

訴訟データ*1の証拠開示プロセスにおいて機微情報の国外流出(懸念国等)を防ぐための提言 ～我が国の企業が保有する技術情報データの適切な管理に向けて～

特定非営利活動法人 デジタル・フォレンジック研究会
令和6年6月14日

*1訴訟データとは、eディスカバリが必要になる民事訴訟(知財訴訟、PL訴訟等)、各国の政府機関からの調査(独禁法、品質不正、海外腐敗行為防止法等)に関するデータを示す。そのデータとは企業のコンピュータ、ストレージ、サーバ、データセンター等にあるデータのほか、メール、SNS等のデータをデジタルフォレンジックにより解析用に加工し、検索しやすいようにインデックス化(時刻、その他の属性情報等)し整理・分類されたデータである。

1 提言の社会的背景

国際的な安全保障環境の変化に伴い、2022年5月に経済安全保障推進法が可決され、柱となる4つの項目「(1)サプライチェーン強靱化 (2)基幹インフラの信頼性・安全性の確保 (3)先端技術の官民協力の枠組み構築 (4)特許非公開制度」が整備されたことで、我が国の経済安全保障を取り巻く環境を強化する基礎が整えられた。

その一つとして、今回提示したいのは、『訴訟データにおける証拠開示のプロセスにおける技術情報開示について』である。我が国では、国益に関わるような機微データを、民間企業が国外に送ることを制限する規則がなく、日本企業の機密情報が訴訟を通じて他国に流出することを防げない状況にある。訴訟という名目で合法的に情報を取得できる訴訟データの取り扱いに関しては、極めて重大な課題であり至急解決すべき事案である。

一方で、先進諸国は法律において国内企業の保有するデータ管理が規定されているのが実情であり、これが全くない我が国は、国内情報保護の分野において大きく出遅れている。

中国では、2021年以降、複数のデータ管理に関連した法律が策定・施行され、許可なく国外の司法機関にデータを提供することが禁じられた。つまり、例えば日中の企業間で紛糾が生じ、訴訟に発展した場合、中国側は法律に基づきデータ移転を規制できるが、日本側は中国に機微情報が渡ることを規制できない。中国政府が、国内民間企業に対しても情報開示や政府の指示を徹底することを求める現行法制度や、中国が経済の分野においても覇権主義的挑戦を今後も継続することが考慮される現状において、安全保障上の観点からも、十分に警戒し早急に対策を講じる分野であると言える。

そもそも、我が国の民間企業間では、訴訟データの証拠開示プロセスにおいて、機微情報流出の可能性があるという認識は一般的ではなく、これまでも一切の対策がなされてこなかった。重要経済安保情報の保護及び活用に関する法律が成立した中、日本国として本件においても早急に改善すべき課題である。

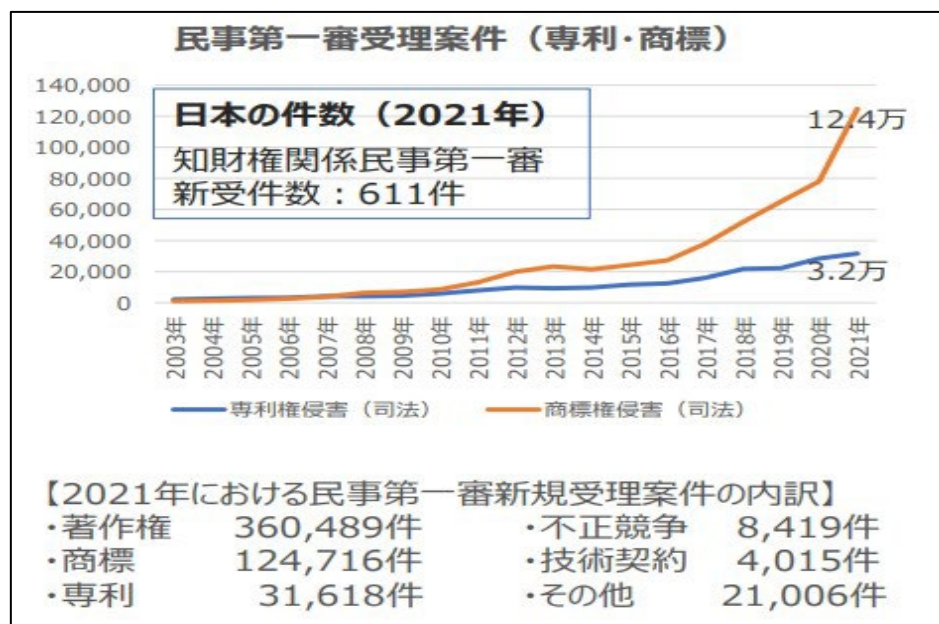
■ 中国の*21782条ディスカバリを適用した情報取得の脅威

これまで日本企業は、米国や欧州を中心とした国際訴訟の対応を行ってきたが、近年、中国における、知的財産に関する訴訟の件数が急増している。中国における特許の出願数を見ると年々増加傾向にある。2011年には年間52万件を超え世界一となり、2021年までに約3倍に増大している(図1)。同様に知財 訴訟の件数も商標権侵害を例にすると2012年から2021年で約6倍に増えている(図2)。これまでのように、弁護士に言われるまま、eディスカバリにおける選別作業で扱う電子データを中国の法律事務所にすべて送る状況が頻発すれば、安全保障及び経済安全保障上の極めて大きなリスクとなることは明らかである。

また、1782条ディスカバリを適用した日本企業からの機微情報流出事例も存在する。一方、我が国は民間保有データに対する越境的収集に対抗できていないケースも多い。今後、政府関連情報だけではなく民間保有の企業秘密情報においても、中国に限らず諸外国によるデータの越境的収集に対抗措置が必要である。

*2米合衆国法典 28 編 1782 条

図2：中国の知財訴訟件数



※出典：2022年11月「中国における知的財産を巡る現状と課題」(JETRO 北京)より抜粋

https://www.kyushu.meti.go.jp/seisaku/titeki/oshirase/221207_1_5.pdf

2 eディスカバリの実態

米国では民事訴訟の際に、ディスカバリ(証拠開示手続き)という制度が存在し、証拠となる資料を当事者が提出する必要がある。電子的に保存されている情報に対してこれを行うことをeディスカバリとよぶ。

FTC(連邦取引委員会)、SEC(米国証券取引委員会)、ITC(米国国際貿易委員会)等による企業に対する調査でも同様の制度が存在しており、企業にとって大量の電子データの中から証拠を選別して提出する作業負担は大きなものとなっている。そのため、これを支援するeディスカバリベンダーと呼ばれる業者が存在する。

eディスカバリ制度において裁判所に開示するデータは、本来、弁護士を選別し、秘匿特権等で提供できない部分を隠した上で訴訟の関連証拠として提出するデータのみであるが、我が国では、eディスカバリ作業の便宜のため、選別前の全てのデータを海外に持ち出してしまふことがしばしば発生する。その原因となるのが、日本では、eディスカバリにおける選別作業で扱う電子データを置く場所(保全場所)やデータを見て証拠か否かを選別する人間に関する規制がないことである。

このため、eディスカバリによって米国の裁判所に証拠となる情報を提出する必要が生じた場合、米国の弁護士事務所の指示に従い、選別作業で扱うデータが米国に送られ、弁護士事務所ではなくeディスカバリベンダーが保管(ホスティング)する事態がしばしば発生する。eディスカバリベンダーは世界中にあるため、ホスティングは中国を含む世界のあらゆる場所で行われる可能性がある*。

eディスカバリにおける選別作業で扱うデータは、具体的には日本を代表する自動車関連や半導体、鉄鋼、重工業企業等の最先端技術に関する研究段階の技術資料や設計書、図面、実験結果、性能評価資料、事故調査資料、社長など経営陣のやり取りも含むメールである。前述のとおり、これらのデータは多くの場合、海外のeディスカバリベンダーへ送られ、実際にはさらに複数の下請け企業が作業に関与する状態となっている。経営会議や戦略に関する資料が最終的にどこに保管され、誰が見ているかを把握することが不可能に近い状況は危機的であるといってもよいが、日本ではこの状況が継続している。

米国において、eディスカバリが必要になるケースは民事訴訟(知財訴訟、PL訴訟等)、各国の政府機関からの調査(独禁法、品質不正、海外腐敗行為防止法等)である。すでに水面下では eディスカバリベンダー経由で日本企業の技術情報が流出し、莫大な被害が生じた例も確認されている。

※本リスクについて認識している一部の弁護士は、担当する訴訟案件のデータを日本にとどめておくことを推奨している。実際、eディスカバリ支援を行う日本企業がデータを保全する場合は、データを日本国内に置いているが、訴訟に支障をきたしたことは一度もなく、訴訟上不利になったこともない。

3 訴訟により海外に提出されたデータのゆくえ(米国の例)

2010年12月、米国第9巡回区連邦控訴裁判所において、「訴訟や調査で米国内に入ったデータに対しては、大陪審への召喚命令を禁じることはできない」という判例が出された。

(In re: Grand Jury Subpoenas, No. 10-15758, slip op. at 19638 9th Cir. Dec. 7, 2010 ※)

本案件は、液晶パネルに関わる犯罪行為の嫌疑で、米国政府がある日本企業に対して独占禁止法上の捜査を実施したものである。非米国企業が米国外から証拠を含む文書を提出し、米国内の法律事務所はその文書を所持していた。犯罪捜査の一環として、大陪審による文書提出命令で米国内の法律事務所にあるものは、大陪審の管轄内になったわけであるが、大陪審が管轄するという事は、すでにこの時点でデータは米国に管轄権が移ったという論理である。(同種のことは、米国以外の国々においては特段の告知が行われていないが、同様に扱われていると考えるのが妥当であろう。)逆に日本に進出している米国企業は、訴訟対応を 米国本社が行っており、データの解析・閲覧・ホスティングの場所や取扱者への規制を設けることで、米国外への情報流出を防いでいる。

※ <https://cdn.ca9.uscourts.gov/datastore/opinions/2010/12/07/10-15758.pdf>

4 国内民間企業が保有する機微情報に対する諸外国の動向

先進諸国を中心に、諸外国においても、データを国内で適切に管理する機運が高まりつつある。EU、英国、中国、韓国の動向を以下に挙げる。

欧州連合(EU)では、個人情報の保護を目的とした「EU一般データ保護規則(General Data Protection Regulation:GDPR)」が、2018年から適用されている。GDPRは、EUを含む欧州経済領域(EEA)域内で取得した「氏名」や「メールアドレス」「クレジットカード番号」などの個人データをEEA域外に移転することを原則禁止している。訴訟において証拠となる情報の中には、当然個人データも含まれる可能性が極めて高く、保全した全個人データを個人データ以外と区別して除外するのは不可能であるため、GDPRは事実上、eディスカバリの過程での収集データは国内で保管することを規定していることになる。

英国では、EU離脱前はGDPRが適用されていた。EU離脱後の移行期間終了後は、2018年6月に採択された2018年EU離脱法に基づいてGDPRが英国法に置き換えられ、そのまま英国法として適用された。GDPRを英国の事情に合わせて補完し調整する「2018年データ保護法」も継続して適用された。これにより、電子データの処理を行う場所やホスティングする場所は英国国内に限定されることになり、データが英国国内に保管される制度が整っている。

中国では、2016年6月施行のサイバーセキュリティ法(网络安全法)第37条により、重要データの国内保存義務や、許可なく国外にデータを提供してはならないことが規定された。さらに、2021年9月施行のデータセキュリティ法(数据安全法)第36条、2021年11月施行の個人情報保護法(个人信息保护法)第41条では上述の規定に「司法機関」という単語が追記され、許可なく国外の司法機関にデータを提供してはならないと規定された。

韓国では、2022年8月4日に「国家先端戦略産業競争力強化および保護に関する特別措置法」(国家先端戦略産業法)が施行された。同法では国家先端戦略技術保有者に対する規制や、先端戦略産業の育成、保護などの支援について盛り込まれた。その他、2007年4月28日に「産業技術の流出防止及び保護に関する法律」(産業技術保護法)が施行されており、その後も複数の改正を経て産業技術の流出防止・保護に対する法律が整備されてきた。現時点では中国のように許可なく司法機関へのデータ提供を禁止しているわけでは

ないが、韓国企業が保有する機微情報が外国に輸出されることを規制する法体制は整備されている。実際に韓国企業が係る国際訴訟において、韓国当局がハイテク企業に対して訴訟データは韓国内に保管し、国外へ出さないことを要請し、最小限の証拠データのみを米国へ提出するよう指示したケースが複数ある。ハイテク企業のみならず金融機関においても同様の措置が取られている。

5 提言『訴訟データの国内処理・保存』

諸外国では、訴訟データに関わるデータ処理・保存をどこで行うのか、安全保障上の規制がなされているが、我が国では対応する規制がない。日本企業の機密情報の海外流出を防止するため、訴訟に関するデータ処理・保存の場所を日本国内に限定する規制もしくはガイドラインを定めるべきである。

特に経済安全保障推進法の中で指定されている特定重要物資に関する案件に関しては、訴訟を通じた流出への対処を喫緊に進めるべきである。セキュリティ・クリアランスを取得した職員の所属する企業・団体は、訴訟データの域外移転を規制する措置を早急に講じる必要がある。

参考:e ディスカバリベンダーの質の担保

日本語データの処理が適切にできないeディスカバリベンダーに作業が委託された事例もあるため、eディスカバリベンダーの質を担保する必要がある。ガイドラインとして、例えば、NPOデジタル・フォレンジック研究会^{*}が提供している日本語解析評価試験^{**}などの点数を開示すること等を定めるべきである。

※ <https://digitalforensic.jp>

※※ <https://digitalforensic.jp/category/jpap/>

以上