Cyber Security and Democracy

Cyber Security and Democracy

サイバーセキュリティと民主主義

まえがき

溶けだした世界で民主主義は可能か

若林恵（編集者）

Photo by Paul Hennessy/NurPhoto via Getty Images

Starlinkの衛星を積んだロケットの打ち上げ

後退する「国家」

サイバーセキュリティをめぐる議論は、「国家安全保障」という語をひとつのキーワードとしている。国のインフラストラクチャーの安全、国家機密から個人情報に至るまでの各種の情報資源の安全、さらには国を不安定化させるようなメッセージやナラティブからメディア空間を守るという意味での安全。保障されるべき安全は、多岐にわたる。デジタルテクノロジーが行政から民間企業、そして個々人が生きる社会空間や経済空間のすみずみにまで行き渡った結果、サイバーセキュリティが安全を保障すべき空間は、すでにして「国家が管理する社会の全部」に及んでいる。であればこそ、サイバーセキュリティが「国家安全保障」という命題のなかで遂行されるのは、当然のことと言える。

けれども「国家安全保障」は、グローバル経済以前の世界やデジタルテクノロジー以前の世界において想定されていたものよりも、はるかに複雑なものとなっている。デジタルテクノロジーを提供するプレイヤーやグローバル経済を牽引するプレイヤーは、国家の枠組みを超えて活動し、国家の舵取りに多大な影響を与えるものとなっている。別の言い方をするなら、「国家」はもはや、政治・経済・文化等の安全を保障する最高にして無二の主体ではなくなっている。1999年に刊行されたある軍事書は、その成り行きを、20年以上前にこう喝破している。

> *歴史的に見ると、国家はかつて安全理念の最高形態であった。（中略）今は民族や地理的意味における国家は、「地球村」の中にある人類社会という鎖の大小さまざまの輪にすぎない。現代国家はますます地域的および全地球的な超国家組織（例えば、EU、ASEAN、OPEC、APEC、IMF、世界銀行、WTO、および世界最大の組織である国連等）の影響を受けて*

いる。このほか、複数の国家にまたがる多くの組織やさまざまの非国家組織（例えば、多国籍企業、業種組織、グリーンピース、オリンピック委員会、宗教団体、テロ組織、ハッカーグループなど）も同様に、国家の進む方向を左右している。これらの複数の国家にまたがる組織、あるいは非国家組織、超国家組織は、新興のグローバルパワー・システムを共同で構成している。

気づいた人があまりいないかもしれないが、以上の要因は、大国の政治が超国家政治に席を譲る転換期へとわれわれを導いているのである。この時期の主な特徴はつまり、過渡的ということであり、多くの手がかりが現れ、多くのプロセスが現在始まっている。国家の力を一つの主体とし、超国家、多国家、非国家の力をもう一方の主体とすれば、国際舞台でどちらが浮き、沈むかはまだ定まっていない。（中略）

いくつかの兆候が一種の趨勢を示している。すなわち、国と国との戦争によって勝負を決める時代は終わりつつあり、超国家的手段を用いて、国家よりもっと大きな舞台で問題を解決し目標を実現する時代が、静かに幕を開けようとしている。

超国家／多国家／非国家的なプレイヤー

新たな時代の幕開けをこのように予告したのは、喬良、王湘穂というふたりの中国の軍人が著した『超限戦：21世紀の「新しい戦争」』（角川新書）[*1]という本だ。この本は、そもそも「21世紀の戦争」がどのようなものになるのかを分析することに主眼を置いたものであるがゆえに、国家の役割の後退を論じるにあたって、来るべき戦争のあり方に焦点があてられている。

なればこそ、戦争という極限的な状況を通じてサイバーセキュリティを理解することを必ずしも主旨とはしていない本レポートにおいて、本書を参照することはいささかの飛躍があるかのようにも見えるかもしれない。しかしながら、前記の引用で示された通り、国家の構成要素を成す「国民」の命運の舵取りが、国家というものによって一元的にガバナンスされず、国家をはるかに凌駕するパワーをもつ超国家／多国家／非国家的なプレイヤーによって左右される状況が進行し、その影響力の拡大が経済、政治、文化にまで浸透していくほどに、わたしたちが直面する状況は恐るべきものとなっていく。本書には、こんなことも書かれている。

戦争を軍事領域に限定し、死傷の多少をもって戦争の熾烈度を測る観念が日増しに時代遅れのものになっている。戦争は血まみれの殺戮の世界から抜け出し、少ない死傷者、ひいては死傷者ゼロでありながら熾烈度がかえって高いという趨勢を示しつつある。これは情報戦、金融戦、貿易戦など全く新しい戦争様式が、戦争の領域で新たに切り開いた空間である。この意味では、もう戦争に利用されない領域などなく、戦争の攻撃的な形態を備えない領域もほとんどなくなっている。

（中略）

経済援助、貿易制裁、外交斡旋、文化の浸透、メディアによる宣伝、国際ルールの制定と利用、国連決議の利用などといった手段は、それぞれ政治、経済、外交など異なる領域に属すると同時に、政治家たちによって、準軍事手段としてますます運用されている。

政治は戦争の延長である

近代戦争論を体系化したとされるクラウゼヴィッツは、「戦争とは別の手段

をもってする政治の延長である」という名言を残した。そして、その議論を下敷きに、わたしたちは「政治」において万策が尽きたあとに検討される最終手段として「戦争」というものをイメージしてきた。しかし、『超限戦』はそうした戦争のイメージを180度転換させてしまう。『超限戦』が語るのは、もはや「政治とは別の手段をもってする戦争の延長である」ような世界だ。いや、政治だけにはとどまらない。経済、文化を含めたあらゆる社会活動の領域が「戦争の延長」として展開されるのが21世紀の世界だとするのが、『超限戦』の見立てなのだ。

突拍子もない見立てのように思えるかもしれないが、サイバーセキュリティという問題を考えていくと、それが必然的に、個人情報の保護やソーシャルメディアにおける誤情報・偽情報の管理といったミクロのレベルから、軍事的な意味での国家防衛を含めたマクロな政治のレベルまでをも包括せざるを得なくなるという状況を説明する上で、この見立ては有効に思える。この見立てが、アメリカ、ロシアをして「ハイブリッド戦争」なる新たな戦争の形態の整備を急がせたことを思えば、なおさらだ。

2022年2月に発生したロシア軍によるウクライナ侵攻以後、頻繁に語られた「ハイブリッド戦争」の語は、現代の「戦争」がもはや物理空間に限った闘争ではなく、サイバー空間、経済空間、情報メディア空間にまたがっている状況を説明するが、それが指し示す内容を深く真に受け入れるなら、ハイブリッド戦争は、軍事侵攻が始まる前に、経済制裁やメディアを通した情報操作といった行為を通して、すでに始まっていたことになる。わたしたちが「平時」だと思っていた時間は、すでに「戦争の時間」だったのだ。そして言うまでもなく、そのような「平時における戦争」に関与しているのは、国家的主体ばかりではない。そこには超国家／多国家／非国家的なプレイヤーが縦横無尽に入り乱れている。

その象徴的な出来事のひとつとして、ウクライナ戦争においてイーロン・マスクが保有する通信衛星企業「Starlink」が引き起こした騒動がある。

騒動の発端は2022年の秋、ウクライナ政府がクリミア半島上空で衛星通信網を利用させてくれとイーロン・マスクに依頼したことに始まる。ところが、マスクがそれを拒否したことでアメリカのメディアから強い非難の声が上がった。アメリカが支持し支援している軍事作戦への協力を、アメリカを拠点とする企業が拒否するとは何事か、というわけだ。マスクは、のちに、もし協力依頼がアメリカ政府からのものであったなら喜んで協力しただろうと語っているが、実際の経緯はもう少し複雑だ。

クリミア半島上空にはすでにStarlinkの衛星が飛んでいたのだが、それが2022年の秋時点で稼働を停止していた。その理由として、ロシアによって接収されたクリミア半島は「ロシア領」と見なされアメリカによる制裁の対象となっていたことから、稼働を停止していたといったことが挙げられている。つまるところ、Starlinkは経済制裁とウクライナ軍の実際の軍事作戦の間で板挟みになったというのが真相だったと、イーロン・マスクの評伝を書いたウォルター・アイザックソンも認めている（評伝『イーロン・マスク』における記載が誤りであったことを、アイザックソンは刊行後にX上で認めた）[*2]。

イーロン・マスクの政治的意図はどうあれ、彼が保有する企業はアメリカ国内外問わず政治的争点が交差する地点において、各国の判断を左右する重要なキャスティングボートとなっているが、それはStarlinkに限らない。宇宙開発をめぐる国家間競争における「SpaceX」、各国が発信する政治的言説やナラティブのせめぎ合いにおける「X」、あるいは熾烈を極める米中のEV戦争における「Tesla」など、イーロン・マスクのビジネスの影響力は、もはや国家のいくつもの重点領域にまたがる広範なものとなっている。実際、

イーロン・マスクのXをめぐる戦略はアメリカ大統領選の帰趨に絶大な影響を与えているだけでなく、マスクの訪中[*3]やアルゼンチン大統領ハビエル・ミレイ[*4]との会談は、国家首脳同士の会談と同等もしくはそれよりも大きな注目を集めている。

輪郭を失う「民主主義」

サイバーセキュリティをめぐる困難は、端的に言うなら、領域というものをセグメントすることの困難にほかならない。国家的な領土に基づく物理的な領域の線引きも、軍事・外交・政治・経済・文化といった対象領域における線引きも、あるいは政府・企業・超国家／非国家組織といった行為主体における線引きさえもが融解してしまい、あらゆる境界線が不分明なものとなってしまう。

そうした状況のなかで、ついこの間まで、国家というもののひとつの統治原理として掲げられていた「民主主義」といった理念も、枠組みを失って曖昧化してしまう。それどころか、2024年のわたしたちに見えているのは、むしろそれが「戦争の延長」に置かれ、恒常的に兵器化されているといった景色なのかもしれない。

物理空間における統治主体として独占的な地位にあった国家／政府が、その座から後退を余儀なくされ、融通無碍にかたちを変えていくグローバルパワー・システムの一部へと組み込まれていくなか、市民・国民ひとりひとりの主体性も輪郭を失ってしまう。民主主義国家において主権性をもつとされた、かつて「国民」と呼ばれた集団は、いまはむしろ、ソーシャルメディア上で闘争に明け暮れる顔なき歩兵としての役割において、その存在意義を見いだされているかのようにも見える。

そもそも「民主主義」というものは、戦争状態となった際には、真っ先に放棄されるものでもある。わたしたちの生活する空間と時間のすべてが、戦争の延長線上にあるものとして位置付けられたとき、そこに民主主義というものが存在しうる余地があるのかすらわからない。

本レポートは、そうした難題に取り組むための手がかりを探るもので、言うまでもなく、そこに答えを見つけるには到底至らない。『超限戦』が記した通り、この時期の主な特徴は、過渡的ということだ。現れつつある手がかりのなかにおいて始まっている、多くのプロセスを洗い出し検討することを、本レポートでは試みた。

＊1｜喬良、王湘穂『超限戦：21世紀の「新しい戦争」』、坂井臣之助＝監修、劉琦＝訳、角川新書、2001年に共同通信社より刊行。2020年に一部加筆修正の上、角川新書より復刊
＊2｜“Elon Musk biographer moves to ‘clarify’ details about Ukraine and Starlink after backlash” CNBC, Sep. 9, 2023 https://www.cnbc.com/2023/09/09/elon-musk-biographer-moves-to-clarify-details-on-ukraine-starlink.html
＊3｜“Elon Musk wins official praise for Tesla during surprise visit to China” CNN, Apr. 29, 2024 https://www.cnn.com/2024/04/29/cars/elon-musk-surprise-visit-china-premier-li-intl-hnk/index.html
＊4｜“Argentina’s populist president meets billionaire Elon Musk in Texas — and a bromance is born” AP, Apr. 13, 2024 https://apnews.com/article/milei-musk-tesla-spacex-argentina-us-texas-economy-7af43102c5dcf5398a97d1010463f5a1

若林恵｜Kei Wakabayashi｜黒鳥社コンテンツ・ディレクター。平凡社『月刊太陽』編集部を経て2000年にフリー編集者として独立。以後、雑誌、書籍、展覧会の図録などの編集を多数手がける。音楽ジャーナリストとしても活動。2012年に『WIRED』日本版編集長就任、退任後の2018年に黒鳥社設立。著書『さよなら未来』（岩波書店）、編著『次世代ガバメント：小さくて大きい政府のつくり方』『ファンダムエコノミー入門：BTSから、クリエイターエコノミー、メタバースまで』『週刊だえん問答』シリーズなど。「こんにちは未来」「働くことの人類学」「blkswn jukebox」「音読ブラックスワン」などのポッドキャストの企画制作でも知られる。

特別講義

サイバーセキュリティと民主主義
山本龍彦

山本龍彦｜Tatsuhiko Yamamoto｜慶應義塾大学大学院法務研究科教授、慶應義塾大学グローバルリサーチインスティテュート（KGRI）副所長。1976年生まれ。2005年、慶應義塾大学大学院法学研究科博士課程単位取得退学。博士（法学）。桐蔭横浜大学法学部専任講師、同准教授を経て現職。2017年、ワシントン大学ロースクール客員教授、司法試験考査委員（2014年・2015年）。主著に『デジタル空間とどう向き合うか』（日経BP、共著）、『AIと憲法』（日本経済新聞出版）など。

※本テキストは2024年2月5日（月）、7日（水）に行われた「サイバーセキュリティと民主主義」における山本龍彦氏の講義、およびその後の有識者らによるラウンドテーブルの内容を再構成したものです。

1

私企業と国家

講義

リヴァイアサンとビヒモスの戦い

山本龍彦（憲法学・慶應義塾大学大学院法務研究科）

Kean Collection/Getty Images

ギュスタフ・ドレ「リヴァイアサンの破壊」。19世紀

わたしの専門は憲法学ですが、最近はプライバシー、個人データの保護など、主にテクノロジーと人権、民主主義の関係について考えてきました。その関係でいろいろな政府の会議にも参加しています。

直近では総務省の「デジタル空間における情報流通の健全性確保の在り方に関する検討会」（2023年11月～）に座長代理として参加しています。この検討会ではフェイクニュース、フィルターバブル、エコーチェンバーなどの問題に対してどういった対策、対応があり得るのかということを考えていますが、さらにもうひとつワーキンググループが立ち上がりまして、その主査も務めているところです。

設置の直前に能登半島地震が起き、そこで偽情報の拡散があって注目されましたが、実際にはその前からすでにプラットフォームに対して一定の法規制が必要なのではないか、ワーキンググループを立ち上げるべきだという議論はずっとありました。

公衆衛生から国家は生まれた

第1部のテーマは「私企業と国家」です。特に巨大テック企業、デジタルプラットフォーム企業について考えたいと思います。わたしがこのテーマに関心をもったのは、新型コロナウイルス接触確認アプリ（COCOA）の有識者検討会議（接触確認アプリに関する有識者検討会合）に参加したときのことです。

当初、日本における接触確認アプリの開発はシビックテック団体「Code for Japan」が手掛けていましたが、アプリ開発にあたって利用を想定していたGoogle、Appleが共同開発した濃厚接触者との接近を知らせるAPI（Exposure Notification API）の提供条件が「提供先は各国の保健当局（日本は厚生労働省）のみ」「1国1アプリ限定」とされたため、開発体制が急遽大幅に転換され、一定の混乱が生じました。

このとき、「こう進めたい」という政府の方針があっても「Google、Appleの利用条件がこうなのでできません」と覆されるような格好になったわけです。感染症対策というのは主権国家において非常に重要で、ヨーロッパでは「公衆衛生から国家が生まれた」と言ってもいいほどの歴史があるにもかかわらず、プラットフォーム企業にそれを規定されるということを目の当たりにして「これは何か大きなことが起きていそうだ」と思ったのがひとつのきっかけです。

余談ですが、Google、AppleのAPIを利用しなかった国のひとつにフランスがあります。フランスでは自国民の健康保護を主権の問題と捉えており、こうした問題を民間の、しかも外国のプラットフォームに委ねるべきではないとして、自前のアプリをつくるという考え方を取ったわけです。結局どちらが良かったのかは非常に難しいところですけれども、やはり国家主権の問題とかなり密接にリンクしているということがわかるかと思います。

国家を凌駕する権力

憲法は基本的に国家権力を相手にする法であり、権力を統制して自由と民主主義を守るという、リベラルデモクラシーの考え方に則っているわけですが、もはやプラットフォームの権力が国家を凌駕しつつあるとするなら、そのとき、憲法学はいったい何をすればいいのだろう。そういった近代の主権体制のあり方そのものに大きな悩みを抱き始めました。

「国家を凌駕しつつあるプラットフォームの権力」の例は他にもあります。2016年の米大統領選で起こったケンブリッジ・アナリティカ事件もそうです。これはイギリスの選挙コンサルタント会社が、Facebookのデータを使ってユーザーの心理特性、認知傾向などをプロファイリングし「フェイクニュースに騙されやすい人」に対してフェイクニュースとの接触頻度を高めることによって、投票行動を操作していたのではないかと指摘されました。

ケンブリッジ・アナリティカ元社員のクリストファー・ワイリーが『マインドハッキング：あなたの感情を支配し行動を操るソーシャルメディア』[*1]という暴露本を書いていますが、彼はこのやり方を「心理戦版大量破壊兵器」と呼んでいます。つまりAIやアルゴリズムは、われわれの精神や内面、特に認知過程に深く介入してコントロールすることを可能ならしめるということがわかってきたということです。そういった「AIとかアルゴリズムを支配している存在は誰か」といえば、今後は、例えばOpenAIなのかもしれませんが、OpenAIの後ろにはMicrosoftがいるわけで、やはりプラットフォームということになってきます。

プラットフォーム権力の源泉

では巨大テック企業、プラットフォーム企業の権力の源泉とは何か。わたしは以下の7つが挙げられると考えています。

1. 巨大性・独占性

例えばFacebookの月間アクティブユーザー数は30億人を突破しており、Appleも売上高がイスラエルや香港のGDPに相当するほどになっています。商品やサービスの利用者が増えれば増えるほどその価値も増大する「ネットワーク効果」もあるでしょうが、これに拍車をかけたのが、アメリカで1996年に制定された通信品位法だろうと考えています。

通信品位法第230条において、プロバイダーやプラットフォーム企業は投稿される情報に対して基本的には責任を負いません。この法では、プラットフォーム企業が仮に有害なコンテンツをホストし

てしまったとしても、単なる媒介者でしかないのだとしています。国際慣習法では「被告側が国家ならば外国の裁判権から免除される」という「主権免除」の考え方がありますが、通信品位法はプラットフォームにデジタル領域を裁量的に統治する「主権免除」を与え巨大化させる口実を与えたようなものです。

2. インフラ性・親近性

プラットフォーム企業は、いまやそのサービス抜きではわたしたちは日常生活を送れないほどのインフラの提供者になっています。加えて、これまでの生活インフラと比べて、極めて親近性が高いものでもあります。親近性とは、スマートフォン、スマートウォッチなどのガジェットを通じて個人の身体に最も近い領域、身体に近接する領域にその場所を占めていることを意味します。新聞やテレビ・ラジオの放送に関わる企業と比べても、それはわたしたちのはるか近くに存在しています。

3. 国家に対するデータ的・技術的優位性

Yahoo! は2020年4月、政府に対して新型コロナウイルス感染拡大防止に資するデータを提供しました。いままでは国家がデータを出せと言えば「はい、わかりました」と出していたでしょうが、このときYahoo! 側はプライバシーに関する外部有識者で構成される「プライバシーに関するアドバイザリーボード」を設置し、ユーザーのプライバシーを守るため、さまざまな条件をつけるかたちで提供しています。これも国家がプラットフォーム企業の言い分を聞かざるを得なかった事例のひとつです。

また2019年にFacebookが脳の電気信号をリストバンド経由でコンピュータに入力できるスタートアップの「CTRL-Labs」を買収したニュースがありましたが、今後、脳に関する情報までプラットフォームが得るようになった際、プラットフォーム企業の優位性はさらに高まっていくように思います。

4. ブラックボックス性・判読困難性

ブラックボックス性とは、アルゴリズムがブラックボックスとなり、暗闇のなかでさまざまな重要な意思決定がなされていくことを指します。われわれは暗闇のなかで行われる意思決定にコントロールされることになるだろうということです。

後でお話ししますけれども、いまのプラットフォーム企業と国家の関係というのは、中世におけるカトリック教会と世俗の国家・帝国との関係に近いものがあるのではないかと考えています。もちろん厳密には大きな違いもありますが、当時カトリック教会が権威性をもった大きな要因のひとつに、聖書がラテン語で書かれていたことが挙げられます。一般市民はわからないことばで行動がコントロールされているという権威性ですね。プラットフォームも同様に、一般市民にはわからないアルゴリズムでわれわれを統治しているというところに共通性があるように考えられます。

5. グローバル性・実態把握困難性

これはプラットフォーム企業だけでなく、いわゆるGAFAMへの課税の問題として話題に上ることが多いですが、従来の国際的なルールではオフィスや工場など恒久的施設がある国でのみ課税できるという考え方がなされており、世界各国でビジネスを行うIT企業への課税に困難が生じていました。つまりいまや個別の国家では、その実態を把握できないということです。2021年にようやくOECDがデジタル課税の考え方を取りまとめ、多国間条約として2025年の発効

を目指しています。

6. 経済的・政治的影響力

これはロビイングが非常に組織的、戦略的に行われているということです。アメリカでのロビイングに多額の資金が投入されていることはよく知られていますが、GAFAは日本でも官僚をヘッドハンティングしており、Apple日本法人の「政務部長」は総務省出身の人物であると言われています[*2]。

7. 感情の操作可能性・「部族」動員可能性

かつてマーシャル・マクルーハンは「メディアが視聴覚メディアに移っていくと、人間は原始的感情を取り戻してしまう」と予言していました。これは第3部でもう少し詳しく見ていくことになるかと思いますが、ショート動画なども活用しながら原始的感情を揺さぶり、ある種の「部族」をアルゴリズムによって構築できる時代になってきました。特にSNSのビジネスモデルは人びとの感情を高ぶらせて滞在時間を増やすアテンション・エコノミーですので、誹謗中傷も彼らのビジネスにおいてはなくなっては困るのです。

2021年にFacebook元社員のフランシス・ホーゲンが大量の内部資料をもち出しメディア経由で公開した「The Facebook Papers」でも、Facebookは、憎悪と怒りの感情がエンゲージメントを高め、アテンションを得やすいということがわかっていたにもかかわらず、それを止めなかったと指摘しています。プラットフォームがエコーチェンバーに基づく独自の「部族」を形成し、国を超えた社会的・政治的分断が生じれば、国民国家の崩壊をもたらしうるということです。

新しい民間主権

ホッブズは国家権力を海の怪物であるリヴァイアサンになぞらえましたが、プラットフォームの権力は陸の怪物「ビヒモス」になぞらえられるのではないかと指摘したことがあります。

例えばアメリカの国際法学者であるクリスティン・アイケンサーは、プラットフォームが疑似的な主権をもっているということをすでに指摘しています。またアメリカのジャーナリスト／ブロガーのレベッカ・マッキノンは、2012年の段階で、こんな指摘をしています。

> *フレンドリーかつ知的で若い青いジーンズを穿いたカリフォルニアンたちが立法者、裁判官、陪審員、警察の役割を同時に果たしており、サイバー領域においてある種の民間主権（プライベート・ソブリンティ）を行使している。*

「フレンドリーかつ知的で若い青いジーンズを穿いたカリフォルニアンたち」というのはFacebookの経営層のことを指しています。さらにケイト・クロニックという情報法の学者は、ハーバード・ロー・レビューに寄稿した論文で「the New Governors」[*3]という概念を提唱しました。

プラットフォーム企業のこうした権力性は、近年Web3や生成AIといった新しいビジネスモデルや技術によって抑制されていくようにも見えたものの、どうもそう簡単には制御できなさそうです。生成AIなどは、むしろプラットフォーム側にとっての強力な武器となって、権力の独占がますます加速していく可能性すらあるようにも思えてきます。

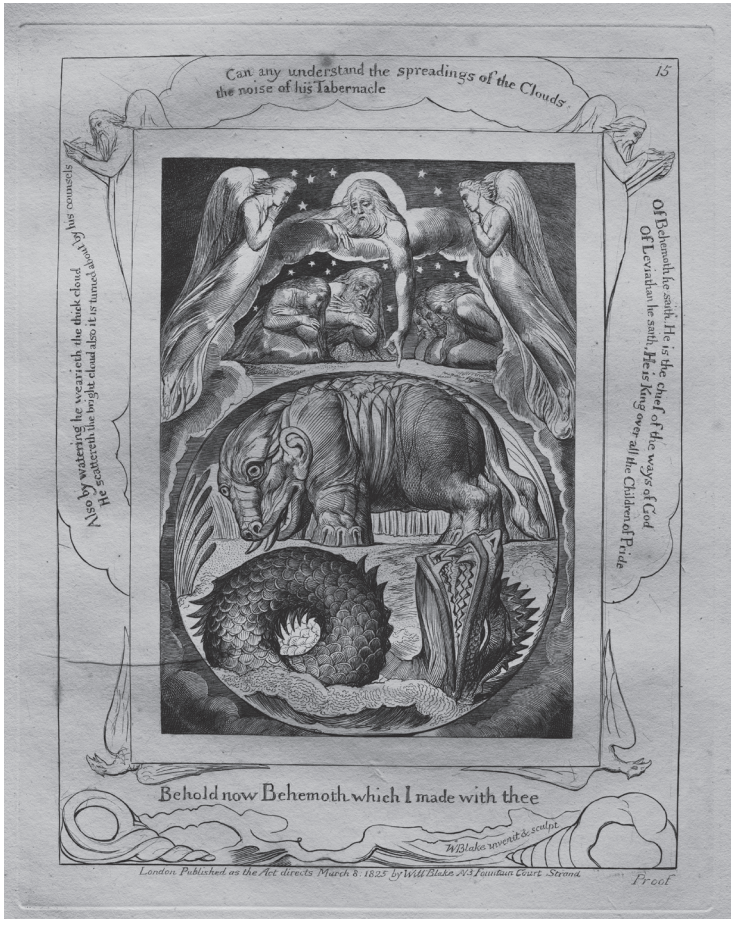

Photo by Sepia Times/Universal Images Group via Getty Images

「ヨブ記」より。ウィリアム・ブレイクによるエッチング。19世紀

権力の二重構造

中世という時代には、教会や封建領主などの多層的に存在する権力構造のなかに個人が埋没しているような環境がありました。それに対して近代の主権国家は、そうした中間権力を排除し権力構造をスッキリさせ、国家と個人を向き合わせるという二極構造の図式を取ったわけです。その単一化された権力、すなわち国家を憲法によって縛ることで自由と民主主義を守るというのが、近代の基本的な構造でした。しかし、プラットフォームが、すでに国家とは異なる主権性をもつに至っている現状は、近代国家の基本構造からはみ出してしまっています。わたしたちは、どうやら、権力構造が多元化・多層化する、新たな時代に入ってきているのかもしれません。

近代主権国家は物理的な領土の一元性、単一性をベースとしていたわけです。しかし、近年はこの領土にデジタル領域が複層的に混入してきています。わたしたちは、国民というステータスと、あるプラットフォームのユーザーというステータスの両方を抱えながら生活しているわけです。そうしたなか、デジタルの領域において、国家が国民をもはや統治できないという問題が生じています。実際、国家が国民を統治しようとすれば、プラットフォームユーザーとしての国民に働きかけなければならず、いちいちプラットフォームにお伺いを立てなければならない。プラットフォームの同意を得ないとユーザーに働きかけられないような、二重化した権力構造になってきているわけです。

脅される国家

プラットフォーム権力のこうした台頭は、単に想像上のものに過ぎないという指摘もあるかもしれませんが、すでに実例が出てきています。先ほどお

話しした公衆衛生や課税の問題にとどまりません。

例えばオーストラリアでは、2021年に新聞など旧来のメディアとデジタルプラットフォーム企業の関係性を是正すべく、プラットフォーム上で表示されたニュース記事によって得られた収益をメディア企業にしっかり還元させるための法律（ニュースメディア・デジタルプラットフォーム契約義務化法）を制定しましたが、国会での議論中、同法への抗議としてGoogleは同国からのサービス撤回を示唆し、Facebookはニュース記事表示を一時停止する措置を行いました。主権国家に対して「脅し」を利かせた格好となったわけです。それにより、最終的に法律案はプラットフォームの意向を汲むかたちで修正されることとなりました。

こうした動きは世界各国で起こっています。日本においても、プラットフォームだけの規制ではありませんが、2022年の電気通信事業法の改正（施行は2023年）が議論された際に近しい出来事がありました。国内経済団体の新経済連盟、そしてGoogle、Facebook、Amazonなどが加盟する在日米国商工会議所（ACCJ）が同法改正案についての抗議や政治家へのロビイングを行い、土壇場で規制内容が大幅に修正されたのです。

このときにACCJなどから提出された異論の内容は複数ありますが、最も大きな論点となったのがウェブサイトやアプリの利用者情報（閲覧・購買履歴など）の外部送信についてでした。これまで、こうした情報が広告事業者など第三者に送信されていたわけですが、「今後は必ず利用者の同意を得るように」という方向で決まりかけていたところ、「通知や公表のみでもOK」というかたちになり、対象となる事業者の幅も狭いまま変更されませんでした。この一連の議論内容や結果についてはさまざまな言い分[*4]があると承知していますが、今後、日本政府がヨーロッパなどに倣ってデジタルプラットフォームの規制を行う際にも同様の事態が発生する可能性は高いでしょう。

立法権だけでなく捜査権についても有名な事例があります。2015年、アメリカで起こった銃乱射事件の被疑者が保有するiPhoneのロック解除を、FBIが裁判所の令状を得た上でAppleに要請したものの、Appleは暗号化データへのアクセスを可能にするバックドア構築によるプライバシー上の懸念を理由として拒否しました。

この問題について、アメリカ政府とAppleは何度も衝突しており、大統領時代のトランプも「われわれは貿易や多くの問題で常にAppleを助けてきたんだ。しかし、彼らはロック解除を拒否している。彼らはこの素晴らしい国を助けるべきだ」とツイートして強い圧力をかけ続けましたが[*5]、それにもAppleは屈しませんでした。

プラットフォームの地政学

安全保障上の領域でもデジタルプラットフォームの影響力は相当強まってきています。詳しくは第2部でお話ししますが、エレナ・チャチコという若手の国際法研究者はStanford Technology Law Reviewで2021年に発表した「National Security by Platform」[*6]という論文において、プラットフォームの「地政学的転回」（ジオポリティカル・ターン）という概念を提示しました。つまりプラットフォームがすでに地政学的な影響力をもち始めているということを2021年に指摘したのです。これはまさに2022年のロシアによるウクライナ侵攻によって現実化しました。

具体的には、Facebookはこれまでヘイトスピーチに対するポリシーを有しており、違反した投稿の削除、投稿者のアカウント凍結などを行っていましたが、ロシアによる侵攻が発生すると、ロシア政府やロシア兵に対する暴力的投稿をウクライナやその周辺国では削除しないとする、ニュートラリティに欠くような方針転換を行いました。その数日後にはプーチンなど国家元首の死を求める呼びかけは禁止され、対象地域もウクライナのみ

に再変更されるなど二転三転しています。こうしたケースは、2022年以降だけを見ても、いくつも存在します。戦局がプラットフォームや経営者のスタンス次第で大きく左右される状況になっているのです。以下はその数例です。

- ロシア政府が、FacebookやInstagram、X（旧Twitter）への国内からのアクセスを遮断
- 西側プラットフォームがロシア国営放送関連コンテンツの掲載を停止
- イーロン・マスクがSpaceXの衛星通信システム「Starlink」の端末をウクライナへの支援として無償提供していたものの、彼の一存で追加の提供要請を拒否、ネットワーク切断が度々行われている（2024年に入ってからはロシア軍がStarlinkを活用しているというウクライナ当局の発表もある）

こうした状況を見るにつけ、国家がプラットフォームから独立して安全保障政策を実現しようと思っても、いまや不可能となりつつあることがよくわかります。

新しい「新しい中世」

1996年に国際政治学者の田中明彦先生が『新しい中世：21世紀の世界システム』[*7]という本を刊行しました。かいつまんで言えば冷戦終結後、多国籍企業やNPO、NGOといった国際機関が台頭してくる世界を、田中先生は「新しい中世」と呼んだわけですが、わたしはさらにその次の「新しい『新しい中世』」の時代に差し掛かっているのではないかと考えています。そこ

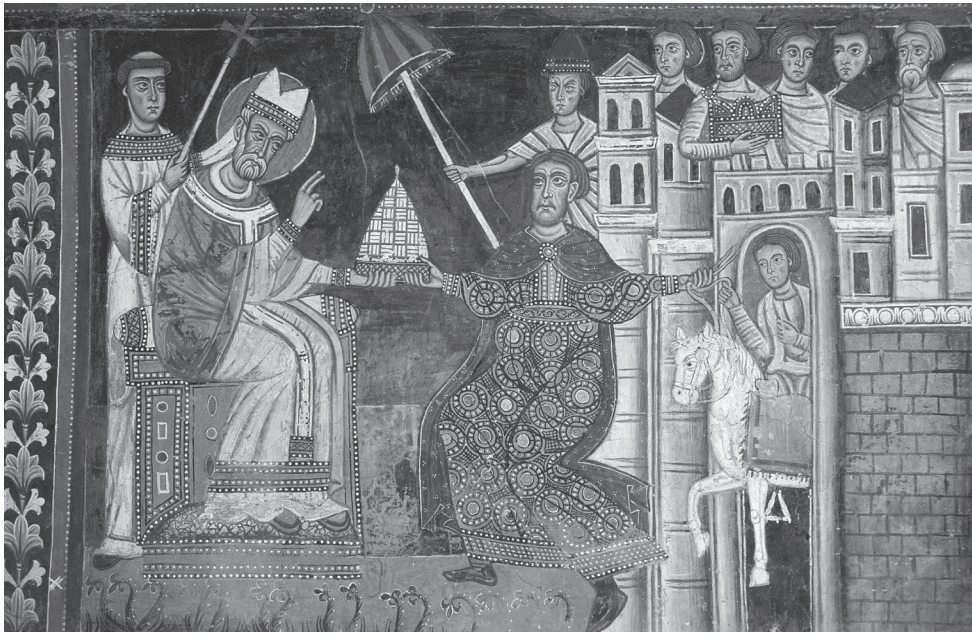

Photo by Fine Art Images/Heritage Images/Getty Images

作者不詳「コンスタンティヌス帝の寄進状」

におけるメインアクターがデジタルプラットフォームとなるわけです。

その「新しい『新しい中世』」における国家とデジタルプラットフォームとの関係性について、あくまでも試論ですが、中世のローマカトリック教会と国家の関係性を教科書的に整理するかたちで考えてみたいと思います。これらの関係がどのように変遷し、近代国家の枠組みに収斂していったか。そこには5つの段階がありました。

第1段階：権力の認識

初期のキリスト教はローマ帝国から迫害を受けてきたわけですが、313年にローマ皇帝コンスタンティヌス1世の「ミラノ勅令」によって信教の自由が保障され、392年にはテオドシウス1世によって国教に制定されました。以後、急速にカトリック教会が力を拡大し、世俗の政治権力と教会勢力というふたつの権力が並立していきます。

ローマ帝国はその後395年に東西分裂することとなりますが、東ローマ帝国は、皇帝が教会の最高聖職者を兼ねる「皇帝教皇主義」を採用し、皇帝＝政治権力が優位となるかたちで双方の権力が結びつきました。これは現代の中国において習近平がAlibaba、Tencentなど国内プラットフォーム企業を抑え込むような動きをしていることと重なります。

一方、西ローマ帝国では皇帝と教会のどちらが強いかという関係がなかなか定まらない競合的な状態が続きます。そうしたなかでそれぞれの役割分担や権限配分、つまり権力の均衡をどう保つのかが問われてきたわけですが、そこに憲法論のプロトタイプとなるような議論が発生していたと考えられます。

ちなみに、この時代のカトリック教会の司祭だったアウグスティヌスは「人間というのは神の恩寵に従うべきで、自己決定してはいけない」という考え方を取りました。アダムがまさに自己決定によって果実を食べてしまったことが人間の原罪となったので、人間は自分で決めちゃいけないんだと自由意志を否定します。つまり、神に従うことが道徳的に良い行いということになっていきます。

第2段階：教会権力の優位

その後、800年にカール大帝が西ヨーロッパを統一するのですが、帝国と教会の権力関係はより複雑化していきます。この年にカール大帝の戴冠式があり、冠を授けるのはローマ教皇でした。ローマ帝国皇帝であると認められたカール大帝と、その冠を授けたローマ教皇はどちらのほうが偉いのか。これは肉体に対する「霊魂（バーチャルな存在）」の優位性という意味において、現在の国家とプラットフォームの関係にも近いのではないかと感じます。

この辺りの話は政治学者の佐々木毅先生が書いた『宗教と権力の政治：「哲学と政治」講義II』[*8]に詳しいですが、教皇は「人間の魂の在り方にまで深く踏み込む権力」をもっていたとされます。まさに現在、プラットフォームがアルゴリズムによって人間の「内面」に入っていく、すなわち基底的な領域を統治するという点においても近いものを感じるわけです。

また、この頃、地域の司祭を帝国と教会のどっちが決めるんだという叙任権闘争もあり相克が激しくなっていき、1077年、キリスト教を破門されたハインリヒ4世がローマ教皇に対して、雪のなか裸足で許しを請う「カノッサの屈辱」も起こりました。

ちなみに、2023年6月11日付の朝日新聞に「AIルール動かすのは『G11』――G7と肩を並べた巨大IT企業たち」[*9]という記事が掲載されました。この年のG7サミットの関連イベントで日本の大臣たちがアメリカのビッグテックと討論を行ったものの、政治的な議論が彼らによってリードされているのではないかと指摘する内容です。つ

まり「G7」だけではすでに意思決定がままならず、Google、Amazon、Meta、Microsoftの4社を加えた「G11」によって実際には政治が動かされているというわけです。それまでも政府幹部がビッグテックの人間と非公式の会合をもつことは多数あったかもしれませんが、ここでは、すでに、それが「首脳会談」のような位置付けとなっていることを明かしています。

中世に話を戻しますと、先ほどお話ししたカール大帝の戴冠式や叙任権闘争などは、315年に書かれたとされていたものの、その後偽書と判明した「コンスタンティヌスの寄進状」を根拠に行われていました。これは、当時のローマ皇帝のコンスタンティヌス1世が教皇領を寄進したという内容で、この寄進状によって教皇至上権が法的に正当化されていたのです。これを現代と重ね合わせてみますと、アメリカの通信品位法第230条をもって、政府がデジタル空間・領域の統治の一部をプラットフォーム企業に委ねてしまっている構図に似ていなくもありません。

第3段階：国家権力の逆襲

第3段階は13 〜 15世紀の話です。この頃になると国家が教会権力をいつまでも放置できないということで、権力を奪い返すような動きが生じてきます。これは、いまで言えば、EUがデジタルサービス法、デジタル市場法、AI法を相次いで制定していくような動きと重なります。

それ以前には、すでにトマス・アクィナスの登場により、哲学（理性）と神学（信仰）の役割分担が整序され、両者の調和・均衡を図る動きも出ていました。これは、ごく簡単に言えば、キリスト教的な神学的世界観と、古代ギリシアのアリストテレス的な、つまり人間の理性というものを重視する考え方とをどう調和させるのかという問題です。ここからさらに、14世紀のルネサンス期に入ると、人間の理性、あるいは人間の自己決定の価値を尊重するヒューマニズム（人文主義）といった、いまにも通じる考え方が登場します。

またこの時期、フランス王フィリップ4世がローマ教皇ボニファティウス8世に退位を迫り、教皇が憤死したアナーニ事件（1303年）や、ペストの流行を止められないことによる教皇権のゆらぎ、カトリック教会が分裂する教会大分裂（シスマ）なども起こっています。

第4段階：混沌

続いて16世紀になると、マルティン・ルターらによる宗教改革が起こります。ルターが行った改革のひとつにラテン語で書かれた聖書の世俗語（ドイツ語）翻訳がありますが、これはある意味、アルゴリズムの透明化の話に近いのかもしれません。その他にも贖宥状（免罪符）問題の告発をするなど、教会権力の源泉になっていたものを暴いていったわけですが、ルター派の活動によってプロテスタントが誕生し、個人が聖書と直接向き合うような考え方が出てきます。

第5段階：均衡

その後、ヨーロッパ各地でカトリック対プロテスタントの宗教戦争が勃発していくことになりますが、多くの血が流れたこの闘争への反省から、ヨーロッパの政教分離原則が誕生しました。さらに時計の針を進めると教会権力に対して国家権力が勝利するかたちで、現在に至る近代立憲主義が成立するわけです。外面＝物理的な領域から教会勢力を追い出し、内面＝人間の精神を個人の問題とする、つまり信教の自由の確立をみたのです。

独自の法と秩序

デジタルプラットフォームと中世のカトリック教会が同じだというのはあまりにも乱暴な議論ではありますが、類似性を見ているのは、実はわたしだけではありません。例えば法哲学者の大屋雄裕先生もそうですし、ヨーロッパでも哲学者のルチアーノ・フロリディが同様の指摘をしています。憲法学でも京都大学の曽我部真裕先生がコメントのかたちでおっしゃっていたことがあります。では、デジタルプラットフォームと中世のカトリック教会の類似点は、いったいどこにあるのか。以下、整理をしてみたいと思います。

1. 法

デジタルプラットフォームにはコード、アルゴリズムといった主権国家の法律とはまた違った独自の法体系が存在していますが、それはまさにカトリック教会の「教会法」に相当するものと言えます。

例えばFacebookは2020年に、同社が行うアカウント停止やコンテンツ削除に関する異議申し立てを審査する機関「監督委員会」（Facebook Oversight Board）をつくりました。この組織はハーバード・ロースクールの憲法学者、ノア・フェルドマンの助言から立ち上がったものですが、マーク・ザッカーバーグは、この委員会が「最高裁」にあたるといった言い方をよくしています。委員会には弁護士や学者も参加していますが、これは、テックプラットフォームがその内部に独自の法体系をもつに至っていることの表れと言えそうです。

2. 独自の制裁

教会法においては「破門」という強力な制裁の形式がありましたが、デジタルプラットフォームには「アカウント凍結」という同様の制裁が存在しています。命はすぐに取られないものの、権利をすべて剥奪するというのが教会法における破門でしたが、社会的なライフラインが集約しつつあるデジタルプラットフォームにおける「アカウント凍結」は、場合によっては破門に比する重罰となり得ます。LINEのアカウントが凍結されてしまったら、社会生活に大きな支障を来す人は、実際少なくないのではないでしょうか。

3. 税

デジタルプラットフォームにおいては、例えばAppleのアプリストア手数料は「Apple税」という言い方をされますが、これも、カトリック教会が教区農民に対して独自の課税システムを適用していたのと類似性があります。

4. 人間の相対化

国家権力や憲法は人間を中心とする哲学（人文科学）を基盤としています。その一方で、教会およびデジタルプラットフォーム権力は人間を相対化するような学問体系（神学／自然科学≒データサイエンス）に拠っています。つまり、人間というものをどう見るかという点でも教会とデジタルプラットフォームは近いところがあるように感じます。人間の理性や能力を批判的、相対的に見る学問体系を、両者とも基礎としているところがあるのではないかということです。

心理学者のダニエル・カーネマンが著した『ファスト＆スロー：あなたの意思はどのように決まるか？』[*10]によれば、人間は「システム2」というスローで熟慮的な思考モードと、反射的でファストな思考モードである「システム1」の両方をもっています。デジタルプラットフォームは「アテンション・エコノミー」で成り立っていることもあり、いかにシステム1を駆動させるかが非常に重要になっています。先ほどアウグスティヌスの「人間は神の恩寵に従うべきで、自

己決定してはいけない」という考え方を紹介しましたが、デジタルプラットフォームにも、そうした、つきはなした人間観と近い考え方があるのかもしれません。

「政」と「情」の関係構築

では今後、国家とデジタルプラットフォームの関係性はどのようになっていくのでしょうか。近年はEUがプラットフォームの統制に向けた動きを進めていますが、それが本当に功を奏するのかはわかりません。ここまでお話ししてきた通り、日本を含む世界各国で、こうした規制に抵抗するプラットフォーム側の動きが顕在化してきています。

おそらくは簡単に「国家権力の逆襲」のフェーズにはならないでしょう。リヴァイアサン（国家権力）とビヒモス（プラットフォーム権力）の間で戦略的な関係を構築しつつ両者が牽制し合うような、そうした関係に入っていくようにも思われますが、ここでは、その新たな関係構築のモデルとして、カトリック教会と国家とが、どのような関係性を結んでいたのかを見てみたいと思います。

1. 協約モデル（コンコルダート）

協約モデルでは、デジタルプラットフォームをひとつのグローバルな政治主体として捉えます。ローマ教皇が治めるバチカン市国は投票権のないオブザーバーとしてではありますが国連に参加していますし、EUとも協力関係にあるのと同様です。

つまりプラットフォームをひとつの政治主体として捉えていくということですが、これはすでに現実化しています。米バイデン政権は2023年に、政府としてAI規制を進める前にテック企業との間で業界自主規制の合意を交わしていますが[*11]、これも中世ヨーロッパで帝国・国家と教会の間で両者の対等性を前提に締結された協約になぞらえることができるのかもしれません。

2. 政情一致モデル

政府と教会の「政教一致」ならぬ、政府とプラットフォーム（情報基盤）の「政"情"一致」というモデルは、先ほどお話しした東ローマ帝国や、習近平政権下の中国のデジタルプラットフォームのイメージです。国家がプラットフォームを丸呑みしてしまう、もしくは国家が背後にいてプラットフォームを腹話術的に操縦していくかたちです。このモデルでは、国家とプラットフォームとの間で各種データの一元化も進みますので、監視国家化し、少数派の権利は制限されがちになりますが、功利主義的な観点から見れば、効率的な統治が可能になるとも言えます。

3. 政情分離モデル

政情分離モデルはフランス革命時に政教分離を定め信教の自由を保障した「ライシテ」の歴史に則って、現在ヨーロッパが進めようとしているものです。プラットフォームは政治権力をもつべきではなく、デジタル空間も国家が主権性をもって統治していくんだという考えです。これは「デジタル主権」という言い方もよくされています。

わたしとしては1.の「協約モデル」が現実に存在し始めていることを踏まえて、プラットフォーム権力を含めたかたちで、自由と民主主義のあり方、両者のチェックアンドバランスをどうつくっていくかを考えることが憲法学の新しい役割になるのではないかと考えています。

とはいえ明確に態度を決定できるかといえばまだそうではなく、やはり

3. のヨーロッパ型の「政情分離モデル」のほうが良さそうだという結論になるかもしれません。しかしながら、ヨーロッパのモデルが万全だとも言えない気持ちもあります。なぜそのモデルに疑問をもつかといえば、「プラットフォーム＝ビヒモスが、そんなに悪い存在なのか」とも考えてしまうからです。これは、裏を返せば「政府＝リヴァイアサンはそんなに信頼できる存在なのか」という問いでもあります。

プラットフォームの意義

リヴァイアサン（国家）同士の争い＝戦争はいまもなくなっていません。2021年にトランプが扇動した米連邦議会議事堂襲撃、つまり一種のクーデターの扇動に対してアカウント停止などで抑え込もうとしたのはプラットフォームでした。具体的に何が最大の貢献をなしたかは議論の余地もありますが、リヴァイアサンが暴走したときに止められる存在が生まれたということは、ある意味でポジティブなことだとも言えます。

プラットフォームやテック企業が金儲けしか考えていないかといえばそうではなく、例えば2018年にMicrosoftやFacebookなどは、「政府が仕掛けるサイバー攻撃を支援しない」などの原則を定めた「サイバーセキュリティテック協定」（Cybersecurity Tech Accord）を結ぶなど、安全保障に対する責任をもとうとしているところもあります。あるいは東南アジアなどの軍事政権下においては、抵抗勢力の支援になる存在がプラットフォーマーであるということも挙げられます。ヨーロッパで見るプラットフォームの姿と、東南アジアで見るプラットフォームの姿は真逆だったりもするのです。

そう考えると、プラットフォームを政治領域から排除していくのか、巻き込んだ上であるべき関係性を構築していくのかということが、今後の憲法学の課題でもあるし、政治的にもそうだろうと思います。第2部でお話しする安全保障に関する問題でも、同じような課題が出てくるのではないでしょうか。

国家の独占が壊れていく

強大化するプラットフォームと国家の関係を、中世の教会と国家の関係になぞらえた山本先生の刺激的なレクチャーを受けて、ラウンドテーブルの席では、多種多様な視点から、以下のような意見や感想が飛び交った。

政府のデジタルケイパビリティがなかった｜国家公務員

新型コロナウイルス感染症拡大防止対策の接触確認アプリの話がありましたが、これにつきましては、多様な関係者がさまざまな振り返りをnoteやウェブメディアなどで多数公開しています。そうしたなかで一番問題だと感じるのは、日本政府にデジタルに関するケイパビリティ（能力）がなかった、ということだと思います。その結果、国がどうしてもプラットフォーマーに依存せざるを得なくなってしまう。デジタル庁が外部からエンジニアを集めていますが、従来の官僚と民間のエンジニアが融合し、「デジタル時代において統治をなす」とはどういうことかを言語化し、組織化していくことが課題だと感じます。

情報の独占が壊れている｜哲学研究者

改めて確認しておくべきことだと感じるのは、20世紀までの国家は、国家内の社会・経済・政治に関するあらゆる情報を、ほぼ独占的に集約・管理できていたということです。ところが、GAFAのような情報プラットフォームの登場によって、その優位性が崩れてしまった。結果、情報を独占していた20世紀における「国家」のイメージは過去のものとなっています。日本でもマイナンバーと各種サービスの紐づけに関して、私企業がむしろ国家に対して「早くやれ」と催促する立場になっているわけですよね。国家を規定していた独占性が奪われ、どこからどこまでが政府の管轄で、どこからが民間の管轄なのかが見えなくなり、その境界が溶け出してしまっていくなかで、国家と私企業を、これまでのような二元論をもって扱うことすらできなくなっていくのではないか、という懸念があります。監視国家と言ったときも、これまでの古典的な監視国家のイメージで語っていては、その実態を捉え損なうことにもなりそうです。

私企業のなかが見えなくなる｜神経法学研究者

さまざまな科学技術が人間の認知過程を操作・干渉しうる社会において、われわれはそもそも何を守りたかったのかということを、いま一度科学のことばで捉え直さないと、「守るんだ」というスローガンだけが先行して、結局何も守れなくなってしまうのではないかという危機感をもっています。

コロナ禍前に中国の某テック企業の方に何を監視しているのか説明してもらったことがあるのですが、例えば長距離トラックドライバーがいつどこを出発し、どこでどれだけ休憩し、何時にどこに着いたかということを物流・人流含めすべて把握していると言うんですね。かつ各地区でどれだけのリスクがあるかというフィードバックも見せてもらい「うちの国はリスク管理がきちんとできる安全な国なんだ」と自慢気に話しているのを見て、こちらの顔が引きつるという出来事がありました。

監視と言えば間違いなく監視なのですが、懸念すべきなのはむしろ、こうしたことが起きていても、国家が私企業のなかで何が行われているかを

わかっていないということではないでしょうか。こうした状況において、国家の優位を前提とした、これまでの規範は適用できないし、国家には可能な情報公開請求ですら「企業秘密だ」とはね除けられてしまうことになります。

　山本先生が説明された協約モデルに移行したくとも、統制の対象として浮かび上がってこないグレーゾーンにおいて経済原理に基づいて行われることが、中国とはまた別の方向で過激に進行してしまうリスクが、かなりあるのではないかと感じます。

不透明化し、外から見えなくなる｜ジャーナリスト

私企業のデジタルプラットフォームで何が行われているのかを、行政機関の人間も把握できていませんし、専門的でわかりにくく、アルゴリズムという独自のルールで動いてしまっている部分があるように感じます。その一方で行政との結託も進んでおり、そこには透明性はないですし、外から見るともはや何が行われているのかが見えないことが非常に気になっています。

アジャイル・ガバナンスの陥穽｜憲法学者

政府内にデジタル分野のケイパビリティがないからこそ、民間人材を大量に迎え入れることが必要となっているのだとは思いますが、一方で政府の民間に対する依存関係が生まれてしまうのは問題かもしれません。例えば経済産業省が急激に変化する環境に対応すべく、迅速にシステムやルールを変更していく「アジャイル・ガバナンス」の考え方を政府内で推進しようとしていますが、この考え方は、基本的なフレームワークが法律に根拠

づけられていませんので、ルールメイキングが実質的に民間企業に委ねられてしまうところがあります。アジャイル・ガバナンスもひとつの協約モデルのあり方ではあるとは思いつつも、ちょっと不安に感じているところがあります。

政府内に「民間」が入る意義｜国家公務員

とはいえ、現在の生え抜きの国家公務員だけでは、新しい世の中をガバナンスできません。そのやり方を学んでもいません。そこで、どうしましょうということなんだと思います。政府における民間採用に関しては、ガバナンスを私企業に仕事として依頼するよりは、国家公務員として雇用して一定の規律に服して働いていただいたほうが、ガバナンスが効くはずです。デジタルの世界とリアルが融合していくなかで、いったいどのような統治構造をつくっていくことができるのか。それを考えるためにも、まずは政府のなかに、レイヤー構造となってしまっているデジタル世界のありようを感覚的に理解できる人間を入れていくことが大事だと思います。プラットフォームだけでなく、これからの国家運営のインフラとなるクラウドサービスも半導体もAIなどの新たなテクノロジーもすべて同様だと思います。

リターンを返してくれるのはどちら？｜民間企業研究員

市民の感覚からすると、国だろうが私企業だろうが、自分の生活にとってメリットをもたらしてくれるなら、どちらでも構わないという感覚があります。いままでは国家に対して多くの情報を提供してきたけれども、リターンという視点から見れば、デジタルプラットフォームのほうがよほど多くを返し

てくれているというのが、リアルな感覚です。加えて、国家が一元的に情報を管理していた頃から、個人情報なんて最初から保護されていないだろうという感覚も強くあります。デジタルプラットフォーム上で何かが失われていく、あるいはコントロールされていくという議論は、頭ではわかるものの、何が具体的に失われていくのかということになると、いまひとつ実感できないところがあります。

認知に介入するプラットフォーマー｜神経法学研究者

現時点で指摘できる問題は、まず情報のインプットがアルゴリズムによってダイレクトに操作されるようになってきたということだと思います。それがさらに進み、フィルターバブルどころではなく個々人で異なる世界観が出来上がっていってしまうリスクはある気がします。

もうひとつ気がかりなのは、わたしたちの情報のアウトプットの部分にプラットフォーマーが大きく関与し始めている点です。2023年にAppleがAirPodsを脳波計にする特許を申請しました。Vision Proも脳波計として使えるというリークが開発者から出ています。生体情報を網羅的、経時的に取得していくことによって、本人の心理状態の変遷をかなり詳しく予測するということがいずれできてしまうのかもしれません。いまはまだ投薬管理などの分野で生体情報が用いられていますが、今後は日常生活、消費行動、もっと極端なことを言うと投票行動にまで転用できると考えられます。

プラットフォーマーはこれまで脊髄反射的な、システム1の部分にアプローチしてきていたわけですが、いよいよ認知の処理過程、つまりシステム2が操作の対象になるだろうということは、いまはまだディストピアSFの世界かもしれませんが今後気にして見ておかないといけない領域なのかなと思います。

フィルターバブルの何が問題か｜憲法学者

「最大多数の幸福は実現できている中国の何が悪いのか」という問題は重いですね。若い人たちと話していても、フィルターバブルに覆われたコンテンツに接することの何が悪いのかとよく訊かれますが、そのたびに答えに窮してしまいます。

それでも現時点で何が問題か言うとすれば、フィルターバブルについては「ハムスターの回し車」というメタファーをよく使うのですが、過去の閲覧履歴にずっと追い回され続けて、もしかすると自分が見られたかもしれない世界が奪われている、つまり人生の機会損失になっている可能性が挙げられます。

またアテンション・エコノミーについては小説『ジキル博士とハイド氏』の話をよくします。作中でジキルは非常に理知的な人物である一方、ハイドの人格になると周囲に暴力を振るってしまう。アテンション・エコノミーの世界では人びとのハイドの部分を増幅させており、そのように好き勝手に振る舞うということが快楽を呼び起こしているわけです。

ですが、この辺りはまだエビデンスが取り切れていないところはたしかにあります。先ほどお話ししたアメリカの連邦議会襲撃事件のような事例にしても、もう少し実証的な研究が必要だろうと思います。

これまでのインフラと何が違うのか｜編集者

アメリカのあるメディア研究者が、「われわれが考えるデジタル社会というのは、テレビ的な社会構成をそのままデジタルに置き換えただけで、本質的にはデジタルの特性を活かしたものにはなっていない」と語っていました。新聞やテレビを見て「自民党が酷いな」「共産党が酷いな」と感じた人はい

ままでにもたくさんいたと思いますが、ある種の認知のパターンみたいなものは実はそこからそんなに変わっておらず、ただそれがさらに広範囲に可視化されちゃっただけという状況かもしれないという気もしなくないのですが。

知らず知らずのうちに使っていた｜ジャーナリスト

テレビとデジタルの違いに関連して、以前友人と「ITやデジタルはバレたら負けだ」という話をしたことがあります。新しいデジタルツールは、ユーザーが技術や事業者のビジネスモデルを意識することなくLINEのように「知らず知らずのうちに使っていた」という状況にならなければ一般の人に広く使ってもらえない。だからそこをいかにわからせないようにしつつ浸透させるか、に取り組んでいるということがひとつ言えると思います。だからこそ何が問題かがそもそもわかりづらい、構造的な問題があるのではないかと。

民主的ガバナンスの欠如｜国家公務員

原子力、電力、通信など公益事業と呼ばれる領域は、それぞれの事業規制に即していますよね。何のためにそれをやるかが明確で、ユニバーサルサービス制度があって、料金体系をどうするのかなどを決めてきました。ところが、クラウドもITもさまざまな分野でそうした公益事業に関する法的なものがない。何のためにそれをやるのかを民主的プロセスによって決定しないままに、デファクトとしてわれわれが依存している状況になっています。

クラウドを利用するときは産業政策の観点もあるし、セキュリティの観点もあるし、当然コストの観点もある。例えば、突然プラットフォーマーが料金を値上げすると言い出したらどうしようもない状況になってしまうことに対して、ある種の独占をしている事業体へどのような公益性の縛りをかけられるのかということも争点ですよね。

「社会保障の代替」というシナリオ｜憲法学者

まだ現実味がない話かもしれませんが、日本の少子高齢化が進み、今後誰が社会保障の担い手になるのかという問題がありますよね。そうした際、例えばAppleがApple Watchで健康データを収集し、その報酬としてベーシックインカム的にお金を払う、つまりプラットフォーマーが社会保障を代替するようなイメージもあり得るんじゃないかと思っています。そこでは政府のマイナンバーも紐づけされているかもしれません。

徴税権までいくと国の統治ができなくなると思うのでそこは手放さないでしょうけれど、例えば日本国憲法で定められている社会権、つまり「健康で文化的な最低限度の生活を営む権利」の担い手がプラットフォームになった際、国家の消滅まで行ってしまうのではないかということも頭の片隅にあります。

そうなった場合、国家は、どのプラットフォームを用いて統治するのかという、競争法的な役割しか負わなくなるかもしれません。

潰せないプラットフォーム｜憲法学者

そうなるとGAFAのようなプラットフォーム企業は絶対に潰せない存在になり、独禁法をもって分割させるみたいなことはできなくなります。プラットフォームが国家＝リヴァイアサンに対抗できる存在となるためには、ある程度図体が大きくて力をもっている必要がありますので、むしろ分割などは

すべきでないという議論も出てきます。

最近はヨーロッパで「デジタル立憲主義」という考え方も出てきていますが、これは要するにプラットフォーム企業に対しても立憲主義的なあり方を守ってもらうという発想です。それをプラットフォーマーにどう守らせて執行するかというと、国家＝リヴァイアサンの集合体をつくる必要がある、という理屈になります。EUがなんとかプラットフォームをマネジメントできているのは、それが国家の集合体だからですよね。今後もしかすると国連のような枠組みのなかに、引っ張り出していくことも考えられます。

国家の安全保障もある程度そうなっていくように思うのですが、サイバーセキュリティという問題ひとつを取っても、MicrosoftやGoogleの人間がいないところでは、もはや政策はつくれなくなっています。国家とプラットフォームの双方のパワーバランスが微妙に変わりながら、お互いに牽制し合うような、不安定な関係性になっていきますが、そこにむしろ可能性を見いだしていく必要があると感じます。

「国内の事情」の反映が難しい｜国家公務員

プラットフォーマーは経済的な合理性をもつので、公共サービスを共同的に担う社会の到来は避けられないのではないかと思います。一方で、「国内の事情」みたいなものがどこまで考慮されうるのかという点は考えてしまいます。例えばいまでも学校教育向けにGoogleのChromebookが大量配布されています。世界中のデータを使いながらサービスが良くなっていてわれわれはそれを享受していますが、サービス自体がグローバルに均されて国内の事情を反映することが難しくなることも起きていくかもしれません。

国際的新秩序の必要性｜憲法学者

プラットフォーム規制においてその問題は大きいですよね。例えば日本国内でも固有のヘイト問題がありますが、海外プラットフォームの場合、日本人スタッフがそれをモデレートしているのかといえば、そうでもなさそうだということがわかってきています。ですが、総務省が単独で「なんとかしてください」とお願いをしたとしても、おそらく無視されるでしょう。

であればこそ戦略的な関係構築が必要で、省庁間の連携もそうですし、もっと言えばG7、G20、国連など、リヴァイアサンたちの集合とも言える国際的な場で訴えなければいけないのだと思います。そこにプラットフォーマーを呼んできて、各国の事情や価値観をちゃんと反映するように促さないといけない。そうした新しい秩序をどうつくっていくか、ということではないでしょうか。

第1部｜脚注

＊1｜クリストファー・ワイリー『マインドハッキング：あなたの感情を支配し行動を操るソーシャルメディア』、牧野洋=訳、新潮社、2020年

＊2｜「アップル側には総務省出身『政務部長』、政府と水面下で攻防…規制案に『謹んで異議』」、読売新聞オンライン、Jun. 20, 2023
https://www.yomiuri.co.jp/economy/20230620-OYT1T50059

＊3｜Kate Klonick “THE NEW GOVERNORS: THE PEOPLE, RULES, AND PROCESSES” GOVERNING ONLINE SPEECH、Apr., 2018
https://harvardlawreview.org/wp-content/uploads/2018/04/1598-1670_Online.pdf

＊4｜「電気通信事業法の改正の方向性に対する懸念について」、新経済連盟、Dec. 17, 2021
https://jane.or.jp/proposal/pressrelease/15987.html
「新経済連盟の『懸念』に対する懸念」、一般社団法人MyDataJapan、Dec. 23, 2021
https://mydatajapan.org/documents/public_comments/concerns2112

＊5｜https://twitter.com/realDonaldTrump/status/1217228960964038658

＊6｜Elena Chachko "National Security by Platform" Dec. 31, 2021
https://law.stanford.edu/publications/national-security-by-platform

＊7｜田中明彦『新しい中世：相互依存の世界システム』、講談社学術文庫、2017年（原題『新しい中世：21世紀の世界システム』日本経済新聞社、1996年）

＊8｜佐々木毅『宗教と権力の政治：「哲学と政治」講義II』、講談社学術文庫、2012年（原著2003年）

＊9｜渡辺淳基「AIルール動かすのは『G11』――G7と肩を並べた巨大IT企業たち」、朝日新聞デジタル、Jun. 11, 2023
https://www.asahi.com/articles/ASR6B0162R5YULFA024.html

＊10｜ダニエル・カーネマン『ファスト&スロー：あなたの意思はどのように決まるか?』、村井章子=訳、早川書房、2014年

＊11｜甲斐野裕之「米テック企業が安全なAI開発を約束、バイデン政権が発表」、JETROビジネス短信、Jul. 25, 2023
https://www.jetro.go.jp/biznews/2023/07/457119945150b629.html

2

戦争／外交／経済

講義

まつろわぬプラットフォーム

山本龍彦（憲法学・慶應義塾大学大学院法務研究科）

2021年1月6日、米連邦議会議事堂周辺に集うトランプ支持者たち　Photo by Samuel Corum/Getty Images

第2部のテーマは「戦争／外交／経済」です。安全保障をめぐる問題については、「いくらプラットフォーマーが国家に対して優越しようとしても、国家ないし国内企業が下部構造である物理的なインフラを押さえているから統制できるのでは」といった意見も見かけます。しかしながら日経ビジネス副編集長（現・日経ビジネスLIVE編集長）の堀越功さんが担当した特集「GAFAMに飲まれる通信インフラ」（『日経エレクトロニクス』2022年4月号に掲載）[*1]などを読むと、どうもそうした古典的な見方が成り立たなくなっているのではないかと感じられてきます。

どういうことかと言いますと、AmazonやMicrosoftといったクラウド事業者による「通信インフラのソフトウェア化」がどんどん進行しています。またGoogleなども国際通信を担う海底ケーブルの建設に乗り出しているのです。

わたしも「まつろわぬインフラ」という論文（『法律時報』2022年9月号に掲載）[*2]で指摘したことがありますが、インフラの担い手が主権国家・国民の言うことを聞かない、まさにまつろわぬ存在になってきているなか、当然それは安全保障に重大な影響を与えるようになるのではないかというのが、第2部の主題となります。

まつろわぬインフラ

情報通信インフラというのはコミュニケーション基盤であるとともに、現代の情報戦においては極めて重要な「戦場」ともなります。近年の戦争は情報戦、特に認知戦というものが非常に重要なウエイトを占めるようになってきていますが、それが展開される場というのが、まさにここまで議論してきたプラットフォームです。

この場をどう利用するかによって、当然戦局が大きく左右されることに

なりますので、プラットフォーマーは、こうした観点からも相当強い地政学的な影響力をもつに至っていると言うことができます。国際政治学者として有名なイアン・ブレマーは「Foreign Affairs」にこう書いています。

> *ほぼ400年にわたって国家は国際政治の主要なアクターとして活動してきたが、（中略）いまやビッグテックは政府に匹敵する地政学的影響力をもち始めている。*[*3]

さらに、米中のテクノロジー競争に関する分析の多くは依然として国家主義的パラダイムに囚われており、テクノロジー企業を敵対国との抗争における歩兵のような存在と見なしているが、もはやそうではないとも語っています。

またブレマーは、2021年の米連邦議会議事堂襲撃後にプラットフォームが取ったアカウント停止などの行動は、政府や法執行機関の要請によるものではなかったことに注意を向けています。それは、営利目的の企業が自らの管理下にあるコード、サーバー、規則に対して権力を行使したプライベートな決定だったと言うのです。今後、安全保障を議論し地政学を論じる上で、プラットフォーマーを考慮に入れることは不可避であると、ブレマーは指摘しているわけです。

プラットフォームによる国家安全保障

第1部でも少し触れたエレナ・チャチコは、論文「National Security by Platform」において「プラットフォームの地政学的転回」ということばを使って、この現象を分析しています。

このシフトがいつ頃から起きているかというと、2016年のケンブリッジ・アナリティカ事件が大きな転回点だったと指摘しています。また、ミャンマーでのロヒンギャ難民問題にまつわるヘイトスピーチの放置、タイで軍事政権の要求に応じて反体制勢力のコンテンツを削除した問題などをめぐって、Facebookが厳しい批判に晒されていたのも同じ時期です。さらにこの2016年には国内外の暴力組織やISISなどの国際テロ組織のリクルーティングをプラットフォームが実質上支援しているのではないかという批判も目立つようになっていました。

こうした批判に対応すべく、プラットフォーム自身が地政学上の、あるいは安全保障上の脅威に対する専門部局を設置することになりました。チャチコは、このことをして「National Security by Platform」（プラットフォームによる国家安全保障）と表現したのです。プラットフォーム自体を地政学上・安全保障上のアクターとして定位したということです。

安全保障人材の引き抜き

実際、2016年以降、Facebookでは安全保障関連の職員数が3倍になっており、2021年8月時点でその数は約4万人に達していると言われています。具体的にどういった業務にあたっているのかはよくわかりませんが、「アメリカの外交官の数（約1万5600人）と比較しても圧倒的な人数である」と指摘されています。

また2019年には当時アメリカ国務省の法律顧問だったジェニファー・ニューステッドを同社の最高法務責任者としてヘッドハンティングしました。そのほか安全保障上の脅威に対応するために、いくつかの役職を新設、再編成し、そのなかにはサイバーセキュリティ責任者（Head of Cybersecurity Policy）、グローバルな脅威と混乱に関する主査といったポジションなどもつ

くっています。

このサイバーセキュリティ責任者にはホワイトハウスの国家安全保障会議（NSC）でもディレクターを務めていたナサニエル・グレイチャーが就任しました。さらに後者の「グローバルな脅威と混乱に関する主査」にもNSCの元インテリジェンス所長をあてていることからおわかりの通り、国家安全保障に関わってきた人材を政府からどんどん引き抜いています。

エレナ・チャチコは、こうしたFacebookの人事は、「地政学的分析をより詳細に行うため」「グローバルな脅威をモニタリングするため」「対応プロトコルを改善するため」、そして「これらの活動に関する政府との関係を強化するため」に、自らの組織構造や手続きを再調整しようというFacebook社の試みを反映していると分析しています。

諜報機関としてのFacebook、Google

こうした人材の引き抜きに関連して、チャチコが指摘するのは、Facebook内部におけるこうした業務が、政府による諜報活動とかなり似通ってきているという点です。

例えばFacebookは、2016年の米大統領選に関与したとして有名なロシアの「インターネット・リサーチ・エージェンシー」（IRA）社に関する情報を収集し、FacebookやInstagramのアカウントを削除するという措置を実際に執っています。チャチコは2020年のアメリカ大統領選挙においては、こうしたプラットフォームの関与が功を奏した部分があるのではないかとも述べています。

また反テロ、国際紛争への対応としてもそれぞれ専門家を採用したチームを編成しています。先ほどFacebookがミャンマーではロヒンギャ難民に関するヘイトスピーチを放置したとして批判を浴びたと言いましたが、同

Photo by Chip Somodevilla/Getty Images

2017年10月31日。米上院司法委員会で証言をするGoogle、Facebook、Twitter社の法務顧問

国で軍事クーデターが起こった2021年には軍によるフェイクニュースの削除、表示頻度の制限、軍関係者のアカウント停止などを行っており、ジャーナリストの海野麻実さんは同社を「民主主義を懸けて軍と戦うもう1つの『戦士』」[*4]だとさえ評しています。

一方のGoogleには「脅威分析グループ」（Threat Analysis Group：TAG）という組織があります。2018年～21年の責任者はクリスティ・カネガロという人物で、オバマ政権下では首席補佐官代理を務めていました。2022年から彼女は再びアメリカの国家公務員に戻り、国土安全保障副長官代行を担っています。この組織は「小さな諜報機関」「民間の大規模な反スパイ組織」などとも呼ばれ、やはりロシアによる影響工作に対して一定程度の成果を上げていると言われています。カネガロはインタビューで自身の活動をこう解説しています。

> *「プラットフォームへの干渉に対抗するための継続的取り組みの一環として、FBIの外国影響タスクフォース（Foreign Influence Task Force）などの政府機関や他のテクノロジー企業と緊密に連携しています。また、GoogleのTAGやYouTubeに所属するメンバーと協力して、悪意のあるアクターを特定し、彼らのアカウントを無効とし、ユーザーに警告し、関連情報を業界関係者や法執行機関と共有しています。今後も国家を後ろ盾としたフィッシング攻撃、組織的な影響工作、偽情報の拡散に関する調査結果を踏まえアップデートを続けていきます」*

これだけでも、Googleがかなり緊密に政府と連携を図っていることがうかがえます。また、Microsoft副会長兼社長のブラッド・スミスは安全保障に対して積極的だと言われており、ロシアによるウクライナ侵攻直後の2022年3月、ロシアの侵略行為を非難するという非常に政治的な発言をした上で、ロシアでの新サービス・新製品の販売をストップするとアナウンスしました。

彼は2017年に国連においてプラットフォーマーが赤十字国際委員会（ICRC）のような積極的役割を果たすべきだと演説し、実際に翌18年にはテック企業34社が参加し、サイバー犯罪集団や国家による攻撃からユーザーを守ることを定めた「サイバーセキュリティテック協定」（Cybersecurity Tech Accord）を制定する呼びかけも行っています。この協定を「デジタル版ジュネーブ条約」だと評する向きもあります。

プラットフォーム企業を中心としたテック企業がいまや国家を抜きにして、こうした安全保障についての協定を結ぶことが現実に起きています。法学者のイド・キロバティは、こうした状況をして、「プラットフォームはいまや自らが国際秩序に責任をもつ政治主体であることを自認し始めた」と語っています。

憲法9条とサイバーセキュリティ

チャチコはプラットフォームがこのような優位性をもつに至ったのにはふたつの背景があるとしています。ひとつは、コミュニケーションインフラとなっているプラットフォーマーは、安全保障上の脅威に対抗しうる「制度的に最適なアクター」であること、もうひとつは「国家の政治的決定の回避」です。

「国家の政治的決定の回避」とは、国家が積極的にサイバーセキュリティを推進するとなると、国内では通信の秘密やプライバシーなどの問題を指摘されがちで政治的分断が生じかねないことから、国家が積極的に進めづらい状況を指しています。また、ある特定の国からサイバー攻撃を受けたことを国家が名指しした場合にも、外交上の軋轢になることから、国家がおおっぴらに推進することを懸念する声が上がります。積極的なサイバーセキュリティは、とりわけ民主主義国家の現行制度においては、何かと足

枷が多いのです。

こうした「国家の政治的決定の回避」は、もちろん日本にとっても他人事ではありません。日本の場合は、とりわけ憲法9条の問題が大きく絡んできます。

現代の戦争は物理的な兵力だけでなく、デジタル空間内におけるサイバー攻撃や認知戦なども大きく影響するハイブリッド戦争となっていますので、サイバー攻撃やネットワーク機器への攻撃、さらには偽情報の流布などが他国から行われることが想定されます。そうした「攻撃」に対する事前対応のために担当組織を設置し、先制的に活動することは「アクティブ・サイバーディフェンス」と呼ばれますが、これは憲法9条で保有を禁止されている「戦力」に該当してしまう懸念もあります。

しかし、だからといって日本の情報空間が偽情報の流布・拡散に対して無防備なままでは、ハイブリッド戦争を優位に戦うことはできません。さらに言えば、ハードウェアとしてのインフラに対するディフェンスであるならまだしも、情報戦・認知戦に対する防衛となると、今度は言論の自由に関わってくるような側面もありますので、それを憲法上どのように取り扱い、制御していくことができるのかとなると、さらに難しい議論となります。具体的な処方箋はいまのところありませんが、すでに考えるべきフェーズには来ていると思います。

実際、ウクライナ侵攻を例に取ってみても、ロシア、ウクライナの双方が互いの情報を封じ合いながら、同時にグローバルな共感を生み出しつつ戦局を優位に保つべく行われた情報戦は熾烈なものでした。そうした観点からも、第1部でお話ししたように、政府がプラットフォーム側と戦略的な関係を築き、認知戦において一定のパートナーシップを結んでいくようなことは、ますます不可欠になっていくのではないでしょうか。

言うまでもなく、こうした状況は当然危うさも孕んでいます。これまでの歴史のなかでも、国家が安全保障の実務を傭兵や民間企業にアウトソーシングすることはありましたが、先に紹介したチャチコは、現在の状況は、かつてのそれとはまったく違うと釘を刺しています。

これまでの民間委託は委任、契約といったフォーマルな取り決めを通じて国家が垂直的にコントロールできていましたが、国家とデジタルプラットフォームの関係は水平的ですし、プラットフォームがカバーしているドメインや裁量の幅もこれまでの民間企業とは比べ物にならないほど広がっています。加えて、突然いなくなってしまうリスクも十分あり得ます。ウクライナ政府がイーロン・マスクに右往左往させられているのは、まさにそのケースです。

まつろわぬ者の価値

そうした危うさを想定した上で、EUは「デジタル主権」を掲げ、「GAIA-X」というデータ流通基盤において、自前のクラウドサービスやデータベースの構築を進めています。この背景にあるのは「まつろわぬインフラ」を極力排除していくという考え方です。ですが、いまのところその先行きはどうにも不明瞭ですし、私企業による「まつろわぬインフラ」には、まつろわぬなりの価値もあるのではないかと思えば、ヨーロッパのやり方が最善とも言えません。

ここまで何度か言及してきた米連邦議会議事堂襲撃についても、アメリカ政府がプラットフォーム事業者をガチガチに統制できていたとしたら、当時まだ大統領だったトランプのSNSアカウント停止は、政府の介入によってむしろ実現していなかったかもしれません。

またバレンティーナ・ゴルノーバという、デジタル立憲主義を主張する若手国際法研究者は、第1部で紹介したAppleによるFBIからのiPhoneロック解除要請拒否について、「歴史的称賛に値するプラットフォームの不服従である」と評価しています。つまり、まつろわぬ存在であることが、国家の

2021年1月6日、アメリカで最も影響力のある「陰謀論者」アレックス・ジョーンズが米連邦議会議事堂前で演説を行う　Photo by Jon Cherry/Getty Images

強権に対する抵抗力としても機能しうるということです。プラットフォームをとにかく叩けば良いわけではなく、むしろプラットフォーム権力をどう立憲主義的に使わせるかという方向で議論したほうが建設的ではないかと、彼女もまた主張しています。

国家とプラットフォーム企業が提携するような事例は、実際数多く見られるようになってきています。ウクライナ副首相のミハイロ・フェドロフは、侵攻に対処すべく志願制の「IT軍」を設立し、大手テック企業に協力を要請しています。スウェーデンは2022年にフェイクニュースや偽情報に対抗するための「心理防衛庁」を設立していますし、デンマークでは2017年に「デジタル大使」というポストを設置し、同様に大手テック企業との関係構築を担っています。当時のデンマークの外務大臣アナス・サムエルセンは、こんなことを語っています。

「他の国家と外交的な対話を行うのとまったく同様に、Google、Facebook、Appleといったテックアクターとの包括的な関係を構築し、これを重要視する必要がある。多くの企業、そして新技術は、多くの点でデンマーク市民の日常生活に関わり、その一部になっているからだ。これらの企業のなかには、国家に匹敵する規模の企業もある。かくして、われわれが現在進行中の出来事に参加し、その物語において何か発言権をもとうとするならば、デジタル大使を擁する必要がある」

日本で「協約モデル」を実施するには

日本においてこうした取り組みを進めていくためにはどのような仕組みが必要なのかを考えてみますと、まずは、国家とプラットフォームの関係を、外交関係に類するものと捉えていく必要があるように思います。

日本国憲法72条は、外交関係については国会に報告することを求め、73条3号は内閣が他国と条約を締結する場合には国会の承認を得ることが必要だとしています。プラットフォームと国家の関係を、第1部でお話しした「協約モデル」で考えるのであれば、政府がプラットフォームと交わした約束も国会に報告して統制を受けるべきだとなります。

接触確認アプリ「COCOA」の開発のケースでは、Google、Appleの仕組みに乗っかるという政府の決断がどのように行われたのかは、国会においては立憲民主党の中谷一馬議員が質問されていましたが、政府見解は十分なものではありませんでした。今後のセキュリティを考えたときに、一定程度は国家機密にしなければいけない部分があるのは仕方ないとしても、テック企業とどんな取引が成されたのかをできるだけ透明化していくことが求められるのではないでしょうか。

第1部で触れたテックセクター、経済セクターによる「ロビイング」につ

いても、アメリカであれば「ロビイング開示法」（LDA）という法律がありますが、日本には、それに類する法規制がありませんので、こうしたこともサイバーセキュリティを考える上で重要な問題になってきています。

サイバーセキュリティの共通原則

最後に、Microsoftがウクライナ侵攻後の2022年7月に発表したレポート「ウクライナの防衛：サイバー戦争の初期の教訓」[*5]を紹介します。こちらはオンラインで日本語の抄訳も読むことができます。このレポートはMicrosoftの脅威インテリジェンスチームとデータサイエンスチームが実施した調査をまとめたもので、今後サイバー脅威を阻止するためには、以下の4つの共通原則が重要だと記されています。

第1の原則
デジタルテクノロジー、AI、データの進歩が必要であること

第2の原則
サイバー攻撃への対応には官民の協力強化が必要であると認識すること

第3の原則
開かれた民主的社会を守るための、政府間の緊密な協力体制の必要性を認識すること

第4の原則
たとえサイバーインフルエンス工作活動を含む、あらゆるサイバー脅威に対処するための新たな措置が必要であるとしても、民主主義社会における表現の自由を守り、検閲を避けること

これを民間企業であるMicrosoftが提言していることの意味をどう捉えるべきなのでしょうか。当然、これを推進することでMicrosoftにとって自社の利益になるのだろうと推測することはできますし、あくまでも一般論として、政府自体をどこまで信用できるのかという問題もあります。政府は政府で自分たちの私益だけを追い求めてしまうのではないかと疑うことも可能です。

法学者やテクノロジー分野のリサーチャーなどが集まってつくられた団体「デジタル立憲主義者 ― 立憲主義の未来」（The Digital Constitutionalist — The Future of Constitutionalism）は以下のような声明を出していますが、これは日本においても考えていかなければならないことだと思います。

> *民間の諸アクター、特にビッグテック企業は、デジタルインフラストラクチャーや公的空間の形成において不可避的な役割を果たしており、デジタルガバナンスに関するすべての議論は、彼らによって行使される権力を検討するものでなければならない。*

ここで紹介したエレナ・チャチコや、第1部で言及したケイト・クロニックのように、アメリカではすでに、プラットフォームの「法」を研究する「プラットフォーム法学者」とでも言えそうな専門家が出てきています。中世の神学者たちが世俗法（宗教的権威でない存在が定める法律）と教会法の両方を見ていたのと同様に、国家の法律だけでなくプラットフォームの「法」やガバナンスの体系を把握できなければ、すでに法学自体が完成しなくなっているのかもしれません。日本でもそうした研究をする人がようやく数人出てきたところです。

議論

民主主義はサイズダウンしていく

「サイバーセキュリティ」のお題目のもと、プラットフォームと国家はいかに手を結ぶことができるか。あるいはできないのか。そもそも手を結ぶべきなのか、すべきでないのか。難問をめぐってラウンドテーブルも白熱する。

AWSで本当にいいの？ | ジャーナリスト

日本政府は2017年に「クラウド・バイ・デフォルト原則」を打ち出していますが、ガバメントクラウドとして利用されるクラウドサービスの多くがAWS（Amazon Web Services）であったりするのが現状です。ところが、「それって外国のサービスだけど本当にそれでいいの？」ということは日本ではまったく議論されないですし、他国の人からすればなんで平気なんだと、よく不思議がられます。

国産か、アメリカ産か | 憲法学者

日本においてサイバーセキュリティを考える際の困難は、デジタル空間以外のリアル空間もアメリカの安全保障の傘下に入ってしまっていることです。ですから、この問題を考えるときに国産プラットフォームが整備されるのを前提にこれから起こりうる問題を検討すべきなのか、アメリカのプラットフォームを使うことを前提として考えるべきなのか、実はここからしてすでに難しい問題です。ただ、第1部にもあったように、プラットフォームは、もはや単独の国家だけで統御できる存在ではありませんので、いずれにせよ、

「リヴァイアサンたちの集合」、つまり国際協調的な枠組みのなかで関係を構築していくということが落とし所になるのだろうと思います。

新しい会社法が必要なのでは？ | 民間企業研究員

大手プラットフォーム企業をひとつの国のように扱うというお話はとても面白いと思いました。ただ、その際にいくつか気になる点もあります。例えば、自国の民間企業が敵対国に協力していた場合、政府はどのような根拠に基づいて、法的に罰しうるのか、といったこと。あるいは、民間企業のなかでも、特にベンチャーと言われるようなところは独裁にも近いガバナンスを行っているケースもあると言いますから、そうした企業の内部におけるガバナンスをどのように外部から制限することができるのか、その際、新しい会社法のようなものが必要になるのか、といった点に興味が湧きました。

プラットフォームの公的責任 | 憲法学者

民間企業をどのように制御するのかという点について言えば、これまでは企業対企業（BtoB）、あるいは企業対政府という問題だけを考えていればよかったわけですが、同じフレームのなかでプラットフォーム企業を捉えようとしてしまうと、どうもこれまでの法律の枠組みとマッチしなくなってくるところがたしかにあります。ただ現実的には、「プラットフォーム」がいったい何なのかということはまだ誰もよくわかっていないところもあり、そこが解明されていくなかで、プラットフォームにある種の公共的な責任があるという認識も広がっていくことになるのではないかと思います。

平時のセキュリティこそ問題｜神経法学研究者

個人的には戦争状態に突入してしまう「有事」よりも、逆に「平時」における情報戦から考えていく必要があるのではないかと感じました。憲法学的には、国家はどんなに頑張っても個人の内心を操作することはできないという前提で、これまでずっと議論がなされてきました。ところがGAFAも人間の認知を科学的に操作するための研究者をどんどんリクルートしていますので、平時の政治空間においても、外国からの干渉は十分にあり得ます。平時におけるセキュリティとして考えられる問題はたくさんありますし、有事対応はあくまでその応用なんじゃないかという気がしなくもないです。逆に言えば、「平時」はすでになく、すべてが「有事」になっているということなのかもしれませんが。

国産プラットフォームの必要性｜国家公務員

直近では2023年11月に日本政府の共通クラウド基盤「ガバメントクラウド」において、初めて国内事業者としてさくらインターネットのサービスが選ばれました。NTTは独自のネットワーク・情報処理基盤のための「IOWN構想」を進めています。半導体も国産化が重要だというイニシアティブが進められています。

一部の人たちの間では強い問題意識がもたれており、そこに国費も投入され始めているので、きちんとした議論がなされていくことが必要だと感じています。

安全保障と国民主権｜憲法学者

これまでのプラットフォーム規制は、主に「ユーザー保護／ユーザー視点」という観点から論じられてきましたが、それが国家の安全保障を念頭に置いた議論になってきますと、その是非を決する上での根拠は何かというのが重要となります。

例えば日本では、日米安全保障条約が憲法9条に違反しているのではないかと争われた砂川事件に関して「統治行為論」の考えに則って、高度に政治性を有する、国家の命運を左右するような判断は裁判所は行わないという結論が出されています。つまり国家の命運を左右するような判断の是非は、裁判所ではなく主権者である国民が考えるべきであるというわけです。であるならば、プラットフォームを通じた安全保障も、本来、同じく国民の主権の問題になります。ヨーロッパでは、民主主義を勝ち取り守っていくという想いが市民の間にも根強く存在しますが、日本の場合は、そこがピンと来ないところが多分にありそうです。自分たちの安全を誰かが守ってくれる、守ってくれるなら誰でもいいじゃないか、という感覚ですね。ですから、安全保障の議論になった途端、なかなか自分事になりにくいのかもしれません。

であればこそ、本当はプラットフォームのあり方についても、国会で議論して承認するプロセスが必要だということになるはずで、AI規制に関しても日本政府はガイドラインを作成しようとしていますが、本当はフレームワークを法律でつくりつつ、アジャイルでやれるところはそうすべきだとも感じます。いまは一部の有識者たちによって、決して民主的とは言い難いプロセスによってつくられてしまっているところもあります。問題が国民に知られないうちに事態が進行してしまえば、後になって「誰が責任取るの？」という話になりかねません。

ブラックボックス化してしまいがち｜編集者

政府にデジタル関連のケイパビリティがないという話がありましたが、実際のところ、政治家／立法府が、そこにちゃんとコミットし切れていないという印象は強くあります。結果、官僚主導にならざるを得ず、どうしてもブラックボックス化してしまうということが起きているようにも見えます。

具体的なイシューから始める｜国家公務員

EUはこうやっている、アメリカではこうだ、中国ではこうだ、といった情報は断片的にどんどんと入ってはきます。しかしながら現行の立法サイクルでは、そのスピードに追いつけないところもあります。立法府と行政府の関係がどうあるべきかという抽象的なレイヤーの議論ももちろん必要なのですが、もう少し具体的なイシューに落とし込むことができれば違ってくるところがあるようにも感じます。

経済安全保障から考える｜ジャーナリスト

個人的には「経済安全保障」ということばは議論のとっかかりとしては悪くないのではないかと思っています。どんどん円安になっているなかで、2023年の日本のデジタル貿易赤字は5.5兆円にも上っていると言います。「政府も企業も外国のテック企業に高い使用料を払い続けていいんですか？」という問題提起は、多くの人を巻き込むことができるのかもしれません。経済の面から議論をしていくことで、議論が成立しやすくなる側面はあると感じます。

すぐそこにあるAI｜サイバーセキュリティ研究員

今回の議論は「プラットフォームが人間に与える影響」をめぐる話が多かったように思いますが、一方で現代はそのすぐ横にAIが存在する世界になってきています。古い話ではありますが、2013年にAP通信のTwitterアカウントがハッキングされ「ホワイトハウスで爆発が発生」という偽情報が投稿されてしまい、株価が急落したという出来事がありました。現在であれば、AIが偽情報を流し、それによってAIが株を自動売買して、といったかたちで、人間だけでなくAIもがミスリードされ、操作される対象になってしまうことも予想されます。さらに言えば、AIのサポートによって人間が意思決定することが今後増えていくとするなら、AIが出力する情報が操作されることもあり得ます。こうしたことを果たしてどのように法律的に扱い得るのか興味が湧きました。

民主主義はサイズダウンしていく｜憲法学者

あくまでも個人的な見解ですが、今後、法と民主主義の領域がサイズダウンしていくことは間違いないような気がしています。今後、アルゴリズム的な統治が進んでいくとすれば、間違いなく法や民主主義がカバーしうる領域は減っていくと思っています。

もし本当に人間が理性的な存在であるなら、国家も要らないし、法も要らないわけです。ところが、全然理性的ではないので、それを制御するためのアーキテクチャ、システムとして法や憲法が存在するわけです。いまも間接民主主義を採用しています。実際はエリートの集団で決めているだけで、民主主義なんてまったく存在しないじゃないかとの指摘もあります。

また、国会とは別の組織として、裁判所が違憲審査権を有するといった

システムが保持されています。それと同じように、仮に今後、民主主義によって判断される領域が減っていったとしても、どこか別の場所を残していくことは可能だと思います。どこにそうした領域を残しうるのか、それを考えていくのが目下の憲法学の役割なのだろうと思っています。

地方自治から始める｜国家公務員

年間に提出できる法案の上限は議会のスケジュール的に事実上決まっているので、各委員会で年間数本しか通らないのが実際の形式になってしまっています。民意の反映にも、そもそも時間上の物理的な上限があります。民意をどう集約して社会の方向性につなげていくのか、という観点からは、国家全体のイシューに加えて、「民主主義の学校は地方自治だ」ということばの通り、もう少しリアリティのある、手の届く空間において民主主義の実践が試されるのがいいのではないかと感じます。

「良き統治」を考える｜憲法学者

リチャード・タックという政治哲学者が『眠れる主権』(The Sleeping Sovereign)[*6]という本を2016年に出版しています。「主権と統治」というのはもともと「所有と経営の分離」みたいなところがあって、主権者は日々の生活で忙しいし、ガバナンスの仕組みだけつくっておいて基本的には寝ているのだけれども、重要な事項、例えば憲法問題などについては自分たちで決めなくてはいけないと書いているんです。ホッブズもルソーも、本来はそういう発想なんだと言うんですね。

そう考えると、直接民主的に決める領域が自明のものとしてあったわけではなく、「良き統治」を考える上では、民主主義を最大限に発動させる時間と、民主主義を「眠らせておく」時間をいかに上手にバランスしておくのかという観点があったわけですね。そのバランスの取り方が、AI、アルゴリズム、プラットフォームといったものの登場によって変わってくるとしたら、そこをどのように再編成するのかという議論が出てくる必要があります。

もちろん、民主主義で決める領域というのは残っていくし、残るべきだと思ってはいます。主権者も本来的には寝ていてはダメで、起きたときにちゃんとやれるよう、いろんな意見を聞いておかなくてはいけないのも、その通りです。とはいえ、現実的には歴史上それが十全に成されたことはないですし、いままでの民主主義が問題なく回っていたのかといえば決してそんなことはありません。

「良き統治」という観点から、プラットフォームや生成AIといったものを、経済・産業政策とも組み合わせながら、いかに使っていくのかという視点が必要なのではないかと思います。

第2部｜脚注

*1｜堀越功「GAFAMに飲まれる通信インフラ」、日経エレクトロニクス、Apr., 2022
https://xtech.nikkei.com/atcl/nxt/mag/ne/18/00082

*2｜山本龍彦「まつろわぬインフラ」、法律時報、Sep., 2022

*3｜Ian Bremmer “The Technopolar Moment: How Digital Powers Will Reshape the Global Order” Foreign Affairs, Oct. 19, 2021
https://www.foreignaffairs.com/articles/world/ian-bremmer-big-tech-global-order
イアン・ブレマー「地政学パワーとしてのビッグテック：米中対立と世界秩序を左右するプレイヤー」、フォーリン・アフェアーズ・リポート、Dec., 2021
https://www.foreignaffairsj.co.jp/articles/202112_bremmer

*4｜海野麻実「ミャンマー『SNS戦争』、国軍対フェイスブック」、ニューズウィーク日本版、Mar. 9, 2021
https://www.newsweekjapan.jp/stories/world/2021/03/vs-34.php

*5｜ブラッド・スミス「ウクライナの防衛：サイバー戦争の初期の教訓」、Microsoft News Center Japan、Jul. 4, 2022
https://news.microsoft.com/ja-jp/2022/07/04/220704-defending-ukraine-early-lessons-from-the-cyber-war

*6｜Richard Tuck "The Sleeping Sovereign : The Invention of Modern Democracy" Cambridge University Press, Feb., 2016

3

メディアと表現の自由

講義

アテンション・エコノミーという問題系

山本龍彦（憲法学・慶應義塾大学大学院法務研究科）

Photo by Art Media/Print Collector/Getty Images

オデュッセウスを誘惑するセイレーン。2世紀頃

新ブランダイス学派の台頭

第3部のテーマは「メディアと表現の自由」です。もう少し詳しく言えば、プラットフォームのアテンション・エコノミーの問題を憲法、人権、民主主義の視点から考えてみようということになるかと思います。

「アテンション・エコノミー」ということばは、ノーベル経済学賞を受賞した認知心理・経済学者のハーバート・サイモンという人が1960年代後半に提出した“予言”を元に、アメリカの社会学者マイケル・ゴールドハーバーによって1997年に提唱されました。

法学者のなかでは、早い時期からインターネットと社会の関係についての論考を多数発表してきたコロンビア大学ロースクールのティム・ウーが、精力的にこの問題を取り上げてきました。「ネットワーク中立性」ということばの提唱者でもある彼は、2021～23年にバイデン政権の大統領特別補佐官を務めており、弟子筋にあたるリナ・カーンも米連邦取引委員会（FTC）の委員長を務めています。

ティム・ウー、リナ・カーンは「新ブランダイス学派」と呼ばれる学派の急先鋒で、これは企業の競争や独占に関する政策（競争政策）をどのように構築するかをめぐる思想的立場のひとつですが、新ブランダイス学派は、そのなかでも巨大プラットフォームの規制を積極的に推進すべきとする立場です。

これまで、この領域で主流を占めていたのは、シカゴ学派の「法と経済学」（Law and Economics）の系譜です。ざっくりと言えば、法学もある意味数学的に、コスト・ベネフィットを計算して経済的損得で考えていけばいいという考え方です。ところがそれだけでは金銭的な利益に還元されない諸価値がないがしろにされてしまうとの批判が、ハーバード学派から提出され、それをさらに推し進めて、民主主義を守るという観点を織り込むかたちで競争政策を考えていこうというスタンスを取ったのが、新ブランダイス学派でした。

最近は日本の公正取引委員会でも、プラットフォームと新聞社・出版社の関係において、果たして対価が適正かどうかという議論を始めていますが、徐々に、民主主義の視点を加味した新ブランダイス学派の影響が強くなってきていると感じます。

アテンション・エコノミーの構造的問題

では、「アテンション・エコノミー」とは何かを改めて説明します。人間の可処分時間の総数は一定で、それが稀少であればこそ、経済的な価値を有することになります。その可処分時間を、無料のコンテンツやサービスで引きつけ、広告価値へと転換してプラットフォーム企業が広告主に販売するというビジネスモデルによって、人の「アテンション＝注意」を引く扇情的なコンテンツやサービスがどんどん増えてしまう現象、もしくはその経済のあり方を指しています。

経済学者でMicrosoftの首席研究員でもあるグレン・ワイルは、こうしたアテンション・エコノミーで成長するプラットフォームのことを「セイレーン・サーバー」（Siren Server）と呼んでいます。

ホメーロスの叙事詩『オデュッセイア』には、セイレーンという魔女／海の精が登場します。彼女たちは魅惑的な歌声で航海している人間を引き寄せ、最終的には船を沈没させて船員たちを食べてしまいます。非常に恐ろしい存在です。英雄オデュッセウスは、自分がセイレーンの術中にはまって、海に飛び込んでしまわぬよう、自らをマストに縛り付けてセイレーンの誘惑に抗います。

ワイルは、このギリシア神話を下敷きに、アテンションを求めて視聴者を誘惑するサービスやコンテンツをセイレーンになぞらえることで、「アテンション・エコノミー」の構造的問題を指摘しました。

言うまでもなく、これは古くからある問題で、日本に限らずテレビやラジオといった多くの民間の放送事業は、このビジネスモデルによって成立しています。ただ旧来の放送事業とインターネットでは何が違っているのかといえば、テレビ局やラジオ局には放送法という規制法があり、政治的公平原則を守る、真実を曲げないといった制限が課せられているほか、電波の有限性から参入できる事業者が免許制度によって厳しく制限されている点です。

一方で、スマホを通じて誰もがサービスやコンテンツを配信できてしまう現在の世界では、誰でもアテンション・エコノミーに参入することが可能となり、これまでのメディア産業を支えてきたビジネスモデルを制御してきた制限が、なし崩し的に決壊してしまっています。

ティム・ウーは「現在では情報の受け手のすべての時間、かつては非商業的な時間であった友人、家族と過ごす時間でさえもが、激しい奪い合い・競争の対象になっており、われわれの毎時間、実際には毎秒がそれを支配しようという商業的アクターの標的になっている」と若干情緒的に語っていますが、ユーザーの可処分時間を奪い合う「商業的アクター」に誰もがなれてしまうという状況が、ユーザーのアテンションの奪い合いを加速度的に熾烈化させています。

思想の自由市場

憲法学は、これまで「思想の自由市場」という考えを前提にしてきました。「思想の自由市場」とは、有害な思想・情報は対抗言論が浴びせられることによって自然淘汰されるので、政府は情報の良し悪しを判断すべきではないという考え方です。ですが現在の言論空間では、もはや情報の説得力や真実性を争うというより、いかにユーザーを刺激してインプレッションや

2024年3月12日、ワシントンDC。TikTok規制法案に反対するTikTokユーザーたち　Photo by Anna Moneymaker/Getty Images

PV（ページビュー）を奪い取るのかが競われています。

こうした議論を人より理解しているはずのわたしでさえ、TikTokを開くといつの間にか30分以上経ってしまっていたりします。この「縦スクロール＋スワイプ＋レコメンデーション」の仕組みは利用者のドーパミンを誘発し、スワイプする指を止められなくなる「究極のスロットマシン」「デジタル・コカイン」などとすら言われています。

加えてここまでも何度か触れてきたケンブリッジ・アナリティカ事件のように、プラットフォーマーがSNSユーザーのデータを取得し、それを個々のユーザーに合わせてパーソナライズするかたちで認知変容を迫るといったことも可能になっていますので、ユーザーは知らず知らずのうちに偏った情報にばかり触れていくことにもなります。

表現の自由と自己決定権

ティム・ウーは、こうした状態を「囚われの聴衆」（Captive Audience）と表現しています。ただし、このことば自体は、実は古くからあるものです。日本では1970～80年代の裁判で最高裁まで争われた「囚われの聴衆事件」というものがあります。これは大阪の弁護士が「電車内での強制的なCM放送は人格権の侵害にあたる」として大阪市を提訴した裁判で、車内という「囚われ」の空間で強制的に聞かされるCM放送が、聞きたくないものを聞かないというプライバシーの権利を侵害し、安全、快適な輸送という運送契約に違反しているかどうかを争う内容でした。最終的には原告が敗訴しましたが、アメリカでも表現の自由との兼ね合いで同じような裁判が行われています。

ティム・ウーはこうした過去の議論をアテンション・エコノミーを考える際に援用しています。パーソナライズが進んだレコメンデーションに基づい

てコンテンツを他律的に享受しているわたしたちをして、ウーは「囚われの聴衆」と呼びました。そしてさらに強いことばをもって、その状況を「同意によらないアテンションの強奪」「認知損傷」（Cognitive Impairment）とすら呼んでいます。これは「思考の自由」（Liberty of Thought）、つまり自己決定権にまつわる問題提起なのだと思います。

日本国憲法21条1項では「表現の自由」を保障していますが、法廷でメモを取る権利を勝ち取ったことで有名な「レペタ訴訟」（法廷メモ訴訟）の判例において、最高裁がこの条文について以下のように述べています。

> *各人が自由にさまざまな意見、知識、情報に接し、これを摂取する機会をもつことは、その者が個人として自己の思想及び人格を形成、発展させ、社会生活の中にこれを反映させていく上において欠くことのできないものであり、民主主義社会における思想及び情報の自由な伝達、交流の確保という基本的原理を真に実効あるものたらしめるためにも必要であって……*

「各人が自由にさまざまな意見、知識、情報に接し、これを摂取する機会」は、自己実現と民主主義のために必要だということを言っているわけです。

ここから汲み取るべきことはふたつあるのではないかと思います。ひとつ目は、多様な考え方に自律的、主体的に触れる自由を政府が制度的に保障する努力を重ねてきたことをどう評価するかということ。ふたつ目は、ここから、フェイクニュースや偽情報、誹謗中傷の問題にどう対処すべきかということです。

ひとつ目の論点に関して、新聞記者と話をしていると「とにかく国家は何もしてくれるな」というスタンスの方が一定数いらっしゃいますが、実態としましては、新聞社も出版社も独占禁止法上の再販制度で守られているわけです。第三種郵便物といった制度も、日本全国どこでも安く郵便が届けられる仕組みとなっていて、この恩恵を新聞社は受けています。テレビ局やラジオ局を対象とした放送法や、公職選挙法上の選挙運動規制などがあることで、言論に恣意的な偏りが生まれないように制限がかけられてきました。このように、多様な情報が行き渡り、誰もがそれに接することのできる機会が、いわば制度的にデザインされてきたところもあるわけです。

ふたつ目のフェイクニュースや偽情報、誹謗中傷の問題も、アテンション・エコノミーと構造的に結びついています。能登半島地震のときもそうだったように、偽情報だろうと何だろうと刺激的なことばや画像でインプレッションを稼いでお金儲けをしようとする人が、少なからず出てきます。極端な話、誹謗中傷などがなくなってしまえば、プラットフォームはビジネスとして成立しなくなるだろうとすら思えてしまうほどですが、第1部で紹介した「The Facebook Papers」は、まさにこの点を批判していたわけです。

「やった者勝ち」の世界

関連して、一見しただけでは見分けがつかないディープフェイク画像・音声の問題について、カリフォルニア工科大学教授の認知心理学者で『サブリミナル・インパクト』[*1]という著書もある下條信輔さんとお話しする機会が先日ありました。

彼もこうした議論には非常に興味をもたれていて、とりわけディープフェイクはかなり問題だとおっしゃっていました。かいつまんでお話ししますと、人間には顕在的な認知システムと潜在的な認知システムのふたつがあり、ディープフェイクの画像や動画は顕在意識では否定できるものの潜在意識では打ち消せないのだと、彼は指摘しています。さらに、そうやって潜在意識下に残ったイメージや音声が政治的な判断にも影響を与え、選挙結果の操作などもできてしまうのではないかという危惧をもたれていました。もと

もと「否定的で真新しい情報」は人間のアテンションを引く傾向がありますので、ディープフェイクの世界は、ある意味「やった者勝ち」の世界になってしまいます。

加えて「フェイク群衆」（Fake Crowd）という問題もあります。Microsoft脅威分析センターが2023年に発表したレポート「Digital threats from East Asia increase in breadth and effectiveness」[*2]では、アメリカの有権者になりすましたXユーザーによる銃規制や人種問題などへの印象操作、扇動目的で作成されたとみられるAI生成画像の投稿事例などを確認したと報告されていますし、またロシアでは官民協働の「トロール（荒らし）工場」を設立し、親ロシアの印象操作をするための偽情報コンテンツを膨大に作成している[*3]のも周知の通りです。

フィルターバブルの何が問題か

ここまで「メディアと表現の自由」をめぐって起きている事象をいくつか紹介してきましたが、具体的にどの分野で何が懸念されるかを整理しますと、以下の3つが挙げられるのではないかと考えています。

1. 個への影響：自己決定

2. 社会への影響：民主主義

3. 安全保障への影響：情報戦（認知戦）

2. と3. については第1部、第2部でもそれぞれ触れましたので、ここでは1. についてのみ、もう少しお話ししたいと思います。

Elyse Samuels/The Washington Post via Getty Images　マーク・ザッカーバーグ本人の動画とディープフェイク動画の比較

学生などと話していても「フィルターバブルが問題だと言われても自分が好きで心地良い情報に囲まれて何が問題なんですか？」と問いかけられることが多いのですが、そんなときわたしは自分の修士論文の話をよくします。

修士論文では遺伝情報のプライバシー保護をテーマにしました。指導教官からも「憲法学なのに何をしているんだ」と怒られたんですが、たまたま書店で遺伝子に関する書籍を見つけて、やってみたいと思ったんです。ですが、自分の得る情報が過去の履歴から完璧にパーソナライズされていたら、おそらくこうした偶然の出会いは、なくなるか非常に少なくなってしまうのではないでしょうか。

ただ、これは第1部でも少し意見をいただいて本当にその通りだなと思っているのは、フィルターバブルやエコーチェンバーには、自分の好きなものに囲まれているという快適さや安心感はあるわけですね。それに対して他人がどうこう言うのは、実際、非常にデリケートで難しい話なのだと思います。

これは図式的に言えば、功利主義的な快楽計算で快適さを優位に置くのか、もうちょっと規範的に、ジョン・ロールズの『正義論』[*4]のように幸福というものを考えていくのか、というものすごく根源的な問題なんですね。ただ、結局アテンション・エコノミーはフィルターバブル、エコーチェンバーを必然的に引き起こし、非常に抑圧的な政治体制と親和性が高くなってしまう懸念は大いにあると思います。

「情報的健康」という視点

何にせよ、そうやってひょんなことから始まった遺伝子に関する研究を進めるなかで、個人的には確率の問題が非常に気になっていきました。例えばがんは遺伝子の変化によって起こる病気ですが、その遺伝子の変化は次世代に伝わる可能性があります。それが発現するかどうかは統計的な確率の問題なんですね。そこから遺伝の話とアルゴリズムの話とが自分のなかで結びついたのですが、そうやって考えていくと、今後生体データに基づいたパーソナライゼーションによって「あなたは◯%の確率でがんを発症するので保険料が上がります」といったサービスが生まれてくることが想定されてきます。インターネットのガバナンスと規制に関する法学の第一人者ビクター・マイヤー＝ショーンベルガーはそれを「確率という名の牢獄」と呼んだわけです。

現在の憲法が保障する個人による自己決定権が、確率という牢獄のなかにますます拘束されていくのだとすると、どのように自己決定権を制度的に担保しうるのか。それを考えていくことが、わたしの研究のひとつの重要な基盤となっています。

こうした問題意識から、計算社会科学者の鳥海不二夫さんとの共著で『デジタル空間とどう向き合うか：情報的健康の実現をめざして』[*5]という本を2022年に出版しました。情報的健康とは何かというと、わたしはいまのところ以下のような定義をしています。

> さまざまな情報をバランスよく摂取したり、自らが摂取する情報の真正性や安全性等について意識したりすることで、偽情報等への「免疫」を獲得し、各人が希求する幸福を追求できている状態

逆に言えば、現代は情報の偏食が問題なのではないかということです。学生と話していても、ネットで読んだコンテンツがどんな媒体により発信されているのかを意識している人は多くありません。すべてが「ネットで読んだアレ」「Yahoo! ニュースになったアレ」といったように、平板で一元的な理解になってしまっています。

その情報がどういったメディアによるものか、取材を経ているのか、どの程度の信頼性を有しているのかといった背景情報に対する感覚もまた平準化され、さらにフィルターバブルに囲まれて中間集団のようなコミュニティとの接触頻度が減っていくと、フェイクニュースや偽情報などに対する耐性、免疫のようなものが損なわれるのではないかという危惧があります。生成AIが進歩してくると、そもそも人間がつくった情報なのかすら、曖昧になってきます。

これまでのメディアリテラシー教育は、どこか人間が理性的な存在である、未熟な子どもでも教育すれば理性的な存在になることができるといった理念を前提にしているように感じられますが、こうした考え方に対して、実験心理学者の田中優子さんは「接種理論」（Inoculation Theory）[*6]という考え方を紹介しています。

これは要するに、ワクチンを打つように心理的な予防接種をしておこうという提案です。具体的には「プレバンキング」という表現をされていますが、これは「事前曝露」という意味で、なりすましや誤ったデータの提示方法など、デマを広めるためによく使われるテクニックを用いた記事・動画の教材を使って、その手口を知ってもらうという方法です。フェイクニュースのつくり方を学ぶことで、いわば「抗体」をつくろうということですが、Google子会社のJigsawとケンブリッジ大学、ブリストル大学が共同制作した動画教材[*7]がヨーロッパでは公開されてもいます。

食育から学ぶこと

また、個人的には食育の歴史も参考になるのではないかと考えています。森田倫子さんという国会図書館の調査員が2004年に発表した「食育の背景と経緯：『食育基本法案』に関連して」[*8]というレポートがあるのですが、

1990年代以降の食育において以下のような問題が指摘されてきたとしています。

1. 脂肪摂取の過剰など、栄養バランスの悪化傾向
2. 朝食欠食の習慣化、孤食（一人で食べること）や個食（家族が各々異なった料理を食べること）の増加傾向など、食習慣の乱れ
3. 児童生徒の肥満の増加、過度の痩身、体力の低下傾向など、健康への影響
4. 食の安全に対する信頼の喪失
5. 体に良い食品・悪い食品に関する情報が氾濫する一方、適正な情報が不足していること
6. 食の外部化、ライフスタイルの多様化などにより、保護者が子どもの食生活を把握し、管理していくことが困難になっていること
7. 家庭において、食材に関する知識、調理技術、食文化、食に関するマナーなどを継承することが難しくなりつつあること
8. 食料資源の浪費
9. 食料の海外依存が進行し、食料自給率が低下していること

これらの項目を「情報」に置き換えると、いまの状況にマッチしていると言

えないでしょうか。これまで「おいしいんだから食べてもいいじゃん」と思っていたところ、毎日カップラーメンを食べるのに後ろめたさを感じてしまうようになるというのは、食育の成果のひとつであると言えるでしょう。

もちろん、情報的健康を実現する上で、個人が気をつけようという話だけでは終わりません。メディア企業であればファクトチェック団体とのさらなる連携、釣り見出しやコタツ記事問題の改善、プラットフォーム権力の監視など、やれそうなことがたくさんあります。

一方、プラットフォームに関しては、EUの「デジタルサービス法」(Digital Services Act) のような規制もあります。ここでは、例えば「レコメンダーシステム」の透明性（主なパラメーターの明示）を求めているほか、「VLOP」(Very Large Online Platforms。EUの人口4億5000万人の10%以上にリーチする超大規模プラットフォーム）については個々人のプロファイリングに基づかないレコメンデーション・システムの提供、（リスク対応として）重大な危機（公共の安全、公衆衛生など）発生時の対応メカニズムの検討なども多数義務付けています。

理性には限界がある

こうした取り組みが進みつつある一方で、個人的には「人間の理性にはやはり限界がある」ということを認めることを出発点にすべきなのではないかという思いがあります。もちろん、だからといって加速主義者のような「膠着した社会状況を変革するためには、資本主義やテクノロジーを際限なく進歩させればいい」という考え方にも必ずしも賛同はできません。わたしとしては、今回ご紹介した「オデュッセウスの強さ」と言いますか、弱さを自覚して自らを縛り付けられるようなアーキテクチャをつくっていくことが求められるのではないかと考えています。

そのアーキテクチャについて、どこまで法律として強制すべきかはさらなる議論が必要です。プラットフォーム間で一定の競争が維持されていれば、ユーザーの情報的健康にどこまで配慮しているか自体が競争の対象になりうるでしょう。ですが、このような競争＝市場による統制が可能となるためには、情報的健康の実現に向けてプラットフォームが行っている取り組みがユーザーに開示されていく必要があります。従って、少なくとも透明性＝情報開示については法律によって強制する必要があるように思います。

その他の取り組みについてはEUの「デジタルサービス法」のように、基本的には各プラットフォームの自主性を尊重し、その効果等を外部から検証・監査するようなやり方、あるいはプラットフォームの自主的な取り組みを政府が促進する「共同規制」のアプローチなども考えられるかもしれません。

議論

メディアと国家の行方

フェイクニュース、ディスインフォメーション、フィルターバブルを加速させるソーシャルメディアと国家の関係は、難題だらけだ。優先すべきは、表現の自由か、国民の安全か。議論は深まりながら、さらに広がっていく。

日本のプラットフォーム政策 | 民間企業役員

今回の話に関連する動きとして、政府と民間が共働する格好で「Trusted Web推進協議会」という組織が2020年に立ち上げられています。経緯としては、2019年に内閣官房が「デジタル市場競争本部」を立ち上げ、GAFAなどのプラットフォームに対する法規制も検討しつつ、それだけでは限界があるからと、民間も巻き込んでデータや情報の信頼性を担保する仕組みをつくろうということで設立されました。

プラットフォーマーがいなくても、中小企業などさまざまな人たちが自由にビジネスをつくることができたり、行政関連などパブリックなサービスもつくることができたりするように、多様な実証実験も行われています。例えば医療カルテであれば、これまでは個々の病院がただ保有しているだけだったものを、患者の同意のもとで病院同士のデータ連携ができるようにできないかとか、外国人が来日して就職する際、それが悪質な企業ではないことの証明ができないか、本人の就労歴がきちんと記録され閲覧できるようにできないか、といったことが具体的な取り組みとして挙がっています。

ただ個人的には、テクノロジーもそれを説明することばもどんどん専門的になってしまい、複雑で難しい議論になってきてしまっているなとも感じます。

消費者であり、事業者でもある | 弁護士

お話を非常に興味深く伺いましたが、わたし自身、どの立場でものを考え発言すべきなのかと考え込んでしまいました。一個人としては「気を抜くとすぐ30分ぐらいTikTok動画を観てしまう」ような弱さももっていますし、子どもの教育においてもアテンション・エコノミーの問題とどう向き合うかを考えさせられます。ですが弁護士という事業者として働く身としては、いかに現在のレギュレーションのなかで自分たちのことを認知してもらい、勝ち抜くかを考えなければなりません。その意味では、必然的にアテンション・エコノミーのなかに参入せざるを得ない。つまり、自分もまたその経済の一部であるとの自覚はありつつも、その一方で、ネット上で誹謗中傷を受けた被害者の弁護などを行う立場でもありますので、まずはどの立場から議論をすべきなのか、という点ですでに悩んでしまいます。

新たなビジネスモデルの開拓 | UXコンサルタント

SNSのビジネスモデルは広告モデルだけかといえば、そうではありません。Facebookは売り上げの90%以上が広告ビジネス経由である一方、中国のネット企業として有名なAlibaba、Tencentといった巨大プラットフォーム企業は、売上構成がゲーム事業、金融事業でそれぞれ3割ずつぐらいになっています。

中国には銀行口座をもてず、信用情報もないことからクレジットカードもつくれず、銀行借入もできないという人が少なからずいます。そうした環境のなかで、プラットフォーマーたちは、個人の金融取引データを活用しつつ、少額融資のビジネスを伸ばしていきました。それを知ったマーク・ザッカーバーグがそういった方面にも進出したいという思惑もあって立ち上げ

を宣言したのがデジタル通貨「Libra」（リブラ）でしたが、アメリカをはじめ世界中の金融当局から懸念を表明され計画は中止となってしまいます。ですが、この施策にはアテンション・エコノミー偏重から抜け出すという側面もありました。アメリカでは2023年にTikTokでのEC、ライブコマースの機能が始まっていますが、その結果、コンテンツが広告だらけになってしまって批判も出ています。こうした動きの背景には、インフルエンサーやクリエイターが広告以外で収益を上げることをできるようにする、いわゆる「クリエイター・エコノミー」の促進という観点もあったはずですが、そこに参入者が増えてしまうと、結局広告費を払ってリーチを取らないといけなくなるという堂々巡りも起きてしまっています。

いずれにせよ、アテンション・エコノミーの問題を考える上では、ビジネスモデルを新たに開拓していく余地はまだまだあると思いますし、プラットフォームを、思想や言論に限らない、もっと多様な「市場」へとつくりかえていくことは可能なのではないかと考えています。

「表現の自由」原理主義｜憲法学者

現在はプラットフォームがコミュニケーションインフラになってしまっており、政治や行政もそのアテンション・エコノミーの枠組みに乗らなければ、十分な情報発信ができない、つまり非商業的な存在まで商業的なロジックのなかで情報戦略を展開せざるを得ない状況になってしまっているということは、改めて問題として検討されるべきだと思います。

プラットフォームに掲載されるコンテンツに対する責任をプラットフォームに問い、もう少し規制を強めるべきだという意見もあるとは思いますが、アメリカについて言えば、いまだにこうした規制への反対は根強くあります。そこには、プラットフォーマーたちの強力なロビイングを通じた抵抗もありますが、1970年代頃から、ある種の「表現の自由」を原理主義的に捉えてきた歴史的な傾向が影響しているようにも思われます。企業による巨額な政治献金も、「表現の自由」という観点から合憲になってしまう国ですから、当然プラットフォーム側も政府による規制に対しては、表現の自由の論理で抵抗することが予想されます。

「インターネットに固有の問題」は何なのか｜編集者

ことメディアの問題に関して言いますと、「インターネット登場以降に生じた固有の問題」と「インターネット登場以前から存在していた問題」とが、適切に切り分けられておらず、メディア規制に関する議論それ自体が、単純な二元論に還元されてしまったり、極論化してしまっていたりするように感じます。既存のメディアがすでに抱えていた問題や、そのビジネスモデルを支えていた制度の限界などをよく見極めた上でないと、そもそも「何が変わってしまったのか」がよくわかりませんし、それが明確化されていないところでは、「問題」もきちんと抽出できないのではないかと感じます。

1947年の大衆メディア批判｜哲学研究者

お話のなかにあった『オデュッセイア』のセイレーンの神話は、アドルノとホルクハイマーのよく知られた名著『啓蒙の弁証法』のなかでも触れられています。1947年に出版された『啓蒙の弁証法』は一言で言ってしまえば、「近代以降人間は啓蒙されたはずなのに、なぜナチスの蛮行を許してしまったのか」を主題として扱った本ですが、そのなかには、アメリカの大衆メディアに対する批判も多く登場します。つまり、アメリカの大衆文化という

「セイレーン」にいかに対抗するのかという主旨なんですね。大衆メディア化していく社会に対して警鐘を鳴らしているわけですが、とりわけアドルノは、アメリカのハリウッド映画やジャズといった大衆文化を非常に嫌悪していました。簡単に言うと、大衆文化にばかり触れていたらバカになる、というわけです。こうした大衆文化、大衆メディアに対する批判は、20世紀を通じてずっと繰り返されてきました。そして、いまもなおSNSやYouTubeといったものをめぐって同じ批判が繰り返されているわけですね。

そうやって歴史を振り返ってみたときに、インターネットにおける大衆文化と、これまでの大衆文化とではどこが違っているのかを、やはり詳細に検討してみる必要はあるように感じます。例えば、セイレーンの神話のアナロジーでいけば、インターネットがもたらしている問題は、わたしたちは必ずしもオデュッセウスの側にばかりいるわけではなく、むしろその部下たちの側に、さらにはセイレーンの側でもあるという点にあるのかもしれません。そう考えると、オデュッセウスのモデルが使えるのかどうか、疑問ではあります。あるいは、リヴァイアサンとビヒモスの対比についても、もはや、そのふたつの怪物を切り分けて特定することができなくなっているところに、難しさの根源があるのかもしれません。

「食育」のアナロジー｜情報法研究者

「インターネット登場以前から存在していた問題」に関してはわたしも連想するものがありました。情報量が爆発的に増えて洪水のようになったという状況は、例えば14世紀のルネサンス期の頃にもあったと聞きます。十字軍の遠征を受けてビザンチン文化が流入し、ギリシア・ローマ時代の知識のリバイバルが起こり、さらに活版印刷の発明もあって一種の情報爆発が起きたそうですが、そこで何が生まれたかと言うと、インデックスやレファレンスブックのような「メタ情報」だったといいます。こんな話も、案外現在のインターネットにつながるところがありそうで、いまでも「メタ情報が大事」といった議論はよく聞きます。もちろん現在起きている問題は、昔と単純に比較できるものではありませんが、必ずしもすべてが新しい問題なのではないのではないかという感覚はたしかにあります。

また、お話のなかで「情報的健康」を目指すために食育の歴史を参考にすべきという提案がありましたが、栄養における「良いバランス」はある程度科学的な合意が取れると思う一方、政治や思想上の「良いバランス」を誰がどのように決定しうるのかという点からも、合意に至るのが不可能であるようにも感じます。アナロジーとしては魅力的ではあるのですが。

多様なモードを許容する｜自由研究員

お話を伺っていて思ったのは、メディア空間のなかに各人の多元性のようなものをつくっていかなければならないのかなということでした。

人は本来、相対する人や環境に合わせて、距離を置いたり、距離を縮めたりといったことをごく自然にやっているはずです。対話する相手によって、異なる自分を演じるようなことも日常的にやっています。ところが、それがソーシャルメディアのような空間に入った瞬間、アテンション・エコノミーにも駆動させられるかたちで、自分の正義を貫くために他者を排撃し続けなければならないような、非常に単純化されたモードに集約させられてしまいがちです。多様なモードを十全に許容できる空間になっていないんですね。

現実社会のなかで行っているような、いわば無意識的で多様なロールプレイを、一種の習慣として身につけていくような、そうした訓練や練習が、わたしたち自身に必要なのかもしれません。「情報の予防接種」というのはそういうことなのかな、と理解しました。

予防原則的な施策を｜神経法学研究者

「情報の予防接種」に関連することかもしれませんが、インターネット以降と一口に言っても、何歳頃にどんなメディアに接してきたかで前提が変わってくるのかな、とも思います。以前、「YouTubeの動画視聴者は10分間ぐらいしか集中力がもたない」などと言われていましたが、いまのTikTokが流行する環境では10秒ぐらいしかもたないとも言われています。その一方で、長時間の連続ドラマを一気見するような習慣が生まれたりといった矛盾するような現象もあります。この辺り、まだSNSが登場してから1世代も経っていませんし、その実際の影響については追跡的な調査も必要だとは思うのですが、その一方で「思考力の質が本質的に変容した世代が生まれてしまった」となってからでは遅いので、やはり予防原則的に考えておいたほうが良いのだろうなと感じました。

国家は要らないのか｜憲法学者

インターネット批判、SNS批判も「昔は良かったのにいまは酷い」といったノスタルジーからなされる部分がそれなりにあるのかもしれませんし、もっと言えば「お前らは既得権を守ろうとする守旧派だろう」という批判もあり得ます。パーソナライゼーションについても、昔なら店員が「客はどんな服装でどんな靴を履いているか」といった情報からオススメを決めていたし、それもパーソナライズだろうと言えばそうでしょうが、個人の選択の結果、つまり心の声がデータとして取れ、精神状態を精度高くプロファイリングでき、認知システムに直接かつ意図的にトリガーをかけられるところは、おそらく新しい現象だろうと考えていいのではないでしょうか。

インターネット以前の言論空間はエリートが支配していたというのは事実ですが、それによって国民国家という共同体が維持できていたわけです。一方、それがナショナリズムの問題や戦争を引き起こすブースターにもなっていました。そう考えるなら、パーソナライゼーションの進行は、近代的な主権国家体制を壊してしまう可能性を孕んでいます。そうした動揺のなかで、情報というもののありようも極めて不安定化し、そこにおいて優先されるべきなのは、自由なのか、あるいは安全、幸福なのかが問われているわけですが、それは、極論してしまうと、国家はもはやなくてもいいのか、あるいはやはり残しておいたほうがいいのか、という問いでもあるわけですね。

人間には「死にたくない」という本能的欲求があります。そしてその欲求が、「安全」というものへの希求となっていきます。その安全を維持するために、かつては教会や聖書の教えや、理性といったものが、統治のロジックとして使われてきました。そしていまではアーキテクチャ的な統治、あるいはナッジ的に人間の認知に介入していくかたちの統治が可能になりつつあります。それが極限まで進めば国家という枠組みも必要なくなってしまうかもしれません。

ですが、急激にそこまで進んでしまえば、多くの人が死んでしまうことも予想されます。であればこそ、50年、100年かけて順々にステップを踏んでいこうとする考え方が必要になるのではないでしょうか。フィルターバブルで好きなものだけに囲まれたいというウェルビーイングのあり方も存在するでしょうが、一方でそうでない人生を送りたい人もいるはずだと思っています。幸福のあり方は多様であってほしいという願いもまたあるわけですね。それを許容するためには、この先も、民主主義を残していかなければならないと、わたしは考えています。

第３部｜脚注

＊１｜下條信輔『サブリミナル・インパクト：情動と潜在認知の現代』、筑摩書房、2008年

＊２｜Microsoft Threat Analysis Center “Sophistication, scope, and scale:Digital threats from East Asia increase in breadth and effectiveness”、Sep., 2023
https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RW1aFyW

＊３｜平和博「１週間で閲覧１億超、ロシア『内部文書』が示す偽情報拡散のPDCAとは ウクライナ侵攻３年目に」、Yahoo!ニュース エキスパート、Feb. 26, 2024
https://news.yahoo.co.jp/expert/articles/8ed04bd11cdd349c7ca727e8949af70481f1479b

＊４｜ジョン・ロールズ『正義論（改訂版）』、紀伊國屋書店、2010年

＊５｜鳥海不二夫、山本龍彦『デジタル空間とどう向き合うか：情報的健康の実現をめざして』、日経BP、Jul., 2022

＊６｜田中優子「なぜひとは誤情報を信じ続けるのか：デジタル環境と認知バイアスの交互作用」、電子情報通信学会 DPF研究会、Jan. 31, 2024
https://www.ieice.org/~dpf/wp-content/uploads/2024/01/20240131_DPF%E7%A0%94%E7%A9%B6%E4%BC%9A_ytanaka.pdf

＊７｜https://inoculation.science/inoculation-videos-boosters

＊８｜森田倫子「食育の背景と経緯：『食育基本法案』に関連して」、調査と情報、Oct. 29, 2004
https://dl.ndl.go.jp/view/download/digidepo_1000729_po_0457.pdf?contentNo=1

資料

全社会化するアメリカのサイバーセキュリティ教育

「2023年度 海外におけるサイバーセキュリティ教育調査 調査報告書：米国」抜粋

米国では、国民生活のあらゆる領域にまたがる「国家防衛」を担うサイバーセキュリティ人材の開発に、国を挙げて果敢に取り組んでいる。米国立標準技術研究所によって策定された「NICE Framework」を通じて、連邦政府、地方政府、民間企業、研究・教育機関、市民組織等を横断して、サイバーセキュリティの業務内容や遂行者の能力を標準化したことで、業界やセクターをまたいで、全社会的にサイバーセキュリティ人材を育てていく体制を整備した。ここでは、その「NICE Framework」の成り立ちや概要を踏まえた上で、その活用先を駆け足で紹介していくほか、直接的には「NICE Framework」とは結びつきはないものの、日本のサイバーセキュリティ人材教育において参考になる事例も取り上げた。また、米国における多様な取り組みを概観した上で、人材不足が慢性的な課題となっている日本において、どのような取り組みが求められているか提言する。レポート全文は「2023年度 海外におけるサイバーセキュリティ教育調査 調査報告書：米国」（アクセンチュア テクノロジーコンサルティング本部が調査を担当）に掲載されている。

「NICE Framework」を知る

NICE Frameworkとは何か？

「NICE Framework」は、“National Initiative for Cybersecurity Education Cybersecurity Workforce Framework”の略で、National Institute of Standards and Technology（NIST／米国立標準技術研究所）がサイバーセキュリティの仕事と学習者の能力を説明する標準的なアプローチと共通言語を確立することを目的に策定したフレームワークである。

サイバーセキュリティ人材が当てはまる7つのカテゴリと、カテゴリ毎の専門分野（Specialty Area）、業務内容（Task）や、その職に就くために必要となる知識（Knowledge）、スキル（Skill）等が整理されている。また、組織（雇用者や教育・トレーニング機関）が学習者を評価するメカニズムとして、Competency（ある仕事をするための学習者の全体的な能力を評価する指標）やWork Role（仕事の役割）も整理されており、学習者（学生、求職者、従業員を含む）だけでなく、雇用主、学界、トレーニング及び認定プロバイダーによって幅広く参照されている。

なぜ、いかに生まれたのか？

「NICE Framework」は、サイバーセキュリティの人材が定義及び評価されていないことを課題とし、DHS（国土安全保障省）によって2007年に作成されたITセキュリティ必須知識体系（IT Security Essential Body of Knowledge ／ EBK）をベースに、連邦政府内のサイバーセキュリティの役割を理解するための標準フレームワークとして、連邦最高情報責任者（CIO）評議会によって2012年9月に公開された。その後、米国政府全体のレビューを通してさらなる調査・検証が行われ、「NICE Framework」のバージョン2.0が2014年に一般公開された。

さらに、公共部門と民間部門の両方にとって参照可能なリソースとするため、国土安全保障省と米国立標準技術研究所は、OSD（国防長官室）と協力してバージョン2.0を拡張し、2017年8月に「NIST Special Publication 800-181」としてバージョン3.0が発行され、2019年11月にバージョン3.0の改訂を開始し、コメント募集と反映によって「NICE Framework」の俊敏性、柔軟性、相互運用性、及びモジュール性を向上させた。この現行バージョンは、2020年11月に「NIST 特別出版物800-181 リビジョン1：サイバーセキュリティのためのワークフォースフレームワーク」として発行された。

7つのカテゴリと3つの構成要素

「NICE Framework」のカテゴリは以下の7つ。

- 分析（Analyze）
- 収集と運用（Collect and Operate）
- 調査（Investigate）
- 実施とメンテナンス（Operate and Maintain）
- 統括と管理（Oversee and Govern）
- 保護と防御（Protect and Defend）
- 安全の規定（Securely Provision）

さらにNICE Frameworkには、中核となる以下の3つの構成要素がある。

- タスク（Task）
- 知識（Knowledge）
- スキル（Skill）

以上3つは合わせて「TKS ステートメント」と呼ばれる。「Taskステートメント」は実行する作業を定義し、「Knowledge/Skillステートメント」は学習者がその作業を完了するために何を知っていて、何を実行できなければならないかを定義する。構成要素を一貫して使用することで、ピアレベル、セクターレベル、州レベル、国家レベル、または国際レベルでのコミュニケーションが可能になり、共通の課題に対する革新的なソリューションを推進し、新しい組織や個人の参入障壁を下げ、労働力の流動性を促進することができる。

NICE Frameworkの主だった活用事例

大学の取り組み

National Centers of Academic Excellence in Cybersecurity（NCAE-C）

「NCAE-C」は、サイバーセキュリティ教育に注力している総合大学、単科大学、コミュニティカレッジなどの教育機関をある一定の基準を満たしていることを条件に、サイバーセキュリティ学術分野のセンターオブエクセレンス（CoE）に認定するプログラムで、国家安全保障局と国土安全保障省によって共同で主催されている。

米国の2年制、4年制、大学院のすべての地域認定大学は、CAE-C 指定機関になるための申請資格があり、2023年現在、300を超える教育機関が指定されている。教育機関は5アカデミックイヤー毎に再指定を申請する必要がある。また、本認定の対象となる教育機関は、以下の観点を満たしている必要がある。2023年現在、本認定制度には「Center of Academic Excellence in Cyber Defense」（CAE-CD）、「Center of Academic Excellence in Cyber Operations」（CAE-CO）、「Center of Academic Excellence in Cyber Research」（CAE-R）の3種類があるが、それぞれの教育目的は以下となっている。

Center of Academic Excellence in Cyber Defense（CAE-CD）
サイバー防衛の高等教育と研究を促進することにより、国家インフラストラクチャへの脅威を軽減し、資格のあるサイバーセキュリティ専門家のパイプラインを国に提供すること

Center of Academic Excellence in Cyber Operations（CAE-CO）
サイバーセキュリティ教育のための国家イニシアチブ（President's National Initiative for Cybersecurity Education ／ NICE）

デジタル国家の構築を支援し、サイバーセキュリティ国家をサポートできる熟練労働者のプールを拡大すること

Center of Academic Excellence in Cyber Research（CAE-R）
米国が壊滅的なインシデントを防止及び対応できるようにする堅牢なサイバー防御技術、ポリシー、及び慣行の理解を深めること

サイバーセキュリティ社会基盤安全保障庁の取り組み

CISA

「CISA」（Cybersecurity and Infrastructure Security Agency／サイバーセキュリティ社会基盤安全保障庁）は、連邦政府、SLTT（State, local, tribal, and territorial／州、地方、部族、準州）政府、産業界、中小企業、教育機関、一般国民向けに、さまざまな無料のサイバーセキュリティトレーニングや演習プログラム、出版物を開発・提供している。本プログラムの目的は、国家のサイバー人材の育成をサポートすることによって国家のサイバーインフラストラクチャを保護することである。

一般向け無料公開コースの例

・公共向けのコーディング
・公衆のための重要インフラの保護
・一般向けリバースエンジニアリング
・クラウドコンピューティングのセキュリティ
・クラウドセキュリティ：リーダーが知っておくべきこと
・一般向けの法執行のための暗号通貨
・一般向けのサイバーサプライチェーンリスク管理
・サイバーエッセンシャル
・管理者のためのサイバーセキュリティの基礎
・サイバーリスク管理の基礎
・サイバーインテリジェンスについて
・DNS攻撃を理解する
・Web及び電子メールサーバのセキュリティを理解する

CISAでは、フルタイムの連邦職員を対象にした「Federal Cyber Defense Skilling Academy」（FCDSA／連邦サイバー防衛スキルアカデミー）はサイバー防衛アナリスト（CDA）の基本的な知識、スキル、能力を開発するために作成された3か月の集中的なトレーニングプログラムも提供している。

プログラム内で扱われるトピック

・基本的なネットワークとプロトコルの分析
・CompTIA Security+
・インテリジェンスベースのコンピュータネットワーク防御の概念
・相関攻撃、高度なデータ分析
・Linuxの基礎
・一般的なハッカーのテクニック、手法、ベクトルの特定
・インシデント検出の対応と処理
・Pythonの概要
・セキュリティ分析のためのPython
・Windowsに慣れる

さらにCISAは、送電網や水処理施設などの重要なインフラに対するサイバー攻撃から保護するために、オンデマンドの産業用制御システム（ICS）サイバーセキュリティトレーニングも無料で提供している。「Virtual Learning Portal」

では、ICS/OT関連のサイバーセキュリティトレーニングの受講が可能になる。ICSトレーニングで学ぶことができる主だったコースと、その所要時間は以下の通りである。

ICSトレーニングコンテンツ抜粋

- 制御システムのためのOPSEC（運用上の安全保障）について（1時間）
- ICS（産業制御システム）の展開における違いについて（1.5時間）
- 一般的なITコンポーネントがICSに及ぼす影響について（1.5時間）
- 一般的なICSコンポーネントについて（1.5時間）
- IT及びICS領域におけるサイバーセキュリティについて（1.5時間）
- サイバーセキュリティのリスクについて（1.5時間）
- 現在の傾向（脅威）について（1.5時間）
- 現在の傾向（脆弱性）について（1.5時間）
- サイバーセキュリティインシデントの影響を決定する方法について（1.5時間）
- IT及びICSにおける攻撃手法について（1.5時間）
- マネージャー向けの産業制御システムサイバーセキュリティの現状について（1時間）

国防総省関連の取り組み

DoD Cyber Workforce Framework

「DoD Cyber Workforce Framework」（DCWF）は「国防総省指令（DoDD）8140.01」で定義されているサイバーセキュリティ業務について説明するフレームワークで、7つの分類、33の専門分野、71の仕事の役割からなる階層構造をもつ（作成当時は54の階層だったが、AI、データ、分析、産業用制御システム、及びソフトウェアを含めることで増加した）。このフレームワークの特徴は以下の3点。

1. 各仕事の役割に、主要な機能を実行するために何が必要かを説明する「KSATs」（知識、スキル、能力、タスク）の代表的なリストだけでなく、定義も含まれており、これによって各仕事の役割を明確に理解することができる。

2. 各仕事の役割に求められる基本的な資格オプションと居住条件が「DoD Manual 8140.03」に従って示されており、これによって、それぞれの仕事を担うために必要な学位や資格などの要件を明確に理解することができる。

3. 各仕事の役割を担う上で役に立つトレーニングが明確化されており、各仕事を遂行するために必要なトレーニングの要件を明確に理解することができる。

地方の取り組み

「州のサイバーセキュリティ職員に関するNASCIO-NGA円卓会議レポート」

「州のサイバーセキュリティ職員に関するNASCIO-NGA円卓会議レポート」は、2023年に公開されたNational Association of State Chief Information Officers（NASCIO／全米州CIO協会）と、National Governors Association（NGA／全米知事協会）が、知事の政策顧問、州の情報技術、サイバーセキュリティのリーダー、労働力の専門家、その他の専門家を招集して実施した会議から得られた洞察などをまとめた報告書だ。このレポートでは、各州がいますぐ取るべき行動として下記を特定している。

・就業先として選ばれるために、使命を持った仕事であること、州政府が提供する独自の福利厚生があることを効果的にマーケティング／ブランディングすること

・労働環境を改善し、リモートや在宅勤務のオプションを提供し、燃え尽き症候群や従業員の精神的及び感情的健康への対応に重点を置くことによって、新型コロナウイルス感染症のパンデミックの永続的な影響に適応する

・採用、定着の実践において、多様性、公平性、包摂性、帰属意識に重点を置く

・教育の機会を提供し、人材パイプラインを構築するために、民間部門、学界、非営利団体、連邦政府、少数民族を支援する機関、専門家協会などの主要なテクノロジー及びサイバーセキュリティの利害関係者と協力する

・業界標準の役職を反映してポジションの説明をつくり直し、時代遅れの要件や不要な要件を廃すことで、参入障壁を低くする。NICE Frameworkに合わせることで、サイバーセキュリティの職名をより魅力的で直感的なものにアップデートし、候補者を要件によって排除することを目的とした考え方から、応募を奨励する考え方に変えていく

民間企業の取り組み

Palo Alto Networks Cybersecurity Academy program

「Palo Alto Networks Cybersecurity Academy Program」は、民間企業「Palo Alto Networks」による高校、大学、それ以降の学生を対象とした教育機関向けのプログラム。サイバーセキュリティの基礎、クラウド、ネットワークセキュリティ、セキュリティオペレーションセンターの運営などの包括的な一連のコースを提供している。北米、南米、ヨーロッパ、中東、アフリカ、アジアなど世界70か国以上の1100以上の教育機関で利用されている。このプログラムの主だった特徴は以下3点。

1. 教育機関毎の申し込みが必要だが、申し込めば無料で利用することができる。これによって幅広い教育機関が利用することができる。

2. 教員は関連するすべてのコース評価で80%以上のスコアを獲得し、ラボを修了する必要がある。ラボを修了した教員は、教育機関の学生に「Palo Alto Networks」が提供するカリキュラムとラボ、資格試験などを使ってトレーニングを授けることができる。また、学生向けに認定資格も提供している。

3. すべてのカリキュラムは「NICE Framework」の枠組みに沿っている。これにより、カリキュラムの対象者を明確にすることができている。

NICE Frameworkを活用していない参考事例

奨学金の提供

CyberCorps: Scholarship for Service

「Scholarship For Service」（SFS）は、National Science Foundation（NSF／米国国立科学財団）、国土安全保障省、U.S. Office of Personnel Management（OPM／米国人事管理局）が共同で運営する奨学金制度で、受給者が卒業後奨学金の受給期間分、政府関連機関でサイバーセキュリティ職に従事することを条件に、サイバーセキュリティ分野の学部及び大学院（修士またはPhD）教育に対して最大3年間の奨学金を提供するものである。

本奨学金は、連邦、州、地方、及び部族政府のサイバーセキュリティミッションのニーズを満たすために、次世代の情報技術専門家、産業用制御システム（OT）セキュリティ専門家、及びセキュリティ管理者を採用及び訓練するように設計された独自のプログラムであり、米国国立科学財団の助成金を通じて資金提供されている。

登録研修プログラム

United Services Military Apprenticeship Program

「United Services Military Apprenticeship Program」（USMAP／ユナイテッドサービス軍事登録研修プログラム）は、米国国防総省と United States Department of Labor（DOL／米国労働省）による現役の海軍、陸軍、海兵隊、沿岸警備隊などの隊員を対象とした登録研修プログラム。職務スキルを向上させ、現役中に「民間登録研修」の要件を完了する機会を提供する。これにより、民間労働力への移行時に訓練と経験を証明できる。

この研修プログラムにおいて、サイバーセキュリティ分野のプログラムが最初に登録されたのは2022年1月で、それ以降、5つのサイバーセキュリティ関連プログラムが承認された。2023年9月時点で9つの新しいサイバーセキュリティプログラムが利用可能とアナウンスされている。この研修プログラムの特徴は以下3点。

1. プログラムを利用するためには以下の要件を満たす必要があり、任務に基づいてプログラムが実施される。

・現役及び予備役の訓練及び管理海軍、現役警備予備役陸軍、現役予備役海兵隊、または沿岸警備隊の隊員であること
・入隊期間が最低1年間残っていること
・指定された格付け／軍事専門分野に割り当てられ、その任務を遂行していること
・業界に必要な正式な座学のトレーニングを完了していること
・選択した分野は、担保任務や一時的な任務ではなく、現在所属する部隊の主な仕事であること

2. このプログラムの実習には、教室での指導とOJTの両方の要素が含まれており、これによって知識と実務の両方に基づいた経験を積むことができる。

3. プログラムの進捗状況の測定方法は「時間ベースの実習」と「コンピテンシーベースの研修」の2種類があり、いずれかを選択することができる。「時間ベースの実習」は、その分野の職業に就いたことがなく、コンピテンシーに基づく見習いに必要な経験が不足している人のためのものである。仕事または正式な学習に費やした時間数で進捗状況が測定される。「コンピテンシーベースの研修」は、それぞれの分野において経験豊富な「E-5」以上の人のためのものである。該当分野に関連する知識、スキル、能力の応用を実証することで進捗状況が測定される。

トレーニングの提供

EVOLVE Academy

「EVOLVE Security」が運営するオンラインアカデミーで、サイバーセキュリティのキャリアで優れた能力を発揮するために必要なスキルと知識を身に付けることができる、総合的なサイバーセキュリティトレーニング機関。サイバーセキュリティ全般について学ぶブートキャンプのほか、OSCP準備ブートキャンプと基礎を学ぶオンデマンドコースを提供している。Evolve Academyは6年連続でフォーチュン誌の「最優秀サイバーセキュリティブートキャンプ」に選出されている。

地政学とサイバーセキュリティ

Alperovitch Institute for Cybersecurity Studies

「Alperovitch Institute for Cybersecurity Studies」は、ジョンズ・ホプキンス大学内の「School of Advanced International Studies」（SAIS／高等国際問題大学院）の研究所のひとつで、ワシントンDCの地政学シンクタンク「Silverado Policy Accelerator」の会長であり、「CrowdStrike」共同創設者で元最高技術責任者でもあるドミトリ・アルペロビッチ氏とモーリーン・ヒンマン氏の支援を受けて、2021年秋に設立されたサイバーセキュリティ研究センター。

地政学的観点からサイバーセキュリティと国家戦略の交差点における最先端の研究を行い、大学院生を将来のセイバーセキュリティ分野の政策立案者や大手企業・政府機関の実践者となるよう訓練するために設立された。また、この研究所は、業界幹部、取締役会、議会職員、政府関係者、軍・諜報員に幹部教育プログラムも提供する予定だという。

アルペロビッチ研究所では、1種類の修士課程コース「Master of Arts in Strategy, Cybersecurity, and Intelligence」（MASCI）と、PhD学生への奨励金制度「PhD Alperovitch Fellowship」が提供されている。それぞれの詳細は以下の通り。

Master of Arts in Strategy, Cybersecurity, and Intelligence（MASCI）

・将来のサイバーセキュリティ分野のリーダーやオペレーターが戦略、運用、戦術レベルで健全な意思決定を行えるように準備するための1年間の学位
・MASCIはSAIS全体の学位プログラムであり、サイバーセキュリティのコースワークは主にアルペロビッチ提携教員によって教えられる
・MASCIの学生は、テロリズム、過激主義、サイバーセキュリティ、偽情報、政治戦争、秘密作戦、制裁、特殊作戦、経済スパイなどの主要な戦略と諜報のトピックを習得する

PhD Alperovitch Fellowship

・サイバーセキュリティ政策における次世代の学際的な教育者や学者を訓練することを目的として、博士号取得を目指す学生に経済的援助とサポートを提供する研究奨励金制度
・授業料全額、最長4年間の年間生活費、健康保険が提供される
・本プログラムの博士号候補者は、サイバーセキュリティと国際性の交差点で独自の研究を行う

高校教師への教材提供

Teaching Security

「Teaching Security」は、International Computer Science Institute（ICSI／国際コンピュータサイエンス研究所）のカリキュラムプロジェクトである。高校で脅威モデリングと人間中心の認証の性質を中心とした重要なサイバーセキュリティ原則を教えるための、教室ですぐに使える教材と授業計画を提供している。2023年9月時点で以下の3つのレッスンが提供されている。

1. セキュリティマインドセット：脅威モデリングを通じたサイバーセキュリティ
2. 認証とは何か：なぜ必要なのか
3. 社会工学：最も古いハック

本プロジェクトの教育対象は高校生であり、サイバーセキュリティやコンピュータサイエンスを学ぶ学生だけでなく、あらゆる学生が対象となっている。教育目的は、「サイバーセキュリティに対する学生の興味を刺激すること」「あらゆる分野の将来のエンジニアにセキュリティへの影響を理解させること」「すべての生徒にオンラインでの安全と個人情報を保護するための基本的なスキルを提供すること」の3点であり、サイバーセキュリティを学ぶ学生、エンジニア志望の学生、その他すべての学生をターゲットにした目的設定となっている。

子どもと高齢者

AFA CyberPatriot

「AFA CyberPatriot」は、主にK-12（幼稚園から高校までの児童・学生）に対して、サイバーセキュリティやSTEM分野への進学・就職を推進するために、Air & Space Forces Association（AFA／航空宇宙軍協会）によって作成されたプログラムで、米空軍、米テクノロジー企業「Science Applications International Corporation」（SAIC）と「Center for Infrastructure Assurance and Security」（CIAS／テキサス大学サンアントニオ校インフラストラクチャ保証セキュリティセンター）が共催している。

CyberPatriotには以下6つのプログラムが含まれるが、中心的なプログラムは中高生向けの世界最大のサイバー防衛コンテスト「National Youth Cyber Defense Competition」である。

CyberPatriot プログラム一覧

1. National Youth Cyber Defense Competition（K6-12）
2. AFA CyberCamps（K6-12）
3. Elementary School Cyber Education Initiative（ESCEI）（K-5）
4. Cyber Education Literature Series（K-5）
5. CyberGenerations（高齢者）
6. Tech Caregivers（14歳以上の市民ボランティア）

上記の中の「CyberGenerations」は、高齢者向けのサイバーセーフティイニシアチブで、パスワードの衛生、マルウェアとランサムウェア、マーケティングと詐欺、ソーシャルメディアの認識について高齢者に教えるように設計されている。また、サイバー詐欺の被害者へのリソースも提供している。プログラムは、自分のペースで進められるガイドとして活用することも、グループ単位でワークショップとして実施することも可能。プログラム内容は以下の通りである。

CyberGenerations プログラム概要

- サイバーセキュリティ入門：サイバーセキュリティの重要性を理解し、Webを安全に閲覧し、個人情報を保護する
- パスワード管理：強力なパスワードを作成し、適切なパスワード衛生を維持する
- 一般的なインターネットの脅威：マルウェアとソーシャルエンジニアリングを認識して回避する
- インターネット詐欺：インターネットと電話の詐欺を認識し、身元を保護し、オンラインで安全に買い物をする
- ソーシャルメディアの安全性：ソーシャルメディアのエチケットとプライバシー設定の利用の重要性を理解する

上記の「CyberGenerations」のコンパニオンプログラムとして実施されている「Tech Caregivers」というプログラムは、高齢者に基本的なセキュリティ対策をわかりやすく教えるためのボランティア教師を育成するプログラムだ。14歳以上の学生や社会人のボランティアはオンライントレーニングコースを修了し、試験に合格することで「CyberGenerations」の教師となる資格を取得することができる。プログラムの目的は、高齢者が頻繁に標的となるオンライン詐欺を認識・理解し、安全に回避できるようにすること。トレーニング内容は以下の通り。

トレーニング内容

1. パスワード

2. インターネットにおける脅威
3. 詐欺
4. ソーシャルメディアの安全性と持つべき意識
5. サイバーセキュリティリソース
6. 認定取得 Quiz

Photo by Daniel Reinhardt/picture alliance via Getty Images

日本のサイバーセキュリティ教育に必要なこと

米国の教育事例を調査する中で見えた7つの論点

1. 教育用コンテンツや演習基盤共通化

米国では、教育機関が利用できるコンテンツや演習基盤が充実している。また、これらのコンテンツや演習基盤の中には、教える側の立場である教師向けのトレーニングを含むことも多い。日本においてもさまざまな教育機関が利用できるコンテンツや演習基盤を拡充させていく必要がある。また、その際には、教師向けコンテンツや演習基盤も含めて拡充されることが望ましい。

2. 政府による施策推進

米国では、法律などに基づき政府主導で推進しているセキュリティ施策が数多くある。日本においても「サイバーセキュリティ基本法」に基づいて「サイバーセキュリティ戦略」が定められてはいるものの、サイバーセキュリティ人材の不足解消という観点では、米国の推進力のほうが強い。日本においても政府主導の推進策を活用していく必要がある。

3. 大学認定制度の創設

米国では、サイバーセキュリティ教育を提供している教育機関を認定する制度がある。この認定制度によって、提供されている教育の質を確認できるだけでなく、その大学が地域全体を巻き込んでサイバーセキュリティ教育に対する意識を高めている事例もある。サイバーセキュリティ分野の活動を活発化させるためにもこのような認定制度を活用したい。

4. 日本語による無料教育コンテンツの拡充

米国では、政府提供のものから民間企業提供のものまで、無料及び低価格で利用できるセキュリティ教育コンテンツが充実している。これらの中には日本国内からでも利用可能なものも多いが、英語での提供になっているので、使いこなせないと感じる人も多いと考えられる。日本語の無料教育コンテンツの拡充が望まれる。

5. 政府や企業との連携による助成金と奨学金の提供

米国では、セイバーセキュリティ教育を提供したい教育機関への助成金や、サイバーセキュリティを勉強したい学生向けの奨学金が充実している。日本においても財政面の課題がサイバーセキュリティ人材確保の阻害要因にならないように、助成金や奨学金を拡充させていくことが望まれる。

6. 政府や企業との連携による職業教育制度やインターンシップの提供

米国では、企業において有給で就労しながら、教育機関を利用した教育を受け、資格も取得できる制度（登録研修プログラム）の活用が広く見られる。日本においてもさまざまな人材をサイバーセキュリティ領域に呼び込めるよう、政府や企業が連携し、こうしたプログラムを拡充していくことが望まれる。

7. 多様なバックグラウンドを持つ人材の活用

米国では、サイバーセキュリティ人材として、コンピュータサイエンスバックグラウンドの人材だけでなく、リベラルアーツ人材なども取り込んだ大学のプログラムが開講されている。その他、地政学的観点からサイバーセキュリティ人材教育を行う大学のセンターもある。幅広い視座、バックグラウンドを持つ人材を活用していくことが望まれる。

サイバーセキュリティと民主主義

発行日	2024年4月1日　第1版1刷
企画	国立研究開発法人情報通信研究機構（NICT）／山本龍彦／黒鳥社
制作	黒鳥社
編集	神保勇揮／若林恵（黒鳥社）
デザイン・AD	藤田裕美
校正	校正集団「ハムと斧」
DTP	勝矢国弘
発行	国立研究開発法人情報通信研究機構（NICT）

〒184-8795 東京都小金井市貫井北町4-2-1
代表電話：042-327-7429
https://www.nict.go.jp

Cyber Security

and

Democracy