データセキュリティワーキンググループ

とりまとめ

2026年3月11日

本とりまとめの趣旨・対象

AI 等の先端技術の急速な進展に伴い、データはイノベーションの創出や価値創造の源泉となり、その重要性は高まり続けている。データは単に自組織内で利活用するだけでなく、他の組織、例えばサプライチェーン上の他の事業者と共有・連携し、AI 等に読み込ませることで従来では得られなかった価値の創出が期待でき[1]、デジタル化が急速に進む中で、事業者や業界、さらには国といった領域を越えてデータを共有・連携することは、企業等が事業を行う上で、もはや不可欠の営みになりつつある。

本とりまとめ[2]は、上記認識の下、国の内外を問わず他の組織とデータの共有・連携を推進することで生じ得る、法益侵害リスクに対処するための一連の営みを「データセキュリティ[3]」と定義し、その基本的な考え方を提示するものである。

なお、本稿の主な想定読者としては、デジタル庁『データガバナンス・ガイドライン[4]』で対象とした経営者はもとより、同ガイドラインで提唱した CDO（Chief Data Officer）等、データに関する全社に渡っての責任を有する者や組織も対象としている。

1. データの連携や流通に伴って増大するリスク

デジタル化の進展に伴い、企業や行政機関等においてクラウドサービスの利用が一般化しつつあり、SaaS[5]として複数のクラウドサービスを組み合わせて利用するケースも

---

[1] 例えば、サプライチェーン上の事業者が自社の在庫部品のデータを共有することで、重要半導体の供給不足等が生じた場合に、事業者間で融通しあうことによって生産可能数の最大化を図れるようになる等が挙げられる。

[2] 本稿は、国際枠組の下で DFFT（後段脚注参照）の具体化における日本政府の取組や提案形成のために、データの越境移転に関わる情報や企業等からの要望を反映するための有識者による議論、検討、提言を行う場である「国際データガバナンス検討会」の下に設置された、「データセキュリティワーキンググループ」の検討結果をまとめたものである。
（デジタル庁）https://www.digital.go.jp/councils/global-data-governance

[3] 経済安全保障に係る議論の中でも、データセキュリティという言葉が使われ、安全保障上重要なデータ等のセキュリティを中心に議論がされているが、本稿が対象とするデータセキュリティは、一般の民間企業等によるデータ利活用におけるセキュリティを念頭としたものであり、その目的及び対象は異なるものである。なお、本稿における定義であることを明確にするため、以降「 」付きで表記している。

[4] 主として企業の経営者を対象に、Society 5.0 の実現に向け、企業が DX（デジタル・トランスフォーメーション）に取り組むに当たり、データガバナンスの必要性とその在り方、実践するに当たっての要点や留意すべきポイントをまとめたもの。
（デジタル庁）https://www.digital.go.jp/news/71bf19c2-f804-488e-ab32-e7a044dcac58

[5] SaaS（Software as a Service）：サービスとしてのソフトウェアの意味であり、インターネット経由でソフトウェアが有する効用を提供・利用する形態のこと。

増えている。また、AI の急速な進展によって、クラウド上の AI がその内部処理を実行する際、複数の SaaS を連携させて回答を抽出することもあるため、SaaS 事業者とデータの適切な管理を規定する契約を締結するのみでは、データに付随する法益への侵害リスクに十分に対応することがもはや困難となっている。

これらのデジタル化や AI 等の先端技術の急速な進展に伴い、以下の(1)から(4)に例示するような、データの連携や流通によって生じるリスクが増大している。

(1) データを処理するサービスの多様化・複雑化等に伴うリスク

多くの企業や団体において、従来のオンプレミス等のシステムから、第三者が提供するクラウドサービス等の利用への転換、さらには生成 AI の登場、高度化もあり、複数のクラウドサービス上の AI 等を連携する形態の利用も活発化している。これに伴い、データの格納場所や一時保管場所、各サービスにおけるデータに対する処理の内容、更にはサービス提供者とのデータの取扱いに関する契約内容などを一元的に管理し、データの窃取や改ざん等の予期せぬ問題が生じた場合に、その原因や責任の所在を解析することが難しくなっている。

(2) データの共有・連携先に起因するリスク

共有・連携先でのデータの取扱いにおいて生じ得るリスクである。データを共有・連携した事業者が、利用しているクラウド事業者等の第三者に無断でデータを共有したり、他のデータと組み合わせて利用したりしてしまうなど、データ提供者が想定していなかった処理に使われる可能性がある。このような場合、従来は契約書等によって提供したデータの利用目的や利用範囲を制限する等していたが、データの提供先が AI を利用する場合等は、提供したデータがその制限の範囲内で利用されたかを把握するのは困難であり、当該データに付随するデータ提供者の「法益[6]」が侵害されるリスクが生じている[7]。

(3) AI 等の先端技術に起因する予期せぬリスク

生成 AI 等の先端技術を利用する場合、それらが行う処理内容をあらかじめ完全に把握しておくことは困難であり、予期せぬ法益侵害のリスクが生じる可能性がある。例えば、ある企業が顧客対応の効率化のために生成 AI を導入し、過去の

---

[6] 「法益」に関しては「3. 「データセキュリティ」の基本的な考え方」で詳細を説明している。

[7] 例えば製造業において、設備データや品質データを外部の分析サービスに提供し、AI による最適化等を行うケースが増えている。この場合、データそのものは匿名化されていたとしても、分析結果によって特定の工場や取引先の状況等を推測可能になり、競争上の不利益が生じる可能性がある。

問い合わせ履歴を学習データとして利用した場合、入力データの取扱いが法令に沿ったものであっても、AI の出力結果が、性別や年齢、人種などの特定の顧客属性に対して不利な対応を示唆した場合、当該制度が保護している法益の侵害が生じる可能性がある。

(4) データに関する法令等の増加・多様化に伴うリスク

データの価値が高まるにつれ、生成されたデータを当該法域外へ移転することについて制限するような動き[8]が、世界的に増加傾向にある。その結果、自社で生成されたデータであるにも関わらず、法域外の拠点に持ち出すことができないという問題に直面している。また、データの移転に限らず、個人情報保護をはじめとする、データの取扱いに関する規制には様々なものがあり、かつ技術の発展によって急速に多様化する傾向にある。それぞれの国や地域で定められている法令や、業界の規範等に対する最新の状況を把握していない場合に、予期せぬ経済的負担等を負うことになる等のリスクが生じる可能性がある[9]。

2. 「データセキュリティ」の必要性

「１．データの連携や流通に伴って増大するリスク」で示したようなリスクは、必ずしもデータそのものに紐付いているわけではなく、データを利用する文脈によって顕在化する。例えば、データを利活用する際に、内部の処理がブラックボックス化された AI 等を利用する場合、意図せずに第三者の法益侵害を生じさせてしまう可能性がある。

従来は、データを自社のシステム内にとどめ、主に外部からのアクセスを技術的措置によって防止する方法等で法益侵害リスクに対応してきたが、このような従来の方法だけでは、「１．データの連携や流通に伴って増大するリスク」に対応することは困難である。

一方で、上記のような法益侵害リスクを過大に捉え、データの共有や連携を不必要に控えてしまうと、データという重要な資産から得られるイノベーションや、経済的価値

---

[8] EU における GDPR では、「十分性認定」を受けていない国から EU 域内にある個人情報にアクセスするには、標準契約条項（SCC：なお、データ移転影響評価を実施し、必要に応じて技術的／組織的補完措置を講じる）、拘束的企業準則（BCR）等の適切な保護措置を講じる必要がある。

[9] Uber がヨーロッパのドライバーの個人データを米国のサーバーに転送した際に、適切な保護措置なしで EU 域外への大量データ移転を行ったとして、GDPR 第 44 条（第三国への個人データ転送）違反に問われ、2023 年に制裁金 2 億 9,000 万ユーロ（約 450 億円）が科された。（現在不服申し立てが行われている）

を享受できなくなってしまう。

そこで本とりまとめにおいては、従来の考え方を念頭に置きつつ、事業主体や業界、さらには国や地域といった領域をデータが越えること、すなわち「データの越境移転[10]」に伴う法益侵害リスクを、データのライフサイクルを通して社会的に受容可能なレベルにコントロールし、AI 等の利活用を実現・促進するための一連の施策を「データセキュリティ」の中心的要素として、具体的な方策案を提示している。

3. 「データセキュリティ」の基本的な考え方

これまでに論じたように、「データの越境移転」や、データの利活用に伴う法益侵害リスクは、データを利活用する際のライフサイクルにおける文脈や、AI 等の技術の進展に伴い変化していくことから、その対応策となる「データセキュリティ」についても、アジャイルにアップデートしていくことが求められる。

どのような観点から「データセキュリティ」を確立すべきかについて、本ワーキンググループでは、次に掲げる(1)から(4)の基本認識を持つことが特に重要であると確認された。

(1) 法益を念頭に置く

リスクを社会的に受容可能な範囲内にコントロールするためには、法令の遵守を大前提としながらも、インシデントが発生した際の経済的・社会的損失をあらかじめ高い解像度で計っておく必要がある。そのためには、遵守の対象たる法令等が保護している「法益」に着目することが重要となる。

ここでいう「法益」とは、不正競争防止法、著作権法、特許法、知的財産基本法、個人情報保護法等の諸法令に加え、業界規定等によって保護されるべき、企業、個人及び社会の経済的・社会的利益を指す。「法益を念頭に置く」とは、法令等をその文言のまま遵守するのみならず、当該法令や規定等が守ろうとしている「法益」を見極め、守るべき対象や事象を可能な限り明確に理解しておくことを指している。

例えば、不正競争防止法は事業者間の公正な競争等を確保し、これをもって国民経済の健全な発展に寄与することを法目的としており、その実現の手段として、同法では、「営業秘密の不正取得等」や「限定提供データの不正取得等」といった

[10] 本稿では、「データの越境移転」を国等の法域を越えてデータを移転する場合に限定せず、組織や企業及び産業界といった、領域を超えてデータを共有・連携する場合や、当該領域外からデータにアクセスする場合を意味しているため、以降「 」付きで記載している。

行為を不正競争として規定している。このことから、当該規定は、営業秘密や限定提供データが不正取得されるといった行為を禁止することで、事業者間の公正な競争を法益として保護しているものと考えられる。また、個人情報保護法では、個人情報の有用性に配慮しつつ、個人の権利利益を保護することを法目的としており、その実現の手段として、個人情報の利用目的を特定しこれを本人に通知し又は公表すること、個人データの安全管理のために必要かつ適切な措置を講ずること、といった情報の取扱いに関する規律を定めている。そのうえで、例えば、安全管理のために講ずべき措置について、その情報の取扱いによるリスク等の程度に応じて講ずることとすることで、個人の権利利益を法益として保護し、その際、個人情報の有用性にも配慮しているものと考えられる。

これらの法律等によって、どのような利益が、どのような方法で、どの程度保護されているのかを具体的・分析的・機能的に捉えることにより、「データセキュリティ」の確保を通じて実現されるべき保護の内容やレベルを考察する上でのベンチマークを得ることができると考える。

なお、「1.(4) データに関する法令等の増加・多様化に伴うリスク」で述べたとおり、技術の進展等に伴って各国では新たな法令が制定され、また既存の法令が改正される傾向にあるため、法令情報提供サービス等を利用して関係する法令の動向を確認し、適宜見直しを図ることも法益を念頭に置くにあたっては重要となる。

(2) リスクを社会的に受容可能な範囲内にコントロールする

AI 等の先端技術が進展している現在において、「データの越境移転」に伴うすべての法益侵害リスクをゼロにすることはできない[11]。「データセキュリティ」を実装することにより、法益侵害リスクを「社会的に受容可能なレベル」にコントロールすることが重要である。

なお、ここで言う社会的に受容可能なレベルとしては、法令が本来もたらそうとしている法益保護を実現できるようにリスクをコントロールしたレベルが考えられる。法令は、その制定過程における公的な議論や国際的な合意等に基づいて法益を守るための措置を講じること等を求めることにより、当該法令の名宛人がそのような措置を講じることにより生じうる負担等も踏まえた上で、社会的に望ましいレベルの法益保護のあり方を示していると考えられる。したがって、技術や運用の組合せによる法益保護措置を考える際にも、法令が本来想定している法

[11] 例えば、「信頼の構造」(山岸俊男著、東京大学出版、1998 年)における「信頼」の定義が多くの議論で引用されているが、「信頼」はリスクをゼロにするものではなくリスクが不可避的に伴う状況下でこそ必要とされるものとしている。

益保護レベルを満たす形でリスクを抑えることができれば、それは社会的にも許容されると考えられる。

(3) 「制度」「技術」「運用」の三位一体で対策する

データの共有・連携や、AI 等の先端技術の利活用によって生じ得るリスクを、社会的に受容可能なレベルにまで低減させるには、「制度」だけではなく、「技術」・「運用」の三位一体の措置を講じることでより実効性のある対策が可能となる。

まず、「制度」とは、法令や規則、明文化された業界規定等の規範を通じてデータの取扱いに関わる義務や責任等を定め、規範の名宛人に対して適切な対応を促すことで、法益侵害のリスクを低減する措置を指している。

法令や明文化された業界規定などを補完する社内「制度」としては、例えばデータ利用に関する基本方針や責任分担を明確にし、データ分類と法益観点からの重要度の明示や、データを共有する第三者に対する利用目的・委任範囲の明確化、責任分界点とエスカレーション設計など、現場が判断に迷わないルール・責任構造といった枠組みを整えることが考えられる。

「技術[12]」とは、データの共有・連携や AI 利用における秘密計算などの可読データの秘匿化技術や PETs 等に加え、データの共有・連携先の信用性を計るための手段である Verifiable Credentials（VC：検証可能な資格情報）などの技術的手段を用いて、データに付随する法益侵害リスクを社会的に受容可能なレベルに低減する措置一般を指している。

ここで、「技術」は「制度」による「法益」保護の実効性を高める関係にあるという基本認識に立つことができる。なぜならば、現状において「法益」は、法令や契約などの「制度」によって社会的に保護されており、「技術」は「制度」が「法益」の保護において果たしている機能を担保し、またこれを侵害しようとする行為を防止する役割を担うからである。

そして「運用」とは、前述の「制度」及び「技術」を実効的に機能させるためのガバナンス体制の整備等を通じて、データの処理や利活用を行う現場での法益侵害リスクを、社会的に受容可能なレベルに低減するための一連の措置を統制・管理することを指している。

「運用」においては、現場の柔軟なデータ利活用を前提としつつ、問題が生じ

[12] 例えば、暗号化以外にも秘密計算等の PETs（Privacy-enhancing technologies）が挙げられる。PETs はハードウェア、ミドルウェア、ソフトウェア等、データ処理における様々なレイヤーでの活用が可能であり、我が国企業が提供しているものもある。

た場合には迅速に共有・是正できるガバナンス体制を構築し、現場を統制することが重要である。禁止を前提とするのではなく、定められた利活用の範囲内での裁量を認めることで、データ利活用と統制の両立が図られるようになる。

そして、「データの越境移転」等によって生じる法益侵害リスクを、「制度」「技術」「運用」によって社会的に受容可能なレベルにコントロールするにあたっては、それぞれを単独に見るのではなく、それらを三位一体の総体として、考えることが不可欠である。例えば、「制度」と「運用」のみで目的を達成しようとすれば、本来不要な労力等が生じ、結果的に得られる可能性のあった「データの越境移転」へのインセンティブを阻害するおそれがある。同様に、「技術」のみで対応しようとすれば、技術的難易度が高い技術の導入が必要となるなど、実装における実現可能性が低くなることが懸念される。また、「制度」や「技術」そのものに不備があれば、「運用」のみでこれを補完することには限界があることも明らかである。

また、「制度」「技術」「運用」の三位一体を考える上で、「技術」の進化はあまりに早く、その全容把握が困難になりつつある。そこで、データの利用文脈で生じ得るリスクへの「技術」的措置を、CDO 等のデータに関する全社に渡っての責任を有する者・専任組織がマッピングし、最新の動向を注視しながら、新規の「技術」が登場した際には、「制度」「運用」相互との総合的な適用性を評価し、アジャイルにアップデートして行くことが重要となる。

以上のとおり、従来のようにデータが自組織内に留まることを前提として、外部等からの不正なアクセスを主にシステムなどの「技術」で防いでいた措置とは異なり、「データセキュリティ」を講じるにあたっては、越境移転するデータを主体として、データ利用の文脈で生じ得るそれぞれのリスク対策について、制度・技術・運用の三位一体の措置で見直すことが重要となる。

(4) データのライフサイクルにおける各フェーズで施策を講じる

データの連携や流通に伴って増大するリスクは、データのライフサイクルの各フェーズにおける現場でのデータの処理や利活用の際に生じるため、組織全体に対する画一的な施策のみでは対応することが困難である。「データセキュリティ」においては、適宜他者との共有・連携を可能とするデータを主体として、データの生成・収集、加工・各種処理、他社との共有・連携、データ共有先での取扱いから削除に至るまでのライフサイクルの各フェーズと、そこでの具体的なデータの処理・利活用内容を捉えることが重要となる。

そして、それぞれのフェーズにおける現場でのデータの処理や利活用によって起こり得る固有のリスクに対し、「制度」と「技術」では十分な「データセキュリティ」が講じられない部分においては、行動指針や作業要領等の社内ルールでそ

れを補完し、「制度」にフィードバックすることによって、リスクを社会的に受容可能な範囲内にコントロールする必要がある。

4. 試行例　―データセキュリティワーキンググループ監修によるアイディアソンの成果

本とりまとめの作成に際して、データの「制度」「技術」「運用」等の各分野に関わる有識者によるアイディアソンを開催し、３．(3)で述べた最新の技術的措置のマッピングを試みた。その成果を【別紙】に提示する。

なお、マッピング作成の際には、「法益」を保護するための具体的な「制度」がどのような効力を持つかを参照しながら進めた。また、「制度」「技術」「運用」の三位一体の中で、全体として合理的かつ実効的なものにしていくという点に注意を払った。

本試行例では時間等の制限により、主に「法益」に対する「制度」と、それを補完・代替し得る「技術」のマッピングに留め DFFT[13]推進のために特に考慮すべき、「データの越境移転」に伴って生じ得る特有の課題に焦点を絞って検討を進めたため、【別紙】マッピングの図中において灰色で示した部分については、本検討の対象外としていることに留意されたい。

5. 今後継続して取り組むべき項目

本とりまとめは、「データセキュリティ」の確立に向けた一つの考え方を提示している。今後、「データの越境移転」等の多様な取組が進む中で、本とりまとめが広く参照され、「データセキュリティ」に関わるプラクティスが蓄積されることを通じて、将来的なソフトローの形成、すなわち、業界内やサプライチェーン内等での「制度」の形成等に寄与することを期待するものである。

しかしながら一方で、ここで示した考え方や試行例は基本的なものながら、今後の「データの越境移転」等の実際の進展に合わせて、見直し・修正を行う必要があるため、今後の継続的な検討が必要であると考えられる事項を以下に挙げる。

---

[13] DFFT（Data Free Flow with Trust：信頼性のある自由なデータ流通）とは、「プライバシーやセキュリティ、知的財産権に関する信頼を確保しながら、ビジネスや社会課題の解決に有益なデータが国境を意識することなく自由に行き来する、国際的に自由なデータ流通の促進を目指す」というコンセプトであり、2019 年 1 月にスイス・ジュネーブで開催された世界経済フォーラム年次総会（ダボス会議）にて、安倍総理（当時）が提唱し、2019 年 6 月の G20 大阪サミットにおいて各国首脳からの支持を得て、首脳宣言に盛り込まれた。

第一に、具体のユースケースに基づく、「データセキュリティ」の具体化である。ユースケースごとに、データライフサイクルの各フェーズにおいて生じ得る固有のリスクも異なり得ることから、組み合わせるべき「制度」「技術」「運用」も変化するため、具体のユースケースの中で、「データセキュリティ」の実装を図ることが重要である。

第二に、マッピングされた「技術」の更新である。近年においては、非常に早い速度で技術革新、ユースケースの深化、また、これらに伴う新たなリスクの出現が生じると予測されるため、それまでに効力を有していた技術的措置が、新たな法令の制定等によって当該法益侵害リスクへの充分な対応が困難になる可能性が起こり得る。したがって、最新の技術動向やユースケースにおける現実に即した状況を、CDO や専任組織が調査・モニタリングし、それら技術的措置の効力だけでなく、提供主体との相互信頼等を踏まえ、組み合わせるべき技術的措置を適宜見直していく必要がある。

第三に、「データの越境移転」における国際的な相互運用性の確保である。特に国境を越えるデータの共有・連携にあたっては、各国や地域の法令や「技術」に対する規制等との整合が不可欠となる。このため、DFFT 具体化に向けた国際的な枠組みである OECD[14] IAP[15]やその他バイ、マルチにおける議論に対して、産官学が連携して積極的に参加し、我が国がデータガバナンスに関する議論を主導しながら、「データの越境移転」に関わる国際的な発展に貢献していくことが求められる。とりわけ、「制度」と「技術」を架橋し、両者の統合的な「運用」によって、リスクを社会的に受容可能なレベルに収めるという本とりまとめの方法論は、我が国が強みを持つ PETs 等の「技術」を、例えば、OECD の下に設置された DFFT Expert Community のプロジェクト[16]の一環として、より具体的に訴求して行くうえでも極めて有益なモデルとなり得る。

おわりに

AI 時代における「データセキュリティ」は一度きりの対策で完結するものではなく、技術の進化や社会の変化に応じて評価・見直しを繰り返すべき動的な取り組みである。

AI 等の先端技術を活用し、データの連携・共有を行うことで、新たな価値の創出が求められる現代においては、データの越境移転を止めるのではなく、「データセキュリティ」を基盤として、そのリスクを社会的に受容可能なレベルにコントロールしながら流

[14] OECD（Organisation for Economic Co-operation and Development）：経済開発協力機構

[15] IAP（Institutional Arrangement for Partnership）： OECD に設置され、国際機関の既存の委員会や機関を活用し、多国間政策立案と調整を促進している。

[16] DFFT Expert Community では、規制の透明性向上、PETs、国際送金、健康医療データの二次利用の 4 つのプロジェクトでで、それぞれ具体的な検討が進められている。

通させることが求められる。

「データセキュリティ」は単なるコストやリスク回避策ではなく、データ活用を持続可能にするための経営基盤であり、企業価値を向上して行くうえで不可欠の要素である。

【別紙】

本マッピングは、データセキュリティワーキンググループにおいて、「データの越境移転」に伴うリスクへの対応策を、「制度」「技術」「運用」の三位一体で整理した試行例である。データセキュリティワーキンググループの委員をはじめとした、法律や技術分野に知見を有する幅広い関係者に参画いただき、以下の１から５に示すステップで進めた。なお、本マッピングの試行例は、現在の「技術」を基にした一例であるが、本結果をひな型として、今後の技術動向や制度環境の変化等に応じて、継続的に見直し・更新されることを期待している。

1. **ユースケースとデータライフサイクルの整理**
   例示として取り上げた「データの越境移転」における、AI のモデル作成から活用までの一般的なプロセスにおける、データのライフサイクルを各フェーズに分けて横軸に整理した。

2. **関連する法令のプロット**
   次に、データのライフサイクルの各フェーズにおいて適用される可能性がある法令を各フェーズにおいてプロットした。例えば、個人情報保護法や不正競争防止法[17]等が該当する。

3. **法益とリスクの整理**
   抽出された法令に基づき、それぞれが保護している社会・企業・個人等の利益（法益）を整理し、それらが侵害されるリスクがどのように発現するかを整理した。

4. **技術的リスクの抽出**
   法措置を検討する為に、まず法益侵害リスクがどのような技術的リスクとして発現し得るかを検討・抽出した。

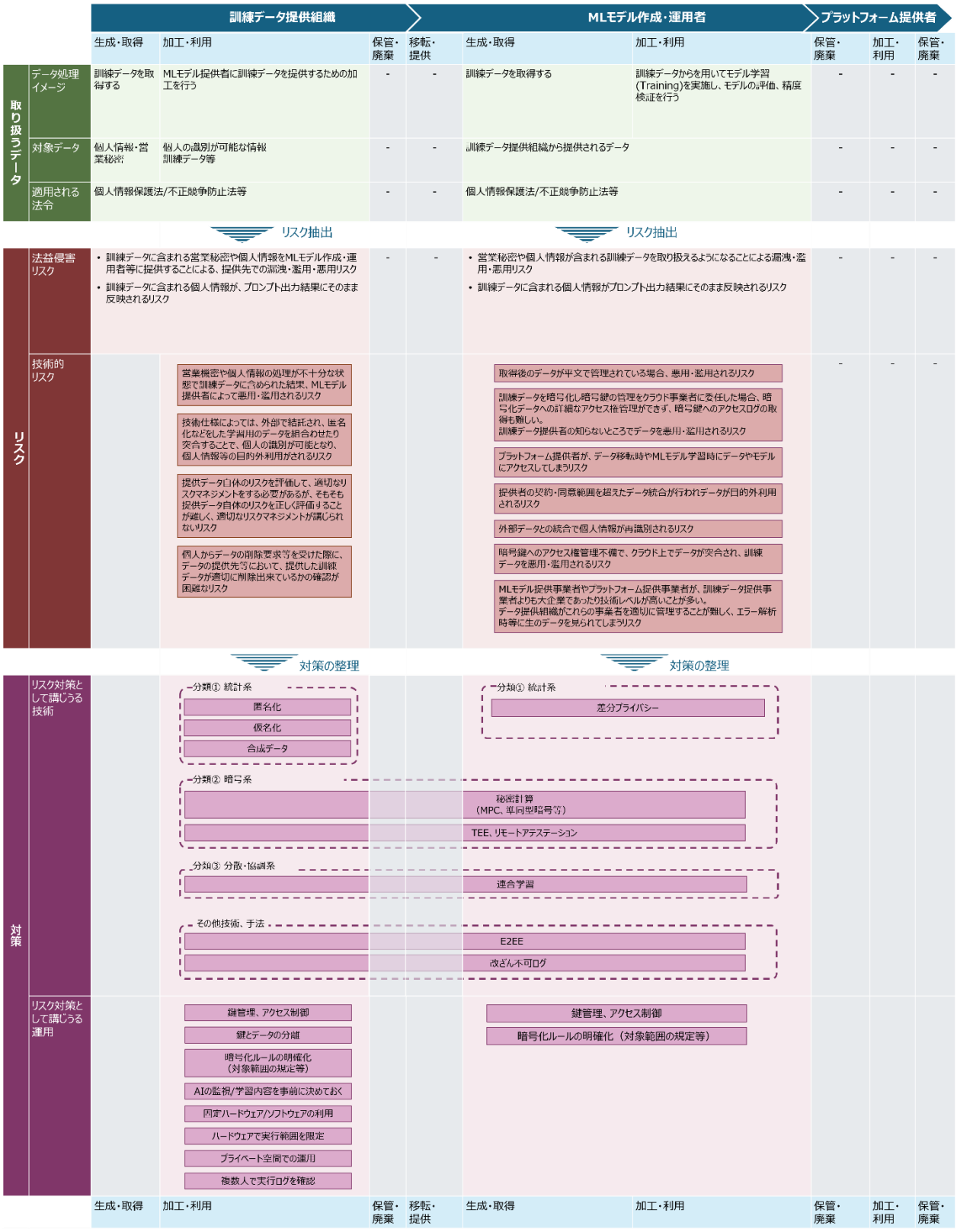
5. **技術的措置の分類とマッピング**
   次に、上記「4. 技術的リスクの抽出」で整理した内容を、低減可能な現在確立されている技術的措置から抽出し、データのライフサイクルにおける各フェーズに対応させてマッピングした。

以上より、データのライフサイクルにおける各フェーズにおいて、どの技術的措置

[17] 不正競争防止法では、法益侵害リスクに記載されている行為が直ちに不正競争行為となるわけではなく、その他の諸事情を考慮して判断される。

がどの場面で有効かを可視化し、制度・技術・運用の三位一体による「データセキュリティ」における「制度」と「技術」の可視化を例示している。

「モデル作成」におけるマッピング試行例



「推論」におけるマッピング試行例