データ保護影響評価（DPIA）の実施に関するガイドライン

WP 248 rev.01（仮訳）

2018 年 8 月

日本貿易振興機構（ジェトロ）
海外調査部 欧州ロシアＣＩＳ課

第 29 条作業部会

17/EN
WP 248 rev 01

データ保護影響評価（Data Protection Impact Assessment：DPIA）、及び処理がEU規則2016/679の目的に照らして「高度のリスクをもたらす可能性」があるかを決定するためのガイドライン

2017 年 4 月 4 日に採択
2017年10月4日に改訂・採択された最新版

本作業部会は指令 95/46/EC の第 29 条に基づき設置されたデータ保護とプライバシーに関する独立した欧州諮問機関であり、その任務は指令 95/46/EC の第 30 条と指令 2002/58/EC の第 15 条に記載されている。

事務局は、欧州委員会の司法総局 C 局（基本的権利及び欧州連合市民権）（ベルギー王国ブリュッセル B-1049、オフィス No MO59 03/075）が担当する。

ウェブサイト：http://ec.europa.eu/justice/data-protection/index_en.htm

個人データの処理に関する個人の保護についての作業部会は

1995 年 10 月 24 日の欧州議会及び理事会指令 95/46/EC によって設置され、

その第 29 条及び第 30 条に鑑み、

その手続規則を考慮して、

本ガイドラインを採択した。

目次

I. 序文

EU 規則 2016/679[1]（GDPR）は 2018 年 5 月 25 日から適用となる。GDPR の第 35 条では、データ保護影響評価（Data Protection Impact Assessment：DPIA[2]）の概念を採用している。EU 指令 2016/680[3] においても同様である。

DPIA は、データ処理を記述し、データ処理の必要性と比例性を評価し、個人データ[4]の処理に起因する自然人の権利と自由に対するリスクの管理を、リスク評価とリスクに対処する措置の決定により支援するために設計されたプロセスである。DPIA は、GDPR の要求事項を遵守するためばかりでなく、EU 規則を確実に遵守する適切な措置を取っていることを立証するためにも管理者にとって有用であり、説明責任のためにも重要なツールである（第 24 条も参照）[5]。言い換えれば、DPIA はコンプライアンスの仕組み構築と立証のプロセスである。

GDPR の下では、DPIA の要求事項を遵守しないことにより、管轄監督機関が制裁金を課すことがある。データ処理が DPIA 実施を要する場合に、DPIA を実施しない（第 35 条第 1 項及び第 3 項ないし第 4 項）、誤った方法で実施する（第 35 条第 2 項及び第 7 項ないし第 9 項）、管轄監督機関との協議が必要であるにも係らず怠る（第 36 条第 3 項（e））などの場合には、最大 1,000 万ユーロ、または事業者については最大で前会計年度の全世界年間売上高の 2%の、いずれか高い方を行政上の制裁金として課すことがある。

訳注：本文、または脚注内で「第 X 条第 X 項」「前文第 XX 項」という記載は、特に断りがある場合を除き、それぞれ GDPR の条文、GDPR の前文を指す。

---

[1] 個人データの処理及びその自由な移動に関する自然人の保護並びに指令 95/46/EC の廃止に関する 2016 年 4 月 27 日付欧州議会及び理事会規則 2016/679（一般データ保護規則（General Data Protection Regulation：GDPR））。

[2]「プライバシー影響評価（Privacy Impact Assessment：PIA）」という用語は、同じ概念を表わす用語として他の文脈でよく使用される。

[3] 犯罪または刑事罰の執行における予防、捜査または起訴を目的とする権限のある機関による個人データの処理に係る個人の保護及び当該データの移動に関する 2016 年 4 月 27 日付欧州議会及び理事会指令 2016/680 の第 27 条は、「当該データ処理が自然人の権利と自由への高いリスクを生じる可能性がある」ためプライバシー影響評価が必要とされるとも述べている。

[4] GDPR は DPIA の概念を公式にはそのように定義してはいないが、

- 第 35 条第 7 項には、最低限、次の内容を含むよう記載されている。
  - *「（a）予想された処理業務及び処理の目的の体系的記述。該当する場合、管理者によって追求される正当な利益を含む。*
  - *（b）目的に関する処理業務の必要性及び比例性の評価。*
  - *（c）第 1 項で定めるデータ主体の権利及び自由に関するリスクの評価。及び*
  - *（d）リスクに対処するために予定された措置。データ主体及び関連する他者の権利及び正当な利益を考慮し、個人データの保護を確実にし、本規則の遵守を証明するための保護措置、安全対策及び安全メカニズムを含む。」*
- その意味と役割については前文第 84 項にて次のように説明されている。*「処理業務が自然人の権利と自由に高いリスクをもたらす場合に本 EU 規則を一層厳格に遵守するためには、管理者はデータ保護影響評価を実施し、特にそのリスクの起源、性質、特殊性、重大性を評価することに責任を持つべきである。」*

[5] 前文第 84 項も参照。*「個人データの処理が本 EU 規則を遵守していることを立証するために適切な措置を講じることを決定する際に、データ保護影響評価の結果を考慮すべきである。」*

II. 本ガイドラインの適用範囲

本ガイドラインは次の文書を考慮している。

- 第 29 条データ保護作業部会（第 29 条作業部会）声明 14/EN WP 218[6]
- データ保護責任者に関する第 29 条作業部会ガイドライン 16/EN WP 243[7]
- 目的制限に関する第 29 条作業部会意見 13/EN WP 203[8]
- 国際標準 [9]

GDPR によって具体化されたリスクベースのアプローチに沿って DPIA を実行することは、すべての処理業務で必須なわけではない。DPIA は、処理が*「自然人の権利と自由に対して高いリスクをもたらす可能性が高い」*場合にのみ必要となる（第 35 条第 1 項）。DPIA が義務付けられている状況を一貫して解釈するために（第 35 条第 3 項）、本ガイドラインは、まずこの概念を明確にし、第 35 条第 4 項に基づきデータ保護機関（DPA）が採用するリストの基準を提供することを目指す。

第 70 条第 1 項（e)に従い、欧州データ保護会議（European Data Protection Board：EDPB）は GDPR の一貫した適用を促進するためにガイドライン、勧告及びベストプラクティスを発行することができる。この文書の目的は、欧州データ保護会議の今後発行するガイドライン、提言、ベストプラクティスを予測し、それにより、管理者が法を遵守することを支援し、また、DPIA を実施する必要がある管理者に対して法的確実性を提供するために、GDPR の関連規定を明確にすることである。

本ガイドラインはまた次の共通リスト、基準、提言の整備が促進されることも狙いとしている。

[6]2014 年 5 月 30 日に採択されたデータ保護の法的枠組みに対するリスクベースのアプローチの役割についての第 29 条作業部会声明 14/EN WP 218。
http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp218_en.pdf?wb48617274=72C54532

[7]2016 年 12 月 13 日に採択されたデータ保護責任者に関する第 29 条作業部会ガイドライン 16/EN WP 243。
http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp243_en_40855.pdf?wb48617274=CD63BD9A

[8]2013 年 4 月 2 日に採択された目的制限に関する第 29 条作業部会意見 13/EN WP 203。
http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf?wb48617274=39E0E409

[9]例えば ISO 31000:2009、*リスク管理 — 原則とガイドライン*、国際標準化機構（International Organization for Standardization：ISO）；ISO/IEC 29134（プロジェクト）、*情報技術 - セキュリティ技術 - プライバシー影響評価 - ガイドライン*、国際標準化機構（International Organization for Standardization：ISO）

- DPIA が必須となる処理業務（第 35 条第 4 項）の EU 共通リスト
- DPIA が不要となる処理業務（第 35 条第 5 項）の EU 共通リスト

- DPIA を実施するための方法論に関する共通基準（第 35 条第 5 項）
- 監督機関と協議する時期（第 36 条第 1 項）を特定するための共通基準
- 可能であれば、EU 加盟国で得られた経験に基づく勧告

III. DPIA：規則における説明

GDPR は管理者に「自然人の権利及び自由に関するリスクの様々な可能性及び重大性」（第 24 条第 1 項）を考慮して、GDPR の遵守を確実に証明することができる適切な措置を実施することを求めている。DPIA を特定の状況下で実施する管理者の義務は、個人データの処理によってもたらされるリスク [10] を適切に管理する一般的な義務を背景として理解されるべきである。

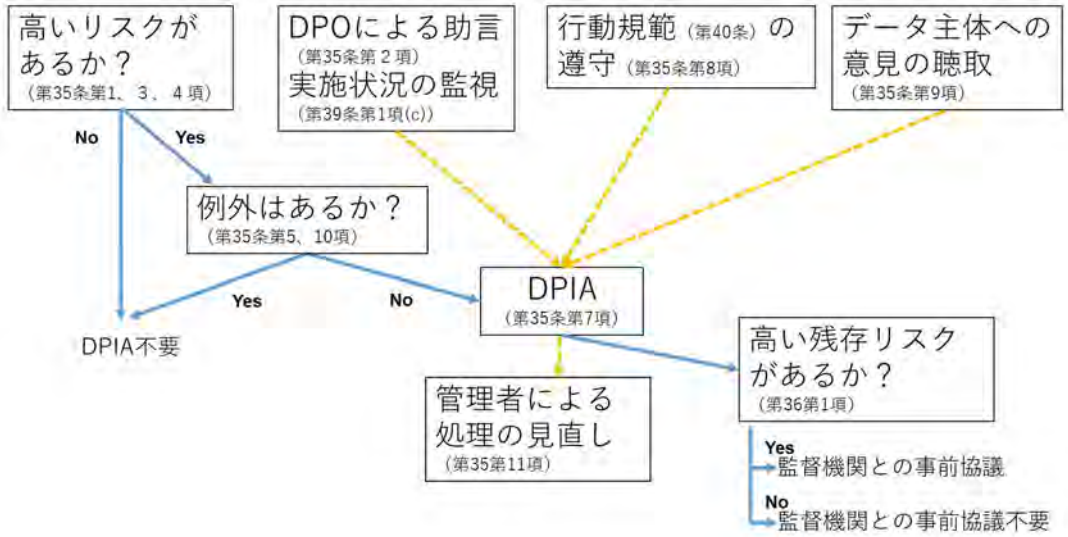
「リスク」とは、重大性と可能性（起こりやすさ）の観点から推定される事象とその結果を記述するシナリオである。一方、「リスク管理」は、リスクに対して組織を指揮し統制する秩序ある活動として定義することができる。

第 35 条は、「個人の権利と自由に対して」可能性の高いリスクについて述べている。データ保護の法的枠組みにおけるリスクベースのアプローチの役割に関する第 29 条データ保護作業部会の声明に示されているように、データ主体の「権利と自由」への言及は、主にデータ保護とプライバシーに関する権利に関係するが、 言論の自由、思想の自由、移動の自由、差別禁止、自由、良心、宗教に対する権利などの他の基本的権利を含む。

GDPR によって具体化されたリスクベースのアプローチに沿って DPIA を実施することは、すべての処理業務において必須ではない。むしろ DPIA は、ある種の処理が「自然人の権利と自由に対する高いリスクをもたらす可能性が高い」場合にのみ必要とされる（第 35 条第 1 項）。ただし、単に DPIA を実施する義務が生じる条件を満たしていないという事実により、データ主体の権利と自由に関するリスクを適切に管理するための措置を実施する管理者の一般的な義務が軽減されるものではない。実際には、ある種の処理がいつ「自然人の権利と自由に高いリスクをもたらす可能性が高いか」を特定するために、管理者が処理活動によって生じたリスクを継続的に評価しなければならないことを意味する。

[10]自然人の権利と自由に対するリスクを管理するためには、リスクを特定、分析、計量、評価、対処（緩和など）し、定期的に見直す必要があることを強調しなければならない。管理者は、保険契約でリスクをカバーすることによって責任を免れることはできない。

次の図は一般データ保護規則（GDPR）におけるデータ保護影響評価（DPIA）に関連する基本原則を示している。



A. DPIA の対象は？単一の処理業務または一連の類似の処理業務

DPIA は単一のデータ処理業務に対して適用する場合がある。しかし、第 35 条第 1 項は「単一の DPIA で類似した高いリスクを伴う一連の類似の処理業務に対応することもできる。」と述べている。前文第 92 項ではこれに付け加えて次のように述べている。「データ保護影響評価の対象が単一のプロジェクトを対象とするよりも幅広いものを対象とした方が合理的かつ経済的な状況がある。例えば、公的機関または団体が共通のアプリケーションまたは処理プラットフォームを構築しようとする場合、または複数の管理者が業界またはセグメント全体にわたって、もしくは横断的活動に広く活用されることを目的として共通のアプリケーションまたは処理環境を導入する予定の場合などである。」

単一の DPIA を使用して、性質、範囲、文脈、目的、及びリスクに関して類似している複数の処理業務を評価することができる。実際、DPIA は、自然人の権利と自由に高いリスクをもたらす可能性のある新しい状況を体系的に検討することを目指しており、検討済みの場合（すなわち、特定の文脈で特定の目的のために実行される処理業務）に対して DPIA を実施する必要はない。これは、同じ目的で同じ種類のデータを収集するために類似の技術が使用される場合に該当する可能性がある。例えば、同様の監視システムをそれぞれ設置する地方自治体のグループは、別々の管理者による処理をカバーする単一の DPIA を実行することができる。または、鉄道事業者（単一の管理者）は、1 つの DPIA を使用してすべての駅でビデオ監視処理をカバーすることができる。これは、様々なデータ管理者によって実装される類似の処理業務にも適用可能である。これらの場合には、参考用の DPIA を共有し、公にアクセス可能とする必要があり、また DPIA に記載されている措置が実施される必要がある。さらに、単一の DPIA を実施する正当性を提示する必要がある。

処理業務に複数の管理者が関与している場合は、それぞれの義務を正確に定義する必要がある。それぞれの DPIA では、リスクを処理し、データ主体の権利と自由を保護するために設計されたさまざまな措置に対してそれを担当する当事者を特定するべきである。各データ管理者は、秘密（企業秘密、知的財産、ビジネス機密情報の保護など）を漏えいすることなく、脆弱性を開示せずに、各自のニーズを表現し、有用な情報を共有する必要がある。

DPIA は、ハードウェアやソフトウェアなどの技術製品が、異なるデータ管理者によって異なる処理業務の実行に使用される可能性が高い場合に、これらの技術製品のデータ保護への影響を評価する場合にも役立つ可能性がある。もちろん、製品を設置し利用しているデータ管理者は、個別システムの実装に関して独自の DPIA を実行する必要があるが、場合により、製品供給者が準備した DPIA によって部分的に情報を補うことができる。一例としては、スマートメーターのメーカーと公益事業会社の関係がある。各製品提供企業または処理者は、秘密を漏えいすることなく、また脆弱性を開示してセキュリティリスクを生じさせることなく、有用な情報を共有する必要がある。

B. どの処理業務がDPIAの対象となるか？例外を除き、「高度のリスクをもたらす可能性」があるデータ処理

本節では、DPIAが必須の場合と DPIA の実施が必要でない場合について説明する。

処理業務が例外（III.B.a）に該当しない限り、DPIAは、処理業務が *「高いリスクをもたらす可能性が高い」*（III.B.b）場合には実施する必要がある。

a) DPIAが必須の場合は？処理が *「高度のリスクをもたらす可能性」*がある場合。

GDPR は、自然人の権利と自由にリスクをもたらす可能性があるすべての処理業務に対して DPIA を実施することを要求してはいない。DPIA の実施は、第 35 条第 3 項で詳述され第 35 条第 4 項で補足されているように、処理が *「自然人の権利と自由に高いリスクをもたらす可能性が高い」*（第 35 条第 1 項。同 3 項で説明され、4 項で補足されている）場合にのみ必須である。新しいデータ処理技術が導入される場合に特に DPIA が必要となる可能性が高い[11]。

DPIA が必要かどうか明確でない場合でも、DPIA は管理者のデータ保護法遵守を支援するツールであるため、第 29 条作業部会は DPIA を実施することを推奨している。

DPIA が要求される可能性がある他の状況も存在するが、第 35 条第 3 項は、処理業務が *「高いリスクをもたらす可能性が高い」*場合のいくつかの例を提供している。

- *「(a) プロファイリングを含む自動的された処理に基づいて自然人に関する個人的側面を体系的かつ広範囲に評価され、当該評価に基づいて決定がなされ、その決定が自然人に関して法的効果を発生させまたは類似の重大な影響を与える場合[12]。*
- *(b) 第 9 条第 1 項で定める特別なカテゴリーのデータ、または第 10 条[13] で定める有罪判決及び犯罪に関する個人データを大規模に取扱う場合。*
- *(c) 一般の人々がアクセスできる場所において大規模な体系的監視を行う場合。」*

[11] 他の例については、前文第 89 項、前文第 91 項及び第 35 条第 1 項、第 3 項を参照。

[12] 前文第 71 項「特に、個人プロファイルを作成、または利用するために、データ主体の職場での実績、経済的状況、健康、個人的嗜好または関心、信頼性または行動、居場所または移動に関する側面を分析、予測すること」を参照。

[13] 前文第 75 項「人種的もしくは民族的素性、政治的意見、宗教的または哲学的信念、労働組合への所属状況を明らかにする個人データが処理される場合、及び遺伝的データ、健康に関するデータ、または性生活や有罪歴と犯罪行為や関連するセキュリティ対策に関するデータの処理」

GDPR 第 35 条第 3 項の導入文の*「特に（in particular）」*という言葉が示すように、このリストは網羅的ではないことを意味する。このリストに挙げられていない類似の「高リスク」処理業務が存在する可能性がある。これらの処理業務も DPIA の対象となる。このため、下記の基準は、GDPR の第 35 条第 3 項に示されている 3 つの例によって理解されるべきものの簡単な説明を超えていることがある。

固有の高いリスクがあるために DPIA を必要とする処理のより具体的な例を提供するためには、第 35 条第 1 項及び第 35 条第 3 項（a）から（c）まで、第 35 条第 4 項及び前文第 71 項、第 75 項、第 91 項に基づき国家レベルで採択されるリスト、*「高いリスクの結果を招く可能性が高い」*処理に関して述べている他の GDPR の記述[14]、などの特定の要素を考慮して、以下の基準を考慮すべきである。

1. 評価またはスコアリング：

   特に、「データ主体の職場での実績、経済的状況、健康、個人的嗜好または関心、信頼性または行動、居場所または移動に関する側面」（前文第 71 項及び第 91 項）から行われるプロファイリング及び予測を含む。この例としては、顧客を信用照会データベース、マネー・ロンダリングとテロ資金供与対策（AML/CTF）データベースまたは詐欺行為に関するデータベースにより審査する金融機関、または疾患/健康リスクを評価及び予測するために直接消費者に遺伝子検査を提供するバイオテクノロジー企業、または自社ウェブサイト上での行動や移動の履歴に基づき行動やマーケティングのプロファイルを構築する会社が含まれうる。
2. 法律上または同様の重要な効果を伴う自動化された決定：
   *「自然人に関する法的影響」*または*「自然人に類似する重大な影響を及ぼす」*（第35 条第 3 項（a））データ主体に関する決定を行うことを目的とする処理。例えば、処理が、個人に対する排除または差別につながる可能性がある場合に該当する。個人への影響が僅かであるか全くない場合はこの基準に該当しない。近く発表されるプロファイリングに関する第 29 条作業部会ガイドラインで、より詳細に説明される。
3. 体系的な監視：ネットワークまたは*「一般の人々がアクセス可能な場所における体系的監視」*（第35 条第 3 項（c））[15]によるデータ収集を含む、データ主体の観察、監視、支配のために行われる処理。このタイプの監視は、データの主体が、誰がデータを収集しており、どのように使用されるかを認識していない状況で、個人データが収

[14] 例えば前文第 75 項、第 76 項、第 92 項、第 116 項を参照

[15] 第 29 条作業部会は*「体系的（systematic）」*とは下記の 1 つ以上に当てはまることを意味するものと解釈する（データ保護責任者に関する第 29 条作業部会ガイドライン 16/EN WP 243 を参照）。

- システムに応じて発生
- 事前に整備され、組織化され、または系統的である
- データ収集のための一般的な計画の一部として行われる
- 戦略の一部として実行される

第 29 条作業部会は*「一般の人々がアクセス可能な場所（publicly accessible area）」*とは、広場、ショッピングセンター、通り、市場、鉄道の駅、公共図書館など、一般市民に公開されている場所であると解釈する。

集される可能性があるため、基準に該当する。さらに、頻繁に公開される（または公開されている）場所では、個人がそのような処理を受けることを避けるのは不可能である可能性がある。

4. センシティブデータまたは高度に個人的な性質のデータ：これには第9 条に定義されている個人的なデータのカテゴリーが含まれ（例えば、個人の政治的意見についての情報など）、また第 10 条に定義されている有罪歴と犯罪行為に関係する個人データも含まれる。一例としては、患者の医療記録を保管している総合病院、または犯罪者の詳細情報を保管している民間調査会社である。このような GDPR の規定に留まらず、データの一部のカテゴリーは、個人の権利と自由に対するリスクの可能性を高めるものとみなすことができる。これらの個人データはセンシティブ（この用語は一般に理解されている意味で使用されている）とみなされる。その理由は、家庭や私的な活動（機密性を保護すべき電子通信など）に関係しているか、基本的な権利（その収集が移動の自由に対する問題となりかねない位置データなど）の行使に影響を与えるか、または機密扱いに違反する行為が明らかにデータ主体の日常生活に深刻な影響（詐欺のために使用されるかもしれない財務データなど）を与える可能性を含んでいるためである。この点で、データが既にデータ主体または第三者によって公に利用可能にされているかどうかは関係がある。個人データが公に利用可能であるという事実は、そのデータが特定の目的のためにさらに使用されることが予想される場合、評価に関する要素とみなされる可能性がある。この基準には、私的文書、電子メール、日記、注釈機能を備えた電子リーダーからの注釈、及びライフログ・アプリケーションに含まれる高度に個人的な情報などのデータも含まれ得る。
5. 大規模なデータ処理：GDPR では大規模であることの構成要件を定義しない。しかし、前文第 91 項にいくつかの指針が記載されている。いずれにせよ、第 29 条作業部会は、処理が大規模に実施されるかどうかを決定する際に、特に以下の要素を考慮するよう勧告する [16]。
    a. 対象となるデータ主体の数（具体的な数、または関連するデータ母集団に占める割合の両方）
    b. 処理されるデータの量、及び／または異なるデータ項目の範囲
    c. データ処理活動の持続時間、または永続性
    d. 処理活動の地理的範囲
6. 照合または結合されたデータセット：
   データ主体の合理的な期待を超える方法で異なる目的や異なるデータ管理者によって実行された2つ以上のデータ処理業務により生成されたデータセットを対象にする場合など[17]。
7. 脆弱なデータ主体に関するデータ（前文第 75 項）：この種のデータの処理は、データ主体とデータ管理者との間の力関係の不均衡増大を理由として、一つの基準となる。つまり、個人がデータの処理に容易に同意または反対したり、権利を行使できない可能性があることを意味する。脆弱なデータ主体には、次のものが含まれる。子供（彼らは自己のデータ処理の内容を理解し、かつ思慮深くデータの処理に反対または同意することができないとみなすことができる）、従業員、特別な保護を必要とするより脆弱な層に属する人々（精神疾患者、亡命希望者、高齢者、患者など）、さらにデータ主体の立場と管理者の関係に不均衡が識別されるいかなる場合もこれに該当する。
8. 技術的または組織的な解決策の革新的な使用または適用：指紋と顔認識を組み合わせて物理的なアクセス制御を改善するなど。GDPR は、「技術的知識の達成状況に従い」（前文第 91 項）定義される新技術の使用により DPIA を実施する必要性が生まれる可能性があることを明確にしている（第 35 条第 1 項及び前文第 89 項、第 91 項）。そのような技術の使用には、個人の権利と自由に対するリスクが高い新たなデータ収

[16] データ保護責任者に関する第 29 条作業部会ガイドライン 16/EN WP 243 を参照。

[17] 目的制限に関する第 29 条作業部会意見 13/EN WP 203、p.24 を参照。

集と使用が関係する可能性があるからである。実際、新しい技術の展開による個人的及び社会的帰結は不明かもしれない。DPIA は、データ管理者がそのようなリスクを理解し、対処するのを支援する。例えば、ある種の「Internet of Things：IOT」のアプリケーションは、個人の日常生活やプライバシーに重大な影響を及ぼす可能性があり、そのために DPIA が必要となる。

9. 処理それ自体が「データ主体が権利を行使したり、サービスまたは契約を使用したりすることを妨げる」（第22条及び前文第91 項）場合。これには、サービスへのデータ主体のアクセスや契約への参加を許可、修正、または拒否することを目的とする処理業務が含まれる。この一例は、銀行が顧客に貸出を行うか否かを決定するために、信用照合データベースに照会して顧客を選別する場合である。

ほとんどの場合、データ管理者は、2つの基準を満たす処理においてはDPIAを実行する必要があると考えることができる。一般的に、第 29 条作業部会は、処理がより多くの基準を満たせば満たすほど、データ主体の権利と自由に高いリスクをもたらし、管理者が採用すると想定する措置にかかわらずDPIAが必要となる可能性が高いと考えている。

しかし場合によっては、**データ管理者は、これらの基準の1つのみを満たす処理においてもDPIAが必要であると考えることができる。**

次の例は、特定の処理業務でDPIAが必要かどうかを判断する基準をどのように使用すべきかを示している。

処理の具体例	関連する可能性のある基準	DPIA が必要となる可能性は高いか？
患者の遺伝子データ、健康データを処理する病院（病院情報システム)	- センシティブデータ及び高度に個人的な性質のデータ - 脆弱なデータ主体に関するデータ - 大規模に処理されたデータ	高い
高速道路上の運転行動を監視するためのカメラシステムの使用。管理者は、高度な処理能力のあるビデオ分析システムを車の特定及びナンバープレートの自動識別を行うために使用することを想定している。	- 体系的な監視 - 技術的または組織的な解決策を革新的に使用または適用	
従業員のオフィス、インターネット上の活動の監視など、従業員の活動を監視する企業	- 体系的な監視 - 脆弱なデータ主体に関するデータ	
プロフィールを作成するために公開されているソーシャルメディアデータの収集	- 評価またはスコアリング - 大規模に処理されたデータ - データセットの照合と結合 - センシティブデータまたは高度に個人的な性質のデータ	
国レベルの信用格付けまたは詐欺データベースを作成する機関	- 評価またはスコアリング - 法的または類似の重要な効果を伴う自動化された決定 - データ主体の権利行使や、サービスの使用や契約締結の防止	

	- センシティブデータまたは非常に個人的な性質のデータ	
研究プロジェクトや臨床試験の脆弱なデータ主体に関する　　仮名化された個人的な機密データのアーカイブ目的での保存	- センシティブデータ - 脆弱なデータ主体に関するデータ - データ主体の権利行使や、サービスの使用や契約締結の防止	

処理の具体例	関連する可能性のある基準	DPIA が必要となる可能性は高いか？
「個々の医師、他の医療専門家または弁護士による患者または顧客からの個人データ」（前文第 91 項）の処理	- センシティブデータもしくは高度に個人的な性質のデータ - 脆弱なデータ主体に関するデータ	高いとはいえない
メーリングリストを使って一般的な日々のダイジェストを購読者に送信するオンラインマガジン	- 大規模に処理されたデータ	
ウェブサイトでの過去の購入履歴に基づいて行われる限定的なプロファイリングを含むヴィンテージカー部品の広告を表示する e コマースウェブサイト	- 評価またはスコアリング	

逆に、処理業務が上記の場合に該当したとしても、管理者が「高いリスクをもたらす可能性が高い」とは考えられないとすることもある。このような場合、管理者はDPIAを実施しない理由を充分な根拠を示し文書化する必要がある。また、文書中にデータ保護責任者の見解を含めて記録する必要がある。

さらに、説明責任原則の一環として、すべてのデータ管理者は*「自らの責任の下で処理活動の記録を保持する」*ものとする。その記録には、特に処理の目的、データのカテゴリーとデータを受領する者の記載、そして*「可能であれば、第 32 条第 1 項に規定する技術的及び組織的セキュリティ保全措置の一般的な記述」*（第 30 条第 1 項）を含む。最終的に DPIA を実施しないと決定したとしても場合も、高いリスクの可能性があるか否かを評価する必要がある。

注：監督機関は、DPIA が必要となる処理業務のリストを確定し、公表し、欧州データ保護会議（European Data Protection Board：EDPB）に報告することが求められている（第 35 条第 4 項）[18]。上記の基準は、監督機関がそのようなリストを作成する一助となる。また、時間の経過と共に、より具体的な内容が追加され潜在的な改善の可能性がある。例えば、あらゆる形式の生体認証データの処理または子供のデータの処理は、第 35 条第 4 項に基づくリストの作成に関連するものとみなすこともできる。

b) DPIAが不要な場合は？*「高度のリスクをもたらす可能性」*がないデータ処理または同様のDPIA が存在するか、2018 年 5 月以前に承認されているか、法的根拠があるか、または DPIA が不要である処理業務の一覧に含まれているデータ処理。

第 29 条作業部会は、以下の場合にはDPIAは必要ないと考える。

- **その処理が*「自然人の権利と自由に高いリスクをもたらす可能性が高く」*（第35条第1項）ない場合**
- **処理の性質、範囲、文脈及び目的がDPIAが実施された処理に非常に類似している場合。**そのような場合には、類似処理のDPIAの結果を使用することができる（第35条第1項）[19]。
- 処理業務が、変更されていない特定の条件で2018年5月以前に監督機関によってチェックされた場合[20]（III.C参照）。
- **処理業務が、**第6条第1 項の(c)または(e)に従い、EU または加盟国の法律に**法的根拠を有する場合、**法律が特定の処理作業を規制し、かつ、**DPIA が法的根拠の確立の一環として既に実施されている場合**（第 35 条第 10 項）[21]。ただし、加盟国が処理活動に先立ちDPIAを行う必要があると述べた場合を除く。
- **DPIA が要求されない処理業務のオプションリスト（監督機関によって制定）に当該処理が含まれている場合**（第 35 条第 5 項）。そのようなリストには、特にガイドライン、特定の決定または認可、遵守規則などを通じて、この当局によって指定された条件に適合する処理活動を含むことができる（例えば、フランスでは、認可、免除、簡略化されたルール、コンプライアンスパック…）。そのような場合、管轄監督機関による再評価を条件に、DPIA は必須ではない。ただし、処理がリストに記載された関連する手順の範囲内に厳密に該当し、関連する GPDR のすべての要件を完全に遵守し続ける場合に限る。

C. 既存の処理業務に関してはどのように対応するか？DPIAが必要となる場合もある

DPIA を実施する要件は、自然人の権利と自由に高いリスクをもたらすような既存の処理業務に対しては、処理の性質、範囲、文脈及び目的を考慮に入れた上で、リスクの変化が生じている処理業務に適用される。

指令95/46/ECの第20 条に従い、監督機関またはデータ保護責任者によって確認作業が実施されており、かつ前回の確認作業以来運用方法が変更されていない処理業務については DPIA の実施は不要である。実際、*「指令 95/46/EC に基づきなされた監督機関による許可及び採択された委員会の決定は、修正、置き換え、または廃止されるまで有効である」*（前文第 171 項）。

---

[18] その状況において、*「管轄監督機関は第 63 条で定める一貫性メカニズムを適用させなければならない。ただし、当該一覧が複数の加盟国におけるデータ主体への商品若しくはサービスの提供、若しくはデータ主体の行動の監視に関わる取扱い活動を含むものであるか、または EU 内の個人データの自由な移動に実質的に影響を与えかねない場合に限る」*（第 35 条第 6 項）。

[19] *「単独の評価は、同様の高リスクを示す同様の処理業務の集合に用いることができる。」*

[20]「95/46/EC 指令に基づきなされた監督機関による許可及び採択された委員会決定は、修正、置き換え、または廃止されるまで引き続き有効である」（前文第 171 項）。

[21] 処理のための根拠法策定の段階でDPIAが実施された場合は、採用された根拠法が提案と異なる可能性があるため、運用開始前にレビューを要求する可能性があることに注意すること。策定段階の提案内容は、プライバシー及びデータ保護に影響する部分で採用された根拠法と異なる可能性があるためである。さらに、法律の採択時においては、たとえそれがDPIA を伴っていたとしても、実際の処理に関して十分な技術的詳細が得られない場合がある。そのような場合、実際の処理活動を行う前に、個別に DPIA を実施する必要がある可能性がある。

逆に、これは、監督機関またはデータ保護当局による事前の検査を受けたデータ処理業務であっても、その後実装の条件（範囲、目的、収集された個人データ、データ管理者またはデータ受領者の身元、データ保持期間、技術的及び組織的対策など）が変更され、かつ高いリスクのあるデータ処理は、DPIAの対象となるべきであるということを意味する。

さらに、例えば新しい技術の使用、または個人データを異なる目的に使用するなど、処理業務に起因するリスクが変化[22] した後には、DPIAが必要となる可能性がある。データ処理の業務は急速に進化し、新たな脆弱性が生じる可能性がある。したがって、DPIAの改訂は継続的な改善に役立つばかりでなく、変化する環境で長期間にわたってデータ保護のレベルを維持するためにも重要である。例えば、特定の自動化された意思決定の影響がより大きくなったり、新しいカテゴリーのデータ主体が差別に対して脆弱になるなど、処理活動の組織的または社会的な文脈が変化したために、DPIAが必要になることもある。

逆に、一定の変化によってリスクも低下する可能性がある。例えば、処理業務が進化して意思決定が自動化されなくなる、または監視活動が体系的でなくなる場合などである。その場合、リスク分析の見直しにより、DPIAの実施がもはや必要ないと判明することもある。グッドプラクティスとして、**DPIAは継続的に見直され、定期的に再評価されるべきである**。したがって、2018年5月25日時点でDPIAの実施が必須ではない場合でも、適切な時期に、管理者の一般的な説明責任の一部としてDPIA を実施する必要が生じるだろう。

D. DPIAの実施方法は？

a）DPIAを実施すべき時期はいつか？処理開始前である。

DPIA は「処理開始前に」実施すべきである（第 35 条第 1 項、第 10 項、前文第 90 項及び第 93 項）[23]。これは、バイデザイン・バイデフォルトの原則によるデータ保護に合致する（第 25 条及び前文第 78 項）。DPIA は、処理に関連する意思決定を助けるためのツールと見なされるべきである。

DPIAは、いくつかの処理業務に未確定部分があっても、処理業務の設計において可能な限り早く開始するのが実際的である。プロジェクトのライフサイクルを通じて DPIA を更新することで、データ保護とプライバシーが考慮され、コンプライアンスを推進するソリューションの作成が促進される。特定の技術的または組織的手段の選択が、処理がもたらすリスクの重大性または可能性に影響することがあるため、開発プロセスの進行に応じて、評価の個々のステップを繰り返す必要がある場合もある。

処理が実際に開始される際に DPIA を更新する必要があるかもしれないという事実は、DPIA を延期するまたは実施しない正当な理由とはならない。DPIA は継続的なプロセスである。特に、処理業務が動的で継続的に変更が必要な場合はこの傾向が顕著である。**DPIA を実施することは、継続的なプロセスであり、1 回だけ実施すればよいというものではない。**

[22] 状況、収集されたデータ、目的、機能、処理された個人データ、受信者、データの結合、リスク（記録媒体、リスク源、潜在的な影響、脅威など）、セキュリティ対策及び域外への移転の観点から。

[23] 監督機関によって事前にチェックされている既存の処理である場合を除き、重大な変更を行う前に DPIA を実施する必要がある。

b) DPIA の実施責任者は？データ管理者が、データ保護責任者及びデータ処理者とともに責任を負う。

管理者は、DPIAを確実に実施することに責任を負う（第35条第2項）。DPIAを実際に行うのはその組織内外の担当者でもよいが、管理者はこの任務に対して最終的に責任を負う。
管理者は、データ保護責任者（DPO）を任命しているならば、その助言を求める必要がある（第 35 条第 2 項）。得られた助言と管理者による決定は DPIA の一環として文書化すべきである。また、DPO は DPIA の実施状況を監督すべきである（第 39 条第 1 項（c））。詳細な指針は、データ保護責任者に関する第 29 条作業部会ガイドライン 16/EN WP 243 で説明されている。

処理がデータ処理者によってすべてまたは部分的に実行される場合、**処理者は DPIA を実行する際に管理者を支援し、**（第 28 条第 3 項(f)に従い）必要な情報を提供する必要がある。

管理者は*「適切な場合」*には「*データ主体またはその代表に意見を求める*」（第35条第9項）必要がある。第 29 条作業部会は次のように考える。

- 管理者がそのような意見を求めることに関わる個人データを処理するための合法的な基盤を確実に有するならば、これらの意見は、状況に応じてさまざまな手段（例えば、処理作業の目的と手段に関する内外の一般的研究、社員代表への質問、またはデータ管理者の将来の顧客に対する通常のアンケート調査）により得ることができる。ただし、処理に対する同意は明らかにデータ主体の意見を求める方法ではないことに注意すべきである。
- もし、データ管理者の最終決定がデータ主体の見解と異なる場合は、処理を進めるか否かの理由を文書化すべきである。
- 管理者は、データ主体の見解を求めることが適切でないと判断した場合（例：これにより企業の事業計画の機密性を傷つけたり、またはかかる行為が不当であったり実行不可能である場合）には、その正当性を文書化すべきである。

最後に、社内の基本方針、手続き、規則などに応じて、他の特定の役割と責任を定義し文書化するのはグッドプラクティスである。

- 特定の事業部門がDPIAの実施を提案する場合、その部門はDPIAに情報を提供し、検証プロセスに関与するべきである。
- 必要に応じて、異なる専門領域の独立した専門家[24]（弁護士、技術者、セキュリティ専門家、社会学者、倫理学者など）から助言を求めることが推奨される。
- 処理者の役割と責任は契約にて定めなければならない。DPIAは、処理の性質と処理者が利用できる情報を考慮して、処理者の支援を受けて実施しなければならない（第28条第3項（f））。
- 最高情報セキュリティ責任者（Chief Information Security Officer：CISO）が任命されている場合は、データ処理責任者（DPO）と同様に、管理者が特定の処理業務でDPIAを実施するよう提案することができ、実施方法に関して関係者を支援し、リスク評価の質を評価し、残存リスクが許容可能かどうかを評価し、データ管理者の置かれた個別の状況に対する見識を高めることに貢献すべきである。
- 最高情報セキュリティ責任者（任命されている場合）及び/またはIT部門は管理者に支援を提供すべきであり、セキュリティまたは運用上のニーズに応じて特定の処理業務でDPIAを実施するように提案することができる。

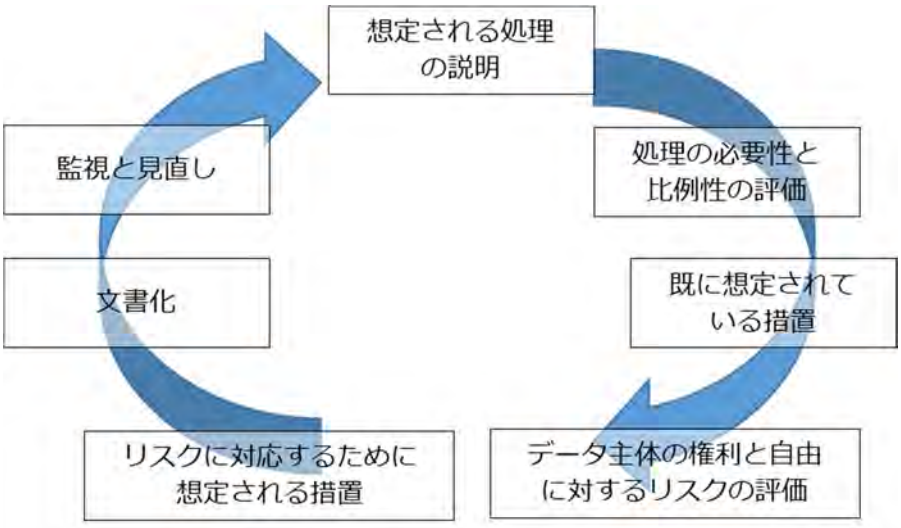
[24] *欧州連合（EU）のプライバシー影響評価枠組みのための勧告、成果物D3*
http://www.piafproject.eu/ref/PIAF_D3_final.pdf.。

c）DPIA の実施の手法とは何か？場合により手法は異なるが共通の基準はある

GDPR は、DPIAの最低限の機能について定めている（第35条第7項、前文第 84 項及び第 90 項）。

- *「想定された処理業務及び処理の目的の記述」*
- *「処理の必要性及び比例性の評価」*
- *「データ主体の権利及び自由に関するリスク評価」*
- *次の目的のために「想定された対策」*
    - *「リスクに対処するため」*
    - *「本規則（GDPR）の遵守を証明するため」*

次の図は、DPIA[25]を実行するための包括的な反復プロセスを示している。



データ処理業務の影響を評価する際には、行動規範（第 40 条）の遵守が考慮されなければならない（第 35 条第 8 項）。これは、行動規範が処理作業に対して適当であれば、適切な措置が選択または実施されていることを実証するのに有用と考えられる。管理者と処理者が処理業務にかかる GDPR の遵守（第 42 条）及び拘束的企業準則（Binding Corporate Rule：BCR）の遵守を示すための認証証明、認証シール及び認証マークも考慮する必要がある。

GDPR に記載されている関連する要件は、すべて DPIA の設計と実施のための幅広い一般的な枠組みを提供している。DPIA の実際の実施は、GDPR で定められた要件に依存し、より詳細な実践的指針により補足される。このように、DPIA の実施は拡張性がある。つまり、小規模システムのデータ管理者であっても、処理業務に適した DPIA を設計して実施することができる。

GDPR の前文第 90 項は、明確に定義されているリスク管理の構成要素（例えば、ISO31000[26]）と重複する DPIA のいくつかの構成要素について概説している。リスク管理上、DPIA は以下の 3 つのプロセスを使用して自然人の権利と自由に対する「*リスクを管理する*」ことを目標とすることになる。

[25] ここに描かれているプロセスは反復的であることを強調しておかなければならない。実際、DPIA が完了する前に各ステージが複数回実施される可能性が高い。

[26] リスクマネジメントプロセス：コミュニケーションと協議、状況の特定、リスク評価、リスクへの対処、モニタリング及びレビュー（用語と定義、及び目次は、ISO31000 プレビュー参照：https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-1:v1:en）。

- 状況の特定：「処理の性質、範囲、文脈及び目的、及びリスク源を考慮に入れる」。
- リスク評価：*「高リスクが起こる可能性と重大性を評価する」*。
- リスクの対処:「当該リスクの軽減」と「個人データの保護の確保」と「この規則（GDPR）の遵守の実証」。

注：GDPR に基づく DPIA は、データ主体の権利に対するリスクを管理するためのツールであるため、特定の分野（例えば、社会的セキュリティ）の場合のように、データ主体の視点を取る。一方、他の分野（例えば、情報セキュリティ）のリスク管理は組織に焦点を当てている。

GDPR は、DPIA が既存の作業手順に適合するように、データ管理者に DPIA の正確な構造と形態を決定する柔軟性を許している。前文第 90 項で説明されている構成要素を考慮した複数の異なるプロセスが、EU 内及び世界各地で制定されている。しかし、どのような構造、方法で実施するのであれ、DPIA は管理者がリスクに対処する対策を講ずることができる真のリスク評価でなければならない。

GDPRに示されている基本的な要件の実施を支援するために、さまざまな方法論（データ保護及びプライバシー影響評価手法の例については付録 1を参照）を使用することができる。管理者がGDPRを遵守できるようにする一方で、これらの異なるアプローチを使用できるようにするために、共通の基準が特定されている（付録2参照）。この基準は、GDPR の基本要件を明確にしているが、さまざまな実施形態を可能とする十分な範囲（enough scope）を提供する。

この基準は、特定の DPIA 実施方法が GDPR の要求する基準を満たしていることを示すために使用できる。**方法論を選択するのはデータ管理者の責任であるが、この方法論は付録 2 の基準に準拠していなければならない。**

第 29 条作業部会は、分野固有の DPIA の枠組みの開発を奨励している。この理由は、特定の分野別知識を当てはめることができるためである。つまり、DPIA は対象とすべき処理業務の特性（例：特定の種類のデータ、企業資産、潜在的な影響、脅威、措置）に言及することができる。これは、DPIA が特定の分野で、または特定の技術を使用したり、特定の種類の処理業務を行ったりするときに発生する問題に対処できることを意味する。

最後に、必要に応じて、*「管理者は、少なくとも処理業務によって生じるリスク変化がある場合、データ保護影響評価に従って取扱いが実行されているか評価の見直しを実行しなければならない」*（第35条第11項[27]）。

d) DPIA を公開する義務はあるか？いいえ、ない。しかし要約を公開することは信頼醸成に役立つ。また、事前の協議を行わなければならない場合、またはデータ保護機関（DPA）により要求された場合、DPIA 全体を監督機関に報告する必要がある

DPIA の公開は、GDPR の法的要件ではなく、管理者の決定に委ねられる。しかし、データ管理者は DPIA の要約や結論など、少なくとも DPIA の一部を公開することを検討するべきである。

[27] 第 35 条第 10 項は、第 35 条の第 1 項から第 7 項の適用のみを明示的に除外する。

このような手順を踏む目的は、管理者の処理業務に対する信頼の醸成、及び説明責任と透明性を証明することである。一般市民が処理業務の影響を受ける DPIA を公開することは特にグッドプラクティスである。特に、これに該当するのが、公的機関が DPIA を実施する場合である。

DPIAを公開する場合には評価結果全体を公開する必要はなく、特にDPIAにデータ管理者のセキュリティリスクに関する特定の情報、企業秘密や商業上の機微に触れる情報が含まれている場合は、この部分を公開する必要はない。このような状況では、公開されたバージョンは、DPIAの主な調査結果の要約、またはDPIAが実行されたという声明だけで構成されていることも許容される。

さらに、DPIAの結果、高い残存リスクがあると判明した場合、データ管理者は、監督機関とその処理に関する協議を事前に行う必要がある（第36条第1項）。その一環として、DPIA の内容はすべて提供される必要がある（第36条第3項（e））。監督機関は勧告[28]をすることができるが、公式文書への公的アクセスに関する各加盟国の適用原則に従い、企業の秘密を危うくすることはなく、またセキュリティの脆弱性を明らかにすることもない。

E. <u>いつ監督機関と協議するべきか？残存リスクが高い場合</u>

前述の通り、次のことが言える。

- DPIA は、処理業務が「自然人の権利と自由に対して、高リスクを生じさせる可能性がある」場合に必要となる（第 35 条第 1 項、III.B.a 参照）一例として、大規模な健康データの処理は、リスクが高くなる可能性が高いと考えられ、DPIA が必要となる。
- さらに、データ主体の権利と自由に対するリスクを評価し、そのリスクを許容レベルまで下げ、GDPRに準拠していることを示す措置[29]を特定するのはデータ管理者の責任である（第35条第7項、III.C.c参照）。例としては、既存の方針（通知、同意、アクセス権、異議を唱える権利）に加えて、適切な技術的及び組織的セキュリティ措置（効果的なフルディスク暗号化、堅牢な鍵管理、適切なアクセス制御、安全なバックアップなど）を備えたノート PC 上の個人データの保管がある。

上記のノート PCの例では、リスクは適切なレベルまで低減したとデータ管理者が考える場合、第36条第1項及び前文第 84 項及び第 94 項の解釈に従えば、監督機関と協議することなしに処理を進めることができる。特定されたリスクがデータ管理者によって十分に対処できない（すなわち、残存リスクが高いままである）場合、データ管理者は監督機関と協議しなければならない。

許容できない高い残存リスクの例には、データ主体が克服できない重大な、または不可逆的な結果に遭遇する可能性がある場合（例えば、データ主体の生命の危険、解雇、破産につながるデータへの不正なアクセスなど）、及び/またはリスクが発生することが明らかである場合

[28] 想定された処理は第 36 条第 2 項の規定を遵守していないという意見を監督機関がもつ場合にのみ、管理者への書面による勧告が必要である。

[29] EDPB及び監督機関からの既存の指針を考慮し、第35条第1項に規定される最新技術及び実施コストを考慮に入れることを含む。

（例えば、データの共有、使用、配布方式のため、データにアクセスする人数を減らすことができないことによるリスクの発生、または、既知の脆弱性が修正されていない場合など）が含まれる。

データ管理者がリスクを許容できるレベルに低減する十分な措置を見つけることができない場合（すなわち、残存リスクが依然として高い場合）、監督機関との協議が必要となる[30]。

さらに、加盟国の国内法が、治安または公衆衛生に関する処理を含め、公共の利益において管理者によってなされる業務の遂行のための管理者による処理に関して、管理者に監督機関と協議すること及び／または監督機関から事前に認可を得ることを要求する場合はいつでも、管理者は監督機関に諮問する必要がある（第36条第5項）。

ただし、残存リスクの水準に基づいて監督機関への諮問が必要かどうかに関わらず、DPIAの記録を保持し、DPIAを更新する義務が当然ながらあることは銘記すべきである。

Ⅳ. 結論と推奨事項

DPIAは、データ管理者がGDPRに準拠したデータ処理システムを実装するための有用な方法であり、一部の種類の処理業務では必須となり得る。これは実施規模の柔軟性があり、さまざまな形態をとることができるが、GDPRは有効なDPIAの基本要件を定めている。データ管理者は、法的遵守を支援する有用かつ積極的な活動として、DPIAの実施を認識すべきである。

第24条第1項は、GDPRの遵守の観点から管理者の基本的な責任を定めている。*「処理の性質、範囲、文脈及び目的並びに自然人の権利及び自由に関するリスクの様々な可能性及び重大性を考慮し、管理者は本規則に従って処理が実行されていることを保証及び証明するため適切な技術的及び組織的対策を実施しなければならない。これら対策は見直され、必要に応じて更新されなければならない。」*

DPIAは、リスクの高いデータ処理が計画されている、または実施されている場合、GDPRを遵守するための重要な部分である。つまり、データ管理者は、本ガイドラインに記載されている基準を使用して、DPIAを実行する必要があるかどうかを判断する必要がある。データ管理者社内方針は、GDPRの法的要件を超えて基準を拡張するこができる。これにより、データ主体及び他のデータ管理者からの信頼及び信用が向上するはずである。

リスクの高い処理が計画されている場合、データ管理者は次の作業を行う必要がある。

- 付録 2の基準を満たすDPIA 手法（付録 1に示されている例）を選択するか、以下のような体系的なDPIAプロセスを特定し実施する。
  - 付録 2の基準に準拠していること。
  - 内部的なプロセス、状況、文化に応じて既存の設計、開発、変更、リスク、運用の見直しプロセスに統合されている。

[30] 注：「個人データの仮名化と暗号化」（ならびにデータの最小化、監視メカニズムなど）は、必ずしも適切な措置ではない。これは例にすぎない。適切な措置は、処理業務に固有の状況とリスクに依存する。

    - 適切な利害関係者（管理者、DPO、データ主体またはその代表者、ビジネス、技術サービス、処理者、情報セキュリティ担当者など）を関与させ、その責任を明確に定義すること。
- 管轄監督機関にDPIA報告書を提出する必要がある場合は、それを実施する。
- 高いリスクを軽減するための十分な措置を決定できなかった場合は監督機関と協議する。
- DPIAとそれが評価する処理を定期的に見直す。少なくとも操作を処理することによってもたらされるリスクに変化がある場合は、見直しを実施する。
- 決定事項を文書化する。

付録 1 - 既存の EU の DPIA の枠組みの例

GDPRは、どのDPIAプロセスに従わなければならないのかを指定するのではなく、データ管理者が既存の作業実務を補完する枠組みを導入することを可能にする。ただし、その枠組みが第35条第7項に記載された構成要素を考慮していることを条件とする。このような枠組みは、データ管理者に特有のものでもよく、特定の業界で共通のものでもよい。EU DPA が策定し、過去に公開したフレームワークと、EUの分野別のフレームワークの例を示す。（ただし、以下のみに限定するものではない）

一般的な EU のフレームワークの例

- ドイツ: 標準データ保護モデル、V.1.0 – 試行版、2016[31]（DE: Standard Data Protection Model, V.1.0 – Trial version, 2016[31]）https://www.datenschutzzentrum.de/uploads/sdm/SDM-Methodology_V1.0.pdf
- スペイン: *Guía para una Evaluación de Impacto en la Protección de Datos Personales (EIPD)*, Agencia española de protección de datos (AGPD), 2014. https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/Guia_EIPD.pdf
  （ジェトロ注：現在リンクが切れており、AGPD サイト内ではガイドラインが見つけられない。AGPD ウェブサイトはこちら：https://www.aepd.es/index.html）
- フランス: プライバシー影響評価（Privacy Impact Assessment : PIA）（FR: *Privacy Impact Assessment (PIA)*）, Commission nationale de l'informatique et des libertés (CNIL), https://www.cnil.fr/en/cnil-publishes-update-its-pia-guides
- 英国: プライバシー影響評価の実施基準、情報コミッショナーオフィス（Information Commissioner's Office : ICO）、2014（UK: *Conducting privacy impact assessments code of practice*, Information Commissioner's Office (ICO), 2014）
  https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf

次に EU の分野別のフレームワークの例を示す。

- RFIDアプリケーションのプライバシーとデータ保護の影響評価の枠組[32]（Privacy and Data Protection Impact Assessment Framework for RFID Applications[32]）
  https://ec.europa.eu/digital-single-market/en/news/privacy-and-data-protection-impact-assessment-framework-rfid-applications
- スマートグリッドやスマートメーターシステムのためのデータ保護影響評価テンプレート[33]（Data Protection Impact Assessment Template for Smart Grid and Smart Metering systems[33]）http://ec.europa.eu/energy/sites/ener/files/documents/2014_dpia_smart_grids_forces.pdf

国際規格は、DPIAを実施するために使用される方法論のためのガイドライン（ISO/IEC 29134[34]）も提供する予定である。

[31]2016年11月9～10日にKühlungsborn で開催された第 92 回連邦及び州独立データ保護機関会議でバイエルンの棄権の下、満場一致で肯定的に認められた。

[32]次の文書も参照。

- RFIDによってサポートされるアプリケーションにおけるプライバシー及びデータ保護の原則の実施に関する2009年5月12日の欧州委員会勧告（Commission Recommendation of 12 May 2009 on the implementation of privacy and data protection principles in applications supported by radio- frequency identification）
  https://ec.europa.eu/digital-single-market/en/news/commission-recommendation-12-may-2009- implementation-privacy-and-data-protection-principles
- RFIDアプリケーションのためのプライバシーとデータ保護の影響評価フレームワークの改訂された業界提案に関する意見9/2011（Opinion 9/2011 on the revised Industry Proposal for a Privacy and Data Protection Impact Assessment Framework for RFID Applications）
  http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp180_en.pdf

[33]委員会のスマートグリッドタスクフォースの専門家グループ2が作成したスマートグリッド及びスマートメータリングシステム（「DPIAテンプレート」）のデータ保護影響評価テンプレートに関する意見07/2013（the Opinion 07/2013 on the Data Protection Impact Assessment Template for Smart Grid and Smart Metering Systems ('DPIA Template') prepared by Expert Group 2 of the Commission's Smart Grid Task Force）も参照。http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion- recommendation/files/2013/wp209_en.pdf

[34]ISO/IEC 29134（プロジェクト）、*情報技術 - セキュリティ技術 - プライバシー影響評価 - 国際標準化機構（ISO）のガイドライン*（ISO/IEC 29134 (project), *Information technology – Security techniques – Privacy impact assessment –Guidelines*, International Organization for Standardization (ISO)）

付録 2 - 許容できる DPIA の基準

第 29 条作業部会は、データ管理者が DPIA、または DPIA を実施する手法が GDPR に準拠するために十分に包括的であるかどうかを評価する際に使用できる以下の基準を提案している。

- ☐ 処理の体系的な記述が提供されている（第35条第7項（a））：
  - ☐ 処理の性質、範囲、文脈及び目的が考慮されている（前文第 90 項）。
  - ☐ 個人データ、データ取得者及び個人データの保管期間が記録されている。
  - ☐ 処理業務の機能記述が提供されている。
  - ☐ 個人データが依存する資産（ハードウェア、ソフトウェア、ネットワーク、人、書類または書類の送付経路）が特定されている。
  - ☐ 承認された行動規範の遵守が考慮されている（第35条第8項）。
- ☐ 必要性と比例性が評価されている（第35条第7項（b））：
  - ☐ 以下の事項を考慮して、規則を遵守すると考えられる措置が決定される（第35条第7項（d）及び前文第 90 項）。
    - ☐ 処理の比例性と必要性に寄与する措置を以下に基づき決定している。
      - ☐ 特定された明示的かつ合法的な目的（第5条第1項（b））
      - ☐ 処理の適法性（第6条）
      - ☐ 適切であり、関連性があり、必要なデータに限定されている（第5条第1項（c））
      - ☐ 保管期間の制限（第5 条第 1 項（e））
    - ☐ データ主体の権利に寄与する措置
      - ☐ データ主体に提供される情報（第12 条、第 13 条、第 14 条）
      - ☐ アクセス権とデータポータビリティーの権利（第15 条及び第20条）
      - ☐ 是正及び消去の権利（第16 条、第 17 条及び第 19 条）
      - ☐ 処理に反対する権利と処理を制限する権利(第 18 条､第 19 条、第 21 条）
      - ☐ 処理者との関係（第28条）
      - ☐ 国際移転に関する安全対策（第V章）
      - ☐ 事前の協議（第36条）
- ☐ データ主体の権利と自由に対するリスクが管理されている（第35 条第 7 項（c））：
  - ☐ 各リスク（不正アクセス、望ましくない変更、及びデータの消失）に関して、データ主体の観点から、リスクの起源、性質、特殊性及び重大性が評価されている（前文第 84 項参照）。
    - ☐ リスク源が考慮されている（前文第 90 項）。
    - ☐ 不正なアクセス、望ましくないデータの変更や消失を含んだ事象の場合に、データ主体の権利と自由に対する潜在的な影響が特定されている。
    - ☐ 不正なアクセス、データの望ましくない変更や消滅につながる可能性のある脅威が特定されている。
    - ☐ 可能性と重大性が推定されている（前文第 90 項）
  - ☐ それらのリスクを処理するために想定される措置が決定されている（第35 条第 7 項（d）及び前文第 90 項）。
- ☐ 利害関係者が関与している。

☐ DPO の助言が求められている（第 35 条第 2項）。

☐ データ主体またはその代表者の意見が求められる（適切な場合）（第35 条第 9項）

作成者　日本貿易振興機構（ジェトロ）海外調査部　欧州ロシア CIS 課

〒107-6006　東京都港区赤坂 1 丁目 12 番 32 号

Tel. 03-3582-5569