Back Number

本論文は

世界経済評論 2024 年 3/4 月号

(2024 年 3 月発行)

掲載の記事です

世界経済評論 定期購読のご案内

年間購読料
1,320円×6冊=7,920円▶6,600円税込
17% 送料無料 OFF

富士山マガジンサービス限定特典
※通巻682号以降
定期購読期間中 デジタル版バックナンバー読み放題!!

世界経済評論　定期購読

[24時間・年中無休]
0120-223-223

お支払い方法
Webでお申込みの場合はクレジットカード・銀行振込・コンビニ払いからお選びいただけます。
お電話でお申込みの場合は銀行振込・コンビニ払いのみとなります。

Fujisan.co.jp
雑誌のオンライン書店

経済安全保障，データガバナンスと日本企業の対応[1)]

野村総合研究所 ICT・コンテンツ産業コンサルティング部エキスパート研究員 渡辺 翔太

わたなべ　しょうた　専門は国際的なデータ関連政策や通商政策の立案。日本政府の国際交渉や外国制度調査などを支援しているほか，経済産業省や外務省などの有識者委員を務める。

野村総合研究所 社会システムコンサルティング部コンサルタント 松本 玲央奈

まつもと　れおな　専門は安全保障貿易管理関連政策の伴走支援，グローバルバリューチェーンを踏まえた外国企業誘致及び在日外資系企業の対日直接投資促進政策の立案，防災政策の立案，人材政策分野における実行支援など。

本稿は，経済安全保障とデータガバナンスの関係を示すとともに，民間企業の対応の現状と今後の方向性を検討するものである。

経済安保推進法を中心とする日本の経済安保政策は，ハードウェアに関する施策が大半を占めている。しかし，LINE 事件等から示唆されるように，民間企業が保有するデータの保護も経済安保における重要テーマである。

各国において政府による民間データを活用する動きが加速する中，対抗措置として民間保有データに対する規制も強化される方向性にあり，日本においても個人情報保護法の改正や経済安全保障推進法を通じて規制強化が進んでいる。

筆者の調査では，企業の経済安保を踏まえたデータガバナンスの状況は，取り組みが一定程度進んでいるものの，本格的な対応は今後の課題であることを示している。

企業のデータガバナンス体制構築には，自社データのリスク評価，およびリスクへの対処を実施し，社外に取り組みを説明できる状態を作る必要がある。また，過剰な政府介入を防ぐためにも，最低限の法令遵守のみならず，企業自身が積極的に政府に対して提言を行うとともに，自らの経営判断に沿って取り組みを推進すべきである。

はじめに

本稿は，経済安全保障（経済安保）―それ自体，多義的な概念ではあるが―とデータガバナンスの関係を示すとともに，民間企業の対応の現状と，その実現に向けた方策を検討するものである。

本稿の背景となる問題意識として，経済安保とデータガバナンスの関係性が，サプライチェーンの保護等と比べ，十分理解されていないのではないかとの危惧がある。そこで，本稿はまず両者が密接な関係を有していることを示す。

次いで，民間企業においても経済安保に関する取り組みを進める上ではデータガバナンスに関する対応を併せて進めるべきであることと，その方法を示すこととする。

Ⅰ　日本企業のデータガバナンスと経済安保上の関係

経済安保が政策上の重要テーマになって久しい。新型コロナウイルスのパンデミックやロシアのウクライナ侵攻に伴い顕在化した半導体やエネルギーをはじめとしたサプライチェーンの脆弱性，米中の地政学的な対立及び技術覇権争い等を背景として，各国政府は経済安全保障の確保に向けた取り組みを強化している。

経済安保は広範な概念であるが，我が国においては「国家安全保障戦略」(2022 年 12 月閣議決定）で「我が国の平和と安全や経済的な繁栄等の国益を経済上の措置を講じ確保すること」と定義されている。また，2023 年 3 月，「経済施策を一体的に講ずることによる安全保障の確保の推進に関する法律（経済安保推進法)」を巡る小林大臣（当時）による国会答弁では「国益を経済的手段や経済面から確保していくこと」，「国家国民の安全を経済面から確保すること」と言及されているにとどまり，その内容は非常に広い範囲を指している。

米国はトランプ政権以降，半導体やその製造装置等，重要技術の国外流出を防ぐための法的基盤を整備し，具体的な対中条項として中国製半導体の政府調達の禁止等を盛り込んだ「2023 年度国防授権法（NDAA2023)」の成立や対外投資の規制等で中国への技術移転を抑止するなど，攻めの施策を推進している。他方で，2023 年に入ると，EU のフォンデアライエン欧州委員長の演説において安全保障上リスクが高い国際取引の制限にフォーカスするデリスキングが，経済安保の基本となる考え方として登場し[2)]，2023 年 5 月の G7 広島サミットの首脳宣言にも採用された[3)]。

他方で，我が国においては，投資審査や輸出管理の強化，研究インテグリティの確保，サプライチェーンの強靭化等を通じて経済安全保障上の取り組みを推進してきたところ，2022 年 5 月には先述の「経済安全保障推進法」が成立した。同法では，法制上の手当てが必要な喫緊の課題に対応するため，「①重要物資の安定的な供給の確保」，「②基幹インフラ役務の安定的な提供の確保」，「③先端的な重要技術の開発支援」，「④特許出願の非公開」という 4 つの制度が構築された。

いずれも，外国との取引を直接制限する米国の施策に比べ，重要な技術情報の保護やインフラの整備・防衛といった日本の戦略的自律性の向上を図る守りの政策である。同法に加え，外為法に基づく「みなし輸出」管理の明確化を通じた輸出管理の厳格化等を通じて我が国の経済安全保障体制の強化が進められているところである。

そして，以上概観した経済安保推進法を中心とする日本の経済安保政策は，現状では，安全保障貿易管理の枠組みに係る特定技術及びそれらを含むモノ・サービス等に関連するものが議論の大半を占めているように思われる。たとえば，経済産業省における半導体・デジタル産業戦略検討会議の議論は，半導体のほか，蓄電池やコンピュータ資源といったハードウェアに関連する施策がほとんどを占めている[4)]。

しかし，データにも経済安保の観点から保護すべきものがある。そしてその範囲は従来，安全保障貿易管理の対象となってきたデータに限られない。日本でこれが顕在化したのが 2021 年 6 月に起きた「LINE 事件」である。

LINE は日本の国民の大半が利用するメッ

セージングサービスであるが，その画像などを保管するサーバーが一部韓国に設置されていたこと，つまり韓国へのユーザーデータの国外への移転（越境移転）があったにもかかわらず日本政府には国内で保管されていると説明していたことや，政府機関による強制力を持ったデータへのアクセス（ガバメントアクセス）の懸念がある中国への再委託[5]，再委託先から日本のデータへアクセス可能となっていたことが問題視された。同事件について，親会社のZホールディングスに有識者委員会が設置され，委員会は「グループ全体で経済安全保障に関するガバナンス体制を構築すること」を求めた[6]。

ガバメントアクセスは，データの越境移転に際して常に留意すべきリスクの1つである。日本人のデータが外国に移転後，選挙介入や大規模なサイバー攻撃等に利用される可能性があるほか，技術情報が外国政府にアクセスされ，それが同じ外国を拠点とするライバル企業に渡り，軍事転用されて外国の軍事力強化に活用されるリスクもある。

Ⅱ　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

以上のLINE事件を敷衍し，なぜ民間企業が保有するデータが，経済安保上の課題となるのかを述べておきたい。

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[7]。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ングに利用したとされる。

また，企業が持つ技術情報を獲得するため，外国政府が関連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が広範になり，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。

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，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。

以前に比べ，民間部門が管理するデータが莫大に増加し，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

前項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。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，前項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，ソフトウェアやインターネット関連の業種が審査対象に追加された[8)]。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，経済安全保障推進法である。同法は冒頭述べた「モノに関する安全保障」に重点があるように見え，実際，実務的な検討もハードウェアが中心となっている。しかし，前項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り，将来的には企業に一定水準のデータガバナンスを求める枠組みとしても利用し得る点に着目すべきである。

まず，4 本柱の 1 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 2022 年 12 月に指定され，その中にクラウドサービスが含まれている[9)]。報道では，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[10)]。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（仏では Orange，独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[11)]。

4 本柱の 2 つ目「基幹インフラの安全性確

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	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

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（カテゴリは筆者が追加）。これに基づき，2023 年 11 月には特定社会基盤事業者として，具体的な会社が主務大臣から指定されている[12)]。

当該分野の企業は重要なシステムを導入する際，サイバー攻撃等の基幹インフラ設備に対する特定妨害行為に対して対抗できるよう，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づけられる。LINE 事件をふまえると，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。

Ⅲ　企業が取り組むべきこと①：リスク評価

以上の動向を踏まえ，経済安保の観点を踏まえたデータガバナンスの体制を，企業としていかに構築すべきか。実現すべきは，企業としてどのようなリスクに対してどのような対処方針をとるのか，その理由は何か，を外部のステークホルダーに説明できる状態を作ることである。

その第一歩として，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べきである。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，本節では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[13)]

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なり得るが，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，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，データの内容に軍事転用可能な技術はあるか，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，といったことも考えていく必要がある。

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 にともな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 事件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 Money Gram 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。

3．リスク評価の実施

最後に，上記の 1 項と 2 項を組み合わせて，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。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Ⅳ節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。

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，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

Ⅳ　企業として取り組むべきこと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，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事前に判断することが困難な点である。ここでは，その時合理的に予期できる範囲で検討を行うしかない。例えば，先に挙げたCFIUS審査等の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（経済安保推進法が定める，基幹インフラの審査に関する各官庁の担当部署等）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

前項の評価の結果，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検討する必要がある。LINE の事案では，経済合理性からは外国のサー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留めるべきと両者の判断がトレードオフとされ，事件を受けた対応では，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だろう。この場合，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・組織的に様々な手法が考えられ得るため，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１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。

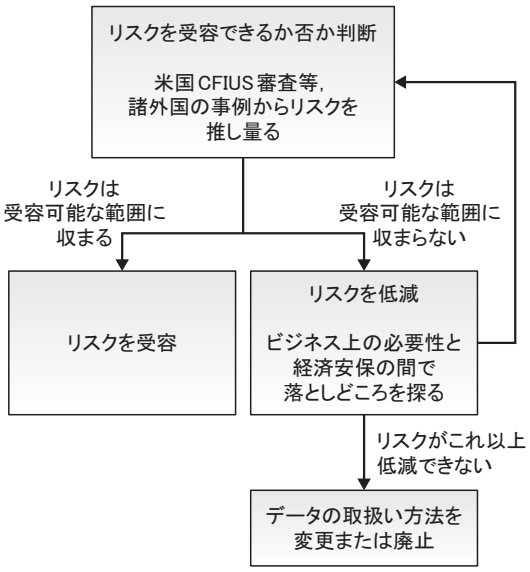
3．リスク評価の実施機関

実務的には，社内のどのような組織で上記１項や２項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。

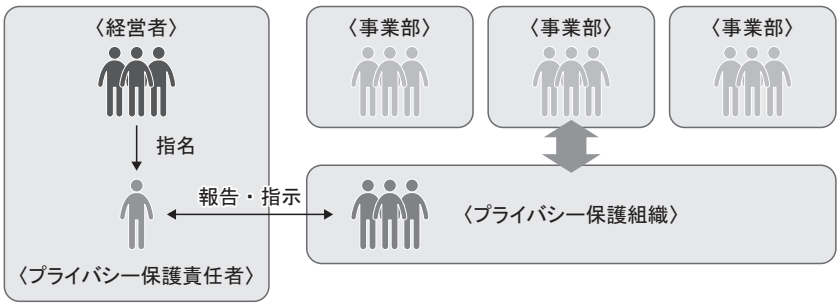
ある程度プライバシー保護への対応が進んだ企業では，「プライバシー保護組織」という組織がプライバシーガバナンスの中核を担うことが想定される[14)]。同組織は各事業部と連携し，経営層に含まれるプライバシー保護責任者に対して報告・指示を行う。また，外部の市民社会や専門家（弁護士やコンサルタント等）とも積極的に関係性を構築し，進展の早い技術トレンドやプライバシー意識等を絶えずアップデートする。

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）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

図表３　経済安全保障リスクへの対処手順



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 ver 1.2」，24 頁

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。

Ⅴ　企業のガバナンス状況

ここでは，筆者が 2023 年に実施した企業向けアンケート調査の結果から，Ⅲ節とⅣ節で述べた企業の取り組みがどの程度実行に移されているかを概観したい。

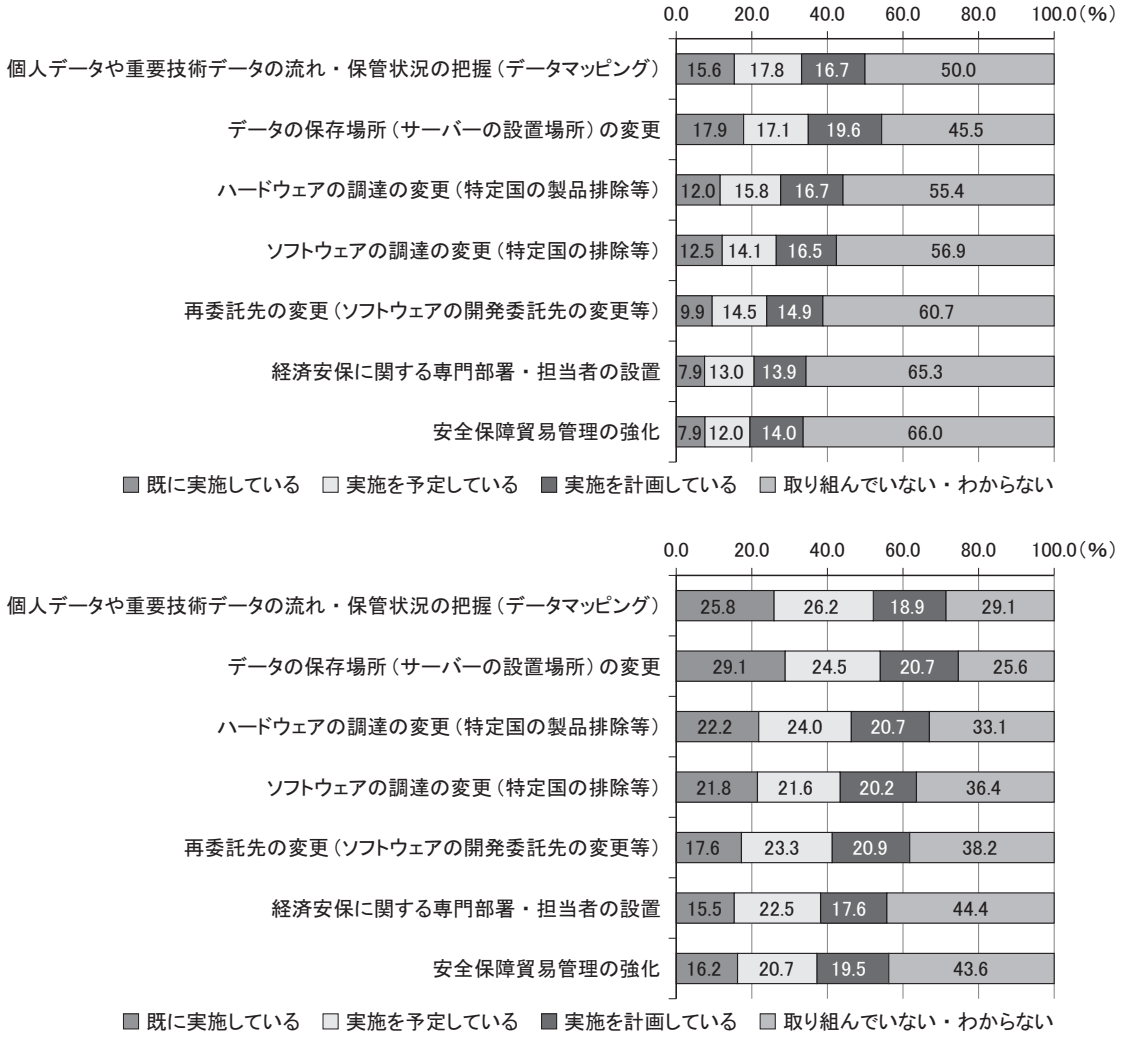
データガバナンスの観点から取り得る措置について，実際のどの程度の措置が取られているかを調査した結果を示す（図表５）。施策として多いのは，サーバーの設置場所等のデータの保管場所の変更であり，これは全体の 50％以上が何等かの対応を予定している，または対応済みである。次いで，データマッピングも約半数が実施しているまたは予定がある。一方，「再委託先の変更」や「経済安保に関する専門部署・担当者の設置」は低い。クラウド等を利用していれば，データの保存場所の変更は容易であるが，再委託先の変更や組織的な対応は長い時間・費用がかかるため検討が進んでいないと推測される。

大規模な企業（ここでは従業員数 1000 名以上を便宜的に取り上げている）については，全般的にそれぞれの措置を取っている割合が高まる。全体に比べ，大企業のほうが，全般的に実施割合が高く，データの保存場所については 75％が何らかの取り組みをしようとしている。

以上の現状を見ると，取り組みは徐々に広まりつつあるものの，調達の変更や再委託先の変更，組織の立ち上げ等については，十分な取り組みが進んでおらず，また大企業と中小企業でも取り組みに差がみられる点が示されたといえる。今後は，以上のような取り組みを更に進めていく必要があるといえる。

政策サイドにおいても，経済安全保障の観点を踏まえたデータガバナンスに関するガイドライン等の策定や，中小企業の対応支援といった企業への支援策を講じるとともに，企業の対応

図表５　経済安保に関連した取り組みの実施状況（上：全体（N＝2550），下：（従業員数 1000 名以上（N＝550））



（出所）野村総合研究所「情報通信サービスに関するアンケート調査」

に関する継続的なモニタリングが求められる。

おわりに

日本企業のデータガバナンスの基本姿勢として，経済安保の考慮は不可避となったといわざるを得ない。LINE 事件の有識者委員会報告書においても，経済安保観点の欠落が問題点として指摘されるとおりである。

問題はその程度にあり，信頼とデータの自由流通が相互補完的であれば，企業として目指すべきは事業の円滑な実施に向けた顧客の信頼獲得だろう。経済安保の観点をどの程度自社の事業に取り入れ，どの程度事業上の非効率を受け入れるかは各社の経営判断である。

この点，法令を遵守することで足りるという意見も多いと思うが，２つの点で認識を改めるべきである。第１に，経済安保においては，法

令の規定自体が曖昧であり，政府も手探りで進んでいる。時には政府による過剰介入の可能性もあるため，企業自身が，自らの信じるバランス感覚に沿って政府に対して提言していく必要がある。また，経済安保は1国の政策だけで決まるものではなく，グローバルな政策形成の場に対しても，企業から積極的に提言する必要がある。たとえば，2023年4月のG7デジタル・技術大臣会合宣言の中では，DFFT実現に向け企業にも参加余地のある「相互運用のための制度的取り決め（IAP）」の立ち上げが決定され，これが2023年12月の同大臣会合宣言でさらに具体化された[15)]。グローバルな提言に向けた体制を企業側が整える必要があるが，個別企業で対応が困難であれば，業界団体やビジネス団体を通じてインプットの経路を確保すべきである。

第2に，法令は最低限度の要求事項に過ぎない。LINE事件も，越境移転に関する法令上の義務違反があったわけではないが，世間からの批判を招いた。先に述べた通り，リスクを特定し，それをどの程度受容するか，それはなぜかを対外的に説明できる状態を経営陣が作る必要がある。これができるかどうかで，株価の下落や事業上の支障が生じた際に経営陣の説明責任をどの程度果たせるかが変わり，ダメージコントロールにつながる。

冷戦後，企業は地政学的な影響と距離を取って事業に集中することができた。それが国境を超えたバリューチェーンの構築など，グローバルな資源の最適活用を促すことで，世界経済は成長を続けてきた。しかし，こうした経済成長は新興国の経済力・軍事力を拡大させ，グローバルなパワーバランスの変化に伴って再び安全保障と経済の再接近を生じ，これが企業経営にも影響を与え始めている。このため，冷戦時代のココム規制等を念頭に置き，いわば冷戦に戻ったという意識で経済安保を推進することがイメージされることもある。

しかし，この認識は改められる必要がある。冷戦時代との大きな違いは，社会のデジタル化である。今や世界大に拡大したインターネットや，半導体やクラウド等コンピュータ資源の圧倒的な進化，それらを組み合わせたデータ活用という，当時とは大きく異なる環境変化が生じている。そして，このデータを活用した経済の進歩は非常に速い。政府関係者，企業経営者はこのことを念頭におき，従来とは全く異なる対応が必要になることを前提として，経済安保に取り組んでいく必要がある。

[注]

1）本稿は，渡辺翔太「データ流通と経済安全保障」『IT ナビゲータ 2024 年版』（東洋経済新報社，2023 年）および同「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」『NRI パブリックマネジメントレビュー』（Vol.228，2022 年 6 月）を基に，執筆時点までの情勢の変化などを踏まえて加筆修正したものである。

2）“Von der Leyen calls for de-risking EU-China relations in speech to MERICS”, https://merics.org/de/pressemitteilung/von-der-leyen-calls-de-risking-eu-china-relations-speech-merics

3）「G7 広島首脳コミュニケ（2023 年 5 月 20 日）」（外務省仮訳），パラグラフ 51

4）経済産業省「半導体・デジタル産業戦略（改定案）」（2023 年 5 月）（https://www.meti.go.jp/policy/mono_info_service/joho/conference/semicon_digital/0009/4hontai.pdf）

5）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」（中曾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）

6）Z ホールディングス「グローバルなデータガバナンスに関する特別委員会　最終報告書」（https://www.z-holdings.co.jp/notice/2021/10/da483e6a533c560435dbe6bcbf17ead2.pdf）

7）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）

8）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）

9）内閣府「特定重要物資の指定について」（https://www.cao.go.jp/keizai_anzen_hosho/supply_chain.html）
10）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））
11）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 および 39 頁を参照
12）内閣府「特定社会基盤事業者として指定した者の公表」（https://www.cao.go.jp/keizai_anzen_hosho/infra.html）
13）同様にデータマッピングの重要性を述べるものとして，山郷琢也・三代川英嗣「経済安全保障の視点を取り入れたデータガバナンスの実務：各国において高まるガバメントアクセスの懸念を背景として」『NBL』（1227），45-47 頁
14）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―」『NRI パブリックマネジメントレビュー』（Vol. 228, 2022 年 6 月）を参照。
15）G7 デジタル・技術閣僚声明附属書 1「DFFT 具体化のための国際枠組み（Institutional Arrangement for Partnership: IAP）の設立及び G7 の期待に関するコンセプトペーパー」（https://www.digital.go.jp/assets/contents/node/information/field_ref_resources/d5208f71-317d-425b-9677-c64a06000e3c/80bfa1ad/20231201_news-g7_result_02.pdf）

季刊「国際貿易と投資」掲載論文のご紹介

一般財団法人 国際貿易投資研究所が発行している研究季刊誌、
季刊「国際貿易と投資」に掲載している全論文をダウンロードすることができます。
ご一読をお勧めいたします。（https://iti.or.jp/）

134 号　特集「東アジアにおける米中対立」
米中対立の中で米国依存度を高める韓国経済（百本和弘）／「ASEAN 企業の対ベトナム投資、三つの視点」―加速する動きから見えるもの―（牛山隆一）／予算を巡る米議会の対立から透けて見える 24 年大統領選～見え隠れする共和党保守強硬派を介したトランプ前大統領の影～（高橋俊樹）／アンワル連立政権発足１年のレビューと課題（小野沢 純）

133 号　特集「脱中国の動きがより鮮明に」
米国の 2023 年上半期の対中輸入の急減は何を意味するのか～ターニングポイントの兆しが見え始めた米国の対中ビジネスモデル～（高橋俊樹）／世界貿易における脱中国の動き～中国の経済不振とデカップリング～（大木博巳）／近年の日本の貿易構造変化―円安と企業内貿易が与えた影響―（永田雅啓）／ロシアのウクライナ侵攻はドイツに何をもたらしたのか～対ロシア貿易の激変とエネルギー危機（田中信世）／コロナ禍から復興する南欧３か国（新井俊三）

132 号　特集「コロナ後のグローバルサウスの動き」
インド太平洋構想（FOIP）と日印協力～覇権主義に抗しアフリカ開発で連携～（山崎恭平）／外資を呼び込み、ベトナム中小企業の持続可能なバリューチェーン構築に向けて（Nguyen Manh Quan・Nguyen Trong Hieu）／タイ経済は外国人観光客の支出と個人消費の拡大で成長が加速～タイの通商・外国投資政策～（Jirada Prasartpornsirichoke）／急速に変化する韓国の貿易と投資～低い対日貿易での FTA の関税削減効果～（高橋俊樹）／日本の輸出競争力の凋落～世界輸出に占める日本のシェアは 1960 年の水準を下回る～（大木博巳）

131 号　特集「混迷深める世界経済とグローバリゼーションの行方」
ブラジル左派政権、ルーラ流プラグマティズムの復活？―社会復興とグローバル・サウスの再挑戦（堀坂浩太郎）／ウクライナ戦争、米中「新冷戦」、高止まりするインフレ、2024 年大統領選～「どうするバイデン」～（木村 誠）／第 20 回党大会後の中国（今村弘子）／ソ連邦崩壊後の世界貿易・直接投資とグローバリゼーションの行方～覚醒する米国の同盟国とグローバル・サウス～（大木博巳）／膠着する CPTPP をいかにして進展させるか～激変する貿易構造に対して FTA 活用や輸出主導による通商戦略は有効か～（高橋俊樹）

130 号　特集「ドイツの経済敗戦と欧州のエネルギー問題」
ドイツの経済敗戦～欧州を脆弱化させた経済モデルの破綻～（大木博巳）／欧州のグリーンディールとエネルギー問題（川野祐司）／韓国企業のベトナム進出ブームとベトナム・リスク顕在化の兆し（百本和弘）／中国は CPTPP の代わりに RCEP によるサプライチェーン戦略を打ち出すか～中国の RCEP 活用による関税削減額は日本・韓国よりも大きい～（高橋俊樹）

一般財団法人 国際貿易投資研究所（ITI）
〒104-0045 東京都中央区築地１丁目４番５号 第 37 興和ビル３階
TEL：03（5148）2601 / FAX：03（5148）2677
E-Mail：jimukyoku@iti.or.jp　URL：https://iti.or.jp/