グローバルな文脈での日本

REEXAMINING JAPAN IN GLOBAL CONTEXT

Suntory Foundation Research Project

FORUM REPORT 020

「グローバルな文脈での日本」フォーラム第20回　2022年10月

サイバーセキュリティ

サイバーグレートゲーム：デジタル技術による国際政治の変容

土屋大洋

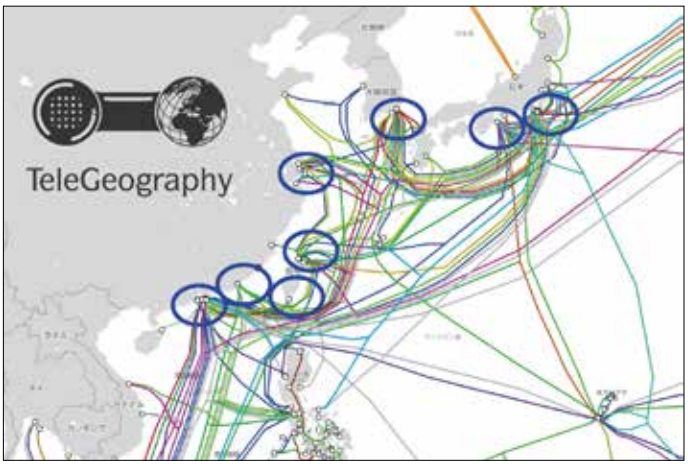
慶應義塾大学大学院政策・メディア研究科／総合政策学部 教授

2022年10月13日、「グローバルな文脈での日本」プロジェクトは東京で会議を開催し、サイバーセキュリティとサイバーガバナンスについて議論した。会議ではまず、慶應義塾大学の土屋大洋教授によるプレゼンテーションが行われた。

その冒頭、土屋教授は、19世紀から20世紀初頭にかけ、アフガニスタンや中央アジアへの影響力を巡って大国（主にロシアと英国）間で繰り広げられた「グレートゲーム」と、現在サイバースペースの支配権を巡って大国（主にロシア、中国、米国）間で繰り広げられている対立関係との類似性について説明した。前者は、基本的にはニコラス・スパイクマンが言及した「リムランド」、あるいはそれ以前にハルフォード・マッキンダーが述べていたユーラシア大陸の「ハートランド」の周辺地域で引き起こされた物理的領域の支配を巡る地政学的抗争である。一方、後者には言うまでもなく、空間的要素は一切存在していない。よく言われるように、サイバースペースには「国境は存在せず」、したがってデータは全世界を移動することができる。この事実は、地政学はサイバーグレートゲームを分析するための概念レンズとしては相応しくないようにみえる。しかし、本当にそうなのだろうか？

実際には、サイバーグレートゲームは極めて地政学的な性質を有していることを示唆する2つの考察がある。第1の考察は空間的な側面が存在することをほのめかすものですらある。なぜなら、米国はサイバー攻撃に関して、ロシアと中国、北朝鮮、イランを常に非難しているからだ。そのうち、ロシアはハートランドに位置し、中国と北朝鮮、イランはすべてリムランドに位置している。いずれも19世紀から20世紀初頭にかけて対立が生じていた不安定な地域であったが、その状況は現在も変わっていないのである。

第2に、サイバードメインがもう一つの地政学的抗争が展開する領域になりつつあることは明白である。例えば、ウラジーミル・プーチン政権下のロシアは、米国などの地政学的に対立する主要国に対し、国内での分断や不和、混乱の種を播き、国内政治への干渉を通じて自由民主主義を側面から攻撃することにより、その弱体化を図っていることが知られている。さらにイランなどの国も脅迫的な行為を行っている。これらの国々は、偽のソーシャルメディア・アカウントやフェイク・ビデオ、ボット、標的型電子メール攻撃などを利用して陰謀論を広め、党派的分裂を激化させ、選挙結果に影響を与えようとしてきた。例えばロシアのハッカーは、アメリカ政府と民主党双方の情報システムに侵入してデータを盗み、マルウェアを忍ばせ、システムの運用を混乱させた。イランのハッカーは、プラウド・ボーイズなどの過激派グループを装って選挙に介入した。2017年、米国国土安全保障省は対抗策として、自由で公正な信頼性の高い選挙にとって不可欠な情報システムを「重要インフラ」に指定した。同じく2018年には、米国国防総省が武力衝突のレベルには至らない活動を含め、不正なサイバー活動を未然に根絶もしくは中止させることを目的とした「前方防衛（Defend Forward）」サイバー戦略を採用した。例えば米国サイバー軍は、2018年の米国中間選挙当日にロシアにあるトロール行為（オンライン上の迷惑行為）の拠点を、インター



ネットから遮断する作戦を決行した。米国では日々、国外の情報システムを積極的に調査し、サイバー攻撃が差し迫っていることを示す兆候に注意を払っている。この事実は、真の意味において、サイバースペースに国境が存在しないとは到底言えないことを示している。

国土安全保障省サイバー・インフラ安全局（CISA）の初代局長を務めたクリストファー・クレブスによれば、米国による取り組みの結果、2020 年の連邦選挙は、歴史上、最もセキュリティの高い選挙となった。にもかかわらず、ドナルド・トランプ大統領は大統領選挙に不正があったと主張し、2021 年 12 月 6 日にはトランプ大統領の支持者たちが米国国会議事堂へとデモ行進を行い、合法的な当選者であるジョー・バイデンの認定を阻止しようとした。この事実は、民主政治に対する国外からの干渉との闘いは、単なるハードウェアやソフトウェアの問題に留まるものではなく、偽情報や偽の風説が有機的に伝播するのを防止する必要があることを示している。

現在、サイバースペースが、陸、海、空、宇宙に続く第 5 の軍事作戦領域になったことは明らかである。ただし、サイバースペースは人工的な領域である。宇宙の人工衛星、「クラウド」にデータを保存しているサーバー、さらには自宅と企業、オフィスを繋いでいるケーブルやスイッチ、ジャンクションボックスは、いずれもサイバースペースを構成する物理的な要素である。サイバースペースを構成する物理的インフラのなかでも最も重要な要素が海底光ファイバーケーブルである。例えば、島国である日本の国際インターネットトラフィックのうち、99% 程度が海底ケーブルを通じて送信されている。原理的には、海底ケーブルの位置が判明すれば、ケーブルを簡単に切断することができる。また多くの国では、海底光ケーブルの陸揚げはほんの数カ所で集中的に行われているという現実もある。例えば日本の場合、ほとんどは千葉と伊勢志摩で陸揚げが行われている。また海底光ケーブルの陸揚げ場所の多くには、目視で確認できる標識が表示されている。このような脆弱な場所を一般市民が簡単に探し出すことができるのであれば、テロリストや脅迫行為を行う外国も同様に探し出すことができるのである。

2014 年のロシアによるクリミア半島の占領と併合が明確に示すように、現代においては、情報システムを標的としたサイバー軍事作戦と物理的な軍事作戦を組み合わせる能力が、国力にとっての重要資源となっている。ロシアは一回の迅速な軍事作戦によりクリミア半島を掌握し、ウクライナの他地域から切り離し、有効な対応や防衛が開始される前に既成事実を手に入れることができた。最近のプーチンによるウクライナの他地域への侵略を巡る大きな謎のひとつは、なぜロシアが同じ戦略を遂行する上で

これほどに努力を怠ったのかという点である。今回の軍事作戦はほぼすべて旧来の軍事的手法で遂行され、惨憺たる結果をもたらしている。特筆すべきはウクライナのインターネットインフラが概ね無傷で残っており、正常に機能していることである。その背景には、ウクライナのインターネット当局がクリミア半島での教訓を活かし、インターネットインフラをはじめとする安全保障対策を積極的に強化したことがある。また今回の場合、ウクライナは西側諸国、特に米国サイバー軍の支援からも大きな恩恵を獲得している。

日本にとって、これらの状況が持つ意味とはどのようなものなのだろうか。2018 年 3 月、安倍晋三首相は防衛大学校における演説のなかで、現在ではサイバースペースと宇宙空間において優位に立つことが極めて重要であると語っている。当時は領域横断作戦に関する議論が行われていた。2018 年 12 月に日本政府は「防衛計画の大綱」（NDPG）を閣議決定し、今後 10 年以上を対象とする日本の安全保障政策の周知を図った。しかし、岸田文雄首相は就任直後に NDPG と「国家安全保障戦略」、「中期防衛力整備計画」を見直す意向を発表した。現在は脅威が急速に高まりつつある情勢にあり、さらに技術的な制約や機会も急速に増加しているのは明らかである。その状況に即時に対応するのは難しい。

サイバースペース、特にサイバーグレートゲームにおけるハートランドとは、具体的にはどの場所を指すのだろうか？ 土屋教授は二つの場所を指摘している。ひとつはデータセンターである。我々は次第に、生活のあらゆる要素をデータに依存するようになっている。この依存性を示唆する現象のひとつが、現金の減少である。純粋にデジタルドメインのみで行われる金融取引が増え続けている。この種の金融取引をはじめとする金融サービスは、信頼性の高いデータセンターに依存して行われているのだ。ロシアは、この事実の重要性を認識し、侵略作戦の早い段階でウクライナのデータセンターに対する巡航ミサイルによる攻撃を開始した。しかし、この攻撃を予想していたウクライナは、自国の重要情報の多くを事前に他国のデータセンターに移転していた。

現在のサイバースペースにおけるハートランドを構成するもうひとつの重要な要素が認識空間、すなわち我々の脳である。我々はツイッターやフェイスブックなどのソーシャルメディアに耽溺し、あまりにも多くの偽情報を消費している。現在の若者は、その情報のほとんどを信頼性の低いソーシャルメディアから入手している。いまや IoT（モノのインターネット）については当然のように語られているが、本当に語られるべきは IoB、すなわち脳（Brain）、あるいは体（Body）、あるいは行動（Behavior）のインターネットなのである。将来的には、我々の脳がインターネットに直接接続される可能性がある。そうなれば、その接続がハッキングされ、破壊されるおそれが生じてくる。

1982 年にクリント・イーストウッドが主演した映画『ファイヤーフォックス』では、パイロットの思考によって完全に制御可能な戦闘機をソビエト連邦が完成させていた。このように当時は絵空事であったものが、いまや現実のものとなっている。我々は自らの思考と機械を接続し、思考のみで機械を制御する方法を発見しつつある。将来的には、その思考をハッキングし、あるいは乗っ取ることにより、この種の機械をハッキングすることが可能になるだろう。

したがって、サイバーグレートゲームにおいて優位に立つためには、2 つの能力が必要となる。すなわち、サイバースペースの物理的インフラを防護する能力、そして我々のデータ空間と認識空間の完全性を保護する能力である。「ハイブリッド戦争」の時代は終わった。いまや我々は、サイバーグレートゲームのあらゆる要素を完全に包括する「スーパーハイブリッド戦争」の時代について検討しなければならない。日本は、以上の経緯のことを踏まえて、NDPG を改訂するにあたり、まずは以下の 4 つの対策を講ずる必要がある。

1. 心理戦と認識戦を担当する部隊を編成すること。
2. 秘密情報収集（SIGINT）能力を強化すること。
3. 憲法面と法律面において、「前方防衛」戦略に匹敵する日本独自の戦略に対応した基礎を築くこと。
4. 虚偽の情報を阻止する「継続的従事」能力を育成すること。

土屋教授によるプレゼンテーションの終了後、会場との質疑応答が行われた。

最初の参加者からは、2 つの質問がなされた。1 つ目はアトリビューションに関する質問であり、サイバー攻撃への対応において、その首謀者と標的を確定することの難易度を問うものであった。2 つ目はサイバースペースの物理的インフラを構成する主な要素の脆弱性に関するものであり、インターネットが複雑な

ネットワークであることを踏まえた上で、特定のデータセンターやケーブル、陸上との接続施設などが遮断された場合、あるいは破壊された場合に、別のノードを通じてデータの通信経路を比較的短時間で迂回させる対策の実現性を問うものであった。第一の質問に対し、土屋教授は、日本ではアトリビューションを特定することが非常に難しいとみられるものの、ファイブ・アイズ加盟国では平時に通信を傍受する法的な枠組を備えていることから、日本と比較すれば非常に容易であると回答した。日本の場合、憲法第 21 条により通信の秘密が保護されており、また政府と民間がともに同条を極めて厳密に解釈していることから、日本のインテリジェンス・コミュニティが傍受の許可を得ることは非常に難しい。２つ目の質問に関しては、ある程度の混乱には対応可能であるが、その程度はセクターやサービスによって異なるものとなる。フェイスブックやツイッターの応答時間については、誰もがある程度我慢して待つことができるが、（例えば）金融セクターでは応答時間に対する耐性は極めて小さい。

２人目の参加者からも、２つの質問がなされた。１つ目は、憲法第９条により、サイバー戦争に関する能力が制限されるのではないか、と問うものであり、２つ目は、現在のサイバースペースには、モンゴル帝国時代の騎兵隊、あるいは 19 世紀から 20 世紀初頭の海軍力に類似した支配的な能力が存在するのではないか、と問うものであった。土屋教授は最初の質問に対し、何をもって「戦争」とみなすかにより、制限の範囲は大きく異なると回答した。憲法第９条では戦争における先制攻撃を明確に禁止しているが、情報ビットは弾丸ではない。また教授は、憲法第９条とは積極的なサイバー防衛作戦を制限するものではないと考えられるとの見解も示した。ただし、この見解は政府によるものではない。２つ目の質問に関しては、最も高度なツールと技術を有する国が優位に立つことは明らかであり、この点に関して米国（特に国家安全保障局）の右に出るものはない。ただし、サイバードメインにおける米国の実効性を高めている要因のひとつとして、マイクロソフトやグーグルなど、インターネットの運用において非常に重要な役割を担う製品やサービスを提供している重要な民間企業と米国政府が協力関係を結んでいることがあげられる。米国以外の国では、このようなサイバーセキュリティに対する「チームワーク」による利点はみられない。

３人目の参加者は、ロシアや中国、イランなどの多くの国では、実質的に政府が自国民とのサイバー戦争に関与し、反対意見を抑圧することにより政治的支配を維持していると指摘した上で、これらの国の市民の代理として他者（米国など）が介入し、当該国の政府による関与を妨害することは可能なのか、と質問した。土屋教授は、外国政府や民間の第三者の双方がそのような動きに介入し、妨害することは可能であると回答した。その一例としては、政府による検閲を国民が回避することを可能とする仮想私設通信網（VPN）ソフトウェアの提供があげられる。その結果、通信と情報へのアクセスを巡り、市民や海外活動家と国家側との間でいわゆるいたちごっこが繰り広げられることになる。

次の参加者は、サイバー技術の発展が今後の戦争に与える影響について質問した。すなわち、サイバードメインの高度化に伴い、脆弱性も高まるおそれがあることを踏まえると、その対応として、ハッキングなど、遠隔操作による混乱が生じることのないアナログな技術に回帰することも予想されるのではないかという問いである。また関連して、サイバー能力の評価が困難である以上、どのようにすれば現在の戦力のバランスを評価することができるのか、という質問もなされた。土屋教授は質問者の見解に同意し、旧来の技術を利用することや、最新技術への依存を回避することが、敵側のサイバー能力に 対する次善策のひとつとなると指摘した。例えば米軍はパイロットや艦長に対し、GPS に頼ることなく航行する能力を備えるための訓練を強化している。また土屋教授は、明確な評価基準がない場合、サイバードメインにおける戦力のバランスの評価が非常に困難であることを認めるとともに、それを可能にする信頼性の高い方法を見いだすには至っていないと認めた。

最後に質問した参加者からは、３つの質問がなされた。１つ目は、サイバー攻撃能力とサイバー防御能力を区別することは可能なのか、また可能でないとしたら、憲法第９条により禁止されていることを根拠として、日本政府がサイバー軍事作戦への関与を躊躇することは正当化されるのか、という問いであった。また２つ目は、サイバー攻撃を阻止する可能性について、３つ目はサイバー攻撃の発生源を特定すること（例えば、ロシアまで遡求すること）が可能であったとしても、それが国家首脳の命令により実行されたものであるかどうかを技術的に判定する可能性について問うものであった。土屋教授は、サイバードメインにおける攻撃と防御を区別することは困難であると認め、一般論として両者は同じコインの裏表の関係にあると指摘した。教授の見解によれば、この事実は「攻撃」と「防御」という用語を使用しても、特に理解を助けるものとはならないことを意味している。ただし、2018 年 NDPG が、国家安全保障の追求を目的とした反撃作戦について承認を簡潔かつ明確に求めていることは、この NDPG の良い点である。しかしながら政府、特に防衛省は関与に消極的である。また攻撃の阻止に関しては、完全に不可能である。その理由のひとつとして、政府首脳はプロキシを利用し、自身の証拠を隠蔽していることがあげられる。ただし、多くのケースでは、政府首脳とハッカーとの間に関係があると想定するのは理にかなっている。土屋教授は、合理的な疑いがある場合には、パブリック・アトリビューションを避けることは誤りであるとの見解を示した。

グローバルなインターネットを介した転移による政策、ガバナ ンス、および地政学に対する影響

マーク・レイモンド
オクラホマ大学サイバーガバナンス・政策センター所長

続いて、オクラホマ大学のマーク・レイモンド教授から、サイバーガバナンスをテーマとするプレゼンテーシ ョンが行われた。

その冒頭、レイモンド教授は、インターネットの成長と癌転移の類似性について説明した。その真意は、インターネットが癌のような性質を持つことを示唆することではなく、両者ともシステム全体に急速に伝播し、システム全体の機能を変化させる可能性があるプロセスの好例であることを示唆することにある。

インターネットの成長に関しては、転移は２段階で進行する。すなわち、第１に技術的な転移が生じ、続いてその技術に伴うガバナンス・アレンジメント の転移が生じるのである。

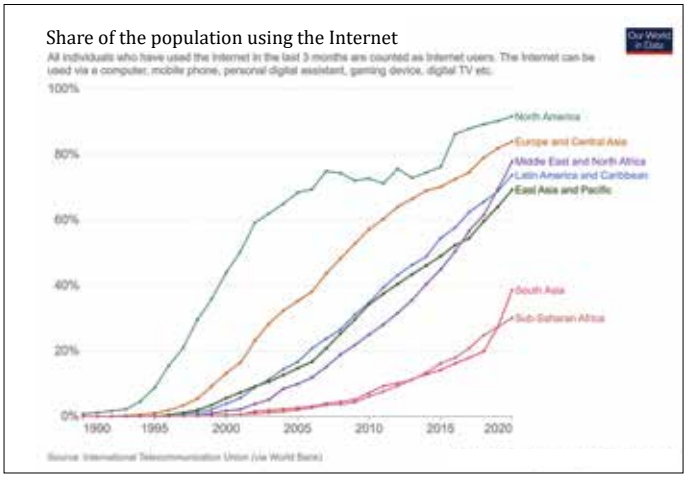
全世界では、約 62% の人々がインターネットを利用している。ただし、インターネット導入の時期と割合には、地域ごとにかなりのばらつきが見られる。また多くの地域では、その内部でもかなりのばらつきが見られる。さらにインターネットに接続した経験は、富裕国と貧困国で大幅に異なることも念頭に置いておかなければならない。後者の場合、総所得に占める接続費用の割合がかなり高く、接続速度と可用性が大幅に制限される傾向がみられる。また非識字率やインターネットにおける母国語表記の少なさも、アクセスの大きな障壁となっている。さらに多種多様な情報格差も存在している。にもかかわらず、全体としては特筆すべき推移が生じている。例えばカザフスタンでは 2007 年以降、インターネットが著しい速度で普及し、その浸透率は約 5% から 86% に上昇した。

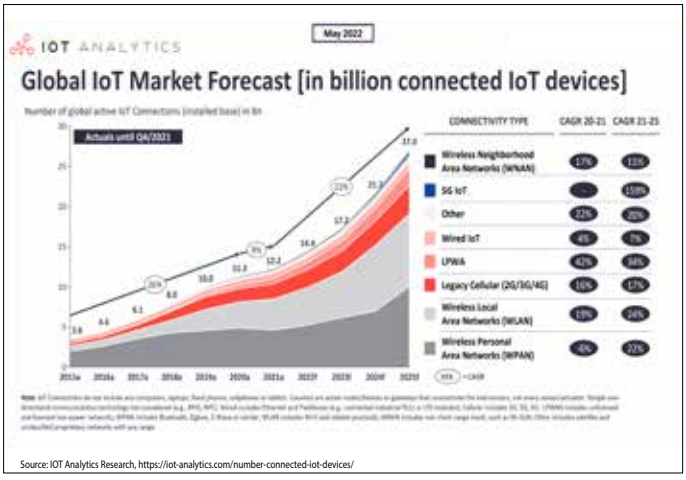
我々は、インターネットに関連するあらゆる技術が、システム全体に急速に伝播する証拠を目の当たりにしている。土屋教授が言及した海底ケーブルは、そのほんの一例にすぎない。別の例として、各サービスプロバイダのネットワークインフラもあげられる。また各ネットワークがトラフィックを互いに受け渡すインターネット相互接続点も例のひとつである。ただし繰り返すが、これらの技術はいずれもシステム全体に急速に伝播したにもかかわらず、その伝播の時期と範囲には、全世界でばらつきが見られるのである。

技術的な転移を示す特に優れた例が、モノのインターネット（IoT）である。IoT デバイスとは、人との直接の相互作用を主たる目的としないインターネット接続機器である。IoT 接続の大部分は機械間で行われる。また人工知能（AI）システムがその接続を監視し、人による介入を要する問題が発生した場合には警告を発するシステムに移行しつつある。このシステムは、高度に自動化された極めて大規模なものである。

IoT デバイスについて語る場合、通常は２種類のモノについて語られる。すなわち、(1) 各種のセンサーと (2) アクチュエータ（またはスイッチ）である。その主な用途としては、消費者向けデバイス（ウェアラブル、医療機器、電化製品など）、産業用モニタリング・制御システム（物流システム、エネルギーシステム、製造プロセスなど）、インフラ（スマートシティ、スマートグリッド、監視）があげられる。注意すべきは、監視は専制国家に特化した用途ではないということである。英国などの一部の自由民主主義国も、同様に監視インフラに多額の資金を投じている。

あるコンサルタント企業によれば、全世界の IoT デバイスの数は 2015 年の 36 億台から増加し、わずか 10 年後の 2025 年には 270 億台に達するとみられている。センサーとアクチュエータの数は、コンピュータとノートパソコン、スマートフォンの数





を大幅に上回る見込みである。言い方を変えれば、インターネットトラフィックの大部分が機械間で行われるようになり、人との相互作用を必要としないどころか、認めないものが大多数を占めるようになるということだ。さらにIoT接続の大多数は無線（Bluetooth、Wi-Fi、セル方式、5Gなど）で行われるようになる。そしてその多くのセキュリティプロトコルは脆弱であり、容易に悪用することが可能なのである。

技術が伝播するにつれ、その技術に対応するガバナンス・アレンジメントが及ぶ範囲も拡大する。したがってインターネットに転移が生じれば、必然的にグローバルインターネット政策体制の複合体、すなわちインターネット・ガバナンスを多少なりとも扱う一連の機関やプロセスの転移が生じることになる。その結果、政策体制の複合体に極度な分散化が生じる。インターネットを統轄する単一の事業体や機関、プロセスは存在せず、多種多様な当事者（国際機関、マルチステークホルダー組織、民間企業、主権国家、国内当事者（国家安全保障機関、規制当局、立法機関、地方政府、裁判所など）など）がそれぞれ関与するガバナンスの拠点が数多く存在するようになるのだ。

当事者間に不協和音が生じ、各々の交流が複雑化しつつあるなかでも、相互接続性を確保するためには、ドメイン名やIPアドレスなどの重要なインターネットリソースを全世界で一意的に割り当て、ネットワーク化されたハードウェアとソフトウェアに共通の規格とプロトコル（TCP/IP、BGP、Wi-Fi、5Gなど）を使用することが極めて重要となる。加えてデジタル経済のほとんどの分野でグローバル化が大幅に進んでおり、市場は西欧と東アジアの企業に集中している。この事実は、ニュースの消費や電子メール、検索、地図 作成などの重要なサービス、さらには重要なハードウェアやソフトウェア全体に大きな影響力を与える巨大テクノロジー企業が国家の前に立ちはだかっていることを意味している。そのため、国家が自ら望むようにインターネット・ガバナンスを形成する能力は大幅に制限されている。にもかかわらず、しばしば使われる比喩に反してインターネットは「未開拓の西部」ではない。インターネットは本質的にルールによって支配される領域であり、高度の協調とコンプライアンスを必要とする領域なのである。サイバー問題とは、ガバナンスに関する新たな課題を提示するものである。しかし、インターネットを統轄する主体として想定される存在があまりにも多すぎること、そしてガバナンス・アレンジメントがあまりにも少なすぎることも、それに匹敵する問題となっているのである。

したがって、インターネット自体と同じく、サイバー政策に関するガバナンス・アレンジメントにも二次元的な転移が急速に生じている。すなわち、(1) グローバルなサイバーガバナンスとサイバー政策への関与を目論む当事者の数と種類という次元であり、(2) 衝突回避、すなわち国境を越えたデータフロー、機密情報や個人情報の取扱、規制当局による監視を巡る対立、サプライチェーンのサイバーセキュリティ、人権保護、政治演説の抑制、ニュースフィードアルゴリズムの調整などの問題に関して、異なる当事者間やガバナンスプロセス間で生じている対立の解決に関する問題という次元である。この２つの次元において転移が生じていることから、あらゆる問題領域とあらゆる国において、インターネットとそのガバナンス・アレンジメントの双方が、さまざまな制度やガバナンス・アレンジメントと複雑に絡みあう現象が生じている。この問題は、まさにシステム全体に関するものであり、国際システムを構成するすべての要素が 避けて通ることができないものである。なぜなら、この問題は急速に、かつ無秩序に発生しているものであり、しかも莫大な影響をもたらすものであるからだ。この問題は、国際システムの運営、さらにはその存続能力にも根本的な変革をもたらす可能性を秘めている。

インターネット・ガバナンスにおける協力と協調とは、自然に生まれるものではなく、計画的に策定し、管理しなければ生まれないものである。そのためには、不正行為を誘引する状況においてコンプライアンスを監視する方法を考案するとともに、緩やかに関連し合い、一部が重複する複数の規則を新たに発生した事例に合わせて解釈し、適用する方法を考案する必要がある。また民主的な管理と説明責任に対する要求を満たし、（規模の大きな当事者ほど、自らの要求を実現しやすい立場にある状況において）公平性を確保するとともに、調和を求める世界的な圧力に直面してもなお、国内政策を形成する力を規模の小さな当事者に与える必要もある。

インターネット転移という現象がもたらす影響は、３つに分類される。１つ目は、政策とガバナンスに関するものである。多くのガバナンス・アレンジメントは、その存続の可否がインターネット・ガバナンス体制の存続の可否によって左右されるようになりつつある。その背景には、インターネットへの依存度の大きさと、政策の重複がある。同時に、インターネット転移が生じることにより、純然たる国内政策の余地が小さくなっている。いまやすべての政治共同体が、システムの影響を受けるがそれを支配できない開放的な小国の様相を呈している。

２つ目の影響は、地政学に関するものである。グローバルな影響を与える可能性があり、さらには国家権力に影響を与える可能性がある規制制度の制定と執行を目論む国が増えつつある。例えば、最近では米国と欧州連合がプライバシー保護と反トラスト対策に関する独自の見解を主張しようと目論んでいる。両者は、自由民主主義の価値観を認める政治制度という点では類似しているが、その見解には大きな隔たりがある。ロシアと中国は、いずれも同じように自国本位の目標に有利な状況をもたらすべく、グローバルに影響力がおよぶ国内規制プロセスを利用することで、大国間の競争に加わっている。

3つ目の影響は、システム全体に及ぶものである。ロシアと中国は、主権国家の管理下におけるインターネット規制を率先して進めているが、そこには「権威主義的多国間主義」と呼ぶことができる思想の高まりを見てとることができる。その思想とは基本的に、グローバルなガバナンス・アレンジメントが有する自由主義的なDNAを弱め、西側諸国を弱体化させることを最終的な目的とするものである。

これらはいずれも、サイバーガバナンスに関するグローバルな協力と協調の重要性が増しているにもかかわらず、その実現がさらに困難になっていることを示唆して いる。

レイモンド教授の報告に続き、質疑応答セッションが行われた。参加者からは最初に、(1) インターネット転移の近年で最も特徴的な出来事は何か、そして (2) 転移を続けるインターネットにガバナンスも追いつこうとして生じた、想定外の影響として、最も重要ものは何かという質問がなされた。レイモンド教授はまず2つ目の質問に対し、ある逸話を例にとって回答した。2022年1月、カザフスタンを深刻な政情不安が襲った。その主な原因は、2021年に中国が暗号通貨のマイニングを禁止したことによって生じた想定外の影響にあった。カザフスタンは開放的なサイバー政策を採用していたことから、暗号通貨のマイナーが中国からカザフスタンに避難した。そのため、マイナーのサイバーファームによるエネルギー需要が急増し電気料金の急騰が生じた。それを引き金として発生した暴動によって政府が転覆したのである。またレイモンド教授は新たに発生した特徴的な傾向として、著しい不安定化と人権の軽視、暴力の増加を最も重要な特性としてあげた。2021年1月6日にワシントンD.C.で発生した暴動は、ある意味において、制御不能なソーシャルメディアが主導して起こった、(偽) 情報環境による政治の二極化と公的制度への不信、規範逸脱行為に対する自己規律の低下だった。

2人目の参加者からは、(1) レイモンド教授の見解は悲観的なものなのか、もし悲観的なものだとすれば、やや悲観的なのか、それとも極めて悲観的なのかという質問、ならびに (2) 現在のサイバーガバナンスに対する主な課題は中国なのかという質問がなされた。レイモンド教授は自らの見解が悲観的なものであると認める一方で、人類の歴史は危機や災害により幾度となく転換点を迎えてきたものの、これまでのところ我々は生き延びているという考えに希望を見いだしていると回答した。また中国が主な課題となっていることは事実だが、中国だけが問題をもたらしているのではなく、自由民主主義世界も同じく過ちを犯し、同じく良からぬ考えを抱いているのだと指摘した。

3人目の参加者はレイモンド教授に対し、抑止力のない状態でインターネット転移が生じた場合に、どのような悪夢的なシナリオが想定されるかと質問した。レイモンド教授は、ソーシャルメディアの規律が守られなければ、壊滅的な政情不安が生じうると考えるのが妥当だと回答した。ソーシャルメディア企業による自主規制を容認するか、あるいはすべてを「市場任せにして」放置してしまえば、自らの最も基本的な本能に従って行動する力を人々に与え、文明社会としての規律は大幅に失われることになる。

次の参加者は、国内の政治体制や法律制度は、グローバルなガバナンスの展開と技術の発展に追随して変化することが可能なのか、と質問した。レイモンド教授は、その点が課題であることを認める一方で、最も賢明な対策は、社会科学研究に多額の資金を投じ、技術の変化を巧みに取り入れる方法を明らかにすることだと回答した。この問題を端的に示す例が、新型コロナウイルスのパンデミックである。多くの地域では、最先端のワクチンを開発すること以上に、人々にワクチンを接種させることの方が大きな問題だった。サイバー政策もまた同じ経緯を辿っている。人々にソーシャルメディアを利用させることは全く難しい問題ではない。明らかになったの は、人々に責任を持ってソーシャルメディアを利用させることが極めて難しいということだ。幸い、社会科学にはさほど費用はかからない。したがって、比較的低コストで改善可能な余地が大きく存在しているのである。同様に、国と国際機関のガバナンス能力の強化に向けて多額の資金を投じ、可能な限り効果的な政策を履行できるようにすべきである。

次の参加者は、個々の政治主体が、各々の嗜好に適したサイバースペースを備えることが可能となるようなインターネットの再拡張を実現する革新的な技術が誕生する見込みはあるかと質問した。レイモンド教授は、人々がそれぞれの嗜好にあわせて情報をフィルタリングし、蓄積する技術は既に存在しているが、この技術が機能するためには、複数のネットワークで構成されるグローバルなネットワークが存在することが条件になると回答した。また技術によって社会問題を解決することは可能かという、より幅広い質問に関しては、人間は邪魔なものを壊そうという強い意志を持ち、そうすることで独創性を発揮するものだと指摘した。社会問題に解決策があるのであれば、その解決策は基本的に社会的な性質のものとなる。したがって技術的な解決策のみに重きを置いて投資することは賢明ではないと述べた。

次の参加者は、政治体制の種類について、民主主義／権威主義という単純な二元論よりも現実的で有用な分類法は存在するか、またそのような分類法が存在するのであれば、それによりサイバーガバナンスに対するアプローチに資する情報を得る方法とはなにか、と質問した。多くの国は、上記の二元論的分類の中間に位置するグレーゾーンに属すると考えられる。レイモンド教授は、二元論的分類のどちらにも完全には該当しない「振子のよう

な国」が存在することを認めたものの、いずれかの分類を代表するような国でさえ想定外の行動を取りうるものであり、そうである以上、どのような分類システムを厳密に確立したとしても、その有用性は損なわれると指摘した。例えば、ロシアと中国は、国連システムにおけるサイバーガバナンスについて、自由度の小さい性質のものにしようと目論んでいる。その際、両国がそのための手段として選択したのは、国連総会の政府専門家会合のプロセスが「民主的ではない」という論拠を持ち出し、そのプロセスを批判するという方法であった。両国は政府専門家会合に代わるものとして、あらゆる国の参加が可能なオープンエンドワーキンググループの設立を最終的に目指している。実際のところ両国は、国連の過半数が権威主義国家であるという事実につけこみ、自由民主的な包摂性を規範とする姿勢に都合よく利用しようとしているのである。

次の参加者は、米国がサイバースペースの「覇権」を享受するための興味深い方法は存在するか、またサイバードメインの脆弱性が増す方向、または強靱性が増す方向に向かうような明確な傾向は見られるか、と質問した。レイモンド教授は、脆弱性が増す方向に向かう傾向が明確に見られると回答した。いまや兵器と化したソーシャルメディアにより、何が起こりうるのかを目の当たりにした時、危機感を実感したという。また脆弱な IoT デバイスへの依存性が急速に高まっていることも、軽視されがちな問題のひとつである。米国がサイバースペースの覇権を手にしているかどうかについては、断言するのは難しい。なぜなら、覇権とは曖昧な概念であり、もし覇権が存在するのだとすれば、それは社会認識によって左右されることになるからだ。インターネットの技術インフラの維持において、米国の企業と組織が極めて大きな役割を担っているのは明らかである。しかし米国全体としては、サイバーガバナンスにおけるリーダーとしての役割を担うことを他国から大いに期待されているとしても、そのためのビジョンが不足しており、その目的にもばらつきがみられる状況にある。

次の参加者からは、脅迫的な行為者との闘争における政府機関とソーシャルメディア企業との間の協力関係について、「対テロ世界戦争」から得た教訓に対するレイモンド教授の見解を問う質問がなされた。レイモンド教授は、この種の協力関係は基本的には重要なものであるが、物議を醸す行動をしがちな比較的少数の人々（マー ク・サッカーバーグやイーロン・マスクなど）により、その協力関係がすぐ難しくなってしまうことが大きな問題であるとの見解を示した。ソーシャルメディア企業に対する適正な規制が施行されるまでは、この種の官民パートナーシップによる利益は限定的なものとなるだろう。

最後の質問は、レイモンド教授が語った物語において、ヒーロー的役割を果たす正義の勢力（たとえば欧州連合など）は存在するか、というものであった。レイモンド教授は、その存在を否定した。EU はデータプライバシーを保護し、傍若無人なソーシャルメディア企業を統制しようと試みたが、EU ウェブサイトを閲覧する際に Cookie を受け入れるかどうか判断することを利用者に強いたことを除けば、ほとんど成果はあがっていない。EU 内では、他のほとんどの地域と同様に、依然として利用者のデータが売買されている。レイモンド教授はさらに重要な点として、ヒーローというものを基本的に信頼していないと言明した。ヒーローとは、我々が自らの問題を解決するために取り組まなければならない苦労から、我々を開放する存在である。しかし、インターネット転移に直面する我々に対し、救いの手を差しのべる存在はどこにもいない。我々は自ら進んで課題に取り組まなければならないのである。

グローバルな文脈での日本

サイバーセキュリティとサイバーガバナンス

2022 年 10 月 13 日
国際文化会館

報告者

・土屋 大洋（慶應義塾大学大学院政策・メディア研究科／総合政策学部 教授）
“Cyber Great Game: International Politics Transformed by Digital Technologies”

・マーク・レイモンド（オクラホマ大学サイバーガバナンス・政策センター所長）
“Policy, Governance and Geopolitical Implications of Global Internet Metastasization”

参加予定者

・田所 昌幸（国際大学大学院国際関係学研究科特任教授）
・デイヴィッド A. ウェルチ（ウォータールー大学教授）
・阿川 尚之（慶應義塾大学名誉教授）
・秋田 浩之（日本経済新聞社本社コメンテーター）
・飯塚 恵子（読売新聞社編集委員）
・川波 竜三（大阪国際大学経営経済学部講師）
・黒木 隆一（NTT コミュニケーションズ株式会社）
・合六　強（二松学舎大学准教授）
・相良 祥之（アジア・パシフィック・イニシアティブ（API）主任研究員）
・彦谷 貴子（学習院大学教授）
・李　承赫（東北学院大学准教授）
・山口　昇（国際大学大学院国際関係学研究科教授）

公益財団法人サントリー文化財団

・尾崎 勝吉（専務理事）
・山内 典子（上席研究員）
・王　量亮（研究員）

土屋大洋

慶應義塾大学大学院政策・メディア研究科／総合政策学部 教授。2019年４月から日本経済新聞の客員論説委員を務める。著書に『情報による安全保障』（慶應義塾大学出版会、2007年）、『サイバー・テロ』（文藝春秋、2012年）、『サイバーセキュリティと国際政治』（千倉書房、2015年）、『サイバーグレートゲーム』（千倉書房、2020年）。また Cybersecurity: Public Sector Threats and Responses s (Boca Raton, FL: CRC Press, 2012年）他、40冊の共著がある。慶應義塾大学法学部政治学科卒業後、同大学大学院法学研究科で修士号（国際関係論）、同大学大学院政策・メディア研究科で博士号（政策・メディア）を取得。2019年に、第15回中曽根康弘賞受賞。

マーク・レイモンド

オクラホマ大学サイバーガバナンスポリシーセンター所長、同大学ウィック・ケリー国際関係学准教授。政策に関する解説記事を *Lawfare* や *The Monkey Cage* などに寄稿。米国サイバースペース・ソラリウム委員会の上級顧問を務め、国連開発のための科学技術委員会において証言し、インターネット・ガバナンス・フォーラムにも参加した。インディアナ大学オストロム・ワークショップ外部会員。これまでにセンター・フォー・デモクラシー・アンド・テクノロジーのフェロー、コロンビア大学国際公共政策大学院カーネギーフェローを務める。主な著書として *Social Practices of Rule-Making in World Politics*（New York：Oxford University Press、2019年）がある。