# 情報未来®

Info-Future®

No. 69 | March 2022

特 集

# 経済安全保障

対談

## 2050年の未来の社会 新しいカタチを考える

NTTデータ経営研究所 創立30周年記念「懸賞エッセイコンテスト」
最優秀賞受賞者インタビュー

NTT DATA
株式会社NTTデータ経営研究所



所属および役職は2022年3月31日現在のものです


# 経済安全保障

## 対談 2050年の未来の社会 新しいカタチを考える 04

**NTTデータ経営研究所 創立30周年記念「懸賞エッセイコンテスト」最優秀賞受賞者インタビュー**

立命館大学　理工学部　機械工学科1年　上西 良彦
NTTデータ経営研究所 代表取締役社長　柳 圭一郎

## 特集レポート

対談

上西 良彦 × 柳 圭一郎
NTTデータ経営研究所 創立30周年記念「懸賞エッセイコンテスト」最優秀賞受賞者インタビュー

# 2050年の未来の社会 新しいカタチを考える

NTTデータ経営研究所は2021年に創立30周年を迎え、それを記念した懸賞エッセイコンテストを行い、最優秀賞には立命館大学1年生 上西良彦さんの「夜明け」が選ばれました。エッセイのテーマである「2050年の未来の社会／新しいカタチ」について、当社の柳社長と上西さんが意見を交換しました。

## 若者を対象に懸賞エッセイコンテストを開催

**柳**　最優秀賞受賞おめでとうございます。

**上西**　ありがとうございます。

**柳**　当社が設立されたのは1991年ですが、まだスマートフォン（スマホ）もSNS（交流サイト）も誕生していませんでした。ドローンやテレビ会議がここまで普及するとは誰も想像していなかったでしょう。

この先の30年についても、大きな変化が起こると思います。私たちだけで想像できるとは思えません。懸賞エッセイコンテストを開催した理由は、これから社会で活躍する若い人たちが、30年後、すなわち2050年の未来の社会をどのようにイメージしているのか知りたいという思いからでした。応募資格を16歳～30歳までとしたのも、その年齢の方なら、30年後にまだ現役で活躍していると考えたからです。上西さんも30年後は50歳でしょうか。まさに会社の中枢で働かれている世代ですね。

**上西**　はい。ちなみに今回、コンテストや公募などの情報が掲載されているサイトで、NTTデータ経営研究所の懸賞エッセイコンテストの告知を知りました。「2050年の未来の社会／新しいカタチ」というエッセイのテーマが面白そうだと感じたのと、文字数が3000字程度と手ごろだったので、夏休みを利用して応募してみようと思いました。1万字だったら長いとやめていたかもしれません。このような公募に応募するのは初めてだったので、まさか受賞できるとは思っていなくて。受賞の通知メールをもらったときには「詐欺メールではないか」と疑ったほどです（笑）。

**柳**　論文ではなくエッセイとしたのは、まさにそこが狙いです。論文と

なると、どうしても、「実際にそれが実現できるかどうか」といった観点が必要で、学術的になってしまいます。それを若い人に求めるのは酷だろうと思って、論文ではなくエッセイにしたのです。上西さんの作品を拝見した第一印象は、文章が上手だということ。日ごろから何か創作活動をしているのですか。

**上西**　実はまったくしていません。読書も、小説より新書などのノンフィクションのほうが好きな位です。ただ、子どものころから、漫画はよく読んでいました。特に、手塚治虫さんの作品は好きです。僕は兵庫県川西市の出身なのですが、手塚さんは隣の宝塚市で5才から24歳まで約20年間を過ごし、市内には手塚治虫記念館もあります。僕もよく行きました。そのため、今回の作品も、手塚作品にインスピレーションを受けたのだと思います。

**柳**　なるほど、上西さんの作品は読んでいて未来の情景が目に浮かんできましたが、手塚さんの影響があるのかもしれませんね。上西さんの作品は、さまざまな題材を多様に表現しているのもいいですね。いろいろなことが、こんなふうに変わっていると表現しているのが楽しいなと思いました。

**上西**　ありがとうございます。僕自身も読んで面白い作品にしたいと思って、実現の可能性の有無よりも、夢のある話、こうあってほしいという願望がかなうような話にしたいと考えて書きました。そのため、想像上のフィクションの話であっても、リアルに感じられるように細かく描写をしました。そこは僕も力を入れたところで、評価していただいてうれしく思います。

## 技術の進歩には、夢もある反面、リスクもある

**柳**　私も作品の審査に参加しましたが、読ませていただいて印象深かったのは、学生の皆さんからの応募に「記憶」をテーマにした作品が多かったことです。試験に苦労しているせいかもしれませんが、記憶を脳の外に出して保管したり、それを自由に取り出して使えるようにしたりといった描写をいくつか見かけました。学生時代には、確かに暗記しなければいけないことも多いです。「こんなことをやる必要はあるのか?」という思いがどこかにあるのだと思います。そのため、記憶をどこかに保存しておいて、必要なときに取り出せばいいじゃないかという感覚の人が多かったですね。

**上西**　僕は理工学部の機械工学科ですが、大学入試センター試験（現・大学入学共通テスト）で地理・歴史が必須科目でした。グローバルな舞台でビジネスをしたり、社会情勢を知ったりするためには世界史や日本史、地理などの知識は、ないよりはあったほうがいいと思います。ただ、古典の単語については、果たして本当に覚えないといけないのか、社会に出てから役に立つのだろうかという疑問はありました。

**柳**　「歴史は繰り返す」とも言いますが、実社会では、歴史などの教養が、ビジネスにヒントを与えてくれることがよくあります。ただし、社会人になると、すべてが頭の中になければならないというわけではないですよね。検索すればすむこともたくさんあります。そこでの問題は、どのように検索すればいいのかということです。正確でなくても頭の片隅に学習したことの記憶が残っていれば、それをキーにしてなんらかの方法で検索して情報を取り出すことができるのですけれど、まったくないと難しいですよね。技術論から言えば、人間のさまざまな臓器の中で、もっとも再生医療が難しいと言われているのが脳なのです。脳と同じものを作るだけなら、いろいろなiPS細部などを使ってやればできるようになるかもしれませんが、脳の中に入っている記憶を移植することは、非常に難しいですね。恐らく、将来的にはさまざまな臓器が再生できるようになるでしょう。脳以外の臓器は、新品になっても困り


**柳 圭一郎**

YANAGI KEIICHIRO

NTTデータ経営研究所 代表取締役社長

1960年福岡県生まれ

1984年東京大学法学部卒業、同年日本電信電話公社入社。2006年10月 株式会社NTTデータ 金融ビジネス事業本部　資金証券ビジネスユニット長。2009年NTTデータ・ジェトロニクス株式会社 代表取締役社長就任。2013年 株式会社NTTデータ 執行役員　第二金融事業本部長。2016年 同取締役常務執行役員 総務部長 兼 人事部長。2018年　同代表取締役副社長執行役員。2020年6月 同顧問およびNTTデータ経営研究所 代表取締役社長に就任。


ません。むしろ、新品のほうが、性能がよくなります。ですから、脳の中の情報を取り出したり、戻したりすることが本当にできるようになれば、それが人類の最後の究極の姿だと思います。極端なことを言えば、永遠に生き続けることだってできるかもしれませんね。

**上西**　欧州で、脳の記憶回路をコンピュータに置き換える実験が行われたと聞いたことがあります。脳細胞は電気信号を発して情報をやりとりしています。コンピュータも0と1の世界ですから、原理としては同じです。今どこまで研究が進んでいるかはわからないのですが…。

**柳**　実は当社にも、脳科学・ニューロテクノロジー分野のコンサルティングに特化したチームがあり、すでに10年以上の実績があります。どこまでできるのかといった議論は、私たちもよく行っています。次第に脳のこともわかってきており、今の技術レベルでは、脳の状態を観察すれば、日本語で換算すると1万語ぐらいなら、「この人はこんなことを考えている」というのがわかるレベルには達しているそうです。

**上西**　それはすごいですね。ひと昔前なら魔法みたいな世界です。技術はそんなに進んでいるのですね。

**柳**　ただし、怖い面もあります。脳の状態を観察するということは、言い換えれば、他人の頭の中を覗けるということです。今、この人が気持ちいいと感じているのか、痛いと感じているのか。無意識のことまでわかります。おいしくないものを食べておいしいとお世辞を言っても、嘘だということが全部わかってしまうのです。

**上西**　僕が心配しているのはそこです。例えば専制的な国家が、国民を監視するためにそのような技術を使うようになってしまうのは好ましくありません。

**柳**　技術が進歩することによって、いいこともたくさんありますが、私たちのように技術を扱うものとしては、それをどのように社会に適応していくかということについて慎重に考えなければなりません。ただし、逆に、これは危ないから止めようと言っていると、技術は進歩しません。中国のようにそういったことを気にしないでやる国がどんどん先に行ってしまう可能性もあるので、私たちもそれに負けないように、リスクに配慮しながら、いろいろなことを進めていかざるを得ないとは思います。

**上西**　人間の欲望は尽きないですから、もっと速いもの、もっと便利なものと、技術はどんどん進化していくと思うので、技術が暴走しないようにするためには、アクセルだけでなくブレーキも必要だと思います。

**柳**　AI（人工知能）の使い方なども、きちんと意識しておかないと、間違った方向に行ってしまう恐れがありますよね。例えば、企業が新卒の学生を採用する際、とある年に「親の年収の高い学生のほうが優秀だ」という相関関係がたまたま分析結果として出たとします。それをもって「わが社は親の年収が高い人だけ採用します」というのは違和感があります。これは極端な例ですが、AIを使えばそのような分析結果も出てしまうのです。使い方を誤ると、非常に不平等な世界になっていきます。日本人はそのような統計などの数字の感覚が鈍い人が多くて、むしろ「AIがそう言うならばOK」と社内の説得材料に使われることがあります。しかし、そのような風潮になるのは怖いことです。

**上西**　コンピュータだからミスはないという先入観を持っていると、そういうことになるのでしょうね。

**柳**　コンピュータも所詮は人間が作ったものですから、ミスはありえるという前提でいろいろなことに取り組んだほうがいいと思います。

## さまざまな社会課題を解決するためにも技術が必要

**柳**　ちなみに今回、上西さんが書かれたエッセイの中で、この技術はぜひ

実現してほしいと考えたのはどれですか。もちろん、実現可能性が高いものとまだ難しいものとがあるでしょうが。

**上西**　冒頭に書いた、指輪型で心拍数や消費カロリーが計測できる機器などは、近い機能のものがすでに開発・販売されていますね。

**柳**　私も今、スマートウォッチを使っています。心拍数のほか、血中酸素飽和濃度、睡眠の深さなども測ることができるので、日常生活で活用しています。ストレス状態までわかります。使ってみると、自分の健康管理に気を遣うようになりますね。深い睡眠が意外と確保できないということもわかりました。お酒を飲むと心拍数が上がるということもわかり、注意するようになりました。

**上西**　僕が書いたものでは、2050年以前に実現しそうな技術もありますし、2050年でも難しそうな技術もあります。例えば、IoB（Internet of Bodies／ヒトのインターネット）分野では、仮想現実（VR）や拡張現実（AR）を体験できるウエアラブル機器はすでに開発されています。さらに、デバイスを体内に埋め込む機器も実現しています。脳に直接接続するIoB機器も研究が進んでいます。エッセイでは、脳内に直接接続して、念じるだけで情報のやりとりができる機器を登場させてみました。2050年でも実現が難しそうなのが、量子テレポーテーションです。ECサイトで注文すると、瞬時に商品が届くといった、まさにSFのような世界ですが、実現までにはまだ時間がかかりそうです。個人的に、あると楽しいと思うのは、調理をしてくれるロボットシェフですね。一人一人の健康や栄養バランスを考えながら、最適なおいしい料理を作ってくれるというものです。日本ではまだ、女性の家事負担が多いですが、それを軽減するものにもなると思います。

**柳**　私が上西さんのエッセイの中で実現してほしいと思ったのは、まず自動運転ですね。私は車の運転が好きなのですが、高齢になればいつかは運転免許証を返納しなければならなくなります。東京に住んでいると車がなくてもそんなに困りませんが、地方に行くと移動手段がなくなってしまいます。上西さんのエッセイに描かれていたような、自動運転車やドローンタクシーなどが気軽に利用できる仕組みがあるといいですね。もう一つ実現してほしいのは、やはりエネルギー問題の解決につながる技術です。カーボンニュートラルは喫緊の問題ですので、上西さんが示した核融合発電が可能かどうかはさておき、何らかの取り組みが不可欠です。政府は2030年までに、温室効果ガスを13年比で46％削減を目指し50％削減の高みに向け努力する方針を示しています。2030年なんて、すぐそこですよね。当社もエネルギー問題についてはかなり力を入れて、いろいろな取り組みを行っていますが、本当に何とかしなければなりません。例えば日本企業がたくさん$CO_2$を出しながら製品を作っていると言われれば、製品そのものが世界的に売れなくなってしまうことになりかねません。ただ、日本の消費者はそこまで考えてエネルギーを使ったり製品を買ったりしていませんので、消費者の意識も変えていく必要があります。

**上西**　よく日本の食料自給率の問題が議論されますが、同様に、エネルギーについても自給率を高める必要があると思います。EV（電気自動車）を普及させるためには電力が必要だということにも視点を向けるべきだと思います。

**柳**　欧州で地政学的なリスクも高まっていますが、これにはエネルギー問題がかなり関係していると見られています。今や、エネルギーが国家の安全保障に密接に結びついていますので、課題の解決のためにも技術が必要になるでしょう。

## メタバースはビジネスチャンスになり得るか

**上西**　先ほど柳社長から、人間の臓器を新しいものに再生し、さらに脳そのものも再生できる時代が来るという話がありました。そうすると人間の定義とは何なのかということになると思います。肉体を持つことでもなければ脳を持つことでもない。魂や意思だけになってしまうかもしれません。僕は、それはちょっと違うのではないかと思っています。現実世界で友人と会っておいしいものを食べることも大切だと思いますし、味覚や触覚などがVRやARで伝わるのだろうか？という疑問もあります。

**柳**　こういったことは徐々に近づいていくと思います。例えば、おいしそうなにおいがすると感じるのは脳のどの部分なのか、風が心地いいと感じるのは、皮膚の神経をどう刺激したからなのか。これらを分析し、再現することによって、バーチャルであっても同じ感覚を得られるようになるかもしれません。もちろん現実と全く同じになるとは思いませんが、視覚や聴覚だけではなく、さまざまな感覚について研究が進んでいます。今後ＶＲの技術が進んでいくことは確かでしょう。

**上西**　最近、メタバース（仮想空間）が注目されています。ビジネスそのものもメタバースの中で行われるようになるとも言われます。ただ、僕自身は機械工学の専攻ということもあって、どうしても現物のモノを作りたいという思いがあります。バーチャルなものは実体がないように感じるからです。その一方で、大学の授業もコロナ禍のため、テレビ会議システムで行われるようになっていて、オンラインが当たり前になっています。リアルなキャンパスに行く必要性も少なくなっています。

**柳**　当社でもでもコロナ以降、コンサルタントの約７割が在宅勤務になり、それが当たり前になっています。新しい技術や様式はあっという間にスタンダードになります。私が就職したころはスマホもなく、インターネットもありませんでした。しかし今では、これらなしにビジネスや生活はできません。メタバースについても、何かのきっかけで一気に利用が広がる可能性がありますね。ただし、現状はまだ世代間によって受け止め方が異なるでしょう。先ほど上西さんから、目の前にある現物でないと実感がわかないという話もありましたが、私たちの世代も、バーチャルな世界で洋服を買ったり絵を買ったりするために多額のお金を払うといった感覚が理解できる人はまだ少ないです。例えば若い人の中には、戦闘ゲームで強くなるための強力な武器を購入するだけでなく、戦闘用に気に入った服を購入する人も少なからずいると聞きます。このあたりは、生まれたときからネットが身近にあったデジタルネーティブとシニア世代とでは感覚がだいぶ違うと思います。

**上西**　メタバースをビジネスに活用するのは時期尚早という感じでしょうか。

**柳**　特定の分野に関してはニーズがあると思います。例えば観光旅行です。コロナ禍でなかなか旅行に行けないという状況ではありますが、仮にコロナが収束したとしても、雲海を空から見るといったことはなかなかできないでしょう。メタバースの世界であれば、ドローンで撮影した映像などを活用して普段なかなか見られないような光景を見ることもできます。世界の秘境を巡るといった体験もできるでしょう。ここで大事なのは、メタバースの世界は決して現実のリアルな世界の代替ではないことです。観光旅行であっても、これまでにない新しい価値観からスタートしていくのではないかと思います。このほか、教育や医療などの分野でも新しいメタバースを利用した新しいサービスが創出できそうです。

**上西**　現実とは違う世界ということですね。まさにメタ（超越した）バース（宇宙）ですね。

**柳**　テレワークがいい例だと思います。恐らく、リアルな世界しか信じない人にとっては、テレワークが行われているという現象をいまだに理解できないでしょう。なお、テレワークはリアルの世界を代替することはできません。いくら画質を高めても、回線の速度を上げても、対面で会話しているのと同じにはなりません。それでも、テレワークにはリアルとは異なるさまざまなメリットがあります。新しい技術とはそういうものだと私は思います。メタバースもきっと、新しい技術として成長していくでしょう。

**上西**　市場の拡大にともなって、関連する法律なども整備されていくのでしょうか。２０１８年に米国で公開された映画に「レディ・プレイヤー１」という作品があります。監督はスティーヴン・スピルバーグです。近未来では世界が荒廃し、人類はＶＲ世界に逃避しているのですが、ＶＲの世界では人はアバターに姿を変えるので、本当はそれが誰なのかはわかりません。それはそれで課題もあると思います。ＶＲの世界で買ったブランド品のバッグは本物なのかという問題もあります。

**柳**　ＮＦＴ（非代替性トークン）などを活用した信ぴょう性の保証などのニーズも高まってくるでしょう。当社自身が洋服や絵を売ったりすること

は今のところ考えていませんが、NFTを利用できるプラットフォームの構築やメタバース内でのコンテンツ制作支援といった仕事は今後出てくるかもしれませんね。さらには、メタバース内でのビジネスをどう創出するかといったコンサルティングなども私たちの仕事になるかもしれません。

## 若い人たちには、好きなことを見つけて追及してほしい

**上西**　メタバースだけでなく、今後はますますデータが大事になると思います。私はエッセイの結びに、2050年の未来の社会では「データが湧く場所が大事である。石油の一滴は血の一滴から1ギガが血の一滴になった。」と書きました。「石油の一滴は血の一滴」は第一次世界大戦中にフランスのクレマンソー首相が言った言葉だそうです。これからは、データを持っている者が強く、持たざる者が弱いという時代になっていくように思います。先ほど柳さんが中国の話をされましたが、中国なら個人情報保護などを考慮せずに自由に国民の行動データなどを入手できます。そうすると自動運転車やAIの開発でも、日本は遅れを取ってしまうように思います。

**柳**　データの重要性が増してくるのはその通りですが、最近ではGAFA（グーグル、アップル、旧フェイスブック〈現・メタ〉、アップル）など、データを独占しようとする企業に対する風当たりが強くなっています。私は、この傾向は正しいと思っています。というのも、データが他の資産と異なるのは、共有しても減らないことです。非常に面白い資産なのです。石油なら取り合いになりますが、データはお互いに見せ合って、一緒に利用できます。これからはこの「データの民主化」を進めていくべきだと思います。データを利用するけれど、お互いでうまく融通し、共有し合いながら、次の世界の製品なりを作っていくという方向に行くべきです。もちろんこれは1社だけではできません。データの所有権は各社がしっかり持ちながら、クラウドなどで情報を共有し、やり取りする仕組みを作っていく。一社独占型のGAFAでなくてもできることがたくさんあると思います。その価値に、日本の企業は気付いてほしいですね。

**上西**　僕は、GAFAのような企業がもっと日本で生まれてもいいのではないかと思っています。ご指摘のように、いろいろと問題もあるけれども、彼らはこれまでになかった新しいことに挑戦していますよね。そのような企業がたくさん出てくれば、新しい風も吹くし、若者の雇用にも貢献すると思います。ただ、僕自身としてはやはり、ハード寄りのモノづくりがやりたいのですが。

**柳**　ハードとソフトの組み合わせは日本企業も強みを発揮できると思います。例えば災害救助の現場で活躍する口ボットです。今でも、報道などを見ると、災害の現場では人や犬が自らを危険にさらしながら活動しています。そこでAIを搭載した口ボットがあれば、危険な現場でも迅速に救助作業が行えると思います。人手不足が課題となっている介護・福祉の現場なども同様ですね。政府もこのような分野にもっと投資をしてもいいのではないでしょうか。今回、懸賞エッセイコンテストを実施し、応募作品を読ませていただいて、若い人たちの発想力に感心しました。これからを担う日本の若者に大いに期待しています。当社の社員にもよく、好きなことを見つけて追及してほしいと言っています。残念ながら日本ではまだ、大きい組織で上の指示に従っていればなんとかなると思っている人も少なくありません。2050年に活躍する方たちにはぜひ、目的意識、そして夢を持って、挑戦してほしいですね。上西さんも夢の実現に向け、頑張ってください。

**上西**　はい。ありがとうございます。

**上西 良彦**
UENISHI YOSHIHIKO
立命館大学　理工学部　機械工学科1年

※対談は十分な距離を保ち、パーテーション設営など新型コロナ対策を徹底した上でマスク着用にて実施しました。

# 夜明け

最優秀賞受賞作品

立命館大学　理工学部　機械工学科1年　上西 良彦

私のいる時代は、２０３５年７月６日金曜日の朝８時57分。竜の巣のような積乱雲が夏空に上り、只今、焦げ茶色の丸テーブルで憂鬱な朝食中である。料理は、母が作るのではなく、ましてやインスタントラーメンしかできない料理下手な自分が作るのでもない。この時代では、調理マシーンによって作られる。これは冷蔵庫ぐらいの大きさで、私たちが個々にはめている指輪型の計測器から睡眠、栄養状態、心拍数、消費カロリーのデータを元に全自動で作ってくれる。まさに専属シェフである。もちろん個人の好みに合わせて作られる。今朝の朝飯は、私好みのミディアムレアなスクランブルエッグと葡萄パン。サラダは、家の下の農場で作られた新鮮な採れたて野菜。野菜はＬＥＤ照明によって味が変化し、好みに合わせて調合してくれる。私は少し苦みのある瑞々しい野菜が好みだ。中指に装着している指輪型計測器で健康状態を把握するため、病気の早期発見はもちろん、事前予測までも可能。健康データは国が一括管理し、医療保険の大きな削減に貢献した。87歳の祖母もこのシステムにより心筋梗塞の予兆を事前にキャッチし、助かった。今でも健康で趣味の卓球を楽しんでいる。

この時代では、スマホなんてもう博物館か家の押し入れの中にしかない。親父はスマホを記念として仕事部屋の机の左の引き出しにしまっている。今では、脳内に直接接続されているＩｏＢ機器とＡＲを利用したメガネ型デバイスにより通話、ラインのやり取り、検索、課題の作成などが頭の中で思えばできる。「念じたらできる」に近いかもしれない。ＩｏＢとデバイスの両方があるのは、人体に埋め込むことに抵抗がある人がいるからだ。ＩｏＢ機器はサイボーグの入り口かもしれない。ＩｏＢ機器とメガネ型デバイスは自宅の量子コンピュータに接続されていて、「現代」でいうところのクラウド技術が応用されている。私のメガネ型デバイスは13ｇ程。ジョン・レノンの様な丸型眼鏡だ。念じたらメッセージが送れて便利だが、意図もしない内容が送信されることがあるのが難点。そんなことは「現代」でもよくある。例えば、誤送信が恋に発展すればいいが友人関係の亀裂に発展するかもしれない。私は未経験者だが、妹はひどい目にあったようだ。ニューロテクノロジーでは直接脳内埋込み型なので動画を見るときも脳が直に見ているため没入感が映画館と比べ物にならない。そのため、動画中毒が流行病の一つとなっている。

11時３分、私はネットショッピング中。朝から一歩も家から出ておらず、一見すれば椅子に座りながら二度寝しているようにみえる。しかし、私は脳内に送られてくる映像でショッピングモールを飛び回っている。鉄腕アトムのようにではなく、浮遊感のある宇宙ステーション内での無重力状態の移動と同じように。モールは非常に広く、歩いていたらきりがない。ショップ内は多くの人で溢れており、その視点において現代と全く変わらない。もちろん友達ともすれ違うこともある。今日は途中から友達と８階の広場で待ち合わせてして一緒に買い物。ショッピング中、物を持てば重さ、質感、光沢、肌触りなどが実感できる。脳内のチップが神経に電子信号を送るからだ。そのため、感覚は全く変わらない。現代の買い物と何ら変わらないが、買い物の場所が私たちの時代では、仮想空間内であるのだ。最近のトレンドは切手収集。「趣味の王様」が80年ぶりに流行っている。人気切手は、見返り美人図や１９６４年の東京オリンピック切手。様々なものがあるがもちろん値段はピンキリだ。

ショッピングが終わりソファから起きれば自宅にある半径１ｍ程の金属の球体の前から買った品物が出てくる。この球体は、アマゾンが開発した量子テレポーテーション技術を利用した配送機械である。工業製品であれば配達が可能だ。もちろん送られてきた品物はオリジナルであり、唯一無二の存在。

14時21分。大学の授業へ。自宅は兵庫県の神戸市。大学は京都市。授業開始は14時50分から。絶対間に合わない――「現代」の常識でなら。ただ私のいる時代なら間に合う。ショッピング中にドローンタクシーを予約した。ただ

し、予約したのは私ではない。ＡＩコンシェルジュである。ＡＩコンシェルジュだが、個々の性格が違い、まさに人格が備わっているので喜怒哀楽があり、家族という関係性に近く何でも相談できる親友である。ただ地域によってはＡＩやロボットに対する差別意識が高いところもあり、この時代では、人種差別より人間とＡＩの共存が大きなテーマとなっている。本筋に戻して、自宅の屋上に行けばタクシーが到着している。用事を忘れグセな私としてありがたいがＡＩコンシェルジュのウィンストンに叱られた。ウィンストンは私のＡＩコンシェルジュの名前。人格もあれば名前もある。少し内向きでふてくされている私は機内へ駆け足で乗り込む。14時35分から雷雨予報だけど操縦は大丈夫なのか。もちろんオートパイロットなので誰でも安心。赤ん坊でも乗れる。安全性は新幹線と同じである。つまり通常の事故はゼロ。飛行機自体の安全性が高いだけでなく、天気予報が三次元的に予測できるため、気流が荒い所や不安定な場所を避ければいいのだ。また全自動運転のため、機内にはハンドルがない。簡易的なリムジンに近い内装で、席は向かい合わせである。機内は、適湿適温。というよりは、個人個人お好みに合う設定がされている。音楽は私の大好きなビートルズの「a hard day's night」が流れている。気分を晴れやかにとコンシェルジュが気を利かしてくれたようだ。タクシーは、家の屋上から離陸し、航空道路を通行する。ただここでは、現代のような渋滞が存在しない。それどころか「渋滞」は死語となっている。なぜならビックデータとＡＩコンシェルジュからのデータにより人の行動が予測されているからである。飛行中下を見れば大きな球体の建物が。これは、水素を用いた核融合発電所。低レベル放射性廃棄物が発生するが、世界的流れであった二酸化炭素を出さない。生活ばかりでなく社会を維持するのに必要な電力が増え続いた結果、再生可能エネルギーのみで安定的かつ大量に電力を供給できなくなり、今では核融合発電が普及している。やはり安価で大容量の発電可能なところが魅力であったのだろう。日本では、２０１１年の福島第一原子力発電所の事故を期に原発が減ったが２０４０年代頃から核融合発電所が総電力中の割合を増やし続けている。

16時20分。授業が終わりここからは、友達との雑談。議題はもちろん夏休みの旅行についてだが、行先は火星。最近流行りの旅行先である。現代では非常に時間がかかるが、未来のロケットは、オリオンロケット。原理自体は、１９５０年代にできている。核パルス推進ロケットなので速度は一般的な化学や水素ロケットと比べものにならない。同時に大量輸送も可能になり、料金が大規模に下がっている。感覚的に現代の海外旅行みたいなもの。１９６０年代に大型ジェット機の登場により航空運賃が下がったのと同じ現象が、90年ぶりに起こっているのだ。

8月23日。待ちに待った夏休みの大イベント、惑星間旅行の日だ。宇宙エレベーターの発射時刻は午後18時30分。種子島の透明で淡い海を背景にエレベーターを見た瞬間、私ばかりでなく友達もミライを感じる。まさに宇宙への玄関口である。エレベーター自体は、地上から見上げれば雲より高くそびえ、高く黒い極細のビルが数本立っているように見える。連絡船は前後が半球で、円柱の丸い窓がついた高層ビル。種子島にある宇宙エレベーター地上基地から高度５７０００ｋｍにある火星連絡ゲートまで行く。私の時代では、地球を抜けるのに宇宙エレベーターを利用。電磁カタパルトで加速し、連絡ゲートへ舞い上がる。打ち上げロケットでは、地球の重力圏を抜けるのに水素燃料を大量消費するのでその分旅行代が高くなるが、エレベーターを使えば安く済む。連絡船内はロケットのように締め付けられた古典的な席に加え強烈なＧに耐え座るのではなく、旅客機の席に座るようなものだ。ただシートベルトは無重力状態に備えて装着する。また、地上でマジックテープシューズを購入する。もちろん無重力になれば通路を歩くのも苦になるからだ。エレベーターが上がっていくにつれ、カプセルから見える地球は非常に美しく生命感で溢れている。万里の長城も微かながら確認できる。地球の背景には漆黒の世界が、光が永遠に反射できないほど続いている。夜なので都市部の灯りが眩しく優しく輝いている。ただ、場所によっては、暗い部分もぽつりぽつりある。これは、データを支配した国もしくは企業や個人が富を得ることができ、データを得られなければ底なしの貧困へ溺れてしまうからだ。地球上の光の明暗は、格差の明暗。20世紀は、石油を制するものが世界を制したが、21世紀は、データを支配する者が世界を制する。現代は石油が湧く場所が重要だが、私たちの時代は、データが湧く場所が大事である。石油の一滴は血の一滴から1ギガが血の一滴になったのだ。


参考文献

「宇宙はどこまでいけるか」 中公親書　小泉宏之

「AIの壁」 PHP新書　養老孟司

「ハイブリット戦争」 講談社　廣瀬陽子

「イーロンマスク次の標的」 祥伝社　浜田和幸

「2030年すべてが加速する世界に備えよ」
ニューズピックス ピーターディアマンディス／ スティーブンコトラー

「2025年を制する企業」 SBクリエイティブ　山本康生

Webサイト

「宇宙エレベーター建設構想」：季刊大林
https://www.obayashi.co.jp/kikan_obayashi/detail/kikan_53_idea.html

「オリオン計画」
https://ja.wikipedia.org/wiki/%E3%82%AA%E3%83%AA%E3%82%AA%E3%83%B3%E8%A8%88%E7%94%BB

今回の「情報未来」は「経済安全保障」がメインテーマだ。少し前までは、前回取り上げた「グリーン」に比べると、今一つ盛り上がっていないように感じていたが、ここ数日で、読者の皆さんの認識も相当変わったのではないかと思う※。

「経済安全保障」は、特定の国との関係の悪化に備えた特定の業種の問題と誤解されやすいが、ロシアのウクライナ侵攻を受け、ロシアとの関係が悪くない国も、取引を停止せざるを得ない状況になってきている。ドイツのように天然ガスの約50％をロシアから輸入している国ですら、協調のため取引を断念せざるを得ない状況には愕然とするしかない。

経済安全保障には大きく区分して二つの側面がある。一点目は、グローバルな視点でのサプライチェーン全体の問題である。

ウクライナ侵攻により、全世界的に天然ガスや小麦が不足することが懸念されるが、この2年間も、全世界で一斉かつ急速にCOVID-19が拡大したことにより、今まで考えられなかったような問題が多く発生した。もう記憶の彼方にあるものもあるが、最初はマスク、防護服が不足し、そしてワクチン、注射器、最近では治療薬、検査キットなどの不足がクローズアップされた。さらには外国での都市封鎖による工場の不稼働、コンテナ流通停止による輸入の遅れなどの影響もあった。また必ずしもコロナ禍だけの影響ではないが、半導体の不足は多くの産業に多大な影響を与えている。もはやコメと石油さえ自給（もしくは備蓄）をしていれば安全が確保されるという時代ではないことは明確である。

企業は自らの一次調達先（仕入先）のことはよく解っていても、二次調達先やその先は解りにくい。企業にとっての調達先は、その企業のノウハウの一つであり、開示に対する抵抗感が強いであろう。しかしながら、サプライチェーン全体でどのようなリスクがあるのかを把握するためには、その可視化は極めて重要である。

なお、経済安全保障の戦略的自立性確保の重点分野としては国民生活に与える影響の大きい、エネルギー、情報通信、交通・運輸、医療、金融の5分野が定められている。特にこれらの分野の企業は自らのサプライチェーンの中で、経済安全保障観点での調達先選定ウェイトが飛躍的に高まる可能性が高い。一般的に、物品やサービスの調達先の選定は、価格、品質、納期が重視されてきた。これに加え、$CO_2$の排出量、そして経済安全保障上の観点が追加されると想定できる。その結果として、右記5分野以外を含む多くの産業に影響を与えることとなるだろう。

経済安全保障が大事だとしても、企業は全てのリスクに対処することはできない。多くのリスクに対処すれば、コストが大幅にアップし、たちまち競争力を失ってしまう。ただ、ある程度のことを事前に想定しているか否かによって、いざという時の対処スピードが全く異なってくる。今やサプライチェーンは全世界的である。何かが不足する時は全世界で不足が発生する。早いタイミングでそれに対処できるか否かは、その後の経済活動に大きな差異を生む。従来は在庫圧縮、資本効率アップが良い経営だと言われていたが、今はコストは意識しつつも、リスクヘッジを意識した経営が求められている。リスク対策は直接には収益を産みにくいので、経営者にとっては悩ましく、決断には勇気が必要だ。

ちなみに、サプライチェーンと言うと購買や生産に意識が

# 「経済安全保障」問題

※2月28日現在

向かいがちだが、実は物流・販売・マーケティングやこれらを支える間接部門機能（人事やIT管理機能など）に対する経済安全保障も重要である。そういう意味ではサプライチェーンというより、バリューチェーン全体と言った方が良いのかもしれない。

経済安全保障から少し離れるが、調達先の綿花が強制労働で作られた可能性があれば非難され、開発した製品が（特に人権侵害や武力侵害目的などの）武器の部品に使用されていれば非難される。自社の仕入れ側、販売側双方に対する意識は、ますます重要となっている。

柳 圭一郎
YANAGI KEIICHIRO
NTTデータ経営研究所
代表取締役社長

## リスクが急拡大している

二点目の側面は「情報の保護」の観点である。ここでいう「情報」には、先進的重要技術に関する情報、知的財産、ビッグデータなどを含む。

ウクライナ問題では、サイバー攻撃、ハイブリッド戦などの脅威などが話題となっている。SNSで多くのフェイクニュースが拡散されており、アメリカ大統領選で見られた「分断」がロシア同盟国とそれ以外で起こっていることにも注目が集まっている。極論すれば、東西冷戦の時代はイデオロギーの違いが対立を生んでいたが、今は情報に関する国家戦略が対立の根本原因と言えるかもしれない。

なお、トンガの火山噴火では海底ケーブルの切断等が、通信インフラに重要な影響を与えることが明確となった。30年前に比べて、情報の価値は飛躍的に高まった。企業などの中で、情報（システム）が使用される局面が限定的だった30年前に比べ、今は情報インフラが使用不能になれば影響は大きい。また、AIなどによる自動化が進むにつれて、不正な情報が意図的に混入されてしまうと、そもそも満足な経済活動ができなくなってしまうし、偽情報による世論操作などにより、結果的に自国の安全が脅かされる可能性もある。

例えば製造業におけるノウハウは、昔は属人的で、すり合わせ技術が重視された。そこでは製品を分解して調べたとしても、すぐに同じ製品を作れるわけではなかった。ノウハウのデータ化、ネットワーク化、可視化が進んだ結果、今はノウハウに対するアクセス性が改善した一方、情報漏洩のリスクも高まっているし、情報が漏洩すればライバル企業は簡単に製品をコピー・製造することができる。終身雇用を原則としている文化的影響や日本語というバリアへの安心感もあるかもしれないが、日本企業は情報漏洩に関する感度が諸外国に比べて低いと感じる。経済安全保障はリスク管理であり、それ自体は利益を生みにくいため経営者にとって悩ましい。しかし、そのリスクはこの数年で著しく拡大していることは疑う余地はない。もはや特定5分野の企業だけにリスクがあるという状況ではない。

本号で紹介できるテーマは以上のうちほんの一部であるが、読者の皆様の何らかのお役に立てれば幸いである。


# リアルデータで経済を強化

NTTデータ経営研究所
デジタルイノベーションコンサルティングユニット
ユニット長／パートナー
**木村 俊一**
KIMURA SHUNICHI

## リアルデータと経済安全保障

経済安全保障の観点から我が国は、国際社会におけるプレゼンスを今まで以上に経済的に強化していく必要があり、そのため競争力の強化は必須である。今後の競争力強化に、いわゆるデジタルトランスフォーメーションの推進は欠かせないが、その際、コアとなるのがデータであり、データが新たな付加価値の源泉となるといわれている。

データは、それ単独では意味をなさないが、上手く活用することで、新たなビジネスモデルの創出や、オペレーションの高度化、効率化に寄与する。自国のデータに関して、セキュリティを確立し、しっかりと守るという観点も重要であるが、単にデータを守るだけでなく、他国に先んじてデータ活用を推進することで、高度なＡＩ等の技術を活用し、国の競争優位を確立することができる。

データに関する一つの分類として、「バーチャルデータ」と「リアルデータ」という分類がある。バーチャルデータは、ＷｅｂのログデータやＳＮＳなどのデータなど、デジタルサービスに付随してデジタル空間上の事象で発生したデータである。従来、ビッグデータといえば、バーチャルデータを指すことが多かった。ＧＡＦＡなど、世界レベルでサービスを展開する巨大プラットフォーマーによるデータの独占問題が紙上を賑わすケースも、このバーチャルデータに関するものであった。

一方で、リアルデータとは、工場や製品の稼働状況、移動データ、生体データなど、個人・企業の実世界（リアルの空間）での活動に伴い生成されたデータを指す。本格的な取得や蓄積が進めば、データ量はバーチャルデータよりも圧倒

外資系コンサルティングファーム、国内大手シンクタンクなどを経て現職。専門は新規事業企画、マーケティング、CRM、営業改革など。現在は民間企業に対する幅広い領域のコンサルティングや、官公庁の調査プロジェクトに従事する。

的に多くなることが予想される。

今後、第４次産業革命を通じて産業を高度化し、国際競争力を高めていくためには、これらリアルデータの活用が極めて重要になる。

現在、リアルデータの活用については様々な取り組みが推進されており、次第に効果が見えてきている。工場などにおいては、稼働中設備の様々な状況をセンサーで把握・蓄積し、事前に故障を予測することで、生産ラインのダウンタイムを減少差せるといったスマートフォクトリーといわれる取り組みが推進されている。さらに、様々なリアルデータを駆使して構築したＡＩなどが実現する自動運転など、これまで、人間のみが実現してきたことの一部代行は、我々の日常生活にも大きなインパクトを与えるだろう。

## 広がるリアルデータの世界

少子高齢化が進み、生産人口の減少が危惧される我が国では、今後、様々な領域で今まで以上の機械化や省人化が進むことが予想される。その結果、取得および蓄積可能なリアルデータは、更に拡大することが予想される。これまでセンサーを活用したデータ収集といえば、工場の生産ラインなどが思い浮かんでいたと思うが、これからは、流通小売や物流の現場や、農林水産業などにおいても、多くのリアルデータが生成され、活用されていくことになる。

例えば、流通小売の場合、自動倉庫の導入や、無人店舗の試行が推進されている。世界最大のｅ-コマース企業であるアマゾンは、搬送ロボットメーカーを買収し、倉庫にて無人の自動搬送ロボット（Automatic Guided Vehicle，以下、ＡＧＶ）の活用を推進している。同社の倉庫では、商品の搬送やカートの棚への移動など、目的に応じた複数種のロボットが運用されている。但し、目的の商品を探し出してピックアップするという作業は、多くの場合、まだロボットには難しく、人間との役割分担が重要になっているという。これらの仕組みの中で、様々なリアルデータが新たに蓄積されており、ＡＧＶの高度化やオペレーションの効率化に活用されている。

無人店舗については、中国で一時期かなりの盛り上がりを見せたが、現在は落ち着いているという。これから日本で展開が進みそうな「無人店舗」は、決して無人ではない。バックヤードの管理や、品出しなど、人間の作業が望ましい作業も多いし、踏み込み型の店舗であれば、人がいなくては販売できない商品（アルコール類、タバコなど）を販売するためにも、店員は必要である。ただ、従来よりは、少人数で店舗を運営することが可能となるだろうし、これから拡大するといわれるマイクロ店舗（非常に狭い範囲で、必要なものに限定して販売する店舗）の効率的な運営などへの適用は、期待されるところである。

これらの無人店舗には、様々なカメラやセンサーが設置され、店舗の中で様々なデータが生み出されることになる。店頭在庫を棚の位置と紐づけて管理することも可能となってくるだろう。これらの


木村 俊一

データや店内での顧客導線データを組み合わせることで、効率化などを推進することが可能となる。

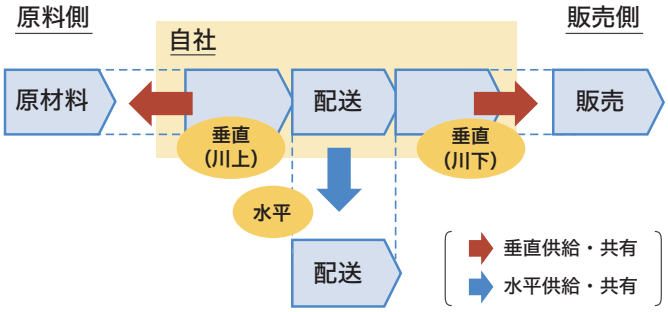
農業などの現場でもセンサーを活用して、生育の状況などをモニタリングすることで、様々な効率化が可能となってくるだろう。実際に、気温や、土壌水分などを計測して、実際の作業計画に活用するなどの取り組みも試行されている。

このようなリアルデータは、我々を取り巻くあらゆる産業で生成され、活用されていくことになるのである。

## 「リアルデータサプライチェーン」の重要性

リアルデータを獲得・蓄積・活用する取り組みは、目指す最終的な到達点から考えれば、まだ始まったばかりといえる。現時点で多くの取り組みは、自組織内に閉じたものとなっているケースが多い。ただ、リアルデータを最大限活用するためには、自社内での活用にとどまっていては限界がある。そのため、自社を取りまくバリューチェーン（顧客や、顧客の先の顧客も含めて考える）内で、リアルデータを相互に供給・共有しあい、活用するための「リアルデータサプライチェーン」（図1）とでも呼ぶべきものが必要となってくるだろう。

図1｜ リアルデータのサプライチェーン（イメージ）




バリューチェーンの垂直方向（川上、川下双方あり）へのデータ供給・共有により、需要予測の精度向上や、バリューチェーン上の他企業に対する、より付加価値の高いサービス企画や提供などが期待できる。例えば、小売からメーカーに対しては、店舗で把握した顧客の店頭行動データを供給・共有することで、メーカーの需要予測精度はより高まり、最終的には廃棄ロスなどの削減にもつながる可能性がある。

コロナの様な緊急時においても、患者に利用している医療品などの状況がリアルタイムで提供・共有されれば、サプライヤーは早い段階で、必要量の確保や、流通ボトルネックの解消に動ける可能性が高い。

バリューチェーンの水平方向へのデータ供給・共有では、同業種における様々な共通業務の効率化を図ることが可能となるであろう。既に物流計画データを共有しての共同配送などが実施されている。今後は、物流に利用される車両の様々なデータ（積載データ、走行データ等）をリアルタイムで供給・共有することにより、更なる効率化を目指せる可能性もあるだろう。また、生産設備のデータの一部も供給・共有することにより、更なる生産の効率化や共同生産の推進などが可能となる。

もちろん、特に水平領域におけるデータ供給・共有にあたっては、技術戦略でいわれるオープン&クローズ戦略と同様の考え方で、差別化領域と非差別化領域の峻別が必要となる。今後は、リアルデータの供給・共有がもたらす効率化の効果は大きくなっていくことが予想される。このため、例えば、これらで得られた効率化によるコスト低減分を原資として、新たなサービスを展開することで、非差別化領域を従来より広げることも可能ではないだろうか。

## リアルデータサプライチェーン実現に向けての課題

このようなリアルデータの活用が現実的なものとなってきた背景には、５Ｇなどの通信インフラの高度化により、様々なデータをネットワークでやり取りすることが可能となってきたことである。また、クラウドなどの進展により強力なコンピューティングパワーを柔軟に低コストで活用できるようになってきたという周辺技術の進歩が大きい。

しかし、これらのリアルデータが、確実に流通・活用されるためには、「技術的に可能となる」だけでなく、データに関する制度やビジネス上の課題を含めて、様々な課題が解決されていく必要がある。ここでは、三つの課題について言及する。

一つは、個人データに関する扱いである。我が国では、２０１９年１月に、当時の安倍政権が「信頼ある自由なデータ流通（ＤＦＦＴ[※1]）」という概念を打ち出しているが、個人情報などについては、各国が同等のレベルで保護する必要がある。この面では、先進的な欧米を追いかける形で、我が国では個人情報保護法が改正され、中国でも２０２１年11月には、個人情報保護法が施行された。個人情報などの守らなくてはならないデータはしっかりと守りつつ、可能な限りデータを流通させ、活用することは極めて重要である。

二つ目の課題は、データ品質の確保である。流通するデータは、ＡＩモデル等の構築に活用される。ＡＩのモデルはインプットデータから「学習」するため、データの質が悪いと、ＡＩモデル自体の質が低下してしまう恐れがある。ここでデータの質が低いとは、そのデータがどのようなデータであるかという、データの定義や収集条件などがあやふやなことも含んでいる。データ自体がいくら厳密に管理されていても、その「データに関するデータ（メタデータ）」が、きちんと整備されていないと、実際の活用は難しくなる。

最後の課題は、データを流通させる際の「値付け」の問題である。データの供給・共有は、相互にメリットがあるため、無償で提供しあう場合はよいとして、そうでない場合は、対価が発生する可能性がある。ただ、データは活用の方法によって大きくその価値が異なるため、その査定が難しい。単にデータを共有するだけでなく、何らかの「機能」にまで作り込んで提供する、もしくはデータの価値を認める事業者がクラウドファンディングのような形でコストを負担し、データ共有を受けるなど、様々な方法が考えられる。

多くの製造業や流通小売業を抱え、今後リアルデータを活用するポテンシャルの高い我が国は、少子高齢化など、社会課題の先進国でもある。我が国が、国際競争力の向上と社会課題の解決のために、リアルデータをいち早く積極的に活用する方法を確立し、今後の世界のリアルデータ活用をリードしていくことを願いたい。

**本稿に関するご質問・お問い合わせは、下記の担当者までお願いいたします。**

NTTデータ経営研究所
デジタルイノベーションコンサルティングユニット
ユニット長／パートナー
木村 俊一
E-mail kimuras@nttdata-strategy.com
Tel. 03-5213-4218

※1　DFFT : Data Free Flow with Trust


# 課題に直面するサイバーセキュリティ

## ～経済安全保障の基盤としての備えは十分であると言えるか～

NTTデータ経営研究所
金融政策コンサルティングユニット
エグゼクティブスペシャリスト

**三笠 武則**
MIKASA TAKENORI

### 1 はじめに

経済安全保障とは、我が国の独立と生存および繁栄を経済面から確保することであり、このために「戦略的自律性の確保（守りの戦略）」と「戦略的不可欠性の維持・強化・獲得（攻めの戦略）」を推進する戦略が必要とされている。サイバーセキュリティはその両方に深く関わる。守りの戦略は基幹インフラの安全性・信頼性確保に直接活かされる。そして攻めの戦略は、官民協力で育成された技術に関する機密保護や非公開の対象となる発明の情報保全に貢献する役割を果たすことになる。基幹インフラに対しては事業継続のためのランサムウェア対策と、安全で信頼性の高いインフラ構築のためのサプライチェーンセキュリティ対策が重要な柱である。技術に関する機密保護や非公開発明の情報保全に対しては、内部不正防止を含む機微な技術情報の漏洩対策が重要である。しかし、これらはいずれも現在の我が国社会の重要課題として取り組みが進められているものであり、対策が十分な成熟度を持って社会に浸透しているとは言い難いのが現状である。

### 2 情報セキュリティにおける重大な脅威の現状

2022年1月27日にIPAが公表した「情報セキュリティ10大脅威2022」によると、組織の上位5脅威は以下の通りである。

① ランサムウェアによる被害（昨年1位）
② 標的型攻撃による機密情報の窃取（昨年2位）
③ サプライチェーンの弱点を悪用した攻撃（昨年4位）

サイバーフィジカル融合分野の安全・セキュリティ対策、秘密の漏えいやデータの不正利用対策等の調査研究、及びその成果の空港運営への適用の提言に力を入れている。

④ テレワークなどのニューノーマルな働き方を狙った攻撃
（昨年3位）
⑤ 内部不正による情報漏えい
（昨年6位）

④を除けば、まさに1.で述べた3つの重要な柱と合致している。そして④のテレワークは、これらの重要な脅威をさらに増大させる要因になると言える。

これらの脅威の中でも、特にランサムウェア攻撃の衝撃は大きい。企業の事業継続を直撃する攻撃の拡大は、まさに喫緊の課題である。その進化も急であり、技術面における二重脅迫型の拡大や、攻撃インフラ面におけるRaaS（Ransomware as a Service）の登場など、リスクは年々高まっている。これは、基幹インフラを長期間破壊してしまうことにも繋がりかねない。さらに情報漏えいの中でも重要技術情報の漏えいは、いまや個人情報の漏えいと比肩する深刻なリスクとして捉えられ始めている。

このように、サイバー攻撃が事業継続に与える衝撃や重要技術情報漏えいへの危機感が近年大きく変化しており、これがまさに、サイバーセキュリティから見た経済安全保障の中核として重視されることに繋がっている。

## 3 経済安全保障推進法案におけるサイバーセキュリティ対策に関する法制化の動き

経済安全保障推進法案が規定するサイバーセキュリティ対策は大きく分けると「基幹インフラの安全性・信頼性確保」と「戦略的不可欠性を守るための秘密保持及び情報保全」に分けられる。以下ではこれらについて概説する。

### (1) 基幹インフラの安全性・信頼性

現在、あらゆる経済活動の領域がサイバー攻撃の対象となっており、基幹インフラ事業も例外ではない。基幹インフラ事業者が利用するICT設備が高度化するとともに、サプライチェーンが複雑化、グローバル化しており、さらには当該設備の維持などを他の事業者に委託することも当たり前になってきたことから、サプライチェーンの過程で設備に不正機能が埋め込まれるリスクが高まっている。リスクのある事業者からひとたび設備を導入してしまうと、当該事業者が当初より不正機能を組み込む、事後的に発見した脆弱性を放置する、ソフトウェアアップデート時に不正機能を埋め込むといった行為を行ったとしても、これを基幹インフラ事業者が検知することは容易ではない。さらには、これが原因で不意に基幹インフラ機能に支障が生じた場合には、対応に多大な費用と時間を要し、その間は基幹インフラ役務が安定的に提供されず、国家・国民の安全に多大な影響を及ぼす恐れがある。

そこで国は、これに対抗するために、経営者の事業判断、競争法との関係、国際ルールとの整合に気を配りつつ、現在立法措置による規制の導入に取り組んでいる。経済安全保障推進法案における基幹インフラの安全性・信頼性に係る規定の骨子を以下に示す。

■対象とする事業：エネルギー、水道、情報通信、金融、運輸、郵便
■対象とする事業者：基準を定めて指定
■対象とする設備：基幹インフラ事業の中心的なシステムを構成しており、その機能が停止または低下した場合は、基幹インフラ役務の安定的提供に大きな影響を及ぼす重要な設備、機器、装置など（情報システムを含む）、およびこれらに係るソフトウェア
■業務委託：当該設備の重要な維持管理などの委託は規制の対象
■データセンター・クラウドサービス：その上でシステムを構築して基幹インフラ役務の提供に利用する場合は規制の対象
■手続き：国による事前審査、勧告・命令


三笠 武則

■命令に従わない場合の罰則：検討中　等

### (2) 戦略的不可欠性を守るための機密保持及び情報保全

選択された技術の研究開発を効果的に推進するための官民協力として協議会を設置する際、協議会の参加者間で機微な情報も含む有用な情報の交換や協議を円滑に行うことができ、同時に研究者やスタートアップが参画しやすい情報管理制度の導入が求められている。さらには、特許制度の例外措置として、機微な発明の特許出願について出願を非公開とするとともに、流出防止措置を講じることで、当該発明が外部からの脅威に利用されることを未然に防ぐ制度が必要である。そこで、経済安全保障推進法案では次のような規定が設けられている。

■協議会で交換される機微情報の取り扱い：第三者提供や不正な利用を禁じ、これに従わなかった場合は国家公務員と同等の罰則を伴う守秘義務を参加者に課す

■機微な発明の取り扱い：非公開の決定をした発明については、出願者などに情報保全を求め、発明の実施を制限する。当該発明の情報は、営業秘密として厳格に管理する。

## 4　サプライチェーンセキュリティ対策における課題

米国では、トランプ前大統領が「情報通信技術・サービスサプライチェーンの安全性を確保する大統領令（EO13873）」に署名し、米国内の個人・民間企業による「外国敵対者」およびその支配下の企業との「一定条件を満たす情報通信技術・サービスに係る取引」を禁止した。その後ドイツでは、2021年5月に「情報技術システムのセキュリティを高めるための第2の法律（ITセキュリティ法2.0）」が発行された。同法では重要インフラ運用者は、インフラに係る重要部品の使用を開始しようとする場合、事前に政府に通知する義務がある。この制度は、我が国の経済安全保障推進法案の「基幹インフラの安全性・信頼性」の部分の検討において参考にされたと言われている。このように、欧米ではサプライチェーンセキュリティリスクに対する規制にいち早く取り組み、その重要性を国際的にアピールしている。我が国でもIPAの「情報セキュリティ10大脅威」に見られるように、近年サプライチェーンセキュリティリスクに対する危機感が益々高まってきている。

サプライチェーンセキュリティはいくつかのケースに分類される（図1参照）。攻撃者はセキュリティ対策が進んでいない組織を狙う方が容易に攻撃を成功させられるため、海外拠点や脆弱な取引先を踏み台にした攻撃が顕著になってきている。しかし、その対策はまだ十分に進んでいないのが実状である。

さらには開発だけでなく、運用段階も含めたITシステム／サービスに関する業務の外部委託が増えており、リスクが高まっている。また、再委託先以降の管理は委託先任せになっているケースも多く、サプライチェーン全体の可視化は非常に困難とされている。[※1] このように、サプライチェーンセキュリティ対策には課題が多く、企業による取組のレベルにも大きな差異が生じている。企業の自主性だけに任せていては喫緊の課題に適時に対処できないとの考えから、米国やドイツのように、サプライチェーンセキュリティを規制化して基幹インフラ企業などに義務を課す動きが広がっても不思議ではない。従来は、サイバーセキュリティ分野は規制になじまないという常識があったが、この考えは崩れ始めている。

## 5　進化する技術情報窃取の手口

技術情報窃取の手口は着実に進化している（図2参照）。従来は転職時などに人が技術情報を不正に持ち出すことが中心だった。しかし

※1　IPA “サプライチェーンのセキュリティ脅威に備える”（2019年5月）

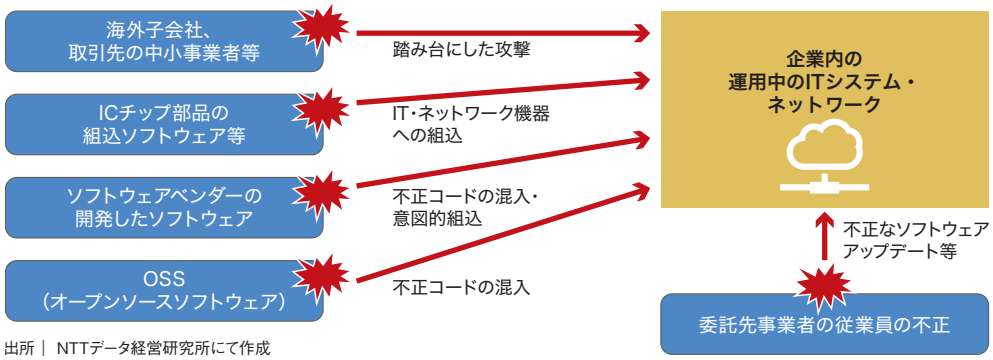
近年はサイバー攻撃、内通者の悪用、サプライチェーンの脆弱な箇所からの攻撃など手口が複雑化している。テレワークも組織の目が届きにくいので、外部脅威者に付け入る隙を与えやすい。これらの変化を踏まえ、今後は重要技術情報を護ることに重点を置く必要がある。

また、キーマンを保護することの必要性を指摘しておきたい。システム・ネットワークの高度な運用ができるエンジニア、DXを陣頭指揮できる高度な専門人材、重要な発明の中核を成す一流の研究開発者などは希少であり、攻撃のターゲットになりやすい。攻撃者は求人情報、社報の人物紹介、論文発表、特許出願等のネットに露出した様々な情報を通じて、こうしたキーマンの動きを盗み見ている。ヘッドハンティングの目的は転職時に重要技術情報を持ち出させることだけでなく、履歴書ファイルにマルウェアを組み込んで社内ネットワークへの侵入の手段とすることもある。真のキーマンにはできるだけ論文発表をさせない、ネットに露出させないなど、社内にしっかりと隠して護ることが必要な時代になったと言える。

## 6 まとめ

現在の情勢を踏まえると、まずは経済安全保障に限定されることなく、各企業がランサムウェア対策、技術情報漏えい対策、サプライチェーンセキュリティ対策を強化することが喫緊の課題と言える。社会全体でさらに対策を強化していくことが求められている。経済安全保障のセキュリティ対策は、これを高いレベルで基幹インフラ事業者、機微情報を共有する協議会参加者、非公開の決定をした発明の特許出願者などに求めるものである。規制であるため、義務もある。しかし、だからこそサイバーセキュリティ対策のノウハウが蓄積され、専門人材の育成も進むと期待できる。ここで蓄積されたノウハウと育成された専門人材を社会に広く還流させることで、我が国社会のサイバーセキュリティ対策の成熟度が底上げされることを期待したい。

図1｜ サプライチェーンセキュリティの分類




出所｜ NTTデータ経営研究所にて作成

図2｜ 手口の多様化が進む技術情報の不正な窃取

**伝統的な不正窃取の手口**

【内部不正】

- 転職時等に人が不正に持ち出し
- 転職直前に、人が電子メールやオンラインストレージ等で社外に不正送信

**新たに定着したサイバー攻撃による不正窃取の手口**

【サイバー攻撃】

- 標的型攻撃による機密情報（重要技術情報等）の不正窃取

出所｜ NTTデータ経営研究所にて作成

**最近注目されている新たな不正窃取の手口**

【内部不正】

- 外部脅威者が、従業員やシステム運用委託先の要員を脅す・金銭で唆す等の手口で内通者を作り、内通者が不正に技術情報を漏えい

【サイバー攻撃】

- 上記と同様の方法で従業員やシステム運用委託先の要員に内通者を作り、内通者に手引きさせてサイバー攻撃を実施（手引きの例：マルウェアを意図的に社内ネットワークに持ち込む、不正なコードを含むソフトウェアアップデートを適用する等）
- 運用委託先を踏み台として、運用を委託しているシステムにマルウェアを送り込む
- OSS（オープンソースソフトウェア）を踏み台にして、運用システムに不正なコードを組み込む


**本稿に関するご質問・お問い合わせは、下記の担当者までお願いいたします。**

NTTデータ経営研究所
金融政策コンサルティングユニット
エグゼクティブスペシャリスト
三笠 武則
E-mail mikasat@nttdata-strategy.com
Tel. 03-5213-4115


# 経済安全保障に欠かせない サードパーティリスク対応

NTTデータ経営研究所
金融政策コンサルティングユニット
ユニット長／パートナー

**大野 博堂**
OHNO HAKUDO

経済安全保障において金融機関として欠かせないのがサードパーティリスク対応だ。フィンテックブームの中、金融機関は様々なカウンターパートとの連携を深めつつある。資本規模が小さく、創業から日の浅い国外企業とのパートナーシップも当たり前となり、重厚長大企業との連携を前提としていた従前の対応とは景色が一変したとも言える。また、金融機関の現業部門においてもクラウドサービスが多用され、情報システム部門が直接に関与しない外部企業が提供するITサービスの利用も盛んだ。他方で、これまでにない規模とスピードで外部企業との連携や外部サービスの利用が進む中、金融機関は新たなリスクも抱えることとなった。すなわち「サードパーティリスク」の台頭である。そこで本稿では、金融セクターにおける経済安全保障としてサードパーティリスクへの対応手法を取り上げ、今後の我が国金融機関が留意すべきポイントを解説する。

## 米国政府における情報システム調達上の懸念

契機となったのは、数年前の米国における中国企業・ファーウェイ社を取り巻く騒動だ。当時米政府は、ファーウェイ社および関連法人40数社が米国製半導体などを事実上調達不可となる輸出管理規則を適用。そもそも、米国政府および政府機関との取引に関しては同社製品の情報システムへの組込・実装・利用は制限されていたのだが、この規制によりさらに強化された格好となった。この背景には、サイバーセキュリティに関する米国政府の懸念がある。政府調達の大規模情報システムが、外部との接続チャネルなどにおける脆弱性を排除し、いかに高度化さ

大手SIerにてデリバティブ取引管理システムなどの企画に従事した後、当時の大蔵省にて金融マーケットを中心にマクロ経済分析を担当。平成18年より現職。計量経済分析や事業戦略立案、中央省庁における調査分析活動支援のほか、最近ではサイバーセキュリティ、フィンテック、マイナンバーなど、金融レギュレーション分析による金融業務へのインプリケーション支援や、地方創生をキーとした地方自治体向けアドバイザリー業務などを中心に活動。

れたセキュリティを具備したとしても、そもそも情報システムに組み込まれている一部製品が「不自然な」動作をするようなことがあれば、システム全体のセキュリティが担保できなくなるためだ。もちろん、同社による明確な産業スパイ事案などは報告されておらず、米国政府の懸念の実態については我々も子細を知る術はない。

　このように、米国では政府調達を中心に、情報システム開発や運用を直接に担うITベンダーに対して情報システムに組み込む機器やソフトウェア製品へのチェック機能の強化を求めており、「情報セキュリティ強化」を御旗に他の同盟国（英、豪、カナダ、ニュージーランドが対象とされる）にも同様の対応を呼びかけている。すなわち、米国を含めた5カ国間における諜報（インテリジェンス）活動から得られた情報の共有基盤「FIVE EYES」である。日本はこの「FIVE EYES」への加盟を目指しているとされ、水面下では米国から同様の要請を受けていたようだ。そしてこれが我が国においても政府調達の情報システムにおける事前のセキュリティチェックが厳格に運用される契機となった。すなわち、経済安全保障における喫緊の重要性を我が国政府が認識した契機がこの騒動であったと言っても過言ではない。

## 忘れてはならない諸外国におけるローカルルールの存在

　一大消費地であることに加え、オフショアでのシステム開発や企業のデリバリー拠点としても重視されてきた中国では、2010年7月に国防動員法が施行されている。中国国内で有事が発生した場合に発令され、企業が保有する財産や資源は必要に応じて中国政府に接収されることとされている。また、交通インフラや金融機能についても政府もしくは軍の管理下に置かれるとされており、中国企業のみならず、外資系企業もその対象となっている。有事に際しては空港や港が閉鎖される見通しであり、邦人の中国国外への出国も困難になろう。そのため、中国国内における有事は、我が国企業の事業撤退リスクに直結する可能性が否定出来ないことに改めて留意が必要である。さらに、中国では2017年より国家情報法が施行された。中国人はいかなる組織・個人においても、中国の情報活動に協力する義務があると定められており、中国国外に居住する中国人もこの規制を受けると解釈される。さきの米国におけるファーウェイ社を取り巻く懸念も、これが一つの契機ともなっている。

　中国にとどまらず、国によっては通信保秘に関するルールが整備されていないなど、当該国政府組織はもとより第三者による通信傍受が物理的に可能となっている恐れがあるとされるケースも存在する。こうした国に我が国の国民情報などが格納されたサーバなどが設置されていた場合、第三者による通信傍受の懸念も出てくることだろう。国民に関する情報が国内のITベンダーによって厳格に管理されていたとしても、サプライチェーンを通じて第三者が当該情


大野 博堂

報を部分的にであっても取扱い、さらに第三国に設置されたサーバをクラウドサービスなどによって間接的に利用している、といったことがあれば、当該格納情報はもはや安全に保秘されているとはいえまい。

こうしたケースを考慮のうえ、我が国政府では情報取扱方針を徐々に厳格化してきており、その過程において、いわゆる「サードパーティリスク」という概念が浮上したものと理解される。

## 金融機関における経済安全保障はサードパーティリスク対応そのもの

政府がカウンターパーティとの取引に配意しようとしているのであれば、これを金融機関側の立場に当てはめた場合、どのようなケースが想定されるのであろうか。

金融機関ではＩＴベンダーとの取引に際し、従前より財務状況はもとより経営者の信頼性などについても十分に考慮されてきたことだろう。ただし、ＩＴベンダーの開発体制が再委託、再々委託といった重畳的な体系へと移行する中で、金融機関としては再委託先などのチェックが十分に行き届かなくなる可能性も否定できない。とかく大規模システム開発などの場面においては、テンポラリーなスタッフを短期で大量雇用し、当該スタッフが重要システムの開発の一部を担う、といったシーンも想定されることから、委託先企業そのもののチェックはもとより、従事するスタッフ一人一人の属性チェックも今後は欠かせない。最近の中央省庁では、国の委託業務において実際に業務に従事する委託先企業の職員についてもフィルタリング機能などを用いた信用チェックを実施するのがデファクトとなっている様子がうかがえるが、これは企業そのもののチェックだけでは情報管理上の「抜け漏れ」が生じることを懸念しているためだ。

かたや金融機関をみると、昨今は新興企業との連携へと加速する風潮がみられる。「ほぼ完璧ではないか」とも思える、ベストプラクティスともいうべき対応が施されている金融機関も存在するものの、全ての金融機関で同様のチェック機能が働いているとは限らない。こういった点が金融庁の懸念材料となっているようだ。

## 新たなサービス利用形態で生じる金融機関の脆弱性

こうした金融庁の懸念はサードパーティリスク対応そのものにまつわる課題といってもよい。ただし、従来の金融機関はＩＴシステムの安全対策を忠実に履行してきたといっても差し支えない状況にあった。金融庁と歩調を合わせる格好でＦＩＳＣ（The Center for Financial Industry Information Systems：金融情報システムセンター）が推進してきた金融機関の安全対策基準は厳格に定義されており、少なからずこれを踏まえた管理体系を施しているのであれば「凡そは安心」できたためだ。従前の全社利用ＩＴシステムをみると、ＩＴ部門が管理のう

え、システム台帳でサーバの設置場所やシステム停止時の代替手段、データのサプライチェーンについても網羅的に捕捉・管理されてきたことだろう。この点において、我が国の金融機関の情報システムは他国に比して堅牢性や安全性が機能してきたものと考えられる。ところがフィンテック企業との連携という新たなシーンが生まれたことに加え、業務部門が単独で他社のITシステムを利用するケースが増加してきた。SaaS(Software as a Service)やクラウドサービスと言われるものの多くがこれに該当する。これらの外部サービスの利用に際しては、IT部門が関与しないケースもあり、システム管理台帳上でも管理対象外となっていたりもする。IT部門が管理していないこのような外部サービスはセキュリティなどの対処が現業部門に委ねられてしまう可能性も否めず、当該サービスに入力された金融機関の情報が、外国に設置されたサーバ上でひっそりと管理されている可能性も否定できない。メインサーバが国内に設置されていても、バックアップサーバの設置場所まで確認しきれていないかもしれない。

## システムリスクアセスメントが実施されていない可能性

そもそもFISCでは「金融機関のためのコンティンジェンシープラン策定のための手引書」を公表しており、金融機関は当該手引書を用いたリスクアセスメント作業を要請されている。FISCでは金融機関を取り巻くリスクを原因系に着目し、「内部起因のリスク」「外部起因のリスク」と峻別して定義。それぞれの発生確率やリスク発現時に金融機関が受ける影響の大きさを評価するよう促している。発生確率が高く、影響が甚大なリスクについては優先的に対応方針を整えることになるのだが、中には「10年前に実施したアセスメント結果をそのまま採用している」といった金融機関もみられるのが実態だ。すなわち、リスクアセスメントが陳腐化した結果、リスクへの対応がおざなりになってしまっているのだ。

金融機関が利用するITシステムは多岐に亘り、多くはIT部門が直轄で管理下に置いている。これらはIT資産台帳にも掲載され、管理対象として厳格視されている。ところが昨今、業務部門や営業部門が外部のフィンテックベンチャーなどとダイレクトに契約を締結し、当該企業が提供するソリューションを利用する、といった形態が一般化している。これらのソリューションは顧客と金融機関との間に位置付けられ、顧客情報が流通するにも拘わらず、IT部門が関与しないケースもあるようだ。結果として従前のITシステムのように「厳格な管理対象」として見做されず、セキュリティチェックも外形的なものにとどまっている可能性が否めない。

## フィンテック企業で散見されるガバナンスやセキュリティ上の問題

業歴の浅い企業においては、頻


大野 博堂

繁に経営者が替わったり、「ラウンド」と称した第三者割当増資を通じて資本関係、株主、その持ち分構成比も短期に変貌を遂げることだろう。金融機関側の情報管理態勢がいかに厳格なものであったとしても、顧客情報を連携する提携先企業における情報システムにセキュリティ上の瑕疵が存在していたり、そもそも当局が要請するレベルのレギュレーション対応が施されていなかったとしたら、金融機関のリスク管理上の脅威となりうる。とかくスタートアップでは、アイディアベースで事業規模拡大が志向される傾向にあり、ガバナンスやセキュリティが劣後されている可能性がある。それを念頭に、経営者そのものや経営の意思決定メカニズムを含めた全体像を踏まえた、金融機関としてのリスクコントロールやチェックの機能が必要となるはずだ。

## 公衆Wi-Fiに接続して業務を実施する社員とこれを容認する企業

筆者はPCを外部で人目につく場所で利用することは極力避けており、会社貸与のスマホでさえ、外部で利用する際には接続先ネットワークの利用にも留意している。しかし、喫茶店、ホテルや空港のロビーなどでは、周りを気にせずにPC操作をしている方が多く、場合によっては業務上の会話なども耳にすることがある。公衆の場でも、無料でWi-Fiが利用できることもこの傾向を助長している。フリーWi-Fiは通常のインターネット利用やホビー需要のためのツールとして無料開放されていると理解すべきであり、業務上の情報を格納した端末を接続するという発想を持つのは危険だ。また、フリーWi-Fiの中には、「敵」があえて情報窃取を目的に設置したものも存在している。第三者が設置した、セキュリティの緩い、もしくは悪意を持って敵が設置したフリーWi-Fiに接続したターゲットの端末へ侵入を試み、端末内の情報を窃取せしめる事例も確認されている。ターゲットの端末への直接への侵入にはちょっとしたスキルが必要だが、「どんなサイトを見ているか？（アクセスしているか）」「何を打ち込んでいるか」を知ることは簡単だ。

喫茶店などでの会話を聞いていると、取引先とのシステム開発の進捗に関するやりとりを複数名で実施している様子が伺えることも珍しくない。オフィスを持たずにデリバリーを実現するといったベンチャー企業もみられる中、セキュリティの視点が抜け落ちているこうした「危機感のない企業」の存在を、我々は十分に認識する必要がある。

## 金融機関は接続先事業者や業務委託先企業の実態を捕捉しているか？

もちろん、金融機関は新たに提携する企業の財務情報その他の信用調査は「入口段階」での所作として当然のように事務手続きに組み込んでいることだろう。重要なのは提携後の「継続審査・監査」の視点である。融資でいう「途上審査」に似た要件と考えれば良い。前述のとおり、頻繁にラウンドがこなされ資本関係が変わる可能性も踏まえ、最低限必要な相手先企業の情報収集を継続的に行わねばならない。

例えば、当該企業における外部提携関係に変化はないかといったことも確認項目としては重要だ。自社との業務提携の後、新たに第三国のカウンターパートとの間で自社のリスクとなりかねない新たな提携関係が生まれている可能性もある。その際、第三者割当増資を通じ、第三国の企業体が当該企業の株主として登場していたりは

しないだろうか。我々が知らない間に、当該企業における業務が実質的に第三者に一部にせよ再委託されたりしていないだろうか、サーバの設置場所に変化はないか、といった視点でもチェックを施す必要があるだろう。

また、最近のフィンテックベンチャーで多いのが「当局レギュレーションの認識不足」に起因するトラブルだ。中には、金融庁の問いかけに際し、「FISCって何ですか？」と問い返した企業があり検査官が唖然とした、という話も耳に入ってくる。このようにレギュレーションも含めた法令意識や金融サービスに独自に要請されている事項への対応状況についても継続的に確認を求める必要があることは言うまでもない。そこで問われるのがリスクアセスメントを実施するための具体的なチェックリストの有無である。

## サードパーティリスクのコントロールに向けたチェックの視点

例としてここでは金融機関が外部企業との提携に際して、また継続的にチェックすべき視点として重要なポイントを取り上げる。なお、理想的には内部監査部門とも連携し、組織横断的なチェック体制を構築のうえ、提携先企業の精緻なアセスメントを速やかに実現すべきだろう。

**■相手先企業の経営体制**

・経営者の属性（国籍、履歴）
・実質的経営者の属性（国籍、履歴）

**■法的制約と当局の課すレギュレーションの理解**

・金融関連業法の理解
・FISCの安全対策基準の理解
・明文化されていないその他の金融業を取り巻く過去の通達や慣行の理解

**■相手先企業の内部管理態勢**

・意思決定メカニズムの実態
・牽制機能の実装
・内部犯罪への対処の考え方とこれを避止するチェック態勢
・内部監査の機能実態と外部監査の結果
・当局が期待するレベルの各事務処理の手続き

**■相手先企業のシステム開発の基盤と態勢**

・基盤となるハードやソフト（製造者）
・サーバの設置場所（国、地域）
・バックアップのカバー範囲（本番系のフルバックアップor一部機能に限定）
・バックアップシステム（サーバ）の整備状況と設置場所、もしくはデータの隔地保管の実態（設置国、設置場所）
・バックアップシステムへの切り替え/切り戻し手順の可視化
・システム開発および運営の体制（委託、再委託の実態）

以上、あくまで一例として参考となるポイントを取り上げたが、今後厳しさを増すことが予想される経済安全保障を念頭に、こうした論点整理を先行して実施しておくことが有効となるだろう。


**本稿に関するご質問・お問い合わせは、下記の担当者までお願いいたします。**

NTTデータ経営研究所
金融政策コンサルティングユニット
ユニット長／パートナー
大野 博堂
E-mail onoh@nttdata-strategy.com
Tel. 03-5213-4115


# 経済安全保障が求める官民技術協力とは何か？

NTTデータ経営研究所
社会システムユニット
コンサルタント
**三藤 米利紗**
MITSUFUJI MERISA

## 1 はじめに

2021年10月に発足した岸田内閣では、経済安全保障担当大臣が設置されたことが話題となった。2022年1月に召集された通常国会では、小林 鷹之・経済安全保障担当大臣が中心となって取りまとめた経済安全保障推進法案（以下、推進法案）が提出される見通しだ（2022年1月末時点）。本法案は、①サプライチェーン（供給網）の強化、②基幹インフラ機能の安全性・信頼性の確保、③特許非公開化、④官民技術協力の4分野から構成される予定である。本稿では、まず推進法案を中心に日本における近年の経済安全保障の取り組みを振り返った上で、推進法案を構成する1分野である「研究開発支援」に関する国内外の動向を概観する。

## 2 経済安全保障に関連する日本の取り組み

### (1) 2020年以降の政府および与党の取り組み

近年の経済安全保障に関連した日本政府による取り組みの起点は、国家安全保障局経済班の設置（2020年4月）と言えるだろう。国家安全保障局経済班は、経済分野における国家安全保障の課題に対応するために設置された。その二か月後には与党である自民党内に新国際秩序創造戦略本部が設置され、2020年12月、「『経済安全保障戦略』の策定に向けて」[※1]と題した提言がとりまとめられている。この提言においては、経済安全保障を「わが国の独立と生存及び繁栄を経済面から確保すること」と定義している（なお、筆者が確認した限りでは、現時点では経済安全保障推進会議及び経済安全保障法

※1 自由民主党　政務調査会　新国際秩序創造戦略本部「『経済安全保障戦略』の策定に向けて」
(https://jimin.jp-east-2.storage.api.nifcloud.com/pdf/news/policy/201021_1.pdf)

日系コンサルティングファームを経て、現職。スマートシティや情報通信分野を中心とした研究開発・国際標準化動向に関する調査・コンサルティング業務に取り組む。

制に関する有識者会議の資料には明確な定義は示されていない）。さらに同提言では、経済安全保障を「戦略的自律性の確保」と「戦略的不可欠性の維持・強化・獲得」という2つの考え方により推進するべきであるとしており、これらの考え方は関係閣僚が構成する経済安全保障推進会議の資料にも登場する。参考として、自民党による戦略的自律性と戦略的不可欠性の定義を左記（図1）に示す。

図1｜戦略的自律性と戦略的不可欠性の定義

| | |
|---|---|
| **戦略的自律性** | わが国の国民生活および社会経済活動の維持に不可欠な基盤を強靭化することにより、いかなる状況の下でも他国に過度に依存することなく、国民生活と正常な経済運営というわが国の安全保障の目的を実現すること |
| **戦略的不可欠性** | 国際社会全体の産業構造の中で、わが国の存在が国際社会にとって不可欠であるような分野を戦略的に拡大していくことにより、わが国の長期的・持続的な繁栄及び国家安全保障を確保すること |

2021年5月には自民党同本部から「中間とりまとめ」[※2]が出された。この中で、戦略的自律性・戦略的不可欠性の双方において重要な一部である「技術」については喫緊の課題があるとして、技術の保全・育成について詳細に取り上げており、ここで示された内容は政府の『経済財政運営と改革の基本方針2021』に盛り込まれた。その約半年後、岸田新内閣の目玉人事として経済安全保障担当大臣が任命され、現在は推進法案のとりまとめを担当している。

このように、政府による経済安全保障への対応はこの2年間で急速に進展してきた。この背景には、あらゆる面での米中対立の深化など、日本を取り巻く環境の変化が挙げられる。また、新型コロナウイルスの感染拡大により、複雑化したグローバルサプライチェーンが抱えるリスクが顕在化したことが経済安全保障の議論を加速させたと考えられる。さらに、パンデミックによりデジタル技術の重要性が再認識されると共に、フィジカル空間とサイバー空間の統合が進むことによる新たなリスクへの対応を迫られているという背景もあるだろう。

### (2) 経済安全保障推進法案の概要

2022年の通常国会での成立が目指される推進法案は、4本の柱から構成される見通しである（図2）。また、経済安全保障推進会議の資料では、これら4つ以外

図2｜経済安全保障推進法案の4本柱

| | | |
|---|---|---|
| 戦略的自律性 | ①サプライチェーン | 国民生活や産業に重大な影響が及ぶ状況を回避すべく、重要物資や原材料のサプライチェーンを強靭化 |
| 戦略的自律性 | ②基幹インフラ | 基幹インフラ機能の維持などに係る安全性・信頼性を確保 |
| 戦略的不可欠性 | ③官民技術協力 | 官民が連携し、技術情報を共有・活用することにより、先端的な重要技術を育成・支援する仕組み |
| 戦略的不可欠性 | ④特許非公開 | イノベーションの促進との両立を図りつつ、特許非公開化の措置を講じて微妙な発明の流出を防止 |

出所｜ 経済安全保障推進会議（第1回）資料（※3）を基にNTTデータ経営研究所にて作成

※2 自由民主党　政務調査会　新国際秩序創造戦略本部「中間とりまとめ『経済財政運営と改革の基本方針2021』に向けた提言」（https://jimin.jp-east-2.storage.api.nifcloud.com/pdf/news/policy/201648_1.pdf）

※3 経済安全保障推進会議（第1回）　資料3「経済安全保障の推進に向けて」（https://www.cas.go.jp/jp/seisaku/keizai_anzen_hosyo/dai1/shiryou3.pdf）


三藤 米利紗

にも、13の分野が経済安全保障上の主要課題として示されている。

経済安全保障推進法案の4本柱として示された分野では、いずれも大学等の研究機関や民間企業に当事者としての対応が求められるだろう。したがって、大学や企業にとり今後これらの分野に関する国内外の情勢を注視することがより重要となると筆者は考えている。

## 3 「官民技術協力」とは具体的には何か

経済安全保障の強化においては、企業や大学に対して何かしらの制約が課される場面もあることが想定される一方、図2の「官民技術協力」は先端的な重要技術への育成・支援を取り組み内容としている。官民技術協力について有識者会議がとりまとめた提言骨子[※4]では、先端的な重要技術の研究開発への資金提供や、産学官が参加する協議会の設置、国内外の情勢や研究開発動向の調査・分析を行う調査研究機関（シンクタンク）の設置が提案されている。

提案された協議会については、研究開発に有用な情報の提供や必要な規制緩和の検討、国際標準化の支援等の伴走支援の実施に加えて、協議会における情報管理の取り組みについても提言している。ここでは研究者やスタートアップへ広く門戸を開きながらも、「国家公務員に求められるものと同等の守秘義務を参加者に求めるべきである」との提言がなされている。

有識者会議がとりまとめた提言骨子の中では、「先端的な重要技術」について具体的な技術は示されていないものの、分野として宇宙、海洋、量子、AI、バイオなどが挙げられた。その上で、重点的に支援すべき技術の絞込みにおいては、前述の調査研究機関（シンクタンク）による調査分析や専門家の知見を活用しながら「我が国の技術的強み、諸外国の研究開発状況、社会実装に関するニーズ情報等を考慮することが必要である」としている。

他方、先端的な重要技術として挙げられた各分野の研究開発支援は、現在も「戦略的イノベーション創造プログラム（SIP）」「ムーンショット型開発制度」「官民研究開発投資拡大プログラム（PRISM）」などにおいて実施されているところである（図3）。「統合イノベーション戦略2021」[※5]においても、国内外の情勢変化として「技術覇権争いの更なる先鋭化」を説明した上で、「イノベーション政策における経済安全保障を念頭に置いた対応が必要である」との記述がなされている。筆者は、既に実施されているプログラムとの連携がどのようになされていくかという点も重要な論点となると考えている。

## 4 他国の政策

他国においても、自国の技術を保護・育成するための戦略策定や取り組みが行われている。日本の戦略的不可欠性を維持・強化・獲得していく上では、他国の研究開発動向を踏まえた視点が欠かせないだろう。ここでは、米国と欧州の例を紹介する。

### (1) 米国

米国では、2020年10月にトランプ政権が「重要・新興技術国家戦略（National Strategy for Critical and Emerging Technologies）」[※6]を発表した。この戦略は、米国が同盟国やパートナーとの協力のもと重要・新興技術（C&ET）において世界をリードし続けるための柱として「イノベーション基盤の強化」と「技術的優位性の確保」の2つを示すと共に、重要新興技術リストを公開した。リストには、各政府機関が優先分野として特定し国家安全保障会議に報告した20の技術分野[※7]が挙げられている。

※4　経済安全保障法制に関する有識者会議「経済安全保障法制に関する提言骨子（官民技術協力）」（https://www.cas.go.jp/jp/seisaku/keizai_anzen_hosyohousei/dai3/teigenkossi3.pdf）
※5　「統合イノベーション戦略2021」（令和3年6月18日閣議決定）（https://www8.cao.go.jp/cstp/tougosenryaku/togo2021_honbun.pdf）
※6　White House “National Strategy for Critical and Emerging Technologies”（https://trumpwhitehouse.archives.gov/wp-content/uploads/2020/10/National-Strategy-for-CET.pdf）

図3｜実施中の研究開発プログラム

| プログラム名 | プログラム概要 |
|---|---|
| 戦略的イノベーション創造プログラム（SIP） | 総合科学技術・イノベーション会議が府省・分野の枠を超えて自ら予算配分して、基礎研究から出口（実用化・事業化）までを見据えた取り組みを推進。 |
| 官民研究開発投資拡大プログラム（PRISM） | 高い民間研究開発投資誘発効果が見込まれる「研究開発投資ターゲット領域」に各省庁の研究開発施策を誘導し、官民の研究開発投資の拡大、財政支出の効率化などを目指す。 |
| ムーンショット型開発制度 | 我が国発の破壊的イノベーションの創出を目指し、従来技術の延長にない、より大胆な発想に基づく挑戦的な研究開発（ムーンショット）を推進。野心的な目標設定の下、世界中から英知を結集し、失敗も許容しながら革新的な研究成果を発掘・育成。 |

出所｜総合科学技術・イノベーション会議の資料を基にNTTデータ経営研究所にて作成

これに続いてバイデン政権は、2021年3月「American Job Plan」を発表した。ここでも、新興技術における米国のリーダーシップは経済競争力と国家安全保障の両方にとって重要であるとの観点から、半導体や先進コンピューティング、先進通信技術、先進エネルギー技術、バイオテクノロジーなどの分野への500億ドルの投資を表明している。

昨年4月の日米首脳会談で出された共同声明では、バイオテクノロジー、AI、量子科学、民生宇宙分野などの多様な分野での研究開発に関する両国の協力深化が確認された。また、今年1月の日米首脳テレビ会談においても、先進技術に関する協力を進めることが確認されている。

必ずしも経済安全保障の強化という枠組みの中で行われるものばかりではないものの、筆者は、これらの協力は日米を取り巻く国際情勢の変化を反映していくこととなると考えている。

### (2) 欧州

欧州では、研究とイノベーションへの投資プログラム「Horizon Europe」[※8]による約1000億ユーロの支出が欧州委員会から公表されている。具体的な取り組み分野については、第2の柱「グローバルチャレンジ・欧州の産業競争力」の中で6つのクラスター（①健康、②文化、創造性、包括的な社会、③市民の安全、④デジタル、産業、宇宙、⑤気候、エネルギー、モビリティ、⑥食料、バイオエコノミー、自然資源、農業、環境）として示されている。

## 5 今後に向けて

以上、日本の経済安全保障に関する取り組みと国内外の技術に対する支援動向を概観した。経済安全保障においては規制や制約の面が注目されることが多いが、筆者は、研究開発を行う大学や企業にとってはチャンスとして捉えることもできると考える。他方、政府としては、まずは国内外の技術開発動向や他国の政策を踏まえ、経済安全保障推進法案において育成・支援の対象とする先端技術を提示することが求められるだろう。また、それと並行し、現行の取組も踏まえつつ、経済安全保障の視点から官民協力を進めるための土壌づくりが必要であると筆者は考える。引き続き、国内外の動向を注視していきたい。


**本稿に関するご質問・お問い合わせは、下記の担当者までお願いいたします。**

NTTデータ経営研究所
社会システムユニット
コンサルタント
三藤 米利紗
E-mail mitsufujim@nttdata-strategy.com
Tel. 03-5213-4295


※7 20の分野は次のとおり。先端コンピューティング、先端在来型武器技術、先端エンジニアリング素材、先端製造、先端センサー、航空エンジン技術、農業技術、人工知能、自動化技術、バイオ技術、化学・生物・放射線物質・核（CBRN）軽減技術、通信・ネットワーク技術、データサイエンスおよびストレージ、分散型台帳技術、エネルギー技術、ヒューマン・マシン・インターフェース、医療・公衆衛生技術、量子情報科学、半導体・微細電子工学、宇宙技術。邦訳は日本貿易振興機構（ジェトロ）「米政府、重要・新興技術に関する国家戦略を発表」（https://www.jetro.go.jp/biznews/2020/10/64bfada743af53df.html）を参照した。

※8 European Commission “Horizon Europe”（https://ec.europa.eu/info/research-and-innovation/funding/funding-opportunities/funding-programmes-and-open-calls/horizon-europe_en）


# 海外技術移転リスクに打ち勝つ国際産学連携コンソーシアムのススメ

## ～参加者が全員得するプラットフォーム仕組みづくり～

NTTデータ経営研究所
先端技術戦略ユニット シニアマネージャー

**堀野 功**

HORINO ISAO

ニューヨーク州立大学バッファロー校卒業後、ロックフェラー公共政策大学院を経て、大阪大学大学院国際公共政策研究科（単位取得退学）。大手自動車部品メーカー、科学技術・学術政策研究所等を経て、2017年からNTTデータ経営研究所にて、産学連携、知財経営、ベンチャー支援等のプロジェクトに取り組む。

### 1 はじめに

一国の安全保障を適切に維持する上で、技術革新（イノベーション）は不可欠である。特に20世紀において、各国ともに安全保障を確保するために莫大な研究開発費を様々な技術領域に戦略的に投資し、それらの投資はイノベーションの向上に寄与してきた。例えば、実社会で活用されている技術の例を挙げると、①船舶などの位置を確実に把握する即位システム（GPS）、②世界中に広がる米軍基地などを分散型ネットワークで繋げるARPANET（インターネット）、③人工知能研究から生まれた音声認識ソフト（Siri）などは、全て米国国防高等研究計画局（DARPA）の研究プロジェクトから生まれた。また、宇宙開発は米国と旧ソ連の冷戦が結果的に宇宙空間におけるイノベーションに貢献したといっても過言ではない。

本稿では、安全保障とイノベーションの関係性は、20世紀型の「国内産官モデル」から、21世紀型の「国際協働モデル」に移行していることを、米国などの事例により示したい。特に、国際協働モデルでは、国境を超えた産学官連携（オープンイノベーション）が重要視されている。そして最後には国際協働モデルにおける人材マネジメントなどについても提議したい。

### 2 国際協働モデル

まず、「国内産官モデル」について定義する。「国内産官モデル」とは、一国の安全保障を最大限に維持するために、一国の政府が中心となり国内の産業（主に重工業）の技術革新を促進するモデルである。一例として、輸送機およびレーダーなどに係るイノベーションが挙

NTTデータ経営研究所
先端技術戦略ユニット　主任

**浅井 明**

ASAI AKIRA

同志社大学大学院博士課程修了、松下電器産業（現パナソニック）にて半導体デバイスの研究開発や通商産業省（当時）の外郭団体にて半導体系国家プロジェクト運営を担当。研究企画に携わった後、同社知財部門に異動しR&D部門全体の知財戦略、産官学連携契約等を担当。2019年からNTTデータ経営研究所にて、大学知財の支援や半導体関連プロジェクトに従事。博士（工学）、修士（経営学）。

NTTデータ経営研究所
先端技術戦略ユニット シニアコンサルタント

**渡辺 光美**

WATANABE TERUMI

大手総合化学メーカーのR&D部門にて研究開発、技術戦略立案、産学連携プロジェクト、海外拠点立ち上げ等を担当した後、2020年から現職。5G・半導体分野を中心に、幅広いテーマのプロジェクトに取り組む。


げられる。当該モデルでは、重工業産業を中心として経済的勢力の連合体が組成されるケースが多い。一方、「国際協働モデル」とは、一国の安全保障を他国とともに維持するために複数のステークホルダーが協働し、国内外の産業の技術革新を促進するモデルである。後者においても、一国の安全保障が最も重要視されるが、他国の企業等を巻き込むことにより、経済的機会損失コストを最大限に上げることが特徴である。機会損失コストを引き上げることで、現状（status quo）から外れることに（各ステークホルダーが）メリットを感じないため、安全保障が維持される。企業の経済活動にとっても、安全保障維持は重要な要因なのである。

「国内産官モデル」から「国際協働モデル」に移行した一例として、米国の国際産学官連携コンソーシアムであるISMI（International SEMATECH Manufacturing Initiative）の事例を紹介する（図1）。ISMIは1980年代に米国半導体業界組織であるSIA(Semiconductor Industry Association)からSEMATECHとして生まれた。当初の出資は産官共同出資であり、米国国防省（DARPA/ARPA）が半分、米国の半導体メーカーが半分出資し、本部はテキサス州オースティンに置かれた。1996年には連邦政府からの資金援助を返上すると発表し、参加企業のみの運営に変わった。全米の大学等にSEMATECH Centers of Excellence（SCOE）を立上げ、米国における半導体関連技術の基礎研究の発展にも貢献した。1980～90年代のSEMATECHは連邦政府と国内企業が連携して半導体業界の底上げに促進しており、「国内の産官モデル」と言える。

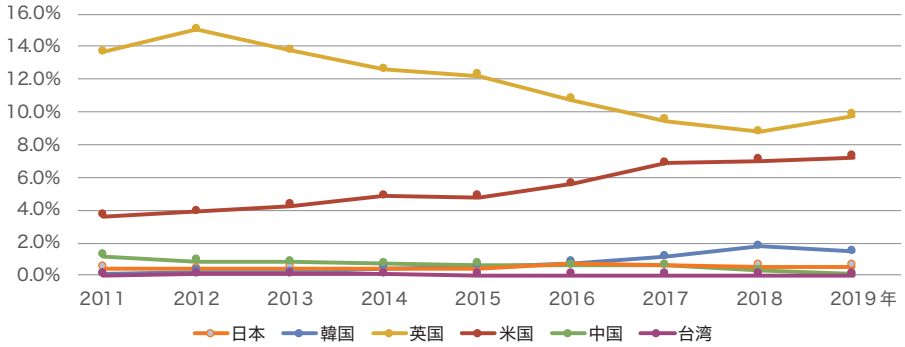
一方、2000年台になると、海外メーカーの当該コンソーシアム参加増加に伴い、SEMATECHは名称に@「International」を付けたISMIに変更した。2010年には本部をニューヨーク州に移し、当該コンソーシアムは海外メーカーを次々と巻き込んでいく。事務局はニューヨーク州立大学機構（CNSE）が担っており、ニューヨーク州を半導体開発のグローバル拠点にすることに成功した。海外メーカーにとってISMIは魅力的である。なぜなら、関連プロジェクトや莫大な研究整備などを参加メーカー間で利用できるためである。また、最新の研究動向を大学や他社の研究者などと議論することができる。

図1｜ 半導体コンソーシアム形態の推移


出所｜ NTTデータ経営研究所にて作成


堀野 功
渡辺 光美
浅井 明

図2｜ R&D国内総支出に対する外国企業負担比率の推移




出所｜ OECD Science, Technology and R&D Statistics database/Gross domestic expenditure on R&D by sector of performance and source of funds（2022年1月20日時点）各国データを基にNTTデータ経営所作成

一方で、ISMIで創出された研究成果（特に、特許などの知財財産）は基本的には運営組織であるニューヨーク州立大学機構（CNSE）に帰属される。このように、ISMIはニューヨーク州、ニューヨーク州立大学、国内外の半導体メーカーなどが集結し、半導体研究のグローバル発展に寄与した「国際協働モデル」と言える。

ISMIの例で分かるように、産業の国際競争力を強めるためには国内外を問わず一流の企業・研究開発機関・研究者との連携強化が不可欠である。しかしながら、我が国においては、外国企業からの投資金額が諸外国と比較し低く、外国企業との連携が活発であるとは言えない状況である（図2）。

安全保障の観点から、大学においては、関係法令遵守、リスクマネジメントのための組織的なマネジメント体制の整備などが求められる。企業においては、外国からのエンジニアなどによる技術流出は妨げられないとの前提で、知的財産による保護や事業として成立するための仕組みを担保し、他国では収益化できないようにするなど、企業自体の知財経営強化が求められる。

## 3 大学におけるイノベーションの創出と人材育成

「国際協調モデル」では、外国からの研究者やエンジニアを通じた技術のスピル・オーバーが懸念されている面もある。一方、米国では多くの留学生が長年の米国発イノベーションを支えている。米国NSF（National Science Foundation）によれば、2015年の米国の理工系大学院入学者は約68万人であり、うち約24万人（約36%）が留学生である。[※1] 同年の我が国の外国人留学生の比率は約19%であり、[※2] 米国の研究室が多くの留学生によって支えられていることが示されているが、それでも米国のイノベーション・システムは揺るがず、新技術新産業を創出し続けている。イノベーションは「単発」ではなく「継続性」が必要であり、大学などの研究機関が多様性を許容し（研究成果というゴールに向けて）協働していることが分かる。

留学生による技術のスピル・オーバーとイノベーション創出速度との関係については、イノベーション創出速度が早ければ国際競争力は維持されるであろう。留学生によって創出された知的財産等が蓄積され、米国は世界で最初にそれらの研究成果を活用できる立場となっている。何故ならば、知的財産等は国籍に関わらず、研究者やエンジニアが在籍している組織（米国の大学など）に帰属する傾向が高いからである（知財の取扱いについては、当該研究のファンディングエージェンシーの規程に依存する）。また、別のNSFの統計によれば、2005年から2015年の留学生の博士取得者の米国内滞在率は約75%である。特に留学生の多い中国およびインドからの留学生の米国内滞在率は約90%と高い数値となっており、[※3] 留学生が米国内でのイノベーションの創出および米国産業への展開に寄与している。そのため、外国からの優秀な留学

※1 https://nsf.gov/statistics/2018/nsb20181/report/sections/higher-education-in-science-and-engineering/graduate-education-enrollment-and-degrees-in-the-united-states
※2 https://www.e-stat.go.jp/stat-search/files?page=1&layout=datalist&toukei=00400001&tstat=000001011528&cycle=0&tclass1=000001078255&tclass2=000001082515&tclass3=000001082516&tclass4=000001082517&tclass5val=0 より計算

生を自立的に留まらせる環境づくりも重要である。例えば、企業は海外からの優秀な留学生を早めにリクルートする必要がある。言葉の問題については、留学生は現地法人等で採用すれば問題ない。

## 4 おわりに

世界の緊張関係は、各国の戦略的な科学技術への投資を呼び、イノベーションの引き金になってきた。我が国では、企業内の新製品の開発や既存製品の改良に用いることによりイノベーションを成功してきた。インターネットで全世界がつながった今では、一国の企業のみでのシェア拡大は難しい傾向である。場合によっては、海外の競合他社とも戦略的に協働（もしくはM&A）し、企業間国際連携によるイノベーション創出も必要となってくる。その場合、外国の研究者・エンジニアなどによる国外への技術のスピル・オーバーを危惧するよりも、国際協調（多様性）によるイノベーション創出の加速および留学生の国内定着を試みた方が、我が国にとって良い結果が得られる可能性が（米国の事例により）示唆されている。費用（コスト）と便益（ベネフィット）の分析に例えると、イノベーション加速による便益が技術スピル・オーバーによる費用を大幅に上回ると解釈できるのだ。そのため、ISMIのように、企業は大学という「ハブ」を通じて、海外企業とつながる可能性が広がる。

最後に、コロナ禍はバーチャルなボーダーレスコミュニティを加速させている。スマートフォンさえあれば、世界中のどこにいようが、世界中の誰ともつながることが出来、情報がリアルタイムに取得できる。例えば、バーチャルでのコミュニケーションが盛んな昨今では、テレワークでの国際協働が容易となる。世界中の研究者とWeb会議などでどんどんコミュニケーションを実施してみるのも効果的かもしれない。そのためのプラットフォームも必要かもしれない。これにより、そう遠くない将来、（バーチャル世界での共同研究を可能とする）「e-国際協働モデル」が産まれるであろう。

**本稿に関するご質問・お問い合わせは、下記の担当者までお願いいたします。**

NTTデータ経営研究所
先端技術戦略ユニット
シニアマネージャー
堀野 功
E-mail horinoi@nttdata-strategy.com

※3 https://www.nsf.gov/statistics/2017/nsf17306/report/international-students-staying-overall-trends/stay-rates-country-of-origin.cfm


# 特許出願の非公開化時代の到来と新たな研究開発戦略

## ～鍵となりうる「デュアルユース」とリスク回避～


NTTデータ経営研究所
産業戦略ユニット
マネージャー

**江木 淳**
EGI JUN

化学メーカーの創薬研究部門を経て、現職。AIPE認定知的財産アナリスト。化学・ライフサイエンス領域×知的財産に関する調査研究・コンサルティングを得意とし、技術動向調査や医療分野の研究開発振興のための施策調査、ニーズ・シーズ・マッチング、異業種から新規事業領域への参入支援を手がける。直近では大学の有望な研究成果の発掘・活用支援や、民間企業向け新規ビジネス創出支援を担当。


### 1 はじめに

岸田政権が経済安全保障を重点政策として掲げて以来、有識者会議を中心に多くの議論がなされている。令和4年2月10日現在、経済安全保障法制に関する有識者会議からは「サプライチェーンの強靭化」「基幹インフラの安全性・信頼性の確保」「官民技術協力」「特許出願の非公開化」の4分野が提示されており、この結果を受けて、政府は重要技術の守秘義務の規定も定めるとされている。

本稿では、この4分野の中で「特許出願の非公開化」に特に焦点を当てて、特許出願の非公開化が今後の研究開発活動にどう影響を与えるかを考察し、特に民生用と軍事用の両方の用途へ結びつくデュアルユース性※1を予見する方法についての私見を述べる。

### 2 特許出願の非公開化とその論点

一般的に、特許出願された発明は出願後1年6ヵ月経過後に公開される。その理由は、出願技術をいち早く公開することによって、産業の発展を促すためとされている。特許を出願した出願人はその発明の内容を公開することの対価として、特許登録された発明に関する独占権を与えられる。

一方で、公開されること自体がリスクになる発明も存在する。例えば、防衛技術や国家機密に相当する機微情報を含んだ発明についての公開がなされてしまうと、他国への技術流出や大量破壊兵器をテロリストが開発することにつながる可能性がある。このような技術情報の特許出願を非公開化することで、技術流出などを防いでいこうという取り組みの一つが「出

※1 デュアルユース：一般的には複数の使用用途や目的を前提とする技術を指す言葉である。本稿では民生用と軍事用の両方に利用可能な技術を「デュアルユース」、他方、軍事用としてのみ利用される技術を「シングルユース」と呼称する。

医療系メーカーで研究職および知的財産職を経験し、さらにシンクタンクの研究員を経て、2020年より現職。現在は老人保健関連や介護ロボットおよび医療機器分野における調査研究に携わる。

NTTデータ経営研究所
先端技術ユニット
シニアコンサルタント

**古川 和良**
FURUKAWA KAZUYOSHI

願特許の非公開化」である。

かつて我が国にも類似の制度が存在しており、軍事上機密性を要する発明が秘密特許として非公開とされていた。しかし、戦後の昭和23年にこの制度が廃止され、それ以来、特許出願された発明は例外なくすべて公開されることになっている。その一方で、海外に目を向けてみると、機微技術に関する特許出願の非公開化は比較的一般的である。G20諸国の中で同様の制度がないのは日本とメキシコ、アルゼンチンのみとなっており、他の国では、多くの機密情報に関する特許出願は非公開とされている。諸外国で機微技術についての特許出願が非公開化されている一方で、我が国においては例外なく公開されている状況は好ましいとは言えず、早急に是正していく必要がある。

現在、特許出願の非公開化は、経済安全保障法制に関する有識者会議において特に①制度新設の必要性・制度の枠組み、②対象にすべき発明のイメージ、③機微発明の選定プロセスの在り方／④選定後の手続と漏えい防止措置、⑤外国出願制限の在り方／⑥補償の在り方について議論されている。[※2]

## 3 特許出願の非公開化と研究開発活動への影響

特許出願が発明の独占のために行われることを踏まえると、特許出願の非公開化が研究開発活動に与える影響は少なくない。例えば、検討を進めている研究開発が特許出願非公開化の対象となってしまった場合、発明の成果を活用したビジネスを行うことへの制限がかかってしまうためである。非公開化によって得られなくなった特許収入を国が補償する旨の報道もあるが、クロスライセンスやアライアンスによるビジネス展開を踏まえると、非公開化の影響は特許収入に留まらず、特許収入の補償だけでは発明者が受ける制限を十分に補えるとは言えない。

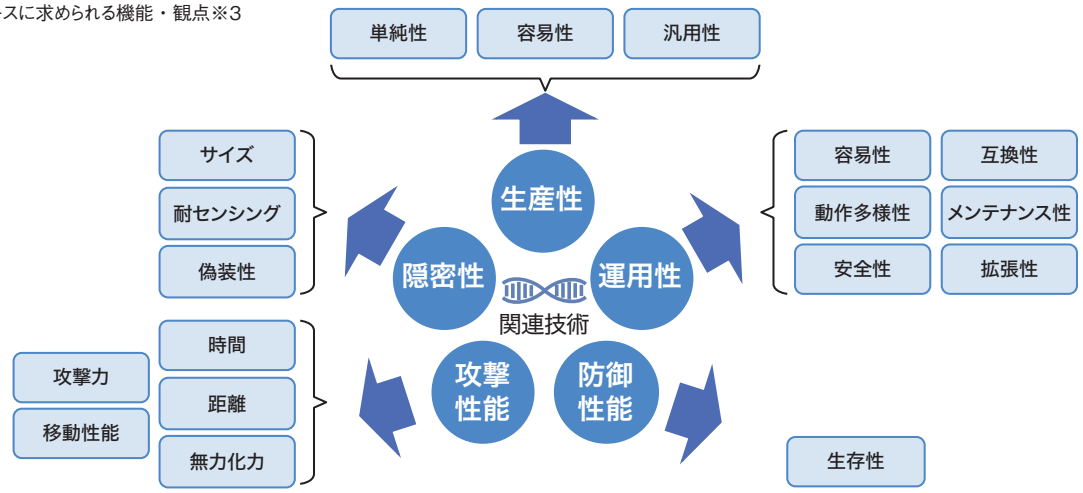
では、特許出願の非公開化の対処となりうる発明としてはどのようなものがあるだろうか。先述の経済安全保障法制に関する有識者会議によると、「非公開の対象となる発明の選定に当たっては、公になれば我が国の安全保障が著しく損なわれるおそれがある発明に限定することに加え、経済活動やイノベーションに及ぼす影響を十分考慮するべきである」とされており、研究開発への影響は最小限にとどめるように配慮されているようである。この中でも、核兵器の開発や武器のみに用いられるシングルユース技術については積極的にその対象とすべきとされている。一方、民生用と軍事用の両方の用途が想定されるデュアルユース技術については、経済活動やイノベーションへの影響が想定されるため、国費による委託事業の成果である技術や、防衛等の用途で開発された技術、あるいは出願人自身が了解している場合などを念頭に、支障が少ないケースに限定するべきと提言されている。

以上を踏まえると、デュアルユース技術については、出願人に対し、事前の通知なしに非公開の対象とすることは想定しにくいと考

※2 https://www.cas.go.jp/jp/seisaku/keizai_anzen_hosyohousei/dai3/teigenkossi4.pdf


江木 淳
古川 和良

図1｜ デュアルユースに求められる機能・観点※3




| | 性質・性能 | 説明 |
|---|---|---|
| 生産性 | 単純性（シンプルさ） | 部品・工数が少ないこと |
| | 汎用性 | 部品・生産治具が汎用であること |
| | 容易性 | 精製や組立に必要なスキルが高くないこと |
| 運用性 | 動作環境の多様性 | 陸・海・空(宇宙)フィールドにおける温度(差)、可視範囲、気圧、重力など物理制約 |
| | 容易性 | 運用に必要なスキルが高くないこと |
| | 安全性 | フェイルセーフ、フールプルーフの仕組みがあること |
| | メンテナンス性 | 機能維持にスキル・時間・コストがかからないこと |
| | 互換性 | 他の機材の部品が流用可能なこと |
| | 拡張性 | 必要な機能が(無改造で)アドオンできること |
| | UI | 人の認知・理解・反応に働きかけをする仕組み |

| | 性質・性能 | 説明 |
|---|---|---|
| 隠密性 | 物理的な大きさ | 各種センサからの発見されにくさ |
| | 光学 | 可視光線、不可視光線での捕捉可能性 |
| | 電波 | 距離分解能 |
| | 熱 | 排出熱処理 |
| | 静音性 | 静音化技術 |
| | 偽装性 | 敵性兵器に「見た目を化ける」 |
| 攻撃性能 | 作戦行動範囲（時間） | 哨戒・待機・攻撃・帰投(待機)サイクルが長いほど捕捉・撃滅可能性が高まる |
| | 作戦行動範囲（距離） | 作成行動範囲(時間)　×速度 |
| | 打撃力 | 敵性戦力に対するインパクト |
| | 無力化力 | 敵性戦力の構成要素に対するインパクト |
| | 運動性能 | 空間における移動能力とその安定性 |
| 防御性能 | 生存性 | 目的達成の後に機能が発揮できる状態であること。 |

出所｜ 公開情報を基にNTTデータ経営研究所で作成

えられる。例えば、出願人が自己の出願の取り扱いに関し予見性を確保できることや出願手続きから離脱できることが検討されている。とはいえ、出願人自身が、事前に非公開化の可能性があることを念頭に置いておく必要があるだろう。

## 4 どういった技術がデュアルユース技術となりうるか

そもそもデュアルユース技術としてはどのような事例があるのか。公開情報を基に調査すると、例えば、①無人飛行機や自動運転技術は沿岸警備や国境警備、重要施設警備、施設のメンテナンス、②蓄電池は有事においても平時に活用する配電網から切り離したマイクログリッドの形成、③人工知能技術はロボット兵器から効率的な作戦立案、④医薬品や半導体の製造技術は有事に必要な物質や製品の生産・製造を行うための拠点として検討されている。※3

これらに関連する技術がデュアルユース技術として取り扱われる

※3 各種ホームページを基にNTTデータ経営研究所作成

可能性が高い。ここで、これらの事例をベースにデュアルユース技術の要件となる機能や観点を深掘りしてみよう。公開情報から得られた軍事用途をベースに検討すると、有事に何かを生産・製造する「生産性」、平時とは別のコンディションでも技術を容易に活用できる「運用性」、相手に気付かれずに行動を行うことを目指す「隠密性」、相手に何かしらの危害を与える「攻撃性能」、相手からの攻撃を防ぐ「防御性能」のような観点が挙げられる（図1）。

## 5　デュアルユース性を予測するには

では、自身が企画している、あるいは実施している研究開発がデュアルユース性を帯びる可能性があるかを検討することはできるのだろうか。厳密には軍事技術やデュアルユースについての有識者の助力を通して確認する必要があるが、特許情報を活用して簡易的に検討することもできる。

特許情報は発明の名称や発明の内容、実現する機能や用途、実施例などから構成されるものであり、複数の特許情報を組み合わせて統計分析することで、調査対象とするシーズの用途展開性や、シーズホルダーと相性の良いパートナーを探索[※4]するような際に活用される。

デュアルユース性の予測は、特許情報を活用した分析の中で用途展開性について検討する方法（用途展開検討手法）を応用して実施することができる。具体的には、調査対象とするシーズと機能・用途面で類似性の高い特許母集団を作成し、その母集団に対して図1で示したデュアルユース性と一致するかを簡易的に確認する。以下にその手法を示す。

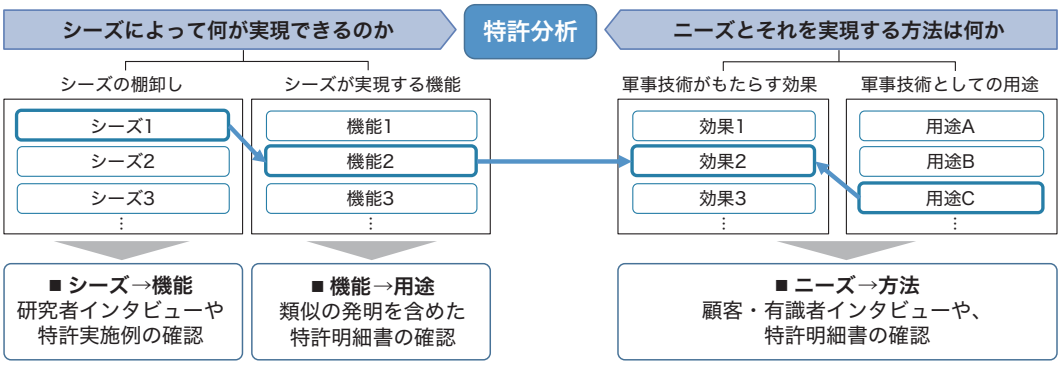
1　社内にあるシーズの機能を棚卸しする。

2　1の機能をベースとして特許検索を行い、社内シーズと類似性の高い特許を抽出し、特許母集団とする。

3　2で作成した母集団に対して、デュアルユースに係る用途やデュアルユースに求められる機能が実現できるかについて分析を行う。

4　3の結果を基にデュアルユース性について判断する。

図2｜ 特許情報を活用したデュアルユース性の検討




出所｜ NTTデータ経営研究所で作成

※4　https://www.nttdata-strategy.com/services/business/IPinformation.html


江木 淳
古川 和良

このプロセスの中で、特に難しいのが1である。理由としては、シーズが持っている機能の中には、シーズの所有者自身が気づいていない潜在的な機能も多いためである。このような潜在的な機能を抽出するためには、研究開発の際の気付きを足がかりとして機能に結びつけることや、シーズやその関連技術に関する特許に記載されている発明の効果や実施例を参考に抽出することが効果的である。

この方法を用いることのメリットとしては、シーズの機能やニーズを解決するための方法を客観的に判断することができる点である。インタビューではインタビュイーの常識や思い込みによって得られる情報が偏ってしまう可能性がある。その一方で、特許情報は、実験データや先行特許などの根拠のある情報で構成されており、複数の出願人の特許情報を統合することで、ある程度の客観性を担保することができる。また、特許情報には実験データや用いている素材の情報、素材によってもたらされる効果などの技術情報が数多く含まれている。もちろん、この特許分析だけでは精度の高い予測は難しいが、特許分析の情報から仮説を立て、必要に応じて有識者へ仮説をぶつけることでデュアルユース性についての予測精度をあげることができると考えられる。

## 6 おわりに

本稿では、特許出願の非公開化とその論点や研究開発活動への影響を起点として、特にデュアルユース性の予測方法について私見を述べた。研究開発を行っているシーズがデュアルユース性を帯びていたとしても、即座に研究開発やビジネス化の妨げになる可能性は少ない。しかし、現在の研究開発では複数のプレーヤーとの協業を通して行うケースが増えていることや、異業種参入のようなケースが増えてきている。このことを考慮すると、自身が持つシーズ、あるいは協業先が有するシーズがデュアルユース性を帯びているかの仮説を持つことは、その後の研究開発やビジネス化のリスクを低減することにつながると考えられる。また、軍事技術に係りそうな部分については分割出願を行うなどの方法で、ビジネス等への弊害を事前に防ぐ手立てを講じることもできる。

特許出願の非公開化はこれから制度化されていく段階ではあるが、研究開発への影響を踏まえて、先手を打って動いていく必要があるのではないだろうか。

**本稿に関するご質問・お問い合わせは、下記の担当者までお願いいたします。**

NTTデータ経営研究所
先端技術ユニット
シニアコンサルタント
古川 和良
E-mail furukawak@nttdata-strategy.com
Tel. 03-5213-4171


# DX推進がパンデミックから地域医療を守る処方箋


NTTデータ経営研究所
ライフ・バリュー・クリエイションユニット
アソシエイト・パートナー

**北野 浩之**
KITANO HIROYUKI

病院のコンサルティング会社、会計系ファームを経て現職。医療から健康・予防領域における事業戦略立案、新規事業化支援、PoC支援、行動変容モデルや個別化など次世代アプローチ手法の創出支援を中心にプロジェクトを推進。また「健康×街づくり」をテーマに、街づくりなどに取り組んでいる。



**概要**

新型コロナウイルスの蔓延による医療サービスの提供体制の逼迫により、わが国にとって医療サービスの継続性確保が安全保障上、極めて重要な政策であることが明らかになった。

東日本大震災以来、医療機関のBCP対策の重要性は強く意識されてきたものの、パンデミックでは期間が長期に及ぶこと、地域(国)全体で医療の提供体制が逼迫すること(周辺から支援が受けられないこと)などから、通常の震災対策としてのBCPでは限界がある。

本稿では、パンデミック下における医療サービスの継続性確保のための重要な解決策は、医療機関および医療圏全体のDXの推進であることから、今後の医療分野におけるDX推進の意義について述べる。


## 1 パンデミックの医療機関に対する影響

### (1) パンデミックの歴史

コロナウイルスは、2019年12月以降全世界で猛威を振るい、全人類の生活に大きな影響を与えている(感染者数3・8億人、死亡者570万人[※1])が、人類がウイルスの脅威にさらされた事例は20世紀以降で少なくても4度あった。中でも最も人類に大きなダメージを与えた例は、1918年~20年のスペイン風邪で、3年の間に5億人が感染、死亡者は1億人を超えていたとされる[※2]。1978年以降は、鳥インフルエンザによるパンデミックの危険性がたびたび指摘され、2009年にはヒトヒト感染の事例が確認されたが、幸いなことに急速な感染拡大の段階

※1 2022年2月6日時点
※2 https://ja.wikipedia.org/wiki/%E3%82%B9%E3%83%9A%E3%82%A4%E3%83%B3%E3%81%8B%E3%81%9C#cite_note-Spreeuwenberg-7


北野 浩之
土屋 裕一郎

自治体病院、外資系医療機器メーカー、コンサルティングファームを経て現職。デジタルを活用した事業開発・事業構想策定、ワークショップを活用した伴走型課題解決、行動変容支援などを担う。ビジネス（事業化）×リサーチ（研究）×サイト（現場）の視点でユーザー価値の最適化を支援。博士（医療技術学）、MBA、診療放射線技師。

NTTデータ経営研究所
ライフ・バリュー・クリエイションユニット
マネージャー

**土屋 裕一郎**
TSUCHIYA YUICHIRO

には至らなかった。

### (2) コロナ禍による医療機関への影響

国内でのコロナ感染患者は2020年の1月28日に認められ、30日にはヒトヒト感染が確認されたと厚労省より発表。その後、感染者数の拡大を受けて、緊急事態宣言などによる都市機能の封鎖などが行われ、全ての国民の生活に重大な影響を与え続けているが、特に大きな影響を受けているのが医療機関（と医療従事者）である。新型コロナウイルスが指定感染症2類であるため、診察、入院などの対応ができる医療機関が限られ、少ない対応医療機関に、多くの患者が集中した。その結果、医療提供体制のひっ迫などが起こる事態となっている。

これまで医療機関は、東日本大震災などを契機に、医療提供サービスの継続性確保の観点で様々な備えをしてきた。例えば、電源の二重化や貯水槽設備の増設などのライフラインの損失に対する対策、薬品や医療材料の損失補充対策として一定期間の在庫の確保（余剰在庫）や複数取引先との契約、医療機器の破壊やネットワークの破損、紙データ、電子媒体の破損などに起因するデータの消失に対する対策として耐震対策や設備の冗長化・情報のデジタル化やバックアップの取得などが挙げられる。

### (3) パンデミックの特殊性（震災との相違点）

このような備えがあったにも関わらず、現在、医療機関に大きな影響が生じている。これは、通常の震災などの災害とパンデミックとの相違があったためと考えられる。

具体的な相違点は、①影響が及ぶ期間が一時的ではなく長期に及ぶこと、②災害の範囲が広範（今回は全世界規模）に及ぶこと、③物理的な損傷を伴わないため、既存の提供体制を維持することを前提に対策が取られること、である。①②の観点では、地震などの災害の際には国内の医療従事者の支援、物資供給などを受け、災害直後の混乱期を乗り越えることができるが、パンデミックでは外部からの支援が極めて困難となる。また③では、日本の特徴である多くの病床数と民間医療機関が医療を担う体制を維持したまま対策を取ろうとしたため、ガバナンスが効かず、医療リソースを集中させるなどの対応が取れなかった。仮に大きな地震発生時であれば、医療機関のハードが損傷することで既存の体制を取ることをあきらめ、早々にドラスティックな対策を取る可能性がある。しかし上記のような事情が重なり、我が国における医療提供体制は大きな影響を受けている。

図1｜ 過去のパンデミック

| 名　称 | 時期（年） | 死亡者数 |
|---|---|---|
| ロシア風邪 | 1889-1890 | 100万人～ |
| スペイン風邪<br>A/H1N1 | 1918-1920 | 1億人 |
| アジア風邪<br>A/H2N2 | 1957-1958 | 100万人<br>～400万人 |
| 香港風邪<br>A/H3N2<br>A香港型 | 1968-1969 | 100万人<br>～400万人 |
| 新型<br>インフルエンザ | 2009 | |
| 新型コロナ<br>ウイルス | 2019-2022<br>(継続中) | 570万人 |

出所｜ NTTデータ経営研究所にて作成

## 2　解決策の提示（DXの推進による解決）

次にパンデミックへの対応の反省に立ち、国民の安全保障の観点から、今後の同様な事態において適切に医療提供体制を維持・継続するための方策を、国内の取り組み事例を交えつつ考察する。

### (1)　検討方針

被害が長期化、広域化する中で、限られたリソース（医療従事者のほか、もの、情報などを含む）の効率的な活用のために、DXを推進することが必要であるとの仮説に基づき、(2)以下で、経営資源である「ヒト」「モノ」「ジョウホウ」の観点で検討を行う。

### (2)　ヒトの効率化

医療サービスの主体は「ヒト」である。現在コロナ感染の第6波による感染者数、濃厚接触者の増加により、医療従事者の出勤停止が相次ぐ事態となっている。パンデミックでは長期化という特徴があるため、少ない人員でサービスを維持するための方策が必要であるが、オンライン診療の実用化が進むなど、すでに政策的な対応が見られる。

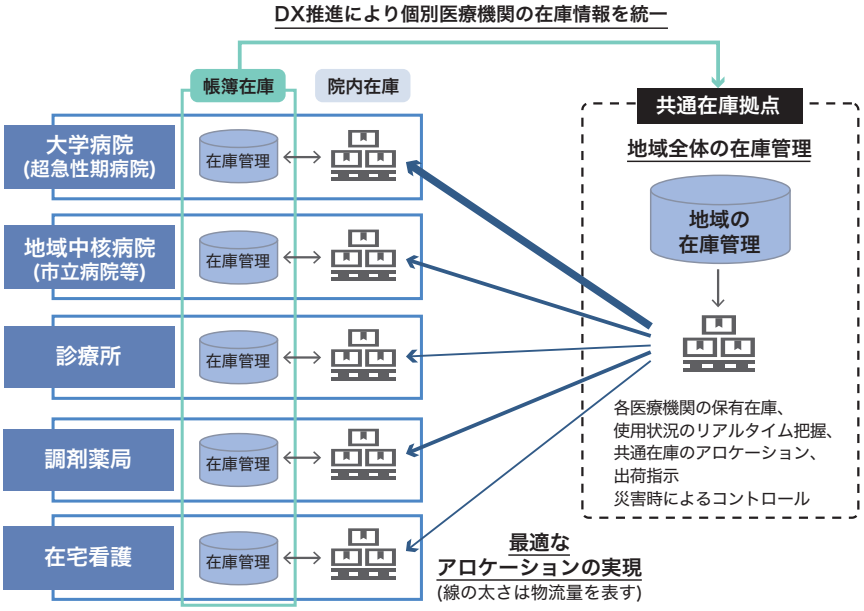
昭和大学では、通常の診療はもちろん、ICU（集中治療室）の遠隔管理として、病院と離れた場所にある支援センターをネットワークでつなぎ、支援センターにいる専門医が、病院のICU患者の様子をモニタリングできる取り組みを行っている。また、長野県伊那市では、モバイルクリニックとして、医療機器と看護師を乗せた専用車両が住民宅を訪問。医師が遠隔地からビデオ機能を使ってオンライン診療を行い、看護師がその指示に従って検査や処置を施しており、僻地の患者に医療を提供している。また、慶応義塾大学病院（産科）では、オンライン妊婦検診として、MeDaCa Proのビデオ通話機能と、中部電力のプラットフォームを介して体重、血圧などのデータを医師と共有し、診察に活用。ハイリスク妊婦と院内感染のリスクを同時にヘッジできる取り組みを行っている。医師の診察などは感染リスクが極めて高いシーンである。このリスクをヘッジするため、オンライン診療の活用への期待は大きい。診療報酬制度上も点数化されるなど、オンライン診療の間口は広がりつつあるものの、まだ導入する医療機関のメリット（主に診療報酬）が少ないこと、ユースケースが限られること、必要な医療行為ができないことなどの課題も多い。少なくとも最後の課題については、DXの推進により解決可能であり、医療業界に広くオンライン診療が普及することにつながると考えられる。

### (3)　モノの効率化（物流）

医療サービスは想像以上に「モノ」が必要である。モノがなければあらゆる処置・処方ができない。パンデミックの特徴である長期化は、製造工程における人員不足などによる供給能力の低下や物流段階での遅延などを引き起こすことで医療提供体制に影響を与える。震災時には、被災を免れた地域から物資の供給などを得られるが、パン


北野 浩之
土屋 裕一郎

図2｜ DXを活用したモノの効率化




出所｜ NTTデータ経営研究所にて作成

デミック下では国内はもとより海外からの供給も止まる可能性がある。限られた資源（製薬や医療機器、消耗品などの医療用資材）を、どのように最適に配分するかが重要な課題になる。

この解として、モノの管理を単独医療機関ではなく、地域単位（例えば2次医療圏単位）で行うことが想定される。限られた物資（薬剤や医療機器など）の優先順位の設定を地域全体で行い、そのモノを使える人員がいる医療機関に集中的に投下し、患者を集約することで、継続的な治療を実現できると期待される。そのために必要となる仕組みが、現在は医療機関ごとに管理している在庫管理機能を、物流を担う医薬品・医療機器卸とつなぐという仕組みの導入である。医療機関の在庫管理は、RFID（Radio Frequency Identification：近距離無線通信を用いて、ID情報などのデータを記録した専用タグと非接触による情報のやりとりをする技術）やSPC（Statistical Process Control：統計的工程管理）による発注自動化など、DXが進みつつある分野である。この営みをさらに地域の卸（物流）システムと統合することで、それぞれの医療機関が持つ在庫を非常時に一元的に管理可能な仕組みとなる。これによりハード、ソフト両面を見て医療提供体制を維持するために最適なモノの配分が実現する。

なお、医療機関の在庫と地域の物流システムとの連携は、災害時のみではなく平時でも医療機関に効果がある。上記連携を行うことで、在庫管理業務が自動化、効率化するとともに、在庫点数が減少し、キャッシュフロー改善が期待できるからだ。

### (4) ジョウホウの効率化（情報連携）

医療提供を支えるため、患者情報は必須である。前記の通り、パンデミック下において、オンラインで受診する際やかかりつけ医に行けないため初めての医療機関にかかる際など、検査が難しい状況も想定される。また、地震など物理的な損傷を伴う災害では、院内のサーバが損傷し、患者情報が消失してしまう事態もある。そこで、現在多くの医療機関が採用している院内サーバでの患者データ保管から脱却し、外部（クラウド）にバックアップをとり、災害時のデータ損失リスクを大幅に削減して医療の継続提供を担保する方策が考えられる。

例えば、独立行政法人地域医療

機能推進機構（以下ＪＣＨＯという）は、ＪＣＨＯクラウド・プロジェクトとして、２０１５年７月から10病院を対象としたクラウド型医療情報基幹システム（電子カルテ・医事会計）の構築を進め、複数の病院で運用を開始している。このシステムは、院外のデータセンターに設置されたＪＣＨＯ専用の共有仮想サーバ上にクラウド型医療情報基幹システムを配備し、閉域データ通信ネットワークで院内の部門システムおよび本システムを操作する端末設備を接続して複数病院の診療業務を遂行するものである。ここでは、サーバを共有することによるシステムの構築および運用のコスト削減に加えて、病院業務データの均質化や活用などを視野に入れている。また、データセンターは東日本・西日本の二か所に設置し、両データセンターに同じ構成でシステムを構築することで、そのデータの相互バックアップを行っている。これにより、地震・津波・洪水などの広域災害発生時における患者情報の消失を防止すると同時に、災害時にも診療業務の継続を確実に遂行する体制を整えている。

さらに、クラウドのデータを地域内連携として、相互に閲覧できる仕組みの導入も必要である。現状では大学病院や急性期病院のカルテを診療所が閲覧できる仕組みの導入が多いが、災害時においては、診療所の持つ平時の患者データを、地域中核病院が参照できる仕組みが求められており、地域連携システムの発展が必要である。

## 3　最後に

このように医療業界のＤＸ化を通じて様々な課題からサプライチェーンを守ることは、結果的に国民に対して良質な医療サービスを提供するため（安全な暮らしを守るため）に必要不可欠であり、特に今回のパンデミックにより、強く求められていることが明らかとなった。ＤＸ化の推進は、通常の診療の品質向上や受診の効率化など、平時での医療機関、患者双方のメリットも大きい。今回の状況は極めて不幸な事象であるが、このことを契機として、医療業界のＤＸが進むことを願いたい。

**本稿に関するご質問・お問い合わせは、下記の担当者までお願いいたします。**

NTTデータ経営研究所
ライフ・バリュー・クリエイションユニット
アソシエイト・パートナー
北野 浩之
E-mail kitanoh@nttdata-strategy.com

社会基盤事業本部
ライフ・バリュー・クリエイションユニット
マネージャー
土屋 裕一郎
E-mail tsuchiyay@nttdata-strategy.com


# 経済安全保障から見た米中関係


NTTデータ経営研究所
グローバルビジネス推進センター
主任研究員

**岡野 寿彦**
OKANO TOSHIHIKO

上智大学法学部卒業後、NTTデータにてSE、法務を経験した後、中国郵便貯金システム構築プロジェクトマネジャー、北京現地法人経営、インド、東南アジアでの日系企業ITサポート事業開発責任者などを歴任。2011年より上海にて、人民銀行（中央銀行）直系企業グループとの資本提携に取り組み、合弁会社に経営陣No. 2としてで経営参画。2016年からNTTデータ経営研究所にて、中国における現地化、合弁経営やデジタルビジネスをテーマに、企業人視点での分析・発信に取り組む。早稲田大学ビジネス・ファイナンス研究センター「日中ビジネス推進フォーラム」研究員を兼務


わが国の経済安全保障を推進するうえで、米国と中国の経済安全保障政策に対する理解は不可欠である。本稿では、米国の米中経済・安全保障検討委員会（USCC）の2021年年次報告書に基づいて米国の経済安全保障政策を分析し、これに対する中国政府の方針・政策、特に情報・データのコントロールの取り組みを概観する。

## 米国の経済安全保障に関する動向：米中経済・安全保障検討委員会（USCC）の提言

### 1 はじめに

2021年11月、米国の米中経済・安全保障検討委員会（以下、USCC）は議会に2021年年次報告書を提出した。[※1] USCCは議会に設置された超党派の諮問機関で、そのミッションは、米中の経済通商関係が米国の安全保障に与える影響に関して調査分析し提言を行うことである。[※2] 激しく党派対立している米国議会であるが、中国に対しては厳しい姿勢で臨むというコンセンサスがある。USCCの年次報告書も中国への対決姿勢を明確に打ち出しており、米国の政治エスタブリッシュメントにおける中国を見る目の厳しさを伺い知ることができる。政治面においては、米国は中国を主要な競争相手と位置づけて強硬な姿勢を取っている一方、米国企業は中国を重要な市場としており、中国との貿易や中国への投資は堅調である。米国経済の中国経済への関与が強まることが米国経済や安全保障にリスクをもたらすことにUSCCは懸念を持っており、リスクに対処する様々な提言を行っている。

### 2 USCCの中国経済評価 ～国家による経済管理の一層の強化～

中国はコロナによる経済の落ち込みからいち早く抜け出したが、それは地方での支出拡大や企業への補助金によるもので、投資リターンの減少など中国経済の構造的問題の解決によるものではない。中国経済の構造的問題に関しては、中国指導部は経済の自由化によってではなく、国家主導の技術開発や企業に対する政府管理の強化によって解決を図ろうとしている、とUSCCは評価している。

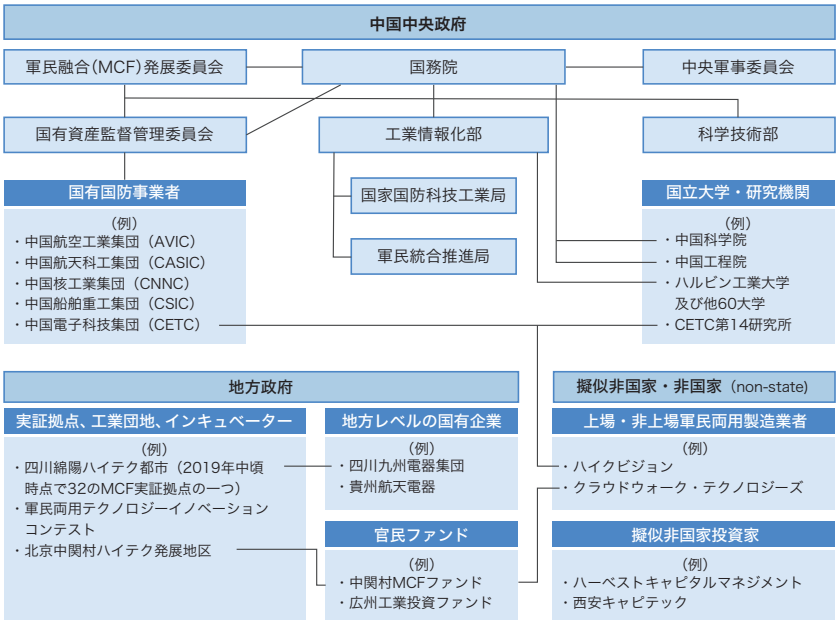
※1 USCC（U.S.-China Economic and Security Review Commission）：https://www.uscc.gov/annual-report/2021-annual-report-congress
※2 USCCの組織や委員については、経営研レポート「米中経済・安全保障検討委員会と2020年年次報告」（https://www.nttdata-strategy.com/knowledge/reports/2021/0817/）を参照されたい。

NTTデータ経営研究所
社会システムデザインユニット
グローバルビジネス推進センター(兼務)
シニアスペシャリスト

**新開 伊知郎**
SHINKAI ICHIRO

慶応義塾大学大学院法学研究科政治学専攻修士課程修了後、NTTデータ通信株式会社(現 株式会社NTTデータ)に入社。社内シンクタンクにて、価値観に基づくライフスタイル分析、IT時代の政治・行政への市民参加「eデモクラシー」、技術革新への対応手段としての純粋持株会社、社会マクロトレンド分析等の調査・研究活動に従事。2018年4月にNTTデータ経営研究所に入社、アジア諸国の経済・社会情勢調査、諸外国のIT政策調査、ITSに関する国際周波数標準化活動などに従事。1993年～1995年　スタンフォード大学経済政策研究センター(CEPR　現SIEPR)客員研究員、2016年～2018年戦略国際問題研究所(CSIS)客員研究員


図1｜ 中国軍産エコシステム




出所｜ 2021 REPORT TO CONGRESS OF THE U.S.-CHINA ECONOMIC AND SECURITY REVIEW COMMISIONの図を元に、NTTデータ経営研究所で作成

### (1) 国家主導の技術開発

USCCは、国家主導の技術開発という点では、合成生物学、ニューモビリティ(自動運転や新エネルギー、ゼロエミッションといった技術とカーシェアリングといったビジネスモデルの双方を含む)、クラウドコンピューティング、デジタル通貨(デジタル人民元)への取り組みを注視している。前者3つは今後の有望な産業において中国が優位に立とうとするもので、米国の脅威になるものと評価している。最後のデジタル人民元については、短期的には米国の脅威になるものではないが、長期的には基軸通貨である米ドルの地位を掘り崩し、金融制裁の有効性を損なう恐れのあるものとして注意を促している。

### (2) あらゆる企業に対する国家管理の強化

中国政府は様々なチャネルを通じて企業をコントロールし、企業の意思決定を政策目標に合致するよう誘導している。中国政府は法により、出資比率に関わらず、出資企業のガバナンスにおける特権的なステータスを保有する。そのため、中国政府は出資する全ての企業を影響下に置くことができ、非国有企業に対しても事業活動を国の管理下に置くため幅広く出資を行っている。その他、補助金、助成金、税優遇といったインセンティブを用いて企業活動を共産党の政策利害と一致させている。米国企業および投資家は、「中国では他の市場経済とは全く異なり、国と事業活動、国有企業と非国有企業の境界が曖昧で、中国経済への参入は、共産党の政策目標の制約を受け、その管理下に置かれることを意味するということを理解しなければならない」と警告している。この点は、中国企業と合弁で事業を行う日本企業も留意すべきであろう。

### (3) 軍産エコシステムへの資金流入

2014年以降、中国政府は中国の金融市場の開放を拡張し、2018年以降、外国の金融サービス事業者に中国の金融市場に参入することを勧誘した。こうした一連の動きにより、米国および諸外国の投資家が中国に投資するようになり、主要投資インデックスに中国証券が加えられるようになった。その結果、米国の資産は自動的に中国市場に配分されるようになり、米国投資家に対する経済リスクのみならず、米国に安全保障上のリスクがも


岡野 寿彦
新開 伊知郎

たらされるようになった。米国および諸外国の中国資本市場への参入増加と、中国政府による企業セクターに対する管理強化は同時に進行している。さらに、中国軍産複合体に資金を誘導するため、中国政府は官民ファンドや軍事目的投資商品といったツールも利用している。米中の金融市場が結びつき、中国政府が金融市場を戦略的に利用する事態は、米国に新たな政策課題を生じさせている。なぜなら、米国資本と専門知識が、中国軍の能力向上と、将来人権侵害に使われるかもしれない技術を開発中の中国のスタートアップ企業を、意図せずに支援している恐れがあるからである。USCCは、従来の個々の企業や取引をスクリーニングする方法では、軍産エコシステムに関わる多様なプレーヤーを補足しきれず、中国の軍民融合戦略に対応できていないと指摘する。今後、米国がこれに対応して輸出・投資管理を強化する場合、日本にも同様の措置を取るよう要請することが想定され、日本企業は今後の動向を注視する必要があるであろう。

## 3 USCCの主な提言

上記の評価・分析に基づいて、USCCは以下のような提言を行っている。※3

### (1) 合成生物学、ニューモビリティ、クラウドコンピューティングに関する提言

・非ヒト遺伝子データの保護、収集、商用化に関するモデルフレームワークを作成し、遺伝子データが収集された国の知的財産権に関する原則の確立を目指すとともに、国のバイオテクノロジー資産の保護や中国の略奪的なデータ収集に関して国際社会の関心を喚起すること。

・自動走行車を開発する中国企業に対するアクセス規制法を制定し、特に中国の軍や情報機関を利用するようなデータ収集活動の規制や、自動走行車によって収集されたデータの保護を行うこと。

・中国企業によって米国民にどのようなクラウドコンピューティングサービスが提供されているか、それらに対しどのような法や規制が適用されているか、米国民はクラウドコンピューティングサービス事業者のオーナーシップに関する情報に用意にアクセスできるかどうか、米国企業は中国国内において同様なサービスを自由に提供することができているか、もし制約があるとすればどのようなものかを調査した報告書を作成すること。

### (2) 中国政府による経済管理の強化に関する提言

・重要なサプライチェーンや生産能力の中国への移転が米国の国家・経済安全保障に悪影響を与えないか審査する機関を設けること。

・輸出管理改革法および外国投資リスク審査現代化法の効果的な実施のために、大統領府にTechnology Transfer Review Groupを設置し、対象となる振興技術や基盤技術を特定し、その輸出管理を商務省に指示する権限を与えること。特にその技術のエンドユーザーの確認を確実に行えるリソースを確保すること。

・中国に施設を保有する米国上場企業に対し、中国での事業運営への中国共産党の委員会の関与の有無、あるとすればその内容について米国証券取引委員会に毎年報告することを義務付けること。

### (3) 金融取引に関する提言

・ある米国政府当局の下で制裁を受けた中国の企業・団体は他の省庁によっても自動的に制裁されることを確実にする包括的な法律の制定を検討すること。

・NS-CMIC企業リスト（中国軍産複合企業リスト）に掲載された中国企業を対象とした既存の米国投資規制の管轄権およびそのような規制の対象となる企業・団体のスコープを拡大する法律を制定すること。

・中国の株式、債券、デリバティブへの投資に伴う米国の投資家および国益に対するリスクに対処する

※3 経済面での提言に関しては、安全保障貿易情報センターのレポート、「米議会 米中経済・安全保障調査委員会（USCC）2021 年版報告書の主要提言内容について（解説）―経済関連規制に関わるものを中心に」が詳細に分析している。https://www.cistec.or.jp/service/uschina/45-20211130.pdf

ための包括的な法整備を検討すること。具体的には、中国企業に紐づいた変動持分事業体（ＶＩＥ）[※4]への投資を禁止またはその投資リスクを明示させること、上場企業に新疆ウイグル地区の強制労働を利用した製品やサービスに直接間接的に関連するサプライチェーンに関与する企業からの調達やデューデリジェンス活動、商務省のエンティティ・リストや財務省の中国軍産複合企業リストの掲載企業との取引について米国証券取引委員会への報告を義務付けること、中国や香港の株式取引所で発行される証券、ＶＩＥを通じて米国株式取引所に上場している中国企業の証券、これらの証券のデリバティブ商品をインデックスに含めているインデックスプロバイダーを米国証券取引委員会の規制下に置くこと。

## 中国の経済安全保障に関する動向 ～国家安全と米国依存の低下～

中国政府は、経済成長の鈍化、米中対立の激化などを踏まえて、政策の軸足を「成長」から「安全」にシフトしつつある。習近平政権が推進する「共同富裕」や一連のプラットフォーマー規制の背景には「国家安全」の重視がある。

本章では、中国共産党政権の安全保障に関する基本方針を定めた「総体的国家安全観」（第１節）と米国ＵＳＣＣ年次報告への対応（第２節）を踏まえて、経済安全保障政策の変遷（第３節）と中国政府が重視する「情報・データのコントロール」（第４節）について概説する。

### １　総体的国家安全観

「総体的国家安全観」は、中国の安全保障に関する観念と基本的方針として習近平国家主席が２０１４年から提唱しているものである。ここでは、人民の安全を主目的とし、政治の安全（共産党体制の護持）、経済の安全（経済安全保障）を基礎と位置付けている。その上で、具体的な安全保障の対象として、政治、国土、軍事、経済、文化、社会、科学技術、情報、生態、エネルギー資源、核（原子力）の11領域を挙げている。軍事などの伝統的な安全保障に加えて、政治や文化も安全保障との対象と位置づけていることが特徴である。また、「情報」も２０１４年から安全保障の対象とされている。

総体的国家安全観の背景には、中国の世界経済・産業におけるプレゼンスが高まるにつれてこれを抑え込もうとする動きが強まり、この対外的な圧力が中国国内に存在する発展の不均衡など「矛盾」と結びついて国家の「安全」が脅かされることを警戒しているとされる。従って、国内の脆弱な要素を解決し、国内と対外関係とを合わせた一体的な国家安全システムを構築する方針を示していると理解できる。

総体的国家安全観は、国家安全法として具体化されるとともに、国家情報法、データセキュリティ法などにおいても指導的概念として明示的に言及されている。14次五カ年年計画でもその堅持と経済発展の統合などが言及されている。

#### 「共同富裕」と国家安全

中国政府は米中対立など自国を取り巻く環境が複雑化するなかで、発展の不均衡など中国国内の「矛盾」が国家の安全を脅かす要因になることを強く警戒している。「戦狼外交」とも称される対外的な強硬姿勢のおおもとは、国内の課題にあると言える。そして、国家の安全や持続可能性の確保を目的に、経済成長の鈍化を前提とした政策の転換を進めている。その理念である「共同富裕」は、従来のような経済成長によるパイの分配が難しくなる中で、国家がコントロールして「分配システムの再構築」を行うものである。その一環として、これまで中国経済の成長の恩恵を受け、増加するネットユーザーを集客して成長してきたプラットフォーマーに、社会への利益還元を促している。

### ２　米国ＵＳＣＣ年次報告への中国の対応

ＵＳＣＣ年次報告など米国議会や政府の対中政策について中国の研究機関で分析・提言が行われている。例えば、北京市科学技術情報研究所　劉彦君研究員等による『中国の科学技術革新に関する米国の研究と判断の歴史的変化と将来の傾

※4　変動持分事業体（Variable Interest Entities, VIE）とは、変動持分（当該事業体の期待損失の一部を負担する、または期待残存利益の一部を享受する投資）により連結対象となる事業体。議決権により連結対象になる事業体と対応する概念である。2014年にアリババグループが利用して以降、中国企業が米国上場するスキームの一つとして広まったと言われている。（会計エージェント, https://accounting-agent.com/vie-model/、BESPOKE PROFESSINALS, https://bespoke-pro.jp/2021/07/04/didi-ipo/など）


岡野 寿彦
新開 伊知郎

向』[※5]では、USCC年次報告書について「超党派のコンセンサスとしてまとめられており、これまでの提言内容は概ね1～2年以内には、規制として具体化されている」との認識を示している。そして、2020年度USCC年次報告について、米国はハイテク科学技術を対象に、「人材をめぐる戦い」を核に、「標準化をめぐる戦い」を重要手段として、中国の発展を「点から面で」制御していくと予測。「持久戦の準備」「科学技術の安全に関する攻撃および防御能力を高める」「技術導入と自立化を同時に進める」「ハイテク技術の人材・組織を強化する」「国際標準制定における発言権を強める」ことを提言している。

さらにはUSCC 2020年度年次報告で提言された次の事項を、米国が規制として具体化してくると想定されるため、対応策を策定するよう提起している。

- 相互主義原則の採用による立法
- 中国への技術移転目的のプログラム関係のビザ拒否方針の明確化
- 中国の金融システムの危険性と脆弱性によるリスク分析
- 重要治療薬や医療機器の国内か同盟国からの調達
- 米国在台湾協会事務所長の大使と同様の手続き導入の検討
- サプライチェーンの連携と安全保強化のための民主主義有志国の多国間レベルでの取り組みに、台湾を含めることを推奨。情報通信技術、集積回路、電子部品など、重要な戦略的産業に必要不可欠な材料の確保と、サプライチェーン回復力保証に重点を置く
- 香港からの亡命受入れ拡大の検討

米国の経済安全保障政策に関する分析レポートでは、このほか、米国政府の中国ハイテク企業制裁や貿易戦争の特徴、インド・太平洋戦略などについて分析されている。

## 3 中国の経済安全保障政策の変遷

総体的国家安全観に基づき2015年に「中華人民共和国国家安全法」が採択・公布された。同法で「経済安全」について、「国家は基本的な経済体制と社会主義市場経済秩序を維持し、経済安全リスクを防止・解決する制度的メカニズムを改善し、国家経済の生命線である重点産業とインフラ、その他の重要経済利益における発展事業を推進する」（19条）と規定されている。

また、同法に先立ち2015年5月に中国共産党中央委員会と国務院は、対外開放を標榜しながらも同時に「核心利益」を守り、開放経済における経済安全体制を確立するために、① 外資に対する国家の安全審査機構の整備、② グローバル化のリスク防止・管理体制と管理システムの構築、③ 経済貿易安全システムの構築、④ 金融リスクの予防と管理システムの整備、を行うことを声明した。2010年台半ばに中国政府が経済安全保障で重視したのは、① 国家安全保障に影響を与える分野での対中投資の事前審査、② 市場管理・監督の強化による安定維持、③ 資源の安定供給のための国際ルートの確保、④ 輸出管理システムの構築、であった。

### 米中対立下の経済安全保障政策

2018年以降、米国トランプ前政権が経済安全保障を重視した対中政策を進めたことを受けて、中国における経済安全保障の概念も変化した。中国政府が「経済安全保障」という言葉を使う文脈では、コアテクノロジーと関連する知的財産、情報・データ、重点産業の保護、サプライチェーンの確保を強調するようになった。

第14次五カ年計画（2021年3月制定）では第53章「国家経済安全保障の強化」で、「食料安全戦略の実施」「エネルギー資源安全戦略の実施」および「金融安全戦略の実施」について言及している。さらに同計画において「安全」という言葉が150回以上登場し、「安全」を発展の前提条件として位置付けている。

第14次五カ年計画を分析すると、中国の最新の経済安全保障政策は「科学技術イノベーションの強化、

※5 中国語原文タイトル『美国対中国科技創新研判的历史変迁与未来走向：基于《美国中国经济安全审查委员会（USCC）年报》的分析』、英語タイトル：The Historical Changes and Future Trends of U.S. Research and Judgment on China's Scientific and Technological Innovation : Based on the analysis of "USCC Annual Report"

技術の自立」と「サプライチェーンを自主的にコントロール出来る能力（双循環）」との相乗効果を中核とし、「食糧、エネルギー、金融の安全」と「情報・データのコントロール」が下支えをすることで、長期的に米国との依存解消を目指す「体系的なシステム」であると理解できる。また、取り組み方については、巨大な市場や企業（国営、IT、製造、中小企業）の資源、政府機能をフルに動員した「組織戦・総力戦」として理解できる。

## 4　国家安全と情報・データのコントロール

安全保障や産業競争力におけるデータの重要性が高まるなか、世界各国でデータやサーバー空間に対する国家安全と主権の確立のためのルール作りが活発になっている。中国では、国家や企業の競争力を左右する情報・データの国家によるコントロールが、安全保障の重要な要素として位置付けられている。2000年台にはグーグルやフェイスブックなどの米国企業のサービスを利用できないよう制限し、BAT（百度、アリババ、テンセント）などの中国プラットフォーマーが成長する環境を整えた。2017年に施行した「サイバーセキュリティ法」に続き、2021年9月にはデータの統制を強化する「データ安全法」、11月には「個人情報保護法」を相次いで施行。3本の法律で中国国内の重要データの流出を防ぐ体制を固めた。

米中技術覇権競争が激しくなる中で、特に、情報・データの国外への移転に中国政府は神経を尖らせている。滴滴出行（中国配車サービス最大手）は、2021年6月末にニューヨーク証券取引所に上場したが、半年も経たぬ同年12月3日に上場を廃止し、香港株式市場への上場準備に入ることを発表した。米国当局からの要求に基づく中国国内からの情報流出を警戒した中国政府の意向を踏まえた判断だとされる。上場直後の7月に、国家安全法とサイバーセキュリティ法に基づいて、同社のデータ管理に問題がないか中国国家インターネット情報弁公室（CAC）による審査が行われた。さらに、中国国務院と中国共産党中央弁公室の連名で、外国でのIPOに対する取り締まりを強化するガイドライン「法に基づき証券違反行為を取り締まる意見」を発表した。海外上場の中国企業について国境を越えるデータの流通や機密情報の管理に関する法律・規則を整備するとしている。中国政府はさらに、北京証券取引所の新設を打ち出すなど自国資本市場の強化に動き、中国本土や香港での資金調達を促している。米中間のデカップリングが、貿易や技術からマネーに及んできた。

## 最後に

日本の経済安全保障政策と企業経営は、同盟国である米国と最大の貿易相手国である中国の両国関係に依存することは不可避である。米国は中国とのハイテク覇権争いを制するために、半導体などハイテク産業の技術開発やサプライチェーン強化に政府の介入を強めていくだろう。一方中国は、米国への依存度を下げるために、政府主導での科学技術イノベーションやサプライチェーンをコントロールできる能力の強化を時間をかけても進めるだろう。米中両国内の国民の支持や政治的力学を考えると、ハイテク技術・産業におけるデカップリングが進み、日本企業が「踏み絵」を踏まされる局面が長く続くことは避けられない。

日本企業にとって最大の防御策は、米国、中国のいずれにおいても必要とされる技術を開発して守り、「依存関係」を作り続けることだ。そして、必要不可欠な技術力という「企業が行使できるパワー」を最大限に活かすためにも、米国、中国政府の政策や国内の議論、そして両国の企業の動向を深いレベルで分析していくことが不可欠である。


**本稿に関するご質問・お問い合わせは、下記の担当者までお願いいたします。**

NTTデータ経営研究所
グローバルビジネス推進センター
主任研究員
岡野 寿彦
E-mail okanot@nttdata-strategy.com

社会システムデザインユニット
グローバルビジネス推進センター（兼務）
シニアスペシャリスト
新開 伊知郎
E-mail shinkaii@nttdata-strategy.com


# 2021年度情報未来研究会活動報告
# デジタルガバメント推進の方向性

**情報未来研究会事務局**

NTTデータ経営研究所
執行役員
エグゼクティブコンサルタント
**三谷 慶一郎** MITANI KEIICHIRO

デジタルイノベーションコンサルティングユニット
シニアインフォメーションリサーチャー
**小田 麻子** ODA ASAKO

デジタルイノベーションコンサルティングユニット
コンサルタント
**中村 夏美** NAKAMURA NATSUMI

## はじめに

「情報未来研究会」はIT社会の潮流を見つつ、健全な社会や企業の在り様を探るため、弊所創立以来継続的に実施してきた活動である。経営学および情報技術分野の有識者とNTTデータおよびNTTデータ経営研究所メンバーの合計13名を委員として、定期的に開催されている。弊所のアドバイザーを務める慶應義塾大学の國領二郎教授を座長に据え、2021年度は「デジタルガバメント推進の方向性」をテーマに活動してきた。

## 第1回 社会システムとしてのデジタルガバメントの在り方 ～デジタル改革と政治のリーダーシップ～

**武蔵大学 社会学部メディア社会学科 教授 庄司 昌彦先生 ご講演**

情報未来研究会委員　（敬称略、50音順）※2022年1月時点

| 氏　名 | 所　属 |
|---|---|
| 稲見 昌彦 | 東京大学先端科学技術研究センター教授 |
| 井上 達彦 | 早稲田大学商学学術院教授 |
| 岩下 直行 | 京都大学公共政策大学院教授 |
| 江崎 浩 | 東京大学大学院情報理工学研究科教授 |
| 國領 二郎（座長） | 慶應義塾大学常任理事総合政策学部教授/株式会社NTTデータ経営研究所 アドバイザー |
| 柴崎 亮介 | 東京大学空間情報科学研究センター教授 |
| 庄司 昌彦 | 武蔵大学社会学部メディア社会学科教授 |
| 妹尾 大 | 東京工業大学工学院経営工学系教授 |
| 本間 洋 | 株式会社NTTデータ　代表取締役社長 |
| 三谷 慶一郎 | 株式会社NTTデータ経営研究所　執行役員　エグゼクティブコンサルタント |
| 柳 圭一郎 | 株式会社NTTデータ経営研究所　代表取締役社長 |
| 山口 重樹 | 株式会社NTTデータ　代表取締役副社長執行役員 |

### ■日本でデジタル改革が上手く進まなかった理由

日本は今まで、素晴らしいインフラを作り様々なＩＴ戦略を作ってきたが、上手く使えておらず、「敗戦」だと言われている。デジタル敗戦は国際比較による相対的なものだが、なぜ課題認識はされているのに解決出来なかったかという経緯の検証をする必要がある。これまでデジタル改革が上手く進まなかった理由としては、現場の人たちが新しいことをやることに躊躇してしまう構造があることや、「デジタルは冷たい」というステレオタイプによって非効率でも人手でやると判断していたことなどがあるように思う。また、政府の構想を自治体職員に話すと、業務量が増えるのではないかと自治体職員が懸念する傾向がある。今後は、組織ごとの事情を踏まえて作ってきたローカルルールを、自分たちで見直して変えていくことが必要だ。

### ■デジタル改革による「誰ひとりとり残さない」デジタル社会の実現に必要なこと

今や「誰ひとりとり残さない」、全員に必要なものとしてデジタル化が求められている。「誰ひとりとり残さない」を実現するためには、改めてインフラに注目し、問題なく使える性能かどうかを気にしていく必要がある。また、子どもに限らず、あらゆる立場や年齢の人を対象にしたリテラシー教育が必要だ。実際にデジタルを利用する上では、助け合える人や組織との繋がりについても気に掛ける必要があるだろう。さらに、人にやさしくデジタルを使うという観点から、人海戦術はもうしないことも大事だ。支える人を支えるという観点で、教員、介護職や役所の窓口の方々がデジタルを使うことによって、人との対応を強化するということを行うべきだ。

デジタルデバイスの世帯保有率は、スマートフォンが86・8％と圧倒的に強い。スマートフォン利用を前提とした「誰ひとりとり残さない」の実現検討が必要ではないか。

### ■自治体ＤＸというデジタル改革

デジタル改革として、現在日本において取り組まれている中心的な活動のひとつが「自治体ＤＸ」である。自治体ＤＸの重点取り組み事項は6つあり、「自治体の情報システムの標準化・共通化」「マイナンバーカード普及促進」「手続きオンライン化」「ＡＩ・ＲＰＡ」「テレワーク」「セキュリティ」である。自治体ＤＸをやる理由は、２０４０年問題にある。少子高齢化が進む中で、自治体職員が不足したり、予算が不足したりする。行政サービスの需要が非常に多く、品質を下げることもできない中で行政サービスを維持することが求められているのだ。このような状況下では、人でなくても良いものは積極的にＡＩやロボティクスを使ったり、自治体の行政で同じようなことをしている部分は標準化、共通化したりしていこうという考えがある。

### ■データ活用と行政への「信頼」

デジタル改革への批判、特に野党からの批判で多いのは、政府がデータを利用することに対する懸念である。年金記録問題（２００７年）、統計不正問題や公文書管理問題（２０１９年）、ＰＣＲ検査結果などの警察への提供（２０２０年）など、政府の情報管理・データ利用に問題があるのは残念ながら事実でもある。欧州を参考に、政府・自治体のデータ利用への監督、透明性向上、本人への報告／開示など信頼獲得のための方策を続けていく必要がある。具体的には、個人情報保護委員会がしっかりと政府自治体のデータ利用を監視、監督し、時には止めるといった取り組みによって、信頼を獲得していくべきだ。

### ■デジタル改革と政治のリーダーシップ

冒頭で日本はデジタル敗戦をしているという話をしたが、コロナ禍においては「ハンコ問題」への着手や「デジタル庁」創設など、平時の行政では実現できなかったような横断的取り組みや骨太な変更ができている部分もある。この動きは社会的な機運作りに繋がったが、ス


情報未来
研究会事務局

ケジュールややり方について、現場との乖離があった点は問題だ。スケジュールややり方は柔軟に見直して対処して目標を実現すべきである。また、高い目標を達成するまでに熱が冷めてしまわないように、デジタル改革を外部から評価し続けていくことも必要だ。

歴代のＩＴ関連担当大臣の在任状況を調べると、平均在任期間は９・６ヶ月であった。政策サイクルを１年だと考えると、ＩＴ戦略を担うためにはもう少し長期在任する必要があるのではないだろうか。また、ＩＴ関連担当大臣の兼務状況を見ると、平均で３・７個、最大６個兼務しているが、過剰な兼務はＩＴ担当およびデジタル大臣の力を弱める方向に働いてしまうのではないか。なお、ＩＴ戦略本部会合の開催回数を数えると低下傾向にある。単に本部会合を数えるだけでは、活発かどうかの評価はし難いかもしれないが、総理や大臣などの出席する政治的リーダーシップが発揮される会議でこそ大事なことが決まるのだとするならば、本部会合がどれだけ行われているかということにも意味はあるはずだ。

## デンマークのデジタルガバメント

**第２回**

デンマーク・ロスキレ大学　准教授

**安岡 美佳先生　ご講演**

### ■デンマークにおいて電子化が進んだ背景

デンマークは、デジタルインフラが整っている国として知られている。なぜデンマークでは電子化が進められるようになったかと言えば、福祉国家として、福祉の質を落とすことなく資源を有効活用するためである。１９６８年には個人番号（ＣＰＲ）が導入されたが、これは、国民にきちんと納税してもらい、再分配する仕組みが必要であったため、きちんと管理できるような中央の納税管理システムを作ったのがきっかけだ。電子政府政策ができはじめた２０００年頃、デンマークでは、高齢化、国庫逼迫、労働者不足などの問題や、産業育成が不十分などの課題があった。そこで注目されたのが、電子化による業務の効率化だった。

デンマークにおける電子政府政策は、20年かけて段階的に導入されたところに特徴がある。例としてeDayがわかりやすい。eDayは１、２、３、４とあり、電子化を行政から企業、最後に市民へと段階的に社会の中に広げるための一連のプロジェクトとなっている。約10年に渡る段階的な導入は、成功に繋がる重要要件の１つであろう。

### ■デンマークのアドバンテージ

電子政府政策が始まって約20年が経った今、政策は上手くいっている。私の考えるデンマークのアドバンテージは３つある。１つ目は蓄積されたデータ基盤だ。デンマークでは、68年以降に様々な個人データや、技術進展に伴うデータのオープン化がきちんと進められてきた。２つ目は共通基盤の整備。かつて、自治体システムはＫＭＤ社による独占的なマーケットだったため、システム連携が比較的簡便だったと言われる。３つ目に基礎ＩＴリテラシーのある市民の存在である。デンマークでは１９７０年代あたりから女性の社会進出が進み、今の70代、80代前半ぐらいの人たちが若い頃、男女ともに社会に出て働いていた。その頃にオフィスオートメーション化が進み、多くの女性がＩＴ分野で活躍した。このような背景もあり、デジタルデバイドの課題になりがちなシニア世代のＩＴリテラシーが比較的高かったのである。

## ■セキュリティ国家戦略の推進

電子政府の進展によって、より良い効率的なサービスを提供できるようになっている反面、改ざん、なりすまし、個人情報漏えいが起きている。これらへの対応は不可欠であり、近年もセキュリティ強化は段階的に行われている。

日本では、セキュリティや個人情報というと、暗号化や技術的手段によって守るというような、技術的な話になりがちだと思うが、デンマークのセキュリティ国家戦略において、技術は3本の柱のうちの1つに過ぎない。国家戦略の2つ目の柱は、協力体制である。政府、専門企業、大学、研究者との協力を強化しようということを挙げている。3つ目の柱は、知識を増やすということである。市民、産業界、公共機関の全ての社会構成員が、適切な知識を取得することが重要との考えから、ウェブサイトで情報提供や注意喚起をしている。完全なシステムはない、ということを前提に人の教育をしっかりやろうという考えだ。

## ■デジタルデバイドへの対応

デンマークでは高齢者のIT利用率も非常に高く、2020年の報告では、75歳から89歳の人たちのインターネットの利用率が95％超だった。デンマークでシニアがICTを利用できている理由として、1つ目に、強制的に導入されたということがある。2つ目は、ユーザビリティやユーザーエクスペリエンスが非常によく考えられた、使い勝手の良いシステムやアプリが提供されていること。3つ目は、トラストが構築されていること。すなわち、個人のデータは自分のものであり、自分のデータに誰がアクセスしたか分かるといったような透明性が確保されている。4つ目は、インフォーマルサポートが充実していること。身近な子どもや孫、ローカルな支援NPOによるサポートを上手く活用することで、高齢者のユーザーを増やせているようだ。

デジタルデバイドの解消に向けてできることは、他にもある。女性、身体障がい者、子ども、外国人など、少数者と呼ばれるあらゆる人たちを巻き込んだ、ITシステムの開発（参加型デザイン）である。

## ■残された課題と今後の展開

デンマーク政府は、やり残しているところはまだ多々あると捉えている。2021年6月に発表された、「デジタル社会におけるデジタルインクルージョン」では、デンマークの重点分野として、デジタルスキル、管理能力、子どもやティーンエイジャーにも分かりやすい言葉の使用などが、挙げられている。また、全国民がサイバー攻撃やセキュリティに関する知見をある程度備えておくことが今後必要であるということが強く言われている。

対策として、デンマークのデジタル庁で働いている人たちに対して、身に付けるべきキー・コンピタンスを定義している。戦略とビジネス開発、プロジェクト開発、知識、コラボレーションするための能力、データ保護の能力などだ。また、キー・コンピタンスを確実に公共機関やデジタル庁内部の職員に根付かせるため、ITアカデミーを設立している。同じようなものは、地方自治体でも作られている。

## ■なぜデンマークでは電子化が上手くいったのか

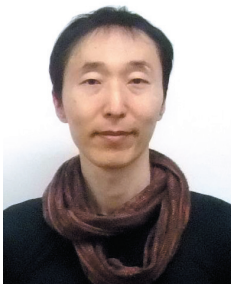
ここで改めて、なぜデンマークでは上手くいったのかを考察したい。最も大切であるのは、人間中心の考え方に基づいたデジタル促進をしたことだろう。デンマークではこの30～50年ぐらいで、テクノロジー導入時には、人、組織、社会などの理解が不可欠という考えが常識になった。人、組織、社会を考えることは、長期視点を持つことでもある。医療保険ポータルsundhed.dkを長らく統括していたMorten Petersen氏は、「システムの構築は1年で終わった。その後、導入し浸透するのに20年かかった」と言っている。人間のマインドセットの転換に沿った長期視点でシステム導入をしていったことが、デンマークが今ここまで上手くいっている理由ではないか。


情報未来
研究会事務局

# エストニアのデジタル国家について

**第3回**

一般社団法人 日本・エストニア／EUデジタルソサエティ推進協議会（JEEADiS）
理事
**牟田 学様　ご講演**



## ■デジタル国家エストニア

エストニアはデータ連携や自動化を非常に早く始めた。人もお金もないエストニアは、自動化を進めなければサービスを維持することは出来ないという状況だったため、データ連携や自動化は死活問題だったのだ。エストニアはデジタル国家を進める上で、コンピュータと人が共存でき、互いが得意なことを、パートナーシップを組んで行ってきた。今後は、人間の意思決定を支援したり人間の介在する部分を減らしたりすることで、AI同士、コンピュータ同士の連携がさらに強化されるのではないか。

## ■デジタル国家への「信頼」

電子政府において、国民の政府への信頼性が必要かという話がある。エストニアの場合、ソ連による統治という歴史的背景もあり、国民は政府をそれほど信頼していないが、国民の多くが、デジタル国家という仕組みについては信頼している。国民がデジタル国家を信頼する上で重要な点が、透明性や、追跡可能性だ。エストニアでは、国民、政治家、医者、公務員、皆が同じ土俵に立つことで、国民が政府を監視するということを実現している。また、国民IDカード、電子署名の利用者は、公的な業務に携わる人全てとなっている。IDカードや電子署名を業務遂行の必須事項とすることで、透明性や責任追及性が担保されている。

## ■エストニアにおける情報管理

エストニアでは公共情報を資産であると考え、情報管理に非常に注力している。かつて情報管理は、組織管理や文書管理という観点で行われていたが、現在ではサービスと情報の管理という観点で行われている。提供するサービスにとってどのような情報が必要なのかを考えながらサービス自体が設計される。日本でデータ連携が上手く行かない理由は、自治体がデータ管理の部分を組織単位で管理しているためではないか。

## ■公的データベースのガバナンス体制

エストニアの公的データのガバナンス体制には、データコントローラーであるデータ管理者と、データ処理者、データ提供者がいる。データ管理者とは、法律上、そのデータベースの管理責任者になる人、データ処理者とは、実際にそのデータベースを作ったり運用したりする、技術的なところを行う人たち、データ提供者とは、そのデータベースにデータを提供する義務がある人たちである。

## ■法律とITシステムの体系化

エストニアでは法律とITシステムが上手く体系化されているというところが特徴である。法体系を作成するにあたり、コンピュータで処理できるよう配慮し、曖昧性を可能な限り排除している。そのため、ITアーキテクチャの中に法律が組み込まれているといえる。

## ■デジタル公共サービス

情報のアクセス権に関して、公営図書館にインターネット環境の提供が義務付けられているため、コンピュータを持っていない人でも公共サービスを利用できる。公開文書そのものを国民が閲覧できたり、自分がどのようなサービスを利用できるかを検索できたりする。

エストニアの重要な仕組みの1つとして、政府会議情報システムがある。会議自体が非常に効率化されており、事前に共有される資料

に対して、イエスかノーか保留かを回答したり、意見を言いたいというようなことを表明したりできる。全員が事前に賛成した議案は、当日の会議ではパスされるため、会議の時間短縮になる。また、閣議で決まったことは法案情報システムに送られ、国民にも知らされるため、意思決定に国民が参加できる。

データコントローラーがオープンデータ化を進めるため、制度毎、分野毎に、アクセス制限のないデータが原則全て公開されている。データを使える環境が全国的に整備されていて、それらを使ったサービスというものも登録されている。

### ■公共とプライバシー

公共情報には公開されている部分と制限されている部分がある。個人データは制限されている部分に含まれているが、公務員の給与など、法律の規定によって公開する場合がある。

GDPR（EU一般データ保護規則）においてプロファイリングは原則禁止で、公共サービスの中でプロファイリングに相当する処理をする場合は法的根拠が必要であると定義されている。プロファイル分析を含む自動化された意思決定が許可されるのは3つのパターンで、「1. 顧客との契約締結や履行のため」「2. 自動意思決定を法律で規定している」「3. 自動決定とプロファイル分析に本人が同意した」だ。本人が同意するというのはかなり大変なことであるため、エストニアでは非常に慎重に運用している。

エストニアでは公共空間において顔認識を使うことは原則禁止で、法的根拠もない。但し、正当な理由があれば法的根拠になる可能性はある。なお、監視カメラを設置する場合は、目的、基づく法的根拠、利益、責任者の連絡先といったラベル登録が必要だ。また、公共空間におけるリアルタイム監視は基本的にはNGであり、ビデオ分析ソフトウェアでの生体認証データ処理は原則認められていない。

## 終わりに
### ～先進的取り組みの本質を見極める～

日本では、政府に対する信頼が不十分であることが、デジタルガバメント推進への批判の中にみられる。一方エストニアでは、政府への信頼が不十分であるからこそ、政府の行動を国民が監視する仕組みとしてデジタルガバメントを推進させており、これはとても興味深い。「デジタルガバメントは、政府のものではなく、国民のものである」という方向性で考えることが重要なのではないだろうか。

また、日本ではテクノロジーの導入のみに注力しており、現場の人々や現有のルールをそのまま放置してしまっていることが問題ではないか。デンマークでは「人間中心のデジタル推進」をしており、「テクノロジー導入時には、人、組織、社会などの理解が不可欠という考えが常識」となっている。つまり、テクノロジーだけでなく、周囲の組織や制度も含めたデジタルガバメント推進になっているのだ。また、「人間中心のデジタル推進」をする上では、「誰ひとりとり残さない」ために、ユーザビリティを考慮したテクノロジーを設計しつつ、ITリテラシーを磨くために学ぶ機会を用意している。エストニアに至っては、「法律とシステムが体系化されている」「ITアーキテクチャの中に法律が組み込まれている」という。これは、テクノロジーを活用することを前提に、テクノロジー活用と整合の取れた法体系が作り上げられているということだ。そして、テクノロジーは短期で変革できるが、制度や人が変わるには時間がかかることを忘れず、デンマークのように「長期視点」を持って取り組むことが必要だ。

日本では2021年9月にデジタル庁が発足し、いよいよデジタルガバメントの実現に向けた動きが本格化してきた。今後日本がデジタルガバメントを推進するにあたっては、デンマークやエストニアなどの先進的な取り組みは大いに参考にすべきだ。そして、より重要なのは、取り組みそのものの表層的な部分を模倣することではなく、その背景にあるデジタルガバメントに関する本質的な考えを十分に理解した上で、我々が進むべき次の一歩を見極めることだろう。

# 書籍案内

NTTデータ経営研究所のコンサルタントおよび役員が執筆、あるいは執筆参加した書籍をご案内いたします。


今日からモノ知りシリーズ
## トコトンやさしい サービスロボットの本

**清水祐一郎 著**

利活用の視点を中心に、ロボットと人とのコミュニケーション、サービスに応対するための自律移動、生体信号を用いたロボットのインターフェイスなど、キーになるテーマに焦点を当て、それぞれの導入課題を含めて紹介。

**出版社**　日刊工業新聞社
**発行日**　2022年2月10日
**価　格**　1,650円（税込）


## マネロン・テロ資金供与対策
### ―金融機関に求められる高度化の取組み―

**NTTデータ経営研究所：大野博堂／田中公義／山本邦人／武内俊吾 著**
**NTTデータルウィーブ：村田隆洋／永山貴文 著**

国内外のマネロン・テロ資金供与対策の変遷や事例、今後の課題・将来像を紹介し、金融機関としてどのような取組を行うべきかを明らかにした1冊。

**出版社**　近代セールス社
**発行日**　2022年2月5日
**価　格**　1,870円（税込）


## 金融DX戦略レポート
### 2022-2026

**第7章3-5 CBDC（戸田幸宏）**
**第7章5-4 決裁ネットワーク（加藤洋輝）　著**

導入実態調査、市場規模、ライバルの戦略…DXで成果を上げるための、すべての情報がここに。2022年以降、さらに加速するEmbedded Financeの最新動向や主要プレーヤーの戦略を徹底解説。

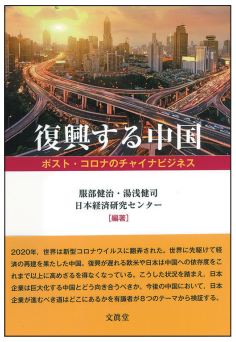
**出版社**　日経BP社
**発行日**　2022年1月31日
**価　格**　書籍のみ：660,000円（税込）
書籍+オンラインサービス:990,000円（税込）


## 2022年版 金融時事用語集

「エンベッデッドファイナンス」増井宏樹、「レグテック」「クラウド活用(2頁)」福光典子、「NFT」中道大智、「大阪デジタルエクスチェンジ」浅居洋輔、「QRコード決済」「サブスクリプション」戸田幸宏、「アジャイル開発」松川あゆみ、「地域通貨」武内俊吾、「ATM連携・共同化」岡村純平、「グローバル・ステーブル・コイン」中村泰士、「オープンイノベーション」岡田明子、「デジタル通帳」松岡結衣 著

各界のエキスパートが用語の背景、金融商品・取引の仕組みなどを、直近のデータを使って平易・簡潔・具体的に解説。

**出版社**　金融ジャーナル社
**発行日**　2021年12月14日
**価　格**　1,650円（税込）

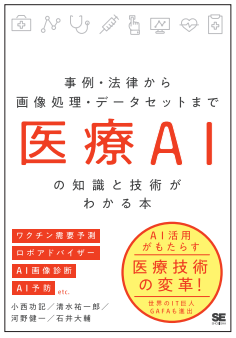



## 復興する中国
### ポスト・コロナのチャイナビジネス

**服部健治/湯浅健司著/日本経済研究センター編/岡野 寿彦共著**

新型コロナウイルスに翻弄された世界に先駆け、経済の再建を果たした中国。復興が遅れる欧米日が中国への依存度をこれまで以上に高めざるを得なくなっている状況を踏まえ、日本企業は巨大化する中国とどう向き合うべきか。今後の中国において日本企業が進むべき道はどこにあるのかを有識者が8つのテーマから検証。

**出版社**　文眞堂
**発行日**　2021年7月19日
**価　格**　2,640円（税込）




## 医療AIの知識と技術がわかる本
### ―事例・法律から画像処理・データセットまで

**小西 功記／清水 祐一郎／河野 健一／石井 大輔 著**

AI技術は病理学や医用工学、解剖学、神経科学、細胞生物学、脳神経外科や内科学、眼科学、放射線医学、手術医学など、基礎医学から臨床医学まで幅広い領域に浸透し始めている。本書では、最新の事例、技術、法律と行政の取り組みについて解説。国内において医療AIをより活用できる1冊。

**出版社**　翔泳社
**発行日**　2021年5月26日
**価　格**　2,860円（税込）


## ポストコロナ時代の高齢者ケア
### ―2025地域包括ケア転換期に立って

**朝田 隆・村川 浩一　編著／第4章　本田幸夫、足立圭司　共著**

感染症の脅威が前提となった高齢者福祉現場において、その最新動向を「認知症」「老年医学」「地域ケア」といった観点から理論的解説と、医療的観点から今回の新型コロナウイルス感染症が現時点で高齢者ケアにもたらした影響を総括する。

**出版社**　第一法規
**発行日**　2021年4月30日
**価　格**　2,970円（税込）


## 経営のイロハをDX化する「開発しないシステム」導入のポイント
### ～パッケージで、管理業務を早く・安く改善

**広川 敬祐 編著／大場 みち子・木村 俊一 監修／板井 実・緒方 瑛利・髙橋 昌太郎・倉本 真司・東 義弘・秋元 隆・渡辺 康雄・植木 貴三・上條 英樹 著**

パッケージ（開発しないシステム）を利用して、会計・人事などを含めた経営管理業務改善の勘所を解説する。無駄なコストをかけない、迅速なシステム導入のポイントがわかる1冊。

**出版社**　中央経済社
**発行日**　2021年3月22日
**価　格**　3,300円（税込）


## M&A失敗の本質

第15回 M&Aフォーラム賞 RECOF賞 受賞

**人見健　著**

日本企業が本当の意味で復活・再生するためには、他社の技術・人材・ノウハウを吸収し、自社の強みを磨くM&Aが不可欠だが、いまだに失敗事例が後を絶たない。その原因は会社の古い価値観、ルール、行動様式にある。300件以上のM&A案件を手がけてきたコンサルタントが、数多くのM&A事案の裏側や失敗事例を紹介し、失敗の本質を明らかにしていく。

**出版社**　ダイヤモンド社
**発行日**　2021年3月2日
**価　格**　1,980円（税込）

# 情報未来®

*Info-Future®*

No.69 March 2022

No.69
発行日　2022年3月25日
発　行　株式会社NTTデータ経営研究所
〒102-0093
東京都千代田区平河町2-7-9 JA共済ビル9階・10階
発行人　柳 圭一郎
編集人　成田 正人
編　集　村岡 元司／加藤 賢哉／野中 淳／三谷 慶一郎
野々山 清／米倉 智子／山添 由美



『情報未来』は弊社Webサイトでもお読みいただけます。
http://www.nttdata-strategy.com/knowledge/infofuture/

電子メールによる発行のお知らせをご希望の方は
下記URLページよりご登録ください。
https://www.nttdata-strategy.com/forms/infofuture/

情報未来、当社サービスに関するお問い合わせは、
NTTデータ経営研究所
コーポレート統括本部
業務基盤部　広報担当
Tel.　03-5213-4016
Fax.　03-3221-7022
E-mail　webmaster@nttdata-strategy.com
まで　お寄せください。

# 情報未来®
*Info-Future®*

株式会社NTTデータ経営研究所
http://www.nttdata-strategy.com
〒102-0093　東京都千代田区平河町2-7-9　JA共済ビル9階・10階
Tel. 03-3221-7011（代表）　Fax. 03-3221-7022