経済安全保障の観点を含めたデータガバナンスを推進するうえでの企業実務対応のポイント

株式会社 野村総合研究所
CX コンサルティング部
チーフコンサルタント　渡辺　翔太

1　はじめに

米中対立に起因する重要インフラ保護への意識の高まりや、新型コロナウイルス感染症によってマスクなどの感染予防に必要な医療製品のほか、半導体などの重要な部品のサプライチェーンが大きな影響を受けたことを背景として、日本でも経済安全保障への意識が高まり、2022 年 5 月には経済安全保障推進法が成立した。

日本企業においても、近時、大手企業を中心に経済安全保障を専門とする部署を設置する動きが見られる※1。現状の日本企業における経済安全保障への体制整備は、輸出管理やサプライチェーンの再編など物理的なモノに関する対応が中心である。しかし、筆者はデジタル化された情報、つまりデータに関する経済安全保障に関しても重要性が増しており、対応を進める必要があると考える。

そこで本稿では、なぜモノに加えてデジタルデータのガバナンスでも経済安全保障への対応を進める必要があるのか、対応が不十分な結果生じた問題や諸外国の規制の進展を説明したのち、企業が取り組みを進めるポイントを解説する。

2　民間企業がデータ経済安全保障の観点を取り入れる必要性

デジタル経済の発展に伴って、外国政府による選挙介入や、産業政策としてガバメントアクセスが実施されるリスクの高まりといった近時のトレンドを解説する。次いで、その対抗策として民間企業が持つデータの取り扱いに関する規制強化が進んでおり、経済安全保障の観点を取り入れなかった場合に生じるリスクについて述べる。

1）民間企業の保有するデータの重要性が増大

英国の EU 離脱を決める、いわゆる Brexit に関する国民投票や、トランプ前大統領が登場した 2016 年の米国大統領選挙において、英国や米国の有権者に対する外国政府による影響工作・浸透工作（influence operation）が問題視された。特に後者の米大統領選挙では、ロシア政府によって Facebook 等の SNS で米国民への政治広告を通じた選挙介入が大規模に実施されたと米国の調査で指摘されている※2。この調査によれば、ロシア政府は、傘下のロシア企業を通じて Facebook 等の SNS の広告配信サービスを活用した。SNS から提供される米国民のデータ、つまり民間企業が保有する米国民の年齢・居住地等のデータを、政治広告のターゲティ

※1　報道では、三菱電機、NEC、富士通、日立製作所等の名前が挙げられている（時事ドットコム 2022 年 3 月 15 日記事）
※2　川口貴久「ロシアによる政治介入型のサイバー活動～2016 年アメリカ大統領選挙介入の手法と意図～」https://www.spf.org/iina/articles/kawaguchi_01.html

NRI パブリックマネジメントレビュー
Public Management Review
Vol.228
July 2022

ングに利用したとされる。

また、企業が持つ重要な技術情報を獲得するため、外国政府がこれに関するデータを強制的に提出させる動きも顕在化している。この背景として、近年、新興国が持つ安全保障観は広範になり、軍事力を支える産業基盤の維持・発展が含まれるようになったことがある。典型例が中国であり、EU や米国は、中国市場へのアクセスと引き換えに自国企業が持つ技術の提供を強制されているとしてかねて問題視してきた。例えば「中国製造 2025」で育成対象とされた自動車産業において、中国における公道テストの実施と引き換えに、走行データそのものの提出を外資系を含む自動車メーカーに求めている。このような政府による強制力を持った民間保有データへのアクセスは「ガバメントアクセス」と呼ばれ※3、データを国外に移転する際に注意を払うべきリスクの一つである。

より俯瞰（ふかん）的な観点から見ると、上記の政府による民間データを活用する動きには情報の流通経路としてのインターネットの発達が大きく関連している。今後、サイバー空間とフィジカル空間が融合され、多様なデータが AI によって解析・活用される世界＝ Society5.0 が到来するとされる。Society5.0 の情報流通基盤となるインターネット、プラットフォーム（SNS 等）、クラウドサービス等はすべて民間企業が主体となって管理している。具体的には、インターネットは通信キャリアや ISP（インターネット・サービス・プロバイダー）、プラットフォームやクラウドサービスは GAFA 等が管理・運営している。今後拡大が見込まれる IoT 、例えば自動運転車等のリアル世界のデータ収集が加わっても、その運営主体はやはり民間企業が多くを占めるだろう。

このように、以前に比べ、民間部門が管理するデータが莫大（ばくだい）な量となり、政府は民間部門が保有するデータを活用した各種の活動が実施できるようになった。これが、経済安全保障の文脈で、民間企業が自らの持つデータの保護を真剣に検討する必要が生じる理由である。

2） 民間保有のデータに対する規制が拡大

1）で述べた外国政府による民間保有データアクセスへの対抗措置として、特に西側諸国を中心に、民間保有データに対する規制が強まっている。西側諸国である日米 EU はいずれも大枠では類似した規制を導入しているため、以降、特に読者に影響する日本の動向にフォーカスしてこれを解説していく。

まず、個人情報保護法の改正である。2022 年 4 月 1 日に改正法が施行されたが、この改正では、越境移転における情報提供義務が拡大された。同法を所管する個人情報保護委員会（PPC）は、その理由として、1）で述べた外国に移転されたデータにリスクを生じる動向、具体的にはガバメントアクセスとデータローカライゼーション（データを国内にあるサーバー等に保管する義務）を指摘している。

また、2017 年に行われた外国為替及び外国貿易法（外為法）改正では、データに関する安全保障上の重要性が増している点も考慮して、ソフトウエアやインターネット関連の業種が審査対象に追加され

※3　ガバメントアクセスについては、拙稿「ガバメントアクセス（GA）を理由とするデータの越境移転制限―その現状と国際通商法による規律、そして DFFT に対する含意―」（RIETI Discussion Paper Series 19-J-067）や同「GA のリスク拡大とその経済安全保障への影響」（中曽根平和研究所　経済安全保障研究会）を参照されたい https://npi.or.jp/research/data/npi_note_watanabe_20201224.pdf

た※4。従来、外為法の投資審査は、自国の重要な産業基盤（軍需産業）や重要インフラ（電力、通信など）への影響を避けるために審査対象を選定していたが、米国においては外国企業が自国民の大量の個人データや政府職員の個人データへのアクセスを可能とするような対内直接投資に対しても審査を強化する動きがあり、同法の改正はこれを日本においても制度上反映するものと理解できる。

最後に、2022 年 5 月に成立した経済安全保障推進法である※5。同法はサプライチェーン強靭（きょうじん）化、基幹インフラの安全性確保、官民重要技術支援、特許出願の非公開化という四つの柱からなり、半導体や非常事態における医療品等の確保など、冒頭述べた「モノに関する安全保障」に重点があるように見える。しかし、1）で述べたトレンドを踏まえるなら、データに関する規制にも活用できる条項がある点に着目すべきである。

まず、4 本柱の一つ目「サプライチェーン強靭化」では、対象として「特定重要物資」が指定される。報道では、その一つとしてクラウドサービスが検討されており、政府や重要産業に向けては国産クラウドの利用が義務化される可能性が指摘される※6。筆者はこの動きは欧州で独仏を中心に進む「主権クラウド（Sovereign Cloud）」を手本とした動きではないかと推察している。独仏では、日本同様、主要なクラウドサービスが米国企業に独占されており、米国政府によるガバメントアクセスを懸念したこれら政府が、政府機関や一定の重要インフラ企業に主権クラウドの利用を義務付ける。主権クラウドとして指定されるには自国企業が運営を含む管理権を持つことが求められ、自国企業（フランスでは Orange、ドイツではドイツテレコム子会社の T-System 等）と米大手クラウド事業者（現時点では Google と Microsoft）との合弁企業を政策的に構築し、米系企業の優れた技術を、米国政府の干渉を排して自国のクラウド基盤として利用する制度を整えている※7。

4 本柱の二つ目「基幹インフラの安全性確保」では、基幹インフラとして図表 1 に示す 14 分野が指定された（カテゴリーは NRI が追加）。当該分野の企業は重要なシステムを導入する際、設備の概要や部品、維持・管理の委託先などの計画を、主務大臣に届け出て審査を受けることが義務付けられる。後述する LINE 問題等を踏まえると、主務大臣による審査においては、クラウドサービスの利用や外国企業を含む第三者へのアウトソーシングといった、データの流通に関連した審査がなされる可能性が高いといえる。

3） 経済安全保障の観点を取り入れたデータガバナンスが求められる

以上の動向を念頭に、企業においても経済安全保障の観点を取り入れる必要があるといえる。データ

※4　総務省、財務省、経済産業省「対内直接投資等に係る事前届出対象業種の追加」https://www.soumu.go.jp/menu_news/s-news/01tsushin08_02000105.html

※5　同法の概説として、木内登英「経済安全保障推進法成立へ。企業活動への過剰関与のリスクも」https://www.nri.com/jp/knowledge/blog/lst/2022/fis/kiuchi/0511

※6　日本経済新聞「国産クラウド推進 政府、経済安全で『重要物資』指定へ サイバー攻撃に備え」（2022 年 5 月 7 日朝刊）

※7　独仏の進める主権クラウドについて、野村総合研究所（経済産業省委託）「デジタル経済発展に向けた諸外国におけるデータ流通関連制度等に関する調査 報告書」https://www.meti.go.jp/meti_lib/report/2021FY/000018.pdf　31 ～ 34 ページおよび 39 ページを参照

図表 1　経済安全保障推進法が規定する基幹インフラ

カテゴリー	14分野
ライフライン	電気、ガス、水道
放送・通信	電気通信、放送、郵便
金融	金融、クレジットカード
運輸	鉄道、貨物自動車運送、外航貨物、航空、空港
その他	石油

出所）内閣府説明資料より NRI 作成

ガバナンスが体制構築の途上にある中、さらに対応事項が増えることは企業実務者に負荷が大きいといわれるかもしれないが、この点を軽視した結果重大な経営リスクを招いたのが、LINE をめぐる問題である。

2021 年、LINE が日本ユーザーの個人情報を、グループ会社である LINE China およびグループ外の再委託先 1 社（いずれも中国企業）からアクセス可能な状態としており、数千万単位という巨大なユーザーを抱える通信サービス、つまり社会インフラを担う企業として不適切だと大きな批判を浴びるとともに、PPC や総務省への報告徴収、行政指導を受けたことは記憶に新しい。

また、LINE は韓国のサーバーに日本ユーザーが LINE 内で送受信した動画や画像等を保存していた。ただし、現行の個人情報保護法上、データを外国に移転することは必ずしも法令に反するものではない。実際、同社への PPC による行政指導の内容は委託先の適切な監督やアクセス制御に関するものであり、データを国外のサーバーに移転したことはその対象外とされている※8。

しかし、違法な点がなかったにもかかわらず、大量の日本ユーザーの通信内容という機微情報をガバメントアクセスの懸念がある国外のサーバーに移転、保管したことを問題視する批判が同社に寄せられた。同社が上記対応のため設置した「グローバルなデータガバナンスに関する特別委員会」は報告書の中で、「LINE 社においてガバメントアクセスへのリスク等の経済安全保障への適切な配慮ができていなかった」と指摘している。これを受け、LINE は「ガバメントアクセスのリスクを含む経済安全保障分野に関する管理体制が不十分であったことに対し、経済安全保障を考慮したデータガバナンス体制を構築していく必要があると認識しております。今後、当社に限らず、Z ホールディングス等を含むグループ全体として経済安全保障リスクを考慮した一体的な管理体制を構築することが検討されていることに対し、当社としても連携を行ってまいります」と経済安全保障の観点を取り入れたガバナンス強化に努めていくことを発表している※9。

むろん多くの日本企業は、LINE のように大量のユーザーの通信を扱うわけではない。しかし、ではその線引きはどう行えばよいのか。経済安全保障の観点を踏まえたデータガバナンスをどの程度とるべきか、企業としての姿勢を確認し、その理由を外部

※8　個人情報保護委員会「個人情報の保護に関する法律に基づく行政上の対応について」https://www.ppc.go.jp/files/pdf/210423_houdou.pdf

※9　LINE「当社のガバナンス体制およびリスク管理体制の強化について」https://linecorp.com/ja/pr/news/ja/2021/3951

のステークホルダーに説明できる状態にしておく必要はある。

経済安全保障推進法で基幹インフラとされるような業種については、法令上の義務への対応として主務大臣への説明が求められる可能性が高く、対応は必須といえる。また、これら業種の再委託先についても、委託元となっている企業が行う説明の一環として、ガバナンスの状況に関して委託元への説明を求められる可能性もあるため、注意が必要である。

3　企業が取り組むべきこと①：自社のリスクを評価する

企業としての姿勢を確認し、その理由を外部のステークホルダーに説明できる状態をつくるため重要なことは、経済安全保障の観点を踏まえ、自社のデータガバナンスが対処すべきリスクを適切に評価することである。ここでは、①データマッピングの実施、②データのリスク評価項目の設定、③リスク評価の実施、という 3 ステップを踏む必要がある。③は①と②の照らし合わせであるから、本章では①と②を中心に解説する。

1）経済安全保障の観点を取り入れたデータマッピングの実施

リスク評価の出発点は、データマッピングである。データマッピングとは、自社において、どのようなデータが、どのような場所・相手方にどのように流通しているか、を明らかにする活動である。個人データの文脈では EU 一般データ保護規則（GDPR）対応といった企業実務においても一般的になりつつある。

しかし、日本の個人情報保護法や GDPR に対応するための個人データを対象としたデータマッピングは、本稿が目指す経済安全保障の観点をも取り入れたリスク評価の基礎とはなり得るかもしれないが、十分ではない。というのも、経済安全保障の観点を取り入れる場合、個人データに加えて非個人データを対象とする必要があり、これらの間ではリスク評価の観点が異なるからである。例えば半導体の製造方法や革新的な AI 技術といった技術情報の国外移転は経済安全保障上のリスクといい得るが、個人データを対象としたリスク評価では導出されない。

リスク評価の観点が異なるため、個人データと非個人データでは、データの流れにおいてどの調査項目に着目してデータマッピングを実施するかが異なる。個人情報保護であれば、例えば個人データの取り扱いの目的や法的根拠、第三者提供の有無、機微情報の有無、越境移転の有無、移転先国、越境移転の根拠といった項目が重視されるが、経済安全保障の観点を踏まえると、個人データが要人等を含むかどうか、データの移転件数はどの程度か、移転先国にガバメントアクセスやデータローカライゼーションのリスクはあるかどうか、データの内容に軍事転用可能な技術はあるかどうか、といった要素が必要になる。

データマッピングは、上記の内容を調査するために調査票を作成して各部署の責任者に配布し、特にリスクの高い部署に対しては対面で聴取を行うといった形式で実施する。この調査票には上記のデータの流れに関する調査項目を適切に盛り込んでおく必要がある。

また、調査票の配布先は、個人データでは、各部署に個人情報保護の責任者が任じられることが多いため、これを配布先とすることが一般的である。安全保障の観点を含む場合には、配布先を誰にするか、個人情報保護の責任者から変更すべきかどうか、といったことも考えていく必要がある。

図表 2　経済安全保障を加えた自社のリスク評価手順

	個人情報保護	個人情報保護＋経済安全保障
経済安全保障の観点を取り入れたデータマッピングの実施	**【調査対象】** ● 個人データ **【調査項目】** ● 取り扱いの目的や法的根拠 ● 第三者提供の有無 ● 越境移転の有無・移転先国等	**【調査対象】** ● 個人／非個人データ **【調査項目】**（左記に加え） ● データの件数 ● 技術情報を含むかどうか等
リスク評価項目の設定	● 本人のプライバシーを保護する観点からリスクを評価	（左記に加え） ● データが経済安全保障に与える影響、例えば選挙介入に利用される可能性や軍事転用可能な技術開発に利用される可能性を考慮してリスクを評価
リスク評価の実施	● データマッピングの結果について、リスク評価項目に基づく評価を実施	● 同左

出所）NRI 作成

また、近年ではデジタルトランスフォーメーション（DX）の実践に伴って、現場の部署を中心に独自にアプリ等のシステムを開発し、その過程で外部のクラウドサービスを利用したり、それらを組み合わせたりするといったことが少なくない。結果として本社機構が把握していないシステムが増えている例もあるため、DX に伴ってユーザーに近い場所でシステム開発を行っている実態がある場合、その実態把握のためのデータマッピングは特に重要である。

2）リスク評価項目の設定

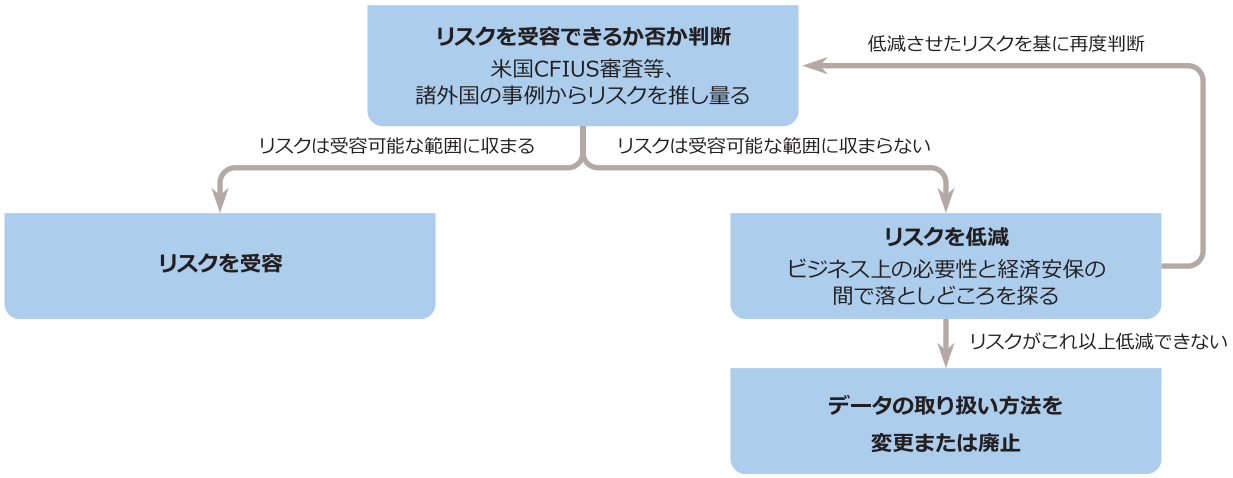
リスク評価項目の設定でまず行うべきは、経済安全保障上の問題とされた過去の事例を分析することである。先に挙げた LINE 問題はその典型であるが、海外に目を向ければ、米国における対米外国投資委員会（CFIUS）が行う、外国企業による買収の審査が参考になる。例えば中国金融大手アントファイナンシャルによる米国の国際送金大手 MoneyGram 社買収が阻止された事案は、同社が金融情報という米国人の機微な個人情報を大量に扱うため安全保障への影響が問題視された。また、米国でホテル運営を支援するクラウドサービスを中国企業である同業他社が買収しようとした際、米国政府職員の個人データを大量に扱っているという理由で、安全保障への影響が懸念され、米政府から阻止される事案があった。

ケーススタディーから、経済安全保障リスクの評価項目として、データ移転先におけるガバメントアクセスの存在、大量の機微データ、政府関連の個人データ、などを抽出することが可能である。ただし、こうした過去事例の分析を企業が個々に実施することは限界があるため、既に企業内でケースの蓄積があるのでなければ、専門性を持った外部のコンサルタントや法律事務所等を活用することが効率的と考えられる。

3）リスク評価の実施

最後に、１）と２）を組み合わせて、自社のデータガバナンス上問題となり得るリスクを抽出する。

図表３　経済安全保障リスクへの対処手順



出所）NRI 作成

抽出の過程ではリスクを対応策と併せて、つまり次に述べる４章の過程と併せて議論しがちであるが、ここではリスクを網羅的に抽出することを心掛け、対応策とは切り離して議論すべきである。

4　企業が取り組むべきこと②：リスクへの対処

リスク特定後の基本的な方針として、特定したリスクが受容できる範囲であれば受容する、受容できないリスクは低減して受容可能とする、それも難しければガバナンス上問題のあるリスクとして、データの取り扱い方法を変更または廃止する、という対応を図る必要がある。

1）リスクを受容できるか否かの判断

リスク評価の結果浮かび上がったリスクについて、企業として受容できるか否かの判断を行うこととなる。出発点として法令上の問題が分析されるべきであるが、法令違反が許容されることはないため（ただし法令解釈自体が議論対象となる可能性はある）、ここではレピュテーションリスク等の法令違反以外のリスクが存在するかどうか、存在するとすれば許容できるか否かを判断していく必要がある。

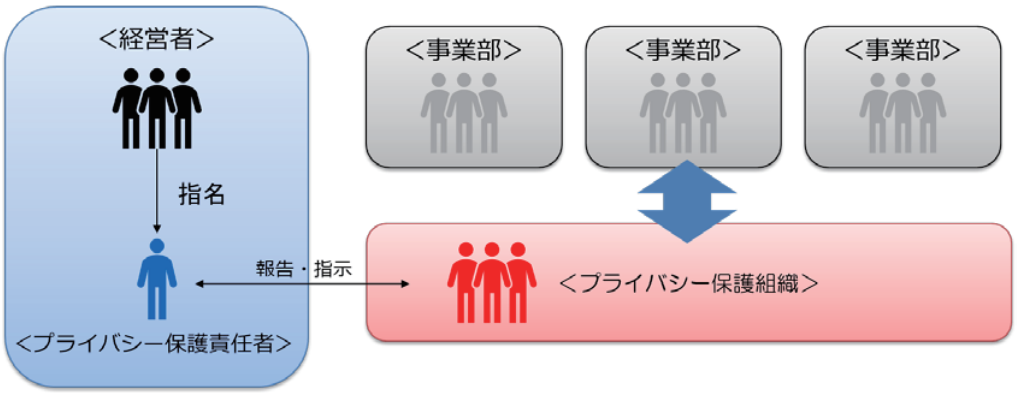
特に難しいのは、経済安全保障という概念自体があいまいなため、レピュテーションリスクが生じるかどうかを事前に判断することが困難な点である。ここでは、そのとき合理的に予期できる範囲で検討を行うしかない。例えば、３章で挙げたように外国の事例を研究し、類似のリスクに対して外国政府がどの程度問題視していたか、どのような反応をとったか、といった分析を通じて、リスクを受容する場合、自社に与える影響を推し量る方法が考えられる。

また、例えば経済安全保障を担う政府当局（経済安全保障推進法の成立により、今後基幹インフラの審査に関して各官庁の担当部署が指定される予定）との関係構築ができていれば、特に判断に迷う部分は事前に相談を行って反応をうかがい、経営層のリスク評価・判断を支援するといった選択肢も考えられる。

2）受容できないリスクの低減

１）の評価の結果受容できないと判断されたリスクは、どのように低減が可能か議論していく必要がある。LINE 問題では、経済合理性からは外国のサー

図表４　プライバシー保護組織の役割



出所）総務省・経済産業省「DX 時代における企業のプライバシーガバナンスガイドブック ver1.2」24 ページ

バーを用いるべきであるが、経済安全保障を踏まえると国内にデータをとどめるべきであると両者の判断がトレードオフとされ、LINE は経済安全保障への配慮からデータを完全に国内で保管することとした。両者の妥協点として、経済安全保障上のリスクを生じるデータのみを国内にとどめ、一般的なデータは外国のクラウドに保存する、といった可能性に関して議論することはあり得る。

この例では、サーバーを分割した際のシステム的な実現可能性や、サービスのUI/UXに与える影響（遅延の度合い等）など、ビジネス、システム面での影響をも考慮する必要があり、事業部やシステムの所管部署とも連携を図る必要がある。リスク低減についても、技術的・組織的にさまざまな手法が考えられるため、対処方法に豊富な知見を有する外部専門家の知見を活用することも選択肢の一つである。

以上を経ても受容できないリスクが残存する場合には、データの取り扱い方法を変更または廃止することとなる。

3） リスク評価の実施機関

実務的には、社内のどのような組織で上記１）や２）の判断を行うかも重要である。最終的には経営層の判断となるが、誰がその意思決定を補佐するか、その事務局を決めておく必要がある。

本号の別稿で指摘した通り[※10]、ある程度プライバシー保護への対応が進んだ企業では、「プライバシー保護組織」という組織がプライバシーガバナンスの中核を担うことが想定される。同組織は各事業部と連携し、経営層に含まれるプライバシー保護責任者に対して報告・指示を行う。また、外部の市民社会や専門家（弁護士やコンサルタント等）とも積極的に関係性を構築し、進展の速い技術トレンドやプライバシー意識等を絶えずアップデートする。

プライバシー保護組織にデータに関わる経済安全保障上の観点を盛り込むためには、（既に設置されている場合）経済安全保障の担当部署と連携を図る、プライバシー保護責任者と経済安全保障の責任者（いずれも経営層のレベル）との連携を図る、経済安全保障を担う当局（例えば 14 分野に該当する

※10　南島安平「プライバシーガバナンス構築に向けた具体的な取り組みの進め方−パーソナルデータの持続的な活用に向けて−」を参照

場合には主務官庁の担当部署）との関係を構築するといった対処があり得る。また、メーカー等においては安全保障貿易管理を担う専門家に参画を仰ぐことも、諸外国がターゲットとする情報や日本政府当局との関係性など、有益な知見を得られる可能性がある。

以上の実践は今後の実務の発展によると思われるが、法令の要求に単に対処することを目的とせず、積極的にそれを超えた要素についても経営判断を促していくことを目指す点において、プライバシー保護とデータの経済安全保障への対応には共通点が見られる。データの経済安全保障への考え方が整理されていない現状では、出発点としてプライバシー保護組織をベースとすることが適切と考えられる。

なお、プライバシー保護組織の形成に至っていない企業については、まずはその段階まで早期に達する必要がある。データガバナンスについては、プライバシー保護が最も取り組みが進んでいる分野であり、それをベースとして経済安全保障に取り組むことが有効と考える。

5　おわりに

以上、簡単ではあるが、昨今展開が進む経済安全保障とデータガバナンスの関係性について説明してきた。この分野は状況の進展が速く、ロシアによるウクライナ侵攻など国際情勢の変化に応じて、関連する国家に所在する企業へのデータ移転や委託等のリスクの度合いも変化するため、常にアップデートを心掛ける必要がある。

また、特に欧米ではデータガバナンスを踏まえた経済安全保障の議論が進んでおり、本稿でもその一端を紹介している。このような外国の知見を踏まえた判断をすることが有益であるとともに、対外的な説明としても納得感を得られやすい。

多くの日本企業では、そもそもデータガバナンスに経済安全保障の観点を取り入れたリスク評価自体が実施されていないと推測されるため、プライバシー保護におけるプラクティスを応用しつつ、まずはリスク評価を行い、経済判断に資する情報を提供していく必要があると考える。本稿がその一助となれば幸いである。

●…… 筆者
渡辺　翔太（わたなべ　しょうた）
株式会社 野村総合研究所
CX コンサルティング部
チーフコンサルタント
専門は、政府機関への国際的なデータ関連政策や通商政策の立案支援、企業のデータ関連コンプライアンス対応支援
E-mail: s4-watanabe@nri.co.jp

NRI パブリックマネジメントレビュー
Public Management Review
Vol.228
July 2022

当レポートに掲載されているあらゆる内容の無断転載・複製を禁じます。すべての内容は日本の著作権法および国際条約により保護されています。
Copyright© 2021 Nomura Research Institute, Ltd. All rights reserved. No reproduction or republication without written permission.