HITACHI
Inspire the Next

# 日立総研

特集

## 規制強化が映す米中欧のデータ覇権競争

vol.13-4
2019年2月発行

株式会社 日立総合計画研究所

表紙題字は当社創業社長(元株式会社日立製作所取締役会長)駒井健一郎氏　直筆による

# 日立総研

vol.13-4
2019年2月発行

巻頭言

# デジタルとフリクション

（株）日立総合計画研究所
所長　嶋田　惠一

北米向け家電製品の輸出営業として社会人生活を始め、ようやく職場の雰囲気に慣れてきたある日、上司に折り入って頼みがある、と声をかけられた。上司の机の前の椅子に座って、顔色をうかがうと困惑したような表情を浮かべている。「申し訳ないが、これからアメリカのテレビの仕事を手伝ってくれないか。ほんの少しの時間だ。地下の倉庫から船積み書類のファイルを出して、必要なだけコピーをとって米国側に送る作業をしてほしい。対象期間はこれから指示する。」家電輸出の花形であるテレビは私の担当外であった。そういえば、テレビ・ビデオを担当している隣のグループが数日前から慌ただしく仕事をしているが、なぜだろう。理由を探る時間もなく、新入社員の私は言われるまま地下の倉庫に向かった。そして、それから約一週間、私は地下の倉庫に張り付けになることになる。

日本と米国との貿易摩擦は1950年代の繊維摩擦にさかのぼり、その後鉄鋼、カラーテレビ、自動車、半導体と対象が変わっていった。カラーテレビは米国電子工業会（EIA）によるアンチダンピング提訴（1968）が起点になっている。その後、米国によるダンピング認定、日本による輸出自主規制（1977）、各メーカーの米国現地生産拡大（1980年代）を経て、状況は落ち着いていたはずであった。しかし、そうではなかった。今回の相手は米国内国歳入庁（IRS）であった。IRSの主張点は「移転価格」であった。日本、アジアなどの工場の製品・部品出荷価格をつり上げ、取引先である米国販売会社、製造会社の利益を過少にすることで、米国で上げるべき収益を本国に移転し、米国当局からの課税逃れをしている、というのであった。

つまり、私は、その対応活動の末端として、東京のオフィスの地下倉庫に張り付けになっていたわけであった。地下作業が終わって、後になって上司から状況を知らされた私は頭の整理がつかず、思わず質問をした。「おかしいのではないですか。ダンピングは原価割れの安い製品価格で不当に市場を占有するといい、一方で移転価格は、原価をつり上げ、不当に現地会社のマージンを削っているという。日本やアジアの工場を起点に考えれば、片や原価割れ、片や原価つり上げ。対象が同じ製品でありながら両者の論理はまったく逆です。なぜこのようなことが許されるのですか？」上司は薄く笑いながら言った。「商務省は商務省、IRSはIRSだと言う。それがアメリカなのだよ。」上司が困惑した表情を浮かべていた理由が分かったような気がした。

時は現代に変わり、貿易摩擦の主役は中国と米国になった。しかも、貿易「摩擦」ではなく貿易「戦争」だと言う。確かに、摩擦ではなく、戦争と言った方が良いかもしれない。2018年3月に米国は国家安全保障上の問題を理由に、鉄鋼とアルミニウムの中国製品に対してそれぞれ25%、10%の追加関税を賦課した。これに対して中国は4月に米国の果物等の1次産品や、豚肉、鉄鋼、アルミニウムの輸入製品の追加関税に踏み切った。その後、米国は7月から9月にかけて、過去日本に使用した通商法301条を中国製品に次々適用し、中国は都度米国輸入製品に対して報復関税を実施してきている。中国から米国への輸出額約5,000億ドルに対して、追加関税の対象はその半分、中国の場合は、米国からの国内輸入額約1,500億ドルの3分の2が追加関税の対象になる。金額をみると、報復の応酬でも、分は中国の方が悪い。

米国にとって、中国のような国の登場はかって経験をしたことがない事態なのかもしれない。これまで、経済・通商摩擦の相手は日本、EUであった。安全保障ではソ連・ロシアが相手であった。中国は今や、経済・通商、安全保障の両面で米国の脅威になりつつある。最近のFIRRMA（2018年外国投資リスク審査近代化法）によるCFIUS（対米外国投資委員会）権限強化は、その懸念の表れのひとつだろう。企業投資先に関する同委員会の安全保障リスク審査の対象分野を、防衛技術のみならず、中国政府・企業が関心を持つ重要デジタル技術、インフラ・個人データに拡大した。当時新入社員であった私が「地下作業」で感じたのは、米国は本気になると徹底的にやる、論理の整合性など関係無しに、である。そう考えると、米中間の政治・経済・社会保障といった、地政学上の摩擦をめぐる緊張関係はこれからも続くと考えられる。

米中対立を核とした、各国・地域間の摩擦は、通商のみならず、デジタル技術、データに拡大している。現時点で解決の糸口はみえず、摩擦は長引くであろうが、個人的には悪いことばかりではないと思っている。過去、日米貿易摩擦は、個人的には米国に一方的に攻められた印象があり（単なる末端のスタッフであったが）、今思い出しても苦々しく感じるが、その一方で、旧NAFTA（北米自由貿易協定）を想定した北米生産拠点の拡大や、アジア成長市場への進出など、日本企業のサプライチェーンのグローバル化が加速したのも事実である。データローカライゼーション政策を始めとして、各国、地域間の利害の対立が先鋭化する可能性があるが、その中で、グローバルなデータのサプライチェーン構築を模索する動きもでてくるはずである。摩擦を機会ととらえて、これからのグローバルデジタルビジネスのあり方をポジティブに考えるスタンスが企業に強く求められる時代が到来したと考えるべきである。

# 持続可能な開発目標（SDGs）で未来をひらく

**2015年に、国連サミットにおいて採択された「持続可能な開発目標（SDGs）」は、この地球が抱える社会、環境、経済問題の解決に向けた行動をすべての人に呼びかけるものです。そこで今回は国連開発計画（UNDP）イスタンブール：開発のための民間セクター国際センター（IICPSD）所長のマルコス・アティアス・ネトー氏をお迎えし、SDGsがどのように世界を変えることができるのか、またSDGsがどうして重要なのかについて伺います。**

## Mr. Marcos Athias Neto
（マルコス　アティアス　ネトー）

国連開発計画（UNDP）イスタンブール：開発のための民間セクター国際センター（IICPSD）所長

国連開発計画（UNDP）イスタンブール：開発のための民間セクター国際センター（IICPSD）の所長を務め、UNDPの民間セクター・基金チームを率いる。現在は、開発における民間セクターと基金に対するUNDPの世界的な働きかけを主導している。UNDP以前は、IDAC（Innovations & Development Alliances Cluster）にてクラスターリーダーを、チャイルドファンド・インターナショナル（ChildFund International）にて防災・減災対策部門のグローバル・アドバイザーや米国北東部の地域開発オフィサーをそれぞれ務めた。それ以前にはCAREインターナショナルに17年間在籍し、本部と現場でさまざまなポストを歴任。最後に就いたパートナーシップ・特別イニシアチブ・気候変動・持続可能生活部門でディレクターとして、気候変動に関する、特に環境団体とのパートナーシップの構築に努めた。CAREでの任務は、英国CAREにおけるアジアおよび南米の地域マネージャー（6年間）から、米国CAREのブラジル進出の陣頭指揮に至るまで、多岐にわたった。2001年には、ブラジルCAREの初代ナショナルディレクター、2006年から2008年までは、CAREの中央アメリカにおけるプログラムディレクターを務めた。このほか、南米の地域ディレクター補佐を3年間務め、リソースの動員、ナレッジ・マネジメント、支持者集めを中心に活動した。

## 民間部門におけるSDGsの進捗

**白井：**2015年に「持続可能な開発目標（SDGs）」が採択されてから3年がたちました。SDGsは、民間部門も含め、全てのステークホルダーの参加を求める画期的な提言でした。2030年の目標達成に向けて、活動の進捗状況をどのように評価されますか。

**マルコス・ネトー：**SDGsの最初の3年間で大きな前進があったと思います。これは主に、SDGsの目標が世界各国で採択されたためです。SDGsは、社会のさまざまなセクター間の共通言語にもなりました。企業と政府が共通の言語で話し合うことは、どの時代でも難しいことでした。ところが、今では「わが社は目標5、6、7に取り組んでいる」と言えば、それがどのようなことを意味しているのか、誰でも理解できるようになりました。

国単位でみても、SDGsは大きく前進しました。これまでに102カ国の政府が、SDGsの実現に向けた国内の進捗状況を独自に調査しており、グローバル目標の達成のために政策アジェンダを調整するとしています。経済界も、SDGsの採用に向けて動き始めています。これはミレニアム開発目標（MDGs）の時代にはなかったことです。

とはいえ、こうした目標を達成するための資金のめどはいまだに立っていないというのが現状です。持続可能な開発のための2030アジェンダ※1を実行に移すには多額の資金が必要ですが、十分な財源を見いだせずにいます。

私たちが直面する問題は大きく、対策の実行よりも速いスピードで拡大しています。気候変動によって多くの人々が避難をしていますが、これは世界が直面する前例のない問題のうちの二つにしかすぎません。2018年10月に、気候変動に関する政府間パネル（IPCC）が気候変動に関する新たな科学的根拠に基づく報告書を出し、地球温暖化による気温上昇はごく近い将来に1.5℃を超えると警告しました。しかし、世界各国の反応はごく限定されたものにとどまりました。

現在、避難生活を送っている人々の数は、歴史上で最大といわれています。UNHCR（国連難民高等弁務官事務所）の統計※2によれば、家を追われた人々の数は、世界で約6,850万人にのぼります。そのうち2,500万人ほどが難民で、半数以上が18歳未満の子どもたちです。残念ながら、多国間主義や国際協調に抵抗を示す人がたくさんいます。2030アジェンダは、すべての人々が力を合わせ、「誰一人取り残さない」ことを求めています。今、自国の利益を最優先する傾向が高まっていますが、自国の利益を実現する最善の策は、他国と協力して進むことなのです。

※1　SDGsを中核とする国際社会共通の目標。序文、政治宣言、SDGs、実施手段、フォローアップ・レビューで構成される。
※2　2018年6月発表

## 開発途上国の環境と回復力

**白井：**SDGsの目標の中でも、特に目標7の「エネルギーをみんなに そしてクリーンに」、目標11の「住み続けられるまちづくりを」などは世界共通の課題ですが、開発途上国では、取り組む優先順位が低い場合もあります。SDGsの課題に対処する上で、どのような活動を優先する必要があるのでしょうか。

**マルコス・ネトー：**SDGs採択以前の開発アジェンダは、開発途上国のためだけのもので、日本のような先進国の役割は財政面などで支援を行うことだけでした。2030アジェンダは、このような分断された状況を打破する初めての普遍的なアジェンダとなり、全ての国に適用されています。コロンビア大学のジェフリー・サックス教授は、「SDGsの目から見れば、全ての国が開発途上国です。SDGsのアジェンダを全て実現している国は世界のどこにも存在しないからです」と発言しています。

ただ、基本的なインフラや福祉制度が整備されていない開発途上国では、アジェンダは複雑なものになるというのはそのとおりです。日本のような先進国では、途上国とは異なるプロセスと、政府の積極的な取り組みが必要になります。私は、二つの観点からSDGsをみています。一つは、国内でSDGsの実現を支援するために必要となる観点、もう一つは、対外援助、外交政策、投資などを通して、開発途上国を支援する国際的な観点です。

従来の開発に対するアプローチとSDGsの間には、緊張関係があるともいえるでしょう。従来のアプローチは、17の目標と169のターゲットの中で優先順位を付ける必要がありました。しかし、SDGsのアジェンダは、ガバナンス、海洋、気候、不平等、健康、教育、仕事などの領域に優先順位を付けません。全ての課題に同時に取り組む必要があるのです。各国政府が自国のニーズに従って政策の優先順位を決める必要がある場合もありますが、アジェンダ自体が、ある目標を別の目標よりも優先させるということはありません。

**白井：**UNDPやIICPSDが行うイニシアチブにはどのようなものがありますか。

**マルコス・ネトー：**UNDPが立ち上げたMAPS（Mainstreaming, Acceleration and Policy Support）というプログラムは、2018年4月時点ですでに31カ国で導入されています。MAPSプログ

ラムでは、各国政府の協力の下、各国の環境政策について機械学習を使って総合的に分析します。IBM Watson®とのパートナーシップにより、AIが情報処理を行いますので、通常3カ月かかる処理が3日で終わります。その国の政策をSDGsに照らして分析し、現在の政策ですでに対応しているものは何か、目標とのギャップがどこにあるかを特定します。その後、私たちが開発したRIA（Rapid Integrated Assessment）と呼ばれるツールなどを使って、SDGsの達成に向けて有効な政策の策定、実施に作用す

るアクセラレータを見つけ出します。

アクセラレータを見つけ出すといっても、目標どうしの優先順位を付けるためのものではありません。むしろ、目標の一つ下にある階層にすでにあるアクセラレータを見つけ、SDGsの実現を加速させるためのものです。そうした複数のアクセラレータに社会が投資すれば、17の目標が同時に動き出すのです。

**白井：**興味深い取り組みですが、アクセラレータとはどのようなものですか。

**マルコス・ネトー：**よく使われるアクセラレータは、ジェンダー（性別）です。これは目標5[※3]に該当します。マッキンゼーによれば、労働市場における女性と男性の割合が同じになれば、約28兆ドルの経済成長が実現できるといわれています。また、女性は男性よりも家族の健康を気遣うことも分かっており、女性が高等教育を受け、自身と子どもたちのためにヘルスケアの知識を手にすれば、目標3[※4]と4[※5]に一歩近づくのです。

例えばアフリカ大陸の農村部では、女性が農作業のほとんどを行っています。女性の労働環境改善に投資すれば、農業の生産高を上げ、目標2[※6]にも対応できます。地方の道路整備に投資すれば、製品を市場に届けやすくなります。そうすれば目標8[※7]と9[※8]が動き出します。このように女性の労働参加への投資により、いくつものSDGsの目標実現に向けての動きが加速するのです。

持続可能なインフラの構築、市街地化は目標9と11につながります。持続可能なインフラ、農村部のインフラ、農村部と都市部を結ぶ交通、再生可能エネルギーに投資すれば、働きがいのある人間らしい仕事、平等といったSDGsが目標の実現に向けて同時に動き始めます。

重要なことは、SDGsの17の目標に別々に取り組むのではなく、目標の下の階層にある、複数のSDGsを同時に前進させるアクセラレータを見つけ出すことです。このやり方は、政府だけでなく、企業が優先順位を決める手法としても最善の方法です。企業は、比較優位のある分野から始めたいと考えるはずです。自社の得意分野は何か。コアビジネスは何か。それを理解した上で、互いに結びついている全てのSDGsに対して、自社のビジネスがどのようなインパクトを与えるかを考え、複数のSDGsに波及することを意識して優先順位を決定します。

UNDPでツールを作成する際に重視したポイントは、「How（どのように）」の質問に答えることです。A地点からB地点に行くにはどうすればよいか。ビジネスでSDGs達成をめざすオープンイノベーション・プラットフォームであるSHIP（SDGs Holistic Innovation Platform）がその一例です。

※3　目標5「ジェンダー平等を実現しよう」
※4　目標3「すべての人に健康と福祉を」
※5　目標4「質の高い教育をみんなに」
※6　目標2「飢餓をゼロに」
※7　目標8「働きがいも 経済成長も」
※8　目標9「産業と技術革新の基盤をつくろう」

**白井：**近年、世界各地で気候変動の影響による自然災害などのリスクが広がっています。災害は開発途上国にも影響を及ぼしています。開発途上国が自然災害によって直面する課題を乗り越えていくためには、どのような戦略が必要でしょうか。

**マルコス・ネトー：**開発途上国では、防災に投資できる予算が限られています。新たなインフラは、今後直面する災害を考慮して整備する必要があります。空港、道路、橋を建設する際は、従来よりも精巧な建設工程が必要になります。そこでは官民のパートナーシップが重要です。今後さらに多くの地震、ハリケーン、台風、洪水、干ばつなどの自然災害が起きても、耐え得るインフラを構築することが重要です。

もう一つの課題は人口移動です。気候変動や自然災害の防止に何も手を打たなければ、近い将来、人口の大移動、特に途上国からの移動が避けられません。

気候変動による海面上昇の最悪のケースを例にみると、マンハッタンでも、満潮時に海水が街に入ってこないよう、マンハッタン島の周囲に高いゲートを張り巡らせなければなりません。そうなるとインフラにかつてないほど多額の予算を費やすことになります。直ちに行動を起こさなければ、そのような時代がやってくるのです。

危機感を持つことはもちろんですが、経済界、特に大企業には切迫感が必要です。水やエネルギーのシステムを提供する日立のような企業にはチャンスがあります。より優れた技術、効率性の高いシステムが今後必要になります。さまざまな問題を軽減するサービスを社会に提供し、世界各地の自然災害リスクに対処するビジネスチャンスが目の前にあるのです。

**白井：**IICPSDは、民間部門を減災、防災、災害対応、災害復旧に戦略的に巻き込み、自然災害に対するレジリエンスを高める活動をしています。これまでどのような活動に携わってこられましたか。

**マルコス・ネトー：**2015年に、宮城県仙台市で開催された「第3回国連防災世界会議」で採択された「仙台防災枠組2015-2030」に、グローバルな基準が示されています。日本が防災に多大な努力を払ってきたからこそできた枠組みです。UNDPは過去数十年にわたって各国政府と協力して災害に備える活動を進めてきました。

防災に投資する1ドルは、災害対応と復旧に支出する7ドルに相当するにもかかわらず、防災に十分な投資が行われているとはいえません。防災に投資することの価値が理解されにくい現状があります。それは、下水管より橋への投資が優先される状況に似ています。一般の人々は、道路の下にある下水管には注目しませんが、目に見える橋には注目します。これと同様に防災も見えないのですが、フロリダで猛威をふるったハリケーンのような災害が発生すれば、誰もが避難しなければなりません。

仙台防災枠組では、政府や企業とも連携します。私たちは、自然災害に直面する準備ができていない企業が多いことを学びました。レジリエンスが高く、災害に対して優れたBCP（事業継続計画）がある企業は消え去ることはないので、復興の一翼を担うことができます。操業を続け、仕事を提供し、自然災害から復旧するために必要な物資を生産することができます。

## SDGsに対する企業の貢献

**白井：**ESG（環境・社会・ガバナンス）投資が広まる今、企業には事業を通じて社会課題にアプローチするさまざまな方法があります。企業が利益を確保しつつ、社会課題を解決するビジネスを開発途上国で展開するためには、どのようなパラダイムが効果的でしょうか。

**マルコス・ネトー：**企業が自社のビジネスモデルにSDGsを組み込む際、二つの課題に直面します。

一つは、SDGsを組み込むことは慈善事業ではなく、市場開拓のチャンスであるとCEOを説得する、という課題です。私たちは、SDGsに投資すべきだとCEOに説明するのが難しいと語る中間管理職の方々を見てきました。これらの内部的な課題は、企業が役員の報酬を決めてきた長年の歴史と関係します。世界的にCEOや経営幹部は短期的な業績に基づいて報酬が支払われる傾向がありますが、SDGsは長期的なアジェンダです。SDGsに取り組むことは、企業を長期にわたり持続可能な組織にすることにつながります。環境の持続可能性だけでなく、さまざまな角度でものを考える必要があります。企業も自らの存続期間を考えることが重要です。今日存在している企業が明日も存在するとは限らないことは歴史が教えてくれています。

1900年にダウ・ジョーンズ工業株価指数に含まれていた企業のうち、2000年まで事業を継続していたのは、わずか2社でした。それ以外の企業は全て消え去りました。SDGsは、企業が長期間存続するための戦略になる可能性がありますが、短期の利益を

上げるという期待との折り合いをどうつけるかという課題が残っています。

二つ目の課題は資本市場からの圧力です。投資家は、米国企業の場合は四半期ごとに報告書を受け取ります。長期ではなく、短期の業績に注目します。企業は、「利益は四半期ごとに報告しません。それでも大丈夫です」と言い放つ勇気を持つ必要があります。必要な期間は、1年、2年、いや数年単位です。

法規制の枠組みが、SDGs実現の障害になる場合もあります。現在の法規制は、従来の化石燃料中心の経済を前提にしています。SDGsが求めるのは、経済モデルや経済システムを、長期的な視点で、財務的側面だけでなく、社会的側面、環境的側面にも着目する「トリプルインパクト」を考慮したものに変更することです。

インパクト投資の父、ロナルド・コーエン氏は、「企業の成功を測る物差しは150年間、利益のみだった」と述べています。利益が企業を分析する唯一の枠組みでした。どれだけ投資して、どれだけ収益があったのか、という物差しです。その後、1960年代から1970年代の初めにかけて「リスク」という二つ目の物差しが導入されました。企業分析の枠組みが、利益とリスクという2要素となった結果生まれたのが、リスク調整後利益という概念です。

今必要な三つ目の物差しが「インパクト」です。インパクトとは、企業が社会全体に与える影響です。今後は、投資家と社会全体が企業のインパクトを評価する分析的枠組みも必要になります。利益とリスクという２要素に社会全体へのインパクトという要素を追加し、3要素で企業を評価することが可能になるのです。

ここにボストン・コンサルティング・グループが最近実施した調査があります。同社が社会全体のインパクトを重視する方向にシフトしつつある200社を分析した結果分かったのは、今なお企業の成功を測る主要な枠組みであり、株主にどれだけの利益があったかを示す指標である株主総利回り（Total Shareholder Return）が、こうした企業で上昇しているという事実でした。長期間にわたり社会全体のインパクトを念頭に戦略構築した企業は、短期的に株主利益だけを追求する企業よりも大きな利益を生み出しているのです。長期的なインパクトと短期的な株主利益のバランスを正しく保つことが決定的に重要です。

投資家ももっと企業に要求すべきであり、日本のような高齢化社会では、実際にそうした動きがみられます。例えば、年金基金には債務を負う期間をこれまでより長期で求めるようになり、企業には長期間利益を出し続けることを求めます。10年、20年では足りません。50年、60年にわたって年金を支払い続ける必要があるからです。長期的に利益を出す企業に投資すれば、長期的・短期的利益のバランスが変化するため、投資に当たっての考え方が変化します。

バランスを変えるもう一つの重要な誘因はミレニアル世代です。この世代が、力を持ち、豊かになり、消費者になれば、これまで以上に企業や製品に社会的価値を求め、それを基にどの企業から購入するかを選択するようになります。次の変化の波が来て、バランスや緊張関係が本格的に変化し始めるでしょう。

**白井：**人々の姿勢やアプローチに何らかの変化が生まれることは確かでしょう。これから私たちが目にする可能性がある変化はどこに現れるでしょうか。

**マルコス・ネトー：**消費財メーカーのユニリーバは、持続可能性

を前面に押し出したブランドを生み出し、従来よりもはるかに良い業績を残しています。決断に当たって、同社は生産現場を見渡し、どうすればもっと環境に配慮した方法で生産できるか、どうすれば水の使用量を減らすことができるか、再生可能エネルギーを使用できるか、を考えました。そして持続可能性を特徴とするブランドで消費者に販売する方法、貧困層に商品を販売する方法にも着目しました。世界人口の半数の人々がその市場にいます。同社は、従来の流通ネットワークでは貧困層にまで到達できないことに気付き、新しい流通戦略の策定に乗り出しました。

貧しい人々が、巨大な多国籍企業の製品を販売する代理店となり始め、貧困層に突如、新たな仕事が生まれ、新たな企業が誕生

し、新たな起業家精神が育ちました。全ては、そのような戦略を策定したことから始まりました。これが優先順位を付けることの一例ですが、同時に複数のSDGsを実現することの例でもあります。経済界にとって、SDGsはビジネスチャンスなのです。

BSDC（Business & Sustainable Development Commission）は、SDGsを通して毎年12兆ドル規模のビジネスチャンスが生まれる可能性があると試算しています。企業が社会的責任を果たすだけでは、こうしたチャンスは生まれません。企業がSDGsを分析し、自社のビジネスモデルをSDGsに合わせることで、チャンスにできるのです。UNDPがJapan Innovation Networkとパートナーシップを結び、SHIPを創設したのも、そういう理由です。SHIPは、

現在日本でのパイロット期間中ですが、いずれは世界的に導入していきます。

SHIPの目的は、実際のプロセスを企業に順を追って紹介することです。SDGsとは何か。ビジネスの枠組みとしてSDGsをどうみるか。ビジネスモデルをどのように変更するか。利益をもたらし、社会を進歩させ、環境に配慮したビジネスモデルをどう立ち上げるか。そうしたことを一つ一つみていきます。

**白井：**技術革新と新たなビジネスモデルで生まれる市場も存在します。そこには、大きなチャンスと、乗り越えるべき重要な課題があります。

**マルコス・ネトー：**経済界がSDGsに高い関心を抱いているのも、そのような理由です。SDGsは、収益性、商業性、新しい市場、イノベーションといった企業の中心的な目的に訴えかけた最初の開発アジェンダです。慈善や社会的責任を求めるだけのアジェンダではありません。企業の社会的責任は入り口としてはすばらしいのですが、それだけでは不十分です。世界各国の企業の方々と話した結果、企業は、どうすればよいのかという「How」の部分で悩んでいることが分かりました。「12兆ドル？ それはすばらしい。その一部にあずかりたいが、どうすればよいのか。大きくて複雑な問題に照らして、自社のビジネスモデルを批判的にみるようにといわれるが、どうすればよいのか」ということです。

**白井：**十分な財源を確保して、さまざまなプレイヤーに参加してもらうために、官民のパートナーシップを推進することが重要です。そこには他国の企業との協働も必要になるでしょう。企業と政府の協力関係を推進するには、どのようなパートナーシップが望ましいのでしょうか。UNDPはどのようなサポートを提供してくれるのでしょうか。そこには官民の新しい連携が生まれるのでしょうか。

**マルコス・ネトー：**官民のパートナーシップは今後、必要不可欠になっていくでしょう。各国の政府は、市場に、これまでとは異なる方向性を示す必要があります。投資家にも、SDGs中心の市場機能を望むことを知らせていく必要があります。

例えば、化石燃料に補助金を出している政府は依然としてたくさんあります。再生可能エネルギーに補助金を出すよう方向転換することは、先進国だけでなく、開発途上国でもすばらしいことですが、財政制約のなかでは、永久に補助金を出し続けることも、新しい補助金制度をたくさん設けることもできません。政府は、これからの補助金制度やインセンティブはどのようなものであるべきか、選択を迫られます。

国連事務総長も方向性を明確にしていますが、化石燃料への補助金をやめて、再生可能エネルギーに補助金を出す方向に転換し、持続可能な開発を推進する方向に舵を切るときが来ています。政策と法規制の重点をシフトし、市場が向かう方向を調整することが、政府の役割として重要になります。

UNDPでは、SDGsに沿った投資とビジネスモデルが普及する環境を政府がつくる際に助言するための研究を行っています。

**白井：**ESG投資が推進され始めてから、企業がビジネスを通してどのように社会的課題に取り組んでいるかに注目する投資家が増えてきました。今後、企業が社会や環境に与えるインパクトと企業の価値を正確に評価するために、投資家はどのようなアプローチを採用する必要がありますか。

**マルコス・ネトー：**UNDPでは、2018年9月、インパクト・マネジメント・プロジェクト（Impact Management Project）とのパートナーシップの下、SDGインパクトプラットフォーム（SDG Impact Platform）を立ち上げました。これは、投資家、銀行、プライベート・エクイティ・ファンド、ベンチャー・キャピタルを対象に、自らの投資が社会と環境に与えるインパクトを知る明確な基準を示したものです。UNDPは、SDGを推進する投資家や企業に認定マークを提供することも視野に、こうした基準を作成しています。将来は、投資家が自らの投資が社会に与えるインパクトを説明できる認定プロセスをつくりたいと考えています。企業にも同様の「ビジネス行動要請（Business Call to Action）」というプラットフォームを示し、現在、住友化学、味の素、良品計画など、日本企業を含む220社がメンバーになっています。このプラットフォームでは、社会の貧困層を製品の生産者、供給業者、販売代理店、消費者として組み込むビジネスモデルを推進しています。

企業が変わり始め、投資家の注目も集まりつつありますが、まだまだ長い道のりです。UNDPの重要な役割は、「How」の部分を企業に説明することであり、全力でこの課題に取り組んでいます。

## 日本への期待

**白井：**日本政府は、国際的にもSDGsに貢献したいと考えています。加えて、日本は自然災害に対応してきた経験から、防災に関する技術とノウハウを持っています。防災の分野で、またSDGsの課題に協調して対応する環境づくりの面で、日本にどのようなことを期待されますか。

**マルコス・ネトー：**最初に、UNDPと国連が日本から受けている支援に対して、日本政府に感謝の意を表します。日本政府と国民のみなさんは寛大で、世界で果たすべき役割、UNDPのような組織をサポートする意味をよく理解してくださっています。

日本のみなさんが政府を通して、世界中にある私たちの組織を資金的に支援してくださっていることに感謝し、最大限に生かせるよう、全力を尽くします。

リソース、財政的サポート、経験、技術など、日本はさまざまな面で貢献できるというお話はそのとおりです。日本が持つイノベーションのエコシステムは、世界の羨望（せんぼう）の的です。どうすれば、それを開発途上国でも再現して、発展の諸段階を飛び越えていけるのでしょうか。例えば、ケニアは、大規模な固定電話回線がない国から、たいていの人が携帯電話を所有している国へと移行できました。日本には、このような一足飛びの発展を実現しようとする国を効率的にサポートするための経験、技術、ソフトスキルがあります。UNDPは、こうした日本の努力をお手伝いできることを大変うれしく思っています。

今回の日本訪問で、多くの政府高官や経済団体の方々とお会いしました。日本政府と経済界は、SDGsを評価し、積極的に取り入れようとしていることが分かりました。企業、政策、SDGsの3者を結びつけるエコシステムが出現しつつあり、短期間のうちに強固

なものになる可能性があります。

**白井：**デジタルテクノロジーは、SDGsの目標達成を実現させる大きな可能性を秘めています。日立は技術を通して、またエネルギー、水、ヘルスケア、情報技術の各分野におけるソリューションを提供することで、社会に貢献しています。日立がSDGsの目標達成に向けて取るべき行動について、アドバイスをいただけますか。

**マルコス・ネトー：**日本のエコシステムは、日本がSDGsを実現する際に役立ちます。日本から提供されるものを全て吸収したい、またSDGsにかなう形で日本の企業に対して市場を開放したいという強い願いが世界にあることは間違いありません。日本の中小企業や日立のような大企業が、アフリカや中南米に進出する際にSDGsに責任ある姿勢で取り組むことが、支援の一つの形です。企業の利益になり、事業を展開する国に、経済的、社会的、環境的にプラスとなるビジネスモデルを携えて行くことも支援になります。自社のビジネスモデルを分析してください。競争力のある市場を求めて海外に進出してください。その際は、今日の世界的な課題を解決するSDGsと同じ方向性のビジネスモデルやソリューションを世界に示してください。

国連の潘基文元事務総長はよく、「私たちは絶対的貧困を終わらせることができる歴史上で初めての世代であり、最悪の気候変動に対処できる最後の世代でもある」と言っていました。

私たちがチャンスを逃せば、子どもたちが代償を支払うことになります。日本企業も含めて、企業の前には、技術を人類のために使う方法を示す途方もなく大きな機会が広がっています。企業は、人類に奉仕しながら利益を上げることができるのです。政府と企業が手を携えて、人類の未来を守るために働くことが重要です。

こうした課題に取り組み、災害防止や気候変動に投資して開発途上国を支援することは、世界のすべてのプレイヤーに有益です。こうした支援は、気候変動による最悪の事態がもたらす影響、例えば祖国を離れることを余儀なくされるような事態を緩和するでしょう。人々は自国にとどまり、人間らしい生活を送り、自分が住むと決めた環境で子どもたちを教育できるようになります。私たちは、SDGsの目標達成に向けて、行動を加速しなければなりません。SDGsのパートナーを増やし、もっと速く進むのです。解決すべき課題も、これまで以上に速く進行しているのですから。

**白井：**日立は、水、エネルギー、交通などの社会インフラシステムを提供する企業です。近年の自然災害を見ると、現在のインフラでは想定を超える災害に耐えられない可能性があります。一方で、今あるインフラを入れ替えるには、多額の資金が必要になります。このような課題をどのように解決すればよいのでしょうか。

**マルコス・ネトー：**技術が決定的に重要です。AIや、私たちがまだ見ていないイノベーションが求められるのです。世界の開発途上国が構築すべきインフラと、先進国がアップグレードすべきインフラを考えると、必要な資金は天文学的な数字になります。そのような資金はどこにもありません。インフラの構築と機能向上を効率的に行い、コストを削減するために技術を生かし、イノベーションを生み出す体系的なプロセスが求められます。現存するインフラの中で、アップグレードを早めるべき部分と時間的に余裕のあるものを、ビッグデータを活用して見分けることができれば、限られたリソースの使い道に優先順位を付けやすくなります。

「Society 5.0」の時代がすぐそこまで来ています。現在は不可能と思えるような課題を「Society 5.0」の時代ではどのように解決していくのでしょうか。

私が敬愛するネルソン・マンデラ氏は「何事も成し遂げるまでは不可能に思える」と発言されています。私たちは成し遂げなくてはならないのです。

**白井：**本日は貴重なお時間をいただきまして、ありがとうございました。

## 対談後記

今回は、UNDP・IICPSD所長であるマルコス・アティアス・ネトー氏をお迎えし、SDGsにおける民間セクターの役割をはじめ、社会課題解決に向けた企業の持つべき視点や課題などについて幅広く話をお伺いしました。利益を上げることが求められる民間企業の立場から社会課題に向き合うことは、非常にチャレンジングです。社会課題への取り組みを市場開拓の契機と捉え、技術力を生かしたイノベーションの重要性を改めて感じました。

# データ覇権競争を背景に強化される米中欧のデータ流通・保有規制

研究第二部　部長　松本　健

近年データは「21世紀の石油」と呼ばれるようになった。2011年には世界経済フォーラムは、既に個人データの価値に注目、同年の報告書「Personal Data: The Emergence of a New Asset Class」で、「個人データは、インターネットにおける新しい石油であり、デジタル世界における新たな通貨である」とし、その経済的価値の高さを論じた。それから約8年、今ではIoT・AIなどデジタル技術の進展により、ヒトだけでなくモノのデータもまた、その活用が経済成長の源泉になると認識されるようになった。他方、ヒトであれモノであれ、それらに関わるデータはインターネットを介して容易に収集でき、結果企業による囲い込みや寡占化も生まれやすい。実際、米国のGAFA[1]や中国のBAT[2]などプラットフォーム企業が、個人データの収集・活用を武器に急成長した。さらに国レベルでも、国外へのデータ流出は極力制限し、流入は促進したいと考える国も現れている。本稿では、国・企業をめぐるデータ覇権競争の観点から、中国・米国・EUにおけるデータ越境規制の動向を論じる。

## 1. 拡大するデータ越境移動と強化されるデータ越境規制

### 1.1　拡大するデータ越境移動

経済のグローバル化の進展により2000年代初めより拡大してきた世界のヒト・モノ・カネの越境移動は、2008年金融危機後に停滞、一方データの越境は、国・企業・個人を結ぶインターネットの構築により爆発的に成長している。2005年から2014年の10年間で、越境データの帯域（量）は約4.7Tbps（毎秒テラビット）から約221.3Tbpsへと約45倍に拡大した。特に、米国、中国を中心とするアジア、EUの3地域間での拡大が顕著であり、これら地域が世界の越境データ拡大をけん引している。

越境データは、大きく個人データと非個人データに分けられる。個人データは、氏名・住所、さらには社会保障番号や購買履歴、位置情報を含む。非個人データには、個人データ以外のものすべてが含まれるが、例えば製造業における設計図面や製造工程の配置図などの産業データ、交通・エネルギーなどの設備稼働情報を含むインフラ関連データが含まれる。近年では、両者の境界線は曖昧になっており、例えば、医療における診療歴や金融における口座情報などのデータは、個人データでもあり、非個人データでもある。

### 1.2　中米欧で強化されるデータ越境規制

国境を越えた大量のデータ移動をけん引してきた中国・米国・EUを中心に越境データを規制する動きが加速している。規制には、国外へのデータ流通に対するものと、国外からデータを取得・保有することに対するものに分けられる。データ流通規制は、企業などに対し物理的サーバを国内に設置させ、そこに当該国内で取得したデータを保存・運用することを求める規制である。他方、データ保有規制は、当該国にとって重要なデータを、企業買収などの直接投資を通して第三国企業が取得しようとする際に、これを否認するものである。

こうした流通と保有という規制手段の違い、そして前述の個人データと非個人データという規制対象の違いを踏まえ、中国・米国・EUが進めている実際の規制を整理すると、図1の通りとなる。

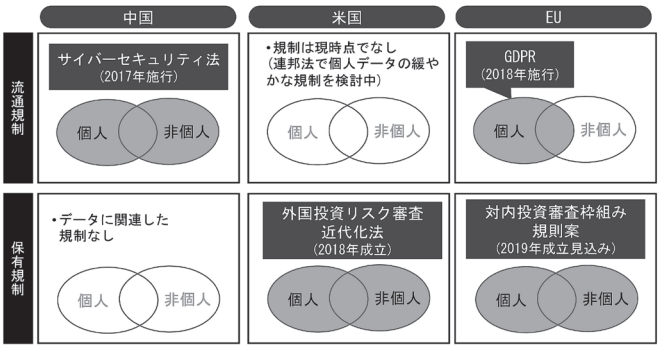
現時点で成立している規制として、中国の個人・非個人データを対象とした流通規制「サイバーセキュリティ法」、米国の個人・非個人データを対象とした保有規制「外国投資リスク審査近代化法（FIRRMA[3]）」、がある。また、EUでは個人データの流通規制「一般データ保護規則（GDPR[4]）」が2018年に施行、加え

[1] Google、Apple、Facebook、Amazonの4社の総称

[2] Baidu、Alibaba、Tencentの3社の総称

[3] FIRRMA: The Foreign Investment Risk Review Modernization Act

[4] GDPR: General Data Protection Regulation




注：白い楕円は規制なし、網掛けの楕円は規制あり、を示す
資料：各法律・規則などより日立総研作成
図１　中国・米国・EU のデータ流通規制と保有規制

て保有規制でも「対内投資審査枠組み規則案[5]」が欧州議会で議論されており、個人・非個人データを対象としたEU全体の規制として2019年春から夏にかけて成立見込みである。各国・地域のデータ規制にはそれぞれ、プライバシーの保護やサイバー空間の安全確保だけでなく、データの国際的覇権獲得を通して国家安全保障の保全と次なる成長を実現しようとする政策的意思が込められている。実際にいずれの規制も、内容自体は諸外国に対して無差別な適用をうたっているが、特に米国とEUではその運用面において、特定の相手国を念頭に置いている。2章以降で、中国・米国・EUそれぞれの規制をデータ覇権の観点も交えて考察する。

## 2. 中国：国内の膨大なデータを国家の管理下へ置くデータ流通規制

データ越境規制について国際的に広い関心を集めるきっかけとなったが、2017年6月に中国が施行したサイバーセキュリティ法(中華人民共和国網絡安全法)である。同法では、何らかの情報システムを所有・運営する「ネットワーク運営者」のうち、特に国家の安全や経済、公共の利益に与える影響が大きい「重要情報インフラ運営者」を指定し、中国国内で収集・生成した個人情報と「重要データ」を国内に保存することを義務付けている。「ネットワーク運営者」や「重要情報インフラ運営者」、「重要データ」の定義については、サイバーセキュリティ法本文の中では明確にされておらず、現在策定が進められている各種の条例・弁法（日本の政省令に相当）やガイドラインの制定を待つ必要があるが、現在意見募集稿として公開されている草案を確認する限り、ほぼすべての企業に対し、個人・非個人問わず実質すべてのデータについて、国内保存を義務付けることになると予想される[6]。なお、どうしても国外に持ち出す必要がある場合、企業はデータの越境移転を業種所管当局（工業情報化部、交通運輸部など）に申請し、安全評価を含む審査を受けることになるが、実際の運用に際して当局から許可が得られる可能性は未知数である。また、特に個人情報は、仮に個人の同意があっても当局の承認がなければ国外に持ち出せない。ここに、個人の同意があれば越境移転できるEUのGDPRとの決定的な違いがある。このように、サイバーセキュリティ法により、中国のデータは国家の管理下に置かれているといえる。

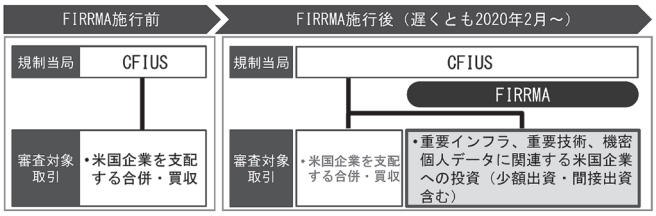
中国政府は過去、データは自由に流通させて活用すべきとの考えを持っていた。しかしその後、中国でのインターネット普及などを背景に、2016年より「互聯網＋（インターネットプラス）」を国家戦略として推進、インターネット技術（モバイル・インターネット、クラウド・コンピューティング、ビッグデータ、IoT）に製造業や医療、物流などの産業システムを結び付け、経済成長を探るようになった。中国政府は、サイバーセキュリティ法の目的として、サイバー空間の安全を維持するため、政府・企業のネットワークや制御・管理システムなどへのサイバー攻撃・不正侵入を阻止する、と説明している。確かにこれも背景にあると思われるが、インターネットプラス政策が生み出した膨大な産業データこそが成長の源泉であると捉え、巨大な中国市場から生まれるデータは諸外国ではなく自ら管理し活用したいとする考えが根強くあると考えられる。同法1条「サイバー空間における国家主権を維持する」がいみじくもこれを言い表している。

## 3. 米国：国家安全保障上の対中政策を主眼にデータ保有規制を強化

米国では、1989年以降、国家安全保障、特に防衛産業の保護を主な目的に、対内直接投資に対する規制が設けられ、実際の審査は省庁横断組織である対米外

[5] Framework for Screening of Foreign Direct Investments into the European Union

[6]「重要情報インフラ運営者」について、同法37条は、通信、金融、エネルギー、水、交通など産業分野を挙げているが、あくまでも例示列挙であり、「重要情報インフラ安全保護条例（意見募集稿）」や法令の運用により、より広い産業分野が対象となる可能性がある。「重要データ」は、「データ海外送信安全評価ガイドライン（意見募集稿）」にて、電力、交通、電機・電子など全27業種において対象データを広範に規定している。

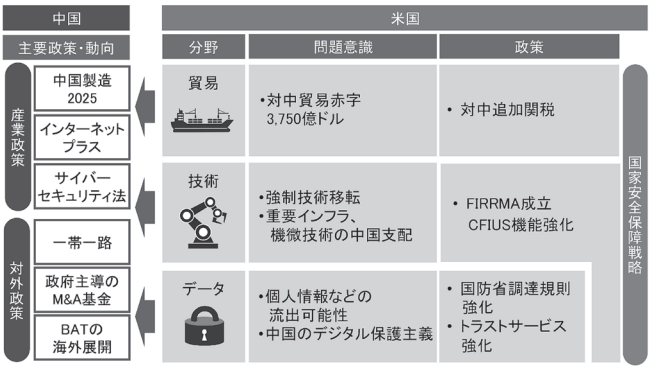



資料：各種資料より日立総研作成
図２　FIRRMA が規定する CFIUS による審査対象取引

国投資委員会（CFIUS[7]）が担ってきた。現在もこの規制の大枠は変わらないが、2018 年 8 月に成立した FIRRMA は、CFIUS の審査対象を、安全保障上懸念のあるデータ取得を伴う投資へと拡大した。FIRRMA が規定する CFIUS の審査対象を図 2 に記したが、今回新たに、重要インフラ・重要技術・機密個人データの三つが明文化されている。重要インフラや重要技術については、インフラ施設の配置データや障害データ、重要技術では自動運転などの設計・実験データといった非個人データが対象となることが想定される。

データ保有規制強化において、米国が安全保障上対策すべき国として念頭に置いているのは、中国であると考えられる。2016 年には、Tencent によるドイツ HERE Technologies（デジタル地図サービス）への出資を不承認とし、2018 年 1 月にも、Ant Financial による米国の MoneyGram（国際送金サービス）の買収を不承認とするなど、中国企業によるデータ取得を安全保障上の脅威とみなし対処してきた。上記はいずれも今回の FIRRMA 成立前の運用面での対応であったが、今回の FIRRMA 成立で、データ取得を伴う対内直接投資も安全保障の観点で厳しく審査する、という米国政府の姿勢が規律化された点に、注目すべきである[8]。

また、FIRRMA によるデータ保有規制は、米国による包括的な対中政策の重要な構成要素の一つである点にも触れるべきであろう。米国には、国家安全保障は、軍事だけでなく、経済・貿易、技術さらにはデータも含めた包括的な優位性によって保障されるとの基本的な考え方がある。図 3 は、中国による主要政策・動向と、それに応じた米国の対中政策をまとめたものである。近年中国は、中国製造 2025 や、第 2 章でもみたインターネットプラス、サイバーセキュリティ法などの産業政策、そして一帯一路などの対外政策の強化を進め、国際的プレゼンスを高めてきた。米国は中




資料：各種資料より日立総研作成
図３　中国の主要政策・動向と米国の対中政策

国のこれらの一連の動きを国家安全保障上の脅威として位置付けていることが分かる[9]。例えば貿易では、対中貿易赤字 3,750 億ドルを背景に 2018 年に相次いで追加関税を発動したが、中国による知的財産侵害を根拠としたことからも分かるように、貿易不均衡の是正だけでなく、知的財産という産業基盤保護による安全保障確保のための措置でもある。また、データにおいても、FIRRMA による対内直接投資への規制に加えて、米国政府機関による中国製通信機器使用を契機とした情報流出を懸念し、国防省調達規則を強化、これら機器の政府調達を禁止した。米中両国の対峙は今後長く続くことが予想される中、米国のデータ保有規制は対中国を念頭に今後一層強化されることが予想される。

## 4. EU：流通規則・保有規則の両輪で域内データを囲い込み

### 4.1　データ主権を米国企業から EU 市民に取り戻す GDPR

EU は、2018 年 5 月施行の GDPR でデータ流通を規制している。この規制により EU は、域内の個人データの自由な流通を担保しつつ、域外移転を原則禁じた。GDPR の内容は、既に多くの文献で説明されているため本稿では割愛するが、個人の基本的権利を保護するという基本理念の下、事業者によるデータ利用に対する個人の権利の明確化や、事業者が違反した際の高額な制裁金の設定など厳格に定めている。

GDPR は、条文上はあくまでも個人の権利保護に主眼が置かれているが、運用面ではこれまで EU 域内でサービスを拡大してきた米国プラットフォーム企

[7] CFIUS: Committee on Foreign Investment in the United States

[8] FIRRMAによる対内直接投資規制とデータ保護をめぐる動向は、本誌後段の論文で渡井氏が論考している。

[9] 米国政府によるサイバーセキュリティ法の評価については本誌後段の論文で Lundell 氏他が触れている。

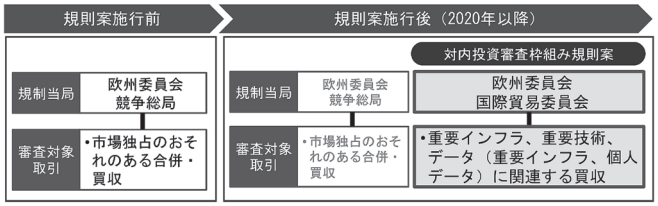
業 GAFA へのけん制を意図しているようにみえる[10]。2018 年 5 月 25 日の GDPR 施行日に、フランスの非営利プライバシー保護団体が Google と Facebook に対し、強制的に個人からデータ利用の同意を取得したとして提訴、同国データ保護監督当局が調査を開始している。このうち Google に対しては、2019 年 1 月、施行後初めて GDPR 違反として、5,000 万ユーロ（約 62 億円）の罰金支払いを命じるに至っている。これは、EU 市民のデータは米国企業のものではなく EU のもの、としてデータ主権を EU に取り戻す動きとも言える。

### 4.2　中国を念頭に草案進む対内投資審査枠組み規制案

EU では欧州議会が、個人・非個人両データを対象に、データ保有規制導入に向けた検討を進めている。それは「対内投資審査枠組み規則案」と呼ばれ、米国の FIRRMA と同様の規制内容になる。

EU は、これまで独占禁止法を通して、外国企業による企業買収を防いできたが、その適用範囲はあくまでも市場独占のおそれがある事案に限定されていた。2019 年春から夏にかけ成立が見込まれる対内投資審査枠組み規則案では、独占の有無を問わず、対内投資が EU の安全保障を脅かすと当局が判断する場合に買収を差し止める。これまでも EU 加盟国には各国で同趣旨の対内投資規制があったが、本規則により欧州委員会と加盟国間で情報共有し判断を下す。審査対象には、現在の草案を見ると、EU 市民の個人情報や重要インフラデータなど、データ取得を伴う買収が含まれる。今後、データを保有する EU 企業、例えばインフラ運営会社や施設保守会社、シェアリング・サービス会社などの買収が審査対象となる可能性がある（図 4）。

EU はこの規則案で、特に中国企業への対応を念頭に置いている。近年、ロボット・メーカ Kuka 社や半導体メーカ Aixtron 社の買収（ともに 2016 年）など、ハイテク分野を中心に中国企業による EU 企業買収事案が増えている。これに対し EU は、防衛・軍事さらには経済面での安全保障の確保には、EU 全体での対中投資規制の強化が必要、との問題認識を持つようになり、本規則案の策定が始まった経緯がある[11]。また、本規則案策定の際、欧州委員会の草案に対し、欧州議会がデータも審査対象とすべしとして加筆修正した経緯があることからも、いかに EU がデータ保護を重視しているかが分かる。対中国でもしかり、本規則案で EU は、ロボットなどハイテク分野だけなく、BAT などエンドユーザ・データを扱うサービス企業による投資にも備えていると考えられる。




資料：対内投資審査枠組み規則案などより日立総研作成
図 4　対内投資審査枠組み規則案が規定する審査対象取引

## 5. むすび

本稿ではこれまでデータ越境規制の動向をみてきたが、最近はデータの越境移動を促す枠組みの構築や、それに向けた国際的議論も始まっている。例えば、2018 年 12 月に発効した TPP11 には、データ越境移動の自由化に関するルールが盛り込まれている。また、WTO の場でも、ここ 1 年の間に日本・米国・EU が協議を重ね、2019 年 1 月、WTO 加盟の有志 34 カ国・地域に具体的なルール作りを呼び掛けた。WTO での正式交渉開始の意思を確認する共同声明も既に発出され、今後ルール作りの加速が見込まれる。日本・米国・EU が検討しているルールは、データの保護が十分で収集・活用の仕組みも信頼のできる国・地域の間で、個人・非個人両データの移転を相互に認め、他方それが不十分な国へのデータ移転は厳しく制限する、というものである。そこにはデータを国家管理下に置く中国へのけん制の目的もあるとされており、実際 EU にとっては、米国企業への脅威はあるものの、対中関係では米国と連携する、との政策的意思も垣間見られる。日本政府はこの枠組みを「信頼ある自由なデータ流通」と呼んでいるが、まさに今後のデジタル技術やデータ流通に関わる国際的な枠組みやルールは、条文だけではなく相互の「信頼」を基盤に成立するようになると考えられる。それには多国間で「信頼」を担保する仕組みも重要になる。流通させるデータの真正性を証明する機関の整備や、その機関の信頼性を担保する国家間の相互承認の枠組みなど、越境流通基盤構築への期待も高まる[12]。

[10] GDPR の持つ対米国企業の戦略的位置付けについて、本誌後段の論文で池貝氏が紹介している。

[11] 欧州議会の 2017 年 5 月報告書「Foreign direct investment screening-A debate in light of China-EU FDI flows」

[12] データの国際流通を支えるトラスト基盤について、本誌後段の論文で手塚氏が論考している。

# アメリカにおける対内直接投資法の改正とデータ保護

慶應義塾大学　大学院法務研究科
教授　渡井　理佳子

（わたい　りかこ）慶應義塾大学法学部法律学科卒業、同大学院法学研究科修士課程修了、Harvard Law School LL.M. Program 修了、筑波大学大学院ビジネス科学研究科企業科学専攻後期博士課程修了、博士（法学）。米国ニューヨーク州弁護士。

CONTENTS



アメリカでは、オバマ大統領の民主党政権の時代より、安全保障の見地からの対内直接投資法の見直しが始まり、トランプ大統領の共和党政権に入ってもその動きは踏襲されてきた。その結果、2018 年 8 月に、改正法である外国投資リスク審査現代化法（Foreign Investment and Risk Modernization Act of 2018, FIRRMA）が成立した。この背景には、中国が「中国製造 2025」等の政策を通じて製造強国を目指してきたことがあり、FIRRMA は規制の強化を図るものであった。

本稿は、FIRRMA による新たな対内直接投資規制を概観し、データ保護をめぐる動きについての若干の検討を試みたものである。

## 1. アメリカにおける対内直接投資規制

### 1.1　アメリカにおける対内直接投資規制法の変遷

対内直接投資規制の対象となる典型的な取引は、外国国家や外国法人を含む外国投資家による、自国企業の買収である。日本やアメリカなどの、経済協力開発機構（OECD）の加盟国は、OECD 資本移動自由化コード 3 条の下で、①公の秩序を維持し、または公衆の衛生・道徳・安全を保護する目的、②安全保障上の利益を確保する目的、そして③国際平和と安全に関する保護を履行する目的から、必要と考える行動をとることができる。そこで、加盟国は、対内直接投資は原則自由であるとの前提に立ちながらも、国内法を設けて必要な規制を導入してきた。

アメリカにおいて、対内直接投資規制法が制定された契機は、1988 年に日本企業がアメリカの半導体企業の買収を計画したことにあった。この時は、アメリカ国内より安全保障上の懸念が相次いだために日本企業が買収を断念したが、アメリカ議会は政治的圧力でしか買収を阻止する術がなかったことを重視し、翌 1989 年に最初の規制法（Exon-Florio Amendment）を設けた。この法は、防衛産業の保護を主たる目的に、OECD コード 3 条の安全保障の見地からの規制を対内直接投資に導入したものである。具体的には、アメリカの安全保障のために、対内直接投資の中止を命令する権限を大統領に付与したものであり、この枠組みは今日の FIRRMA に至るまで維持されている。

実際の審査は、投資計画の当事者からの任意の通知を受けて、財務長官を委員長とする省庁横断的な機関である対米外国投資委員会（Committee on Foreign Investment in the United States, CFIUS）が行っている。取引の当事者が外国同士であり、アメリカ企業が直接関わっていない場合であっても、当該取引がアメリカの安全保障に外国の支配をもたらすものであるならば、CFIUS の審査の対象となる。大統領が判断をするのは、CFIUS が取引に安全保障上の脅威があると判断した場合に限られているため、CFIUS の審査過程が非常に大きな意味を持っている。

法は、幾度かの改正を経ているが、2001 年 9 月 11 日のテロ事件を受けての 2007 年の改正法である外国投資及び国家安全保障法（Foreign Investment and National Security Act of 2007, FINSA）では、安全保障の概念に国土安全保障（Homeland Security）が加えられた。これにより、重要なインフラへの対内直接投資について、CFIUS の審査密度が高められることとなった。しかし、1989 年の法の導入から、2018 年の法改正に至るまでの約 30 年間には、データ保護に関する規定は設けられていなかった。

### 1.2　安全保障とデータ保護

これまで、実際に大統領が対内直接投資の中止を命令したケースは 5 件あり、1 件を除いては、全て中国に関わる案件となっている[1]。1990 年に最初の中止命令が出されているが、その次に出されたのは 22 年後の 2012 年のことであった。オバマ大統領によるこの中止

命令は、データ保護にも関わるものである[2]。

この事件は、中国の大手建設機械メーカーの子会社であるアメリカのRallsが、風力発電所計画に持分を有するアメリカ企業を買収したというものである。買収の目的は、中国の親会社の部品を用いて風力発電所を建設することにあった。中止命令の理由は、RallsがCFIUSに通知することなく買収を完了していたことに加え、風力発電所の計画区域が海軍の施設に近接していたことにあったと考えられている。

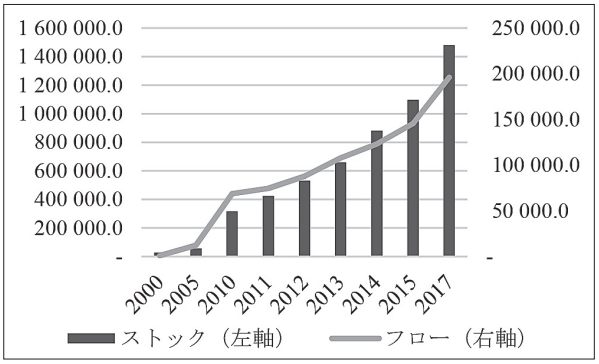
Rallsに対する中止命令の教訓は、不動産取得を伴う対内直接投資のうち、安全保障に関わる施設に近接するような計画については、情報流出への懸念がCFIUSの審査の際に考慮されることである[3]。中止命令とほぼ時期を同じくする2012年10月に、アメリカ下院の情報特別委員会は、中国のHuaweiおよびZTEの機器の排除を推奨していた[4]。これは、両社と中国政府とのつながりを理由に、情報流出のリスクを指摘したものである。

なお、本稿で取りあげている対内直接投資とは異なるが、2018年の8月に成立した2019年会計年度国防授権法（National Defense Authorization Act for Fiscal Year 2019）も、同様の危険とサイバー攻撃に対応するため、アメリカ政府がHuaweiとZTEの機器の使用を全面的に禁止することを定めている。日本においても、2018年12月19日に開催された高度情報通信ネットワーク社会推進戦略本部の官民データ活用推進戦略会議で、政府・公共調達において安全性を確保する体制を強化する方針が打ち出された[5]。アメリカは、同盟国にも同調を求めているため、今後の各国の動きが注目されている。

## 2. 中国による投資とデータ保護

FIRRMAの成立前は、CFIUSによる審査は最長でも75日間であったため、安全保障上の問題がクリアできなければ、当事者が計画を取り下げ、中止命令を避けることが行われていた。そこで、中止命令が出された以外にも、中国からの投資が安全保障との関係で問題視されたケースは、相当の数に上ったであろうことが推測できる。現に、アメリカ議会の諮問機関である米中経済・安全保障検討委員会は、2016年11月の議会への報告書において、中国からの投資についてはCFIUSの権限を強化する必要性に加え、中国の政府関連企業による対内直接投資の禁止も検討すべきであるとの提言を行っていた[6]。

表1　中国の海外投資（単位100万ドル）




Source：国際連合貿易開発会議（UNCTAD），FDI/MNE database（www.unctad.org/fdistatistics）

中国との関連でデータ保護が問われた例は、Ralls事件後にも幾つか見受けられる。2016年には、デジタル地図を扱うドイツのHEREが、中国のインターネット大手のTencentからの出資の受け入れを表明したが、2017年9月になってCFIUSの不承認を理由にこれを断念した[7]。HEREは、カーナビゲーションシステムで大きな市場シェアを持っており、デジタル地図ではGoogleと肩を並べる企業である。HEREはドイツの企業であるが、米国にも子会社があり、HEREへの出資を通じて米国市場に中国企業が参入することになる。こうした取引を通して中国企業が地図情報を容易に取得できるようになることが、アメリカによって問題視されたものと考えられる。

---

[1] ジョージ・H・W・ブッシュ政権下の1990年のMAMCO事件、オバマ政権下の2012年のRalls事件と2016年のAIXTRON事件、トランプ政権下の2017年のLattice事件と2018年のQualcomm事件である。

[2] この事件の事実関係については、渡井理佳子「アメリカにおける対内直接投資規制と国家安全保障の審査 ―Ralls事件を中心に―」慶應法学27号139頁以下（2007年）参照。

[3] Kevin J. Wolf (Partner, Akin Gump Strauss Hauer & Feld LLP). "Testimony on Examining CFIUS before the Senate Committee on Banking, Housing, and Urban Affairs" (Date: Sept. 14, 2017).

[4] House Permanent Select Comm. on Intelligence, 112th Cong. Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE (Oct. 8, 2012).

[5] 高度情報通信ネットワーク社会推進戦略本部・官民データ活用推進戦略会議決定「デジタル時代の新たなIT政策あの方向性について～デジタル時代に対応した「新たな社会システム」への移行に向けて～」（2018年12月19日）。2019年1月17日には、サイバーセキュリティ戦略本部の重要インフラ専門調査会も、情報保護に関する安全基準の強化を検討する方針を打ち出した。

[6] U.S.-China Economic and Security Review Comm'n, 2016 Report to Congress of the Executive Summary and Recommendations 26 (Nov. 2016).

[7] Yuan Yang, *Chinese bid for mapping company falls at US hurdle*, Financial Times (Sept. 27, 2017), https://www.ft.com/content/6f0e519c-a33f-11e7-9e4f-7f5e6a7c98a2.

2018年1月にも、中国のAlibaba Groupの関連企業であるAnt Financialが、アメリカの海外送金大手であるMoneyGramを12億ドルで買収しようとした計画が、同じくCFIUSの承認が得られなかったことを理由に断念された[8]。承認されなかった理由は明らかではないが、MoneyGramに蓄積されている送金データが中国に渡ることへの懸念があったものと考えられる。MoneyGramのサービスは、全米に展開するチェーンの薬局などで簡単に利用することができ、身近な海外送金手段として定着している。米軍にも、MoneyGramの利用者が多数あることから、取引が成立すれば、米軍の人員配置や個人の経済状況が中国に通じ、安全保障上の懸念が生じるとの指摘が、議会によって出されていた[9]。

対内直接投資との関係で、データが安全保障上のリスクをもたらす可能性は、アメリカにおいても2010年代前半までは問題になっていなかったということができる。対内直接投資規制を正当化する安全保障の概念は、当初は防衛産業の保護にあり、その後に国土安全保障が加わったが、FIRRMAによってさらに広がりをみるようになる。

## 3. FIRRMAとデータ保護

アメリカの対内直接投資規制の見直しをめぐっては、2010年代の後半に目立つようになったデータ保護をめぐる問題が、どのように反映されるのかが注目されていた。FIRRMAの全面施行は、成立から最大で18カ月となっているため、2019年の後半以降に正式な規則が定められるものと予想されている[10]。また、FIRRMA1709条は、CFIUSの審査期間を、従来の75日間から105日間に延長している。

### 3.1 アメリカ市民の機微情報

改正前においては、外国投資家による支配の有無がCFIUSの審査の対象であり、重要事項を直接・間接に決する権限の所在が重視されていた。これに対し、FIRRMA1703条（a）（4）（B）は、支配に至らない投資であっても、安全保障を損なうようなアメリカ市民の機微情報（Sensitive Personal Data of U.S. Citizens）を保持し収集する事業を、CFIUSの審査対象に加えている。すなわち、アメリカは、データ保護が安全保障に直結する問題であると明示したことになる。

表2　CFIUSの審査対象の拡大（概要）

| 支配に至らない投資 | 取引対象業種 |
|---|---|
| 不動産投資 | アメリカ国内不動産、港湾、政府施設、等 |
| その他の投資 | 重要産業基盤、重要技術、アメリカ市民の機微情報 |

何がアメリカ市民の機微情報に該当するかについては、規則の制定を待つ必要があるが、ビッグデータにも関わることになるであろう。ビッグデータの規制においては、データの量的な面のみならず質的な面が重視されるため、今後のCFIUSの審査では、どのような性質のデータがどのように利用されると安全保障上のリスクをもたらすのかがポイントとなるはずである。

そこで、MoneyGramのような金融取引や信用に関するデータの取得につながる企業買収は、外国による支配をもたらすものでなくても、アメリカ市民の機微情報として、CFIUSの審査対象となる。このほか、保険会社などアメリカ市民の健康状態に関するデータを保持している企業の買収も、市民の勤務先などと照らし合わせることにより、安全保障上の懸念をもたらすものとなるため、やはりアメリカ市民の機微情報として、CFIUSの審査対象となるものと考えられる。

### 3.2 支配に至らない投資

外国投資家の支配に至らない投資であるものの、CFIUSの審査の対象に加えられたのは、①アメリカの事業が保有している未公表の重要な技術情報へのアクセスを可能とする取引、②アメリカ事業の取締役会やこれに相当する機関の構成員等となり、またはその指名権を得るような取引、そして、③議決権行使以外の方法により、アメリカ事業に関する実質的な意思決定への関与を可能とする取引である。

技術情報をめぐる問題は、これまで輸出規制によって対処してきた領域であり、実際に人工知能（AI）など重要技術の輸出制限に向けた動きは、各国でみられるようになってきた。しかし、企業買収による技術の取得は、輸出規制によっても防止できないことから、対内直接投資規制と連動させて考えていく必要がある。FIRRMA

[8] Greg Roumeliotis, *U.S. blocks MoneyGram sale to China's Ant Financial on national security concerns*, Reuters (Jan. 3, 2018), https://www.reuters.com/article/us-moneygram-intl-m-a-ant-financial/u-s-blocks-moneygram-sale-to-chinas-ant-financial-on-national-security-concerns-idUSKBN1ER1R7.

[9] Josh Rogin, *China's Jack Ma has penetrated the Trump administration - and he knows what he wants*, The Washington Post (July 19, 2017), https://www.washingtonpost.com/news/josh-rogin/wp/2017/07/19/chinas-jack-ma-has-penetrated-the-trump-administration-and-he-knows-what-he-wants/?utm_term=.596d2ae70c4b.

[10] 2018年10月に暫定規則（パイロット・プログラム）が設けられ、11月より運用されている。Determination and Temporary Provisions Pertaining to a Pilot Program To Review Certain Transactions Involving Foreign Persons and Critical Technologies, 31 CFR Part 801, 83 Fed. Reg. 51322 (Oct. 11, 2018).

が、未公表の重要な技術情報について海外流出の予防を視野に入れたことは、データや情報の価値に注目した新たな時代の規制の実現ということができる。

## 4. 中国に対する評価

### 4.1 中国をめぐる問題

FIRRMA の成立に先立つ 2017 年 9 月、トランプ政権となって初めての中止命令が出され、新政権でもアメリカが中国に対して大きな懸念を抱いていることが明確となった。この取引は、アメリカで設立された中国系の投資ファンドである Canyon Bridge Capital Partners が、アメリカの半導体メーカーの Lattice を 13 億ドルで買収するというものであった。CFIUS の委員長であった財務省の Steven Mnuchin 長官は、大統領の中止命令にあたって声明を発表し、取引を中止すべき理由として、中国政府と関わりを持つ外国投資家にアメリカの知的財産が潜在的に移転し得ること、そして中国政府が本件取引を支援する役割を果たしていることを冒頭で指摘した[11]。

FIRRMA1719 条（b）は、商務長官に対し、FIRRMA の成立から 2 年以内に､そしてその後は 2026 年まで 2 年ごとに、アメリカに対する中国からの対内直接投資について議会に報告するよう求めている。これにより商務長官は、中国からの投資額、投資対象産業、投資の種類、中国政府関連投資とそれ以外からの投資の内訳、中国政府関連投資によって設立された企業名、中国の管轄下にある企業のアメリカの子会社に関する情報、投資パターン別についての分析、商務長官がこれらの情報を収集する上での限界について、報告書を作成することとなる。なお、投資パターン別の分析においては、「中国製造 2025」に示されている目的との関連についても、明示することとなっている。

中国以外の国からの投資については、このような報告書の提出は求められてはいない。中国からの投資は、これまでにも CFIUS の厳格な審査の対象であったといえるが、FIRRMA の下で、名実ともに他の諸国とは別の扱いがなされることになったといえよう。そして、これがアメリカの中国に対する評価ということができる。

### 4.2 特定懸念国

FIRRMA では、CFIUS の審査における考慮要素を定めた 1702 条（c）に特定の国家に注目する規定がある。考慮要素の最初の項目は、審査対象となっている取引が、安全保障の上でアメリカの優位を脅かすような重要な技術または重要インフラの獲得を戦略的な目標として掲げている特定懸念国（country of special concern）に関わるものであるかである。これが、どの国を想定したものであるのかは明らかではないが、中国が念頭にあることは否定できないであろう。

FIRRMA の立法過程では、CFIUS が原則として取引を承認し得るホワイト国のリストを作成することも検討されていた[12]。仮に、リストが設けられていれば、アメリカの同盟国である日本は含まれていたものと思われる。ただし、日本企業によるアメリカ企業の買収であっても、その日本企業がアメリカにとっての特定懸念国とのジョイントベンチャーを設立していた場合には、結局のところ当該国家にデータや技術が渡ってしまう。したがって、リストが作成されなかった理由としては、ホワイト国とそれ以外の特定懸念国に分類しても、分類には実益がないことが挙げられる。

## 5. おわりに

FIRRMA は、対内直接投資においてデータ保護の必要性を打ち出した法であると同時に、アメリカの持つ中国への懸念に対処するための法であるということができる。FIRRMA1713 条は、CFIUS の保有する安全保障に関する分析や行動についての情報を、一定の条件の下に同盟国と共有することを定めており、そのために必要となる手続を設けるとした。そこで、日本政府としてもアメリカとの連携を密にし、データ保護を含む対内直接投資規制の問題に対応していくことが求められている。

日本の対内直接投資規制は、外国為替及び外国貿易法（外為法）によっている。外為法は、2017 年の改正で、安全保障の見地から、無届で対内直接投資を行った外国投資家に株式売却等の命令を行うことができる制度を導入したほか、外国投資家が他の外国投資家から非上場株式を取得する行為を審査付事前届出制の対象に加えて､規制の強化を図ったところであった｡今後、アメリカに倣って、データ保護に特化した規制の導入も検討されるものと思われる。

第 5 世代移動通信規格（5G）の展開が迫る中、対内直接投資規制の見直しは、まだ始まったばかりということもできる。今後の規制のあり方については、安全保障に関わる問題ではあるが、規制の透明性が必要以上に損なわれていないか、そして規制手段が自由な経済取引を損なっていないかが課題となるものと考えられる。

[11] U.S. Dept. of the Treasury, Statement On The President's Decision Regarding Lattice Semiconductor Corporation (Sept. 13, 2017).

[12] H. R. Rept. No. 115-784, pt.1, at 41 (June 26, 2018).

# A U.S. Perspective on Foreign Data Protection Policies: Impacts on Economic Competitiveness and National Security

Eric Lundell
President and CEO, ITTA, Inc.

Bobby Shields
Manager, S&T Policy, ITTA, Inc.

**Please note that the views expressed in this presentation are our own, and do not necessarily represent the opinion of International Technology and Trade Associates, Inc (ITTA)*
*Mr. Lundell serves as the President and CEO of ITTA, which provides advisory services in a range of policy, regulatory and business development areas. Mr. Shields leads ITTA's science and technology business practice.*

The U.S. federal government has not developed a unified data protection law or regulatory system. Rather, the United States relies upon a "patchwork" of state laws and sector-specific federal laws to protect U.S. citizens' data and information. However, recent incidents of major data breaches (such as the Marriot hack) have prompted members of the U.S. Congress to begin considering efforts on comprehensive data protection legislation.

As members of Congress discuss and debate possible data protection legislation, the United States' peers and competitors are advancing their own national data protection policies. The intents and purposes of these laws and regulation are manifold: to protect consumer privacy; to enhance government surveillance powers; to increase competitiveness of domestic businesses; and so on.

This article reviews U.S. perspectives on the impact of foreign data protection policies on U.S. economic and national security interests. We examine three cases: the EU's General Data Protection Regulations (GDPR); China's Cybersecurity Laws; and India's data localization policies.

Each case presents regulatory challenges to U.S. business interests that could, in turn, undermine U.S. global economic competitiveness. Many in the U.S policy community argue that a weakened economy undermines the U.S. defense industrial base, U.S. military strength, and thus, U.S. national security. Moreover, foreign data protection regulations may also curtail the development of cutting-edge technologies vital to U.S. national security and weaken cyber threat information sharing practices.

## 1. China's Cybersecurity Law

### 1.1 Background on China's Cybersecurity Law

In an effort to improve cybersecurity and better control data transfers, the People's Republic of China adopted the Cybersecurity Law in November 2016. Since adopting the measure, the Chinese government has begun to implement various provisions of law.

Overall, the Chinese Cybersecurity Law is a comprehensive set of provisions governing the use of information and communication technology (ICT) in China. The law outlines Chinese policies on issues such as personal information protection, data management, and cross-border data transfers.

The three key provisions of the Cybersecurity Law salient to this article are: cybersecurity inspections of businesses in China; protections for "critical information infrastructure;" and data localization requirements.

First, on November 1, 2018, the Chinese government began to enforce a cybersecurity provision that empowers China's Public Security Bureaus (PSBs) to conduct inspections of companies that use or provide internet services in China. Under this measure, PSBs are given broad authority to physically or remotely access and inspect company networks that may impact national security or public safety.

Second, the Cybersecurity Law imposes new requirements on entities that operate so-called "critical information infrastructure" (CII). Notably, the Chinese government has not yet provided a clear definition of CII. As detailed in an August 2018 Brief[1] by the Center for Strategic and International Studies (CSIS), operators of CII must use network products and services that have undergone a national security review process, store certain data within China's borders, and undergo periodic security assessments. However, the Chinese government has not yet approved implementing regulations for this provision.

Third, the Cybersecurity Law's data localization provision requires that CII and other data deemed "important" or "personal" can only be transferred outside of China if it successfully passes a security assessment by the Chinese government. Like the CII provision above, the Chinese

[1] "How Chinese Cybersecurity Standards Impact Doing Business in China", CSIS BRIEFS, 2018

government has not yet approved implementing regulations for this data localization requirement.

### 1.2 Impact on the U.S. Economy and National Security

China's Cybersecurity Law presents a significant challenge to U.S. companies currently operating within China's borders as well as U.S. companies looking to expand operations into China.

To begin, the law's vague language in its inspection provision gives PSBs authorities broad discretion when inspecting corporate networks and data. For example, although there are no clear definitions for terms such as CII and "important" or "personal" data, Chinese government entities may use a broad interpretation of these definitions when determining whether it has authority to access and inspect a U.S. company's network or data. If interpreted liberally, China's Cybersecurity Law could extend to virtually any U.S. company operating in China.

Many business representatives and policy experts have warned that Chinese government officials could use the guise of "national security" or "public safety" to inspect a U.S. corporation's sensitive data. Given the widespread allegations of Chinese government's theft of foreign trade secrets and intellectual property to benefit its own domestic industry, U.S. industry has justifiably raised alarms at the prospect of allowing Chinese government officials expansive access to their networks and data.

Moreover, the law's data localization regulations could undermine U.S. trade-in-services with China. A September 25, 2017 statement[2] by the U.S. delegation to the World Trade Organization outlined the potential negative consequences of China's data localization efforts:

> *The result would be to discourage cross-border data transfers and to promote domestic processing and storage. The impact of the measures would fall disproportionately on foreign service suppliers operating in China, as these suppliers must routinely transfer data back to headquarters and other affiliates. Companies located outside of China supplying services on a cross-border basis would be severely affected, as they must depend on access to data from their customers in China.*

[2] "COMMUNICATION FROM THE UNITED STATES, MEASURES ADOPTED AND UNDER DEVELOPMENT BY CHINA RELATING TO ITS CYBERSECURITY LAW", WTO, 2017

Furthermore, once fully implemented, China's Cybersecurity Law could be "weaponized" to meet Beijing's broader geopolitical goals. For example, the Chinese government could potentially use PSBs cybersecurity inspections as a retaliatory measure against the U.S. in the context of the ongoing trade war. Indeed, Chinese officials could conduct overly burdensome reviews and inspections to slow down U.S. business operations in lieu of the imposition of additional tariffs on U.S. products.

China's Cybersecurity Law also presents national security concerns for the United States. The U.S. policy community (and especially the Trump Administration) has increasingly advanced the conviction that U.S. "economic security" is a fundamental component of U.S. national security. The Trump Administration believes that a vibrant economic sector promotes a robust defense industrial base and strong military. Ultimately, a secure and strong economy strengthens the United States' strategic position against China in the escalating great power competition.

The concept is a guiding principle of the Trump Administration's trade and economic policies. Indeed, over the past year, major trade policy decisions of the Trump Administration (to include Section 232 tariffs on steel and aluminum and Section 301 tariffs on Chinese products) were predicated on this concept of "economic security is national security."

If China's Cybersecurity Law begins to yield major negative impacts on U.S. businesses, the Trump Administration will not only see this as an affront to its economic interests — but also as a threat to its national security apparatus.

## 2. The EU's GDPR

### 2.1 Background on the GDPR

The European Union previously relied upon a patchwork of data privacy laws across EU member states, much like the United States' current data privacy regulatory framework. Seeking a unified regulatory approach, the EU adopted the General Data Protection Regulation (GDPR) in April 2016, which later went into effect in May 2018.

The GDPR is often considered the most comprehensive piece of data protection legislation in the world. In general, GDPR places the responsibility of data protection on organizations that process personal information of EU citizens. It establishes the principle of "privacy by design

and by default" for organizations that control or process such data. It also requires organizations to maintain a data protection officer to ensure the privacy of EU citizen data. The GDPR lays out strict financial penalties for organizations that do not meet its privacy standards. The maximum fine under the GDPR is 4 percent of an organization's annual turnover or 20 million Euros (whichever figure is greater).

GDPR's data privacy requirements apply to *any* organization — to include any organization outside the EU's border — that offers goods and services to individuals in the EU or that monitors their behavior. As such, the GDPR has a global reach.

Each nation within the EU is required to create an independent public Data Protection Authority (DPA) to enforce the GDPR. However, the DPAs cannot formally enforce the GDPR outside of its borders. As such, the EU must rely upon agreements with foreign courts and other relevant bodies to effectively enforce the GDPR outside of the EU.

### 2.2 Impact on the U.S. Economy and National Security

The GDPR places considerable regulatory burdens on U.S. companies. Any U.S. organization that controls or processes EU citizens' data is subject to DPA enforcement. Fines of up to 4 percent of an organization's annual turnover or 20 million Euros pose a significant financial risk to U.S. companies. Costs of complying with GDPR regulations—and the potential inefficiencies resulting from such compliance—can also hurt U.S. companies.

However, there are still many "unknowns" regarding how GDPR enforcement will manifest in the coming years. For instance, it remains unclear how DPAs will interact with counterparts in the United States to penalize non-complaint U.S. companies. Furthermore, the cost of GDPR compliance for U.S. companies relative to foreign counterparts is unclear. In turn, we do not yet know how the GDPR might affect the competitiveness of U.S. companies compared to foreign counterparts.

One potentially significant technological consequence of GDPR is that it will limit the amount of global data available to U.S. organizations, which will, in turn, complicate the development of artificial intelligence (AI) algorithms. AI systems require large amounts of data to process in order to mature their algorithms. As such, data limitations resulting from GDPR enforcement could ultimately impede AI development. And while this concern applies to data protection regulations across the globe, the GDPR represents the most significant risk to U.S. AI developers, given the large amount of data shared between U.S. and EU entities.

As the global leader in AI technology, the United States would suffer the greatest opportunity cost from a decrease in available data. A slowdown in AI development would jeopardize the rapid growth of AI in U.S. industry. Consequently, the U.S. national security community, which relies heavily upon industry to develop and operationalize cutting-edge AI capabilities, would assuredly be concerned about the impact on AI-related national security efforts.

However, some experts have countered these concerns, noting that the GDPR may ultimately facilitate AI development. For example, in a June 2018 *TechCrunch* article[3], Ivy Nguyen of Zetta Venture Partners argues that the GDPR will require companies to better organize and manage their data. These data management processes will help organizations better understand their data and, in turn, more effectively develop and deploy AI systems. Moreover, GDPR also requires all EU citizen data to be portable (i.e., available for download by a user), meaning that more data will be digitized and thus accessible for AI development and application.

At this point, only time will tell exactly how the GDPR will impact AI development in the United States.

Lastly, the GDPR may undermine cyber threat information gathering and sharing between U.S. threat analysts. In short, GDPR forbids the publication of information that identifies EU individuals. GDPR thus bans publication on so-called WHOIS databases, which provide information on registered owners and operators of domain names and IP addresses. According to security experts, including Chris O'Brien from EclecticIQ[4], these databases have traditionally help inform threat analysts in their research for cybersecurity threats. With these databases, cyber threat gathering and information sharing in the United States may become less effective.

## 3. India's Data Protection Policies

### 3.1 Background on India's Data Protection Policies

The Indian government has begun pursuing stricter data

[3] https://techcrunch.com/2018/06/07/gdpr-panic-may-spur-data-and-ai-innovation/

[4] https://www.informationsecuritybuzz.com/articles/gdprs-impact-on-threat/

protection policies over the past several months, with a focus on data localization.

In April 2018, the Reserve Bank of India (RBI) established a requirement for all global payment firms to store transaction data of Indian customers within its borders. This data localization requirement went into effect on October 15, 2018.

Despite protests over the regulatory burdens of RBI's data localization requirement, major U.S. payment firms such as Visa and MasterCard confirmed in October that they had begun complying with this new rule. According to news reports[5], however, these companies remain in discussions with RBI to try to relax data storage requirements on certain, older financial transactions.

In addition to the RBI requirement, the Indian parliament will soon consider a comprehensive data protection bill. The proposed legislation, called the Personal Data Protection Bill, was drafted by the Indian Ministry of Electronics and Information Technology (MEITY) and is now undergoing reviews within the Indian bureaucracy. The Indian parliament is expected to introduce the bill around June 2019.

Although it is still under review and subject to change, the current version of the bill places restrictions on cross-border data transfers. It requires that every "fiduciary" (meaning any processor or controller) of personal data of an Indian citizen must have at least one copy of the personal data stored in India. More sensitive personal data must be processed in India. The bill also prescribes several conditions for the transfer of non-sensitive personal data outside of India.

### 3.2 Impact on the U.S. Economy and National Security

U.S. companies and many members of the U.S. Congress have characterized India's data localization policies as a form of protectionism that hurts U.S. business. For example, Nigel Cory of the Information Technology and Innovation Foundation has argued[6] that data localization policies place regulatory burdens on businesses by forcing them to use or establish local services. This duplicative cost makes "these firms and their services less competitive compared to local firms, which may only use domestic data services." Many in the U.S. Congress are concerned about these developments. For instance, U.S. Senators John Cornyn (R-Texas) and Mark Warner (D-Virginia) said in an October 2018 letter to Indian Prime Minister Narendra Modi that data localization disrupts bilateral digital trade and, in turn, threatens the U.S.-India economic partnership.

Indeed, given India's massive potential as an export market with its 1.3 billion population, many view restrictions on digital trade with India represents as a significant opportunity cost for U.S. businesses.

India's burgeoning economy is not alone in its growing preference for data localization and limitations on cross-border transfers. Others, such as Indonesia and Vietnam, have similar policies. Growing trend of data localization policies across emerging, high-potential economies represents a major threat to the U.S. digital services economy—and the broader U.S. economy.

And, as discussed earlier, the Trump Administration believes that a weakened economy also impacts the defense industrial base and U.S. military posture.

### 4. Conclusion

As the U.S. Congress debates its own data protection legislation over the next several months or years, global partners and competitors are taking actions to protect and control their data. Taken together, this global web of data protection laws and regulations can severely impact the U.S. business community and undermine efforts to advance key technologies of economic and national security importance such as AI.

Data protection can also be viewed in the context of the emerging great power competition between the United States and China. Many in the United States view China's Cybersecurity Law as part of a broader effort to promote its domestic industry at the expense of U.S. economic and security interests. Predatory actions against U.S. companies resulting from the Cybersecurity Law could put the United States at an economic and security disadvantage against its rising competitor.

In light of these challenges, U.S. policymakers will likely push for pro-business data policies to promote digital trade and services and fight against "digital protectionism." These efforts require balance between legitimate demands for personal privacy and promotion of digital innovation that contributes to U.S. prosperity and security.

[5] https://www.livemint.com/Industry/Wmq7Sr5YtNBPcet8aGBRQP/Visa-Mastercard-begin-storing-India-payments-data-locally.html

[6] https://www.livemint.com/Opinion/bHelcN7RR5rQ5r3hPxXGRP/Opinion--The-RBIs-misguided-digital-protectionism.html

# プラットフォーム企業によるデータ寡占への政策的対応
## ～EU一般データ保護規則とデジタル単一市場戦略～

東洋大学　経済学部
准教授　生貝　直人

（いけがい　なおと）1982年埼玉県川口市生まれ。
2005年慶應義塾大学総合政策学部卒業、2012年東京大学大学院学際情報学府博士課程修了。博士（社会情報学）。東京大学大学院情報学環客員准教授、東京芸術大学特別研究員などを兼務。国立情報学研究所特任研究員、東京大学附属図書館・大学院情報学環特任講師、情報通信総合研究所研究員などを経て2018年4月より現職。著書に『情報社会と共同規制』など。
専門分野は情報政策の国際比較。

CONTENTS



プラットフォーム企業による膨大なデータの集積が引き起こす社会的・経済的課題に対応するため、EUはGDPRによる個人データ保護の強化に加え、通信データの保護や競争環境の整備を含む総合的な規制改革を進めている。グローバルなデータ経済の中で消費者保護と持続的なイノベーションを実現するため、我が国でも関連する法制度の包括的な再設計が求められる。

## 1. プラットフォームとデータ集積

現在世界各国において、GAFA（Google, Apple, Facebook, Amazon）と呼ばれる企業群をはじめとした、米国資本の巨大プラットフォーム企業による、いわゆるデータ寡占への政策的対応のあり方が活発に論じられている。多面市場（multi-sided market）のモデルに基づく強いネットワーク外部性によって国境を超えた成長を続けるプラットフォーム企業は、世界中のユーザー間のインタラクションを媒介し、またその行動履歴を集積する中で、膨大なデータを収集することができる。そのように集積されたデータは、開発に大量のデータを必要とするディープラーニングなどの人工知能技術の発展と相まって、プラットフォーム企業の競争優位をさらに揺るぎないものとしつつある。

データの集積は、個別企業の経済的な競争力を左右するのみならず、今後の社会統治のあり方にも多大な影響をもたらしうる。「あらゆるモノがインターネットにつなげ、そこで蓄積されるさまざまなデータを、人工知能などを使って解析し、新たな製品・サービスの開発につなげる[1]」ことが日常化する第4次産業革命の中では、モノのみならず、ヒトまでもがデータの集合体として社会的に認識・管理される状況が生じる。データ社会における人間そのものである個人データを集積するプラットフォーム企業は、行動ターゲティング広告やレコメンデーションなどに顕著であるように、そのデータを用いて個々人の行動をコントロール可能となるのみならず、われわれ個々人の社会的評価をも決定しうる立場にも立つ。それは個人データの分析によって個々人を評価し、与信や就職・転職などの評価にも活用しようとするプロファイリングやスコアリングに関連するサービスの隆盛からも明らかであろう。

## 2. GDPRの持つ戦略的意義

2018年5月25日に適用開始されたEU（欧州連合）一般データ保護規則（GDPR, General Data Protection Regulation）[2]は、プラットフォーム企業のデータ寡占による社会的・経済的影響力の拡大への対抗という性質を色濃く有している。EU/EEA（欧州経済領域）域内に拠点を持たない企業であっても、域内の個人に向けられたサービスを提供する場合や域内の個人をモニタリングする際は同規則の適用を受けるという広範な域外適用は、海外のプラットフォーム企業のサービスを利用することが日常化している現代のグローバルな情報環境において、域内の個人を保護するための前提となる条項であり、2,000万ユーロ／全世界連結売上高の4%などを上限とした莫大な制裁

[1] 未来投資会議「優先的に取り組むべきアジェンダについて」（平成28年11月10日）https://www.kantei.go.jp/jp/singi/keizaisaisei/miraitoshikaigi/dai2/siryou1.pdf

[2] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance), OJ L 119, 4.5.2016, p. 1–88.

金は、巨大な規模を持つ企業への実効性を念頭に置いたエンフォースメント措置である。適用開始後早くも2019年1月には、フランスの個人データ保護当局であるCNIL（Commission Nationale de l'Informatique et des Libertés）が、Googleの個人データ処理に関わる同意などの手続きがGDPRの求める基準を順守していないとして、同社に5,000万ユーロ（約60億円）の制裁金を科したことを発表するなど[3]、プラットフォーム企業に対する積極的な執行していく姿勢を明確にしている。

GDPRによって個人に認められるさまざまな権利のうち、本稿の主題から注目すべきは、20条に規定されるデータポータビリティの権利（Right to data portability）であろう。個人が企業などに提供した自らの個人データを、再利用しやすい機械可読なフォーマットで取り戻したり、技術的に可能な場合には他の企業などに直接移転することを求めることを認める同権利は、「スタートアップや小規模企業たちに、デジタルジャイアンツに支配されたデータ市場にアクセスし、プライバシー親和的なソリューションによってより多くの消費者を引きつけることを可能とする[4]」競争促進的効果を有する。そして個人がプラットフォーム企業から過度のロックインを受けず、他のプラットフォーム企業への移転を容易にすることは、プラットフォーム企業が個人を規制する権力としての性質を強めつつある中で、古典的な意味でのプライバシー保護にとどまらない重要な意味を持ちうる。

なお、GDPRに規定されるデータポータビリティの権利の対象は、あくまで本人が提供した個人データに限られたものであり、またフォーマットの特定やAPI解放などの措置が課されている訳でもない、比較的軽微とも言える権利である。この点例えばフランスでは、2016年に成立したデジタル共和国法[5]の48条によって、消費法典の中に新たな「データの回収とポータビリティ（Récupération et portabilité des données、L224-42条）」の権利を設け、GDPRの適用開始と同じ2018年5月25日に施行している。同権利は、一定規模以上のオンライン公衆通信プロバイダについて、消費者が当該プロバイダのサービスにアップロードした全てのファイルや、サービスの利用により生成された全てのデータを取り戻すことを原則として認めており、GDPRを補完する形で、個人データに限らないより広範なデータポータビリティを可能としている。この他にもEU法レベルでは、決済サービス提供者のAPI解放を求めるPSD2（改正Payment Service Directive）[6]が2018年1月に施行されるなど、分野ごとの関連法も存在する。データ寡占という問題へのEUおよび加盟国の政策的対応の中で、GDPRはいわば全体の一部分にすぎないことに留意する必要がある。

## 3. プラットフォーム規制の総合的改革

同様のことは、EUのプラットフォーム規制全体に対しても言うことができる。プラットフォーム企業とその集積するデータの影響は情報社会のあらゆる側面に及ぶため、それが引き起こす各種政策課題への対応も、情報に関わる法制度の広範な分野において行われる必要がある。欧州委員会は2015年から開始したデジタル単一市場戦略の一環として、2016年5月25日、すなわちGDPRが制定された翌月に、「オンライン・プラットフォームとデジタル単一市場：欧州にとっての機会と挑戦[7]」と題する、プラットフォーム関連規制の総合的改革方針を示した政策文書（以下、OP政策文書）を公表した。同文書は、プラットフォーム企業に対する規制枠組みの方向性について、①同等（comparable）なデジタルサービスのための公平な競争条件（level playing field）、②中核的価値を保護するためのオンラインプラットフォームの責任ある行動、③ユーザーの信頼を維持し、イノベーションを保護するための透明性と公正性、④データ駆動型経済における非差別な市場、という四つの原則を示し、それぞれの原則に関わる規制改革の具体的なあり方を示している。

---

[3] La formation restreinte de la CNIL prononce une sanction de 50 millions d'euros à l'encontre de la société GOOGLE LLC | CNIL https://www.cnil.fr/fr/la-formation-restreinte-de-la-cnil-prononce-une-sanction-de-50-millions-deuros-lencontre-de-la

[4] European Commission - Fact Sheet Questions and Answers - Data protection reform http://europa.eu/rapid/press-release_MEMO-17-1441_en.pdf

[5] Loi n°2016-1321 pour une République numérique

[6] Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC (Text with EEA relevance), OJ L 337, 23.12.2015, p. 35–127.

[7] Online Platforms and the Digital Single Market Opportunities and Challenges for Europe, COM(2016)288. 同文書の邦語による解説としては、井上淳[2017]「欧州連合（EU）におけるオンライン・プラットフォームに対する規制等の動向について」メディア・コミュニケーションNo.67, pp65-82.を参照。

同文書で示された方針に直接関連して、現在まで約2年半の間に欧州委員会から提案されたEU立法や法改正は10を超えるためここで全てを取り上げることはできないが、特にプラットフォーム企業によるデータ寡占という本稿の主題と関わりの深いものを紹介していきたい[8]。

### ①Eプライバシー規則案[9]

2017年1月に提案された同規則案は、GDPRの特別法（lex specialis）としての位置付けを有し、電子通信分野に特有のプライバシー問題に対処し、自然人・法人を問わない通信の機密性（confidentiality）を保護することを目的とする。2002年に成立した現行のEプライバシー指令[10]（2009年に大幅改正[11]）を置き換える形で提案されたものであり、現行指令は加盟国に対して、通信データに関わる我が国の通信の秘密（電気通信事業法[12]4条）に近い法的保護を行うよう求めているが、規制対象は伝統的通信事業者に限られており、現在プラットフォーム企業が主として提供するVoIPやメッセンジャー、ウェブメールなどのOTT（Over The Top）通信サービスには適用されない。規則案では、規制対象をOTT通信サービスに拡張し、「同等なデジタルサービスのための公平な競争条件」を確保しようとする。現行指令同様、行動ターゲティング広告などに用いられるクッキーなどの「エンドユーザーの端末に保存または関連する情報」は、オプトインでの利用が原則とされる。

さらに外国から域内の利用者などにサービスを提供する事業者に対しても同規則を適用する、いわゆる域外適用を明確化すると共に、執行はGDPRと同様に各国データ保護当局が担うこととし、制裁金はGDPRの規定を準用するなど、全体としてGDPRと一体での運用が想定されている。実際に同規則は提案当初、GDPRと同じ2018年5月に施行することがめざされていた。加盟国間の交渉の難航により成立は遅れているが、特に機微な情報である通信データに関して、GDPRよりも強固な保護を行う方針は維持される見込みである。

### ②オンライン媒介サービスのビジネスユーザーのための透明性と公正性促進規則案[13]

2018年4月に提案された同規則案は、オンラインショッピングモールなどの、ユーザー企業（出店者など）と消費者の間の取引を媒介するプラットフォーム企業を対象として、交渉力で劣位にあるユーザー企業の保護と予見可能なビジネス環境を実現するために、プラットフォーム企業の行動に関わる透明性と公正性（transparency and fairness）を推進するものである。具体的には、プラットフォーム企業とユーザー企業の間での契約条件（ToC）の明確・明瞭性と変更15日前の通知、サービス停止・終了時の理由の通知、ランキング付けの主要パラメータと理由の明示、プラットフォーム企業自身が自社のプラットフォーム上で商品やサービスを提供する場合の差別的取扱の明示、プラットフォーム企業が保有するデータへのユーザー企業のアクセス可否と条件の明示、最恵国待遇（MFN）条項の理由の明示と一般公表などがプラットフォーム企業に義務付けられる。さらに媒介サービス以外にも、Googleなどの検索エンジン提供者にも、ランキング付けの主要パラメータの明示を求めていることは注目に値する。

内部紛争処理体制の整備（一定規模以上のプラットフォーム企業が対象）や、中立仲裁機関を利用することを求める他、業界団体などによるユーザー企業側の集団訴訟を可能とするなど、紛争の公正な解決を図る

---

[8] OP政策文書で言及される事項以外にも、プラットフォーム・データ寡占の問題に関しては、EU競争法が重要な役割を果たしているが、本稿では紙幅の都合により割愛する。またここで紹介するうち、Eプライバシー規則案およびオンライン媒介サービスのビジネスユーザーのための透明性と公正性促進規則案については、欧州委員会の提案を受けて欧州議会・閣僚理事会において審議が続けられている段階であり、最終的に成立するまでには少なくない変更が生じる可能性があるが、本稿では特に言及の無い限り欧州委員会の当初提案時点の内容を記載している。

[9] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) COM/2017/010.

[10] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJL 201, 31.7.2002, p.37-47.

[11] Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws (Text with EEA relevance) OJ L 337, 18.12.2009, p. 11–36.

[12] 昭和59年法律第86号

[13] Proposal for a regulation on promoting fairness and transparency for business users of online intermediation services, COM (2018) 238.

ための施策も導入される。さらに同規則の提案と同日には、各分野の専門家から構成されるエキスパート・グループを中心とした「オンライン・プラットフォーム経済監視委員会」を設立する欧州委員会決定[14]が出され、規則案の規定に関わる事項を含め、プラットフォーム経済の継続的監視と分析を行い、政策立案に関わる欧州委員会への助言を行うものとされている。プラットフォーム企業が集積する膨大なデータの管理、それを分析・活用するアルゴリズムなどのブラックボックス化が進む中、その実質的な透明性を実現するために、同監視委員会の作業は重要な役割を果たすものと考えられる。

③非個人データのEU域内自由流通枠組規則[15]

2017年10月に提案され、早くも2018年11月に成立した同規則は、非個人データ、すなわち「GDPR（4条1項）に定義される個人データ以外のデータ」の自由な流通を確保することを目的とする。同規則は大きく二つのパートから構成されており、一つは、加盟国による非個人データのデータローカライゼーション[16]関連規制の抑止・撤廃である。GDPRは個人データのEU域外移転に関して強固な規制を有するが、EUの存在意義そのものである域内単一市場を実現する観点から、EU域内での個人データの完全な自由流通が確保されており、原則として加盟国は個人データの「自国内」保存を義務付ける規制を設けることはできない。同規則は、この原則を非個人データに関しても敷衍（ふえん）する規定を置く。

もう一つが、非個人データのデータポータビリティ（porting of data）の促進である。先述した通り、個人データに関してはGDPRなどによって広範なデータポータビリティが確保されているが、本規則においては、それを非個人データにおいても実現し、他者のデータ保存・処理を行うクラウド事業者などのサービス提供者間のスイッチングを容易とするため、ユーザー企業などがサービス提供者に預けたデータを他の提供者に移し替えたり、自らのITシステムに取り戻す仕組みを提供することを促す規定を置いている。ただし本規則では、サービス提供者に対する直接的な強制力のあるデータポータビリティ対応義務という形式は採っておらず、欧州委員会がサービス提供者による自主規制的行動規範（self-regulatory codes of conduct）の構築を促し、その実施状況を監視する方法論を採用している。こうしたソフトロー・アプローチにより産業界での自主的な対応が成功裏に進まない場合には、より強固な法的対応が検討されることになる[17]。

## 4. 我が国の対応のあり方

ここまで紹介したEUにおける規制改革の進展などを受け、ここ数年来、我が国においても政府各部門においてプラットフォーム規制に関わる検討が急速に進められているところである[18]。我が国では2017年に全面施行された改正個人情報保護法において、域外適用の規定をはじめとする一定の法整備がなされたところであるが、EUがGDPRの成立直後にプラットフォーム関連規制の総合的改革方針を公表し、それに基づく各種立法や法改正を矢継ぎ早に進めていることを見れば、プラットフォーム企業とそれによるデータ集積がもたらす広範な政策課題への対応において、個人データ保護法制の整備はそのスタート地点であるとも表現できよう。

特に今後、現在高い関心を集める米国資本のGAFAに加え、中国のBAT（Baidu, Alibaba, Tencent）をはじめとする各国のプラットフォーム企業が我が国にも本格的に進出してくることが見込まれる。我が国の消費者がそれら外国のプラットフォーム企業のサービスを安心して利用できる環境、そして事業者にとっての透明かつ公正な事業環境と公平な競争条件を整備し、持続的なイノベーションを実現していくために、現代のグローバルなデータ経済に対応した、情報社会に関わる法制度の包括的な再設計が求められている。

---

[14] Commission Desicion of 26.4.2018 on setting up the group of experts for the Observatory on the Online Platform Economy, C (2018) 2393.

[15] Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union (Text with EEA relevance.), OJ L 303, 28.11.2018, p. 59–68.

[16] EU以外の世界各国におけるデータローカライゼーション規制の状況と国際協定などを通じた抑止・撤廃の動きに関しては、総務省情報通信白書（平成30年版）pp.21-24.を参照。

[17] このような、法的規制と自主規制の組み合わせに基づく政策手法である「共同規制（co-regulation）」の詳細については、生貝直人[2011]『情報社会と共同規制』勁草書房を参照。

[18] 例えば総務省「プラットフォームサービスに関する研究会」（2018年10月～）ではEプライバシー規則案が、経済産業省・公正取引委員会・総務省「デジタル・プラットフォーマーを巡る取引環境整備に関する検討会」（2018年7月～）ではオンライン媒介サービスのビジネスユーザーのための透明性と公正性促進規則案および非個人データのEU域内自由流通枠組規則が、それぞれの主要論点や中間論点整理などの各種文書において参照されている。

# データ流通を支えるトラストサービス基盤

慶應義塾大学　大学院政策・メディア研究科
特任教授　手塚　悟

CONTENTS



（てづか　さとる）慶應義塾大学大学院政策・メディア研究科特任教授　博士（工学）。
1984 年慶應義塾大学工学部数理工学科卒。1984 年日立製作所入社。システム開発研究所。2009 年東京工科大学コンピュータサイエンス学部教授。2016 年慶應義塾大学大学院政策・メディア研究科特任教授。個人情報保護委員会委員、重要インフラ専門調査会委員、トラストサービス検討ワーキンググループ主査、情報ネットワーク法学会会長、トラストサービス推進フォーラム会長等を歴任。2004 年、2008 年度情報処理学会論文賞、IEEE-IHMSP2006 Best Paper Award.2013 年度情報セキュリティ文化賞等を受賞。

昨今、石油等の従来型資源と同様に、データを貴重な資源として取り扱う動きが、世界中で広がってきている。データ資源獲得を中心とした覇権競争が激化しており、この競争を制したものが世界を制すると言っても過言ではない状況になってきている。このデータ資源をいかに安心安全に流通させ、今後の世界的レベルでの健全なデジタル社会を実現できるかが問われている。

そこで、世界を取り巻くデータ流通を概観し、それを支えるトラストサービスとトラスト基盤について考察すると共に、国際連携を踏まえたトラスト基盤とは何かについても紹介する。

## 1. データ流通の重要性

我が国では、2016 年 1 月に閣議決定された「科学技術基本計画」において、初めて「世界に先駆けた『超スマート社会』の実現（Society 5.0）」が明記された。世界では既に、モノづくり分野を中心に、ネットワークや IoT 等を活用した取り組みが表明されているが、我が国ではモノづくりだけでなくさまざまな分野に拡大し社会変革につなげていくさらに広い概念を提唱している。

実際、Society 5.0 の取り組みとしては、サイバー空間とフィジカル空間（現実空間）が高度に融合した超スマート社会である「データ駆動型社会」を未来の姿として共有し、「データ流通」の基盤構築も現在進行中である。さらには、データ駆動型社会を表している Society 5.0 により、さまざまなデータのつながりから製造業等を中心とした新たな付加価値を創出していく Connected Industries も提唱され、サプライチェーンでのデータ流通の基盤構築も推進されつつある。

以上のように、我が国においては、現在Society 5.0やサプライチェーンが中心的施策となっており、これらをてことして、国際的な産業競争力を付け、重要インフラの輸出にも貢献することが重要である。そのためにも、さらなるビジネス力の強化を目指し、安心安全なデータ流通の基盤構築を推進することは不可欠である。より安心安全の向上が図られた Society 5.0 やサプライチェーンを構築し、一層進化した概念の導入が必要である。

## 2. 世界を取り巻くデータ流通の状況

我が国の Society 5.0 やサプライチェーンにおけるデータ流通の強化により、さらに魅力的なサービス等を提供するのは最も重要な取り組みであるが、さらにこれらのさまざまなサービスの国際的な拡張性をどのように実現するかが重要な課題の一つである。

世界を取り巻くデータ流通の現状を概観すると、日米欧等においては、「自由と信頼」を原則としたデータ流通の概念のもと、個人、企業、政府等が生み出す膨大なデータを越境して利活用できる環境の検討を始めようとしており、特に我が国が先頭に立って推進していこうと国を挙げて掲げている。一方、中国、ロシ

ア等においては、日米欧等とは異なるデータ収集方法を介したデータ流通を実現している。以上のように、世界を取り巻くデータ流通の状況を見ると、「データ流通圏」という概念が導出されつつある。

我が国のような石油等の従来型資源の乏しい国の観点からすると、資源としてのデータは、我が国の国際競争力の源泉となる最も重要なものである。そこで、官民一体となって、このデータ資源を最大限活用する環境整備が必要不可欠であり、データ流通の基盤構築に可及的速やかに取り組まなければならない。具体的には、個人情報、知的財産情報、重要インフラ情報、安全保障情報等の国をまたいだデータ流通の基盤整備となるため、国際連携を踏まえたルール作りを急がなければならないと考える。

## 3. トラストサービス基盤の重要性

サイバーセキュリティの観点から見れば、Society 5.0 やサプライチェーンのさまざまなサービスの安全性をどのように保証するかが最大の課題になる。

一つの解決策として「トラストサービス基盤」の導入がある。トラストサービスとは、従来のサービスの機能とは同じであっても、その品質が全く別次元の高いレベルで保障された、つまり機能の真正性が保証されたサービスである。

このトラストサービスを実現する基盤として、下記のような「トラストサービス基盤」を構築する。一般にサービスを構成する共通の機能から構成するものを基盤と呼ぶが、ここで言う「トラストサービス基盤」は共通機能の真正性を確実に保証した基盤のことである。

機能の真正性を保証するとはどういうことかと言うと、例を挙げていえば、サイバー空間で扱われるヒト、組織、モノ、データ等のオブジェクトの真正性が保証され、これにより初めて、これらのオブジェクトが取り扱うさまざまな機能の真正性が保証されるという、真正性保証の連鎖により実現するものである。さらに、これらの機能の真正性の保証により、それらの機能で構築されたサービスも真正性が保証されると言う連鎖である。

以上のように、真正性保証の連鎖により構成された信頼に値するサイバー空間をいかに実現するかが、今後のサイバー空間の健全な発展に向けて重要となる。

## 4. 米国・EU のトラストサービス基盤の状況

### 4.1 米国の動向

米国の動向を概観すると、米国は政府内のシステムのトラスト化を既に実現している。具体的には、トラスト基盤として、図 1 に示すような政府職員には Personal Identity Verification（PIV）の IC カードを配布し、認証用、署名用、暗号用の三つの秘密鍵とそれに対応する三つの電子証明書を IC チップ内に格納し、資料や設計書等のコンテンツに対して、だれが作成したかを署名用の電子認証書を使って実現する。さらに暗号化をすることで、仮に漏えいしたとしても内容を解読できないようにしている。

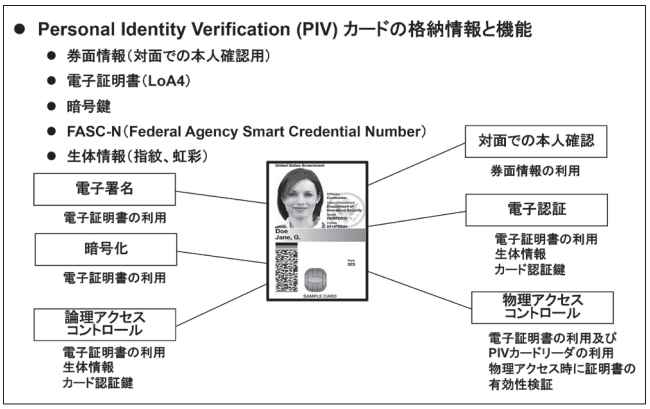



図 1　PIV の IC カードの概要

その上、認証用の電子証明書を使うことで、サイバー空間においても本人認証を確実に行い、米国政府内のさまざまなシステムへのアクセス制御を可能としている。こうすることで、PIV の IC カード一つあれば、サイバー空間での処理が安全に実現されている。併せて、物理的アクセス制御にも使用できる。

さらに、米国政府調達にも使われていることから、民間企業側には PIV-I（Interoperable）という IC カードが発行されている。この発行には、米国 NIST SP800-63[1] のスキームが使われている。

米国の PIV、PIV-I を発行する相互認証を実現する認証局のトポロジー（形態）と我が国のそれとは規模において明らかに違いがある。米国は、この巨大な認証基盤を活用して、米国政府調達にトラストサービス基盤として利用している。なお、米国における

[1] 電子的認証に関するガイドライン

相互認証の技術的な手法としては、Bridge Certificate Authority（BCA）技術で実現している。

具体的な利用としては、現在我が国でも話題になっている米国 NIST SP800-53[2] 対応である。つまり、今までに示してきたサプライチェーンのトラストサービス基盤である。米国はこのような戦略の下に、トラストサービス基盤の整備をしていると考える。

さらに、トラストサービスに関しては、米国政府調達等で導入する米国 NIST SP800-53 の技術仕様で策定されているクラウドセキュリティ基準 Federal Risk and Authorization Management Program（FedRAMP）の認証を取った製品群で構築したクラウドで、トラストサービス基盤を提供する模様である。

### 4.2　EU の動向

EU の動向を概観すると、2014 年 9 月に施行された electronic IDentification, Authentication and Signature Regulation（eIDAS 法）が、EU の 28 ヵ国に共通基盤であるトラストサービス基盤を構築し、その上で実現するトラストサービスを提供することで、EU における「Digital Single Market」の実現を目指している。言い換えれば、EU の 28 ヵ国における市民の経済活動のトラスト化の実現である。

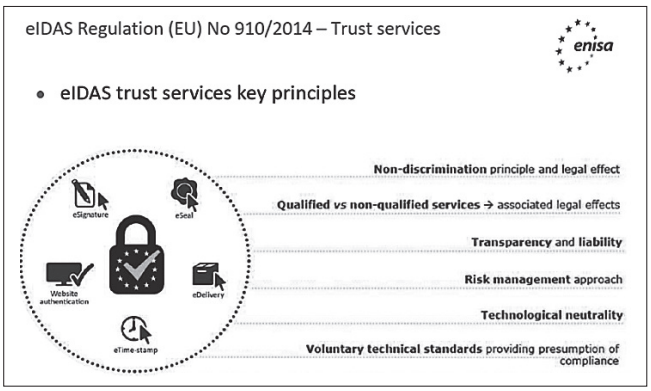
具体的には、eIDAS 法は、我が国のマイナンバー法、公的個人認証法、電子署名法、タイムビジネスに関わる指針を統合した法律であるので、図 2 に示すような EU の加入国で発行されている国民カードの IC チップ内に、認証用、署名用の二つの用途のための秘密鍵と電子証明書が格納されている。

図 3 に eIDAS 法の下で構成されるトラストサービスとトラスト基盤を示す。なお、EU における相互認証の技術的な手法としては、Trust List（TL）技術で実現している。

EU の相互認証を実現する認証局は、技術的には TL で米国の BCA とは異なる技術であるので、米国のような相互認証を実現する認証局のトポロジーはないが、EU の 28 ヵ国が参加していることから、少な

[2] 連邦政府システム及び連邦組織のためのセキュリティ管理策とプライバシー管理策


図２　フランスの国民カードの概要




資料：European Union Agency for Network and Information Security（ENISA）資料より抜粋

図３　EC におけるトラストサービスとトラストリストの状況

くとも我が国の相互認証を実現する認証局より大規模であると考えられる。

### 4.3　米国・EU と我が国の比較

米国は、政府内システムと政府調達に関連する分野において、トラストサービス基盤としての PIV、PIV-I を活用して、トラストサービスを実現している。

EU は、加盟国 28 ヵ国の市民が信頼された経済環境での Digital Single Market を実現するために、eIDAS 法によるトラストサービス基盤としての国民カードを活用して、トラストサービスを実現している。一方の我が国は、Society 5.0 やサプライチェーンの分野において、トラストサービス基盤としてのマイナンバーカードや法人の認証を活用して、トラストサービスを実現することを推進する必要がある。

## 5. データ流通を支える トラストサービス基盤

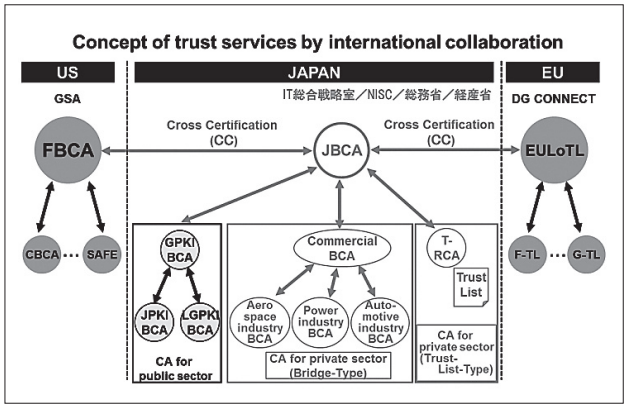
データ流通の重要性については 1 章と 2 章で説明し、3 章と 4 章でトラストサービス基盤の重要性は説明した。具体的には、データはデジタルであるが故、痕跡がなく修正等できてしまうため、改ざん、なりすまし、否認を防がなければならない。そのために、4 章で示したトラストサービス基盤を活用することで防止する。また、データの出所は正しいところからなのかも確認できる機能がトラストサービス基盤には備わっている。

これらに鑑み、安心安全なデータ流通を支えるための機能として、トラストサービス基盤が必要不可欠であると考えられるので、我が国を挙げて、トラストサービス基盤の整備を急ぐ必要がある。

## 6. 国際連携を踏まえた トラストサービス基盤

既に米国・EU のトラストサービス基盤の動向は述べたが、今後近いうちに、米国・EU と我が国がトラストサービス基盤で国際連携をする日が必ず来ると思われる。そこで、図 4 のような「International Mutual Recognition」を検討してみることにする。

図 4 において、米国の FBCA は Federal Bridge Certificate Authority のことである。EU の EULoTL は、EU List of Trust List のことで、28 ヵ国の TL を束ねたリストを表している。




注 1　JPKI：Japan Public Key Infrastructure
注 2　T-RCA：Trusted Root Certificate Authority
注 3　グレー部分は未実現
図 4　トラストサービスとトラスト基盤の国際相互認証

4.3 でも述べた通り、技術的には米国と EU では方式が違うが、概念上は図 4 のように考えても、International Mutual Recognition の検討には問題ない。また、わが国の範囲で、CA for public sector を除く部分はいまだ実現されていない部分であり、今回の国際連携を考える意味では基本的には必要となる認証局であると考える。

JBCA とは、Japan Bridge Certificate Authority のことであり、米国の FBCA と EU の EULoTL との連携をする部分である。この部分の責任元がどこになるのかを決定することが、我が国にとって必須であり、米国政府・EU Commission との International Mutual Recognition を検討するためには、早急に決めなければならない。

そのためにも、直ちに我が国において、政府レベルと民間レベルの検討チームを設立し、さらに官民合同チームでの検討も通して、米国・EU との 3 極での検討を開始するべきである。

我が国が、データ流通を支えるトラストサービス基盤の構築を他の国よりいち早く実現することは、国際的な産業競争力を秀でたものとする最大のチャンスである。そのためにも、本論文で示したトラストサービス基盤は、安心安全なデータ流通を実現するための最も重要な機能であり、それら機能の真正性の保証が必要不可欠である。

今後は、トラストサービス基盤の国際連携を推進することで、いかに世界における我が国の国際競争力を最大限に発揮し、かつ維持していくかが問われている。

# Voice from the Business Frontier
## 日立グローバルデジタルホールディングス社 副社長　林原　正晃

### ～米国におけるデジタル関連市場の潮流と日立の事業の方向性～


（はやしはら　まさてる）
1989 年日立製作所入社、2016 年 ICT 事業統括本部グローバル営業統括本部長、2017 年日立アメリカ社副社長を経て、2018 年 4 月より日立グローバルデジタルホールディングス社副社長、現在に至る。

社会・産業のデジタル化が先行する米国での日立のソリューション事業の方向性について、日立グローバルデジタルホールディングス社の経営に携わっている林原正晃氏にお話を伺いました。

**Q1.　日立グループのデジタルソリューション事業をけん引する、日立グローバルデジタルホールディングス社の事業内容についてお聞かせください。**

日立グローバルデジタルホールディングス社（HGDH）は昨年 4 月に発足した米国に本社を持つ組織で、「Lumada」を活用したデジタルソリューションのグローバル展開に向けた戦略の策定・実行をミッションとしています。HGDH は、プラットフォームソリューションを提供する日立ヴァンタラ社、テクノロジソリューションを提供する日立コンサルティング社を傘下に置く持ち株会社ですが、HGDH の設立によりこれまで個別に進めていた両社のデジタル事業の戦略的なアラインメントを図り、GTM（Go-To-Market）から開発・構築、保守・運用まで、両社の強みを生かした最適なバリューチェーンを構築の上、事業推進していく体制を整えました。また、デジタル事業においては、お客さまの経営課題に関する理解が不可欠となることから、SMEs（Subject Matter Experts）と呼ばれる顧客業務に精通した専門家のチームを HGDH の中に設置し、当社のフロントビジネスユニット（BU）と共に、顧客協創活動（Co-Creation）を通じたデジタルソリューション事業の拡大を図っています。

**Q2.　米国を中心としたグローバルなデジタル関連市場は、各地域間の比較も含めてどのような特徴があるでしょうか。**

HGDH では製造や交通業界を注力分野として取り組んでいますが、製造現場のデジタル化という点では欧州が先行しており、特に強い製造業を擁するドイツでは政府が「Industry 4.0」構想を打ち出し、業界全体をリードしているのはご承知の通りです。米国でも今後労働力の高齢化、大型設備機器の老朽化が見込まれる中、各企業のレベルでデジタル技術を活用した既存の現場システム・プロセスの最適化～新しいビジネスモデルの導入という形でデジタル化が加速されていくと予想しています。交通分野への対応は、その社会構造から、米国は自動車、欧州は鉄道を入り口としてとらえています。当社は米国ではフリートマネジメント市場に着目し、安全な運転、燃費向上、車両管理の改善などの多様なニーズをデジタル技術によって解決する取り組みを始めました。米国最大手の総合トランスポート会社であるペンスキー社とのデジタル技術を活用した車両稼働率向上を実現する協創プロジェクトはその一例です。欧州も自動車社会ではありますが、切り口をやや変えて見る必要があると思っています。例えば、欧州では環境保護の観点から EV 化推進を政策にあげる国も多く、そこでは EV 普及を支えるエネルギーインフラの整備が求められます。昨年末、当社は英国における EV 化による電力管理の課題や給電イ

ンフラ需要予測をデジタル技術を活用して検証する官民連携のプロジェクトへの参加を決めました。アジアでは、政府と並んで現地財閥企業が都市の発展に大きな役割を担っており、特にスマートシティなどデジタル技術の活用を前提とした大規模な都市開発プロジェクトにビジネスチャンスを見いだしています。一方、技術面では5Gの商用化が米国を皮切りにスタートしますが、これによりネットワークの使い方が大きく変わると言われており、モバイルを活用した全く新しいサービスの事業機会が生まれてくると予想しています。こうした地域の特色をとらえ、イノベーションで先行する地域にてユースケースやコアとなるソリューションを確立し、それらを市場の成熟度にあわせて素早くグローバルに展開していくアプローチが重要になると思います。

**Q3. 米国政府は昨今、対米外国投資委員会の機能強化など、技術やデータなどでの対外的規制を強めています。中国への対応が念頭におかれているようではありますが、日本企業の米国子会社として、現時点でビジネス環境の変化を感じていますでしょうか。**

これは非常に重要なテーマだと認識しています。まず、国を問わずデジタル事業に密接に係ってくる規制の論点は、主に個人情報の取り扱いを規定するプライバシー規制、次に、非個人情報も含むデータやサーバの国内保存・設置・照会に関して規定するデータローカライゼーション規制、そして、データのみならず先進的技術に関する輸出・投資規制の大きく三つに分けられると認識しています。プライバシー規制については、EUにおいて一般データ保護規則（GDPR）が策定され昨年春に施行されました。米国ではカリフォルニア州にて昨年6月に消費者プライバシー法（CCPA）が可決されましたが、まだ国レベルの規制は制定されていません。データローカライゼーションについても、一部クラウドでのデータシェアリング規制が制定されたものの、包括的なものには至っていないという理解です。輸出規制については、商務省が国家安全保障を脅かす可能性のある先進技術を規制すべく、人工知能（AI）など14分野を対象に具体的な検討を開始しました。昨年11月には商務省から、規制の対象となる先端技術の範囲についてパブリックコメントを求める通知が出ており、今年の春以降、法案として固まってくると見られています。また、投資面では昨年外国投資リスク近代化法が施行され、対米外国投資委員会（CFIUS）の権限が拡大しています。HGDHグループで行った米国企業の買収案件で、CFIUS審査において追加情報の提供要請が入り、クロージングの期間が予定より遅延したことがありました。これはCFIUS権限拡大の影響が出たものと思われます。プライバシー規制や輸出規制については、まだ検討段階にあり、現時点でわれわれの事業活動が制限されるといった大きな影響は出ていませんが、法案の内容次第では、日本企業の活動にも大きなインパクトを与えることから、HGDHとしても関係部門と連携しながら動向を注視しています。一方で、こうした規制により新たなビジネスチャンスが生まれると思っています。既に当社では欧州のGDPR対応でRegTechソリューションの提供を開始していますが、今後は米国政府の動向を見据え、規制対応が必要となるお客さまのニーズを事業機会としていち早く取り込むような戦略も展開していきたいと思います。

**Q4. 日立グローバルデジタルホールディングス社の今後の成長の方向性をお聞かせ下さい。**

当社では2019年4月より「2021中期経営計画」がスタートします。この新3ヵ年計画では、日立が持つIT、OT、プロダクトの強みを生かし、社会インフラ、ビジネスインフラをデジタルで変革することをグループ一丸となって目指します。HGDHグループとしても、グローバルでより大きな役割を担っていかなくてはいけないと思っています。各地域で注力すべき事業領域を定め、フロントBUと一体となって具体的な戦略を作りこんでいくことになりますが、そこで鍵を握るのは、やはり人財であると考えます。市場でトップクラスのデジタル人財を継続して獲得するとともに、既存人財のスキル転換を行い、日立グループのビジョンの実現を図っていきます。加えて、プロジェクトの確実な遂行のため、デリバリやサービス分野におけるM&Aやパートナリングも検討していきます。事業体制もデジタル＆グローバルに対応した形に進化させていくことも必要になってくると思います。何よりスピードが重要ですので、市場の変化に迅速に対応し、顧客ニーズを先回りして新たな価値を提供できる会社への変革を主導していきたいと考えています。

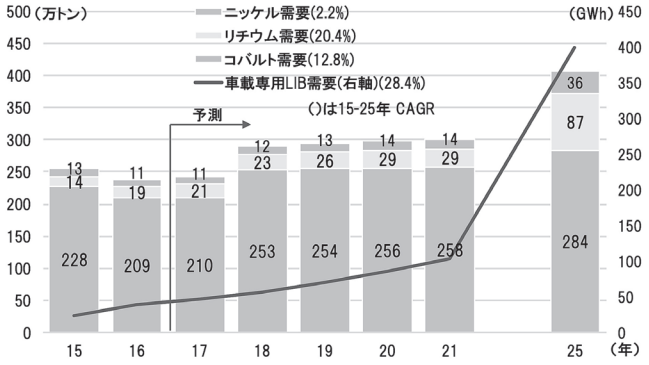
# 資源制約下の車載電池市場

研究第三部　産業グループ　副主任研究員
川上　隼人

2020年以降、世界各国の環境政策を受けて自動車メーカは電気自動車(EV)の普及を急速に推し進める。一方、EVの動力源である電池が、主たる原材料であるレアメタルの供給不足によりEV普及のボトルネックとなる懸念が生じている。本稿では、レアメタル資源制約の現状と、その課題解決に向けた車載電池市場における電池メーカなどの取り組みについて述べる。

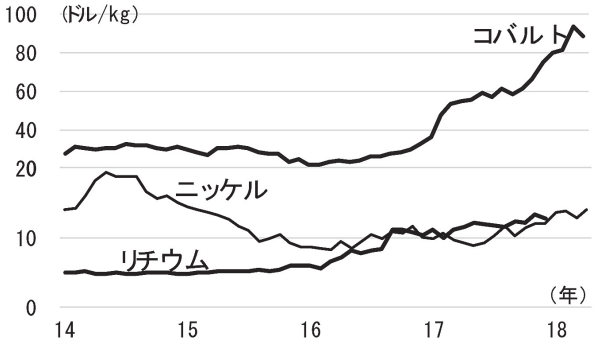
## 1. EV、車載電池市場が直面する資源制約

世界の主要自動車メーカが掲げるEV販売台数の目標値によれば、EVの動力源であるリチウムイオン電池（LIB）の需要は2025年にかけて現在の3～4倍に急増する可能性がある（図1）。LIBの基幹材料であるコバルトを主としたレアメタルは需給逼迫懸念が顕在化し、市場価格は既に高騰している（図2）。特に銅などの副産物であるコバルトは、主産物である銅の市況に生産量が左右されるだけでなく、生産・埋蔵量の約60%が紛争などの深刻な地政学リスクを抱えるコンゴ民主共和国に偏在しているため、サプライチェーンリスクが極めて大きい。また、現在確認されている可採埋蔵量が需要の大きさに比べて少ないことも将来の供給不安に拍車をかけている[1]。




注：2025年のEV販売を約700万台と想定
資料：富士経済ほかより日立総研作成

図1　電池材料レアメタルの需要見通し

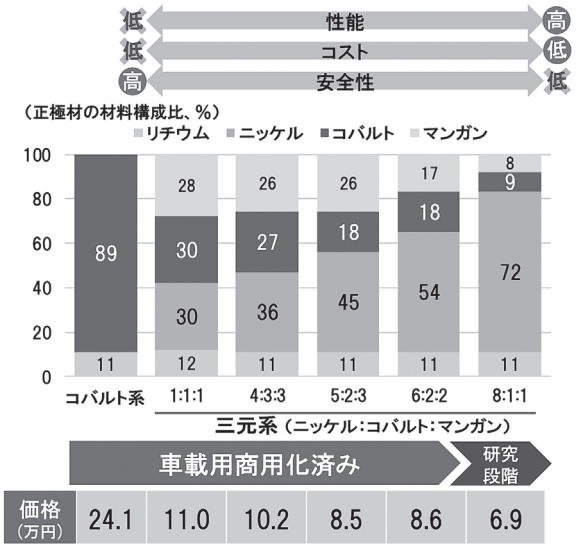



資料：LME ほかより日立総研作成

図2　電池材料レアメタルの価格推移

## 2. 省資源電池開発の重要性拡大

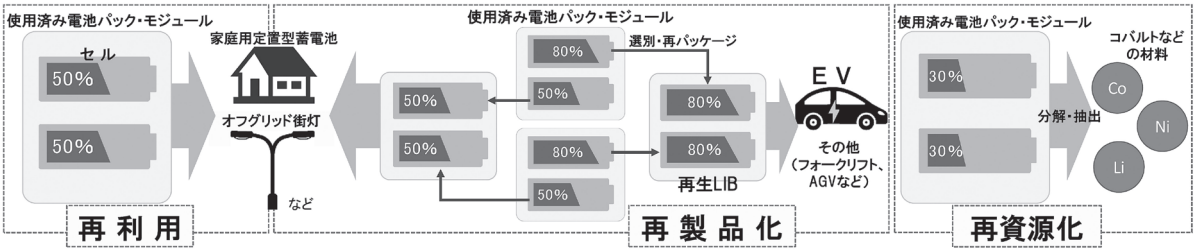
自動車メーカは、EV価格の低減を、LIBのコスト削減により実現させる計画であるが、レアメタルの高騰がその障害となる。そこで、自動車メーカや電池メーカは、コバルトを比較的安価なニッケルやマンガン等に一部材料置換することで使用量を減らし、コストダウンしつつ性能向上や安全性の維持が可能な電池の開発を進めている（図3）。また、レアメタル不使用かつLIBよりも高性能な金属空気電池などの次世代電池も同時に研究開発が進められているが、実用化は早くとも2030年以降の見込みである。




注：価格は17年スポット価格。容量40kWhで試算
資料：富士経済ほかより日立総研作成

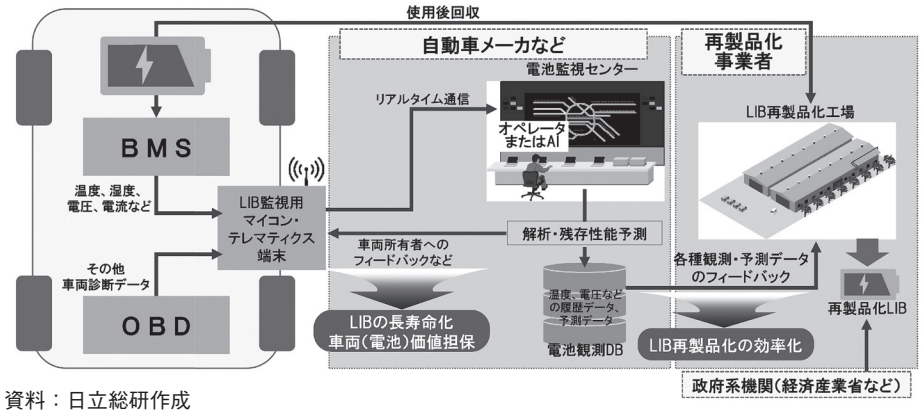
図3　LIB正極活物質の組成パターン

[1] 前述の自動車メーカの目標値に沿う需要量と現在の可採埋蔵量から試算すると2037年に枯渇。ただし、可採埋蔵量はあくまで現在確認されている埋蔵量のうち、技術的、経済的に採掘可能な量を示すものであり、後に増加する可能性がある。




資料：日立総研作成

図 4　LIB の再活用（再利用、再製品化、再資源化）のイメージ




資料：日立総研作成

図 5　LIB の再生効率化に向けた監視・残存性能予測のイメージ

## 3. 使用済み電池の再製品化

レアメタル材料の価格高騰への対応として、使用済み LIB 再活用の重要性も拡大する。LIB の再活用には主に以下三つの方法がある（図 4）。

1.再利用：電池パック[2]をそのまま再利用

2.再製品化：電池パックを構成するセルまたはモジュールのうち、一定の残存性能を持ち、再利用可能なものを選別して再パッケージ

3.再資源化：セルを分解し、レアメタルなどの材料を再資源化

このうち、再製品化した LIB は EV 向けに求められる性能基準を満たし、かつ安価に提供可能という点で活用が期待されている。既に日産自動車は 2018 年から国内において自社の EV「リーフ」向けに再製品化 LIB の供給を開始した。新品 LIB の 78%の容量保証という条件付きながら半額以下の価格で提供している。

使用済み LIB の再製品化には、残存性能（容量、充放電効率など）の評価を事前に行うことが不可欠である。日産自動車と住友商事の合弁会社であるフォーアールエナジー社は 2010 年から回収した使用済み LIB を用いて残存性能評価のノウハウを蓄積することでその技術を確立し、EV 向け LIB の再製品化事業を実現している。

[2] 電池パックは複数のセルで構成されるモジュールを、センサーやコントローラとともに複数個接続し、パッケージしたもの。

## 4. 今後の展望

LIB の残存性能評価は、使用後の評価作業だけによらず、使用中から LIB の稼働状況を監視し、そのデータを蓄積、活用することで評価時間の短縮や評価精度向上が可能である。例えば、EV に搭載の BMS（バッテリーマネジメントシステム）が LIB の稼働状況に関するデータ（温度、湿度、電圧、電流など）を収集、監視し、これらデータと車の OBD（On-board diagnostics 自己診断機能）から得られる車両情報などに基づき、リアルタイムに使用中 LIB の残存性能を予測するといったことが考えられる。この際、自動車メーカなどとの協業により BMS や OBD データをテレマティクス経由で受信し、リアルタイムに管理、残存性能予測を行う監視センターの役割を担う事業者も必要となるだろう（図 5）。

資源制約の克服に向けては、省資源化に向けた電池の技術革新のみならず、電池の長寿命化や使用済み電池の再活用などのアプローチをとる企業が現れ、車両や電池の稼働データなどを用いた付帯サービスの開発などのイノベーションと従来の産業の枠を超えた連携が進むだろう。

日立総研は引き続きこれらの動向を注視し、車載電池、EV およびその関連産業の将来を展望していく。

# Addressing Digital Protectionism in ASEAN: Towards Better Regional Governance in the Digital Age

by Dr Kaewkamol Pitakdumrongkit, Assistant Professor, RSIS, Nanyang Technological University, Singapore

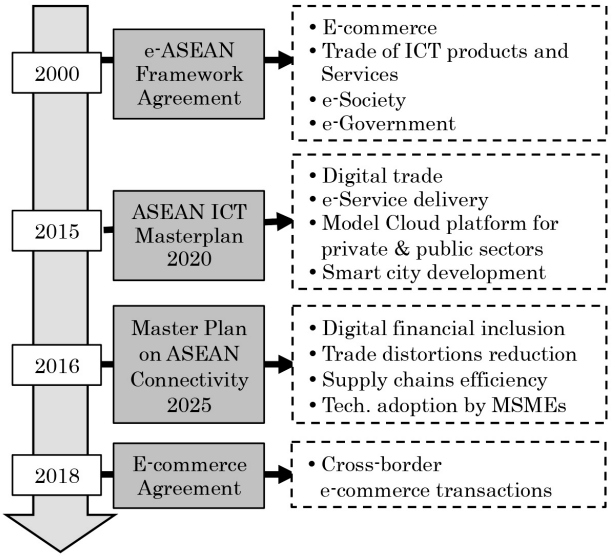
APAC Group, 2nd Research Department

The ASEAN region is increasingly becoming digitalized. It has over 700 million active mobile subscriptions, higher than the population. Number of Internet users is forecasted to reach 480 million by 2020. The size of digital economy is estimated to grow from USD 150 billion in 2016 to USD 200 billion by 2025, reflecting high potential. With this background, this paper points out digital protectionism (data regulations) that exists in ASEAN countries, challenging the regional growth.

Author of this paper, published in March 2018, is Dr. Kaewkamol Pitakdumrongkit. Her research areas include global and regional economic integration.

## 1. ASEAN Regional Frameworks towards Digitalization

The paper points out strong intention of ASEAN nations for regional integration. For this, they have launched several initiatives, but the author focuses attention on digital initiatives (Fig. 1).




Note: Micro, small and medium enterprises (MSMEs)
Source: ASEAN Secretariat

Fig. 1 ASEAN Initiatives towards Digital Integration

It considers digitalization, especially 'digital economy' and 'e-commerce' as the key for regional integration: ASEAN Economic Community (AEC).

## 2. Digital Protectionism in ASEAN

In spite of these initiatives, the paper points out that "digital protectionism" still exists. For the definition, it refers to view of the Office of US Trade Representative (USTR) that digital protectionism includes restrictions on cross-national data flows, digital technology & products, Internet services, and other related issues e.g., e-payment systems.

### 2.1 Data Regulation barriers by ASEAN Nations

The paper highlights regulations among ASEAN nations that create digital protectionism (Table 1).

Table 1 Data Regulations creating Protectionism

| Type | Country | Regulation/ Policy |
|---|---|---|
| Data Localization | Indonesia | Local data center & disaster recovery center for public services. |
| | Vietnam | One server locally for online social networks. |
| | Malaysia | Ask permission to move personal data abroad. |
| Government Procurement | Philippines | Asking agencies to use 'Government Cloud'. |
| Local Content | Indonesia | >30% local parts in hw/sw for LTE devices. |
| Intellectual Property | Thailand | Long pendency period for patent registration. |
| Taxation | Thailand | (plan) VAT on foreign e-commerce businesses. |
| | Indonesia | (plan) Tax e-commerce transactions. |

Source: National Governments; KPMG; Asian Nikkei Weekly

In addition, the paper points out certain other regulations that challenge the advancements of digitalization. Such as Indonesia's Financial Services Authority (OJK) requiring foreign companies (incl. venture capital) to seek local partners before investing in Start-ups.

### 2.2 Impact of Data Regulation barriers

Raising the issue of digital protectionism, the paper perceives it to undermine the ASEAN's efforts towards regional integration. To substantiate this, it highlights role of digital economy and e-commerce in the AEC Blueprint 2025 that seeks to:

- Explore further utilization, coordination of ICT for economic development & promote 'digital trade'.
- Enhance 'digital economy' by harmonizing legal frameworks for online dispute settlement; creating inter-operable, & secure electronic identification & authorization mechanisms, etc.
- Promote financial integration by enhancing 'digital payment services'.

The paper also points out the AEC's emphasis on development of MSMEs (micro, small and medium enterprises), considering them backbone of ASEAN (~96% of regional enterprises, 1/3rd of ASEAN exports to world). It highlights that AEC considers e-commerce significantly beneficial in reducing barriers to entry & operating costs for MSMEs.

Then, looking at the AEC 2025 goals, the paper raises risks from digital protectionism. It perceives regulation barriers to restrict the development of cross-border e-payment system, raise the MSMEs' costs of doing business, and reduce their participation in the regional economies.

The paper also emphasizes the point of individual economies intertwined in transnational production networks (TPNs). Consequently, goods & services are produced across multiple nations in supply chains. In such an environment, companies have to share information e.g., product designs, inventories, and logistics data across national borders. The paper raises concern that digital protectionism blocking cross-border data flow will affect all the companies in production chains and have repercussions across entire ASEAN region.

## 3. Policy Recommendations for addressing Digital Protectionism

To address these challenges, the author lists action points that ASEAN policy makers could consider:

(i) Common definition of "digital protectionism": consider adopting definition of other organizations, e.g., US or EU. This will fast build common understanding instead of defining it from scratch.

(ii) Quantify market-distorting effects of regulations: Develop a database of protectionist measures to guide policy makers. ASEAN nations could use other organizations' approach to quantify damages from barriers. E.g., the Organization for Economic Co-operation and Development (OECD), United Nations Conference on Trade and Development (UNCTAD), Universal Postal Union (UPU), and World Trade Organization (WTO) are collaborating on cross-border digital trade measurement.

(iii) Policy discussion platform: Create an informal forum for member nations to discuss, clarify and exchange views on each other's policies and effects on multilateral trading system.

(iv) Enhance officials' rule-making capacities: Provide trainings for technical knowledge & skill enhancement to policy makers with schemes such as the Initiative for ASEAN Integration (IAI).

This paper raises two interesting topics. One is the role of digitalization in the regional integration initiatives. Second is digital protectionist regulations across nations. But, both cannot go together for long. Digital protectionism will challenge advancements of digitalization and impede ASEAN's progress towards AEC. In this context, the author's recommendation to "Quantify market-distorting effects of regulations" is vital for harmonizing the regulatory environment on regional basis in the ASEAN.

日立総研

vol.13-4

2019年2月発行

発　行　人　白井　均
編集・発行　株式会社日立総合計画研究所
印　　刷　株式会社 日立ドキュメントソリューションズ
お問合せ先　株式会社日立総合計画研究所
東京都千代田区外神田一丁目18番13号
秋葉原ダイビル　〒101-8608
電　話：03-4564-6700（代表）
e-mail：hri.pub.kb@hitachi.com
担　当：主任研究員　宮崎　祐行
http://www.hitachi-hri.com

日立総研

www.hitachi-hri.com