

東京大学公共政策大学院研究プロジェクト
「IT企業の国際展開をめぐる政策課題」
とりまとめ

2023年3月

プロジェクトの経緯と問題意識

東京大学公共政策大学院は、2022年に研究プロジェクト「IT企業の国際展開をめぐる政策課題」（担当教員：宗像直子教授）を実施した。

日本のIT企業、特にインターネットサービスを行う企業（以下「インターネットサービス企業」）は、グローバルな事業の成功のために、人材獲得競争に対応し多様な国籍の人材が幅広く活躍できる環境を確保する必要がある一方で、各国のデータガバナンスの違いや経済安全保障の観点を踏まえたデータ管理、リスク管理の高度化が求められるようになってきている。特に、中国では国家が国民に諜報活動への協力を法律上義務付けたことから、個人が出身国と所属企業の板挟みになるのではないかと懸念が発生している。

本プロジェクトにおいては、こうした課題について、株式会社メルカリほかインターネットサービス企業有志をメンバーとし、政府、研究者、産業界の有識者（注）の参加を得て、国際情勢や各国政策の把握、経営戦略に適合したリスク管理の基本的考え方や着眼点、データガバナンスの具体的なあり方（海外での開発拠点の設置、業務委託先の選定、従業員のデータアクセス元の管理など）について議論を行った。

議論の中では、国際情勢認識やリスクについての考え方に温度差がある点も見られたが、本稿では、この問題を深めていく上で重要と思われる論点と今後の課題を公表に馴染む範囲で示しておく。

（注）研究会に参加した有識者（敬称略、五十音順）

伊藤 隆	三菱電機株式会社 経済安全保障統括室 室長
内田 了司	経済産業省 通商政策局 国際経済課長（当時）
佐橋 亮	東京大学 東洋文化研究所 准教授
佐脇 紀代志	個人情報保護委員会事務局 審議官（当時）
目黒麻衣子	商務情報政策局総務課国際室長

1. 経済安全保障をめぐる内外情勢

①米中対立の常態化

米中関係においては、米国トランプ政権が2017年12月の「米国国家安全保障戦略2017」において中国を初めて名指しで競争相手と位置付けたことを契機として、覇権をめぐる争いが顕在化し、激化している。2018年8月に成立した「国防授權法2019」が上下両院で共和・民主両党の圧倒的支持を得ていたことに示されるように、対中政策の転換は超党派の支持によるものであった。同法には、中国の軍民融合戦略を念頭に、輸出・投資規制強化、政府調達制限等が盛り込まれた。その後バイデン政権下では、サプライチェーン強靱化のための国内研究開発・製造支援、先進半導体の対中輸出規制強化などが導入されている。米中対立の背景には、中国が既存の国際秩序に挑戦する姿勢を行動で示し始めたことだけでなく、軍事力やこれを支える経済力の基盤となる先端技術における競争力で米中が肉薄したことに對し米国が優位を維持しようとしていることもある。このため、米中対立は、特定の政権の政策に左右されるものではなく、構造的に定着したものと捉える必要がある。

②日本の経済安全保障政策の強化

日本は、技術やデータの保護、サプライチェーンの強靱化等を含む経済安全保障政策を導入するとともに、東アジアにおける紛争を抑止するため、同盟国である米国をはじめ、欧州やインド太平洋地域の同志国との結束強化を図っている。岸田政権下では、経済安全保障担当大臣が置かれ、経済安全保障推進法が成立し、2022年末に策定された「国家安全保障戦略」が安全保障関連分野の諸政策の一つとして経済安全保障を位置付けた。日本の経済安全保障政策は、今後、国の安全保障政策の不可分の要素として継続的に実施、充実されていくものと捉える必要がある。

2. IT企業の事業に直接関連する関連する国内制度の状況

①改正個人情報保護法の施行

2022年4月、改正個人情報保護法の施行により、個人データの外国への移転の際、顧客本人の同意を根拠に移転させる場合には、同意を取得する際に当該外国の名称などを本人に伝えることが求められることとなった（法第二十八条第2項）。基準に適合する体制を整備した事業者への移転など、個人データの外国への移転の際に本人の同意が求められない場合であっても、事後的

に本人から開示を求められた場合には、移転先の国名などを本人に伝えることが求められることとなった（改正個人情報保護法第二十八条第3項）。この法改正は経済安全保障の要請に基づくものではないが、経済安全保障の議論における技術・データ保護への注目を踏まえると、個人データの移転先の評価に当たっては、経済安全保障の観点にも留意する必要がある。

②改正電気通信事業法の成立

2022年6月、改正電気通信事業法が成立した。この改正では、一定の規模以上の顧客データ（利用者情報）を取り扱う事業者に対し、個人情報保護法よりも厳格なガバナンスが新たに義務付けられた。具体的には、適正な取扱いが求められる利用者情報（個人情報より広範）が「特定利用者情報」と定義され（法第二十七条の五）、その内容、利用目的・方法、安全管理、苦情・相談等に関する情報取扱方針の公表が義務づけられた（第二十七条の八）。海外のサーバ等を利用する場合には、情報取扱方針の安全管理の内容として、その外国の名称、その外国の個人情報保護制度や外国の第三者が講ずる個人情報保護のための措置に関する情報など幅広い事項を記載することが求められる（電気通信事業における個人情報保護に関するガイドライン等）。

3. 海外の事業環境

①ウクライナ侵略後の国際情勢

2022年2月のロシアによるウクライナ侵略によって、G7を中心とした先進国の自由主義陣営と、中国やロシア等の権威主義陣営との対立が激化しているが、南半球を中心とした途上国（グローバルサウス）は、そのどちらにも属さず個々の問題ごとに自国の利益を最大化する対応を取っている。日本のIT企業が開発拠点を設置したり、業務委託したりする国にも、この第3の類型に属するところが多くあり、各国の状況を個別に確認する必要がある。

②データガバナンス・データ流通の国際的な制度調和の動向

米・欧・中は、データの自由な流通・利用による経済効果、人権としてのプライバシー保護、国家による情報統制など、それぞれ重視するものに応じて異なる制度・市場を形成している。

日本政府は、OECDや多国間協定・個別の経済連携協定（EPA）などを通じて信頼性のある自由なデータ流通（DFFT）を促進する取り組みを進めている。各国とも総論は賛成しているが、具体的な取り組みについては、現時点ではベストプラクティスを共有する段階に留まっている。

③アジア諸国における事業環境とデジタルルールの行方

アジア諸国におけるIT事業環境の予見可能性を高める上で、高いレベルのデジタルルールがこれらの国々に広がることが期待される。

- ・環太平洋パートナーシップに関する包括的及び先進的な協定（CPTPP）には、ASEAN諸国からシンガポール、マレーシア、ベトナム、ブルネイが参加している。ただし、ベトナムでは、個人情報に関する規制を厳格化し、国内保存義務と組み合わせた厳しい越境移転規制を導入する動きがあることに注意を要する。
- ・世界貿易機関（WTO）の有志国による「電子商取引に関する共同イニシアティブ」（88カ国が参加）は、米国・EU・中国が一堂に会する世界最大のデジタル貿易ルール交渉として注目される。
- ・2022年5月のバイデン米国大統領訪日の際に立ち上げられたインド太平洋経済枠組（IPEF）は、デジタルルールを貿易の柱の主要テーマの一つとしており、今後の展開が注目される。

④中国に関わるデータセキュリティ上のリスク

2017年国家情報法第7条により、中国国民は国家の諜報活動に協力する義務を負うこととなった。また、2017年サイバーセキュリティ法、2020年暗号法、2021年データセキュリティ法など一連のデータ関連法が制定され、中国国内で活動する企業のデータは、国内保存が義務付けられると共に、国家安全保障上の理由があれば中国政府が随時アクセスできることとされた。これを受け、米国政府は、2020年12月に、米国企業にデータセキュリティに関する警告情報を発出し、中国が軍民融合戦略の下、国家ぐるみでデータ窃取を行っており、中国関連企業からデータサービスや機器を調達したり、中国関連企業が開発したソフトウェアや機器にデータを保存したりする場合に、経済的、レピュテーション上、法的リスクがあることを認識し、デューデリジェンスによってリスクを軽減すべきとしている。

⑤中国に関わるその他のリスク

日本企業の中国事業拠点については、米国企業同様、有事の際の社員の拘束・資産の接収などのリスクを想定する必要がある。平時における強制技術移転のリスクや供給網における過度の対中依存などの経済安全保障上のセンシティブティは、業種や事業活動の態様によって異なる。中国事業を有する企業においては、今後起こりうるシナリオを具体的に想定し、対応策を検討する動きが見られる。

4. 結論：事業運営上の指針・論点

上記の情勢変化を踏まえ、日本のインターネットサービス企業は、海外市場進出、海外人材の活用等に当たって、経済安全保障の視点を踏まえたリスク管理がこれまで以上に求められている。その際、以下の点に留意する必要がある。

- ①米中対立を契機として顕在化した経済安全保障の要請は、長期的に継続する。国際秩序の安定は、リスクを下げる役割を果たしてきたが、秩序が流動化している現在、新しい均衡が形成されるまでの間、不安定で予測可能性の低い状況が続く。
- ②特定の国や地域からのアクセスを特別に制限することについて、多様性を重視している社内において、外国籍の社員にどう説明するか難しいとの声が多く聞かれた。データアクセス管理については、国籍に基づく形式ではなくリスク管理上の必要性という実質から社内で実施すべきものを決定することで、従業員が納得できる説明を行いやすくなるのではないか。
- ③経済安全保障の視点を踏まえたリスク管理は、各企業が自社の事業特性や社会からの期待を踏まえ、自ら実質的なリスクを評価し、自社の経営戦略に適合する形で行うものであること。その際、例えば「あらゆるデータを国内で保管する」（政府はこれを求めている）といった形式的な基準でリスクを過度に回避することなく、他方、例えば、法令を遵守さえしていれば大丈夫だと考えてリスクを過度に受容することなく、各社が実質的に適切な判断を行えるよう、今後、企業の課題や事例を官民で共有し、分析の観点を充実させることが期待される。
- ④海外の事業環境に影響を与えるWTO等の国際ルールや国際情勢についての理解を深めると共に、自ら望ましい国際ルールを検討し、政府に働きかけていくことが今後の課題である。国際ルールやトレンドの理解にあたっては、個社での情報収集には限界があるため、経済界/産業界として、業界団体による勉強会などを通じて、広く情報が共有される体制や機会を提供することが重要である。また、「経済安全保障基本方針」（第1章第二節（3）事業者との連携）に示される通り、各社の自発的な行動が促進されるよう、政府として、官民の適切なコミュニケーションや情報提供体制の構築に努めていくことも今後の課題である。

以上