

データセキュリティ制度の検討について

- ✓ **国家安全保障戦略**（2022年12月16日閣議決定）では、「データ・情報保護について、機微なデータのより適切な管理や情報通信技術サービスの安全性・信頼性確保に向けた更なる対策を講ずる」こと等が指摘。
- ✓ **諸外国**においても、**機微な個人データや重要インフラを防護するための制度**の検討が進められている。
（諸外国の例）米国：米国人の機微個人データ及び政府関連データへの特定国アクセスの防止に関する大統領令 実施規則
情報通信技術・サービス（ICTS）サプライチェーン保護規則
欧州：改正ネットワーク及び情報システムに関する指令（NIS2指令）
豪州：重要インフラ安全保障法（SOCI法）
- ✓ **2025年11月以降、本有識者会議においてデータセキュリティについて議論**。安全保障の観点から、民間保有データの保護について、国による責任を持った対処の必要性等が指摘。
- ✓ **経済財政運営と改革の基本方針2026**（2026年7月21日閣議決定）においては、「安全保障上重要な個人機微データの防護に関する法案の早期提出を目指すとともに、データセンター・クラウドの安全性等を確保するために必要な措置を講ずる。」とされている。



- ✓ 経済安全保障の更なる推進に向けた提言（2026年1月30日）では、**（１）安全保障上重要な民間保有データ（基幹インフラ役務の安定的な提供に必要なデータ及び個人に関する機微なデータ）や（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**について検討を行うことが必要とされた。
- ✓ （１）のうち、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、制度の見直し・運用改善を行うこととしている。したがって、本会議では、（１）のうち**個人に関する機微なデータに関する措置**について具体的な検討を行うこととする。
- ✓ なお、（２）については、現在のデータセンター・クラウドサービス提供事業者の事業実態等を勘案し、まずは、**事業所管省庁（総務省・経産省）において、データセンター・クラウドサービスに係る認証制度の創設に向けて検討を行う**こととする。

経済安全保障の更なる推進に向けた提言（2026年1月）の概要

- 安全保障は国家の責任であり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べき。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を防護するための措置の検討をすることが必要。
- 個人に関する機微なデータ（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）は、外部によって戦略的に利用されるリスクが考えられ、外部に漏えいした場合、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。当該データは既存法制では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り、当該データの防護に必要な措置を検討する意義がある。
- 外部への情報漏えいを生じさせる行為として、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、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。
- 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が必要。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実行可能な制度とすべき。

これまでの有識者会議等における主な御指摘

- **制度の趣旨**
 - ✓ 民間保有データの保護は極めて重要。個人データを広範にサーチエンジンにかけて必要な者の情報を抽出・加工することは諸外国の諜報機関では一般的であり、情報の安易な国外移転や国外企業への委託などに関する管理方針の明確化が不可欠。個人情報保護とは違う観点で保護の設計が必要。
 - ✓ 個別法との整理が必要。重要なデータを保護する視点に加え活用の視点まで含めた制度設計が望ましい。
- **対象情報について**
 - ✓ 例示されている安全保障上重要なデータについて広く同意が得られるのではないかと。ゲノムデータや健康データを対象とすることは重要。他方、こうしたデータを活用する者が使いやすい形とすべき。
- **講ずべき措置について**
 - ✓ データの保護は行為規制とならざるを得ない。何の目的で、どのようなデータの取扱いが問題になるか整理が必要。
 - ✓ リスクが高いものを規律の対象とし、一律に規律するものではないという方向が重要。何からデータを守るのか、国家だけでなく、非国家主体からの情報窃取も意識する必要。
- **事業者負担、データ利活用等への配慮について**
 - ✓ 安全保障の目的と規制手段のバランスを検証しながら検討を進めるべき。財政的・制度的支援を検討する等、現場のインセンティブに留意することが必要。
 - ✓ 事業者負担を考え、情報の機微度に応じた閾値の設定を検討すべき。
 - ✓ 事業者の関心が高いため、事業者の声を聴きながら慎重に進めてほしい。

- 提言において、外部に漏えいした場合、**外部からの影響力行使等**に利用されるリスクがある**個人に関する機微なデータ**として例示されたゲノムデータ、医療情報、金融情報、生体認証情報、位置情報等のうち、**医療情報と金融情報**は、当該情報が外部からの影響力行使等に用いられる事案が発生している。なお、重要経済安保情報保護活用法等における適性評価（重要経済安保情報の取扱いの業務を行った場合にこれを漏らすおそれがないことについての評価）の調査項目の中にも、精神疾患や信用状態が挙げられており、これらの情報は、適性評価に当たっての総合的な考慮要素の一つとされている。

個人に関する機微なデータが利用された例

- **金融情報**が利用された例
 - ✓ **住宅ローン、クレジットカード債務等**で困窮する元米国CIA職員が、中国の情報機関員の接触を受け、報酬と引換えに中国に渡航予定だった**米国のCIA職員に関する情報、工作計画の詳細等の機密情報**を提供した。（2018年、米スパイ活動法違反）
- **医療情報等**が利用された例
 - ✓ **重病**で特別なケアを要する子を抱え、**住宅ローン等**でも困窮するイタリア海軍大佐が、ロシアのイタリア駐在武官の接触を受け、報酬と引換えに**NATO及びイタリアの機密文書**を提供した。（2021年、伊刑法等違反）

我が国における影響力行使等の例

- ✓ 工作機械関連会社元従業員が、在日ロシア連邦通商代表部員と共謀し、報酬と引換えに同社の**新商品のアイデア等営業秘密に該当する機密情報**を提供した。（2026年、不正競争防止法違反で検挙）
- ✓ 大手通信会社元職員が、在日ロシア連邦通商代表部員と共謀し、報酬と引換えに同社の**営業秘密に該当する第5世代移動通信システムに関する技術情報**を提供した。（2020年、不正競争防止法違反で有罪）

重要経済安保情報保護活用法の規定

○重要経済安保情報の保護及び活用に関する法律（令和6年法律第27号）

第十二条（略）

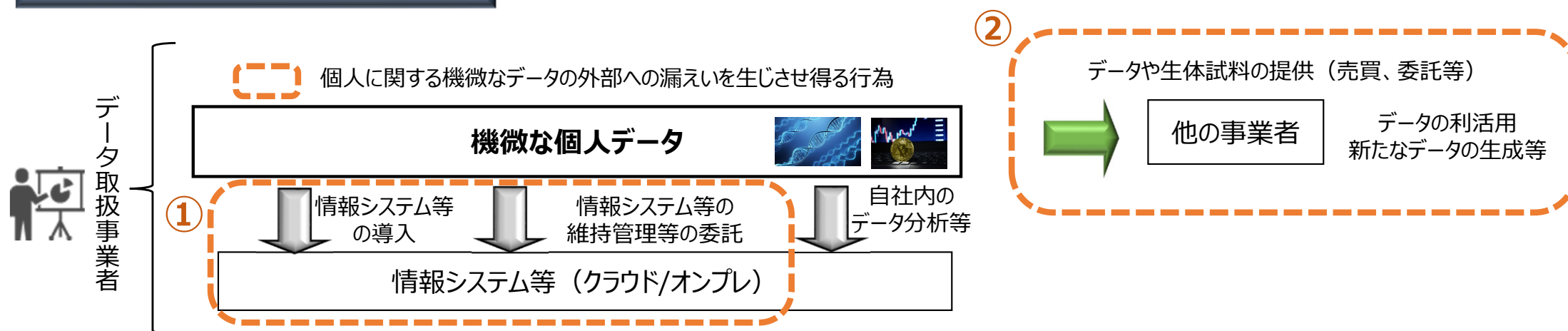
2 適性評価は、適性評価の対象となる者（以下「評価対象者」という。）について、次に掲げる事項についての調査（以下この条及び第十六条第一項において「適性評価調査」という。）を行い、その結果に基づき実施するものとする。

五 **精神疾患に関する事項**

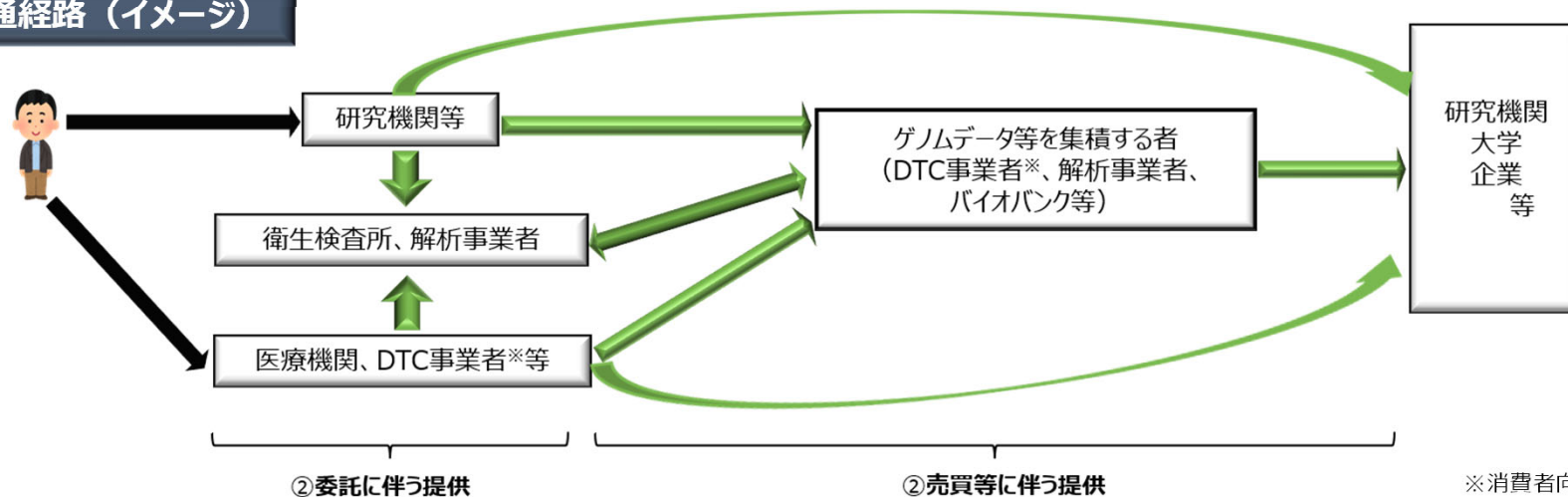
七 **信用状態その他経済的な状況に関する事項**

- 個人に関する機微なデータの取扱いに関する行為としては、①当該データを保存・処理する情報システム等の導入や維持管理等の委託や、②当該データや生体試料の提供（売買、委託等）等の様々なものがあり、それらに関し、**個人の権利利益の保護を目的とする個人情報保護法等の既存の規律はあるものの、安全保障の観点からの規律はない。**
- 個人に関する機微なデータの流通は、そのデータの特性に応じて多様であり、また、当該データを取り扱う者は、スタートアップ企業や大学等を含め広範な事業者が想定される。例えば、ゲノムデータやそれを得るための生体試料（「ゲノムデータ等」）においては、医療機関から衛生検査所への生体試料の解析の委託や、ゲノムデータ等を集積したバイオバンク等によるゲノムデータ等の提供等が行われている。

個人に関する機微なデータの取扱い



ゲノムデータ等の主な流通経路（イメージ）



（１）規律の対象

① 対象とするデータ

有識者会議で講ずるべき措置の検討が必要とされた個人に関する機微なデータのうち、まずは、情報の機微度や安全保障上のリスクを踏まえ、防護の優先度が特に高いと考えられるゲノムデータ・医療情報・金融情報から規律の対象としてはどうか。

② 対象とする事業者

規律の実効性や事業者負担を勘案し、安全保障上のリスクが高いと考えられる個人に関する機微なデータを大量に取り扱う者における当該データの取扱いを規律の対象とする制度としてはどうか。

③ 対象とする行為

外部への情報流出を生じさせ得る行為である「データの処理・保存を行う情報システム等の契約」「データや生体試料の提供（売買、委託等）」に対応する規律としてはどうか。

④ 対象範囲の考え方

規律の対象は、制度開始当初においては、規律の実効性や事業者負担等を勘案し、規律の目的に応じて真に必要な範囲に限定するとともに、施行後においても、我が国の安全保障環境等を踏まえて適時に見直しを行うこととしてはどうか。

（２）規律の内容

データ利活用の重要性、事業者負担及び規律の実効性等に鑑み、安全保障上のリスクが高いと考えられる上記のデータの取扱いの類型において、国が届出を受けリスクを個別に審査をする枠組みとするのはどうか。