経済安全保障推進法改正に関する
提言骨子
（データセキュリティ）

2026 年 1 月 16 日
経済安全保障法制に関する有識者会議

目次

1　基本的な考え方

（1）背景

（ア）デジタル化の進展や生成ＡＩ等の技術革新に伴い、個人や企業のあらゆる情報がデジタル化され活用されている中、厳しさを増す我が国の安全保障環境に鑑み、安全保障上重要なデータ等のセキュリティを確保する重要性が高まっている。

（イ）近年、欧米を始めとする諸外国においても、機微な個人データや、大量のデータの処理・保存を行うデータセンター及びクラウドサービスを防護するための制度の検討が進められている。

（2）措置の必要性

（ア）安全保障は国家の責任であり、民間保有データの中には外部に流出した場合に国家及び国民の安全を害するおそれのあるデータが含まれることから、民間保有データの法制度による保護の在り方についても、国が責任を持って対処することが必要である。外部から行われる行為によってデータが流出する等により、国家及び国民の安全が害されることを防ぐため、安全保障上重要なデータや、データセンター及びクラウド上の大量のデータを防護するための措置を検討することが必要である。

（イ）他方、我が国は、自由なデータ流通を促進するＤＦＦＴ（Data Free Flow with Trust）の提唱国であり、データ利活用を推進していることから、当該検討においては、民間企業等によるデータ利活用や経済活動を必要以上に制限しないよう留意することが必要である。

（ウ）加えて、規律目的及び目的に照らした適切な手段を整理し、経済活動の実態に即し現場が対応可能な制度とすべきである。また、個人情報保護法等の既存法制や国際約束との整合性等を踏まえることが重要である。

2　措置の方向性

（1）安全保障上重要な民間保有データを防護するための措置

①　対象となり得るデータの考え方

（ア）外部に流出した場合に、国家及び国民の安全を害するおそれのあるデータが、安全保障上重要なデータと考えられる。このようなデータとして、政府機関が保有する重要なデータだけでなく、民間企業等が保有する技術情報や営業秘密、我が国の経済活動を支えるインフラに関するデータ、個人に関する機微なデータ等様々なものがあり得る。

（イ）これらのうち、政府機関が保有する重要なデータについては、特定秘密

保護法や重要経済安保情報保護活用法による措置、政府が調達する情報システムに関しては、ＩＳＭＡＰ（Information system Security Management and Assessment Program）やＩＴ調達申合せ等の措置がある。また、民間企業等が保有するデータのうち、機微な技術情報の外国に向けた提供等には外為法の規制が及び得るほか、営業秘密については不正競争防止法による措置がなされている。

（ウ）しかしながら、民間企業等が保有するデータのうち、個人に関する機微なデータや基幹インフラ役務の安定的な提供に必要なデータについては、外部からの影響力行使等の防止や基幹インフラ役務の安定的な提供の確保といった経済安全保障の観点からは個人情報保護法や不正競争防止法等の既存法制で十分な保護がなされていないおそれがある。このため、これらの安全保障上重要なデータについて必要な措置を検討する意義がある。

② 個人に関する機微なデータに係る措置

（ア）個人に関する機微なデータ（例えば、ゲノムデータ、医療情報、金融情報、生体認証情報、位置情報等）が外部に漏えいした場合、これらが国家の意思決定に影響を与え得る個人や我が国の経済安全保障に影響を与え得る技術や情報を有する個人等に対する外部からの影響力行使等に利用されるリスクがあり得る。

（イ）外部への情報漏えい等を生じさせる行為として、例えば、第三者へのデータ提供、データの処理・保存を行う情報システム等の契約、ゲノムデータの解析依頼等が考えられる。そのため、これらの行為に対応する措置を検討することが考えられる。

（ウ）措置の検討においては、既存法制等との整理が必要となる。この点、例えば個人情報保護法は、個人の権利利益の保護を目的としているため、経済安全保障の観点から十分な保護がなされていないおそれがある。このため、個人情報保護法やその他既存の個別の規律との整合性を踏まえた上で、経済安全保障の目的を横串的に実現する観点から必要な措置を検討することが重要である。

（エ）個人に関する機微なデータの保有者には、スタートアップ企業を含め広範かつ多様な事業者が想定される。データの利活用を阻害しないよう、事業者の実態把握、情報の内容及び性質並びに機微度に応じた対象範囲や閾値の設定等措置の実効性や事業者の負担を考慮し、施策の目的に応じた検討を行うことが必要である。

③　基幹インフラ役務の安定的な提供に必要なデータに係る措置

（ア）基幹インフラ役務の安定的な提供に必要なデータ（例えば、特定重要設備を稼働させるために必要なデータ）が外部からの改ざん・滅失等の行為を受けた場合、基幹インフラ役務の安定的な提供に支障が生じ、国家及び国民の安全を損なう事態が生ずるおそれがある。

（イ）これらのデータについては、既存の基幹インフラ制度における特定重要設備の事前審査を通じて、当該データの改ざん・滅失等のリスクを低減できるよう、基幹インフラ制度の運用改善の検討が必要である。その際、基幹インフラ事業者における設備のクラウド化の進展等も踏まえると、クラウド内のデータ保護の重要性にも留意が必要である。

（ウ）なお、サイバー対処能力強化法等による規律も踏まえ、経済安全保障施策全体として、基幹インフラ事業者の負担と措置の実効性のバランスにも留意しつつ、検討を進めることが必要である。

（２）データセンター及びクラウド上の大量のデータを防護するための措置等

（ア）データセンター及びクラウドサービスは、デジタル時代の社会・経済活動を支えるインフラであり、大量のデータの処理・保存先となっている。このため、我が国の外部から行われる行為からデータセンター及びクラウド上の大量のデータを防護するための措置の検討が必要である。

（イ）具体的には、サプライチェーンリスク対策等のデータセンター及びクラウド上で取り扱われる情報の漏えい・滅失を防ぐための措置や、データセンター・クラウドサービス提供事業者を通じた、日本国内のデータセンターの設置状況等の事業実態を把握するための措置が考えられる。

（ウ）規律の検討に当たっては、諸外国との関係や諸外国の制度も踏まえつつ、データセンター・クラウドサービス提供事業者の事業実態の把握、国際標準で求められる内容及びその取得状況等の既に行われているデータ防護に係る取組等の把握を行うとともに、施策の目的を明確化した上で当該目的に応じた規律を定めること等が必要である。