不可欠であった。CERT/CC 設立の 2 年後の 1990 年に、FIRST という CSIRT の国際コミュニティが活動を始める。フランスなどの欧州諸国と米国の CSIRT が立ち上げメンバーであった。1990 年代前半にドイツ、オーストラリアなどでも大学やインターネット・サービス・プロバイダーの技術者たちが CSIRT を設置した。2019 年 2 月現在、FIRST には全世界 90 の国と経済地域から 450 の CSIRT が加盟している[156]。CSIRT コミュニティは 30 年足らずで世界中に広がった。また地域単位の CSIRT のコミュニティが形成された[157]。

その当時の多くの CSIRT は警察やインテリジェンス機関と違い、法律や制度に明文化される権限を持っていなかった。そもそもサイバー空間上の犯罪の構成要件は国によってばらつきがあり、犯罪対策を名目にした国際協力は難しかった。国際条約や法律という拠り所となるルールが整備されていない状況で[158]、国際 CSIRT コミュニティは救済と回復という目的と共有された科学的知識に頼って協力を行った。一方から送られた記録

---

155 インシデント対応というプロセスについては標準化が遅れており、ここで説明するのと大きく違う「インシデント対応」を行っている例も散見される。Chaudhary et al（2018）はそれが「別々の意図、ゴール、行動をすり合わせ統一するために必要となる相互関係のマネジメント」と分析したが、この見方が広く CSIRT をコミュニティに受け入れられているというデータはない。

156 FIRST に加盟するには、既存加盟組織からの推薦を受け、入会審査をパスする必要がある。加盟後は会費の支払いなどの義務がある。その結果、比較的規模の大きい企業の CSIRT でないと会員資格の維持は難しい。日本からは 34 の組織内 CSIRT が FIRST に加盟している。

157 アジアにおける APCERT、アフリカにおける AfricaCERT、中東イスラム圏における OIC-CERT、太平洋島諸国における PacSON、ASEAN 加盟国における ASEAN-CERT などが地域単位のコミュニティの例である。

158 サイバー犯罪条約の起草が欧州委員会で開始されたのが 1997 年、日本において不正アクセス禁止法が施行されたのが 2000 年のことである。

を見て、自らが管理するネットワークから攻撃あるいは迷惑行為が行われている証左であると理解できるだけの科学的知識もまた活動に不可欠であった。

2000 年代前半からは、CSIRT コミュニティの拡大に伴い、CSIRT の目的と機能の理論化が行われた。前掲の CSIRT ハンドブックはその先鞭となった。グローバル・ガバナンスの視座から CSIRT コミュニティを振り返れば、「必要に迫られた技術者集団が必要に迫られてインシデント対応を行う」状態から「共通の信条と科学的知識に依ってインシデント対応という共通の事業を行うレジーム」へと変容する過程と表現することも可能である。理論化の中では「統一された連絡窓口の提供」「サービス対象の明確化」などの発見がなされ、現在に至るまで CSIRT コミュニティの中で引き継がれている。

第２項 拡大を迫られるインシデント対応能力

CSIRT のインシデント対応能力を支える科学的知識は、アップデートされる必要がある。約 20 年前に JPCERT/CC 代表（当時）の山口英らは「大多数の不正アクセスはその予防方法が明らかになっているものであり、ネットワーク管理とシステム管理を適切に行えば防止できるものである」（山口 & 大林 1999）と述べている。当時の CSIRT のミッションの 1 つは対策情報の迅速な共有であり、共有さえすれば防げる攻撃が多かった。その後の攻撃側と防御側のせめぎ合いを経て、昨今のサイバー攻撃は複雑化している。管理を適切に行っても完全に防ぐことが難しい状況へと変化した。

サイバー攻撃の質的な変化、量の増大は CSIRT に変化を促している。FIRST は現代の CSIRT が提供しうるサービスを列挙したが、インテリジェンス分析、相関分析、フュージョン分析などが追加され、かつてウエスト・ブラウン（West Brown）らが検討した頃から CSIRT に求められる機能の拡大が起こっていることを裏付けている（FIRST 2017; West Brown et al. 2003）。さらに CSIRT の組織上の位置付けも多様化している。一口に CSIRT と言っても、国を代表するナショナル CSIRT、企業や組織のためのインシデント

対応を行う組織内 CSIRT、さらに特定企業の製品とそのユーザの救済を目的とする PSIRT などの細分化が進行している。

インシデント対応能力の観点から言うと機能の拡大とコミュニティの裾野の広がりはリスクである。1990 年代にコミュニティ全体に共有されていた科学的知識や妥当性の基準が、現在も存在するという保証はない。CSIRT コミュニティはこのことを自覚しており、最低限の共通の科学的理解が失われることへの対策が取られている。FIRST や日本シーサート協議会などが、新設の CSIRT に対して研修を実施したり、研修資料を準備したりしている。例えば、FIRST は加盟組織がやり取りする情報について、機密性や取扱の基準に応じて赤、オレンジ、緑などのマークを付加するトラフィックライトプロトコル[159]という制度を 2016 年に標準化し、加盟組織に使用を推奨している。暗黙のマナーとして、トラフィックライトプロトコル自体は 10 年以上前から、日常的に利用されていた。暗黙のマナーを明文化した理由を、コミュニティの裾野が広がり多様化したことに求めることができる。オランダ人研究者 Stikvroot が提唱する SIM3 モデルは、CSIRT の成熟度を定量評価しようという試みであり、これもまた未成熟な CSIRT が増加する現状への手当てとも捉えられる（Stikvoort 2010）。

本節に示したとおり、第 2 のレンズ「機能」からは、インシデント対応能力が CSIRT に必要なものであること、国際協力と科学的知識が能力の 2 つの主要なパラメーターであることが示された。

第 1 のレンズ「目的」と第 2 のレンズ「機能」を重ねて映し出されるのは、CSIRT が救済と復旧という目的を掲げ、インシデント対応能力を備え維持しているということである。この条件にあてはまるのは CSIRT 誕生当時も現在も CSIRT だけではない。警察などの法執行機関、インテリジェンス機関、軍隊にはインシデント対処能力が CSIRT 誕生

159 トラフィックライトプロトコル （TLP）については<https://www.first.org/tlp/>を参照のこと。

以前から備わっていた。また民間企業や組織内にリスク対策部、情報システム部などといった名称で設置されたセキュリティ対応を行う組織も、対象を自組織の資産や顧客やサービスに限定して、救済と復旧を目的に活動を行っていた。次章では、それらの組織と CSIRT とを峻別する手段として第 3 のレンズ「文化」を通して、概念化の仕上げを行う。

第 5 節　互恵主義の文化

第 1 項 信条としての互恵主義

第一のレンズ「目的」と第二のレンズ「機能」によるアクターの分析は、依然として CSIRT とインテリジェンス機関や軍隊や警察の違い、CSIRT と企業の情報セキュリティ対策部門との違いを捉えきれない。本章ではこの課題を乗り越える道具として第三のレンズ「文化」を用いる。

図表 6-4 のとおり Skierka et al.（2015）は、CSIRT 研究の中でコミュニティには 4 つの文化があると指摘した。すなわち業務の独立性、互恵主義、機密性、透明性である[160]。この内、特に互恵主義の文化が CSIRT と他のレジームの大きな差異であることを本章で主張する。CSIRT コミュニティの様々な文章に現れる互恵主義の信条や現在の CSIRT コミュニティにおける互恵主義の実例をいくつか紹介する。

CSIRT コミュニティは様々な形で互恵主義を表現してきた。FIRST は 1995 年の創立時のミッションとして「FIRST メンバーは、知識と技術と経験を持ち寄り、安全でセキ

[160] Skierka et al.（2015）は業務の独立性、互恵主義、機密性、透明性という 4 つの文化を CSIRT に見出したが、本論文では互恵主義のみが CSIRT の概念として成立しうるという立場を取る。その理由は業務の独立性、機密性、透明性の 3 つは CSIRT 以外のサイバーセキュリティ関連組織にも等しく求められており、CSIRT にも見られるとはいえ、CSIRT に固有とは言い難いからである。

ュアなグローバル電子環境を実現する[161]」ことをメンバーに求めた。前掲のブラウンらによって書かれた CSIRT ハンドブックは、組織内に CSIRT を設置する際の定番の教科書となったが、この文書では繰り返し組織の枠を超えた協力の重要性を説く。その実例としてハンドブックそのものが CERT/CC だけでなく、オランダやドイツの CSIRT との国際的な協力によって作成されたことを挙げている。2014 年に当時 APCERT 代表の伊藤友里恵は「APCERT メンバーの中にある"私のセキュリティはあなたのセキュリティにかかっている"というスローガンが協力の屋台骨となっている」（Ito 2014）と述べている。

業務の独立性（Operational Independence）	組織として政府や営利企業の中にあっても、業務については政治的目的や営利活動からは一線を画すこと。
互恵主義[162]（Reciprocity）	自らの受益者を守るという目的を果たす上で、他の CSIRT との協力を行うこと。
機密性（Confidentiality）	インシデント対応の上で機密性に最大限の配慮をすること。
透明性（Transparency）	CSIRT の自律性と権威について透明性が確保されること。

図表 6-4 CSIRT の文化

Skierka et al.（2015）より筆者作成。

CSIRT コミュニティの互恵主義を支えるのは単純な善意ではない。CSIRT コミュニティは共通の科学的知識を持つ。そして、そこから「CSIRT 間の協力は非ゼロ和ゲーム（1

[161] FIRST のミッションは<https://www.first.org/about/mission>を参照のこと。
[162] Reciprocity については相互主義と訳されることもある。GATT/WTO 体制における条約目的を達するための手段としての相互主義などと違い、本章に示す CSIRT 間の協力はあくまでグループ内での規範である。対比のため、CSIRT が相互に助けあう関係については互恵主義と表現することとした。

人の利益が、必ずしも他の誰かの損失にならない)」という共通の理解が浸透した（Skierka et al. 2015: 21)。CSIRT 誕生のきっかけとなったモリス・ワーム事件はその典型的な例である。対策の手段である修正プログラムを誰かに提供することは難しくない。そして、誰かに提供しても自らが損することはない。さらに、類似の問題が自身に発生したときには、見返りを期待できる。CSIRT 誕生から長きにわたり、CSIRT コミュニティは互恵主義をとることが、自らにとっても有利な選択であると考えていたと考えられる。

第２項 互恵主義の発露

互恵主義は信条として様々な文書で繰り返されただけでない。現在の CSIRT 国際コミュニティにもそれは受け継がれている。CSIRT はメールのやり取りなどを通して、インシデントの事象、検知手法、対策情報などを日常的に共有している。属人的な信頼を構築するために年次会合への参加が強く推奨されている。またメンバー間での共同サイバー演習を行うコミュニティも多い。自組織における実際に起きたセキュリティインシデントの顛末記とその分析などの、本来であれば大っぴらにするメリットがない、失敗の共有も行われている。FIRST は現在でも、メンバー間の助け合い、集合知の活用をミッション・ステートメントに掲げ、年次会合おいては、経験豊かな CSIRT のメンバーによる、そうでない CSIRT 向けの教育プログラムが提供されている。

さらに本来、協力関係が育まれにくいアクター間の協力が CSIRT というメカニズムを通して実現している点も興味深い。例えば、日本の JPCERT/CC と中国の CNCERT/CC と韓国の KrCERT/CC は 2011 年に協力の覚書を結び、3 カ国に影響を与えるインシデント情報の交換を行い、年に 1 度の定期的な会合をもっている。3 カ間の政治的な関係は絶えず移ろっており、それに呼応してサイバー空間に関する政府間対話、いわゆるトラック 1 協議は定期的に開催されているわけではない。CSIRT 同士の協力は、比較的堅実と

言える。

またネットワーク機器ベンダー（シスコ社とジュニパー社)、家電メーカー（パナソニック社とソニー社)のようなビジネス上の競合関係にある企業に属する CSIRT 同士が規格の作成で協力したり、他方の CSIRT の設置を手助けしたりといった例も珍しくない。

本論文の分析の枠組みに立ち返れば、次のように言える。インテリジェンス機関や軍隊の少なくとも一部は、自組織における被害者の救済とインフラの復旧を目的に活動している。またそのためのインシデント対応能力を備えている。一方で、組織外との連絡窓口を持たず、組織を越えて協力してインシデントに対応するということが想定されていない。したがってサイバーセキュリティガバナンスの文脈で CSIRT という分類に収まるべきではない。

では、企業や組織内で情報セキュリティ対策を担当する部署、あるいはセキュリティサービス提供を本業とする企業セキュリティベンダーと CSIRT に違いはあるだろうか。両者は機能としてのインシデント対応能力を持ち、復旧を目的としている。両者と CSIRT の違いは組織文化としての「互恵主義」が存在するか否かである。CSIRT は対外的な窓口機能を提供し、組織内外の専門家と助け合いながら問題解決にあたる。企業、組織のリスク管理部門、情報セキュリティ対策を担当する部署においては外部との協力は必ずしも必要でない。

第３項 類似のレジームと互恵主義の陰り

ここまで本章では、CSIRT を、被害者救済とシステムの復旧を目的に掲げ、インシデント対応の機能を持ち、互恵主義の文化を持つ組織であると主張してきた。最後にさらなる考察を要する点として、類似のレジームの存在と互恵主義の陰りについて指摘したい。

まず 1 つ目の課題は、被害者救済とシステムの復旧を目的に掲げ、インシデント対応の機能を持ち、互恵主義の文化を持つ組織が、必ずしも CSIRT に限定されていないことである。具体的な例としてアイザック（ISAC）[163]があげられる。サイバー攻撃の対象が先鋭化するにつれ、同一産業内での情報共有の有用性が増し、CSIRT コミュニティを介さない協力が行われている。アイザックでは活発な情報交換だけでなく業界内での互恵主義に基づいた活動が行われている。アイザックは主として情報の共有を目的とするものであるが、一部のアイザックはインシデント対応の機能を持つ。現在は限定的なアイザックの活動が、世界中でさらに受け入れられるのであれば、CSIRT とアイザックの整理を可能にする第四のレンズが必要になる。

2 つ目の課題は、CSIRT コミュニティ内の互恵主義が薄れつつある点である。本論文で振り返ってきたように、互恵主義は CSIRT コミュニティに受け継がれてきた文化である。そのことはしかし、現在や未来において文化が引き継がれることを保証しない。すでに述べたサイバー攻撃の高度化と先鋭化の他に、サイバーセキュリティの安全保障問題化が強く影響している。国家によるサーベイランス活動や国家が支援するとみられる他国の重要インフラに対するサイバー攻撃は枚挙に暇がない。他国が自国を攻撃している疑いがある場合に、その他国に設置された CSIRT との協力は合理的な選択ではない。互恵主義は CSIRT を他のレジームと分かつ最たる違いであった。サイバーセキュリティの安全保障問題化によって互恵主義が失われるとすれば、CSIRT というレジームはユニークさを失い有効性を失う可能性がある。

---

163 Information Sharing and Analysis Center の略。事業者同士でサイバーセキュリティに関する情報を共有し、サイバー攻撃への防御力を高めることを目指して活動する民間組織。日本国内においては通信事業者、IT ベンダー、金融機関による ISAC が組織されている。

第 6 節　国際 CSIRT コミュニティの崩壊あるいは衰退

ここでは CSIRT の活動のうち、国の枠を超えた協力が衰退しつつあり、今後さらに難しさを増すことを主張する。それには国際 CSIRT コミュニティの外部で起きている変化と内部で起きている変化の両面を捉える必要がある。両者は密接につながっており明確な分類は難しい。後者は CSIRT コミュニティ自身の手によって、ある程度コントロールが可能な要因と捉えていただきたい。最終節では、これらの変化の結果として、互恵主義の文化が失われている状況を明らかにする。

第 1 項 とりまく環境の変化（外的要因）

サイバーセキュリティと安全保障

既に第 1 章から論じてきたとおり、2010 年代前半からサイバーセキュリティの安全保障問題化が加速した。サイバーセキュリティが国家の安全保障確保の重要な一部分であるという認識が広がった。CSIRT の互恵主義はサイバーセキュリティ対策が非ゼロ和ゲームであるという理解に立脚していることを前節で述べた。2019 年 2 月現在、サイバー攻撃能力の保有を公式に認める国は米国とイスラエル以外に 21 カ国、保有が疑われている国がさらに 24 カ国ある[164]。国家が支援するサイバー攻撃は、もはや珍しいことではなくなった。そして、ある CSIRT が友好国ではない他国の CSIRT に対して自国へのサイバー攻撃への対処を依頼することは問題を解決しないだけでなく、自らの探知能力という手の内を明らかにする愚行であるという言説が説得力を持ち始めた。この認識は CSIRT 間の国際協力にネガティブな影響を及ぼす。

サイバーセキュリティが国家安全保障の一部分となり、多国間の協力に支障をきたし

[164] Digital Watch という NGO の調査結果に基づく（GIP Digital Watch observatory for Internet governance and digital policy 2019）。

た具体的な例として、南太平洋島嶼国に設立された地域 CSIRT である PacCERT を紹介する。22 の南太平洋島嶼国すべてがそれぞれにナショナル CSIRT を設置することは難しい。初期費用を日本が負担し、維持費用は島嶼国が分担し、島嶼国すべてに対してサービスを提供する CSIRT をフィジーに設立することが島嶼国の通信大臣会合で決められた。国際協力機構（JICA）の支援を受けて、PacCERT は 2012 年 7 月に活動を開始したが、取り決めに従って活動費用を拠出する国がなく 2014 年 12 月に正式に活動を停止せざるを得なくなった（独立行政法人国際協力機構 2012）。島嶼国は単にサイバーセキュリティ対策への資金拠出を嫌ったわけではない。彼らはサイバーセキュリティ対策の機能を近隣諸国と共有することを嫌ったのである。そのことは、パプアニューギニア、トンガ、フィジー、バヌアツがその後自らのナショナル CSIRT を立ち上げ、自国内のサイバーセキュリティ確保のためのコストを甘んじて受け入れていることからも明白だ。

個々の国における治安および安全保障確保と、グローバルなサイバーセキュリティ向上を目指す CSIRT の活動の衝突も起きるようになった。2015 年に CERT/CC は Tor というネットワークの匿名化ソフトの利用者の解析について FBI に協力したとされている。この際にはメディアや著名な暗号学者から「CSIRT は信頼できる仲介者であるべきで、恣意的に公開・非公開の判断をすべきでない」と批判された（Schneier 2015）。つまり政府への協力を咎められた。その CERT/CC は、2018 年 1 月にグーグル社の研究者が発見したインテル社製 CPU の脆弱性情報について情報を公開した。その直後に開かれた米議会の委員会では米国内で対策が不十分な状態で CERT/CC が国外、とりわけ中国の専門家にその脆弱性情報を共有したことが批判の対象となった（U.S. Senate Committee On Commerce Science and Transportation 2018）。この例が如実に語るのは CSIRT がグローバリゼーションと国家主権の板挟み状態になる危険性である。サイバー空間が国家間のゼロ和ゲームへと変容しつつある中で、CSIRT コミュニティは互恵主義に基づく活動

が、国家安全保障に与える影響に無関心ではいられなくなっている[165]。

サイバー攻撃の高度化と先鋭化

前述のとおり、約 20 年前 CSIRT のミッションは対策情報の迅速な共有であった。共有さえすれば防げる攻撃が多かったのである。その後 20 年の攻撃側と防御側のせめぎ合いを経て、昨今のサイバー攻撃は複雑化している。セキュリティ対策を十分に行う予算や人材がいるはずの組織のシステムが侵入され情報漏えいなどの被害が発生している。管理を適切に行なっても完全に防ぐことが難しい状況へと変化した（西本 2012: 349）。「サイバーセキュリティにおける最大の脅威は技術を使いこなした、明確に攻撃の意思を持つ攻撃者であり、技術規制の効果はあまり期待できない」（Berg & Keymolen 2017: 201）ため、単に協力して、国際 CSIRT コミュニティ内で対処情報を回付しても被害の低減効果が薄くなってきた。

加えて、攻撃者が標的を明確に限定したサイバー攻撃を行うようになった。これを先鋭化と表現する。特定の国や産業に限定して侵入を試みる例が多く見られる。この場合、同一産業の企業や、同一国内での情報交換の方が得られるものが多いだろう。事実、産業毎に CSIRT コミュニティを介さない協力が活発化している。攻撃の高度化と先鋭化という現象は、より限定的なコミュニティを求めるのかもしれない。だとすれば FIRST に代表される間口が広い CSIRT コミュニティの有用性が相対的に低下する。

---

165 サイバーセキュリティと安全保障の接近を示す、別の例として、2019 年 9 月に FIRST に加盟していたファーウェイ社が会員資格を停止されたという出来事を挙げられる。同年 8 月 19 日に米国の輸出管理規則（EAR）が改定された。ファーウェイ社などの一部企業に対する米国企業や組織からの「技術移転」が禁止された。この「技術移転」が具体的にどのようなやり取りを指すのか米国商務省産業安全保障局は明らかにしておらず、FIRST は自らが会員向けに提供している情報共有サービスなどが規制に抵触する危険を避けるため、ファーウェイ社の会員資格を停止した。国や立場の違いを超えた互恵主義をモットーに掲げる FIRST が、特定の国の規制に流される形でメンバー資格を停止したことは、メンバーに驚きを与えた（FIRST 2019）。その後も、コミュニティからの中国企業 CSIRT 締め出しの動きは続き、10 月には、ビデオ監視システムなどを製造するダーファ社（Zhejiang Dahua Technology Co., LTD.）およびハイクビジョン社（Hikvision）の CSIRT も FIRST のメンバー資格を停止された。

第２項 とりまく環境の変化（内的要因）

サイバーセキュリティの商業化

多くのアクターがひしめく中で、かつてのようにCSIRTはサイバーセキュリティに関する唯一の専門集団でなくなった。特にセキュリティベンダーと呼ばれるセキュリティ製品またはセキュリティサービス提供企業の活躍が目覚ましい。日本だけをみてもサイバーセキュリティ市場は2017年時点で9965億円、2018年には1兆円到達が見込まれる（日本ネットワークセキュリティ協会 セキュリティ市場調査WG 2018）。市場が拡大し、セキュリティベンダーには優秀な技術者が集まる。最も精度の高いインシデント情報はセキュリティベンダーに所属する技術者の手によって生み出され、公開される。情報には値段がつき、高値で取引されることもある。スマートフォンの基本ソフトやインターネットブラウザのセキュリティ上の問題点は1000万円を超える価格で取引されることが珍しくない[166]。自らの発見に対価を求めず他者に共有することを期待するのは難しい。

国際 CSIRT コミュニティはメンバー同士がときにビジネス上の競合関係にあることを理解し、互恵主義に基づく活動とのバランスを模索してきた。FIRSTの意思決定機関は10人の理事によって構成される理事会である。10人の理事は所属するCSIRTの利益代表者でなくコミュニティ全体への奉仕者であることを求められる。選挙の際には所属組織ではなく候補者個人への投票が行われる。年次会合などでは特定企業の宣伝などを厳しく排除している[167]。これらはコミュニティの活動により特定の企業の利益が損なわ

---

166 例えば、米国のある企業はiPhoneの基本ソフトの脆弱性があれば約2億円の報奨金を払うとし、常時研究者からの報告を受け付けている。これらの取引の全容はわかっていないが、億単位が支払われたという記録が無く、ここでは「1千万円程度の取引は珍しくない」という表現をとる。

167 FIRST年次会合の講演募集でも「マーケティング目的の発表厳禁!（NO SALES OR MARKETING PRESENTATIONS!）」と強調されている。

れることへの配慮である[168]。

第３項 ナショナル CSIRT の行政組織化

CSIRT コミュニティの多様性に起因する曖昧さも指摘しておきたい。サイバー空間における、国家というアクターの重要性が高まるに連れ、ナショナル CSIRT の役割や予算は拡大してきている。ナショナル CSIRT は、公開情報が少なく、特に理解することが難しい。先行研究を振り返れば、資金源・権限・組織のあり方が多様であり、信頼性を損なっていると指摘したもの（Morgus et al. 2015）、またナショナル CSIRT を一枚岩のグループとして捉えることは難しく、共通点は「技術的な問題についての、（国際的に）承認された連絡窓口機能をそなえること」のみであるとしたものがある（Klimburg & Zylberberg 2015）。ナショナル CSIRT の位置付けは、それらの研究が行われた時点からさらに複雑化している。図表　6-5 主要国のナショナル CSIRT と資金拠出組織は主要国におけるナショナル CSIRT とその活動に資金を拠出している組織の一覧である。

2 つの変化が特に CSIRT の互恵主義に悪影響を与えると考えられる。

1 つ目はインテリジェンス機関や軍とナショナル CSIRT の接近である。CSIRT コミュニティが政府からの財政的な援助を受けていた場合でも、その実務が独立していたことは第４節第１項で述べたとおりである。その後、30 年の間にナショナル CSIRT はほぼすべて政府の内部に「吸収」された。主要国においてナショナル CSIRT が政府から独立した形を保っているのは日本[169]、ブラジルなど僅かに残るのみである。一口に政府が支

---

168 サイバー空間において企業は必ずしも自らの利益だけを追求しているわけではない。マイクロソフト社が主導したいくつかの国際的なボットネットの停止のための活動、ランサムウェアの感染拡大際の駆除ソフトの無償配布など、自社の利益を超えてインターネットを安全にするための活動は枚挙にいとまがない。ここで主張したいのは一企業の商業上の成功と、CSIRT の国際協力がときに併存しないことは念頭に置く必要があるということである。

169 日本については、ナショナル CSIRT の役割を内閣官房サイバーセキュリティセンターと JPCERT/CC の 2 組織が共同で果たすという形態が取られている。

える CSIRT と言っても、資金源が警察やインテリジェンス機関なのか、科学技術を担当する機関なのかによってその活動の方向性は変わってくる。イギリス、カナダ、オーストラリア、ニュージーランドは足並みを揃えて、2016-2018 年の間に大統領府や首相室の直下にサイバーセキュリティセンターを組織し、ナショナル CSIRT をその中に設置した。例えば、オーストラリアのサイバーセキュリティセンターのトップは国防省通信電子局というインテリジェンス機関出身者が務める。このようなナショナル CSIRT のインテリジェンス・コミュニティとの接近は、とりわけ非友好国間での協力を阻害する。国際政治の研究者は CSIRT がインテリジェンス機関や法執行機関との距離を保ち、攻撃的活動を行わないなどの取り決めが必要と主張したが（Morgus et al. 2015: 27）、その後数年間で CSIRT はさらにインテリジェンス機関や法執行機関との結びつきを強めた。

2 つ目の変化は、ナショナル CSIRT が他国からのサイバー攻撃を非難する役割を担いだしたことである。2016 年に米国のナショナル CSIRT である US-CERT は FBI と連名で、ロシア発のサイバー攻撃への注意をよびかけた（DHS & FBI 2016）。CSIRT の本来の目的は被害者救済と復旧であることはすでに述べた。攻撃者の特定を行い、その結果を公開するという政治的なメッセージを発出する役割を FBI や国務省ではなく US-CERT という CSIRT が行った。加えて US-CERT が当初公開したロシアが攻撃に関与したという具体的な証拠[170]は記述ミスが多く信頼性を欠いた。US-CERT への信頼は損なわれた。この件がきっかけとなり、その後イギリスやウクライナのナショナル CSIRT もロシア政府が関与したとみられるサイバー攻撃への非難声明を行っている。また当の US-CERT は、北朝鮮や中国やイランからのサイバー攻撃について情報公開を継続している。CSIRT の政治機構化は現在進行形である。

あるインシデントに関わる情報を他国の CSIRT に共有した場合に、それが「インターネットをセキュアな状態に保つために協力する」ために利用されるのか、あるいは国際

[170] IOC とよばれる攻撃に使われた IP アドレスやファイルのリスト。

関係の中で自国が有利な立場を得るために利用されるのか。ナショナル CSIRT は「囚人のジレンマ」に似た、インターネット全体の利益と個々の国にとっての合理性の選択を迫られることが増えるとみられる。

国名	現在のナショナル CSIRT（略称）	資金拠出組織（略称）	設立年
米国[171]	US-CERT	サイバーセキュリティ・インフラセキュリティ庁（CISA）	2003 年
オーストラリア[172]	サイバーセキュリティセンター（ACSC）	通信電子局（CSE）	2010 年
ドイツ[173]	CERT-Bund	情報セキュリティ庁（BSI）	2001 年
カナダ[174]	センターフォーサイバーセキュリティ（CCCS）	通信保安局（CSE）	（2003 年）
フランス[175]	CERT-FR	情報システムセキュリティ庁（ANSSI）	2014 年
日本	JPCERT/CC	経済産業省	1996 年
日本	内閣サイバーセキュリティセンター（NISC）	内閣官房	2005 年
イタリア	IT-CERT	経済開発省	2014 年
韓国[176]	KrCERT/CC	インターネットセキュリティ庁（KISA）	2003 年

171 CERT/CC が長年ナショナル CERT として機能していた。2003 年 9 月に大統領令 13618 号に基づいて US-CERT が国土安全保障省配下に設置され、数年の移行期間を経て、現在は US-CERT がナショナル CERT 機能を多く果たしている。US-CERT の主たる業務は National CSIRT として米国のインシデント一般への対応の他、政府ネットワークへの攻撃対応である。CISA Act （H.R. 3359、 2018 年 11 月に成立）により、DHS の内部部局の 1 つがサイバーインフラストラクチャーセキュリティ庁に格上げされたのに伴い、DHS からは切り離された。

172 1993 年にクイーンズランド大学内に AusCERT が発足し、長年ナショナル CERT として機能していた。2010 年から CERT Australia（当時、司法省配下）にナショナル CSIRT 機能が移行された。その後何回かの組織改編を経て現在にいたる

173 情報セキュリティ庁（BSI）は 1990 年の BSI 設置法により設立。

174 センターフォーサイバーセキュリティ（CCCS）は通信保安局の下に 2018 年に設置された。前身となる組織は公安省（Public Safety Canada）の一部門として、その後カナダサイバーセキュリティインシデントレスポンスセンター（CCIRC）として活動を行っていた。設立年は不明のため、FIRST に加盟した 2003 年を便宜上用いた。

175 CERTA という名前で 2000 年から活動。その後 2014 年前後に CERT-FR という名称で情報システムセキュリティ庁の一部門となった。

176 CERTCC/KR という KrCERT/CC の前身となる組織が 2003 年に活動していた記録が残っているため、ここでは 2003 年と記載した。現在のように情報セキュリティ庁（KISA）の下で活動を始めたのは 2009 年のことである。

韓国[177]	KN-CERT	ナショナルサイバーセキュリティセンター（NCSC）	2004 年
中国[178]	CNCERT/CC	共産党網絡安全和信化委員会弁工室（CAC）	2002 年
シンガポール[179]	SingCERT	サイバーセキュリティ庁（CSA）	1997 年
ニュージーランド[180]	CERT NZ	ナショナルサイバーセキュリティセンター（NCSC）	2016 年
英国[181]	ナショナルサイバーセキュリティセンター（NCSC）	政府通信本部（GCH）	2016 年
フィンランド	NCSC-FI	通信規制局	2002 年
ロシア[182]	GOV-CERT.RU	ロシア政府	2012 年
インド[183]	CERT-In	電子情報技術省	2004 年
メキシコ	CERT-MX	連邦警察	2010 年
ブラジル[184]	CERT.br	NIC.br	1997 年

図表 6-5 主要国のナショナル CSIRT と資金拠出組織

第 7 節 まとめ

[177] KN-CERT は 2004 年の設置以来、国家情報院の下部組織として活動をしてきた。韓国サイバーセキュリティセンターは国家情報院の一部門である。
[178] CNCERT/CC は 2002 年 9 月の設立以来、工業信息化部（MIIT）からの資金提供を受けていた。2018 年に国家互連網信息弁公室（CAC）の管理下に移管される。
[179] SingCERT は 1997 年に設立したアジアでも歴史の長い CSIRT である。活動の資金は長く情報通信開発庁（IDA、現在の情報通信メディア開発庁）が拠出してきた。その後 2015 年にサイバーセキュリティ庁が設置され、SingCERT は同庁配下に移管された。
[180] ニュージーランドナショナルサイバーセキュリティセンター（NCSC）は政府通信保安局（GCSB）の下部組織である。
[181] 長きにわたり、政府 CERT や国防省 CERT などが並立する状況であったが、2013 年 12 月に CERT-UK が設置され、機能統合が図られた。CERT-UK はインシデント対応 、CERT 間国際連携のリード 、英国全体のサイバー啓発と情報共有などを担当した。その後 2016 年に政府通信本部（GCHQ）の配下にナショナルサイバーセキュリティセンターとして移管された。
[182] 1998 年にネットワーク研究所（RIPN）の支援を受けて RU-CERT が設立され長らくナショナル CSIRT の役割を果たしてきた。2012 年に現在の GOV-CERT.RU が政府内に設置された。所管省庁を確認できないため、ここでは単にロシア政府とした。
[183] CERT-In の設立は 2004 年だが、政府が公式に認定したのが 2008 年である。
[184] 1997 年から NIC BR Security Office（NBSO）という名称で活動を行っていた。2003 年の大統領令 4829 号により CERT.br へ改組された。NIC.br はドメイン名など管理する企業である。

ここまで指摘してきた問題を CSIRT コミュニティはいかに克服できるのか、今後の CSIRT コミュニティの道筋を提示したい。直面している課題を整理すれば、サイバーセキュリティの非ゼロ和ゲーム化であり、CSIRT 自身の「被害者救済と復旧」という目的と互恵主義の文化が共に揺らいでいることである。この状況において、CSIRT コミュニティは目的を再設定することが求められる。少なくとも 3 つの選択肢がある。

1 つ目は、コミュニティの目的を「人道確保の観点からサイバー空間の安定を維持する」とし、国家から独立したネットワーク、いわばサイバー版国際赤十字社として発展する可能性である。この場合 CSIRT は所属する国や組織の損得ではなく、システムとしての正しさと人道の保護という新たな価値観にもとづいて行動をすることが期待される（Hollis 2011）。

2 つ目は、共通の目的を「サイバー空間の公衆衛生確保する」とし、サイバー版世界保健機関（WHO）あるいはサイバー版疾病予防管理センター（CDC）として発展する可能性である。サイバー空間への公衆衛生アプローチはこれまで度々議論されてきた。具体的な形として、ジェイソン・ヒーリー（Jason Healey）らのいう「ありのままに近いデータを示すためのグローバルな協力を行うネットワーク」がある（Healey & Knake 2018）。歴史を振り返れば、地球温暖化というグローバルな課題に対して、炭素排出量の推計などで国際的な科学者のネットワークがニュートラルなデータを提供するという独自の役割を果たした。CSIRT コミュニティはサイバー空間における科学的データの供給元として役割を果たせる。

3 つ目は、各国政府の下にある行政機構となり、政府の政策遂行に専念する道である[185]。言い換えれば国際 CSIRT コミュニティ崩壊のシナリオである。肯定的に捉えれば、一部の国際関係論者からはサイバー空間における専門的知識の欠如を指摘する声が多く、その欠落を埋める手段としての CSIRT に期待が寄せられている。「他国の CSIRT に

[185] CSIRT はすでに准外交機能を担っているという指摘もある（Caldwell 2014）。

対するサイバー攻撃を行わない。自国の CSIRT に他国へのサイバー攻撃に関与させない」という国連政府専門家会合の合意は、明示していないものの、ナショナル CSIRT を指していると考えられ、サイバー空間における信頼醸成の手段として CSIRT の役割を見据えてのものと解釈することも可能である。

本論文は Skierka et al.（2015）が見出した固有の文化に着目し、既存研究に繰り返された CSIRT の精緻な定義の議論を離れ、わかりやすいが不正確なアナロジーを避け、CSIRT の概念化を試みた。他のレジームとの比較から、CSIRT は機能としてインシデント対応能力を持ち、被害者救済とシステムの復旧を目的に掲げ、互恵主義の文化を信条とする組織のことであると主張した。中央管理者が不在という、インターネットの特質が国際協力と科学的知識の共有を要請し、それにより互恵主義の文化が根付いたことを示した。

概念を論ずれば、そこに現実の有り様との齟齬が生まれる。本論文における主張は、分析の枠組みを通して可能な限り論理的に描き出そうという試みであったが、CSIRT のありのままの姿を描くためのものではなかった。この概念が、多様性を増す現在の CSIRT をどれだけ捉えられるかは、今後第三者によって冷静な評価がされるべきである。サイバーセキュリティガバナンスの変容に応じて、薄れる危険性をはらむ互恵主義についてはとりわけ観察を要する。

30 年に及ぶ CSIRT の歴史からは、サイバー空間のトリレンマによって、民間組織が行政組織化していく流れが読み取れた。本論文の分析の枠組みに立ち返れば、これはグローバリゼーションの後退であり、国家主権の重要性の高まりを意味する。産業、技術などの大変動が生じたとき、それに見合った民間組織が形成され、さらにそれが国際組織・国家間レジームへ転化していくことはこれまでの歴史においてもみられたことである（Murphy 2000）。CSIRT の行く末は、サイバー空間を支配する者は誰になるのかという大きな問題の一部分ともいえる。そしてそれは今日の社会における国家間レジームの

有効性と切り離して考えられない問題である。

第７章　終章

第１節　各章における検討内容

ここで、本論文において各章で主張してきた点を再度繰り返す。本論文の最大の目的はサイバーセキュリティのグローバル・ガバナンスの理論的考察であった。サイバーパワーを「より多くのデータにアクセスする力」と定義し、各アクターは、生存が保障されないアナーキーなサイバー空間において、より多くのデータにアクセスしようとしている。特に第１章で定義した「情報拡散国家」と「情報支配国家」と「グローバルテックカンパニー」が主要な３アクターであり競争の中心にいる。

先行研究を振り返ると、サイバーセキュリティのグローバル・ガバナンスはインターネットガバナンス論、国際関係論の中で扱われてきたことが分かった。それらは、サイバーパワーを得るために、より多くのデータにアクセスするために最も重要な、「サイバー空間における価値」を論じてこなかったこと、そしてグローバルテックカンパニーの力を正しく評価されてこなかったことを批判した。

そして、「サイバー空間の秩序の土台となる共通の価値観とはなにか」という本論文の核となるリサーチクエスチョンを設定した。「誰がどのようなサイバー空間を実現しようとしているか」と言い換えることもできる。「共通の価値観とはなにか」、その答えが民主主義と国家主権とグローバリゼーションの３つであると仮定して議論を進めた。

第２章「サイバー空間における情報拡散国家の苦悩」では情報拡散国家の戦略を紐解き、同時にロドリックの世界経済の政治的トリレンマの原理を応用したサイバー空間のトリレンマという本論文を貫く分析の枠組みを提示した。サイバー空間においては、民主主義と国家主権とグローバリゼーションを推進しているのが、それぞれ情報

拡散国家、情報支配国家、グローバルテックカンパニーと捉えられる。そして現在のサイバー空間をその 3 つのアクターによる争いとみなすものである。

情報拡散国家はサイバー空間において、グローバリゼーションと民主主義を一貫して追求してきた。その背景にはサイバー空間とインターネットの創成期において米国という国が一貫して主導的な立場にあったことがあげられる。一時、インターネットと民主主義の蜜月と呼べる期間があったが、国家として国民の安全の確保を図る必要があり、そこに国家主権を確立するという新たな目標が加えられた。情報拡散国家は国家主権の確保に舵を切った。しかし、その選択がサイバー空間におけるグローバリゼーションもしくは民主主義のいずれかを諦める覚悟を伴うことに気づいていないことを指摘した。

第 3 章「情報支配国家」では情報支配国家の戦略を検討した。

情報支配国家においては、サイバー空間における情報の自由な流通よりも、治安の維持や政治の安定が優先される。ゆえに国家や政府によるサイバー空間の管理の必要性を正当化されやすいという共通点が見いだされた。サイバー空間は経済や社会活動に欠かせないだけでなく、あらゆる政治活動やテロリズムの場でもある。その場の安全を確保するために主権国家という装置は今も必要である。サイバー空間に国家主権を求める声は確実に強まっていて、情報支配国家はその先頭に立つ存在と言える。

中国、ロシア、北朝鮮の状況を対比して言えるのはサイバー空間に起こっているのは自由を希求する情報拡散国家と統治を望む情報支配国家という単純な対決ではないということである。情報支配国家にカテゴライズした中国とロシアの間には極めて大きな違いがある。中国はグローバルなインターネットを求めており、ロシアはそれを求めていない。その違いを意識せずに既存の国際安全保障の視点から中国とロシアを「中露」と一括にできない。

第 4 章「グローバルテックカンパニー」ではサイバー空間トリレンマ理論における 3 つめのアクターである、グローバルテックカンパニーの戦略を論じた。法、規範、市場、

アーキテクチャのすべてにおいて、国家を凌ぐ強い影響力を持つグローバルテックカンパニーの力を描いた。グローバルテックカンパニーの力の源泉は、数十億人のユーザが日々生成するデータに自由にアクセスできる点にある。

現在のサイバー空間のガバナンスを支えるのは、政府の行動が後手に回る状況を様々な創意工夫で対応してきたグローバルテックカンパニーの貢献が大きい。しかし、グローバルテックカンパニーは自らが、国家の代役はできないことを自覚すべきである。グローバルテックカンパニーには技術と大量のデータと資金が存在するが、それを大規模に行使する民主的な正当性も、ガバナンスも中立性も確保されていない。したがって第４章では、グローバルテックカンパニーが新たな国際秩序を作る可能性は低いとし、今後情報拡散国家もしくは情報支配国家のいずれかを支える役割を担うものと結論づけた。

第５章「合意を巡る戦い」では文字どおり、情報拡散国家、情報支配国家、グローバルテックカンパニーの争いを、合意を巡る戦いとして描いた。ここでの合意とは国家サイバーセキュリティ戦略や国際条約や規範などの総称である。

各国のサイバーセキュリティ戦略という合意を見直すことで、政府はサイバーセキュリティ戦略を作成・公表するという手段を通じて、国内外の利害調整や国際社会に向けた意見表明を行っていることが明らかになった。

サイバー空間に関する国際合意の分析からは、合意の主体の峻別が重要であることが導き出された。サイバーセキュリティのガバナンスの主たるアクターは情報拡散国家、情報支配国家、グローバルテックカンパニーの 3 者である。既存の国際合意は①3 つのグループのいずれかの内部での合意、つまりはグループ内合意②複数のグループ間での合意、つまりグループ間合意③そして議論の場が持つ格式に支えられる国連のもとでの合意の 3 つに分けることができる。そして合意には繰り返し登場するキーエレメントがある。マルチステークホルダリズム、サイバー空間の国際法の適用、サイバー空間にお

ける人権確保、違法有害コンテンツの制限の 4 つで大きく国際合意がスタンスを違えることが明らかになった。

GCSC への参与観察からは合意の文章が明示的に語らない、裏の狙いを解き明かすことを試みた。合意形成が、必ずしも世界平和を目指した高尚な活動ではなく、各参加者の安全保障や経済的反映を得るための手段であるという現実を示した。

第 6 章「インシデント対応コミュニティの発展」では情報拡散国家、情報支配国家、グローバルテックカンパニーの争いにおいて CSIRT というセキュリティ対策組織が果たす役割を取り上げた。サイバーセキュリティガバナンスにおけるレジームのうち、目的に「被害者救済と復旧」を掲げ、かつ機能として「インシデント対応能力」を備え、かつ文化として「互恵主義」を信条とするのが CSIRT である。

サイバーセキュリティの非ゼロ和ゲーム化を、換言すればグローバリゼーションの後退を指摘し、CSIRT 自身の「被害者救済と復旧」という目的と互恵主義の文化が共に揺らいでいることを解き明かした。CSIRT コミュニティは自らの目的を再定義することが求められている。そしてこのような変化は、サイバー空間における価値観が変化してきたことを物語っている。

第 2 節　本論文の課題

最後に、本論文に残された課題を明らかにしておきたい。

サイバー空間のトリレンマは、国際経済学の理論をサイバー空間に当てはめたものである。経済では通貨を、サイバー空間ではデータを、それぞれに限られた財を多く手中に収める戦いをしていると前提した。そのために民主主義と国家主権とグローバリゼーションという価値が必要とされていることは、繰り返し論じてきた。またこの 3 つ価値観のいずれか 2 つが実現した場合について、第 2 章第 6 節「待ち受ける 3 つのシナリ

オ」で論じた。この手続きをもってそこにトリレンマがあると主張している。3 つの価値観がこれまでの社会で並立したことはないが、それが今後も起こりえないと論証するだけのデータを提示できていない。

次に情報拡散国家、情報支配国家、グローバルテックカンパニーという 3 つのグループについてはいくつか課題が残されている。まず、情報拡散国家の中でも、例えばオランダとフランスのスタンスは全く同一ではない。両者ともに民主主義の確保を求めるが、その次に重要になるのはオランダにとってはグローバリゼーションであり、フランスにとっては国家主権となる。同様に同じ情報支配国家に分類した中国とロシアの戦略は異なり、同じグローバルテックカンパニーに分類したアマゾン社とファーウェイ社の戦略は異なる。本論文が目標とした単純化した共通の価値観は、個々のアクターの行動の複雑さを捉えきれていない可能性が残されている。

また、グローバルテックカンパニーについては、これをサイバー空間の秩序を担うものとして論じる研究が少なく、情報拡散国家や情報支配国家との比較において曖昧さが残る。第 4 章にあるように「世界の多数の国において経済活動を行い、且つ情報通信技術分野で競争力を持つ企業のこと」と定義して論じてきた。多数の国とは具体的にどのくらいか、競争力を持つとは具体的にどのような状態か、考察は発展の途上にある。また、本論文では米国のテックカンパニーと中国のテックカンパニーも経済的利益の最大化を追求するグループとして、まとめて論じることができるという立場をとってきた。中国政府と中国のテックカンパニーの関係をより明らかにし、中国のテックカンパニーも利益を追求していることを証明することは現時点で十分でない。グローバルテックカンパニーの行動については、情報支配国家以上に厚いベールに包まれていることがある。例えば、グーグル社が自社の顧客のデータをどの国の領土に保存しているか、頑なに開示しないのはその際たる例である。今後、グローバルテックカンパニーによる情報開示が進むことを期待する。

科学技術と国際政治の複合領域としてサイバーセキュリティの問題をここまで論じてきた。本論文では一貫して技術者が、客観的な事実に基づいた情報を意思決定者に供給することが最良というという、伝統的な前提に立脚している。環境問題、防災問題に象徴されるように、体系の不確実性が高く、決定に関する利害関係が高い状況において、科学的・技術的な分析は必ずしも良い社会的な意思決定を保証するものでない。ポスト・ノーマル・サイエンスなどとよばれる、科学そのものの変質がサイバーセキュリティガバナンスにどう影響するか、さらなる考察を要する。

参考文献

英文

Arterton, F. Christopher. 1988. “Political Participation and ‘Teledemocracy.’” *PS: Political Science and Politics* 21 (3): 620–27.

The Attorney General Jeremy Wright. 2018. “Speech: Cyber and International Law in the 21st Century.” GOV.UK. Retrieved (https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century).

Awan, Jawad and Shahzad Memon. 2015. “Threats of Cyber Security and Challenges for Pakistan.” *Conference on Cyber Warfare and Security* (August): 425–31.

Azmi, Riza, William Tibben, and Khin Than Win. 2016. “Motives behind Cyber Security Strategy Development : A Literature Review of National Cyber Security Strategy.” in *Australian Conference on Information System*.

Bailey, Ronald. 2019. “Do We Need a World Data Organization? - Democratic President Hopeful Andrew Yang Think So. -.” Reason.Com.

Barlow, John Perry. 1996. “A Declaration of the Independence of Cyberspace Governments.”

Bartholomew, Brian and Juan Andres Guerrero-Saade. 2016. “Wave Your False Flags Deception Tactics Muddying Attribution in Targeted Attacks.” pp. 1–11 in *Virus Bulletin*.

Barzashka, Ivanka. 2013. “Are Cyber-Weapons Effective?” *The RUSI Journal* 158 (2): 48–56.

Benn, Tony and Chris Mullin. 1981. *Arguments for Democracy.* Jonathan Cape.

Berg, Bibi van den and Esther Keymolen. 2017. “Regulating Security on the Internet: Control versus Trust.” *International Review of Law, Computers and Technology* 31 (2): 188–205.

Berger, Andrea, Cameron Trainer, Shea Cotton, and Catherine Dill. 2018. “The Shadow Sector : North Korea’s Information Technology Networks.” *James Martin Center for Nonproliferation Studies* (36): 10. Retrieved December 4, 2019 (https://www.nonproliferation.org/wp-content/uploads/2018/05/op36-the-shadow-sector.pdf).

Betts, Richard K. 1978. “Analysis, War, and Decision: Why Intelligence Failures Are Inevitable.” *World Politics* 31 (1): 61–89.

Birnbaum, Michael. 2013. “Germany Looks at Keeping Its Internet, e-Mail Traffic inside Its Borders.” *The Washington Post*. Retrieved December 4, 2019 (https://www.washingtonpost.com/world/europe/germany-looks-at-keeping-its-

internet-e-mail-traffic-inside-its-borders/2013/10/31/981104fe-424f-11e3-a751-f032898f2dbc_story.html).

Bolding, Christopher and Donald Clarke. 2019. "Who Owns HUAWEI?" Retrieved December 4, 2019 (https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3372669).

Bradshaw, Samantha. 2015. *Combatting Cyber Threats: CSIRTs and Fostering International Cooperation on Cybersecurity*.

Braithwaite, John and Peter Drahos. 2000. *Global Business Regulation*. Cambridge University Press.

Bremmer, Ian. 2010. *The End of the Free Market: Who Wins the War Between States and Corporations?* Kindle Edi. Portfolio.

Broeders, Dennis. 2015. *The Public Core of the Internet: An International Agenda for Internet Governance.* Amsterdam: Amsterdam University Press.

Broeders, Dennis. 2017. "Aligning the International Protection of 'the Public Core of the Internet' with State Sovereignty and National Security." *Journal of Cyber Policy* 2 (3): 366–76.

Buchanan, Ben. 2017. *The Cybersecurity Dilemma: Hacking, Trust and Fear Between Nations*. Kindle Edi. Oxford University Press.

Burt, Tom. 2019. "ElectionGuard Available Today to Enable Secure, Verifiable Voting." Microsoft on the Issues. Retrieved January 13, 2020 (https://blogs.microsoft.com/on-the-issues/2019/09/24/electionguard-available-today-to-enable-secure-verifiable-voting/).

C-SPAN.org. 2017. "Director Comey Remarks at Cybersecurity Conference." C-SPAN.Org. Retrieved December 4, 2019 (https://www.c-span.org/video/?424885-2/director-comey-remarks-cybersecurity-conference).

Caldwell, Tracey. 2014. "Call the Digital Fire Brigade." *Network Security* 2014 (3): 5–8.

Canada. 2010. "Canada's Cyber Security Strategy for a Stronger and More Prosperous Canada."

Cave, Danielle, Samantha Hoffman, Alex Joske, Fergus Ryan, and Elise Thomas. 2019. "Mapping China's Technology Giants." *Australian Strategic Policy Institute* (15). December 4, 2019 (https://www.aspi.org.au/report/mapping-chinas-tech-giants).

Center for Long-Term Cybersecurity. 2016. *Cybersecurity Futures 2020*.

Chaudhary, Tarun, Jenna Jordan, Michael Salomone, and Phil Baxter. 2018. "Patchwork of Confusion: The Cybersecurity Coordination Problem." *Journal of Cybersecurity* 4 (1): 1–13.

Cheng, Dean. 2016. *Cyber Dragon: Inside China's Information Warfare and Cyber Operations*. Kindle Edi. Praeger.

China Institute of Contemporary International Relations, Shanghai Academy of Social Sciences, and Wuhan University. 2019. *Sovereignty in Cyberspace: Theory and Practice*.

Choucri, Nazli, Stuart Madnick, and Jeremy Ferwerda. 2014. "Institutions for Cyber Security: International Responses and Global Imperatives." *Information Technology for Development* 20 (2): 96–121.

Cohen, Julie E. 2017. "Law for the Platform Economy." *U.C. Davis Law Review* 51 (133): 1–55.

Connell, Michael and Sarah Vogler. 2017. "Russia's Approach to Cyber Warfare." *Centre for Naval Analysis Occasional Paper Series* (March): 32.

Contractfortheweb.org. 2019. "Contract for the Web." Retrieved December 4, 2019 (https://contractfortheweb.org/).

Crick, Bernard. 2002. *Democracy : A Very Short Introduction*. Oxford University Press.

Cuihong, Cai. 2018. "China and Global Cyber Governance: Main Principles and Debates." *Asian Perspective* 42 (4): 647–62.

Cybersecurity Tech Accord. 2018. "Cybersecurity Tech Accord." Retrieved December 4, 2019 (https://cybertechaccord.org/accord/).

Dahl, Robert A. 2005. "What Political Institutions Does Large-Scale Democracy Require?" *Political Science Quarterly* 120 (2): 187–97.

Davis Cross, Mai'a. 2013. "Re-Thinking Epistemic Communities Twenty Years Later." *Review of International Studies* 39 (01): 137–60.

Deeks, Ashley. 2019. "A New Tool for Tech Companies: International Law." *Lawfare*. Retrieved December 4, 2019 (https://www.lawfareblog.com/new-tool-tech-companies-international-law).

Deibert, Ronald J. 2013. *Black Code: Surveillance, Privacy, and the Dark Side of the Internet*. Signal.

Deibert, Ronald J. 2019. "The Road to Digital Unfreedom: Three Painful Truths About Social Media." *Journal of Democracy* 30 (1): 25–39.

Denardis, Laura. 2015. *Global War For Internet Governance*. Yale University Press.

DHS and FBI. 2016. *GRIZZLY STEPPE – Russian Malicious Cyber Activity Summary(JAR-16-20296A)*.

Diamond, Larry. 2019. "The Road to Digital Unfreedom: The Threat of Postmodern Totalitarianism." *Journal of Democracy* 30 (1): 20–24.

Ebert, Hannes and Tim Maurer. 2013. "Contested Cyberspace and Rising Powers." *Third World Quarterly* 34 (6): 1054–74.

Eichensehr, Kristen E. 2017. "Public-Private Cybersecurity." *Texas Law Review* 95: 469–

538.
Elklit, Jørgen and Michael Maley. 2019. “Why Ballot Secrecy Still Matters.” *Journal of Democracy* 30 (3): 61–75.
ENISA. 2016. “National Cyber Security Strategies (NCSSs) Map.” Retrieved December 4, 2019 (https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map).
European Commission. 2013. “Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace.” *European Commission*. Retrieved December 4, 2019 (https://ec.europa.eu/digital-single-market/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security).
Fanchiotti, Vittorio and Jean Paul Pierini. 2012. “Impact of Cyberspace on Human Rights and Democracy.” pp. 49–60 in *International Conference on Cyber Conflict*.
Feakin, Tobias. 2013. “Playing Blind-Man’s Buff: Estimating North Korea’s Cyber Capabilities.” *International Journal of Korean Unification Studies* 22 (2): 63–90.
Finnemore, Martha and Duncan B. Hollis. 2017. “Constructing Norms for Global Cybersecurity.” *American Society of International Law* 110 (3): 425–79.
Finnemore, Martha and Kathryn Sikkink. 1998. “International Norm Dynamics and Political Change.” *International Organization* 52 (4): 887–917.
FIRST. 2017. “FIRST CSIRT Framework Version 1.1.” Retrieved December 4, 2019 (https://www.first.org/education/csirt_service-framework_v1.1).
FIRST. 2019. “Statement Regarding Huawei’s Suspension from the Forum of Incident Response and Security Teams (FIRST).” FIRST. Retrieved September 19, 2019 (https://www.first.org/newsroom/releases/20190918).
Flournoy, Michèle. 2018. “Battlefield Internet.” *Foreign Affairs*.
France. 2011. “Information Systems Defence and Security: France’s Strategy.”
France Diplomatie. 2018. “Paris Call: For Trust and Security in Cyberspace.” (November). Retrieved December 4, 2019 (https://www.diplomatie.gouv.fr/IMG/pdf/paris_call_cyber_cle443433-1.pdf).
Fukuyama, Francis. 1993. *The End of History and the Last Man*. Kindle Edi. Penguin.
Giles, Keir. 2012. “Russia’s Public Stance on Cyberspace Issues.” pp. 63–75 in *International Conference on Cyber Conflict*.
Giles, Keir. 2015. “Russia and Its Neighbours: Old Attitudes, New Capabilities.” *Cyber War in Perspective: Russian Aggression against Ukraine* 19–28.
GIP Digital Watch observatory for Internet governance and digital policy. 2019. “UN GGE.” Retrieved December 4, 2019 (https://dig.watch/processes/ungge).
Global Commission on the Stability of Cyberspace. 2017. *CALL TO PROTECT THE PUBLIC*

CORE OF THE INTERNET. New Dehli.

Global Commission on the Stability of Cyberspace. 2018a. *Call to Protect the Electoral Infrastructure*. Bratislava.

Global Commission on the Stability of Cyberspace. 2018b. *Norm Package Singapore*.

Global Commission on the Stability of Cyberspace. 2019. *Advancing Cyberstability.*

Grumbach, Stephane. 2013. "The Stakes of Big Data in the IT Industry: China as the next Global Challenger?" *The 18th International Euro-Asia …* 2013: 1–15.

Grunow, Florian and Niklaus Schiess. 2017. "TR17 - Exploring North Korea's Surveillance Technology." *Troopers*. Retrieved December 4, 2019 (https://www.youtube.com/watch?v=xyPft_hOU64).

Haas, Peter M. 1992. "Introduction : Epistemic Communities and International Policy Coordination." *International Organization* 46 (1): 1–35.

Hathaway, Melissa E. and Alexander Klimburg. 2012. "Preliminary Considerations: On National Cyber Security." in *National Cyber Security Framework Manual*, edited by A. Klimburg. Tallinn, Estonia: NATO CCD COE Publications.

Healey, Jason. 2011. "The Spectrum of National Responsibility for Cyberattacks." *Brown Journal of World Affairs* 18 (1): 57–70.

Healey, Jason. 2012. "When ' Not My Problem' Isn't Enough : Political Neutrality and National Responsibility in Cyber Conflict." pp. 21–33 in *International Conference on Cyber Conflict*.

Healey, Jason. 2013. *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012*. Arlington: Cyber Conflict Studies Association.

Healey, Jason and Robert K. Knake. 2018. *Zero Botnets, Building a Global Effort to Clean Up the Internet*. the Council on Foreign Relations.

Hearn, Kay, Patricia A. H. Williams, and Rachel J. Mahncke. 2010. "International Relations and Cyber Attacks: Official and Unofficial Discourse." pp. 7–12 in *the Proceedings of the 11th Australian Information Warfare and Security Conference, Edith Cowan University, Perth Western*.

Heinegg, Wolff Heintschel von. 2012. "Legal Implications of Territorial Sovereignty in Cyberspace." pp. 7–19 in *International Conference on Cyber Conflict*.

Henni, Adrien. 2014. "New Personal Data Storage Rules to Affect Both Foreign and Domestic Players – but Still No 'Chinese Wall' Surrounding Russia." *East-West Digital News*. Retrieved December 4, 2019 (http://www.ewdn.com/2014/07/12/new-personal-data-storage-rules-to-affect-both-foreign-and-domestic-players-but-no-chinese-wall-surrounding-russia/).

Henriksen, Anders. 2019. "The End of the Road for the UN GGE Process: The Future

Regulation of Cyberspace." *Journal of Cybersecurity* 5 (1): 1–9.

Herder, Janosik. 2019. "The Power of Platforms - How Biopolitical Companies Threaten Democracy." *Public Seminar*. Retrieved December 4, 2019 (http://www.publicseminar.org/2019/01/the-power-of-platforms/).

Hill, Jonah Force. 2012. "Internet Fragmentation: Highlighting the Major Technical, Governance and Diplomatic Challenges for U.S Policy Makers." *Harvard Kennedy School Belfer Center.* Retrieved December 4, 2019 (https://www.belfercenter.org/sites/default/files/legacy/files/internet_fragmentation_jonah_hill.pdf).

Hodge, Nathan and Many Ilyushina. 2019. "Putin Signs Russian Sovereign Internet Law." *CNN*. Retrieved December 4, 2019 (https://edition.cnn.com/2019/05/01/europe/vladimir-putin-russian-independent-internet-intl/index.html).

Hoffman, Paul and Susan Harris. 2006. "RFC4677 The Tao of IETF - A Novice's Guide to the Internet Engineering Task Force." *IETF*. Retrieved December 4, 2019 (https://tools.ietf.org/html/rfc4677).

Hollis, Duncan B. 2011. "An E-SOS for Cyberspace." *Harvard International Law Journal* 52 (2): 373–432.

Horenbeeck, Maarten Van. 2019. "Cybersecurity Agreements: Background Paper to the IGF Best Practices Forum On." Retrieved December 4, 2019 (https://www.intgovforum.org/multilingual/filedepot_download/4904/1658).

Howard, Philip N., John Kelly, Camille François, John Kelly, and Camille Francois. 2019. The IRA , Social Media and Political Polarization in the United States , 2012-2018.

Hughes, Rex. 2009. "Towards a Global Regime for Cyber Warfare." in *the Conference on Cyber Warfare 2009*, edited by C. Czosseck and K. Geers. CCD COE Publications & IOS press.

Hunt, Jeremy. 2019. "Deterrence in the Cyber Age: Foreign Secretary's Speech." *GOV.UK*. Retrieved December 4, 2019 (https://www.gov.uk/government/speeches/deterrence-in-the-cyber-age-speech-by-the-foreign-secretary).

Hurel, Louise Marie and Mauricio Santoro. 2017. "Brazil, China and Internet Governance: Mapping Divergence and Convergence." Retrieved December 4, 2019 (http://web.isanet.org/Web/Conferences/HKU2017-s/Archive/f2ab8861-f5a8-44bb-8975-97ff50144e7b.pdf).

ICANN. 2013. "One World. One Internet." *ICANN*. Retrieved December 4, 2019 (https://www.icann.org/en/system/files/files/ecosystem-06feb13-en.pdf).

Ikenberry, John G. 2001. *After Victory: Institutions, Strategic Restraint, and the Rebuilding of Order After Major Wars.* Princeton, New Jersy: Princeton University Press.

Internet Governance Forum. 2014. "Best Practice Forum on Establishing and Supporting Computer Security Incident Response Teams (CSIRT) for Internet Security." Retrieved December 4, 2019 (http://www.intgovforum.org/cms/documents/ best-practice-forums/establishing-and-supporting-computer-emergency-response-teams-certs-for-internet- security/409-bpf-2014-outcome-document-computer-security-incident-response-teams/file).

Ito, Yurie. 2014. "BEST PRACTICES FOR MAKING CYBER SPACE SAFE AND SECURE." *Internet Governance Forum*. Retrieved December 4, 2019 (https://www.intgovforum.org/cms/documents/best-practice-forums/establishing-and-supporting-computer-emergency-response-teams-certs-for-internet-security/198-apcert-best-practices-for-making-cyber-space-safe-and-secure/file).

Jervis, Robert. 1978. "Cooperation Under the Security Dilemma." *World Politics* 30 (2): 167–214.

Kagan, Robert. 2019a. "Dictators Have Reemerged as the Greatest Threat to the Liberal Democratic World." *The Washington Post*, March 14.

Kagan, Robert. 2019b. *The Strongmen Strike Back*. Brookings Policy Brief.

Kalathil, Shanthi and Taylor C. Boas. 2003. *Open Networks, Closed Regimes*. Washington D.C.: Carnegie Endowment for International Peace.

Kavanagh, Camino and Daniel Stauffacher. 2013. *Confidence Building Measures and International Cybersecurity*.

Kettemann, Matthias C. and Stephan Dreyer. 2019. *BUSTED The Truth About The 50 Most Common Internet Myths.* Hamburg, Germany: Verlag Hans-Bredow-Institut.

Khanna, Parag. 2017. *Technocracy in America: Rise of the Info-State*. Kindle Edi. CreateSpace Independent Publishing Platform.

Kim, Eugene. 2014. "North Korean Defector Jang Se Yul Trained WIth Hackers." *Business Insider*. Retrieved December 4, 2019 (https://www.businessinsider.com/north-korean-defector-jang-se-yul-trained-with-hackers-2014-12).

King, Gary, Jennifer Pan, and Margaret E. Roberts. 2013. "How Censorship in China Allows Government Criticism but Silences Collective Expression." *American Political Science Review* 107 (2): 326–43.

Kleinwachter, Wolfgang. 2013. "Internet Governance Outlook 2013 : 'Cold Internet War' or 'Peaceful Internet Coexistence'?" *CircleID*. Retrieved April 15, 2019 (http://www.circleid.com/posts/20130103_internet_governance_outlook_2013/).

Klimburg, Alexander. 2013. "The Internet Yalta." *Center for a New American Security*.

Retrieved December 23, 2019 (https://www.cnas.org/publications/reports/the-internet-yalta).

Klimburg, Alexander and Hugo Zylberberg. 2015. *Cyber Security Capacity Building : Developing Access*. Oslo, Norway: Norwegian Institute of International Affairs.

Komiyama, Koichiro. 2019. "The Information Technology Iundustry in North Korea." *Keio University Global Research Institute* (4). Retrieved December 4, 2019 (http://www.kgri.keio.ac.jp/en/docs/S180620190226.pdf).

Kosinski, Michal, David Stillwell, and Thore Graepel. 2013. "Private Traits and Attributes Are Predictable from Digital Records of Human Behavior." *Proceedings of the National Academy of Sciences of the United States of America* 110 (15): 5802–5.

Kramer, Franklin, Stuart H. Starr, and Larry Wentz, eds. 2009. *Cyberpower and National Security*. Kindle Edi. Potomac Books, Inc.

Kretchun, Nat and Jane Kim. 2012. *A QUIET OPENING North Koreans in a Changing Media Environment*.

Kretchun, Nat, Catherine Lee, and Seamus Tuohy. 2015. *Compromising Connectivity, Information Dynamics Between The State And Society In A Digitizing North Korea*.

Kurbalija, Jovan. 2016. *An Introduction to Internet Governance (7th Edition)*. DiploFoundation.

Lau, Ashley. 2014. "Cisco Chief Urges Obama to Curb NSA Surveillance Activity." *Reuters*. Retrieved December 4, 2019 (https://www.reuters.com/article/us-cisco-systems-nsa/cisco-chief-urges-obama-to-curb-nsa-surveillance-activity-idUSBREA4H0C720140518).

Lechtik, Mark and Michael Kajiloti. 2018. "SiliVaccine: Inside North Korea's Anti-Virus." Retrieved December 4, 2019 (https://research.checkpoint.com/silivaccine-a-look-inside-north-koreas-anti-virus/).

Lee, Kai-Fu. 2018. *AI Superpowers: China, Silicon Valley, and the New World Order.* Kindle Edi. Houghton Mifflin Harcourt.

Lessig, Lawrence. 1998. "The New Chicago School." *Journal of Legal Studies* 27 (S2): 661–91.

Lessig, Lawrence. 2006. *CODE Version 2.0*. Vol. 346. BASIC BOOKS.

Levitsky, Steven and Daniel Ziblatt. 2018. *How Democracies Die: What History Reveals About Our Future.* Penguin.

Lewis, James Andrew. 2018. "State Practice and Precedent in Cybersecurity Negotiations." *Center for Strategic and International Studies*. Retrieved December 4, 2019 (https://www.csis.org/analysis/state-practice-and-precedent-cybersecurity-negotiations).

Li, Vector Guo, Matthew Dunn, Paul Pearce, Damon Mccoy, Geoffrey M. Voelker, Stefan Savage, and Kirill Levchenko. 2019. “Reading the Tea Leaves : A Comparative Analysis of Threat Intelligence.” *28th USENIX Security Symposium*.

Libra Association. 2019. “Libra White Paper.” Retrieved December 4, 2019 (https://libra.org/en-US/white-paper/).

Luiijf, Eric, Kim Besseling, and Patrick De Graaf. 2013. “Nineteen National Cyber Security Strategies.” *International Journal of Critical Infrastructures* 9 (Nos.1/2): 3–31.

Macron, Emmanuel. 2018. “IGF 2018 Speech.” *Internet Governance Forum*. Retrieved December 4, 2019 (http://www.intgovforum.org/multilingual/content/igf-2018-speech-by-french-president-emmanuel-macron).

Mandiant. 2013. *APT1 - Exposing One of China’s Cyber Espionage Units* -.

Mansourov, Alexandre Y. 2005. *BYTES AND BULLETS: Information Technology Revolution and National Security on the Korean Peninsula*. Honolulu, Hawaii: the Asia-Pacific Center for Security Studies.

Mansourov, Alexandre Y. 2011. *North Korea on the Cusp of Digital Transformation*.

Manyika, James, Jacques Bughin, Susan Lund, Olivia Nottebohm, David Poulter, Sebastian Jauch, and Sree Ramaswamy. 2014. “Global Flows in a Digital Age: How Trade, Finance, People, and Data Connect the World Economy.” *McKinsey Global Institute*. Retrieved December 4, 2019 (https://www.mckinsey.com/business-functions/strategy-and-corporate-finance/our-insights/global-flows-in-a-digital-age).

Maurer, Tim. 2016. “‘Proxies’ and Cyberspace.” *Journal of Conflict and Security Law* 21 (3): 383–403.

Maurer, Tim. 2017. “Contested Governance: Internet Governance and Cybersecurity.” pp. 29–32 in *Innovations in Global Governance - Peace-Building, Human Rights, Internet Governance and Cybersecurity, and Climate Change* -. The Council on Foreign Relations.

Maurer, Tim and Robert Morgus. 2014. “Compilation of Existing Cybersecurity and Information Security Related Definitions.” *New America*. Retrieved December 4, 2019 (https://www.newamerica.org/cybersecurity-initiative/policy-papers/compilation-of-existing-cybersecurity-and-information-security-related-definitions/).

Maynes, Charles. 2014. “Russia Tightens Internet Screws with ′server Law′.” *DW*. Retrieved December 4, 2019 (https://p.dw.com/p/1Cb9E).

Menn, Joseph. 2013. “Exclusive: Secret Contract Tied NSA and Security Industry Pioneer.” *Reuters*. Retrieved December 4, 2019 (https://www.reuters.com/article/us-usa-security-rsa/exclusive-secret-contract-tied-nsa-and-security-industry-pioneer-

idUSBRE9BJ1C220131220).

Microsoft. 2014. *Cyberspace 2025*.

Min, Jaewon. 2018a. "Malware on Google Play Targets North Korean Defectors." *McAfee Blog*. Retrieved December 4, 2019 (https://securingtomorrow.mcafee.com/mcafee-labs/malware-on-google-play-targets-north-korean-defectors/).

Min, Jaewon. 2018b. "North Korean Defectors and Journalists Targeted Using Social Networks and KakaoTalk." *McAfee Blogs*. Retrieved December 4, 2019 (https://securingtomorrow.mcafee.com/mcafee-labs/north-korean-defectors-journalists-targeted-using-social-networks-kakaotalk/).

Min, Kyoung Sik, Seung Woan Chai, and Mijeong Han. 2015. "An International Comparative Study on Cyber Security Strategy." *International Journal of Security and Its Applications* 9 (2): 13–20.

Ministry of Foreign Affairs - the People's Republic of China. 2017. "International Strategy of Cooperation on Cyberspace." Retrieved December 4, 2019 (https://www.fmprc.gov.cn/mfa_eng/wjb_663304/zzjg_663340/jks_665232/kjlc_665236/qtwt_665250/t1442390.shtml).

Morgus, Robert, Isabel Skierka, Mirko Hohmann, and Tim Maurer. 2015. *National CSIRTs and Their Role in Computer Security Incident Response*.

Mueller, Milton. 2013. "Are We in a Digital Cold War?" Internet Governance Project. Retrieved April 15, 2019 (https://www.internetgovernance.org/2013/07/19/are-we-in-a-digital-cold-war/).

Mueller, Milton. 2017. *Will the Internet Fragment?: Sovereignty, Globalization and Cyberspace.* Cambridge, UK: Polity.

Mueller, Milton. 2018. *Sovereignty and Cyberspace : Institutions and Internet Governance (Essay from the Lecture at University of Indiana October 3rd 2018).*

Murphy, Craig N. 2000. "Global Governance : Poorly Done and Poorly Understood." *International Affairs* 76 (4): 789–803.

Nakashima, Ellen. 2017. "The NSA Has Linked the WannaCry Computer Worm to North Korea - The Washington Post." *The Washington Post*, June 14.

NATO Cooperative Cyber Defence Centre of Excellence. 2019. "Library - Strategic Cyber Security." Retrieved December 4, 2019 (https://ccdcoe.org/library/strategy-and-governance/).

Nocetti, Julien. 2015. "Contest and Conquest: Russia and Global Internet Governance." *International Affairs* 91 (1): 111–30.

Novak, Matt. 2019. "New Zealand's Prime Minister Says Social Media Can't Be 'All Profit, No Responsibility.'" Gizmode. Retrieved January 13, 2020

(https://gizmodo.com/new-zealands-prime-minister-says-social-media-cant-be-a-1833398451).

Nye, Joseph S. 2010. "Cyber Power." *Belfer Center for Science and International Affairs* (May): 1–31.

Nye, Joseph S. 2014. "The Regime Complex for Managing Global Cyber Activities." *Center for International Governance and Innovation (CIGI) Publications* (1): 1–15.

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*. Organization for Security and Co-operation in Europe Parmanent Council.

Panda, Ankit. 2018. "Exclusive: Revealing Kangson, North Korea's First Covert Uranium Enrichment Site." *The Diplomat*.

Park, Chan-Mo. 2015. "North Korea" edited by K. Chon. *An Asia Internet History – Second Decade (1991-2000)*. Retrieved December 4, 2019 (https://sites.google.com/site/internethistoryasia/book2).

Perlroth, Nicole and John Markoff. 2013. "N.S.A. May Have Hit Internet Companies at a Weak Spot." *The New York Times*. Retrieved December 4, 2019 (https://www.nytimes.com/2013/11/26/technology/a-peephole-for-the-nsa.html).

President of Russia. 2016. "Transcript: Plenary Session of St Petersburg International Economic Forum." *Kremlin.Ru.* Retrieved February 17, 2020 (http://en.kremlin.ru/events/president/news/52178).

Qiang, Xiao. 2019. "The Road to Digital Unfreedom: President Xi's Surveillance State." *Journal of Democracy* 30 (1): 53–67.

Ravetz, J. R. 1999. "What Is Post-Normal Science." *Futures* 31 (7): 647–53.

Raymond, Mark. 2016. "Managing Decentralized Cyber Governance: The Responsibility to Troubleshoot." *Strategic Studies Quarterly* 10 (4): 123–49.

Richmond, Jake. 2015. "The Next Step in the Cybersecurity Plan." *CHIPS, The Department of the Navy's Information Technology Magazine*. Retrieved December 4, 2019 (https://www.doncio.navy.mil/CHIPS/ArticleDetails.aspx?ID=5997).

Rid, Thomas. 2011. "Cyber War Will Not Take Place." *Journal of Strategic Studies* 34 (March 2013): 37–41.

Rid, Thomas and Ben Buchanan. 2015. "Attributing Cyber Attacks." *The Journal of Strategic Studies* 38: 1–2.

Rid, Thomas and Peter McBurney. 2012. "Cyber-Weapons." *The RUSI Journal* 157 (1): 6–13.

Rodrik, Dani. 2012. *The Globalization Paradox: Why Global Markets, States, and Democracy*

Can't Coexist. Kindle Edi. OUP Oxford.

Roose, Kevin. 2019. "A Mass Murder of, and for, the Internet -." The New York Times. Retrieved January 13, 2020 (https://www.nytimes.com/2019/03/15/technology/facebook-youtube-christchurch-shooting.html).

Ruggie, John Gerard. 1992. "Multilateralism : The Anatomy of an Institution." *International Organization* 46 (3): 561–98.

Sang-ho, Song. 2014. "N. Korea Bolsters Cyberwarfare Capabilities." *Korea Herald*, July 27.

Sanger, David E. 2018. *PERFECT WEAPON : War, Sabotage, and Fear in the Cyber Age.* Kindle Edi. Scribe Publications.

Schmitt, Michael. 2012. "' Attack ' as a Term of Art in International Law : The Cyber Operations Context." pp. 283–93 in *International Conference on Cyber Conflict*.

Schmitt, Michael. 2015. "In Defense of Due Diligence in Cyberspace." Yale Law Journal Forum 125: 68–81.

Schmitt, Michael N. and Liis Vihul. 2017. "Respect for Sovereignty in Cyberspace." *Texas Law Review* 95 (7): 1639–70.

Schneier, Bruce. 2015. "Did Carnegie Mellon Attack Tor for the FBI?" *Schneier on Security*. Retrieved December 4, 2019 (https://www.schneier.com/blog/archives/2015/11/did_carnegie-me.html).

Segal, Adam. 2016. *The Hacked World Order: How Nations Fight, Trade Maneuver, and Manipulate in the Digital Age*. Kindle Edi. PublicAffairs.

Segal, A. 2017. "Bridging the Cyberspace Gap - Washington and Silicon Valley -." *Prism* 7 (2): 67–77.

Shackelford, Scott J. 2013. "Toward Cyberpeace: Managing Cyberattacks through Polycentric Governance." *American University Law Review* 62: 1273–1365.

Shen, Ashley and Moonbeom Park. 2017. "A Deep Dive into the Digital Weapons of North Korean Cyber Army." in *hackinthebox*, edited by Hackinthebox.

Shenk, David. 1997. "Data Smog: Surviving the Info Glut." *Technology Review* 100 (4): 18–26.

Sherman, Justin. 2019. "Russia and Iran Plan to Fundamentally Isolate the Internet." *WIRED*. Retrieved December 4, 2019 (https://www.wired.com/story/russia-and-iran-plan-to-fundamentally-isolate-the-internet/).

Siemens AG. 2018. "Charter of Trust For a Secure Digital World." Retrieved December 4, 2019 (https://www.siemens.com/press/pool/de/feature/2018/corporate/2018-02-cybersecurity/charter-of-trust-e.pdf).

Skierka, Isabel, Robert Morgus, Mirko Hohmann, and Tim Maurer. 2015. *CSIRT Basics for*

Policy-Makers -The History, Types & Culture of Computer Security Incident Response Teams-.

Smith, Brad. 2017. "Microsoft and Facebook Disrupt ZINC Malware Attack to Protect Customers and the Internet from Ongoing Cyberthreats." *Microsoft on the Issues*. Retrieved December 4, 2019 (https://blogs.microsoft.com/on-the-issues/2017/12/19/microsoft-facebook-disrupt-zinc-malware-attack-protect-customers-internet-ongoing-cyberthreats/).

Smith, Brad and Carol Ann Browne. 2019. Tools and Weapons: The Promise and the Evil of the Digital Age. Kindle Edi. Hodder & Stoughton.

Snowden, Edward. 2019. *Parmanent Record*. Kindle Edi. Macmillan.

Staten, James. 2013. "The Cost of PRISM Will Be Larger Than ITIF Projects." *Forbes.Com*. Retrieved December 4, 2019 (https://www.forbes.com/sites/forrester/2013/08/15/the-cost-of-prism-will-be-larger-than-itif-projects/#2e699df5795f).

Stevens, Timothy and David Betz. 2013. "Analogical Reasoning and Cyber Security." *Security Dialogue* 44 (2): 147–64.

Stikvoort, Don. 2010. "SIM3 : Security Incident Management Maturity Model." (September 1): 1–11. Retrieved December 4, 2019 (https://www.terena.org/activities/tf-csirt/publications/SIM3-v15.pdf).

Stoll, Clifford. 1989. *The Cuckoo's Egg : Tracking a Spy through the Maze of Computer Espionage*. Kindle Edi. Pocket Books.

Sui, Dang-chen and Yihan Guan. 2018. "Research on 'Combination of Medical Treatment and Endowment' from the Perspective of Digital Economy." pp. 251–54 in *2nd International Conference on Education Innovation and Social Science (ICEISS 2018)*. Vol. 275. ATLANTIS PRESS.

Sulek, David and Ned Moran. 2009. "What Analogies Can Tell Us About the Future of Cybersecurity." in *the Conference on Cyber Warfare 2009*, edited by C. Czosseck and K. Geers. CCD COE Publications & IOS press.

Tabansky, Lior. 2016. "Cyber Power in the Changing Middle East." *Turkish Policy Quarterly* 107–14.

Tanczer, Leonie Maria, Irina Brass, and Madeline Carr. 2018. "CSIRTs and Global Cybersecurity: How Technical Experts Support Science Diplomacy." *Global Policy* 9 (November): 60–66.

TASS. 2019. "Society & Culture - Stable Runet Law Follows Global Information Security Trend, Says Expert." *TASS*. Retrieved December 4, 2019 (http://tass.com/society/1054641).

The Secretariat of the Internet & Jurisdiction Policy Network. 2019. “INTERNET & JURISDICTION GLOBAL STATUS REPORT 2019.” *Internet & Jurisdiction Policy Network.* Retrieved December 25, 2019 (https://www.internetjurisdiction.net/report/).

The White House. 2017. “Press Briefing on the Attribution of the WannaCry Malware Attack to North Korea.” *The White House*. Retrieved December 4, 2019 (https://www.whitehouse.gov/briefings-statements/press-briefing-on-the-attribution-of-the-wannacry-malware-attack-to-north-korea-121917/).

Tija, Paul. 2006. “North Korea : An Upcoming Software Destination Surprising Business Opportunities in Pyongyang.” Retrieved December 4, 2019 (http://www.nkeconwatch.com/wp-content/uploads/2007/03/IT_in_NKorea.pdf).

Tikk, Eneken, Kristine Hochannisyan, Mika Kerttunen, and Mirva Salminen. 2019. *Cyber Conflict Factbook: Effect-Creating State-on-State Cyber Operations.* Cyber Policy Institute.

Timberg, Craig. 2014. “U.S. Threatened Massive Fine to Force Yahoo to Release Data.” *The Washington Post*. Retrieved December 4, 2019 (https://www.washingtonpost.com/business/technology/us-threatened-massive-fine-to-force-yahoo-to-release-data/2014/09/11/38a7f69e-39e8-11e4-9c9f-ebb47272e40e_story.html).

Torbati, Yeganeh. 2012. “Iran, North Korea Agree to Cooperate in Science, Technology.” *Reuters*. Retrieved Retrieved December 4, 2019 (https://www.reuters.com/article/us-korea-north-iran-idUSBRE88005H20120901).

Triolo, Paul, Kevin Allison, Clarise Brown, and Kelsey Broderick. 2020. *The Digital Silk Road : Expanding China’s Digital Footprint.*

U.S. Department of Justice Federal Bureau of Investigation. 1998. *Terrorism in the United States*.

U.S. Department of Defense. 2015. “Drell Lecture: ‘Rewiring the Pentagon: Charting a New Path on Innovation and Cybersecurity.’” Retrieved December 4, 2019 (https://www.defense.gov/Newsroom/Speeches/Speech/Article/606666/drell-lecture-rewiring-the-pentagon-charting-a-new-path-on-innovation-and-cyber/).

U.S. Department of Defense. 2018. *Summary of 2018 National Defense Strategy of The United States of America.*

U.S. Senate Committee On Commerce Science and Transportation. 2018. “Complex Cybersecurity Vulnerabilities: Lessons Learned from Spectre and Meltdown - Hearings.” Retrieved December 4, 2019 (https://www.commerce.senate.gov/public/index.cfm/hearings?ID=77835497-

EC96-41E8-B311-5AF789F38422).

United Nations. 2015a. *A/70/174 Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*.

United Nations. 2015b. *A/RES/70/237 Developments in the Field of Information and Telecommunications in the Context of International Security*.

United Nations. 2018. *A/RES/73/266 Advancing Responsible State Behaviour in Cyberspace Inthecontext of International Security.*

United Nations. 2019. *A/C.3/74/L.11 Countering the use of information and communications technologies for criminal purposes.*

United States of America. 2009. "Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure."

US-CERT. 2018. "Malware Analysis Report (AR18-221A): MAR-10135536-17 – North Korean Trojan: KEYMARBLE." *US-CERT*. Retrieved December 4, 2019 (https://www.us-cert.gov/ncas/analysis-reports/AR18-221A).

Vilmer, Jean-Baptiste Jeangène, Alexandre Escorcia, Marine Guillaume, and Janaina Herrera. 2018. *Information Manipulation: A Challenge for Our Democracies*. Paris: the Policy Planning Staff (CAPS) of the Ministry for Europe and Foreign Affairs and the Institute for Strategic Research (IRSEM) of the Ministry for the Armed Forces.

Watson, Chloe. 2018. "The Key Moments from Mark Zuckerberg's Testimony to Congress." The Guardian. Retrieved January 13, 2020 (https://www.theguardian.com/technology/2018/apr/11/mark-zuckerbergs-testimony-to-congress-the-key-moments).

West Brown, Moira, Don Stikvoort, Klaus-Peter Kossakowski, Georgia Killcrece, Robin Ruefle, and Mark Zajicek. 2003. *Handbook for Computer Security Incident Response Teams (CSIRTs)*.

WSIS. 2005. "Tunis Agenda for the Information Society." ITU. Retrieved March 7, 2020 (https://www.itu.int/net/wsis/docs2/tunis/off/6rev1.html).

World Economic Forum. 2017. *The Global Risks Report 2017 12th Edition*. Geneva: World Economic Forum.

Xi, Jinping. 2015. "Remarks by H.E. Xi Jinping President of the People's Republic of China At the Opening Ceremony of the Second World Internet Conference." Retrieved December 4, 2019 (https://www.fmprc.gov.cn/mfa_eng/wjdt_665385/zyjh_665391/t1327570.shtml).

Zeng, Jinghan, Tim Stevens, and Yaru Chen. 2017. "China s Solution to Global Cyber Governance : Unpacking the Domestic Discourse of ' Internet Sovereignty .'" *Politics &*

Policy 45 (3): 432–64.
Zetter, Kim. 2014. *Countdown to Zero Day: STUXNET and the Launch of the World's First Digital Weapon*. Kindle Edi. Crown Publishers.
Ziolkowski, Katharina. 2012. "Ius Ad Bellum in Cyberspace – Some Thoughts on the ' Schmitt- Criteria ' for Use of Force." pp. 295–309 in *International Conference on Cyber Conflict*. Vol. 2.
Ziolkowski, Katharina, ed. 2013. *Peacetime Regime for State Activities in Cyberspace. International Law, International Relations and Diplomacy*. Tallinn: NATO CCD COE Publication.

和文

東浩紀. 2015. *サイバースペースはなぜそう呼ばれるか+ 東浩紀アーカイブス2*. Kindle Edi. 河出書房新社.
安全保障貿易情報センター. 2018. "<<概要解説>>北朝鮮の国際金融システムを悪用した外貨獲得." *CISTECジャーナル* (173): 100–103.
池島大策. 2013. グローバルコモンズとしての北極海と安全保障：国際法の視点から.
石丸次郎, リジンス. 2012. "拡大するパソコン・IT機器の個人利用." pp. 38–45 in *リムジンガン*. Vol. 6. アジアプレス・インターナショナル.
一般社団法人JPCERTコーディネーションセンター. 2008. "CSIRTマテリアル." Retrieved December 4, 2019 (https://www.jpcert.or.jp/csirt_material/).
岩本誠吾. 2014. "サイバー問題における国際法の課題（特別企画:サイバー戦争の実相）." *外交* 24: 88–91.
ロバート・ウィリアムズ. 2019. "米中貿易戦争とファーウェイ ー テクノロジー競争の政治学." *フォーリン・アフェアーズ・レポート* 70–76.
宇野常寛. 2020. *遅いインターネット*. 幻冬舎.
ウラジミール. 2003. *サイバー北朝鮮*. 白夜書房.
遠藤誉. 2018. "Huawei総裁はなぜ100人リストから排除されたのか？." *Yahooニュース*. Retrieved December 4, 2019 (https://news.yahoo.co.jp/byline/endohomare/20181230-00109633/).
遠藤誉. 2019. "中国政府が遂にHuaweiと組む――「５G+４K・８K」で." *Yahooニュース*. Retrieved December 4, 2019 (https://news.yahoo.co.jp/byline/endohomare/20190411-00121961/).
大木良子. 2018. "オンラインプラットフォームと競争." *Nextcom* 33: 12–21.
大場義洋, 勝部泰弘. 2005. "ネットワークアクセス認証プロトコルPANA." *東芝レビュ*

ー 60 (5).
大野哲哉. 2018. *通信の世紀 ー情報技術と国家戦略の150年史*. 新潮社.
岡部正勝. 2017. “連載:サイバースペースとセキュリティー 第3回 サイバー空間の脅威にどう立ち向かうか 法執行機関の闘い.” *情報管理* 59 (10): 683–89.
小川晃通. 2014. *アカマイ—知られざるインターネットの巨人*. KADOKAWA.
小野純子. 2017. “〈３〉 北朝鮮の核実験及び制裁をめぐる歴史と諸状況.” *CISTECジャーナル* (167): 151–62.
外務省. 2000. “グローバルな情報社会に関する沖縄憲章(仮訳).” 外務省. Retrieved December 4, 2019 (https://www.mofa.go.jp/mofaj/gaiko/summit/ko_2000/it1.html).
外務省. 2017. “米国による北朝鮮のサイバー攻撃に関する発表について（外務報道官談話）.” 外務省. Retrieved December 4, 2019 (https://www.mofa.go.jp/mofaj/press/danwa/page4_003563.html).
外務省. 2018. “中国を拠点とするAPT10といわれるグループによるサイバー攻撃について（外務報道官談話）.” 外務省. Retrieved December 4, 2019 (https://www.mofa.go.jp/mofaj/press/danwa/page4_004594.html).
加藤朗. 2015. “サイバー空間の安全保障戦略.” *戦略研究* 15: 3–24.
神里達博. 2015. “第1章 リスク社会における安全保障と専門知.” pp. 19–48 in *シリーズ日本の安全保障7 技術・環境・エネルギーの連動リスク*.
神谷万丈. 2009. “ポスト9・11の国際政治におけるパワー 変容と持続.” *国際問題* (586): 29–39.
川口貴久. 2013. “サイバー空間における「抑止」についての一考察： 国家安全保障政策の視点から.” 平成22年度「情報セキュリティに関する懸賞論文」受賞作品 13–23.
川口貴久. 2015. “米国におけるサイバー抑止政策の刷新.” *KEIO SFC JOURNAL* 15 (2): 78–96.
川口貴久. 2019. “サイバー空間における「国家中心主義」の台頭.” *国際問題* (683): 37–46.
神田英宣. 2018. “海底ケーブルの海洋管轄権 ― サイバー空間における防御機能の追求―.” 防衛大学校紀要(社会科学分冊) 117.
パラグ・カンナ（玉木悟 訳）. 2009. *「三つの帝国」の時代 アメリカ・EU・中国のどこが世界を制覇するか*. 講談社.
パラグ・カンナ（尼丁千津子, 木村高子 訳）. 2017. *接続性の地政学 グローバリズムの先にある世界 下巻*. 原書房.
菊池努. 1997. “アジア太平洋地域主義のメカニズムとプロセス -APEC・ARFを中心に-.” *国際政治* 114.

菊地毅. 2019. “膨張GAFA 国家が逆襲（分断の先に） - 富の流出歯止めへ 課税や規制の動き -.” 日本経済新聞 電子版, March 10.
スコット・ギャロウェイ（度会圭子 訳）. 2018. *The Four GAFA 四騎士が創り変えた世界*. 東洋経済新報社.
スティーブン・D・クラズナー. 2001. “第2章 グローバリゼーション論批判 主権概念の再検討.” pp. 45–68 in *グローバル・ガヴァナンス*, edited by 渡辺昭夫 and 土山實男. 東京大学出版会.
栗栖薫子. 1996. “欧州安全保障協力機構(CSCE)の人的次元 -レジーム論による考察-.” *国際政治* 139–57.
ジェイムズ・グリック（楡井光一 訳）. 2013. インフォメーション 情報技術の人類史. 新潮社.
経済産業省. 2019. “政策特集首脳会合だけじゃない「G20」 Vol.2 自由で公正なデータ流通の実現主導 世耕弘成経済産業大臣に聞く【前編】.” *METI Journal*. Retrieved December 25, 2019 (https://meti-journal.jp/p/5781-2/).
言論NPO. 2019. 第15回東京-北京フォーラム 2019年10月25日~27日（会議開催報告）.
小泉悠. 2019. *「帝国」ロシアの地政学 「勢力圏」で読むユーラシア戦略*. 東京堂出版.
ジャレッド・コーエン, エリック・シュミット（櫻井祐子 訳）. 2014. *第五の権力 ーGoogleには見えている未来*. ダイヤモンド社.
高坂正堯. 1966. *国際政治 - 恐怖と希望*. Kindle Edi. 中央公論社.
河野桂子. 2015. “サイバー・セキュリティに関する国際法の考察 ータリン・マニュアルを中心にー.” *戦略研究* 15: 25–46.
国連広報センター. 2019. “国連憲章テキスト(日本語版).” 国連広報センター. Retrieved December 4, 2019 (https://www.unic.or.jp/info/un/charter/text_japanese/).
小林良樹. 2008. “中国における「対日感情」に関する考察.” *アジア研究* 54 (4): 108.
小林良樹. 2012. “インテリジェンス・コミュニティに対する民主的統制の制度.” *国際政治* 167: 57–71.
ロバート・コヘイン,ジョセフ・ナイ（滝田賢治 訳）. 2012. *パワーと相互依存*. ミネルヴァ書房.
小宮山功一朗. 2019a. “サイバーセキュリティにおけるインシデント対応コミュニティの発展 - 目的、機能、文化から見るCSIRT -.” *情報通信学会誌* 37 (1): 13–23.
小宮山功一朗. 2019b. “北朝鮮の情報通信技術産業 -金正日がもたらしたいびつな成功と労働力余剰-.” *InfoCom REVIEW* 72: 17–29.
小宮山功一朗, 土屋大洋. 2018. “研究ノート: サイバーセキュリティ戦略の国際比較 ー目的と対象範囲に基づく四類型ー.” *グローバル・ガバナンス* 3 (4).
財団法人防衛調達基盤整備協会. 2009. カウンターインテリジェンスの最前線に位置す

る防衛関連企業の対策について.
エドワード・サイード（大橋洋一 訳）. 1998. *文化と帝国主義 1*. みすず書房.
サイバー救急センター LAC. 2019. サイバー救急センターレポート 仮想通貨を狙うサイバー攻撃の背後にある影.
財務省. 2017. “20か国財務大臣・中央銀行総裁会議声明（仮訳）（2017年3月17-18日於：ドイツ・バーデン=バーデン）.” 財務省. Retrieved December 4, 2019 (https://www.mof.go.jp/international_policy/convention/g20/170318.htm).
財務省. 2019. “ステーブルコインに関するG7作業グループ議長によるアップデート (仮訳).” 財務省. Retrieved December 4, 2019 (https://www.mof.go.jp/international_policy/convention/g7/cy2019/g7_20190719.htm).
佐々木孝博. 2012. “ロシアのサイバー戦略 ―「サイバー戦コンセプト」を中心に―.” *日本大学大学院総合社会情報研究科紀要* (13): 1–12.
佐々木孝博. 2013. “サイバー空間の施策に関するロシアと欧米諸国のアプローチ.” *日本大学大学院総合社会情報研究科紀要* (14): 1–12.
佐々木俊尚. 2013. *レイヤー化する世界*. Kindle Edi. 自主出版(Kindle Storeで販売).
キャス・サスティーン（石川幸憲 訳）. 2003. インターネットは民主主義の敵か. 毎日新聞社.
佐藤仁. 2018. “米中サイバーセキュリティ動向 -国際政治学の視座からの分析-.” *InfoCom REVIEW* 71: 50–68.
佐藤由紀子. 2010. “ロシアのメドベージェフ大統領、公式Twitterをスタート.” *ITmedia NEWS*. Retrieved December 4, 2019 (https://www.itmedia.co.jp/news/articles/1006/24/news034.html).
佐橋亮. 2020. “米中対立と日本: 関与から戦略的競争に移行する米を中心に.” *国際問題* 688: 5–17.
塩原俊彦. 2015. “サイバー空間と国家主権.” *境界研究* (5): 29–56.
塩原俊彦. 2019. *サイバー空間における覇権争奪 個人・国家・産業・法規制のゆくえ*. 社会評論社.
篠田英朗. 2007. *国際社会の秩序*. 東京大学出版会.
朱紅穎. 2018. “中国のサイバー戦略をめぐる国内政治.” 慶應義塾大学大学院政策・メディア研究科 修士論文（未公刊）.
ブルース・シュナイアー（池村千秋 訳）. 2016. *超監視社会: 私たちのデータはどこまで見られているのか?* Kindle Edi. 草思社.
クラウス・シュワブ. 2019. “デジタル世界に即した統治システムを ー 社会・経済のデジタル化を恩恵とするには.” *フォーリン・アフェアーズ・レポート* 3月号: 6–14.
神保謙, 阪田恭代, 佐橋亮, 高橋杉雄, 増田雅之, and 湯澤武. 2011. *アジア太平洋の地*

域安全保障アーキテクチャ -地域安全保障の重層的構造-.
鈴木一人. 2011. *宇宙開発と国際政治*. 岩波オンデマンド. 岩波書店.
鈴木一人. 2015. “序論 科学技術がもたらすリスクと「人間本位」の安全保障.” pp. 1–18 in *シリーズ日本の安全保障7 技術・環境・エネルギーの連動リスク*,. 岩波書店.
須田祐子. 2015. “サイバーセキュリティの国際政治.” *国際政治* 179.
須藤龍也. 2019. “「北朝鮮の犯行」装う? コインチェック事件、ロシア系関与か 北朝鮮説、韓国が示唆.” 朝日新聞, June 16.
スーザン・ストレンジ（西川潤, 佐藤元彦 訳）. 1994. *国際政治経済学入門–国家と市場*. 東洋経済新報社.
スーザン・ストレンジ（櫻井公人 訳）. 2011. *国家の退場 グローバル経済の新しい主役たち （岩波人文書セレクション）*. 岩波書店.
選択. 2019. “脱北「テロ組織幹部」が極秘来日中.” *選択* 45 (9): 32–33.
高野泰. 2007. “『サイバースペース独立宣言』10周年+α--アメリカ起源のネット文化とその行方.” *東京成徳大学人文学部研究紀要* 14: 77–94.
高橋杉雄. 2001. “情報革命と安全保障.” *防衛研究所紀要* 4 (2): 89–104.
高山巌. 2010. “ウエストファリア考 -「象徴的標識」の視点からの一試論 -.” *国際政治* 160: 48–63.
田川義博, 林紘一郎. 2017. “サイバーセキュリティのための情報共有と中核機関のあり方.” *情報セキュリティ総合科学* 9: 17–44.
武貞秀士. 2014. “北朝鮮の軍事戦略と日朝関係.” *海外事情* 62 (9): 2–17.
田所昌幸. 2020. “第2章 武器としての経済力とその限界 - 経済と地政学.” pp. 73–115 in *新しい地政学（*北岡伸一, 細谷雄一 編*）*. 東洋経済新報社.
田中栄一. 2014. “インターネットは誰のものか、自由とセキュリティーを巡る論議（前編）.” *ITUジャーナル* 44: 35–39.
田中宏明. 2011. “スーザン・ストレンジの国際政治経済学 ーリアリズム批判のリアリストー.” *宮崎公立大学人文学部紀要* 18 (1): 77–100.
田中道昭. 2017. *アマゾンが描く2022年の世界 すべての業界を震撼させる「ベゾスの大戦略」*. PHPビジネス新書. PHP研究所.
塚原東吾. 2017. “「メタ科学」へのエクササイズ:「科学の公共性」、「科学者の社会的責任論」、「2つの文化」などをめぐる最近の議論.” *21世紀倫理創成研究* 10: 46–74.
土屋大洋. 2007. *ネットワーク・パワー –情報時代の国際政治–*. NTT出版.
土屋大洋. 2013. “サイバースペースのガバナンス.” *平成25年度研究プロジェクト「グローバル・コモンズにおける日米同盟の新しい課題」分析レポート* 1–6.
土屋大洋. 2015a. “サイバーセキュリティとインテリジェンス機関.” *国際政治* 179: 44–56.

土屋大洋. 2015b. *サイバーセキュリティと国際政治*. 千倉書房.
土屋大洋. 2017. “大規模サイバー攻撃は本当に北朝鮮によるものか.” *東亜* 601: 6–7.
土屋大洋. 2018a. “サイバーに関する安全保障上の課題.” 首相官邸ホームページ. Retrieved December 4, 2019 (https://www.kantei.go.jp/jp/singi/anzen_bouei2/dai2/siryou3.pdf).
土屋大洋. 2018b. “現代の模範村、中国・烏鎮（ウーチン）で開かれた世界インターネット大会.” ニューズウィーク日本版. Retrieved December 4, 2019 (https://www.newsweekjapan.jp/tsuchiya/2018/11/post-31_1.php).
土山實男. 2014. *安全保障の国際政治学 - 焦りと傲り*. 第二版. 有斐閣.
坪内淳. 1996. “「信頼醸成」- 国際安全保障理論の新たな視角.” *早稲田政治公法研究* 51: 31–50.
坪内淳. 1997. “OSCEプロセスとASEAN -アジア太平洋の安全保障分析枠組への序説-.” *国際政治* 116.
太永浩. 2019. *三階書記室の暗号 北朝鮮外交秘録* Kindle Edi. 文藝春秋社.
グレゴリー・ディーエル. 2013. “英国のサイバーセキュリティ戦略 ― 脅威からリスクへの認識変化と組織的対応 ―.” 総務省調査研究.
遠山孝. 2019. “またしてもインターネットに政治主導で規制の動き、国連管轄の「IGF」はどこへ向かうのか？マクロン大統領の演説で沸き起こる波紋.” *INTERNET Watch*. Retrieved December 4, 2019 (https://internet.watch.impress.co.jp/docs/special/1171455.html).
独立行政法人国際協力機構. 2012. “PacCERTオフィスの仮オープンと業務開始.” Retrieved December 4, 2019 (https://www.jica.go.jp/project/fiji/002/news/20120712.html).
トレンドマイクロ フォワードルッキング スレット リサーチ チーム. 2017. “北朝鮮インターネット事情.” トレンドマイクロ セキュリティブログ. Retrieved December 4, 2019 (http://blog.trendmicro.co.jp/archives/16218).
ジョセフ・S・ナイ・ジュニア, ディヴィッド・A・ウェルチ（田中明彦, 村田晃嗣訳）. 2013. *国際紛争－理論と歴史［原書第9版］*. 有斐閣.
内閣サイバーセキュリティセンター. 2015. サイバーセキュリティ戦略.
中澤克二. 2018. *習近平帝国の暗号 2035*. 日本経済新聞社.
中田喜文. 2014. “インドのソフトウェア産業とソフトウェア技術者の現状.” 「日本のソフトウェア技術者の生産性及び処遇の向上効果研究：アジア, 欧米 諸国との国際比較分析のフレームワークを用いて」に関する成果報告書 95–108.
中谷和宏. 2019. “巻頭エッセイ: 国際機関をめぐる現代的位相.” *国際問題* 686: 1–4.
中満泉. 2019. “巻頭エッセイ: 多国間主義の現在と未来、日本への期待.” *国際問題* 678: 1–5.

西岡洋子. 2007. *国際電気通信市場における制度形成と変化―腕木通信からインターネット・ガバナンスまで*. 慶應義塾大学出版会.
西川輝. 2017. “ブレトンウッズ体制の再検討.” *歴史と経済* 234: 38–44.
西本逸郎. 2012. “情報セキュリティ 今後の考え方.” *情報の科学と技術* 62 (8).
日本経済新聞データエコノミー取材班. 2019. *データの世紀*. Kindle Edi. 日本経済新聞出版社.
日本シーサート協議会. 2007. “日本シーサート協議会とは.” Retrieved December 4, 2019 (https://www.nca.gr.jp/outline/).
日本シーサート協議会. 2011. “CSIRTスタータキット.” 1–34. Retrieved December 4, 2019 (http://www.nca.gr.jp/imgs/CSIRTstarterkit.pdf).
日本ネットワークセキュリティ協会 セキュリティ市場調査WG. 2018. “2017年度 国内情報セキュリティ市場調査（速報値）.” Retrieved December 4, 2019 (https://www.jnsa.org/result/2018/surv_mrk/).
河鐘基. 2017. “世界最強だった"北朝鮮の囲碁AI"の現状.” プレジデントオンライン. Retrieved December 4, 2019 (https://president.jp/articles/-/23667).
橋本靖明, 合田正利. 2005. “ルール・オブ・エンゲージメント(ROE) -その意義と役割-.” *防衛研究所紀要* 7 (2・3合併号).
浜田敬子. 2019. “【全文掲載】ファーウェイCEOインタビュー「我々は必ず頂点に登り詰める、そして生きて帰ってくる」.” *BUSINESS INSIDER JAPAN*. Retrieved December 4, 2019 (https://www.businessinsider.jp/post-190963).
林紘一郎. 2016. “サイバーセキュリティ事故情報共有のあり方 (How to Share Cybersecurity Incident Information).” *情報通信学会誌* 34 (3): 97–100.
林紘一郎. 2020. “サイバーセキュリティと国際法・国際政治.” *ITUジャーナル* 50 (1): 28–32.
ばるぼら. 2005. *教科書には載らないニッポンのインターネットの歴史教科書*. 翔泳社.
辺真一. 2019. “衝撃的な「駐スペイン北朝鮮大使館襲撃事件」の全容.” *Yahooニュース*. Retrieved December 4, 2019 (https://news.yahoo.co.jp/byline/pyonjiniru/20190402-00120641/).
平岩俊司. 2013. “北朝鮮・金正恩体制の「遺訓政治」と今後の展望 (朝鮮半島新情勢の構図).” *外交* 18: 108ー113.
平岩俊司. 2018. “公研セミナー、米朝会談後の北朝鮮情勢.” *公研* 56 (7): 56–83.
廣瀬陽子. 2018. *ロシアと中国 反米の戦略*. Kindle Edi. 筑摩書房.
藤巻裕之. 2018. “旧ソ連圏における多国間主義とサイバーセキュリティ.” *東海大学紀要政治経済学部* 50: 1–14.
フランス大統領府. 2019. “オンライン上のテロリズムと暴力的過激主義に対して行動するためのクライストチャーチ・コール.” 在日フランス大使館. Retrieved December

4, 2019 (https://jp.ambafrance.org/article14572).
フランス通信社. 2014. “「ネット版マグナカルタの制定を」、WWW考案者が提唱.” *AFPBB News*. Retrieved December 4, 2019 (https://www.afpbb.com/articles/-/3027287).
アーロン・L・フリードバーグ. 2018. “権威主義諸国の挑戦 中国、ロシアとリベラルな国際秩序への脅威.”
イアン・ブレマー（奥村準 訳）. 2015. *スーパーパワー ―Gゼロ時代のアメリカの選択*. 日本経済新聞出版社.
古川勝久. 2017a. *北朝鮮 核の資金源 ―「国連捜査」秘録―*. Kindle Edi. 新潮社.
古川勝久. 2017b. “東南アジアに潜む北朝鮮のネットワーク ― 迂回取引に巻き込まれるリスク.” *CISTECジャーナル* (171): 69–85.
ウルリッヒ・ベック（山本啓 訳）. 2014. *世界リスク社会 <叢書・ウニベルシタス 1004>*. 法政大学出版局.
細谷雄一. 2012. *国際秩序 - 18世紀ヨーロッパから21世紀アジアへ*. 中公新書. 中央公論新社.
前原透, 片岡徹也. 2003. *戦略思想家事典*. 芙蓉書房出版.
前村昌紀. 2018. “烏鎮サミット：ハイパージャイアント不在も5年目の風格.” *JPNIC Blog*. Retrieved December 4, 2019 (https://blog.nic.ad.jp/blog/wuzhen-summit-2018/).
牧野愛博. 2019. “盗聴率「100％」 世界と接続しない北朝鮮スマホ入手.” *朝日新聞DIGITAL*, July 24.
正村公宏. 1993. *産業主義を越えて*. 講談社.
益尾知佐子. 2019. *中国の行動原理 -国内潮流が決める国際関係-*. 中央公論新社.
真勢徹. 1989. “北朝鮮 (DPRK) の潅漑事情.” *農業土木学会誌* 57 (6): 541–44.
松本栄子. 2014. “米ドル決済システム構造に見る 経済制裁の有効性に関する考察.” pp. 77–94 in *第17回日本安全保障貿易学会研究大会*.
三菱重工. 2019. “三菱重工、サイバーセキュリティのCharter of Trust参加に関する覚書に署名.” Retrieved December 4, 2019 (https://www.mhi.com/jp/news/story/190219.html).
南山淳. 2015. “グローバル・ガバナンスとグローバルな統治性 ー主権/規範 構造としての概念ー.” *グローバル・ガバナンス* 2: 82–96.
宮岡勲. 2015. “軍事技術の同盟国への拡散.” *国際政治* 179: 69–82.
村上隆則. 2019. “「ネットは世の中変えないどころか、むしろ悪くしている」批評家・東浩紀が振り返る ネットコミュニティの10年.” *BLOGOS*. Retrieved December 4, 2019 (https://blogos.com/article/380108/).
村井純. 2019. “基調講演2「UNWIRED: インターネット社会への5Gインパクト」.” *情報通信学会誌* 37 (2): 66–69.

持永大, 村野正泰, 土屋大洋. 2018. *サイバー空間を支配する者 -21世紀の国家、組織、個人の戦略-*. 日本経済新聞出版社.
森健. 1996. “ネットワーク犯罪は防げるか.” pp. 170–74 in 別冊宝島262号 インターネットの激震. 宝島社.
八塚正晃. 2017. サイバー安全保障に対する中国の基本的認識（NIDSコメンタリー 60号）.
山口真典. 2013. *北朝鮮経済のカラクリ*. 日本経済新聞出版社.
山口英, 大林正英. 1999. “解説 JPCERT/CCの現状と展望.” *情報処理* 40 (3): 328–33.
山本武彦. 1986. “序・科学技術「革命」下の国際システム.” *国際政治* 83: 1–11.
山本達也. 2005. “政府によるインターネット・コントロールとイスラーム.” *KEIO SFC JOURNAL* 4: 54–74.
山本達也. 2006. “中東アラブ諸国におけるインターネット・コントロール政策の比較研究.” 慶應義塾大学大学院.
山本吉宣. 2008. *国際レジームとガバナンス*. 有斐閣.
湯川拓. 2011. “レジーム・セキュリティと国際制度.” *国際政治* 164: 58–71.
湯之上隆. 2019. “<1>米中ハイテク戦争と中国半導体産業.” *CISTECジャーナル* 179: 167–83.
横澤誠. 2019. “デジタル・エコノミーの地政学.” *外交* 55 (May/Jun): 32–37.
横江公美. 2008. *アメリカのシンクタンク*. ミネルヴァ書房.
横山恭三. 2016. “中国のサイバー能力の現状.” *鵬友* 42 (4).
吉田圭織. 2019. “北朝鮮、サイバー攻撃で仮想通貨5億ドル奪う 17~18年の国連報告入手.” 日本経済新聞, （2019年3月9日朝刊）.
リ・サンウ. 2001. “朝鮮民主主義人民共和国（北朝鮮）.” *ERINA REPORT* 43: 68.
ホワン・リンス（高橋進監 監訳）. 1995. 全体主義体制と権威主義体制. 法律文化社.
ローレンス・レッシグ（山形浩生 訳）. 2007. *CODE Version 2.0*. 翔泳社.
マーク・ローエンタール. 2011. *インテリジェンス―機密から政策へ*. 慶應義塾大学出版会.
ダニ・ロドリック（岩本正明 訳）. 2019. *貿易戦争の政治経済学:資本主義を再構築する*. Kindle Edi. 白水社.
ダニ・ロドリック（柴山桂太, 大川良文 訳）. 2014. *グローバリゼーション・パラドクス 世界経済の未来を決める三つの道*. 白水社.
渡辺昭夫, 土山實男. 2001. “序章 グローバル・ガヴァナンスの射程.” pp. 1–17 in *グローバル・ガヴァナンス*. 東京大学出版会.
渡部悦和. 2018. “〈1〉 中国が進めるAI軍事革命.” *CISTECジャーナル* (175): 76–86.

付録

第 1 節 アトリビューションについての小論

第 1 項 はじめに

核弾頭ミサイルを発射した国を特定するのは難しい作業ではない。現在、地球上に核保有国は 9 つしかない。放射性同位体の観測技術は向上し続けている。そして核保有国以外のテロリスト、犯罪集団がこれを使用する可能性は極めて低い。関わる組織、人員、要する費用などはいずれも膨大であり、行為を否認することは難しい。対して、サイバー空間においてサイバー攻撃の実行者を特定するプロセスについては未だ検討が始まったばかりである。

土屋（2015）によればアトリビューション問題とは「サイバー攻撃の主体が誰なのかという問題」であり、サイバーセキュリティをめぐる最大の問題の 1 つであるという。アトリビューションの難しさについて指摘する研究は数多く存在する。トマス・リッド（Thomas Rid）はアトリビューションが正しいのか、間違っているのかの二元論ではなく、「程度の問題」であると結論づけている（Rid & Buchanan 2015）。川口（2015）はこれに加えて、サイバー攻撃の行為者と責任ある主権国家の関係の立証の困難さをあげる。Nye（2017）は主たる問題を代理者（Proxy）と偽装（False Flag）に求めた。さらに複数の研究者[186]がアトリビューションの困難さなどを理由に責任ある注意（Due Diligence）を求めている。17 世紀のフーゴー・グローティウスまで遡るこの論理は、代

[186] 典型としては Healey（2011）があげられる。Healey は A 国におかれた B 国大使館に対して、民衆による投石が行われた場合、民衆の国籍の如何によらず A 国の保護責任を問われるのはしかたないというアナロジーを用いてサイバー攻撃についても各国政府が注意義務を持つと主張する。他に Schmitt（2015）、Hollis（2011）の論考も参照した。

理人によるサイバー攻撃がアトリビューションを難しくすることを指摘した。技術的側面に目を転じれば主に偽装の問題について、様々な難しさが指摘されている。

第２項 Q モデルとは

イギリスの研究者トーマス・リッドとベン・ブキャナンは「サイバー攻撃のアトリビューション（Attributing Cyber Attack）」という論文において、アトリビューションを決定する手法として「Q モデル」を提案した。Q モデルはアトリビューションのプロセスを技術レベル（タクティカル・テクニカル）と作戦レベル（オペレーション）と戦略レベル（ストラテジー）[187]の 3 つに分解し、それぞれのレベルについて異なる分析者、異なる視点、異なる分析対象、異なるアウトプットを要するとした。そして最後にコミュニケーションという作業があり、これもアトリビューションを決定する作業の一環であるとした。ここでは Q レベルを用いたアトリビューションについて理解を深めるため、Q モデルを表に変換した。

技術レベル（タクティカル・テクニカル）と作戦レベル（オペレーション）と戦略レベル（ストラテジー）の 3 つの異なるレベルのアトリビューション判定とコミュニケーションを要するというのが Q モデルの斬新な点であり、その違いについて、具体的に内容をみていきたい。

以下の「図表 付録 1」に示すとおり、技術レベルにおいては、「何が、どのように引

---

[187] Rid and Buchanan （2015）はアトリビューション決定の作業を戦略、作戦術、戦術という軍の階層的発想になぞらえて区分している。要すれば戦略とは戦争においてリソースをどう配分するかであり、戦術とはそのリソースをどのように用いるかということである。作戦術とは両者の中間に位置し、複数の戦術を有利にすすめるための技術であるとされている。戦争の規模が大きくなった近代になってロシアの軍人スヴェンチン・トリアンダフィーロフ等によって提唱され、発展してきた。しかしながら今日においても、作戦術と戦術の差異について統一見解は見当たらない。したがって本論文においてはタクティカルレベルを技術レベルと称し、作戦術、戦術という対比を用いないことにした。作戦術について前原＆片岡（2003）に頼った。

き起こされたのか。」を解説するためにフォレンジック技術者がデータ、文書、プロセスを対象に技術分析を行う。このレベルの分析の角度は当然高くなる。

次に作戦レベルでは、「誰が（問題の事象を）引き起こしたのか」という問いに答えるため、アナリストが対象の組織や個人と事象との関連を分析する。このレベルの分析でのアウトプットはいくつかの引き起こした組織・個人の仮説であり、確実性は中程度である。

最後に戦略レベルでのアトリビューションとは「なぜ引き起こされたのか」という問いに答えるために政治指導者レベルの分析を要する。ここでの分析の目的は対応方法、反撃手段を検討することである。

レベル	**技術レベル**	**作戦レベル**	**戦略レベル**
主たる担当者	フォレンジック技術者	アナリスト	リーダー
目的	技術分析	理解	対応/反撃
分析の対象	データ、文書、プロセス	組織、個人	（政府）
確実性	高い	中程度	低い
アウトプット	解説	仮説	推定
解決すべき疑問	何が、どのように引き起こされたのか。	誰が引き起こしたのか。	なぜ引き起こされたのか。

図表 付録 1 Q モデルにおける 3 つのレベル

Q モデルにおいて重要なのは、アトリビューションを上記 3 つのレベルに分類し、その作業の目的を明らかにする点にある。

第３項 アトリビューションの作業

具体的にアトリビューションの作業を行うにあたっては、分析の対象に対して、レベルに応じて以下の問いへの答えをまとめる。次の図表 付録 2 技術レベルの問いは技術レベルの、図表 付録 3 作戦レベルの問い
は技術レベルの、図表 付録 4 戦略レベルの問い
は戦略レベルの問いである。

個別の問い	IOC: : 捜査の出発点となったのは何か。原始的なインディケーターは何か。観測された活動は「疑わしいか」。既知の悪意あるプログラムが確認されているか。
	Entry: どのように侵入が発生したのか。悪用された脆弱性はなにか。ゼロデイ脆弱性は（いくつ）使用されたか。
	Targeting: 標的はなんであったのか。特定のマシン、特定のタイプの文書へのアクセスを試みたか。侵入が成功した後の攻撃者の動きはどのようなものか。
	Infrastructure: 攻撃に用いられたインフラの詳細。どのようなハードウェア、ソフトウェアが用いられたか。インフラの登録者（所有者）は誰か。共通のタグや、設定のテンプレートはあるか。
	Modularity: 攻撃に使用されたコードはモジュールに分解可能か。それぞれの作者は同じか。すでに出回っているものか、一から作成されたものか。
	Language: 攻撃に使用されたコード、関連するファイルから推定される攻撃発信源で使われる言語は何か。コードから固有の言語に依存する情報を表示するか。地域固有の文字列がファイルに含まれるか。
	Personas: 攻撃者はなんらかの仮名やグループ名を用いているか。過去に活動が観

	測されているグループか。ソーシャルメディアで活動が確認できるか。固有の地域や関心やスキルを示す単語やフレーズやスラングが使用されているか。
	Pattern of Life: 攻撃はいつ発生したか。コードがコンパイルされた時間、攻撃が活発な時間帯はあるか。同時期に何らかの関連イベントが発生しているか。C2 などのインフラが設置されたタイミング。攻撃の中でタイムリーな情報を探しているか。
	Stealth: 攻撃者が用いる隠蔽手段、検知回避手段、アンチフォレンジック機能、自らに不利なログ削除機能の有無。
	Cluster: 同様の攻撃がすでに確認されているか。あるとすればいつ。どのように。
	Functionality: 攻撃の結果、何が起きたか。情報の持ち出しか。改ざんか。制御機能の書き換えか。制御機能の停止か。
	Approval: 攻撃作戦の承認は誰か。法律家による承認の形跡。コードに活動の期限が決められているか。巻き添えを防ぐ工夫があるか。標的を確認する機能があるか。
	Mistake: 攻撃者は何らかのミスを犯したか。どのようなミスか。タイポはあるか。不注意による情報漏えいがあったか。
	Unknown: 何がわかっていないか。
個別の問いの結果について	複数の観点からの分析は、一定の容疑者の関与を疑わせるか。結論をサポートするために不要なデータを挿入していないか。どの問いが答えられていないか。

図表 付録 2 技術レベルの問い

Skills: 作戦に特殊な技術が必要か。どのくらい特殊な技術か。誰がその技術を持つか。
Scope: 侵害はより大きな作戦の一部と考えられるか。他にどのような事象が発生しているか。

Stages:　侵害は過去の攻撃のフォロー、あるいはこれから実施される攻撃の準備とみなせるか。複数のチームが作戦の別の部分を担っているとみなせるか。まだ確認されていない次の攻撃段階が想定できるか。
Evolution:　攻撃が実行される期間内に攻撃が進化した形跡はあるか。あったとしてそれらは上層部からの追加の承認を要するものか。
Claims:　攻撃の存在は公にアナウンスされているか。何者かが関与を認めているか。攻撃について第三者からの情報漏えいはあるか。コードの中に攻撃者を類推させる痕跡はあるか。
Insider:　攻撃に内部者しか知りえない情報が必要とされているか。攻撃者は被害組織内部に協力者をかかえていたか。
Intelligence:　作戦には被害組織についてのインテリジェンスが必要であったか。どの程度必要であったか。それらのインテリジェンスの取得難易度は。そのインテリジェンスの出所は。
Cost:　攻撃実施にどの程度の予算が必要か。大掛かりなテストが必要とかんがえられるか。固有のハードウェアやシステムが必要か。
Significance:　攻撃者にとってオペレーションの重要性はなにか。
Context（Aperture）:政治上の、地域問題上の文脈。他の情報源の発言。関連が考えられる他のイベント。

図表 付録 3 作戦レベルの問い

攻撃を命令した責任者は誰か。誰か先導役を果たしたか。
攻撃の目的はなにか。
誰が一番利益を得たか。誰が一番被害を被ったか。
作戦はどの程度成功したか。もしくは作戦は成功したのか、失敗したのか。

攻撃はどのような結果をもたらしたか。予期せぬ副作用はあったか。攻撃は先例を作ったか。攻撃は何を変えたか。
「対処」が必要か。どのような対処が必要か。
対処の結果がどのような二次効果をもたらすか。
結論は充分にサポートされているか。

図表 付録 4 戦略レベルの問い

加えて、Q モデルにおいては、上記の分析結果をどのように用いるかコミュニケーションが重要である。コミュニケーションについて考慮すべきは次の図表 付録 5 のとおりである。

レベル	コミュニケーション
個別の問い	どのレベルまで詳細を明らかにするか。最適な言語はなにか。
	公開することによる、自らの能力への悪影響はないか。
	（自らが実行中の）作戦への悪影響はないか。
	攻撃者は自らの振る舞いについて対応可能か。どのように対応するか。誰が対応するか。
	技術的なインディケーターやシグネチャの公開に際して、再利用や転送などの使用許諾はいかなるものにするか。

図表 付録 5 コミュニケーションに関する問い

第４項 Q モデルを使った分析

本論文では北朝鮮由来とされる以下 2 つのサイバー攻撃について、この Q モデルを用いた分析を試みた。

ケース 1: 韓国金融機関や放送局に対する攻撃（2013 年 3 月）

2013 年 3 月 20 日に韓国放送公社（KBS）、文化放送（MBC）、YTN、農協、新韓銀行、済州銀行で合計およそ 48,000 台のコンピュータがウイルスに感染した。数日後には YTN 関連の 58 のサーバ、14 の反北朝鮮活動サイト（北朝鮮からの亡命者が運営するものも含む）も攻撃をうけた。データを盗み出す攻撃はそれまでも多く確認されていたものの、データの消去という破壊活動を行うという点においてそれまでのサイバー攻撃とは異質である。

ケース 2: ソニーピクチャーエンターテイメント社に対する攻撃（2014 年 11 月）

2014 年 11 月にソニーピクチャーエンターテイメント社がサイバー攻撃を受けた。ガーディアンオブピース（Guardian of Peace）というそれまで活動が確認されていないグループがディスクの消去とソニーピクチャーエンターテイメント社からのデータ盗み出しに成功したと公表した。ガーディアンオブピースはその後、ソニーピクチャーエンターテイメント社から盗みだした情報を公に暴露していった。暴露された情報は、未公開の映画、ユーザ名やパスワードなどを含むソニーピクチャーエンターテイメント社内ネットワークシステムの詳細、従業員の個人情報、給与や雇用契約に関する情報、TV 番組の台本、そして社内メールである。

マルウェアはディスクの消去機能を持つものだけでなく、DDOS 攻撃機能を持つもの、キーストローク収集機能を持つもの、そして攻撃者グループと通信して新たな機能を追

加できるものが確認されている。

これらの 2 ケースはメディアなどでも多く取り上げられ、研究者の間での関心が高く、分析に利用可能な情報の質が高く、量が多かった。しかしながら、結論を先取りすれば、このどちらも Q モデルを使った分析を完遂するには情報が大きく不足していた。本論文が見出した技術レベルでのアトリビューションの課題は以下 2 つである。

まず、アトリビューションの作業は特定のケースに対して、一度きり行うものではない。できるだけ多くのサイバー攻撃について、常日頃から、技術レベル、戦術レベルの問いを投げかけつづけることで、比較分析ができるようになる。例えば「Stealth:　攻撃者が用いる隠蔽手段、検知回避手段、アンチフォレンジック機能、自らに不利なログ削除機能の有無。」は特に攻撃者の個性が現れる部分だが、特徴をグループに紐付けるためには既存の攻撃グループの手口の全体像をある程度掴んでおく必要がある。

また Q モデルの戦略レベル、戦術レベルの問いは攻撃者グループの内部に情報提供者がいたり、攻撃者グループ内でのコミュニケーションを傍受できたりしなければ回答できない部分が多い。Q モデルは民間企業や CSIRT などでなく、軍やインテリジェンス機関の使用を前提にしており、これが使える環境は限られるということがわかった。

第 2 節　グラフ描画のソース

第 3 章第 3 節第 1 項で用いた図表「データのストックとフローにみる国際関係」を描画するためのコードは以下のとおり。vis.js というオープンソースのグラフ描画ライブラリを使用し、データを与えた。用いた vis.js はリリース日が 2017 年 10 月 12 日のバージョン 4.21.0 である。

```
<!doctype html>
<html>
```

```
<head>
  <title>Network | Sizing</title>

  <style type="text/css">
    html, body {
      font: 10pt arial;
    }
    #mynetwork {
      width: 600px;
      height: 600px;
      border: 1px solid lightgray;
    }
  </style>

  <script type="text/javascript" src="./vis.js"></script>
  <link href="./vis-network.min.css" rel="stylesheet" type="text/css" />

  <script type="text/javascript">
    var nodes = null;
    var edges = null;
    var network = null;

    function draw() {
      // create people.
      // value corresponds with the age of the person
      nodes = [
        {id: 1,   value: 40,   label: 'US' },
        {id: 2,   value: 8, label: 'China'},
        {id: 3,   value: 6, label: 'Japan'},
        {id: 4,   value: 6, label: 'UK'},
        {id: 5,   value: 5, label: 'Australia' },
        {id: 6,   value: 5, label: 'Germany'},
        {id: 7,   value: 4,   label: 'Singapore'},
        {id: 8,   value: 4,   label: 'Canada'},
        {id: 9,   value: 3, label: 'India'},
        {id: 10, value: 2, label: 'Brazil'},
```

```
    {id: 11, value: 2, label: 'Hongkong'},
    {id: 12, value: 2, label: 'France'},
    {id: 13, value: 1, label: 'Ireland'},
    {id: 14, value: 1, label: 'Netherland'},
];

// create connections between people
// value corresponds with the amount of contact between two people
edges = [
    {from: 1, to: 2, value: 8, title: '8 connections'},
    {from: 1, to: 3, value: 20, title: '20 connections'},
    {from: 1, to: 4, value: 30, title: '30 connections'},
    {from: 1, to: 5, value: 3, title: '3 connections'},
    {from: 1, to: 7, value: 3, title: '3 connections'},
    {from: 1, to: 8,value: 1, title: '1 connections'},
    {from: 1, to: 10, value: 9, title: '9 connections'},
    {from: 1, to: 11, value: 7, title: '7 connections'},
    {from: 1, to: 12, value: 2, title: '2 connections'},
    {from: 1, to: 13, value: 3, title: '3 connections'},
    {from: 2, to: 3, value: 10, title: '2 connections'},
    {from: 2, to: 7, value: 10, title: '3 connections'},
    {from: 2, to: 11, value: 10, title: '0 connections'},
    {from: 3, to: 5, value: 2, title: '0 connections'},
    {from: 3, to: 7, value: 3, title: '0 connections'},
    {from: 3, to: 11, value: 11, title: '0 connections'},
    {from: 4, to: 6, value: 1, title: '0 connections'},
    {from: 4, to: 12, value: 5, title: '0 connections'},
    {from: 4, to: 13, value: 10, title: '0 connections'},
    {from: 4, to: 14, value: 5, title: '0 connections'},
    {from: 5, to: 7, value: 4, title: '0 connections'},
    {from: 5, to: 11, value: 1, title: '0 connections'},
    {from: 6, to: 12, value: 1, title: '0 connections'},
    {from: 6, to: 14, value: 1, title: '0 connections'},
    {from: 7, to: 9, value: 4, title: '0 connections'},
    {from: 7, to: 11, value: 5, title: '0 connections'},
    {from: 8, to: 13, value: 1, title: '0 connections'},
```

```
            {from: 12, to: 14, value: 1, title: '0 connections'},
        ];

        // Instantiate our network object.
        var container = document.getElementById('mynetwork');
        var data = {
            nodes: nodes,
            edges: edges
        };
        var options = {
            nodes: {
                shape: 'dot',
            }
        };
        network = new vis.Network(container, data, options);
    }
  </script>

</head>
<body onload="draw()">
<p>
    Scale nodes and edges depending on their value. Hover over the edges to get a popup with more information.
</p>
<div id="mynetwork"></div>
</body>
</html>
```

はしがきと謝辞

2002年4月、私は情報セキュリティ技術者として社会人としての一歩を踏み出した。携帯電話やメールが大学生の間で遍く普及し、IT革命というスローガンに代表される、IT 技術が世界を変えるという期待が社会に広く共有されていた時代であった。外資の通信機器ベンダーやデータベースソフトウェアベンダーの採用試験に落ちた私はセキュリティ会社に拾われた。バブル時代はすでに終わっていたが、IT業界だけは景気がよかった。学業成績がよろしくない学生も受け入れた。

その当時、コンピューターシステムの安全を守ることは情報セキュリティと呼ばれていた。情報セキュリティに関する仕事というのは、金銭や名声を求める犯罪者集団から顧客を守るための手段を提供するということであった。当時の上司は「セキュリティはご飯でなくおかず」という言葉でシステムやサービスというメインストリームに対する、裏方としてのセキュリティの役割を的確に表現した。世界中に一気に感染を広げるワームやクレジットカード情報などを盗み取ろうとするフィッシング詐欺への対応などを行っていたが、自分の仕事によって社会全体から情報セキュリティリスクが低減されているという感覚はなかった。毎月のようにこれまでなかった新たな技術を使った攻撃が確認され、セキュリティ対策企業（セキュリティベンダー）からはそれに対応した新たな製品が発表されたが、彼ら（攻撃者側）と我々（防御側）の競争は時が立つほどに防御側が不利になっているという感覚が強くなっていった。

その後、公益性の高い仕事を求めてJPCERT/CCというCSIRT（コンピューター緊急対応チーム）で働くことになった。日夜、国内外から寄せられる大量のインシデントはセキュリティの重要性を改めて突きつけられる思いだった。インシデントの多くは海外からの通信が関係するものであり、対処するためには海外のCSIRTやインターネットサービス事業者や法執行機関との連携を要することが分かってきた。JPCERT/CCで国際連携

を担当する部門を任されてからは、海外のセキュリティコミュニティとの関係の強化にあたった。なるべく頻繁に現地へ出張し、その地でセキュリティ対応をする技術者との交流を図った。途上国の技術者に対する技術トレーニングを実施することも増えた。長期に渡って同じ場所に留まることはできないので、その場所を構造的に理解しようと努めることになった。

2010 年頃からはサイバーセキュリティに関する民間外交の役割を期待されることが増え、安全保障を担当するポリシーメーカーとの接点が増えていく。彼らは国際関係論や安全保障論に関する体系的な知識を持ち、新たな問題領域であるサイバーセキュリティの分野に送り込まれてくるエリートである。「サイバーセキュリティはプレーヤーが多すぎる」という声をよく聞いた。私には当然であった、自律／分散／協調を是とするインターネットやサイバー空間の管理の仕組みは、核兵器の不拡散、生物化学兵器の制限など国家間の合意ですべて決まる世界からは複雑に映るということを知った。同時に、その発言には長きにわたり安全保障という「国家の専管事項」を扱ってきたエリートの自負を感じた。眼の前のトラブルへの対応のため、自分が日常的に行っていた通信内容の分析、ウイルスプログラムの分析などがプライバシー保護や著作権保護などの文脈では好ましからぬ行為とみられることも知った。

気づけば、情報セキュリティという分野は急速に社会的な関心事となっていた。情報セキュリティはサイバーセキュリティ、サイバースタビリティと名前を変え、コンピュータやネットワークだけでなく工場や発電所や旅客機を制御するシステムが守る対象になった。対峙する相手は、金銭や名声を求める犯罪者集団ではなく、国からの命令を受けて入念に執拗に機密情報を狙う軍隊やインテリジェンス機関にシフトしてきた。これらの攻撃は、どれだけ入念にセキュリティ対策をしても完全に防ぐことはできない。前述したイランの核処理施設の破壊と妨害を狙ったウイルスについて調べれば調べるほど、その思いは強くなった。10 数年持ち続けた、技術の問題は技術で解決するとい

うの自身の信条は限界を迎えていることを知った。技術だけではサイバーセキュリティは確保できない。そこにはルール作り、サイバー衛生の確保、キャパシティビルディング、信頼の醸成など未知の道具を活用することが求められていた。

ルサンチマン滲む自らの経歴を長々と開陳したのは、サイバー空間の急速な発展、そして 2010 年代から顕在化した安全保障問題化を語る手段として有効だからである。令和の世になっても、サイバーセキュリティ対策の前面にたっているのは、私同様に技術としてのセキュリティに興味を惹かれたオタクたちである。かつてオタクの遊び場であり、実験場であったサイバー空間は、今日では多くの人の「いつもとかわらない日常」を支えるものであり、ときに人の生死を左右するものであり、世論という抽象的なコンセプトの中心にあり、民主主義国家のリーダーの選択に影響を及ぼすものであり、国際社会の構造を変えうるものであるからである。目の前の技術的な問題に夢中で取り組んでいて、ふと目を上げたら遊び場は戦場に変わっていた、その切実な恐怖が本論文執筆の一番大きな動機になっている。

執筆を終えて、かつての恐怖がすべて取り除かれたとは思わない。可能性は低いとはいえ、サイバー空間はまだジョージ・オーウェルの小説「1984」に描かれるようなディストピアにもなりかねない。一方で、本論文執筆を通じて、私は自身の恐怖を共有してくれる多くの人達に出会った。技術革新が社会にもたらす負の影響というところまで一般化すれば、この種類の恐怖は過去にもあり、人類はそれを乗り越えてきたことを文献から学んだ。恐怖は私一人だけのものでもなく、現代に固有のものでもない。多くの人が、長い間抱え続けた恐怖と分かってしまえば、あとは上手な付き合い方を考えるだけである。

本論文は私が慶應義塾大学大学院政策・メディア研究科後期博士課程に在籍中の研究成果をまとめたものである。この機会を私に与え、支援してくださった皆様すべてにお

礼を申し上げる。紙幅の都合ですべての方のお名前をここにあげることはできない。一部の方だけになってしまうが、ここに感謝の意を表したい。

研究の指導教員を引き受けてくださったのは政策・メディア研究科教授であり、総合政策学部長の土屋大洋先生である。先生はインターネットが世界を理想郷に変えると広く信じられて疑われない時代に、『ネット・ポリティクス』（岩波書店、2003 年）という本を出版された。インターネットにおいてインテリジェンス活動が行われ、軍事行動が行われることを警告されていた。一読して私はそれをナンセンスだと思ったが、刊行から 10 年が経ち、各国の軍隊がサイバー部隊を設け、大規模なサーベイランス活動の存在が暴露された。土屋先生の分析は正しかった。先生の下で研究すれば 10 年後の未来がみえるかもしれない。そう願ってほぼ面識のない状態で湘南藤沢キャンパスの先生の研究室を訪れたのが 2013 年のことである。

修士課程を経ていない、研究の実績が皆無の社会人、しかも先生と近しい研究分野を志す私を快く受け入れてくださった。鋭く未来を見通す力への憧れだけで土屋研の門を叩いたが、先生が研究者としてだけでなく、教育者として学生指導に情熱を注がれる方であったのは僥倖であった。6 年間、すべての論文はまず先生にコメントをお願いした。毎度短時間で枠組みから細部まで様々なご指導をいただいた。構想段階で面白いと自賛していたテーマも、書き上げてみると色あせることが多い。メールに書かれた、「面白いね。」と「ずいぶん良くなったね。」という一言が、先の見えない研究生活における最大の心の支えであった。

同研究科の神保謙先生と中山俊宏先生と逢阪貴士先生には、研究の副査として、常に励ましと適切なアドバイスをいただいた。本論文における研究における問いの立てかた、分析の枠組みのつくりかたなどについて、大きな課題を克服できたのは副査の先生方のご指導の賜物である。学位審査のプロセスを通して、廣瀬陽子先生、鶴岡路人先生には本論文について極めて有益なアドバイスを頂いた。

また、残念ながら学位審査に加わっていただくことは叶わなかったが法務研究科の青木節子先生には、入学以来 5 年にわたり折に触れてご指導いただいた。何かと気にかけてアドバイスをくださった政策・メディア研究科の武田圭史先生にも感謝したい。

一緒に研究をする機会をいただいた方々の中でも、国際社会経済研究所の原田泉さん、日本マイクロソフト社の片山健さん、東京海上日動リスクコンサルティング社の川口貴久さん、SFC フォーラム事務局の綿貫直子さんの 4 名には何度となく助けていただいた。また、土屋先生の下で共に学んだ北川敬三さん、菊地映輝さん、花房真理子さん、戸所弘光さん、Melis Dilişen さん、梶原みずほさん、山内萌さん、小川秀俊さん、多くの優秀な修士課程の学生の皆さんにも感謝したい。研究の構想段階から鋭い指摘をいただき、また研究の作法や事務作業など不慣れな分野についてアドバイスをいただいた。

南山大学の平岩俊司先生、情報セキュリティ大学院大学の林紘一郎先生、ミシガン大学の狩野剛さん、駒澤綜合法律事務所の高橋郁夫弁護士、日本サイバー犯罪対策センターの坂明さん、総務省の佐々木将宣さん、日立製作所の寺田真敏さん、NTT-CERT の神谷造さん、大東文化大学の上村圭介先生には、それぞれ拙稿への示唆に富んだコメントをいただいたことを感謝申し上げる。

様々な海外の研究者および実務者にもヒアリングという形でアドバイスをいただいた。ゼンデスク社の Maarten Van Horenbeeck さん、シーメンス社の Thomas Shreck さん、カーネギー平和財団の Tim Maurer さん、ハーグ戦略研究センターの Alex Klimburg さん、韓国インターネット振興院の Jinhyun Cho さん、APNIC の Klee Aiken さんにはとりわけ感謝したい。成果の一部をなるべく早く英語で公開するのが、なによりの恩返しと考えている。

日本のサイバーセキュリティ向上をミッションとする JPCERT/CC には OB も含めて多彩な顔ぶれが揃っている。働きながら博士号取得をしようとする私を理解し、大いに支えていただいた。とりわけ私の業務の穴埋めをするだけでなく、それ以上の活躍をし

てくれた内田有香子さん、梅村香織さん、森克宏さん、山本健太郎さん、駒場一民さん、佐藤祐輔さん、村上晃さん、久保しおりさん、佐々木理さん、内山貴之さん、米澤詩歩乃さん、中野巧さん、齋藤美香さん、登山昌恵さんに感謝する。また折に触れアドバイスをいただいた小池光さん、久保啓司さん、伊藤友里恵さん、宮地利雄さん、村上憲二さん、歌代和正さん、有村浩一さん、そしてなにより学位取得のきっかけを与えてくれた早貸淳子さんに感謝する。すでに JPCERT/CC を離れたとはいえ、鎌田敬介さん、名和利男さん、山賀正人さん、満永拓邦さん、久保正樹さんを始めとする OB の皆さんの活躍から受けた刺激がこの研究を後押ししてくれた。佐々木勇人さんがオフィス内の書架にこしらえたサイバーセキュリティと安全保障に関する資料ライブラリはこの研究を支えてくれた。

あまり知られていないことだが JPCERT/CC の活動の多くは、経済産業省からの資金で賄われている。本論文で紹介したサイバー空間安定化委員会の活動なども含め、短期的に成果が出にくい国際的な活動の重要性を理解いただき、支援いただいた。同省サイバーセキュリティ課の皆さんに感謝する。

後期博士課程に入学した 2014 年の春、私は FIRST という国際団体の理事に選出された。唯一の日本人理事として様々な国から集った 9 人の理事たちと、同僚として同じ目標を追った 4 年間は刺激と矛盾に満ち溢れていた。研究は大いに滞ったが、本論文に描いてきたサイバーセキュリティガバナンスの実態は、この無二の経験に負うところが多い。辛抱強く付き合ってくれた同僚の理事、そしてスタッフに感謝する。

奈良先端科学技術大学院大学元教授の山口英先生と慶應義塾大学元教授の Kilnam Chon 先生の両名には、アフリカの大地を舞台に、強烈な体験をさせていただいた。インターネット工学の分野の泰斗である両先生は、共に、技術面以外のアプローチを大切にされていた。そのことが一層私を社会科学分野での研究に駆り立てた。山口先生は、2016 年に永眠された。もっともっと教えて頂きたいことがあった。

言うまでもなく、家族の支え無くして本論文はおろか私という人間は存在しえない。働き者の父、古文書を読み続ける母、弟達、祖母、そして叔父の征夫は私を温かく見守り、ささやかな研究成果でも我がことのように喜んでくれた。最後になるが、土屋先生をのぞけば、いつでも私の研究の最初の読者であり、世界一率直なコメンテーターであり、私を明るく励まし続けてくれた妻に感謝する。

小宮山 功一朗