JEITA

IS－12－情シ－4

EU データ保護指令改定に関する調査・分析
報告書

2012 年 3 月

一般社団法人　電子情報技術産業協会

情報政策委員会

目　次

はじめに

1995 年に採択された「EU データ保護指令」（正式名称は、「個人データ取扱いに係る個人の保護及び当該データの自由な移動に関する 1995 年 10 月 24 日の欧州議会及び理事会の 95／46／EC 指令」）は、EU 加盟国及び EEA（欧州経済領域）加盟国合計 30 ヶ国に対して同指令に基づく国内法規を要求するものであり、また、EU 域外の国に対してもデータ移転に当たって「十分なレベル」の個人データ保護を要請するものであるため、個人情報保護の分野では極めて影響力の強いフレームワークである。我が国の個人情報保護法及びプライバシーマーク制度も、EU データ保護指令の影響を受けて制定されている。

今般、2 年以上の検討及びコンサルテーション期間を経て、EU データ保護指令が改定され、新たに EU データ保護規則（Regulation）（「個人データ取扱いに係る個人の保護及び当該データの自由な移動に関する欧州議会及び理事会の規則」）として採択される見込みである。今回の改定は、従来の指令の採択から 15 年以上が経ち、インターネットを初めとする急速な技術的進歩やグローバル化の進展によって発生してきた新たな課題に対処するためのものである。具体的には、クラウドコンピューティング（EU 域外へのアウトソーシング）やソーシャルネットワーキングサービスにおけるデータ保護のあり方、多国籍企業のビジネスに過度な負担をかけるような非効率・非整合的な規制の改善等が課題となっていた。欧州委員会は 2012 年 1 月 25 日に改定案を公表し、今後、欧州議会及び欧州連合理事会と緊密に協力して、2012 年内の合意を目指している。

今回の EU データ保護指令改定では、EU 域内の事業者に対する義務の追加、EU 域外の事業者（EU 市民対象のサービスを提供する場合）に対する義務の新設、個人に対する「忘れられる権利」や「データ・ポータビリティ」の権利の新たな付与など、規制が強化された側面が大きい。他方で、EU 域内から域外への国際データ移転のための手続きを簡素化するなど、規制が緩和された側面もある。これらの観点も含め、EU データ保護指令の改定が日本企業の事業環境に与える影響は少なくないと考えられる。そこで、情報政策委員会では、国際社会経済研究所(IISE)に調査を委託し改定内容の分析を行い、今回の改定による日本企業にとっての問題点・課題を整理した。今後、この整理をもとに、日本企業としての対応を検討していきたいと考えている。

１．EU データ保護指令改定の背景と個別論点の整理

１．１　改定の背景と経緯

今回の EU データ保護指令（以下、EU 指令という）改定は、従来の EU 指令の採択から 15 年以上が経ち、インターネットを初めとする急速な技術的進歩やグローバル化の進展によって発生してきた、以下のような新たな課題に対処するためのものである。

ただし、個人の基本的人権と自由を保護すると共に、個人データの自由な流通を促進する、という 1995 年指令当初からの目的は不変とされている。

EU のデータ保護スキームを巡る課題

① 急速な ICT 技術の進歩とグローバル化の進展と、それによる個人データ保護に対するリスクの拡大

- クラウドコンピューティングに代表される国境を越えたデータ流通の増大
- SNS など、個人データの公開・共有化の拡大
- 行動ターゲティング広告、GPS 携帯電話など、個人データ収集手段の高度化

② 現行のデータ保護スキームに対する企業の不満の増大

- 多国籍企業にとって負担が大きい非効率・非整合的な規制の緩和要求の増大
  - 従来、多国籍企業は各加盟国ごとに異なる国内法や、各国の監督機関の決定を　遵守する必要があった。
  - 管理者は原則として全てのデータ処理内容を監督機関に通知する義務があった。
  - BCR（拘束的企業準則）の承認には少なくとも 3 つの監督機関のレビューが必要だった。

これらの課題に対して既存の EU 指令が適切に対処できるかを検討するために、欧州委員会は 2009 年 5 月に EU 指令の見直しを初め、2 回のパブリックコンサルテーションを実施（2009 年 7 月～12 月、2010 年 11 月～2011 年 1 月）した。

- 2009 年 7 月 9 日から 12 月 31 日までの「個人データ保護の基本的権利のための法的フレームワークに関するコンサルテーション」では、欧州委員会は 168 件の意見を受領し、そのうち 127 件は個人、企業、業界団体からのもの、12 件は公共機関からのものであった。
- 2010 年 11 月 4 日から 2011 年 1 月 15 日までの「EU における個人データ保護に関する欧州委員会の包括的アプローチに関するコンサルテーション」では、欧州委員会は 305 件の意見を受領し、うち 54 件は市民から、31 件は公共機関から、220 件は民間分野、とりわけ業界団体及び NGO からのものであった。

欧州委員会はその後、改定による影響評価（impact assessment）の実施を経て、2012年1月25日に改定案を公表した。欧州委員会は今後、欧州議会及び欧州連合理事会と緊密に協力し、2012年内の合意を目指している。欧州議会による採択から2年後に発効の見込みである。

なお、EUデータ保護指令の改定案は下記2つから成る。

① 「個人データ取扱いに係る個人の保護及び当該データの自由な移動に関する欧州議会及び理事会の規則[1]」（以下、「EUデータ保護規則」又は「EU規則」という）・・・EUにおける一般的なデータ保護のフレームワーク

② 犯罪の防止・捜査・発見・訴追、刑事罰の執行の目的で処理される個人データの保護に関する指令

②については企業活動との関連性が薄いと考えられるため、本報告書では主要な条項を含む①の「EUデータ保護規則」案について記載するものとする。

[1] European Commission, “Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)”
(http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf) 。

１．２　EU データ保護規則案の構成と各条項の概要

１．２．１　EU データ保護規則案の全体構成

EU データ保護規則案の全体構成は、以下のようになっている。

第 1 章　一般的条項（第 1 条～第 4 条）
第 2 章　諸原則（第 5 条～第 10 条）
第 3 章　データ主体の権利
　第 1 節　透明性とモダリティ（第 11 条～第 13 条）
　第 2 節　情報提供と、データへのアクセス（第 14 条～第 15 条）
　第 3 節　訂正と消去（第 16 条～第 17 条）
　第 4 節　異議申立を行う権利、プロファイリング　（第 18 条～第 19 条）
　第 5 節　制限（第 20 条）
第 4 章　管理者と処理者
　第 1 節　一般的義務（第 22 条～第 29 条）
　第 2 節　データセキュリティ（第 30 条～第 32 条）
　第 3 節　データ保護評価と事前オーソライズ（第 33 条～第 34 条）
　第 4 節　データ保護オフィサー（第 35 条～第 37 条）
　第 5 節　行動規範と認証（第 38 条～第 39 条）
第 5 章　個人データの第三国又は国際組織への移転（第 40 条～第 45 条）
第 6 章　独立の監督機関
　第 1 節　独立的な地位（第 46 条～第 50 条）
　第 2 節　任務と権限（第 51 条～第 54 条）
第 7 章　協力と整合性
　第 1 節　協力（第 55 条～第 56 条）
　第 2 節　整合性（第 57 条～第 63 条）
　第 3 節　欧州データ保護評議会（第 64 条～第 72 条）
第 8 章　救済、責任及び制裁（第 73 条～第 79 条）
第 9 章　特定のデータ処理状況に関する条項（第 80 条～第 85 条）
第 10 章　委任法令と実施法令（第 86 条～第 87 条）
第 11 章　最終条項（第 88 条～第 91 条）

１．２．２　各条項の概要

各条項の概要は、以下の通りである[2]。

[2] European Commission, “Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to

第 1 章　一般的条項

第 1 条：本規則の主題と、本規則の 2 つの目的（EU 指令第 1 条に対応）を定義。

第 2 条：本規則の内容的なスコープを規定。

第 3 条：本規則の地域的なスコープを規定。

第 4 条：用語の定義。一部の定義は EU 指令を踏襲しているが、一部については追加要素の補完によって修正、又は新たに導入されている（新たに導入された用語は、「個人データ違反」（2002 年電子プライバシー指令（2009 年の指令 2009/136/EC で修正）に基づく）、「遺伝子データ」、「生体データ」、「健康医療に関するデータ」、「主要な事業所」、「代表者」、「企業」、「企業グループ」、「拘束的企業準則」、「子ども」（子どもの権利に関する国連条約に基づく）、「監督機関」）。また、「同意」の定義では、「あいまいでない」同意との混乱を招く並行性を避け、単一で整合的な同意の定義を行うために、「明示的に」の基準が追加された。

第 2 章　諸原則

第 5 条：個人データ処理に関する諸原則を規定（EU 指令第 6 条に対応）。新たな追加要素は、とりわけ透明性の原則、データ最小化の原則の明確化、及び管理者の包括的責任の設立である。

第 6 条：合法な処理の基準を（EU 指令第 7 条に基づき）規定。

第 7 条：合法な処理のための法的根拠として、同意が有効であることの条件を明確化。

第 8 条：子どもに直接的に提供される情報社会サービスにおける、子どもの個人データの処理の合法性の更なる条件について規定。

第 9 条：特定カテゴリの個人データの処理の一般的禁止と、この一般則の例外（EU 指令第 8 条に基づく）。

第 10 条：管理者は、本規則の条項を遵守する目的のためだけに、データ主体を識別するために追加的な情報を獲得しなくてよいことを明確化。

第 3 章　データ主体の権利

第 1 節　透明性とモダリティ

第 11 条：透明で、アクセス容易で、かつ理解できる管理者の情報提供の義務の導入。

第 12 条：データ主体が権利を行使する手続きの提供を、管理者に義務付け。電子的請求手段を含む。データ主体の請求に対して一定期限内での回答を要件とする。

第 13 条：受領者に関係した権利の提供（EU 指令第 12 条(c)に基づく）。共同管理者や共同

---

the processing of personal data and on the free movement of such data (General Data Protection Regulation)”
(http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf)
の p.7～p.16 に基づく。

処理者を含む全ての受領者に拡大。

第 2 節　情報提供と、データへのアクセス

第 14 条：管理者のデータ主体への情報提供（通知）の義務をさらに規定（EU 指令第 10 条、第 11 条に基づく）。保存期間、苦情申立の権利、国際移転に関する項目、データを収集したソースなど、データ主体への追加的な情報提供項目を規定。同条はさらに、EU 指令 95/46/EC における可能な例外、例えば法令において明示的に記録や開示が規定しされている場合には、そのような義務がないことを維持している。このことは、例えば競争促進機関や、租税機関、社会保障関連サービスによる手続きに適用される。

第 15 条：自己情報にアクセスする権利を提供（EU 指令第 12 条(a)に基づく）。追加的な新たな要素として、保存期間のデータ主体への情報提供、訂正及び消去の権利、苦情申立の権利を規定。

第 3 節　訂正と消去

第 16 条：自己情報を訂正する権利を規定（EU 指令第 12 条(b)に基づく）。

第 17 条：データ主体の忘れられる権利、消去する権利を提供（EU 指令第 12 条(b)における消去する権利を精緻化及び詳細化）。忘れられる権利の条件として、個人データを公開しているような管理者に対し、データ主体の請求があった場合、第三者に当該データへのリンクや、当該データのコピー、複製を消去するように通知することも義務付け。また、「ブロッキング」という曖昧な用語を避け、特定ケースにおいて処理を制限してもらう権利を統合。

第 18 条：データ主体のデータ・ポータビリティの権利を導入。データ・ポータビリティとはすなわち、ある自動処理システムから他の自動処理システムに、管理者に妨害されることなく、データを移転することである。前提条件として、また個人の自己データへのアクセスを改善するために、管理者から自らの個人データを構造化され、通常利用されているフォーマットで入手する権利を提供する。

第 4 節　異議申立を行う権利、プロファイリング

第 19 条：異議申立を行う権利を提供（EU 指令第 14 条に対応、証明の責任や非商業的ダイレクトマーケティングへの適用など、一部修正）。

第 20 条：プロファイリングに基づく評価を受けない権利（自動的な個人の決定に関する EU 指令第 15 条(1)に基づき、修正及び追加的な安全保護措置を含む）。

第 5 節　制限

第 21 条：EU 又は加盟国が、第 5 条にいう諸原則、並びに第 11 条から第 20 条及び第 32 条にいうデータ主体の権利に対する制限を維持したり、導入したりする権限を明確化。（EU

指令第 13 条に基づく。）

第 4 章　管理者と処理者

第 1 節　一般的義務

第 22 条：「説明責任の原則」に関する議論を考慮に入れ、本規則を遵守すること、及び当該遵守について証明することの管理者の責任を記述。遵守を保証するための内部ポリシーやメカニズムの採用方法を含む。

第 23 条：データ保護・バイ・デザイン及びデータ保護・バイ・デフォルトの諸原則から生じるデータ管理者の義務を規定。

第 24 条：共同管理者の責任を明確化。

第 25 条：EU 域内に事業所を持たないが、データ処理活動に本規則が適用される管理者に対する、EU 域内に代表者を指名することの義務付け。

第 26 条：処理者の立場と義務の明確化（一部は EU 指令第 17 条(2)に基づく）。新たな追加要素として、管理者の指示を超えてデータを処理する処理者は、共同管理者とみなされることなど。

第 27 条：管理者と処理者の権限下での処理（EU 指令第 16 条に基づく）。

第 28 条：管理者と処理者が自らの責任で処理に関する文書を維持することの義務を導入。EU 指令第 18 条(1)、第 19 条で要求されている、監督機関への一般的な通知の義務に代わるもの。

第 29 条：管理者及び処理者の、監督機関と協力する義務を明確化。

第 2 節　データセキュリティ

第 30 条：管理者と処理者に処理のセキュリティのために適切な措置をとることを義務付け（EU 指令第 17 条(1)に基づく）。処理者の義務を、管理者との契約に関わりなく、拡大。

第 31 条及び第 32 条：個人データ違反を通知する義務を導入（電子プライバシー指令第 4 条(3)に基づく）。

第 3 節　データ保護評価と事前オーソライズ

第 33 条：リスクのある処理に先立ってデータ保護影響評価を実施する管理者及び処理者の義務を導入

第 34 条：処理に先立ち監督機関のオーソライズ及びコンサルテーションが必要なケース（EU 指令第 20 条の事前評価の概念に基づく）。

第 4 節　データ保護オフィサー

第 35 条：公共部門及び民間部門（大企業等）における義務的なデータ保護オフィサーの導入（EU 指令第 18 条(2)に基づく）。（EU 指令第 18 条(2)は、加盟国が一般的な通知の要件

の代替としてデータ保護オフィサーのような要件を導入する可能性を規定。）
第 36 条：データ保護オフィサーの立場を規定。
第 37 条：データ保護オフィサーの主要な任務を提供。

第 5 節　行動規範と認証

第 38 条：行動規範（EU 指令第 27 条(1)に基づく）。行動規範の内容と手続きを明確化。欧州委員会に行動規範の一般的妥当性について決定する権限を付与。
第 39 条：認証制度やデータ保護シールの設立に関する規定を導入。

第 5 章　個人データの第三国又は国際組織への移転

第 40 条：一般原則として、第三国又は国際組織へのデータ移転の際には本章の義務を遵守することが必須であることを規定。
第 41 条：欧州委員会による十分性の決定の基準・条件・手続き（EU 指令第 25 条に基づく）。欧州委員会による保護のレベルの十分性（又は十分でないこと）の評価の際に考慮しなければならない基準には、明示的な法律上のルール、司法救済、及び独立の監督機関が含まれる。同条はまた、第三国内のある地域やある部門における保護のレベルを欧州委員会が評価できることを明示的に裏付けている。
第 42 条：欧州委員会による十分性の決定がなされていない第三国への移転の要件として、適切な安全管理措置、とりわけ標準契約条項、拘束的企業準則、及び契約条項を提示することを規定。欧州委員会の標準契約条項を利用できることは、EU 指令第 26 条(4)に基づく。新たな要素として、当該標準契約条項は、ある監督機関によって採択され、欧州委員会によって一般的に有効であるとの宣言を受けることも可能である。拘束的企業準則は、法的文脈において明示的に導入された。契約条項のオプションは、管理者又は処理者に一定の柔軟性を与えるものであるが、監督機関による事前のオーソライズを必要とする。
第 43 条：拘束的企業準則（BCR）による移転の条件をさらに詳細に規定。監督機関による現行のプラクティスや要件に基づく。
第 44 条：データ移転の例外事項を明確化（EU 指令第 26 条に基づく）。このことは、とりわけ公共の利益の重要な基盤の保護のために要求され、必要とされるデータ移転、例えば、競争促進機関、租税機関とのデータ移転、社会保障関連サービス、水産管理関連サービスとのデータ移転に適用される。加えて、データ移転は、制限された環境下では、管理者又は処理者の正当な利益に基づき、当該移転の環境について評価及び文書化した場合には、認められうる。
第 45 条：欧州委員会と第三国（とりわけ、保護の十分なレベルを提供していると考えられる第三国）の監督機関とのデータ保護のための国際協力メカニズムを明示的に提供。OECD の 2007 年 6 月 12 日のプライバシー保護法の執行における国境を越えた協力に関する勧告を考慮。

第 6 章　独立の監督機関

第 1 節　独立的な地位

第 46 条：EU 加盟国が監督機関を設立する義務（EU 指令第 28 条(1)に基づく）。その使命を、相互に、また欧州委員会と協力することに拡大。

第 47 条:監督機関の独立性のための条件を明確化。欧州司法裁判所の判例を施行するもの。また EU 規則（EC）No45/2001 の第 44 条も参考にしている。

第 48 条：監督機関のメンバー構成の一般的条件を提供。関連する判例を施行するもの。また EU 規則（EC）No45/2001 の第 42 条(2)-(6)も参考にしている。

第 49 条：監督機関の設立に関するルールは加盟国の法律で規定することを規定。

第 50 条：監督機関のメンバー及び職員の守秘義務を規定（EU 指令第 28 条(7)に基づく）。

第 2 節　任務と権限

第 51 条：監督機関の権能（competence）を規定（EU 指令第 28 条(6)に基づく）。複数の加盟国に事業所を持つ管理者又は処理者のケースにおいて、適用の一貫性を保証するために（ワンストップショップ）、主要な監督機関としての新たな権限を追加された。裁判所が司法機関として機能する場合には、裁判所は監督機関による監視から除外されるが、データ保護の実質的なルールの適用からは除外されない。

第 52 条：監督機関の任務を規定。苦情を聴取し調査する義務や、リスク、ルール、安全管理措置及び権利に関する公衆の意識を向上する義務を含む。

第 53 条：監督機関の権限（power）を規定（一部は EU 指令第 28 条(3)と、EU 規則（EC）45/2001 の第 47 条に基づく）。新たな追加要素として、administrative offences（法定犯罪）を処罰する権限を含む。

第 54 条：監督機関が年次活動報告書を作成する義務（EU 指令第 28 条(5)に基づく）。

第 7 章　協力と整合性

第 1 節　協力

第 55 条：義務的な相互支援に関する明示的なルールを導入（EU 指令第 28 条(6)2 に基づく）。他の監督機関の要求を遵守しなかった場合の帰結を含む。

第 56 条：共同活動に関するルールを導入。監督機関がそのような共同活動に参加することの権利を含む。

第 2 節　整合性（Consistency）

第 57 条：複数加盟国に跨る処理に関する適用の一貫性を保証するための整合性メカニズムを導入。

第 58 条：欧州データ保護評議会の意見のための手続きと条件を規定。

第 59 条：整合性メカニズムの内部で扱われる事柄に関する欧州委員会の意見。第 58 条(3)の下で欧州データ保護評議会によって提起されたことがらに関しては、欧州委員会はその裁量権を行使し、必要な場合には意見を提示することが期待される。
第 60 条：監督機関に措置を差し止めさせる欧州委員会の決定。
第 61 条：緊急手続きにおける暫定措置の採用の可能性。
第 62 条：整合性メカニズムの下で欧州委員会が法律を実施するための要件。
第 63 条：全ての加盟国における監督機関の措置の執行のための義務。

第 3 節　欧州データ保護評議会

第 64 条：各加盟国の監督機関の長と欧州データ保護監督者から成る欧州データ保護評議会の設立（EU 指令第 29 条に対応）。
第 65 条：欧州データ保護評議会の独立性。
第 66 条：欧州データ保護評議会の任務（EU 指令第 30 条(1)に対応）。
第 67 条:欧州データ保護評議会が年次で活動を報告する義務（EU 指令第 30 条(6)に対応）。
第 68 条：欧州データ保護評議会の意思決定手続き。
第 69 条：欧州データ保護評議会の議長及び副議長。
第 70 条：議長の義務。
第 71 条：欧州データ保護評議会事務局の設立とその任務。
第 72 条：守秘義務。

第 8 章　救済、責任及び制裁

第 73 条：監督機関に苦情を申し立てる権利（EU 指令第 28 条(4)に対応）。
第 74 条：監督機関に対する司法救済の権利（EU 指令第 28 条(3)に対応）。
第 75 条：管理者又は処理者に対する司法救済の権利（EU 指令第 22 条に対応）。
第 76 条：裁判手続の共通ルール。
第 77 条：補償（損害賠償）の権利と責任（EU 指令第 23 条に対応）。
第 78 条：本規則の違反に対する刑事罰を加盟国が定める義務。
第 79 条：本条で列挙された禁止行為に対して監督機関が行政罰（課徴金を科すこと）を行う義務。

第 9 章　特定のデータ処理状況に関する条項

第 80 条：表現の自由との関係（EU 指令第 9 条に対応）。
第 81 条：医療目的での処理に特別な安全管理措置を保証する義務。
第 82 条：雇用関係の個人データ処理に関する特別法の採択。
第 83 条：歴史・統計・科学研究目的での個人データ処理のための特別な条件。
第 84 条：監督機関が個人データや施設にアクセスすることの特別ルールの採択。

第 85 条：教会の既存の包括的データ保護ルールの継続的な適用を許可。

第 10 章　委任法令、実施法令

第 86 条：欧州委員会への法令採択権限の委任。

第 87 条：欧州委員会へのコミッティ（欧州委員会を支援するコミッティ）の実施権限の委譲。

第 11 章　最終条項

第 88 条：EU データ保護指令の廃止。

第 89 条：2002 年電子プライバシー指令との関係を明確化、また同指令を修正。

第 90 条：本指令の評価、欧州委員会による報告。

第 91 条：本指令の施行日。

１．３　主要な改定内容（従来の EU データ保護指令からの変更点）

１．３．１　全般

EU データ保護規則案では、その規制の位置づけが、従来の「指令（Directive）」から「規則（Regulation）」に格上げされた。

「規則」は、欧州連合の加盟国の法令を統一するために制定され、加盟国に直接の効力を持ち、個々の国に効力をもたらすための国内法を必要としない。また、すべての国内法に優先するものである[3]。

なお、欧州委員会の Communication（2012 年 1 月 25 日）では、「規則」とすることに関連して、以下のような解説が付されている。

> 「欧州全域でのデータ保護ルールの整合的な執行」
> ○事例：
> EU 内に複数の事業所を持つ多国籍企業がオンライン地図システムを開発し、全ての建造物のイメージを収集し、ストリート上の人々の写真を撮影していた。ある加盟国では、撮影されたことに気付いていない人々のぼかしのない写真が含まれていることは非合法であるとみなされ、他の加盟国ではデータ保護法上の違反はないとみなされた。結果として、この状況の改善に向けた各国の監督機関による整合的な対応は取られなかった。
> ○対策：
> 今回、1 つの EU 規則を EU 全体に直接的に適用することで、このような事態に対処する。

１．３．２　個人データ保護の権利の強化

EU 規則案では、EU 域内の管理者[4]や処理者[5]に対して、以下のような義務が追加又は強化された。

① 「自己情報コントロール権」の強化

- 透明で適切なプライバシーポリシーの提供（第 11 条）：
  現行 EU 指令にも本人への利用目的等の情報提供（通知）義務があるが、企業のプラ

---

[3] EU の規制については、「規則」、「指令」、「決定」、「勧告」、「見解」の 5 種類がある。左ほど強制力が強い。「指令」は、加盟国において国内法に置き換えられたときにのみ各国に効力を持つ。また、国内法への置き換えに際し、加盟国にはある一定の裁量権が与えられている。また指令は、定められた期間内に国内法に置き換えられなければならないということも決められている。（「EU（欧州連合）の主な法体系について」『制電 Vol.32―6 October 2006』http://www.neca.or.jp/control/green/PDF/kank0610.pdf を参考にした。）

[4] 「管理者」とは、個人データ処理の目的、条件及び手段を決定する自然人、法人、公的機関、その他のあらゆる組織を指す。

[5] 「処理者」とは、管理者の代わりに個人データを処理する自然人、法人、公的機関、その他のあらゆる組織を指す。なお、「処理（processing）」とは、個人データに対して実行されるあらゆるオペレーション。収集、保存、変更、利用、開示、消去等の総称である。

イバシーポリシーが煩雑で分かりにくい現状を踏まえ、管理者に対して、新たに「透明性」の義務が追加された。

- 明示的な同意の取得（第 7 条）：
  前項に関連して、プライバシーポリシーが分かりにくいため本人の同意が形式的なものに陥っている現状を踏まえ、管理者に対して、明示的な同意を取得することの義務、また同意を撤回できる権利を保障する義務が追加された。
- 自己情報への容易なアクセスの保証（第 15 条）
- 忘れられる権利、同意を撤回する権利（第 17 条）：
  現行 EU 指令の第 12 条にも自分の個人データを消去する権利が規定されているが、この権利が精緻化された。現行では、データが不正確だったり不法に収集された等の理由がないと消去できないが、EU 規則案では本人が同意を撤回したり、同意した保有期間の期限が来たりした場合には、管理者に消去してもらう権利が保障されることになった。
- データ・ポータビリティの権利（第 18 条）：
  利用者が SNS サービスを他のサービスに切り替える際など、管理者に妨害されることなく、自分の個人データを一定のフォーマットで入手し、他のサービスに移転する権利が保障されることになった。
- 子どもに対する特別な配慮（同意取得や情報提供）（第 8 条、第 11 条）

なお、欧州委員会の Communication（2012 年 1 月 25 日）では、「忘れられる権利」に関連して、以下のような解説が付されている。

「忘れられる権利」
〇事例：
ある SNS サイトの会員だった欧州の学生が、当該サイトに自分に関する全ての個人データへのアクセスを請求したところ、彼が自覚している以上の個人データがサイトに収集されており、彼が削除したはずの個人データまで保存されていた。
〇対策：
このような事態を防ぐため、今回の改定では、以下を導入。

- SNS サイト等のデータ管理者が収集したり処理する個人データを最小限に留めることの義務。
- デフォルト設定においてデータが公開されないようにすること。
- 個人が明示的に個人データの削除を要求し、かつそれらを保持する正当な理由が無い場合、データ管理者が当該データを削除する明示的な義務。

上述の事例では、SNS サイトは学生のデータを直ちに、かつ完全に削除する義務があることになる。

② 個人が権利行使する手段の改善

- 監督機関の独立性と権限の強化（第 47 条、第 52 条、第 53 条）
- 行政的救済措置・司法救済措置の向上（第 73 条～第 75 条）
- 監督機関による課徴金（第 79 条）：
  EU 規則に違反した管理者や処理者に対して、最大で 100 万ユーロ、又は企業の場合には最大で年間連結売上の 2%の課徴金を科す権限が監督機関に付与された。

③ データセキュリティの強化

- プライバシー強化技術（PET）の利用促進とプライバシー認証制度の促進（第 30 条、第 39 条）：
  データ保護の認証制度の促進に関する条項が新たに導入され、特に EU のレベルで、認証制度やデータ保護シールの設立を促進すると謳われている。
- データ違反時の監督機関及び本人への迅速な報告・連絡義務（第 31 条、第 32 条）：
  個人データ違反（personal data breach、紛失・盗難・漏洩・不正利用等）があった場合、その発見後、可能な限り 24 時間以内に、監督機関に報告する管理者の義務が新設された。報告項目は、漏洩データ等の対象人数・データ項目、漏洩等の影響を軽減するために個人等が取るべき対処策、発生した事態（結果）、管理者が取る予定の対応策等である。24 時間以降に報告する場合は、遅れたことについて正当な理由付けが必要である。また、監督機関への報告の後、不当な遅滞なく、本人へも連絡することが必要である。

なお、欧州委員会の Communication（2012 年 1 月 25 日）では、「データ違反時の報告・連絡義務」に関連して、以下のような解説が付されている。

「データ違反時の報告・連絡」
〇事例：
EU の利用者も対象としたゲームサービスがアタックされ、全世界の数千万人分の個人データ（氏名、住所、クレジットカード情報等）を含むデータベースが不正アクセスされた。当該企業がその事実を利用者に知らせるまでに、一週間もかかった。
〇対策：
このような事態を防ぐため、今回の改定では、企業に対して以下のことを義務付けるものである。

- データ違反を防止し回避するための安全管理措置を強化すること。
- 実行可能な場合は、データ違反が発見されてから 24 時間以内に監督機関に報告するとともに、不当な遅滞なく個人にも連絡すること。

④ 管理者（controller）や処理者（processer）の説明責任の強化

- データ保護オフィサーの設置義務（第 35 条）：
  公共部門及び民間部門（大企業等）の管理者や処理者に対して、データ保護オフィサーの設置が義務化された。
- プライバシー・バイ・デザイン原則の導入（第 23 条）
- データ保護影響評価の実施義務（第 33 条）：
  管理者や処理者に対して、プライバシーリスクが高い個人データ処理（経済状況、位置情報、医療健康情報、遺伝子情報、生体情報、監視カメラ情報等を取扱う場合）について、データ保護影響評価（プライバシー影響評価に該当）を新たに義務付けた。

⑤「個人データ」の範囲の拡大の可能性

EU 規則案における「個人データ（personal data）」の定義は、「データ主体に関する全ての情報」（第 4 条(2)）であり、また、「データ主体」の定義は「識別された自然人、又は管理者、若しくは他の自然人若しくは法人によって合理的に利用される可能性の高い手段によって、直接的若しくは間接的に、とりわけ識別番号、位置データ、オンライン識別子、若しくは当該人物の肉体的、生理学的、遺伝的、精神的、経済的、文化的若しくは社会的アイデンティティに特有な 1 つ以上の要素を参照することによって、識別されうる自然人」（第 4 条(1)）であるため、現行 EU 指令[6]と定義上は大きく変わらないように見えるが、個人識別手段（すなわち個人識別可能なデータ）の例として「位置データ」と「オンライン識別子」が追加されている。

また、2012 年 1 月 25 日に欧州委員会が公表した FAQ では、「個人データはある個人に関する全ての情報である。氏名、写真、メールアドレス、銀行口座情報、SNS サイトへの書き込み、医療情報、IP アドレス等の全てが該当しうる」とされている。

なお、EU 規則案の前文（Whereas 条項）の(24)項では「オンラインサービスを利用する際に、個人はデバイスやアプリケーション、ツール、プロトコルによって提供されるオンライン識別子（IP アドレスやクッキー）と関連付けられるかもしれない。このことは、サーバが受信するユニークな識別子とその他の情報に結び付けられて、個人のプロファイルの作成や個人の識別に使用されうるようなトレースを残すかもしれない。したがって、識別番号、位置データ、オンライン識別子（IP アドレスやクッキー）又はその他の特定の要素が、それ自体として、全ての環境において必ずしも個人データとみなされる必要はない

[6] 現行 EU 指令は、第 2 条(a)において「個人データ」を以下のように定義している。「識別された自然人、又は識別されうる自然人に関する全ての情報を意味するものとする。識別されうる人とは、直接的又は間接的に、とりわけ識別番号又は当該人物の肉体的、生理学的、精神的、経済的、文化的若しくは社会的アイデンティティに特有な 1 つ以上の要素を参照することによって、識別が可能な人のことである。」

ことになる[7]」と説明されており、場合によっては、これらのデータが（単独で）個人データとみなされる可能性があることも示唆されている。

また、前文の(23)項では「データ保護の諸原則は、データ主体がもはや識別可能でない仕方で匿名化されたデータには適用されるべきでない」と説明されているので、匿名化[8]されたデータは「個人データ」として取り扱わなくてよいと考えられる。

１．３．３　EU 域内でのデータ保護ルールの一元化

EU 規則案では、EU における「デジタル単一市場」の実現のために、以下のようにデータ保護ルールが一元化されている。

- 単一の EU 規則を各加盟国に直接的に適用すること（上述）：
  加盟国毎のルールに合わせなくてよいので、EU 試算によると、企業にとって年間 23 億ユーロのコスト削減になる。
- データ処理に係る監督機関への通知義務の廃止：
  EU 試算によると、企業にとって年間 1 億 3 千万ユーロのコスト削減になる。
- 「ワンストップショップ」としての監督機関（第 51 条）：
  多国籍企業の監督機関とのやり取り（認可）は、主要事業所（主要拠点）がある加盟国の監督機関に一本化された。

これらは EU 域内の企業（管理者や処理者）にとってメリットとなる。また、下記の点も追加・変更された。

- 監督機関同士の協力と、整合性メカニズムの導入（第 55 条、第 57 条）
- 現行指令の第 29 条作業部会を、独立的な欧州データ保護評議会に格上げ（第 64 条）

１．３．４　グローバル環境でのデータ保護ルールの詳細化

EU 市民の個人データが EU 域外に移転される場合のデータ保護ルールが、以下のように詳細化された。

これらについては、次節で個別論点として整理する。

① EU 規則が第三国の管理者に適用される範囲の拡大（規制強化）（第 3 条）
② 個人データの第三国移転に関するルールの詳細化（第 40 条～第 45 条）

---

[7] この文章は、2011 年 11 月のドラフトの段階では「本規則は、そのようなデータを伴う処理に適用可能であるべきである。」というものであったが、1 月 25 日の EU 規則案においてこのように緩和された。

[8] ただし、匿名化の基準に関する記述はない。

- 欧州委員会による第三国の十分性決定の基準の規定（第 41 条）
- 十分性決定のない第三国へのデータ移転に関するルールの補強と簡素化（BCR を含む）（第 42 条、第 43 条）：
  BCR（拘束的企業準則）については、1 つの監督機関の承認さえ貰えば、EU の他の監督機関は一括でその結果を追認することになった。

１．４　改定内容の個別論点の整理

１．４．１　EU 規則が第三国の管理者に適用される範囲の拡大

（１）現行 EU 指令の規定

現行 EU 指令では、EU 域外企業（管理者）に対しては、EU 域内の設備でデータ処理を行う場合のみ EU 指令の対象となる。すなわち、 現行 EU 指令第 4 条において、EU 域内の管理者（企業等）には（EU 指令に基づき制定された）当該加盟国の法律が適用されるが、EU 域外の管理者であっても、EU 域内の設備でデータ処理を行っている場合は、当該加盟国の法律が適用される旨が規定されている。

（２）EU 規則案の規定

今回の EU 規則案では、EU 域外企業であっても、EU に居住するデータ主体（個人）のデータを取扱う管理者[9]に対しては EU 規則が適用されることとなった（第 3 条第 2 項）。すなわち、EU 域外企業であっても、

(1) EU に居住する個人に商品やサービスを提供している場合

(2) EU に居住する個人の行動をモニターしている場合

には EU 規則が適用される。

ただし、EU 域外企業が EU 域内企業から個人データ処理の委託を受けるような場合、例えば（パーソナルクラウド事業者以外の）クラウドサービス事業者の場合には、EU 規則案第 3 条第 2 項の対象にはならない。同条項の対象になるのは、あくまで EU 市民（消費者）に直接的にサービスを提供する EU 域外企業に限られる。

１．４．２　個人データの第三国移転に関するルールの詳細化

（１）現行 EU 指令の規定

現行 EU 指令では、下記の場合に EU 域内の管理者から EU 域外（第三国）の管理者（又は処理者）へのデータ移転が可能である。

① 十分性認定

欧州委員会が十分なレベルの個人データ保護を保証していると認定した国等については、

9 オンラインサービス事業者、パーソナルクラウド事業者、オンライン広告事業者、スマートフォンアプリ事業者等が想定される。

第三国移転が可能である（第 25 条）。スイス、カナダ、アルゼンチン、イスラエル、ガーンジー、マン島、ジャージー（左記 3 つは英国の王室属領）、フェロー諸島（デンマークの自治領）がこれまでに十分性認定を受けている。この十分性認定に当たっては「個人データの第三国移転：EU データ保護指令第 25 条及び第 26 条の適用（WP12　5025/98）」に基づいて評価がなされている。

日本はまだ欧州委員会から十分性認定を受けていない。また、欧州委員会に対して、十分性認定のための公式要請も提出していない。

② 米国については特例として、セーフハーバー・スキーム

セーフハーバー原則を遵守すると自己宣言する米国企業に対して「十分なレベルの保護」を行っていることを認める、EU と米国間で 2000 年に締結された協定である。セーフハーバー原則への遵守は企業の自己宣言であり、第三者認証はない。米国商務省のサイト（Safe Harbor List）に、自己宣言した企業のリストが掲載されている。2011 年 7 月時点で 2716 社（Not Current を含む）である。IT 企業では Google, Amazon, Facebook, Microsoft, Apple 等が掲載されている。これらの企業は、年に 1 回、自分でセーフハーバー原則への遵守を証明する報告書を商務省に提出する義務がある。セーフハーバー原則に違反した場合には、制裁措置がある。なお、セーフハーバー原則は「通知」「選択」「第三者提供」「セキュリティ」「データの完全性」「アクセス」「執行」の 7 つである。

③ 例外規定

・標準契約条項（モデル契約条項）（第 26 条第 4 項）：

二当事者間（EU 域内管理者－第三国管理者、又は EU 域内管理者－第三国処理者）での個人データ移転が対象で、欧州委員会がこれら二当事者間での国際移転に当たっての標準契約条項を採択している。2001 年様式、2004 年様式、2010 年様式がある。

・2001 年様式、2004 年様式：EU 域内の管理者から第三国の管理者への移転

・2010 年様式：EU 域内の管理者から第三国の処理者への移転

EU 域内管理者（日本企業の現地法人等）が標準契約条項を使用する際には、当該国の監督機関の承認が必要になる。

消費者庁の報告書[10]によると、ヒアリングを受けた日系企業 6 社のうち 4 社が標準契約条項を使って日本等へのデータ移転を行っている。標準契約条項は欧州委員会が採択したものなので、基本的にその条項を使えば、各国の監督機関の承認も下るようである。

・拘束的企業準則（Binding Corporate Rules：BCR）（第 26 条第 2 項）：

多国籍企業の企業グループ内での個人データ移転が対象で、EU 内で主要な事業所（拠点）

10 消費者庁「国際移転における企業の個人データ保護措置調査報告書」（2010 年 3 月）（http://www.caa.go.jp/seikatsu/kojin/H21report1a.pdf）

がある国の第三者機関の承認が必要なほか、他の拠点がある国の監督機関の承認も必要になる。（ただし、監督機関間の相互承認ネットワークが存在する。）

消費者庁の上記報告書によると、EU 全体でも（2009 年度時点で）20 社と承認事例は少なく（GE やハイアット、製薬会社等）、2009 年度時点で日本企業については承認事例はない様子である。

・その他、データ主体が個人データ移転に関して明確な同意を与えている場合や、データ主体及び管理者間の契約の履行のために必要な場合等（第 26 条第 1 項）の例外規定がある。

（２）EU 規則案の規定

EU 規則案においても、「第三国の十分性決定（第 41 条）」「標準契約条項（第 42 条）」「BCR（拘束的企業準則）（第 43 条）」「その他の例外（第 44 条）」という基本的な枠組みは変わっていない。

欧州委員会による「十分性決定（adequacy decision）」では、以下の点を考慮して評価がなされる（第 41 条）。

(a) 当該国の法令の内容、データ主体の権利の保障（実効的な行政的救済及び司法救済措置を含む）
(b) 独立の監督機関の存在、監督機関の機能（データ保護法令の遵守の保証、データ主体による権利行使の支援、EU の監督機関との協力）
(c) 国際的なコミットメント

なお、欧州委員会が決定した既存の「十分性認定国」及び「標準契約条項」は、欧州委員会が修正・廃止しない限り有効（第 41 条(8)）である。また、監督機関が承認した既存の「BCR」も、監督機関が修正・廃止しない限り有効（第 42 条(5)）である。

BCR は、上述の通り、EU 域内の 1 つの監督機関の承認さえ貰えば、他国でも有効となる（第 43 条(1)）。

２．EU 規則案と日本の個人情報保護制度との比較

本章では、EU 規則案と、日本の個人情報保護制度を比較し、日本の現行制度における差分（不足点）について整理を行う。

本調査分析の趣旨に鑑み、日本の個人情報保護制度に関しては、民間部門を対象とする個人情報保護法[11]及びプライバシーマーク制度（JISQ15001：2006 を準拠基準とする）を比較検討対象とする。

日本の社会保障・税番号制度に関しては、「社会保障・税番号大綱[12]」において「番号」に係る個人情報[13]の保護に関する方針が出されているが、あくまで「番号」に係る個人情報に範囲が限定されるものであるため、以下の比較では、第三者機関（個人番号情報保護委員会）や特定個人情報保護評価など、特徴的な項目に限って記載するものとする。

ISMS 制度（JISQ27001：2006 を準拠基準とする）に関しては、個人情報を含む情報資産一般の安全管理をカバーするものであるが、個人情報の適正取得・利用・提供、本人からの開示・訂正・消去請求等の個人情報保護に固有の視点をも包含するものではないため、以下の比較では、情報セキュリティ事象の報告やリスクアセスメントなど、特徴的な項目に限って記載するものとする。なお、参考まで、JISQ15001：2006 と ISMS（JISQ27001：2006）の適用範囲の関係について図 1 に示す。

---

11 正式名称は、「個人情報の保護に関する法律」。

12 政府・与党社会保障改革検討本部「社会保障・税番号大綱」2011 年 6 月 30 日（http://www.cas.go.jp/jp/seisaku/bangoseido/pdf/110630/honbun.pdf）。

13 「番号」に係る個人情報とは、①「番号」、②情報連携基盤を通じた情報連携の対象となるものとして法定された社会保障及び税分野の個人情報、③（情報連携基盤を通じた情報連携の対象とはならないものの、）法令に基づき「番号」を取り扱い得る事務において「番号」と紐付いて扱われる社会保障及び税分野の個人情報をいう（『社会保障・税番号大綱』p.33）。なお、マイナンバー法案では、「番号」に係る個人情報は、「特定個人情報」という表現に改められている。「特定個人情報」は、個人番号（個人番号に代わって用いられる番号、記号その他の符号を含む）をその内容に含む個人情報と定義されている（第 2 条）。

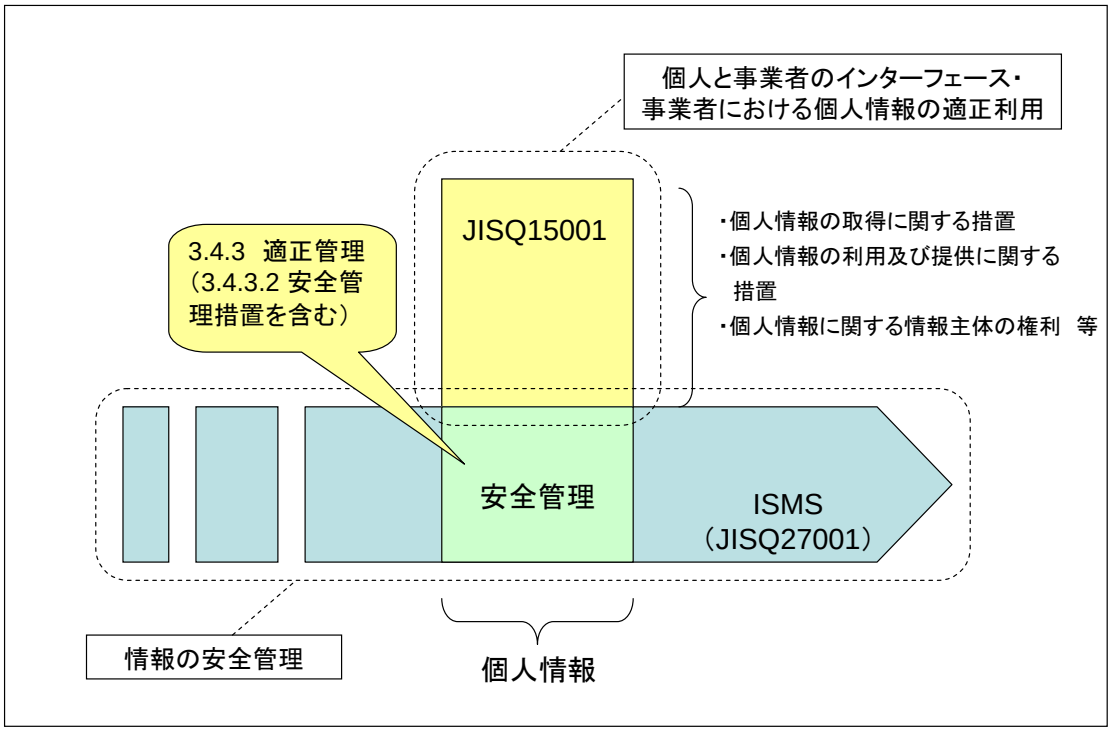

図 1　JISQ15001 と JISQ27001 の適用範囲の関係

２．１　総論

日本の個人情報保護法は、以下に挙げるような多くの点で、EU 規則案よりも規定が緩やかである。詳細については、次節で述べる。

・対象事業者（個人情報取扱事業者）の範囲が狭い
・第三者提供など一定の場合を除いて本人の同意取得が必要とされていない
・特定カテゴリの情報（特定機微情報）の取扱いに関する規定がない
・開示・訂正・消去請求権が本人の権利として明示的には認められていない
・ダイレクトマーケティングに対する異議申立の権利がない
・プロファイリングを受けない権利の規定がない
・個人情報漏洩時等の報告・連絡義務がない
・第三国への個人情報移転を禁じていない
・独立的な監督機関（第三者機関）に関する規定がない
・司法救済を求める個人の権利が規定されていない　等

プライバシーマーク制度が準拠基準とする JISQ15001：2006 は、通商産業省（現経済産業省）が 1997 年に EU 指令を受けて改訂した「民間部門における個人情報保護のためのガイドライン」に基づき制定された JIS Q15001：1999「個人情報保護に関するコンプライアンス・プログラムの要求事項」を前身としているので、個人情報保護法よりも全体的に EU

指令（及びその後継である EU 規則案）寄りの規定となっているが、以下に挙げるような多くの点で、やはり EU 規則案よりも緩やかである。詳細については、次節で述べる。

・開示・訂正・消去請求権が本人の権利として明示的には認められていない
・ダイレクトマーケティングに対する異議申立の権利がない
・プロファイリングを受けない権利の規定がない
・第三国への個人情報移転を禁じていない
・独立的な監督機関（第三者機関）に関する規定がない
・司法救済を求める個人の権利が規定されていない　等

２．２　各論

２．２．１　義務付け対象者

（１）EU 規則案

「管理者」及び「処理者」が規制対象となる[14]。第 4 条により、「管理者（controller)」は、「単独又は他者と共同で、個人データ処理の目的、条件及び手段を決定する自然人、法人、公的機関、その他のあらゆる組織を意味する」、「処理者（processor)」は、管理者の代わりに個人データを処理する自然人、法人、公的機関、その他のあらゆる組織を意味する」と定義されている。

（２）日本の個人情報保護制度

①個人情報保護法

第 2 条第 3 項及び同法の施行令第 2 条において、「個人情報取扱事業者」を「個人情報データベース等を事業の用に供している者」と定義し、ただし「その事業の用に供する個人情報データベース等を構成する個人情報によって識別される特定の個人の数の合計が過去六月以内のいずれの日においても五千を超えない者」は除くとしている。

なお、公的機関については、別途、行政機関個人情報保護法、独立行政法人等個人情報保護法、及び地方公共団体の個人情報保護条例で規制が行われている。

②プライバシーマーク制度（JISQ15001：2006）

「事業者」が対象である。2.3 節において、「事業者」は「事業を営む法人その他団体又は個人」と定義されている。

（３）比較

日本の個人情報保護法においては、対象となる事業者（個人情報保護事業者）の範囲が狭い。すなわち、EU 規則案では処理を行う個人データの件数が少ない管理者／処理者に対しても特に適用除外とされることはないが、日本の個人情報保護法では 5000 人未満の個人

[14] ただし、第 3 条による地域的な制限はある。

情報しか取扱わない事業者は同法の義務を免除されており、この点が EU 規則案に比べて緩やかである。

一方、日本のプライバシーマーク制度では対象人数による適用除外は特に設けられていないが、同制度は民間部門を対象としており、公的機関は対象としていない。

２．２．２　個人データの保存

（１）EU 規則案

第 5 条「個人データ処理に関する諸原則」の(e)において、歴史的、統計的又は科学的研究目的で処理される場合のみ、個人データを長期間保存することができると規定されている。

（２）日本の個人情報保護制度

①個人情報保護法

個人情報保護法には、個人情報の長期間保存を制限する規定はない。

②プライバシーマーク制度（JISQ15001：2006）

JISQ15001 には、個人情報の長期間保存を制限する規定はない。

（３）比較

日本の個人情報保護制度には、個人情報の長期間保存を制限する規定は存在しない。

２．２．３　同意の取得

（１）EU 規則案

第 6 条「処理の合法性」の第 1 項において、契約履行や法的義務の遵守のために必要なデータ処理等の一定の場合を除いて、データ主体が当該データ処理に同意を与えている場合でなければ、データ処理はできないことが規定されている。

（２）日本の個人情報保護制度

①個人情報保護法

第 18 条において、「個人情報取扱事業者は、個人情報を取得した場合は、あらかじめその利用目的を公表している場合を除き、速やかに、その利用目的を、本人に通知し、又は公表しなければならない」と規定されているが、個人情報の取得や利用にあたって本人の同意は必要とされていない。利用目的の変更（第 16 条）、及び第三者提供（第 23 条）にあたって本人同意が必要とされているのみである。

②プライバシーマーク制度（JISQ15001：2006）

本人から直接書面によって個人情報を取得する場合（3.4.2.4 節）、利用目的を超えて個人情報を利用する場合（3.4.2.6 節）、個人情報を利用して個人にアクセスする場合（3.4.2.7 節）及び第三者に提供する場合（3.4.2.8 節）については、事前に本人の同意を得ることが必要とされているが、個人情報の利用一般に先立って本人の同意が必要である旨は規定されていない。

（３）比較

EU 規則案では一定の例外を除いてデータ主体からの同意取得が原則とされているが、日本の個人情報保護法においては一定の場合を除いて本人からの同意取得は必要とされておらず、この点が EU 規則案に比べて緩やかである。

また、日本のプライバシーマーク制度も同様な点で、EU 規則案に比べて緩やかである。

２．２．４　特定カテゴリのデータの処理の禁止

（１）EU 規則案

第 9 条「特別なカテゴリの個人データの処理」において、データ主体が同意を与えた場合等の一定の例外条件を除いて、「人種若しくは民族、政治的見解、宗教若しくは信条、労働組合への加盟を明らかにする個人データの処理、及び遺伝データ、健康医療若しくは性生活に関するデータ、有罪判決若しくは関連する安全対策に関するデータの処理は禁止する」と規定されている。

（２）日本の個人情報保護制度

①個人情報保護法

特定カテゴリのデータの取扱いに関する規定はない。

②プライバシーマーク制度（JISQ15001：2006）

3.4.2.3 節において、明示的な本人の同意がある場合等の一定の例外条件を除いて、「特定の機微な情報」として、以下に示す内容を含む個人情報
の取得、利用又は提供は禁止されている。

・思想、信条又は宗教に関する事項
・人種、民族、門地、本籍地（所在都道府県に関する情報を除く）、身体・精神障害、犯罪歴その他社会的差別の原因となる事項
・勤労者の団結権、団体交渉その他団体行動の行為に関する事項
・集団示威行為への参加、請願権の行使その他の政治的権利の行使に関する事項
・保健医療又は性生活に関する事項

（３）比較

日本の個人情報保護法においては、EU 規則案のような、特定カテゴリのデータ（いわゆるセンシティブデータ）の取扱いに関する規定は存在しない。

一方、日本のプライバシーマーク制度においては、対象となるデータの種類に若干の差異があるものの、EU 規則案と同様に特定カテゴリの個人情報の利用等を禁止する規定が存在する。

２．２．５　適用除外となるデータ処理（個人情報取扱い）

（１）EU 規則案

第 80 条「個人データ処理と表現の自由」において、表現の自由との関連で、「報道目的、又は芸術若しくは文学表現上の目的」でのみ実行される個人データ処理について、管理者や処理者の義務の免除又は軽減が規定されている。

（２）日本の個人情報保護制度

①個人情報保護法

第 50 条において、「放送機関、新聞社、通信社その他の報道機関」が報道の用に供する目的で、「著述を業として行う者」が著述の用に供する目的で、「大学その他の学術研究を目的とする機関若しくは団体又はそれらに属する者」が学術研究の用に供する目的で、「宗教団体」が宗教活動の用に供する目的で、また「政治団体」が政治活動の用に供する目的で個人情報を取扱う場合は、個人情報取扱事業者の義務が適用除外されると規定されている。

②プライバシーマーク制度（JISQ15001：2006）

事業者の義務が適用除外されるような個人情報取扱いのカテゴリについては規定されていない。

（３）比較

日本の個人情報保護法は、報道機関のみならず、著述業、学術研究者、宗教団体、政治団体をも適用除外としている点で、EU 規則案に比べて緩やかである。

２．２．６　情報提供（通知・公表）の透明性

（１）EU 規則案

第 11 条「透明な情報通知と連絡」において、透明かつ容易にアクセスできるプライバシーポリシーを掲載する義務、及びデータ主体に対する情報通知や連絡をデータ主体に合わせた明確かつ平易な言葉を用いて分かりやすく提供する義務が規定されている。

（２）日本の個人情報保護制度

①個人情報保護法

個人情報保護法には、通知・公表の透明性や分かりやすさに関する規定はない。

②プライバシーマーク制度（JISQ15001：2006）

プライバシーマーク制度には、通知・公表の透明性や分かりやすさに関する規定はない。

（３）比較

日本の個人情報保護制度には、通知・公表の透明性や分かりやすさに関する規定は存在しない。

２．２．７　データを直接収集する個人への情報提供

（１）EU 規則案

第 14 条「データ主体への情報通知」において、個人データを収集するデータ主体に対しては、以下の情報を提供しなければならないと規定されている。

(a)管理者、（存在する場合には）管理者の代表者、及びデータ保護オフィサーの身元及び連絡先情報。

(b)意図された個人データの処理目的。処理が第 6 条(1)の(b)に基づく場合は当該契約条件と一般条件、処理が第 6 条(1)の(f)に基づく場合は管理者が追求する正当な利益を含める。

(c)個人データが保存される期間

(d)管理者にデータ主体に関する個人データへのアクセス、及びそれらの訂正若しくは消去を請求する権利、又はそれらの個人データの処理に異議申立をする権利の存在。

(e)監督機関に苦情を申し立てる権利、及び監督機関の連絡先情報。

(f)個人データの受領者、又は受領者のカテゴリ。

(g)適用される場合には、管理者が第三国又は国際組織にデータを移転することを意図していること、及び欧州委員会の十分性決定に言及することによる当該第三国若しくは国際組織の保護のレベル。

(h)個人データが収集される特定の環境を考慮に入れ、データ主体に関係する公正な処理を保証するために必要な更なる情報。

また、データ主体から直接収集する場合は、これらに加えて、以下の情報も提供しなければならないと規定されている。

・個人データの提供が義務であるのか又は任意であるのか

・当該データを提供しない場合に想定される結果

（２）日本の個人情報保護制度

①個人情報保護法

第 18 条において、個人情報を取得した場合は（あらかじめ利用目的を公表している場合を除き）速やかに利用目的を本人に通知又は公表しなければならないと規定されている。また、本人から直接書面に記載された当該本人の個人情報を取得する場合は、あらかじめ本人に対して利用目的を明示しなければならないと規定されている。

また、第 24 条において、以下の事項について、本人の知り得る状態（本人の求めに応じて遅滞なく回答する場合を含む）に置かなければならないと規定されている。

一　当該個人情報取扱事業者の氏名又は名称

二　すべての保有個人データの利用目的(第十八条第四項第一号から第三号までに該当する場合を除く。)

三　次項、次条第一項、第二十六条第一項又は第二十七条第一項若しくは第二項の規定による求めに応じる手続（第三十条第二項の規定により手数料の額を定めたときは、その手数料の額を含む。）

四　前三号に掲げるもののほか、保有個人データの適正な取扱いの確保に関し必要な事項として政令で定めるもの（同法の施行令第 5 条より、「当該個人情報取扱事業者が行う保有個人データの取扱いに関する苦情の申出先」及び「当該個人情報取扱事業者が認定個人情報保護団体の対象事業者である場合にあっては、当該認定個人情報保護団体の名称及び苦情の解決の申出先」）

②プライバシーマーク制度（JISQ15001：2006）

3.4.2.4 節において、本人から直接書面によって個人情報を取得する場合は、あらかじめ本人に対し、以下の情報を書面で明示しなければならないと規定されている。

a) 事業者の氏名又は名称

b) 個人情報保護管理者（若しくはその代理人）の氏名又は職名，所属及び連絡先

c) 利用目的

d) 個人情報を第三者に提供することが予定される場合の事項

- 第三者に提供する目的
- 提供する個人情報の項目
- 提供の手段又は方法
- 当該情報の提供を受ける者又は提供を受ける者の組織の種類，及び属性
- 個人情報の取扱いに関する契約がある場合はその旨

e) 個人情報の取扱いの委託を行うことが予定される場合には，その旨

f) 3.4.4.4～3.4.4.7 に該当する場合には，その求めに応じる旨及び問合せ窓口

g) 本人が個人情報を与えることの任意性及び当該情報を与えなかった場合に本人に生じる結果

h) 本人が容易に認識できない方法によって個人情報を取得する場合には，その旨

（３）比較

日本の個人情報保護法やプライバシーマーク制度に比べ、EU 規則案では、「個人データの保存期間」「監督機関に苦情を申し立てる権利、監督機関の連絡先」「第三国への移転」等の点で本人に通知・提供すべき情報項目が多い。

２．２．８　データを間接収集する個人への情報提供

（１）EU 規則案

第 14 条「データ主体への情報通知」において、個人データを収集するデータ主体に対しては、以下の情報を提供しなければならないと規定されている。

(a)管理者、（存在する場合には）管理者の代表者、及びデータ保護オフィサーの身元及び連絡先情報。

(b)意図された個人データの処理目的。処理が第 6 条(1)の(b)に基づく場合は当該契約条件と一般条件、処理が第 6 条(1)の(f)に基づく場合は管理者が追求する正当な利益を含める。

(c)個人データが保存される期間

(d)管理者にデータ主体に関する個人データへのアクセス、及びそれらの訂正若しくは消去を請求する権利、又はそれらの個人データの処理に異議申立をする権利の存在。

(e)監督機関に苦情を申し立てる権利、及び監督機関の連絡先情報。

(f)個人データの受領者、又は受領者のカテゴリ。

(g)適用される場合には、管理者が第三国又は国際組織にデータを移転することを意図していること、及び欧州委員会の十分性決定に言及することによる当該第三国若しくは国際組織の保護のレベル。

(h)個人データが収集される特定の環境を考慮に入れ、データ主体に関係する公正な処理を保証するために必要な更なる情報。

また、データ主体から直接的に収集しない場合は、これらに加えて、以下の情報も提供しなければならないと規定されている。

・当該データを取得したソース（収集源）

（２）日本の個人情報保護制度

①個人情報保護法

本人から間接的に個人情報を取得するケースについては、同法の中で明示的には言及されていないものの、第 18 条において（直接／間接収集に関わらない一般要件として）、個人情報を取得した場合は（あらかじめその利用目的を公表している場合を除き）速やかに利用目的を本人に通知又は公表しなければならないと規定されている。

また、第 24 条において、以下の事項について、本人の知り得る状態（本人の求めに応じて遅滞なく回答する場合を含む）に置かなければならないと規定されている。

一　当該個人情報取扱事業者の氏名又は名称
二　すべての保有個人データの利用目的(第十八条第四項第一号から第三号までに該当する場合を除く。)
三　次項、次条第一項、第二十六条第一項又は第二十七条第一項若しくは第二項の規定による求めに応じる手続（第三十条第二項の規定により手数料の額を定めたときは、その手数料の額を含む。）
四　前三号に掲げるもののほか、保有個人データの適正な取扱いの確保に関し必要な事項として政令で定めるもの（同法の施行令第 5 条より、「当該個人情報取扱事業者が行う保有個人データの取扱いに関する苦情の申出先」及び「当該個人情報取扱事業者が認定個人情報保護団体の対象事業者である場合にあっては、当該認定個人情報保護団体の名称及び苦情の解決の申出先」）

②プライバシーマーク制度（JISQ15001：2006）

3.4.2.5 節において、本人から直接書面によって取得する以外の方法で個人情報を取得した場合[15]は、速やかにその利用目的を、本人に通知又は公表しなければならないと規定されている。

（３）比較

日本の個人情報保護法やプライバシーマーク制度に比べ、EU 規則案では、「個人データの保存期間」「監督機関に苦情を申し立てる権利、監督機関の連絡先」「第三国への移転」「データ取得のソース」等の点で本人に通知・提供すべき情報項目が多い。

２．２．９　アクセス（開示）・訂正・消去を請求する権利

（１）EU 規則案

開示については、第 15 条において、「データ主体は、自分に関する個人データが処理されているか否かについての確認を、請求に応じて、いつでも管理者から取得する権利を有するものとする」と規定されている。

訂正については、第 16 条において、「データ主体は、不正確な自分に関する個人データを管理者に訂正してもらう権利を有するものとする」と規定されている。

消去については、第 17 条において、データがもはや処理目的にとって必要ない場合やデータ主体が同意を撤回した場合等について、「.データ主体は、管理者に自分に関する個人データを消去してもらう権利、及び自分に関する個人データの頒布を停止してもらう権利を有するものとする」と規定されている。

---

15 個人情報を本人から直接取得する場合であっても、書面によらずに取得した場合、例えば監視カメラによって取得した場合や口頭によって取得した場合は、この 3.4.2.5 節のケースに含まれる。

また、第 13 条において、「管理者は、第 16 条及び第 17 条に則り実行された全ての訂正又は消去について、その連絡が不可能であることが判明したり、不釣合いな努力を必要とするものでないかぎり、データが開示された全ての受領者に対して連絡するものとする」と規定されている。

（２）日本の個人情報保護制度

①個人情報保護法

開示については、第 25 条において、「本人から、当該本人が識別される保有個人データの開示を求められたときは、本人に対し、政令で定める方法により、遅滞なく、当該保有個人データを開示しなければならない」と規定されている。ただし、業務の適正な実施に著しい支障を及ぼすおそれがある場合等は、当該データの全部又は一部を開示しないことが可能である。

訂正については、第 26 条において、「本人から、当該本人が識別される保有個人データの内容が事実でないという理由によって当該保有個人データの内容の訂正、追加又は削除を求められた場合には、その内容の訂正等に関して他の法令の規定により特別の手続が定められている場合を除き、利用目的の達成に必要な範囲内において、遅滞なく必要な調査を行い、その結果に基づき、当該保有個人データの内容の訂正等を行わなければならない」と規定されている。

消去については、第 27 条において、「本人から、当該本人が識別される保有個人データが第 16 条の規定に違反して取り扱われているという理由又は第 17 条の規定に違反して取得されたものであるという理由によって、当該保有個人データの利用の停止又は消去を求められた場合であって、その求めに理由があることが判明したときは、違反を是正するために必要な限度で、遅滞なく、当該保有個人データの利用停止等を行わなければならない」と規定されている。ただし、当該データの利用停止や消去に多額の費用を要する場合その他の利用停止や消去を行うことが困難な場合は、これを行わないことが可能である[16]。

②プライバシーマーク制度（JISQ15001：2006）

開示については、3.4.4.5 節において、「本人から、当該本人が識別される開示対象個人情報の開示を求められたときは、法令の規定によって特別の手続が定められている場合を除き、本人に対し、遅滞なく、当該開示対象個人情報を書面によって開示しなければならな

16 なお、経済産業省「個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン」（2009 年 10 月）では、「保有個人データの全部消去を求められた場合であっても、利用停止によって手続違反を是正できる場合であれば、そのような措置を講ずることにより、義務を果たしたことになり、必ずしも、求められた措置をそのまま実施する必要はない」、「『消去』とは、保有個人データを保有個人データとして使えなくすることであり、当該データを削除することのほか、当該データから特定の個人を識別できないようにすること等を含む」と規定されている。

い」と規定されている。ただし、業務の適正な実施に著しい支障を及ぼすおそれがある場合等は、当該データの全部又は一部を開示しないことが可能である。

訂正については、3.4.4.6 節において、「本人から、当該本人が識別される開示対象個人情報の内容が事実でないという理由によって当該開示対象個人情報の訂正、追加又は削除を求められた場合は、法令の規定によって特別の手続が定められている場合を除き、利用目的の達成に必要な範囲内において、遅滞なく必要な調査を行い、その結果に基づいて、当該開示対象個人情報の訂正等を行わなければならない」と規定されている。

消去については、3.4.4.7 節において、「本人から当該本人が識別される開示対象個人情報の利用の停止、消去又は第三者への提供の停止を求められた場合は、これに応じなければならない」と規定されている。ただし、業務の適正な実施に著しい支障を及ぼすおそれがある場合等は、消去等を行わないことが可能である。

（３）比較

EU 規則案ではアクセス（開示）・訂正・消去請求は本人の権利として明確に認められているのに対し、日本の個人情報保護法やプライバシーマーク制度では（後者では「個人情報に関する本人の権利」という記述はあるものの）開示・訂正・消去は事業者の義務にすぎず、一定の合理的理由があれば、それらの請求に応じないことが可能となっている。他方、EU 規則案では管理者がアクセス・訂正・消去請求に応じないことは原則として認められておらず、請求が明白に過剰であったり反復的である場合に自らそれを証明することと引き換えに許されているにすぎず（第 12 条第 4 項）、その場合でも本人は監督機関に苦情を申し立てたり、司法救済を求めることが可能である。

また、EU 規則案では訂正や削除が実行された場合、当該データが提供された全ての受領者に対してその旨を連絡する義務が規定されているが、日本の個人情報保護制度にはそのような規定はない。

これらの点で、日本の個人情報保護制度は EU 規則案に比べて緩やかなものとなっている。

２．２．１０　アクセス（開示）・訂正・消去請求の手数料

（１）EU 規則案

第 12 条「データ主体の権利を行使するための手続きとメカニズム」の第 4 項において、アクセスや訂正、消去、データポータビリティ、異議申立の請求に対して取られる措置は、無料でなければならないと規定されている。ただし、請求が明白に過剰であったり反復的なものである場合には、手数料を徴収できると規定されている。

（２）日本の個人情報保護制度

①個人情報保護法

第 30 条において、「第 24 条第 2 項の規定による利用目的の通知又は第 25 条第 1 項の規定による開示を求められたときは、当該措置の実施に関し、手数料を徴収することができる」と規定されている。

②プライバシーマーク制度（JISQ15001：2006）

3.4.4.2 節において、利用目的の通知請求や本人情報の開示請求に対して手数料を徴収するときは、実費を勘案して合理的であると認められる範囲内においてその額を定めなければならないと規定されている。

（３）比較

EU 規則案では、アクセス（開示）・訂正・消去請求の手数料は原則無料とされているのに対し、日本の個人情報保護法とプライバシーマーク制度では開示請求の手数料を徴収できると規定されている点で、EU 規則案に比べて緩やかである。

２．２．１１　データ・ポータビリティの権利

（１）EU 規則案

第 18 条「データ・ポータビリティの権利」において、「データ主体は、個人データが電子的手段かつ構造化され通常利用されている形式で処理されている場合、管理者から処理されているデータのコピーを、通常利用されておりデータ主体による更なる利用を可能とするような電子的かつ構造化された形式で、入手する権利を有するものとする」と規定されている。

（２）日本の個人情報保護制度

①個人情報保護法

データ・ポータビリティの権利については該当する規定がない。

②プライバシーマーク制度（JISQ15001：2006）

データ・ポータビリティの権利については該当する規定がない。

（３）比較

日本の個人情報保護制度には、データ・ポータビリティの権利に関する規定は存在しない。

２．２．１２　異議申立の権利

（１）EU 規則案

第 19 条「異議申立を行う権利」の第 1 項において、データ主体は、当該処理がデータ主

体の権利等に優先することの正当な根拠を管理者が示さない限り、いつでも「第 6 条第 1 項(d)(e)(f)」に基づく個人データ処理に対して異議申立を行う権利を有すると規定されている。

ここで言う第 6 条第 1 項とは「処理の合法性」に関する条項であり、そのうち(d)(e)(f)では、「(d)データ主体の重大な利益を保護するために処理が必要なとき」「(e)公共の利益又は管理者に付与された職権の行使において実行されるタスクの遂行のために処理が必要なとき」又は「(f)管理者が追求する正当な利益の目的のために処理が必要なとき」について、個人データ処理が合法であると規定している。

データ主体がこのような異議申立をした場合、第 17 条第 1 項(c)において、データ主体は当該データを消去してもらう権利を有すると規定されている。

（２）日本の個人情報保護制度

①個人情報保護法

第 27 条第 1 項において、「本人から、当該本人が識別される保有個人データが第 16 条の規定に違反して取り扱われているという理由又は第 17 条の規定に違反して取得されたものであるという理由によって、当該保有個人データの利用の停止又は消去を求められた場合であって、その求めに理由があることが判明したときは、違反を是正するために必要な限度で、遅滞なく、当該保有個人データの利用停止等を行わなければならない」、また第 27 条第 2 項において「本人から、当該本人が識別される保有個人データが第 23 条第 1 項の規定に違反して第三者に提供されているという理由によって、当該保有個人データの第三者への提供の停止を求められた場合であって、その求めに理由があることが判明したときは、遅滞なく、当該保有個人データの第三者への提供を停止しなければならない」と規定されている。

ここで言う第 16 条は「利用目的の制限」に関する条項であり、「あらかじめ本人の同意を得ないで、特定された利用目的の達成に必要な範囲を超えて、個人情報を取り扱ってはならない」と規定されている。ただし、「(1)法令に基づく場合」「(2)人の生命、身体又は財産の保護のために必要がある場合であって、本人の同意を得ることが困難であるとき」「(3)公衆衛生の向上又は児童の健全な育成の推進のために特に必要がある場合であって、本人の同意を得ることが困難であるとき」「(4)国の機関若しくは地方公共団体又はその委託を受けた者が法令の定める事務を遂行することに対して協力する必要がある場合であって、本人の同意を得ることにより当該事務の遂行に支障を及ぼすおそれがあるとき」は例外事項とされている。従って、第 27 条第 1 項にいう「第 16 条の規定に違反して取り扱われている」場合とは、上記(1)～(4) に該当しないにもかかわらず事業者が本人同意を得ずに利用目的を超えて個人情報を取り扱っている場合も含まれると考えられる。

また、第 23 条第 1 項は「第三者提供の制限」に関する条項であり、「あらかじめ本人の同意を得ないで、個人データを第三者に提供してはならない」と規定されている。ただし、

第 16 条と同様、「(1)法令に基づく場合」「(2)人の生命、身体又は財産の保護のために必要がある場合であって、本人の同意を得ることが困難であるとき」「(3)公衆衛生の向上又は児童の健全な育成の推進のために特に必要がある場合であって、本人の同意を得ることが困難であるとき」「(4)国の機関若しくは地方公共団体又はその委託を受けた者が法令の定める事務を遂行することに対して協力する必要がある場合であって、本人の同意を得ることにより当該事務の遂行に支障を及ぼすおそれがあるとき」は例外事項とされている。従って、同様に、第 27 条第 2 項にいう「第 23 条第 1 項の規定に違反して第三者に提供されている」場合とは、上記(1)～(4) に該当しないにもかかわらず事業者が本人同意を得ずに個人情報を第三者に提供している場合も含まれると考えられる。

②プライバシーマーク制度（JISQ15001：2006）

EU 規則案にいうような意味での処理の合法性に関する異議申立の権利は、JISQ15001 では規定されていない。ただし、3.4.4.7 節において、本人から個人情報の利用の停止、消去、又は第三者提供の停止の請求があった場合、業務の適正な実施に著しい支障を及ぼすおそれがある場合等を除き、事業者は請求に応じなければならないことが規定されている。

（３）比較

日本の個人情報保護法でも EU 規則案にいうような「処理の合法性」に対して本人が消去等の請求を行うことは可能と考えられるが、EU 規則案のように、本人による異議申立の権利として明確に認められているわけではない。

２．２．１３　ダイレクトマーケティングに対する異議申立

（１）EU 規則案

第 19 条「異議申立を行う権利」第 2 項において、「個人データがダイレクトマーケティングの目的で処理されている場合、データ主体はそのようなマーケティング目的での自分のデータの処理に対して、無料で異議申立をする権利を有するものとする」と規定されている。

（２）日本の個人情報保護制度

①個人情報保護法

ダイレクトマーケティングに対する異議申立の権利については、個人情報保護法では規定されていない。

②プライバシーマーク制度（JISQ15001：2006）

EU 規則案にいうような意味でのダイレクトマーケティングに対する異議申立の権利は、JISQ15001 では規定されていない。ただし、3.4.2.7 節において、事業者が個人情報を利用

して本人にアクセスする場合に、本人の同意を取得する義務については規定されている。また、3.4.4.7 節において、本人から個人情報の利用の停止、消去、又は第三者提供の停止の請求があった場合、業務の適正な実施に著しい支障を及ぼすおそれがある場合等を除き、事業者は請求に応じなければならないことが規定されている。

（３）比較

日本の個人情報保護制度では、EU 規則案にいうようなダイレクトマーケティングに対する異議申立の権利は、本人の権利として明確に認められている訳ではない。

２．２．１４　プロファイリングを受けない権利

（１）EU 規則案

第 20 条「プロファイリングに基づく措置」において、自然人は、本人の個人的側面の評価や、本人の業務パフォーマンス、経済状況、位置、健康、個人的嗜好、信頼性、行動を分析・予測することを意図した自動処理のみに基づく措置（プロファイリング）を被らない権利を有すると規定されている。

（２）日本の個人情報保護制度

①個人情報保護法

EU 規則案にいうような自動処理に基づくプロファイリングを受けない権利については、該当する規定がない。

②プライバシーマーク制度（JISQ15001：2006）

EU 規則案にいうような自動処理に基づくプロファイリングを受けない権利については、該当する規定がない。

（３）比較

日本の個人情報保護制度には、EU 規則案にいうような自動処理に基づくプロファイリングを受けない権利に関する規定は存在しない。

２．２．１５　文書化

（１）EU 規則案

第 28 条「文書化」において、管理者や処理者、管理者の代表者は、その責任の下で行う全ての処理活動に関して文書を維持しなければならないと規定されている。

（２）日本の個人情報保護制度

①個人情報保護法

個々の個人情報取扱いに関して文書を維持する義務は、個人情報保護法では規定されていない[17]。

②プライバシーマーク制度（JISQ15001：2006）

個々の個人情報取扱いに関して文書を維持する義務は、JISQ15001 では規定されていない。

（３）比較

日本の個人情報保護制度では、EU 規則案にいうように全ての個人情報取扱いに関して文書を維持する義務は規定されていない。

２．２．１６　個人データ違反時の監督機関や個人への報告・連絡

（１）EU 規制案

第 31 条「個人データ違反の監督機関への通知」において、個人データ違反（紛失・盗難・漏洩・不正利用等）があった場合、管理者は不当な遅滞なく、実行可能な場合には個人データ違反に気づいてから 24 時間以内に、監督機関に当該違反について報告しなければならないと規定されている。また、24 時間以内になされない場合には、監督機関への通知は合理的な正当化と共に行われなければならないと規定されている。

また、第 32 条「個人データ違反のデータ主体への連絡」において、個人データ違反がデータ主体の個人データ又はプライバシーの保護に悪影響を及ぼしそうである場合、管理者は、監督機関への通知の後に、不当な遅滞なく、データ主体に当該違反について連絡しなければならないと規定されている。

（２）日本の個人情報保護制度

①個人情報保護法

個人情報保護法においては、個人情報漏洩時等に主務大臣や本人に報告・連絡等を行う義務は規定されていない。

②プライバシーマーク制度（JISQ15001：2006）

3.3.7 節において、個人情報の漏洩、滅失又は毀損が発生した場合に、当該個人情報の内容を速やかに通知し、又は本人が容易に知りうる状態に置くことが規定されている。また、事実関係、発生原因及び対応策を関係機関に直ちに報告することが規定されている。

---

[17] 行政機関個人情報保護法においては、行政機関に対して、当該行政機関が保有している個人情報ファイルについて、一定の事項を記載した帳簿（個人情報ファイル簿）を作成し、公表する義務がある（第 11 条）。

③ISMS（JISQ27001：2006）

附属書 A の A.13.1.1「情報セキュリティ事象の報告」において、情報セキュリティ事象をできるだけすみやかに報告するという管理策が挙げられている。しかし、その報告先については附属書 A や、それらの管理策を具体化した JISQ27002:2006 の中では規定されておらず、また当該管理策を適用するか否かはリスクアセスメントの結果に応じて当該組織が選択することとされている。

（３）比較

EU 規則案にいうような個人データ違反時の監督機関や個人への報告・連絡義務については、プライバシーマーク制度に同様な規定が存在するが、可能な限り 24 時間以内に報告する義務までは規定されていない。

２．２．１７　データ保護影響評価

（１）EU 規則案

第 33 条「データ保護影響評価」において、予定されている処理活動がその性質や範囲、目的に基づきデータ主体の権利と自由に明示的なリスクを提示する場合には、管理者又は管理者を代理する処理者は、当該処理活動が個人データ保護に与える影響について評価を実施しなければならないと規定されている。

（２）日本の個人情報保護制度

①個人情報保護法

個人情報保護法においては、データ保護影響評価（プライバシー影響評価）に該当する規定はない。

②プライバシーマーク制度（JISQ15001：2006）

3.3.3 節において、個人情報の取扱いの各局面におけるリスク分析については規定されている。

③社会保障･税番号制度

マイナンバー法案の第 15 条において、行政機関の長等 は「特定個人情報ファイル」（個人番号をその内容に含む個人情報ファイル）を保有しようとするとき、又は特定個人情報ファイルに重要な変更を加えようとするときは、事前に、特定個人情報保護評価（プライバシー影響評価）を実施しなければならないと規定されている。

④ISMS 制度（JISQ27001：2006）

4.2.1 節において、資産一般に対するリスクアセスメント（リスク評価）については規定

されているが、個人情報の取扱いが個人情報保護に与える影響という観点から評価を実施することについては規定されていない。

（３）比較

日本の社会保障・税番号制度においても、EU 規則案にいうようなデータ保護影響評価（特定個人情報保護評価）の実施が規定されているが、あくまで個人番号を含む個人情報ファイルのみがその対象であり、適用される範囲が狭い。

２．２．１８　データ保護オフィサー

（１）EU 規則案

第 35 条「データ保護オフィサー」において、公的機関や大企業等に対して、データ保護オフィサーを指名する義務が規定されている。

（２）日本の個人情報保護制度

①個人情報保護法

個人情報保護法においては、データ保護オフィサーに該当する規定はない。

②プライバシーマーク制度（JISQ15001：2006）

3.3.4 節において、事業者の代表者は、JISQ15001 規格の内容を理解し実践する能力のある個人情報保護管理者を事業者の内部から指名しなければならないと規定されている。

（３）比較

EU 規則案にいうデータ保護オフィサーは、個人情報保護法には該当する規定がないが、プライバシーマーク制度における個人情報保護管理者に相当するものと考えられる。

２．２．１９　第三国へのデータ移転

（１）EU 規則案

第 5 章「個人データの第三国又は国際組織への移転」（第 40 条～第 45 条）において、一定の条件（十分性決定、標準契約条項、BCR、その他の例外事項）が満たされる場合を除いて、第三国への個人データ移転を禁止している。

（２）日本の個人情報保護制度

①個人情報保護法

個人情報保護法には、第三国への個人情報の移転を制限する規定はない。

②プライバシーマーク制度（JISQ15001：2006）

JISQ15001 には、第三国への個人情報の移転を制限する規定はない。

（３）比較

日本の個人情報保護制度には、第三国への個人情報の移転を制限する規定は存在しない。

２．２．２０　監督機関

（１）EU 規則案

第 46 条「監督機関」及び第 47 条「独立性」において、各加盟国に独立的な監督機関の設立を義務付けている。

また、第 52 条「任務」及び第 53 条「権限」において、監督機関の任務と権限について規定している。

第 52 条では、監督機関の任務として、以下が挙げられている。

- EU 規則の適用の監視、保証
- データ主体又はデータ主体を代表する団体からの苦情聴取
- 他の監督機関との相互協力
- 苦情に基づく調査、又は自ら開始する調査
- ICT や商慣習の発展等、個人データ保護に影響がある事柄の監視
- 個人データ保護に関する相談受付
- 管理者／処理者に対する事前オーソライズ及び事前コンサルテーション
- 行動規範案への意見
- BCR の承認
- 普及啓発活動
- データ主体への助言　等

第 53 条では、監督機関の権限として、以下が挙げられている。

- 管理者／処理者への違反の通知、是正命令
- 管理者／処理者へのデータ主体の権利保障の命令
- 管理者／処理者への情報提供命令
- 管理者／処理者に事前オーソライズ及び事前コンサルテーションを遵守させること
- 管理者／処理者への警告、勧告
- EU 規則に違反して処理されていたデータの訂正・消去・破壊の命令
- 個人データ処理の禁止
- 第三国へのデータ移転の中断
- 個人データ保護に関する意見の公表
- 管理者／処理者に対する調査権限（管理者／処理者が保有する情報や施設へのアクセス権限を含む）
- 違反を司法当局に通報する権限

・ 行政罰（課徴金を含む）を行う権限　等

（２）日本の個人情報保護制度

①個人情報保護法

個人情報保護法上は、個人情報取扱事業者における個人情報保護を監督する立場にあるのは主務大臣[18]である。第 32 条～第 34 条において、主務大臣には以下のような権限が与えられている。

・個人情報取扱事業者からの報告の徴収（第 32 条）
・個人情報取扱事業者に対する助言（第 33 条）
・個人情報取扱事業者に対する是正勧告、是正命令（第 34 条）

②プライバシーマーク制度（JISQ15001：2006）

JISQ15001 には、EU 規則案にいう意味での監督機関に関する規定はない。

③社会保障・税番号制度

マイナンバー法案の第 31 条において、内閣府の外局（いわゆる三条委員会）として個人番号情報保護委員会（第三者機関）を設置することが規定されている。また、第 34 条において、委員長及び委員は独立してその職権を行うことが規定されている。

また、第 33 条において、個人番号情報保護委員会の所掌事務を以下のように規定している。

・ 特定個人情報の取扱いに関する監視、監督
・ 特定個人情報保護評価
・ 特定個人情報の保護についての広報、啓発
・ 上記事務を行うために必要な調査、研究
・ 国際協力　等

第 45 条～第 50 条においては、個人番号情報保護委員会の業務（権限）が以下のように規定されている。

・ 個人番号利用事務等実施者[19]に対する必要な指導、助言
・ 特定個人情報の取扱いの違反者に対する是正勧告、是正命令

---

18 主務大臣は、個人情報取扱事業者が行う事業を所管する大臣等が該当する。ただし、雇用管理に関するものについては厚生労働大臣（船員の雇用管理に関するものについては国土交通大臣）及び当該個人情報取扱事業者が行う事業を所管する大臣等の両者が該当する。（個人情報保護法第 36 条）

19 「個人番号利用事務等実施者」とは、個人番号利用事務を処理する者及び個人番号利用事務の委託を受けた者を指す。「個人番号利用事務」とは、行政機関、地方公共団体、独立行政法人等その他の行政事務を処理する者が、その保有する特定個人情報ファイルにおいて必要な限度で個人番号を利用して処理する事務を指す。

・ 特定個人情報の取扱者等からの報告の徴収、事務所等への立入検査
・ 内閣総理大臣に対する意見の申出
・ 国会に対する所掌事務の処理状況の報告、概要の公表

（３）比較

EU 規則案は監督機関に対して行政府や立法府からの高い独立性を求めているが、日本の個人情報保護法で監督機関に相当する主務大臣はそのような独立性に乏しいものであり、また主務大臣に与えられた権限も EU 規則案で規定された権限の一部に相当するにすぎない。

社会保障・税番号制度で予定されている個人番号情報保護委員会は、いわゆる三条委員会であるため独立性は高いものの、以下の点で EU 規則案に規定されている監督機関の要件を満たしていない。

・ 個人番号情報保護委員会は、個人情報保護全般を対象とする監督機関ではなく、現段階では特定個人情報（すなわち個人番号を内容に含む個人情報）の保護を対象とするにすぎない。
・ 個人からの苦情を受け付けたり、個人に助言を与えることが、（マイナンバー法案では）その所掌事務に含まれていない。
・ 公的機関や事業者等に対して行政罰（課徴金を含む）を行う権限がない。

２．２．２１　司法救済

（１）EU 規則案

個人には、EU 規則を遵守しない個人データ処理に関して、監督機関に苦情を申し立てる権利（第 73 条）や、管理者又は処理者を訴える権利（第 75 条）が与えられている。また、苦情に対して適切な決定を行わない監督機関を訴える権利（第 74 条）も与えられている。

まず、第 73 条において、データ主体は、自己に関する個人データの処理が本規則に遵守していないと考える場合には、いずれかの加盟国の監督機関に苦情を申し立てる権利を有すると規定されている。

また、第 74 条において、データ主体は、自己の権利を保護するために必要な決定がなされていない場合等、監督機関に苦情に基づいて行動することを義務付ける司法救済を求める権利を有すると規定されている。

さらに、第 75 条において、自然人は、EU 規則を遵守しない個人データ処理の結果として自己の権利が侵害されていると考える場合には、司法救済を求める権利を有すると規定されている。また、管理者や処理者に対する訴訟は、当該管理者や処理者が事業所を持つ加盟国の裁判所で行うと規定されている。

（２）日本の個人情報保護制度

①個人情報保護法

個人は、個人情報取扱事業者や認定個人情報保護団体に対して個人情報の取扱いに関する苦情を申し出ることはできる（第 31 条、第 42 条）が、事業者における個人情報の取扱いに対して個人が当該事業者に対する訴訟を行う等の、司法手続による救済については同法上で規定されていない。

まず、第 31 条において、個人情報取扱事業者は、個人情報の取扱いに関する苦情の適切かつ迅速な処理に努めなければならないという努力義務が設けられている。

また、第 42 条において、認定個人情報保護団体は、本人等から事業者の個人情報の取扱いに関する苦情について解決の申出があったときは、その相談に応じ、申出人に必要な助言をし、その苦情に係る事情を調査するとともに、当該対象事業者に対し、その苦情の内容を通知してその迅速な解決を求めなければならないと規定されている。

②プライバシーマーク制度（JISQ15001：2006）

JISQ15001 では、司法手続きによる救済については規定されていない。

（３）比較

EU 規則案では司法手続による救済を求める個人の権利が認められているが、日本の個人情報保護法やプライバシーマーク制度では、そのような権利は規定されていない。

３．EU データ保護指令改定の日本企業への影響

EU データ保護指令改定が日本企業の事業環境に与える影響は、以下に分類できる。

（１）EU 域外企業（日本企業等）に対する影響　→3.1 節
　① EU 域外企業への規制強化　→3.1.1 節
　② 第三国移転に関する条項　→3.1.2 節
（２）EU 域内企業（日本企業の現地法人等）に対する影響　→3.2 節

これらの影響について、以下の各節で順に分析・整理を行う。

３．１　EU 域外企業（日本企業等）に対する影響

３．１．１　EU 域外企業への規制強化

1.4.1 節で述べたように、EU 規則案では、EU 域外企業（EU 域内に事業所を持たない管理者）であっても、EU に居住するデータ主体（個人）のデータを取扱う管理者に対しては、以下のような場合には、EU 規則が適用されることとされている（第 3 条第 2 項）。

(1) EU に居住する個人に商品やサービスを提供している場合
(2) EU に居住する個人の行動をモニターしている場合

すなわち、EU 域外の日本企業等であっても、上記に該当するようなオンラインサービス事業者、パーソナルクラウド事業者、オンライン広告事業者、スマートフォンアプリ事業者等には、EU 規則が適用される[20]。

この第 3 条第 2 項は、直接的には Google やフェイスブック等を念頭に置いた規制強化と考えられるが、日本のオンラインサービス事業者やパーソナルクラウド事業者も EU 市民を対象とする場合は EU 規則が適用されうる[21]。

EU 規則案に規定する管理者の義務には、2 章で比較分析したように、日本の個人情報保護法やプライバシーマーク制度（JISQ15001：2006）よりも厳しい義務が含まれるため、上記に該当する日本企業は国内法と EU 規則の二重遵守を強いられ、多大な追加的負担が発生するものと考えられる。

なお、第 3 条第 2 項については、EU 規則案やその他の関連する欧州委員会の文書を調査

---

[20] ただし、上述のように、日本企業が EU 域内企業から個人データ処理の委託を受けるような場合、例えば（パーソナルクラウド事業者以外の）クラウドサービス事業者の場合には、EU 規則案第 3 条第 2 項の対象にはならずに、次節の「第三国移転」の対象となる。同条項の対象になるのは、あくまで EU 市民（消費者）に直接的に商品・サービスを提供する EU 域外企業に限られる。

[21] 具体的には、ソニーのプレイステーションネットワーク（PSN）や、楽天の Global Market 等が該当すると考えられる。

した限りでは、以下の点が不明である。

①どのような場合に「EU 市民に商品・サービスを提供」しているとみなされるか

例えば、日本ドメインの日本語のショッピングサイトで、EU 市民（若しくは EU 在住の日本人）が商品等を購入するような場合も、第 3 条第 2 項の対象となるのか。

第 25 条第 2 項においては、EU 市民に単に時折、商品やサービスを提供する管理者である場合は、代表者指名の義務を免除されている。しかし、大本となる第 3 条第 2 項には、そのような例外規定がない。

②第 3 条第 2 項が適用される「管理者」の範囲

多国籍企業（ex.フェイスブック）が欧州に事業所（拠点）にもち、EU 市民のデータは欧州拠点でのみ処理しているような場合、欧州拠点のみが EU 規則に規定する管理者の義務に従えばよいのか、それとも EU 域外の本社（ex.米国本社）も「管理者」とみなされ、EU 規則に従う必要があるのか。

すなわち、多国籍企業が欧州拠点のみで EU 市民のデータを処理している場合、

（ⅰ）欧州拠点のみが通常の「管理者」として EU 規則の適用を受ける。

（ⅱ）欧州拠点が当該企業の全世界的なサービスの一環として EU 市民のデータを処理している場合は、本社（ex.米国本社）が域外の「管理者」として第 3 条第 2 項の適用を受ける。

（ⅲ）欧州拠点が独自方針に基づくサービスとして EU 市民のデータを処理している場合でも、本社（ex. 米国本社）が域外の「管理者」として第 3 条第 2 条の適用を受ける。

これらのいずれになるのか。

また、もう 1 つの論点として、多国籍企業が欧州に拠点をもつが、EU 市民のデータは EU 域外で処理しているような場合（若しくは EU 域内でも処理するが EU 域外でも処理しているような場合）、第 3 条第 2 項が適用されるのか、それとも、第三国移転の条項が（欧州拠点から EU 域外拠点へのデータ移転として）適用されるのか。

③第 3 条第 2 項と第三国移転（第 40 条～第 45 条）との関係

「十分性決定」を受けている第三国の管理者（企業）は第 3 条第 2 項の義務を免除されうるのか。それとも、第 3 条第 2 項と第三国移転とは全く異なるスキームなのか。

EU 域外企業に対して、EU 加盟国の監督機関や欧州委員会の命令に従わせようとしても実効性に難があるので、EU 規則案の第 25 条において EU 域内に代表者（representative）を指名する義務を設け、監督機関とのやり取りや刑事罰（第 78 条第 2 項）等はこの代表者に適用されることになっている。ただし、第 25 条第 2 項では、十分性決定を受けた第三国の管理者は代表者指名の義務を免除されている。そうすると、十分性決定を受けている第

三国の管理者は第 3 条第 2 項の義務自体も免除される含みがあるとも思われる。

④セーフハーバー原則を遵守する米国企業の扱い

上記③に関連して、十分性決定を受けている第三国の管理者が、第 3 条第 2 項の義務の何らかの免除を受けうる場合、既存のセーフハーバー原則を遵守する米国企業についても第 3 条第 2 項に関して何らかの義務の免除を受けうるのか。

３．１．２　第三国移転に関する条項

1.4.2 節で述べたように、EU 域内の管理者から EU 域外（第三国）の管理者又は処理者への個人データ移転[22]は、以下の場合に限って可能である。

(1) 欧州委員会による第三国の十分性決定（第 41 条）
(2) 標準契約条項（第 42 条）
(3) BCR（拘束的企業準則）（第 43 条）
(4) その他の例外（第 44 条）

(1)の欧州委員会による十分性決定については、第 41 条において、以下の点を考慮して評価がなされるとされている。

(a) 当該国の法令の内容、データ主体の権利の保障（実効的な行政的救済及び司法救済措置を含む）
(b) 独立の監督機関の存在、監督機関の機能（データ保護法令の遵守の保証、データ主体による権利行使の支援、EU の監督機関との協力）
(c) 国際的なコミットメント

しかし、現状では、日本が欧州委員会から「十分性決定」を受けるためには、2 章で述べた以下の点がネックになると考えられる。これらの点の改善を含めた、国としての環境整備には長大な時間がかかると予想される。

- 個人情報保護法ではデータ主体の権利（開示請求権、訂正請求権等）は明示的に認められていない。すなわち、開示、訂正、消去等は個人の権利ではなく、個人情報取扱事業者の義務にすぎない。
- 第三者機関については、社会保障・税番号制度において個人番号情報保護委員会の設置が予定されているが、この個人番号情報保護委員会は、個人情報保護全般を対象とする監督機関ではなく、現段階では特定個人情報（すなわち個人番号を内容に含む個

[22] 具体的には、①日本企業が管理者として、EU 域内企業から個人データの提供を受ける場合（日本企業が EU の現地法人から従業員データや顧客データを送付してもらう場合を含む）と、②日本企業が処理者として、EU 域内企業から個人データ処理の委託を受ける場合（パーソナルクラウド以外のクラウドサービスの場合を含む）がある。

人情報）の保護を対象とするにすぎない。

また、米国セーフハーバー・スキームのような仕組みが、欧州委員会によって追認されて今後も有効なものであり続けるのか、また、新たに米国以外の第三国について承認されることがありうるのかは、不透明な状況である。

背景として、EU 関係者は以前からセーフハーバー・スキームが不十分なものであり、「政治的妥協の産物」だと考えていることがある。ドイツは 2010 年に、米国へのデータ移転についてセーフハーバーのみでは不十分と表明している。また、欧州委員会のレディング副委員長も 2011 年 12 月のスピーチ[23]で、"I am worried that US 'self-regulation' will not be sufficient to achieve full interoperability between the EU and US"と述べている。

他方、標準契約条項や BCR（拘束的企業準則）については、以下の点から、その手続きが簡素化されている。

- 欧州委員会によって採択された標準契約条項については、第 42 条第 3 項において「標準契約条項は更なるオーソライズを必要としない」と規定されているため、今後はこの標準契約条項を第三国移転の二当事者間で用いれば、監督機関による更なる承認等の手続きは必要なくなると考えられる。
- BCR については、第 43 条第 1 項において、（管理者又は処理者の主要な事務所のある）EU 加盟国の 1 つの監督機関の承認さえ貰えば、EU の他の監督機関は一括でその結果を追認することになっている。
- また、欧州委員会が決定した既存の標準契約条項は、欧州委員会が修正・廃止しない限り有効であり、監督機関が承認した既存の BCR についても、監督機関が修正・廃止しない限り有効である（第 41 条第 8 項及び第 42 条第 5 項）。

従って、第三国移転に関しては、日本企業としては当面は、(2)の標準契約条項や(3)の BCR に基づいて、EU 域内の管理者（日本企業の現地法人を含む）からの個人データ移転を受ける方向で対策をとることが現実的である。

ただし、企業にとって BCR の策定や監督機関からの承認にはそれなりの期間やコストを要すると考えられるため、BCR の拡大適用（例えば、BCR を遵守する企業グループについては「十分なレベルの保護」を保証しているとみなし、標準契約条項がなくてもグループ外 EU 企業からのデータ移転を許可する等）の余地があると望ましい。

また、第 43 条第 1 項の規定を見ると、BCR は当該企業グループ内の全メンバー企業に適用する必要があるように解釈できるが、例えば日本の多国籍企業が、EU 域内の現地法人と日本本社の間でのみ個人データを移転し、他の地域の現地法人（中南米、アフリカ等）とは移転を行わない場合には、それらの実際にデータ移転を行うメンバー企業にのみ BCR

[23] http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/11/851&type=HTML

を適用できると望ましい。

さらに、日本企業にとっては従業員データのみに限って EU 域内の現地法人から日本の本社に移転するケースも多いと考えられ、このような場合は標準契約条項や BCR よりも簡易な移転方法があると望ましい。

３．２　EU 域内企業（日本企業の現地法人等）に対する影響

1.3.2 節で述べたように、EU 規則案では、EU 域内の管理者や処理者に対して、かなりの項目の義務が追加又は強化されている。

とりわけ、以下に挙げる義務については、日本企業の現地法人等の事業環境にとって、大きな影響を及ぼしうる。

①透明で適切なプライバシーポリシーの提供（第 11 条）

EU 規則案において、「透明性」の基準は必ずしも明確ではなく、第 11 条において欧州委員会による詳細規定（委任法令や実施法令）の策定は特に予定されていないにもかかわらず、第 79 条第 5 項において「第 11 条に基づき十分に透明な仕方で情報通知を提供しない者」は監督機関の課徴金の対象（企業の場合、最大で年間連結売上の 1%）とされている。

②明示的な同意の取得（第 7 条）

米国商務省の非公式意見書[24]にも同様な意見が載せられているが、同意が必要なあらゆるケースで、何らの重み付けも行わず、一律に明示的な同意（同意チェックボックスへのチェック等）を求めると、個人はどの場面での同意が重要なものなのかが分からなくなってしまい、事業者からの同意のリクエストに対してむしろ機械的・半自動的に「同意」してしまうおそれがある。また、そのような機械的・半自動的な同意を避けるために、個人に対してあらゆるケースでプライバシーポリシーをよく理解した上での明確な同意を求めることは、サービス利用等に当たって個人に多大な負担をかけ、利便性の妨げとなりかねない。

また、第 7 条第 4 項では「データ主体と管理者の地位の間の従属関係に重大な不均衡が存在する場合には、同意は処理のための法的根拠を与えないものとする」と規定されており、前文の（34）項では「同意は、データ主体と管理者の間に明確な不均衡が存在する場合には、個人データ処理のための有効な法的根拠を与えない。このことは、とりわけデータ主体が管理者に依存する状況にあるとき、特に雇用の関係において被用者の個人データを雇用者が処理する場合に該当する」とされているが、これを文面通りに受け取ると、被用者からの同意は雇用者が被用者データを処理することの法的根拠を与えないことになってしまう。そうすると、同意以外の方法で被用者データの処理の合法性を担保する必要が

---

24 米国商務省の EU 規則案ドラフト（2011 年 11 月）に対する非公式意見書（http://www.edri.org/files/US_lobbying16012012_0000.pdf）。

あるが、その方法は明示されていない。

③忘れられる権利（第 17 条）

個人から個人データの消去請求があった場合、表現の自由の権利を行使する、学術研究で利用する等の理由がある場合を除いて、企業は当該データを消去しなければならない。企業サイドとしてはせっかく収集した個人情報なので、個人を識別できる形式での利用は停止するとしても、ビッグデータ活用等の観点から、個人を識別できない属性情報等については継続利用を望む可能性がある。

消去すべき個人データの範囲については第 17 条では「データ主体に関する個人データ」という記述があるが、改定案に定める「個人データ」の範囲は 1.3.2 節で述べたように必ずしも明確ではない。条文の中では明記されていないものの、前文の(23)項では「データ保護の諸原則はデータ主体がもはや識別可能でない仕方で匿名化されたデータには適用されるべきでない」とあり、匿名化されたデータは「個人データ」に該当しないと考えられ、消去対象にも該当しないと想定することはできる。したがって、この前文(23)項に基づく限り、企業は個人から消去請求があった場合でも、個人を識別できない形式にしたデータ（年齢・性別等の人口統計学的データや、位置データ、購買履歴、オンライン行動履歴等）の保持は引き続き許されると解釈しうるものの、必ずしもその旨が明示されている訳ではなく、また匿名化の基準も明らかではないので、現時点では事業者にとって不確実性の高い条項となっている。

さらに、管理者側で付加した、当該個人に対する評価情報（信用情報など）や診療情報（カルテ、検査結果等）も、本人が消去請求した場合には消去対象となるのか、それとも、これらは第 17 条第 3 項(d)にいう例外事由（管理者が従うべき EU 又は加盟国の法律によりデータを保持する法的義務を遵守する場合）に該当しうるのかについても不明である。

④データ・ポータビリティの権利（第 18 条）

利用者から請求があったとき、個人データのどの範囲まで一定の電子的形式で利用者に渡すのか、例えば購買履歴（Amazon 等）やサイト利用履歴等まで渡す必要があるのかが明示されていない。これらの当該企業のビジネスモデルに大きく関わるデータまで、利用者の請求に応じて他のサービスに移転できる一定形式で渡さなければならないとなると、企業が革新的サービスを生み出すインセンティブを損ねるのではないか。

⑤データ違反時の報告・連絡（第 31 条、第 32 条）

2.2.16 節で述べたように、プライバシーマーク制度（JISQ15001：2006）でも「事実関係、発生原因及び対応策を関係機関に直ちに報告すること」や「当該個人情報の内容を本人に速やかに通知し、又は本人が容易に知りうる状態に置くこと」という規定がある。

しかし、「可能な限り 24 時間以内に」、事実関係（漏洩等したデータの種類、件数等）や

対応策、個人への影響も含めて監督機関や本人に報告・連絡することは、今日の個人データ漏洩事件がしばしば（複数のデータベースに渡る）何百万件という単位でのデータを巻き込むものであることに鑑みれば、漏洩範囲の特定や対応策の決定等に或る程度の時間を要すると考えられ、24 時間以内という義務は厳格すぎるのではないか。

⑥データ保護影響評価（第 33 条）

EU 規則案では、公的機関のみならず民間企業も、第 33 条第 2 項に列挙されたような個人データ処理についてデータ保護影響評価を実施する義務がある。第 34 条第 2 項では、データ保護影響評価において監督機関のコンサルテーションが必要とされるケースが挙げられているが、この事前コンサルテーションに長い期間を要してしまうと、民間企業における（当該個人データ処理を伴う）サービス開始時期がそれだけ後ろ倒しとなり、事業活動に影響を与えるおそれがある。

⑦個人データの範囲（第 4 条(2)）

EU 規則案にいう「個人データ」の範囲については、1.3.2 節で述べたように、とりわけ位置データ、IP アドレス、クッキー等の扱いについて、明確なものとなっていない。「個人データ」の定義は、EU 規則案で規定する管理者（や処理者）の義務全体に関わる事柄であり、例えばあるデータが「個人データ」とみなされるか否かによって、それらのデータに対する安全管理措置（第 30 条）や、忘れられる権利（第 17 条）への対応、個人データ違反時の報告・連絡（第 31 条、第 32 条）、監督機関による課徴金（第 79 条）等は大きく異なってくる。そのため、個人データの範囲が明確でないことは、民間企業の事業活動の上で大きな不確実性をもたらす要因となる。

⑧監督機関による課徴金（第 79 条）

監督機関による課徴金は、第 79 条第 4 項～第 6 項において第何条に対するどのような違反かに応じて（企業の場合は）最大で年間連結売上の 0.5%、1%、2%という 3 パターンに分類されている。企業の個人データ違反（個人データ漏洩等）そのものに対する課徴金は設定されていないが、第 30 条（安全管理措置）に基づき適切な措置を実施していなかったり、第 31 条及び第 32 条に基づき監督機関やデータ主体に対して個人データ違反に関する報告や通知をしなかったりした場合には、（企業の場合は）最大で年間連結売上の 2%の課徴金が科されうる。この課徴金の上限額は、非常に高額なものである。

また、課徴金の額の決定については、第 79 条第 2 項において「行政的課徴金の額は、違反の性質、重大性及び持続性、違反の故意的又は過失的性質、当該自然人又は法人の責任の度合い及び当人による以前の違反の度合い、第 23 条に従い実施された技術的及び組織的措置及び手続き、並びに違反を救済するための監督機関への協力の度合いに応じて決めるものとする」とされているが、その具体的な算定基準は不明であり、第 79 条において欧州

委員会による詳細規定（委任法令や実施法令）の策定は予定されていない。

付録１：報告書のサマリー

１．EU データ保護指令の概要

（１）個人データ取扱いに係る個人の保護及び当該データの自由な移動に関する指令。1995 年採択、1998 年発効。

（２）EU 加盟国及び EEA（欧州経済領域）加盟国合計 30 ヶ国に対して同指令に基づく個人情報保護に関する国内法規を要求するもの。

（３）この指令により、EU 域内の企業から、十分なレベルの個人データ保護を講じていない第三国の企業への個人データの移転が禁じられることとなり、日本はその十分性を認められていない。

２．EU データ保護指令の改定の背景と経緯

（１）今回の改正は、EU 指令採択から 15 年以上が経ち、インターネットを初めとする急速な技術的進歩やグローバル化の進展により発生してきた新たな課題に対処するためのもの。

①急速な ICT 技術の進歩やグローバル化の進展と、それによるリスクの拡大

②現行のデータ保護スキームに対する企業の不満の増大

（２）今般、2 年以上の検討及び関係者とのコンサルテーション期間を経て、2012 年 1 月 25 日に欧州委員会が改定案を公表。

①「EU データ保護規則」： EU における一般的なデータ保護のフレームワーク

② 犯罪の防止・捜査・発見・訴追、刑事罰の執行の目的で処理される個人データの保護に関する指令

（→本報告書では①の EU 規則案について記載。）

（３）欧州委員会は今後、欧州議会及び欧州連合理事会と緊密に協力し、2012 年内の合意・採択を目指す。採択から 2 年後に発効の見込み。

３．EU 規則案における主要な改定点

（１）従来の「指令（Directive)」から「規則（Regulation） 」に格上げ

（２）個人データ保護の権利の強化（自己情報コントロール権の強化など）

（３）EU 域内でのデータ保護ルールの一元化（EU 域内企業にとってメリット）

（４）グローバル環境でのデータ保護ルールの詳細化（第三国移転ルールの詳細化など）

４．EU 規則案と日本の個人情報保護制度との比較

（１）日本の個人情報保護法は、「対象事業者の範囲が狭い」「一定の場合を除いて本人同意が必要とされていない」「特定カテゴリ情報の取扱いに関する規定がない」「開示・訂正・消去請求権が明示的に認められていない」「独立的な監督機関に関する規定がない」など多

くの点で、EU 規則案よりも規定が緩やかである。
（２）プライバシーマーク制度（JISQ15001：2006 に準拠）は、個人情報保護法よりも EU 規則案寄りの規定とはなっているが、多くの点でやはり EU 規則案よりも規定が緩やかである。

付録２：EU データ保護規則案 条文和訳集（仮訳）

※本報告書に掲載した条文訳は仮訳になりますので、原文もご参照ください。

第 1 章　一般的条項

第 1 条　主題と目的

1.本規則は個人データ処理に係る個人の保護に関するルール及び個人データの自由な移動に関するルールを規定する。

2.本規則は、自然人の基本的権利と自由、とりわけ個人データ保護の権利を保護する。

3.個人データの処理に係る個人の保護に関連した理由で、EU 域内での個人データの自由な移動が制限されたり禁止されたりしないものとする。

第 2 条　内容的なスコープ

1.本規則は、全部又は一部を自動的手段で行う個人データ処理に適用される。また、ファイリングシステムの一部を構成する個人データ、又はファイリングシステムの一部を構成することを意図した個人データの自動的手段以外での処理に適用される。

2.本規則は以下の個人データ処理には適用されない。

(a)EU 法の範囲外となる活動の過程での処理。とりわけ、国家安全保障に関する場合。

(b)EU 機関、EU 団体、EU オフィスによる処理。

(c)EU 条約の第 2 章の範囲内の活動を実行する際の、加盟国による処理。

(d)自然人が完全な個人的活動又は家庭活動において何らの利益を得ることなく行う処理。

(e)犯罪の防止、捜査、発見若しくは訴追、又は刑事罰の執行のための当局による処理。

3.（略）

第 3 条　地域的なスコープ

1.本規則は、EU 域内に事業所を持つ管理者又は処理者（an establishment of a controller or a processor in the Union）の活動に関係する個人データの処理に適用される。

2.本規則は、EU 域内に事業所を持たない管理者による、EU 域内に居住するデータ主体の個人データの処理に、処理活動が以下に関連している場合に適用される。

(a)そのようなデータ主体に商品又はサービスを提供すること。又は

(b)そのようなデータ主体の行動をモニターすること。

3.本規則は、国際公法の規定に基づき加盟国の国内法が適用される場合には、EU 域内に事業所を持たない管理者による個人データ処理に適用される。

第 4 条　定義

本規則の目的上、

(1)「データ主体（data subject）」は、識別された自然人、又は管理者、若しくは他の自然人若しくは法人によって合理的に利用される可能性の高い手段によって、直接的若しくは間接的に、とりわけ識別番号、位置データ、オンライン識別子、若しくは当該人物の肉体的、生理学的、遺伝的、精神的、経済的、文化的若しくは社会的アイデンティティに特有な１つ以上の要素を参照することによって、識別されうる自然人を意味する。
(2)「個人データ（personal data）」は、データ主体に係る全ての情報を意味する。
(3)「処理（processing）」は、自動的手段によるか否かに関わらず、個人データ若しくは個人データのセットに対して実行されるあらゆるオペレーション又はオペレーションのセットを意味する。収集（collection）、記録（recording）、組織化（organization）、構造化（structuring）、保存（storage）、編集（adaptation）若しくは変更（alteration）、検索（retrieval）、参照（consultation）、利用（use）、伝送（transmission）・頒布（dissemination）若しくはその他の方法による開示（disclosure）、整列（alignment）若しくは結合（combination）、消去（erasure）、又は破壊（destruction）を含む。
（中略）
(5)「管理者（controller）」は、単独又は他者と共同で、個人データ処理の目的、条件及び手段を決定する自然人、法人、公的機関、その他のあらゆる組織を意味する。処理の目的、条件及び手段が EU 又は加盟国の法律で決定されている場合は、管理者又はその任命のための具体的基準は、EU 又は加盟国の法律によって指定（指名）することができる。
(6)「処理者（processor）」は、管理者の代わりに個人データを処理する自然人、法人、公的機関、その他のあらゆる組織を意味する。
（中略）
(8)「データ主体の同意（the data subject's consent）」は、ステートメント又は明確な肯定的動作によって、束縛を受けずに（freely）与えられる、特定の、情報を十分に与えられた、それによって自分に関する個人データが処理されることに合意することを示す、データ主体の明示的な希望の表示を意味する。
(9)「個人データ違反（personal data breach）」は、伝送、保存又はその他の処理がされている個人データの偶発的若しくは不法な破壊、紛失、改変、無権限の開示、又はアクセスを導くセキュリティ違反を意味する。
（中略）
(13)「主要な事業所（main establishment）」は、管理者については、個人データの処理の目的、条件及び手段に関して主要な決定がなされる EU 域内の事業所の場所を意味する。EU 域内で個人データの処理の目的、条件及び手段に関して決定がなされない場合には、主要な事業所は、EU 域内における管理者の事業活動の文脈における主要な処理活動が行われる場所である。処理者については、「主要な事業所」は、EU 域内における中央管理機能が存在する場所を意味する。
(14)「代表者（representative）」は、明示的に管理者によって指名され、本規則の下で当

該管理者の義務に関して管理者の代わりに行為し、EU 域内の監督機関及び他の団体が働きかけを行いうるような、EU 域内に事業所を持つ（established in the Union）自然人又は法人を意味する。

（中略）

(17)「拘束的企業準則（binding corporate rules）」は、EU の加盟国の領地内に事業所を持つ管理者又は処理者によって遵守される、1 つ以上の第三国に位置する同じ企業グループ（group of undertakings）内の管理者又は処理者に個人データを移転するための個人データ保護ポリシーを意味する。

(18)「子ども（child）」は、18 歳未満のあらゆる人間を意味する。

(19)「監督機関（supervisory authority）」は、第 46 条に則り加盟国によって設立された公的機関を意味する。

第 2 章　諸原則

第 5 条　個人データ処理に関する諸原則

個人データは、

(a)合法に、公平に、及び、データ主体との関係において透明な仕方で処理されなければならない。

(b)特定の、明示的、かつ妥当な目的で収集されなければならず、これらの目的と矛盾するやり方で処理されてはならない。

(c)データが処理される目的に十分であり、関連性があり、かつ必要最低限なものでなければならない。また、個人データは、個人データを含まない情報の処理によっては当該目的を果たすことができない場合に限り、処理されるものとする。

(d)正確で、更新されたものでなければならない。処理の目的を考慮して、不正確な個人データが遅滞なく消去又は訂正されることを保証するためのあらゆる合理的な措置が取られなければならない。

(e)個人データの処理目的にとってもはや必要でないデータ主体を特定できるような形式で保存しなければならない。個人データは、第 83 条のルールと条件に則り歴史的、統計的又は科学的研究目的でのみ処理され、かつ保存を続けることの必要性を評価するために定期的なレビューが実施される場合に限り、長期間保存することができる。

(f)管理者の責任の下で処理されなければならない。管理者は、各処理活動において、本規則の条項を遵守していることを保証し、証明するものとする。

第 6 条　処理の合法性

1.個人データの処理は、以下のうち少なくとも 1 つが適用される限りにおいて合法であるものとする。

(a)データ主体が 1 つ以上の特定の目的に対して個人データの処理に同意を与えているとき。

(b)データ主体が当事者であるような契約の履行のために、又は契約締結に先立ちデータ主体の請求に対処するために処理が必要なとき。

(c)管理者が従わなければいけない法的義務を遵守するために処理が必要なとき。

(d)データ主体の重大な利益を保護するために処理が必要なとき。

(e)公共の利益又は管理者に付与された職権の行使において実行されるタスクの遂行のために処理が必要なとき。

(f)管理者が追求する正当な利益の目的のために処理が必要なとき。ただし、そのような利益よりも、個人データの保護を要求するデータ主体の利益又は基本的権利及び自由が上回る場合、とりわけデータ主体が子どもである場合は除く。

2.歴史的、統計的又は科学的研究の目的で必要な個人データの処理は、第 83 条にいう条件及び安全管理措置の下で合法であるものとする。

3.第 1 項(c)及び(e)にいう処理の根拠は以下において提供されなければならない。

(a)EU 法。又は

(b)管理者が従う加盟国の法律。

加盟国の当該法律は公共の利益の目的に合致しているか、又は、他者の権利及び自由を保護するために必要なものであり、個人データの保護の権利の本質を尊重し、かつ追求される正当な目的に釣り合ったものでなければならない

4.さらなる処理の目的が個人データが収集された際の目的と両立しない場合、当該処理は少なくとも第 1 項の(a)から(e)の 1 つに基づく法的根拠を有していなければならない。

5.欧州委員会は、子どもに関する個人データを処理する場合を含め、様々な分野やデータ処理の状況に合わせて、第 1 項(f)にいう条件をより詳細に規定するために、第 86 条に則り委任された法令を採択する権限を与えられるものとする。

第 7 条　同意の条件

1.管理者は、データ主体が特定の目的での個人データ処理に同意を与えたことを証明する責任を負うものとする。

2.データ主体の同意が他の用件にも関係する書面での宣言と一緒に与えられることになっている場合、同意を与えることの要求は他の用件から明示的に区別可能な形でなされなければならない。

3.データ主体は、自分の同意をいつでも撤回する権利を有するものとする。同意の撤回は、撤回の前の同意に基づく処理の正当性に影響を与えないものとする。

4.データ主体と管理者の地位の間の従属関係に重大な不均衡が存在する場合には、同意は処理のための法的根拠を与えないものとする。

第 8 条　子どもの個人データの処理
（略）

第 9 条　特別なカテゴリの個人データの処理
（略）

第 10 条　個人を識別できない処理
管理者によって処理されるデータで、当該管理者が自然人を識別できない場合、管理者は本規則の条項を遵守する目的のためのみに当該データ主体を識別するための追加的情報を獲得する義務は負わないものとする。

第 3 章　データ主体の権利

第 1 節　透明性とモダリティ

第 11 条　透明な情報通知（information）と連絡
1.管理者は、個人データの処理及びデータ主体の権利の行使に関して透明かつ容易にアクセスできるポリシーを有するものとする。
2.管理者は、データ主体に対し、個人データの処理に関するあらゆる情報通知及び連絡を、とりわけ子ども向けの情報について、データ主体に合わせた明確かつ平易な言葉を使って、分かりやすい形態で提供するものとする。

第 12 条　データ主体の権利を行使するための手続きとメカニズム
1.管理者は、第 14 条で規定する情報通知（information）を提供するための手続き及び第 13 条、第 15 条から第 19 条で規定するデータ主体の権利を行使するための手続きを確立するものとする。管理者はとりわけ、第 13 条、第 15 条から第 19 条で規定する措置の請求を容易にするためのメカニズムを提供するものとする。個人データが自動的手段で処理されている場合には、管理者は請求を電子的に行えるような手段も提供するものとする。
2.管理者は、遅滞なく、少なくとも請求の受領後 1 ヶ月以内に、第 13 条、第 15 条から第 19 条に従って何らかの措置が取られたか否かを、データ主体に知らせ、また請求された情報を提供するものとする。この期間は、複数のデータ主体が権利を行使しており、管理者の側の不必要で不釣合いな努力を避けるために合理的な範囲で彼らの協力が必要な場合には、もう 1 ヶ月延長することができる。このような通知は、書面でなされるものとする。データ主体が電子的形式で請求を行った場合には、通知は電子的形式で提供することが可能である。
3.管理者がデータ主体の請求に対して措置をとることを拒否する場合、管理者はデータ主体に拒否の理由、及び監督機関に苦情を申し立てたり、司法救済を求めたりすることが可能

であることを通知するものとする。
4.第 1 項にいう情報通知（information）、及び請求に対して取られる措置は、無料であるものとする。請求が明白に過剰である場合、とりわけ反復的なものである場合には、管理者は情報通知の提供若しくは請求された措置の実施に対して手数料を徴収すること、又は請求された措置を取らないことができる。このような場合、管理者は請求が明白に過剰であることを証明することの責任を負うものとする。
5.欧州委員会は、第 4 項で規定された明白に過剰な請求と料金に関してより詳細な基準と条件を規定するために、第 86 条に則り委任された法令を採択する権限を与えられるものとする。
6.欧州委員会は、第 2 項にいう連絡（電子的形式を含む）に関して標準フォームと標準手続きを規定することができる。そうすることによって、欧州委員会は中小企業のために適切な措置を取るものとする。これらの実施法令は、第 87 条(2)で規定された審査（examination）手続きに則り採択されるものとする。

第 13 条　受領者に関係した権利
管理者は、第 16 条及び第 17 条に則り実行された全ての訂正又は消去について、その連絡が不可能であることが判明したり、不釣合いな努力を必要とするものでないかぎり、データが開示された全ての受領者に対して連絡するものとする。

第 2 節　情報通知（information）と、データへのアクセス

第 14 条　データ主体への情報通知（information）
1.データ主体に関する個人データが収集される場合、管理者は当該データ主体に少なくとも以下の情報を提供するものとする。
(a)管理者、（存在する場合には）管理者の代表者、及びデータ保護オフィサーの身元及び連絡先情報。
(b)意図された個人データの処理目的。処理が第 6 条(1)の(b)に基づく場合は当該契約条件と一般条件、処理が第 6 条(1)の(f)に基づく場合は管理者が追求する正当な利益を含める。
(c)個人データが保存される期間。
(d)管理者にデータ主体に関する個人データへのアクセス、及びそれらの訂正若しくは消去を請求する権利、又はそれらの個人データの処理に異議申立をする権利の存在。
(e)監督機関に苦情を申し立てる権利、及び監督機関の連絡先情報。
(f)個人データの受領者、又は受領者のカテゴリ。
(g)適用される場合には、管理者が第三国又は国際組織にデータを移転することを意図していること、及び欧州委員会の十分性決定に言及することによる当該第三国若しくは国際組織の保護のレベル。

(h)個人データが収集される特定の環境を考慮に入れ、データ主体に関係する公正な処理を保証するために必要な更なる情報。

2.データ主体から（直接）当該個人データが収集される場合、管理者は第 1 項にいう情報に加えて、データ主体に、個人データの提供が義務であるのか又は任意であるのか、及び当該データを提供しない場合に想定される結果について、情報提供するものとする。

3.データ主体から（直接）当該個人データが収集されない場合、管理者は第 1 項にいう情報に加えて、データ主体に、当該データを取得したソースについて、情報提供するものとする。

4.管理者は第 1 項、第 2 項及び第 3 項にいう情報を以下の方法で提供するものとする。

(a)個人データがデータ主体から取得された時点。又は、

(b)個人データがデータ主体から収集されない場合、当該データが収集その他の処理を受ける特定の環境を考慮に入れ、当該データの記録の時点若しくは収集から合理的な期間以内。若しくは、他の受領者への開示が予定されている場合には、少なくとも当該データが最初に開示される時点。

5.第 1 項から第 4 項は、以下の場合には適用されない。

(a)データ主体が既に第 1 項、第 2 項及び第 3 項にいう情報を知っているとき。又は、

(b)データがデータ主体から取得されておらず、かつ、情報の提供が不可能であることが判明するか若しくは不釣合いな労力を必要とする場合。又は、

(c)データがデータ主体から取得されておらず、かつ、記録若しくは開示が明示的に法律で規定されている場合。又は、

(d)データがデータ主体から取得されておらず、かつ、第 21 条に基づき、情報の提供が EU 法若しくは加盟国法に規定された他者の権利及び自由を損なうものである場合。

6.第 5 項(b)にいう場合、管理者はデータ主体の正当な利益を保護するための適切な措置を提供するものとする。

7. 欧州委員会は、第 1 項(f)にいう受領者のカテゴリの基準、第 1 項(g)にいう潜在的なアクセスの通知（？）の要件、第 1 項(h)にいう特定分野及び特定状況のために必要な更なる情報の基準、及び第 5 項(b)で規定された例外のための条件と適切な安全管理措置について詳細に規定するために、第 86 条に則り委任された法令を採択する権限を与えられるものとする。これにより、欧州委員会は中小企業に対して適切な措置を講じるものとする。

8.欧州委員会は、必要な場合には様々な分野とデータ処理の状況に特有な性質及びニーズを考慮に入れ、第 1 項から第 3 項にいう情報を提供するための標準フォームを規定することができる。これらの実施法令は、第 87 条(2)で規定された審査手続きに則り採択されるものとする。

第 15 条　データ主体のアクセスの権利

1.データ主体は、自分に関する個人データが処理されているか否かについての確認を、請求

に応じて、いつでも管理者から取得する権利を有するものとする。そのような個人データが処理されている場合には、管理者は以下の情報を提供するものとする。

(a)処理の目的。

(b)関係する個人データのカテゴリ。

(c)個人データが開示される予定の、又は開示された受領者又は受領者のカテゴリ。とりわけ、第三国の受領者。

(d)個人データが保存される期間。

(e)管理者にデータ主体に関する個人データの訂正若しくは消去をしてもらう権利の存在、又は個人データの処理に異議申立をする権利の存在。

(f)監督機関に苦情を申し立てる権利及び監督機関の連絡先情報。

(g)処理されている個人データに関する連絡、及びそれらのソースについて利用可能な情報に関する連絡。

(h)少なくとも第 20 条にいう措置の場合には、当該処理の重要性及び想定される帰結。

2.データ主体は処理されている個人データについての連絡を管理者から取得する権利を有するものとする。データ主体が当該請求を電子的形式で行った場合には、データ主体によって他の方式が請求されない限り、情報は電子的形式で提供されるものとする。

3.欧州委員会は、第 1 項(g)にいうデータ主体に連絡する個人データの内容に関して、より詳細な基準と要件を規定するために、第 86 条に則り委任された法令を採択する権限を与えられるものとする。

4.欧州委員会は、様々な分野やデータ処理の状況に特有な事情や必要性を考慮に入れながら、データ主体の本人確認方法やデータ主体への個人データの連絡方法を含め、第 1 項にいう情報へのアクセスを請求したり受理したりするための標準フォームと標準手続きを規定することができる。これらの実施法令は、第 87 条(2)で規定された審査手続きに則り採択されるものとする。

第 3 節　訂正と消去

第 16 条　訂正する権利

データ主体は、不正確な自分に関する個人データを管理者に訂正してもらう権利を有するものとする。データ主体は、修正のためのステートメントを補足する方法も含めて、不完全な個人データを完全なものにする権利を有するものとする。

第 17 条　忘れられる権利と消去する権利

1.データ主体は、以下のいずれかの場合、とりわけデータ主体が子どもであった間に取得された個人データに関して、管理者に自分に関する個人データを消去してもらう権利、及び自分に関する個人データの頒布を停止してもらう権利を有するものとする。

(a)当該データがもはやデータの収集その他の処理の目的に関して必要がない場合。

(b)第 6 条(1)(a)に則り、データ主体が当該処理の元となる同意を撤回した場合、又は同意した保有期間の期限が来た場合であって、かつ当該データ処理に関する他の法的根拠が存在しない場合。

(c)データ主体が第 19 条に従い個人データの処理に異議申し立てをした場合。

(d)その他、当該処理がその他の理由で本規則を遵守していない場合。

2.第 1 項にいう管理者が個人データを公開している場合、管理者は、管理者がその公開に責任を負うデータに関して、そのようなデータを処理する第三者に、データ主体が個人データへの全てのリンク、又は個人データのコピー若しくは複製を削除することを請求していることを通知するためのあらゆる合理的な措置（技術的措置を含む）を取るものとする。管理者が第三者に個人データの公開を許可した場合には、管理者はこの公開に対して責任を負うとみなされるものとする。

3.管理者は、以下に挙げるような個人データの保持が必要な場合を除き、遅滞なく消去を実行するものとする。

(a)第 80 条に従い、表現の自由の権利を行使する場合。

(b)第 81 条に従い、公共の健康医療の領域における公共の利益の理由の場合。

(c)第 83 条に従い、歴史的、統計的及び科学的研究の目的の場合。

(d)管理者が従うべき EU 又は加盟国の法律によりデータを保持する法的義務を遵守する場合。当該法律は、公共の利益の目的に適合し、個人データ保護の権利の本質を尊重し、追及する正当な目的に比例したものとする。

(e)以下の第 4 項で規定する場合。

4.以下の場合、管理者は消去に代わって、個人データの処理を制限するものとする。

(a)データ主体によってデータの正確性に異議申し立てがなされている場合、管理者に当該データの正確性を検証することを可能とする期間。

(b)管理者がもはや任務を達成するために当該データを必要としないが、証明の目的のためにデータを維持する必要がある場合。

(c)当該処理が不法であり、かつデータ主体が消去に反対し、その代わりデータの利用の制限を請求した場合。

(d)第 18 条(2)に従い、データ主体が個人データを他の自動処理システムに移転することを請求した場合。

5.第 4 項にいう個人データは、保存を例外として、証明の目的若しくはデータ主体の同意の下で、又は他の自然人若しくは法人の権利を保護する目的若しくは公共の利益の目的の下でのみ処理することが可能である。

6.個人データの処理が第 4 項に従い制限される場合は、管理者は処理の制限を解除する前に、データ主体に知らせるものとする。

7.管理者は、個人データの消去のためのタイムリミット及び個人データの保存の必要性を定

期的にレビューするためのタイムリミットが遵守されていることを保証するものとする。
8.消去が実施された場合、管理者は当該個人データを処理しないものとする。
9.欧州委員会は、以下についてより詳細に規定するために、第 86 条に則り委任された法令を採択する権限を与えられるものとする。
(a)特定の部門及び特定のデータ処理について第 1 項を適用するための基準と要件。
(b)第 2 項にいう、公共に利用可能な通信サービスから個人データの公共のインターネットリンク、コピー又は複製を削除するための基準。
(c)第 4 項にいう、個人データの処理の制限のための基準と要件。

第 18 条　データ・ポータビリティの権利
1.データ主体は、個人データが電子的手段かつ構造化され通常利用されている形式で処理されている場合、管理者から処理されているデータのコピーを、通常利用されておりデータ主体による更なる利用を可能とするような電子的かつ構造化された形式で、入手する権利を有するものとする。
2.データ主体が個人データを提供し、処理が同意又は契約に基づく場合、データ主体は自らの個人データ、及びデータ主体によって提供され、自動処理システムによって保持されているその他の情報を、他の自動処理システムに、通常利用されている電子的な形式において、個人データを撤収する管理者から妨害されることなく、移転する権利を有するものとする。
3.欧州委員会は第 1 項にいう電子的な形式、並びに第 2 項に従って個人データを移転するための技術標準、手順（modalities）及び手続きについて規定することができる。これらの実施法令は、第 87 条(2)で規定された審査手続きに則り採択されるものとする。

第 4 節　異議申立を行う権利、プロファイリング

第 19 条　異議申立を行う権利
1.データ主体は、彼らに固有な状況に基づき、当該処理がデータ主体の利益又は基本的権利及び自由に優先することの説得力のある正当な根拠を管理者が示さない限り、いつでも、第 6 条第 1 項(d)(e)(f)に基づく個人データ処理に対して異議申立を行う権利を有するものとする。
2.個人データがダイレクトマーケティングの目的で処理されている場合、データ主体はそのようなマーケティング目的での自分のデータの処理に対して、無料で異議申立をする権利を有するものとする。この権利は、理解しやすい方法でデータ主体に明示的に提供されるものとし、また他の情報を明確に区別できるものであるものとする。
3.異議申立が第 1 項及び第 2 項に従い提出された場合、管理者はもはや関係する個人データについて利用その他の処理を行わないものとする。

第 20 条　プロファイリングに基づく措置

1.各自然人は、当該自然人に対する法的効果を生み出すような措置若しくは当該自然人に重大な影響を与えるような措置であって、かつ、当該自然人に関する個人的側面を評価すること、若しくはとりわけ業務パフォーマンス、経済状況、位置、健康、個人的嗜好、信頼性若しくは行動を分析若しくは予測することを意図した自動処理のみに基づく措置を被らない権利を有するものとする。

2.本規則の他の条項の下で、以下の場合に限り、ある人は第 1 項にいう種類の措置を被る可能性がある。

(a) データ主体による契約締結若しくは契約履行の請求に応じて、若しくは、人間の介在を得る権利など、データ主体の正当な利益を保護するための適切な措置が提示されることで、当該処理が契約締結若しくは契約履行の過程で実行される場合。又は、

(b)当該処理が EU 法又は加盟国の法律で明示的にオーソライズされ、かつ当該法律がデータ主体の正当な利益を保証する適切な措置を規定している場合。又は、

(c)当該処理が、第 7 条に規定する条件及び適切な安全管理措置の下、データ主体の同意に基づく場合。

3.自然人に関する個人的側面を評価することを意図した個人データの自動処理は、第 9 条にいう特別なカテゴリの個人データのみに基づくものであってはならない。

4.第 2 項にいう場合、第 14 条の下で管理者によって提供される情報は第 1 項にいう種類の措置のための処理の存在、及びそのような処理がデータ主体に与える想定される影響に関する情報を含めるものとする。

5.欧州委員会は、第 2 項にいうデータ主体の正当な利益を保護するための適切な措置に関してより詳細な基準と条件を規定するために、第 86 条に則り委任された法令を採択する権限を与えられるものとする。

第 5 節　制限

第 21 条　制限

1.EU 法又は加盟国の法律は、そのような制限が民主主義社会において以下の事柄を保護するために必要かつ釣り合いの取れた措置を構成する場合には、第 5 条(a)から(e)、第 11 条から第 20 条、及び第 32 条で提供される義務及び権利の範囲を、法制上の措置によって制限することができる。

(a)公共の安全保障。

(b)犯罪の防止、捜査、発見及び訴追。

(c)EU または加盟国のその他の公共の利益、とりわけ EU 又は加盟国の重要な経済的又は財政的な利益。通貨、予算及び租税関連の事柄、並びに市場安定性及び一体性の保護を

含む。

(d)規制された専門職業の倫理違反の防止、捜査、発見及び訴追。

(e)(a)、(b)、(c)及び(d)にいうケースにおける職権の行使に、たとえ一時的にせよ、関連した監視、検査、又は規制機能。

(f)データ主体の保護、又は他者の権利及び自由の保護。

2.とりわけ、第 1 項にいういかなる法制上の措置も、管理者の処理及び決定によって追求される目的に関する明示的な条項を含むものとする。

第 4 章　管理者と処理者

第 1 節　一般的義務

第 22 条　管理者の責任

1.管理者は、個人データ処理が本規則を遵守して実施されることを保証し、証明（demonstrate）できるようにするために、ポリシーを採択し、適切な措置を取るものとする。

2.第 1 項にいう措置は、とりわけ以下のものを含めるものとする。

(a)第 28 条に従い、文書を保存すること。

(b)第 30 条で規定されたデータセキュリティ要件を実施すること。

(c)第 33 条に従い、データ保護影響評価を実施すること。

(d)第 34 条(1)及び(2)に従い、監督機関の事前オーソライズ又は事前コンサルテーションの要件を遵守すること。

(e)第 35 条(1)に従い、データ保護オフィサーを指名すること。

3.管理者は、第 1 項と第 2 項で規定された措置の実効性の検証を保証するメカニズムを導入するものとする。この検証は、それが適切であれば、独立的な内部又は外部の監査者によって実施されるものとする。

4.欧州委員会は、第 2 項で規定された以外の第 1 項にいう適切な措置に関してより詳細な基準と要件を、第 3 項で規定された検証と監査メカニズムに関する条件を、及び第 3 項における適切性の基準を規定し、また中小企業のための特別措置を考慮するために、第 86 条に則り委任された法令を採択する権限を与えられるものとする。

第 23 条　データ保護・バイ・デザインとデータ保護・バイ・デフォルト

1.最先端の技術と実施のコストを考慮しながら、管理者は処理のための手段を決定する時点と処理を行う時点の両方で、当該処理が本規則の要件に合致し、データ主体の権利の保護を保証するようなやり方で、適切な技術的及び組織的な措置と手続きを導入するものとする。

2.管理者は、デフォルトとして、個人データが明示的な処理目的に必要な場合にのみ処理さ

れるように、また特にこれらの目的に必要最小限な範囲（データの量とデータ保持期間の両面）を超えて収集又は保持されないように保証するためのメカニズムを導入するものとする。とりわけ、これらのメカニズムは、デフォルトとして、個人データが不特定の人間にアクセス可能ではないように保証するものとする。

3. 欧州委員会は、第 1 項及び第 2 項にいう適切な措置とメカニズムに関して、より詳細な基準と要件、とりわけ分野、製品及びサービスを跨って適用可能なデータ保護・バイ・デザインの要件を規定するために、第 86 条に則り委任された法令を採択する権限を与えられるものとする。

4.欧州委員会は、第 1 項及び第 2 項で規定された要件のための技術的標準を規定することができる。これらの実施法令は、第 87 条(2)で規定された審査手続きに則り採択されるものとする。

第 24 条　共同管理者

管理者が他者と共同でデータ処理の目的、条件及び手段を決めた場合、当該共同管理者は、共同管理者同士の調整により、とりわけデータ主体が権利を行使するための手続きとメカニズムに関して、本規則の下での義務を遵守するためのそれぞれの責任について決定するものとする。

第 25 条　EU 域内に事業所を持たない管理者の代表者（representative：代理人）

1.管理者が EU 域内に事業所を持たない場合（Where a controller is not established in the Union）、第 3 条(2)で規定された状況下では、管理者は EU 域内における代表者を指名するものとする。

2.この義務は以下の場合には適用されないものとする。

(a)管理者が、第 41 条に則り当該国が保護の十分なレベルを保証していると欧州委員会が決定した第三国に事業所を持つ場合。又は、

(b)250 人未満の職員を雇用する企業の場合。又は、

(c)公的機関又は公的団体の場合。又は、

(d)EU 域内に居住するデータ主体に、単に時折、商品やサービスを提供する管理者である場合。

3.代表者は、商品やサービスの提供においてその個人データが処理されているデータ主体、又はその行動をモニターしているデータ主体が居住する加盟国の 1 つに事業所を持つ（establish）ものとする。

4.管理者による代表者の指名は、管理者自身に対して起こされうる訴訟に影響を与えるようなものではないものとする。

第 26 条　処理者

1.処理活動が管理者の代わりに実施される場合、管理者は、当該処理が本規則の要件に適合し、かつデータ主体の権利の保護を保証するような仕方で、適切な技術的及び組織的な措置及び手続きを、とりわけ実施される処理を管理する技術的安全管理措置及び組織的措置を、実施することの十分な保証を提供する処理者を選ぶものとし、これらの措置の遵守を保証するものとする。

2.処理者による処理の実施は、処理者を管理者に拘束し、かつ処理者にとりわけ以下を行うこと要求する契約又はその他の法的行為によって管理されるものとする。

(a)管理者からの指示のみに従って活動すること（とりわけ、利用されている個人データの移転が禁じられている場合)。

(b)機密保持を誓約しているか、又は法定の機密保持義務の下にある職員のみを雇用すること。

(c)第 30 条において要求される全ての措置を取ること。

(d)管理者の事前の許可を得た場合のみ、他の処理者の協力を得ること。

(e)処理の性質に鑑み可能な場合に限り、管理者との合意の下で、第 3 章で規定されたデータ主体の権利の行使のための請求に応じる管理者の義務を果たすために必要な技術的及び組織的要件を策定すること。

(f)第 30 条から第 34 条の義務への遵守を保証するように管理者を支援すること。

(g)処理の終了後に管理者に全ての結果を引き渡し、その他の用途で個人データを処理しないこと。

(h)本条に規定された義務への遵守を管理するために必要な全ての情報を管理者と監督機関が利用できるようにすること。

3.管理者と処理者は、第 2 項にいう管理者の指示と処理者の義務を書面にて文書化するものとする。

4.処理者が管理者によって指示された以外の仕方で個人データを処理する場合、処理者は当該処理に関して管理者とみなされるものとし、第 24 条で規定された共同管理者に関するルールを守るものとする。

5.欧州委員会は、第 1 項にしたがって処理者に関する責任、任務及びタスクの基準と要件を規定するために、また企業グループ内での個人データ処理を促進するような条件を規定するために、第 86 条に則り委任された法令を採択する権限を与えられるものとする。

第 27 条　管理者と処理者の権限下での処理

処理者、及び管理者又は処理者の権限下で行為する人間であって個人データへのアクセスを有する者は、EU 又は加盟国の法律によってそのように要求されている場合を除き、管理者からの指示なしには個人データを処理しないものとする。

第 28 条　文書化

1.各管理者と処理者は、また（存在する場合には）管理者の代表者は、その責任の下で行う全ての処理活動に関して文書を維持するものとする。
2.当該文書は、少なくとも以下の情報を含むものとする。
(a)管理者、又は共同管理者若しくは処理者の名前及び連絡先の詳細、及び（存在する場合には）代表者の名前及び連絡先の詳細。
(b)（存在する場合には）データ保護オフィサーの氏名及び連絡先の詳細。
(c)第 6 条(1)(f)に基づく処理の場合に管理者が追求する正当な利益を含め、処理の目的。
(d)データ主体及び個人データの種類の記述、又はデータ主体に関するデータの種類の記述。
(e)個人データの受領者、又は受領者の種類。正当な利益のために個人データが開示される管理者を含む。
(f)第三国又は国際組織へのデータ移転。当該第三国又は国際組織の名称を含む。第 39 条(2)(d)及び第 44 条(1)(h)にいう移転の場合は、適切な安全管理措置の文書も含む。
(g)各種類のデータの消去期限に関する一般的記述。
(h)第 22 条(3)にいうメカニズムに関する記述。
3.管理者及び処理者、また（存在する場合には）管理者の代表者は、要求に応じて、監督機関が当該文書を利用できるようにするものとする。
4.第 1 項及び第 2 項にいう義務は、以下の管理者及び処理者には適用されないものとする。
(a)商業的利益なく個人データを処理する自然人。又は、
(b)その主要な活動に付属する 1 つの活動のみで個人データを処理する 250 人未満の職員を雇用する企業又は組織。
5.欧州委員会は、とりわけ管理者及び処理者、また（存在する場合には）管理者の代表者の責任を考慮に入れながら、第 1 項にいう文書の基準と要件を規定するために、第 86 条に則り委任された法令を採択する権限を与えられるものとする。
6.欧州委員会は、第 1 項にいう文書の標準的形式を規定することができる。これらの**実施法令**は、第 87 条(2)で規定された審査手続きに則り採択されるものとする。

第 29 条　監督機関との協力
1.管理者及び処理者、また（存在する場合には）管理者の代表者は、自らの任務の遂行において、とりわけ第 53 条(2)(a)にいう情報を提供することによって、また第 53 条(2)(b)にいうアクセスを与えることによって、要求に応じて、監督機関と協力するものとする。
2.第 53 条(2)にいう監督機関の権限行使に応えて、管理者と処理者は監督機関によって特定された合理的期間内に監督機関に回答を行うものとする。回答は、監督機関の意見に応えて、対応策及び達成される結果についての記述を含めるものとする。

第 2 節　データセキュリティ

第 30 条　処理のセキュリティ

1.管理者と処理者は、最先端の技術と導入のコストを考慮に入れながら、当該処理によるリスク及び保護される個人データの性質に対して適切なセキュリティのレベルを保証するために、適切な技術的及び組織的な措置を導入するものとする。

2.管理者と処理者は、偶発的若しくは不法な破壊又は偶発的な紛失から個人データを保護するために、またあらゆる不法な形態の処理、とりわけ無権限での個人データの開示、頒布若しくはアクセス、又は改変を防止するために、リスクの評価に続いて、第 1 項にいう措置を取るものとする。

3.欧州委員会は、第 1 項及び第 2 項にいう技術的及び組織的措置に関して、特定の分野及び特定のデータ処理の状況において何が最先端の技術を構成するかの決定を含め、とりわけ技術進歩並びにプライバシー・バイ・デザイン及びデータ保護・バイ・デフォルトの解決策を考慮に入れながら、より詳細な基準と要件を規定するために、第 86 条に則り委任された法令を採択する権限を与えられるものとする。

4.欧州委員会は、必要な場合には、様々な状況のために、とりわけ以下のために、第 1 項及び第 2 項で規定された要件を具体化するための実施法令を規定することができる。

(a)個人データへの無権限アクセスを防止する。

(b)個人データの無権限での開示、読み込み、複製、改変、消去又は削除を防止する。

(c)処理活動の合法性の検証を保証する。

これらの実施法令は、第 87 条(2)で規定された審査手続きに則り採択されるものとする。

第 31 条　個人データ違反の監督機関への通知

1.個人データ違反があった場合、管理者は不当な遅滞なく、実行可能な場合には、個人データ違反に気づいてから 24 時間以内に、監督機関に当該個人データ違反について通知（報告）するものとする。24 時間以内になされない場合には、監督機関への通知は合理的な正当化と共になされるものとする。

2.第 23 条(2)(f)に従い、処理者は、個人データ違反が立証された（判明した）後に直ちに管理者に警告及び通知（報告）を行うものとする。

3.第 1 項にいう通知は少なくとも、以下のものでなければならない。

(a)関係するデータ主体の種類及び数、並びに関係するデータ記録の種類及び数を含む、個人データ違反の性質を記述する。

(b)データ保護オフィサーの身元及び連絡先の詳細、又はより多くの情報が入手できるその他のコンタクトポイントを連絡する。

(c)当該個人データ違反の潜在的な悪影響を軽減する対処策をレコメンドする。

(d)当該個人データ違反の影響（consequences）を記述する。

(e)当該個人データ違反に対処するために管理者によって提案された若しくは実施された措置を記述する。

4.管理者は、当該違反の事実関係、その影響及び救済措置を含め、全ての個人データ違反について文書化するものとする。この文書化は、監督機関が本条への遵守を検証することを可能にするものでなければならない。この文書化は、目的にとって必要な情報のみを含むものでなければならない。

5.欧州委員会は、第 1 項及び第 2 項にいうデータ違反を立証するための詳細な基準と要件を規定するために、また管理者と処理者が個人データ違反についての通知を要求される特定条件についての詳細な基準と要件を規定するために、第 86 条に則り委任された法令を採択する権限を与えられるものとする。

6.欧州委員会は、監督機関への通知の標準フォーマット、通知の要件に適合した手続き、及び第 4 項にいう文書化のための形式と手順（modalities）を規定することができる。これらの実施法令は、第 87 条(2)で規定された審査手続きに則り採択されるものとする。

第 32 条　個人データ違反のデータ主体への連絡

1.個人データ違反がデータ主体の個人データ又はプライバシーの保護に悪影響を及ぼしそうである場合、管理者は、第 31 条にいう通知の後に、不当な遅滞なく、データ主体に当該個人データ違反について連絡するものとする。

2.第 1 項にいうデータ主体への連絡は、個人データ違反の性質を記述し、少なくとも、第 31 条(3)の(b)(c)の情報及びレコメンデーションを含むものとする。

3.データ主体への個人データ違反の連絡は、適切な技術的保護措置を取っていたこと、及びこれらの措置が個人データ違反に関係するデータに適用されていたことを管理者が監督機関が満足するように証明した場合には、必要とされないものとする。そのような技術的保護措置は、データへのアクセス権限のない人間に、当該データを理解不能とさせるものとする。

4.個人データ違反をデータ主体に連絡する管理者の義務に影響を与えることなく、管理者がまだ個人データ違反のデータ主体に当該個人データ違反について連絡していない場合には、監督機関は、当該違反のありえる悪影響を考慮に入れ、管理者に連絡するように要求することができる。

5. 欧州委員会は、第 1 項にいう個人データに悪影響を及ぼしそうな個人データ違反の条件に関する詳細な基準と要件を規定するために、第 86 条に則り委任された法令を採択する権限を与えられるものとする。

6.欧州委員会は、第 1 項にいうデータ主体への連絡のフォーマット、及び当該連絡に適用できる手続きを規定することができる。これらの実施法令は、第 87 条(2)で規定された審査手続きに則り採択されるものとする。

第 3 節　データ保護評価と事前オーソライズ

第 33 条　データ保護影響評価

1.予定されている処理活動がその性質、範囲又は目的に基づきデータ主体の権利と自由に明示的なリスクを提示する場合には、管理者又は管理者を代理する処理者は、当該処理活動が個人データ保護に与える影響について評価を実施するものとする。

2.とりわけ以下の処理活動は、本条第 1 項で規定したような明示的リスクを提示する。

(a)自動処理に基づき、かつ当該個人に関する法的影響を生じさせる措置を引き起こす若しくは当該個人に重大な影響を与えるような、自然人に関する個人的側面の体系的かつ広範な評価、又は、とりわけ自然人の経済状況、位置、健康、個人的嗜好、信頼性若しくは行動を分析若しくは予測するための処理活動。

(b)性生活、健康、人種、及び民族的起源に関する情報、又はヘルスケアの提供、疫学研究、若しくは精神疾患若しくは伝染病に関する調査のための処理活動であって、当該データが大きな規模で特定の個人に対する措置又は決定を行うために処理される場合。

(c)公共のアクセス可能なエリアのモニタリング、とりわけ、光学電子機器を利用している場合（ビデオ・サーベイランス）。

(d)子ども、遺伝子データ、又は生体データに関する大規模なファイリングシステムにおける個人データ。

(e)第 34 条(2)(b)に従い監督機関のコンサルテーションが必要とされる、その他の処理活動。

3.影響評価は、データ主体及びその他の関係する者の権利と正当な利益を考慮に入れながら、少なくとも、予定されている処理活動の全般的記述、データ主体の権利と自由へのリスクの評価、リスクに対処するために予定されている対策、安全管理措置（safeguards, security measures）、個人データ保護を保証するためのメカニズム、本規則への遵守を証明するためのメカニズムを含むものとする。

4.管理者は、商業的若しくは公共的利益の保護、又は当該処理活動のセキュリティに影響を与えることなく、意図された処理に関して、データ主体や代表者の見解を求めるものとする。

5.管理者が公的機関又は公的団体であって、かつ当該処理が処理活動に係るルールと手続きを規定した第 6 条(1)(c)に従った法的義務及び EU の法令で規定された法的義務に起因するものである場合、加盟国が当該処理活動に先立つ影響評価の実施を必要とみなさない限り、第 1 項から第 4 項は適用されないものとする。

6.欧州委員会は、本条第 1 項と第 2 項で規定された明示的なリスクを提示すると考えられる処理活動に関して、より詳細な基準と条件を規定するために、また第 3 項で規定された影響評価に関して、スケーラビリティ（拡張性）、検証及び監査可能性の条件を含め、より詳細な要件を規定するために、第 86 条に則り委任された法令を採択する権限を与えられるも

のとする。そのことによって、欧州委員会は中小企業のための特別措置を考慮するものとする。
7.欧州委員会は、第 3 項で規定された影響評価を実施し、検証し、監査するための基準と手続きを規定することができる。これらの実施法令は、第 87 条(2)で規定された審査手続きに則り採択されるものとする。

第 34 条　事前オーソライズと事前コンサルテーション
1.管理者又は処理者は、予定している処理が本規則を遵守していることを保証するために、とりわけデータ主体に関わるリスクを軽減するために、以下の場合には、個人データの処理に先立って監督機関からオーソライズを得るものとする。
・管理者又は処理者が、第三国又は国際組織への個人データ移転のために、第 42 条(2)(d)にいう契約条項を採用する場合。又は、
・第三国又は国際組織への個人データ移転のための第 42 条(5)にいう法的拘束力をもつ法律文書における適切な安全管理措置が提供されていない場合。
2.管理者又は管理者を代理する処理者は、予定している処理が本規則を遵守していることを保証するために、とりわけデータ主体に関わるリスクを軽減するために、以下の場合には、個人データの処理に先立って監督機関のコンサルテーションを受けるものとする。
(a)第 33 条にいうデータ保護影響評価が、処理活動がその性質、範囲、又は目的のために、高い度合いの明示的なリスクを提示しそうであることを示すものである場合。又は、
(b)監督機関が、処理活動の性質、範囲、及び／又は目的のために、データ主体の権利及び自由への明示的なリスクを提示しそうな特定の処理活動、かつ第 4 項に従い特定された処理活動に関して事前コンサルテーションを実施することが必要だと考えている場合。
3.監督機関が、予定された処理が本規則を遵守していないという意見を持つ場合、とりわけリスクが不十分に特定又は軽減されている場合、監督機関は当該処理を禁止し、またそのような不遵守を改善するための適切な提案を行うものとする。
4.監督機関は、第 2 項の(b)に従い事前コンサルテーションを受ける処理活動のリストを作成し、公表するものとする。監督機関はこれらのリストを欧州データ保護評議会に連絡するものとする。
5.第 4 項で提供されたリストが、複数の加盟国のデータ主体への商品やサービスの提供、若しくはそのようなデータ主体の行動のモニターに関連した処理活動、または EU 以下以内における個人データの自由な移動に重大な影響を及ぼすかもしれない処理活動を伴う場合、監督機関は当該リストの採択に先立ち、第 57 条に言う整合性メカニズムを適用するものとする。
6.管理者又は処理者は、第 33 条にいうデータ保護影響評価を監督機関に提出するものとする。また、監督機関が当該処理の遵守を評価できるように、とりわけデータ主体の個人データの保護に関するリスク及び関連する安全保護措置について評価できるように、要求に

応じて、その他の情報を監督機関に提出するものとする。
7.加盟国は、予定された処理が本規則を遵守していることを保証し、とりわけデータ主体を巻き込むリスクを軽減するために、当該処理の性質を規定するような、国の議会によって採択される法制上の措置（legislative measure）の準備、又はそのような法的措置に基づく措置の準備において、監督機関のコンサルテーションを受けるものとする。
8.欧州委員会は、本条第 2 項(a)にいう高い度合いの明示的なリスクを決定するためのより詳細な基準と要件を規定するために、第 86 条に則り委任された法令を採択する権限を与えられるものとする。
9.欧州委員会は、第 1 項及び第 2 項にいう事前オーソライズ及び事前コンサルテーションのための標準フォームと標準手続き、並びに第 6 項に従い監督機関に情報提供するための標準フォームと標準手続きを規定することができる。これらの実施法令は、第 87 条(2)で規定された審査手続きに則り採択されるものとする。

第 4 節　データ保護オフィサー

第 35 条　データ保護オフィサーの指名
1.管理者又は処理者は、以下のいずれかの場合には、データ保護オフィサーを指名するものとする。
(a)処理が公的機関又は公的団体によって実施される場合。又は、
(b)処理が 250 人以上の職員を雇用する企業によって実施される場合。又は、
(c)管理者又は処理者の中核的活動が、その性質、範囲、及び／又は目的のため、データ主体の定期的かつ体系的なモニタリングを必要とする処理活動から成る場合。
2.第 1 項(b)の場合、企業グループは 1 人のデータ保護オフィサーを指名することができる。
3.管理者又は処理者が公的機関又は公的団体である場合、当該公共機関又は公的団体の組織構造を考慮に入れ、1 人のデータ保護オフィサーを複数の団体に対して指名することができる。
4.第 1 項以外の場合には、管理者若しくは処理者、又は管理者若しくは処理者のカテゴリを代表する団体その他の組織は、データ保護オフィサーを指名することができる。
5.管理者又は処理者は、専門資格（professional qualities）並びに、とりわけデータ保護法及びデータ保護プラクティスに関する専門知識及び第 34 条にいう任務を果たす能力に基づき、データ保護オフィサーを指名するものとする。専門知識の必要なレベルは、とりわけ実行されるデータ処理及び管理者又は処理者によって処理される個人データに必要な保護によって決められるものとする。
6.管理者又は処理者は、データ保護オフィサーの他の専門的義務が当人のデータ保護オフィサーの任務及び義務と両立できるものであり、利益相反に陥らないことを保証するものとする。

7.管理者又は処理者は、データ保護オフィサーを少なくとも 2 年間の任期で指名するものとする。データ保護オフィサーは再任されることが可能である。任期中、データ保護オフィサーは、その義務の遂行に必要とされる条件をもはや満たさない場合に限り、データ保護オフィサーの地位を解任されうる。
8.データ保護オフィサーは管理者又は処理者によって雇用されることができる。また、サービス契約に基づき、任務を果たすこともできる。
9.管理者又は処理者は、データ保護オフィサーの名前と連絡先詳細を監督機関に連絡し、また公けにするものとする。
10.データ主体は、当該データ主体のデータの処理に関する全てのイシューについてデータ保護オフィサーにコンタクトを取ったり、本規則の下での権利を行使する権利を持つものとする。
11.欧州委員会は、本条第 1 項(c)にいう管理者又は処理者の中核的活動に関する詳細な基準と条件を規定するために、また第 5 項にいうデータ保護オフィサーの専門資格の基準を規定するために、第 86 条に則り委任された法令を採択する権限を与えられるものとする。

第 36 条　データ保護オフィサーの地位
（略）

第 37 条　データ保護オフィサーの任務
（略）

第 5 節　行動規範と認証

第 38 条　行動規範
1.加盟国、監督機関及び欧州委員会は、様々なデータ処理分野に固有な事情を考慮に入れながら、とりわけ以下の点に関して、本規則の適正な適用に寄与することを意図した行動規範の策定を促進するものとする。
(a)公正で透明なデータ処理。
(b)データの収集。
(c)公衆及びデータ主体への情報提供。
(d)権利を行使するデータ主体の請求。
(e)子どもへの情報提供及び保護。
(f)第三国又は国際組織へのデータ移転。
(g)管理者が従うべき行動規範への遵守を監視し保証するためのメカニズム。
(h)第 73 条及び第 75 条に従うデータ主体の権利に影響を与えることなく、管理者とデータ主体の間の個人データ処理に関する紛争を解決するための裁判外手続きその他の紛争

解決手続き。
2.行動規範の策定又は既存の行動規範の修正若しくは拡張を意図する、ある 1 つの加盟国内における管理者又は処理者のカテゴリを代表する協会その他の団体は、当該加盟国の監督機関の意見を求めるためにそれを提出することができる。監督機関は、行動規約案又は修正案が本規則を遵守しているか否かに関する意見を提供することができる。監督機関は行動規約案又は修正案についてデータ主体又はその代表の見解を求めるものとする。
3.複数の加盟国における管理者又は処理者のカテゴリを代表する協会その他の団体は、行動規約案及び既存の行動規約の修正案又は拡張案を欧州委員会に提出することができる。
4.欧州委員会は、第 3 項に従い欧州委員会に提出された行動規範案及び既存の行動規範の修正案又は拡張案が EU 内で一般的な有効性を持つことを決定するための実施法令を採択することができる。これらの実施法令は、第 87 条(2)で規定された審査手続きに則り採択されるものとする。
5.欧州委員会は、第 4 項に則り一般的な有効性を持つと決定された行動規範の適切な広報を保証するものとする。

第 39 条　認証
1.加盟国と欧州委員会は、とりわけ EU のレベルにおいて、データ保護認証メカニズムの設立並びにデータ保護シール及びマークの設立を促進するものとする。これらは、データ主体が管理者及び処理者によって提供されるデータ保護のレベルを迅速に評価することを可能とする。データ保護認証メカニズムは、様々な部門及び様々な処理活動の具体的特徴を考慮に入れながら、本規則の適正な適用に貢献するものとする。
2.欧州委員会は、第 1 項で規定されたデータ保護認証メカニズムに関して、付与及び剥奪の条件、並びに EU 域内及び第三国内での認証の要件を含めて、より詳細な基準と要件を規定するために、第 86 条に則り委任された法令（委任法令）を採択する権限を与えられるものとする。
3.欧州委員会は、認証メカニズム並びにデータ保護シール及びマークのための技術標準を規定したり、認証メカニズム並びにデータ保護シール及びマークを普及促進及び認識することを規定したりすることができる。

第 5 章　個人データの第三国又は国際組織への移転

第 40 条　移転に関する一般原則
第三国又は国際組織への個人データ（処理の対象となっている個人データ又は今後処理が予定されている個人データ）の移転は、本規則のその他の条項の下、第三国又は国際組織から他の第三国又は国際組織への個人データの送信を含め、本章によって規定された条件が管理者及び処理者によって遵守されている場合のみ実施することができる。

第 41 条　十分性決定がなされた国への移転

1.欧州委員会が当の第三国若しくは当該第三国内の領域若しくは処理分野、又は国際組織が保護の十分なレベルにあると保証する決定を行った場合には、移転を行うことができる。そのような移転は、さらなるオーソライズを必要としないものとする。

2.保護のレベルの十分性は、欧州委員会によって、以下を考慮することで評価されるものとする。

(a)パブリックセキュリティ、防衛、国家安全保障に関する法、刑法を含め、施行中の法律、関連制度のルール（一般法及び個別分野法）、当該国又は国際組織で遵守されている専門的ルール及び安全管理措置；実効的な行政的救済及び司法救済措置を含む実効的かつ施行可能なデータ主体の権利、とりわけ個人データが移転される EU のデータ主体の権利。

(b)当の第三国又は国際組織においてデータ保護に関するルールの遵守を保証したり、データ主体による権利行使のサポート及び助言をしたり、EU 及び加盟国の監督機関と協力したりすることに責任を負う 1 つ以上の独立の監督機関の存在及び、それが実効的に機能していること。及び、

(c)当の第三国又は国際組織が行っている国際的なコミットメント。

3.欧州委員会は、第三国若しくは当該第三国内の領域若しくは処理分野、又は国際組織が、第 2 項の意味において、保護の十分なレベルを保証していると決定することができる。これらの実施法令は、第 87 条(2)で規定された審査手続きに則り採択されるものとする。

4.実施法令はその地理的及び分野的な適用を明示化し、また、可能な場合には、本条第 2 項(b)で言及した監督機関を特定するものとする。

5.欧州委員会は、第三国若しくは当該第三国内の領域若しくは処理分野、又は国際組織が、第 2 項の意味において、保護の十分なレベルを保証していないと決定することができる。特に、第三国又は国際組織において施行中の関連法制度（一般法及び個別分野法）が実効的な行政的救済及び司法救済措置を含め、実効的かつ施行可能なデータ主体の権利、とりわけ個人データが移転されるデータ主体の権利を保障しない場合には、そのような決定を行うことができる。これらの実施法令は、第 87 条(2)で規定された審査手続きに則って、又は個人データ保護の権利の観点から個人にとって極めて緊急を要する場合には、第 87 条(3)で規定された手続きに則って採択されるものとする。

6.欧州委員会が第 5 項に従って決定した場合には、当の第三国若しくは当該第三国内の領域若しくは処理分野、又は国際組織への個人データの移転は、第 42 条から第 44 条の規定に反しない限りで、禁止されるものとする。適切な時期に、欧州委員会は第 5 項に従ってなされた決定に起因する状況を救済することを目的とした当該第三国又は国際組織とのコンサルテーションに入るものとする。

7.欧州委員会は、EU 官報に、保護の十分なレベルが保証される、又は保証されないという

決定のなされた第三国、第三国内の領域及び処理分野、並びに国際組織のリストを公表するものとする。
8.EU 指令 95/46/EC の第 25 条(6)又は第 26 条(4)に基づいて欧州委員会によって採択された決定は、欧州委員会によって修正、置換又は廃止されるまで、効力を持ち続けるものとする。

第 42 条　適切な安全管理措置による移転
1.欧州委員会が第 38 条に従った決定を行っていない場合、管理者や処理者は、法的拘束力のある文書において個人データ保護に関する適切な安全管理措置が提示した場合にのみ、第三国又は国際組織に個人データを移転することができる。
2.第 1 項で言及された適切な安全管理措置は、とりわけ、以下のいずれかによって提供されるものとする。
(a)第 43 条に則った拘束的企業準則。又は、
(b)欧州委員会によって採択されたデータ保護の標準契約条項。この実施法令は、第 87 条(2)で規定された審査手続きに則り採択されるものとする。又は、
(c)第 57 条で規定された整合性メカニズムに則り監督機関によって採択されたデータ保護の標準契約条項であって、第 62 条(1)の(b)に従い欧州委員会によって全般的に妥当であると宣言がなされた場合。又は、
(d)本条第 4 項に則り監督機関にオーソライズされた、管理者又は処理者とデータの受領者の間の契約条項。
3.第 2 項の(a)(b)(c)で規定されたデータ保護の標準契約条項又は拘束的企業準則は、さらなるオーソライズを必要としないものとする。
4.移転が第 2 項(d)で規定された契約条項に基づくものである場合、管理者又は処理者は監督機関から第 34 条(1)(a)に従い当該契約条項の事前のオーソライズを得るものとする。移転が他の加盟国におけるデータ主体に係る処理活動に関連している場合には、又は移転が EU 域内における個人データの自由な移動に重要な影響を与えるものである場合には、監督機関は第 57 条で規定した整合性メカニズムを適用するものとする。
5.個人データ保護に関する適切な安全管理措置が法的拘束力のある法律文書（legally binding instrument）で提供されていない場合、管理者又は処理者は当該移転について、又はそのような移転の根拠を提供する管理上の協定（administrative arrangements）に挿入する条項について、事前オーソライズを得るものとする。監督機関によるそのようなオーソライズは第 34 条(1)(a)に則るものとする。当該移転が他の加盟国のデータ主体に係る処理活動に関連している場合、又は EU 域内における個人データの自由な移動に重要な影響を与えるものである場合、監督機関は第 57 条にいう整合性メカニズムを適用するものとする。EU 指令 95/46/EC の第 26 条(2)に基づいて監督機関によって承認された内容は、当該監督機関によって修正、置換又は廃止されるまで、効力を持ち続けるものとする。

第 43 条　拘束的企業準則による移転

1.監督機関は、第 58 条で規定された整合性メカニズムに則り、以下のような拘束的企業準則を承認するものとする。

(a)拘束的企業準則が、法的拘束力を持つものであり、管理者又は処理者の企業グループ内の全てのメンバーに適用され、全てのメンバーによって実行され、それらの被用者を含むものであること。

(b)拘束的企業準則が、データ主体に行使可能な権利を明示的に授与するものであること。

(c) 拘束的企業準則が、第 2 項で規定する要件を満たしていること。

2.拘束的企業準則は少なくとも以下を規定するものとする。

(a)企業グループ及びそのメンバーの構造と連絡先詳細。

(b)データの移転。個人データの種類、処理の種類、処理目的、関係するデータ主体の種類、当の第三国の名称を含む。

(c)当該準則の法的拘束性の性質。内的な拘束性と外的な拘束性の両方。

(d)一般的なデータ保護原則。とりわけ、目的制限、データ品質、処理の法的根拠、センシティブ個人データの処理。データの安全管理措置。こちら側のポリシーに拘束されない組織への移転に関する要件。

(e)データ主体の権利及びこれらの権利を行使する手段。第 20 条に則りプロファイリングに基づく措置を受けない権利、第 75 条に則り加盟国の監督機関及び裁判所に対して苦情を申し立てる権利、並びに拘束的企業準則の違反に対する救済及び（適切な場合には）補償を得る権利を含む。

(f)EU 域内に事務所を持たない企業グループメンバーによる拘束的企業準則の違反に対して、EU 加盟国内に事務所を持つ管理者又は処理者が責任を負うこと。管理者又は処理者は、その責任の全体又は一部を、損害を引き起こした出来事について当該メンバーに責任がないことを証明した場合に限り、免責されることができる。

(g)拘束的企業準則に関する情報、とりわけ(d)(e)(f)の条項に関する情報が、第 11 条に則り、どのようにデータ主体に提供されるか。

(h)第 35 条に従い指名されたデータ保護オフィサーの任務。企業グループ内で拘束的企業準則の遵守を監視することや、教育訓練及び苦情取扱いを監視することを含む。

(i)拘束的企業準則の遵守の検証を保証することを目的とした、企業グループ内のメカニズム。

(j)ポリシーへの変更を報告し、記録し、また、これらの変更を監督機関に報告するためのメカニズム。

(k)企業グループのメンバーによる遵守を保証するための監督機関との協力メカニズム。とりわけ、(i)にいう措置の検証の結果を監督機関が入手できるようにするもの。

3.欧州委員会は、本条の意味における拘束的企業準則に関して詳細な基準と条件、とりわけ

それらの承認の基準、第 2 項(b)(d)(e)(f)を処理者が遵守するための適用、及び関係するデータ主体の個人データの保護を保証するために更に必要となる要件を規定するために、第 86 条に則り委任された法令を採択する権限を与えられるものとする。
4.欧州委員会は、本条の意味における拘束的企業準則のための管理者、処理者、監督機関の間での電子的手段による情報の交換のためのフォーマット及び手続きを規定することができる。これらの実施法令は、第 87 条(2)で規定された審査手続きに則り採択されるものとする。

第 44 条　例外
1.第 41 条に従った十分性の決定がなされていない場合、又は第 42 条に従った適切な安全管理措置が取られていない場合、第三国又は国際組織への個人データの移転又は一連の移転は以下のいずれかの条件でのみ行うことができる。
(a)データ主体が提案された移転に対して、十分性の決定や適切な安全管理措置がないことによる移転のリスクについて十分に情報を与えられた後に、同意を与えた場合。又は、
(b)移転が、データ主体と管理者の間の契約の履行のために必要な場合、又はデータ主体の要求により契約締結間の措置の実施に必要な場合。又は、
(c)移転が、データ主体の利益のために管理者と他の自然人又は法人の間で締結された契約の締結又は履行のために必要な場合。又は、
(d)移転が、公共の利益の理由から必要な場合。又は、
(e)移転が、法的要求の立証、実行又は抗弁に必要な場合。又は、
(f)移転が、データ主体が物理的又は法的に同意を与えることが不可能な場合であって、データ主体又はその他の人間の重大な利益を保護するために必要な場合。又は、
(g)移転が、EU 又は加盟国の法律に従って公衆に情報を提供することが意図され、かつ公衆一般又は正当な利益を示せる人によるコンサルテーションに門戸を開いている官報（register）によってなされ場合。ただし、EU 又は加盟国の法律でコンサルテーションのために規定された条件が当該ケースに当てはまる範囲に限る。又は、
(h)移転が、管理者又は処理者が求める正当な利益の目的にとって必要であり、それが頻繁、又は大量とはみなされず、かつ管理者又は処理者がデータ移転又は一連のデータ移転の運用に関わる全ての環境を評価し、必要あればこの評価に基づき個人データ保護に係る適切な安全管理措置を提示している場合。
2.（以下略）

第 45 条　個人データ保護のための国際協力
（略）

第 6 章　独立の監督機関

第 1 節　独立的な地位

第 46 条　監督機関

1.各加盟国は、個人データの処理に係る自然人の基本的権利と自由を保護し、EU 域内での個人データの自由な移動を促進するために、1 つ以上の公共機関が本規則の適用を監視すること及び EU 全域における整合的な適用に寄与することに責任を負う旨を定めるものとする。これらの目的のために、監督機関は相互に、また欧州委員会と協力するものとする。

2.ある加盟国で複数の監督機関が設立された場合、当該加盟国は、欧州データ保護評議会へのこれらの機関の効果的な参加のために、単一のコンタクトポイントとして機能する監督機関を指名するものとする。また、その他の機関が第 57 条にいう整合性メカニズムに関係するルールを遵守することを保証するためのメカニズムを規定するものとする。

3.各加盟国は、欧州委員会に、本章に従い採択する法律の条項について、遅くとも第 91 条(2)で規定する日までに、通知するものとする。また、遅滞なく、影響を与えるような重大な修正について、通知するものとする。

第 47 条　独立性

1.監督機関は、委ねられた任務と権限を行使するに当たって、完全な独立な立場で行動するものとする。

2.監督機関のメンバーは、その任務の遂行に当たって、誰からの指示も仰いだり受けたりしないものとする。

3.監督機関のメンバーは、その任務と矛盾するいかなる行動も慎むものとする。また、その在任期間、有給か無給かに関わらず、両立不可能ないかなる仕事にも従事しないものとする。

4.監督機関のメンバーは、在任期間の後、職位と恩恵の享受に関して誠実さと分別をもってふるまうものとする。

5.各加盟国は、監督機関に、相互支援、相互協力および欧州データ保護評議会への参加の文脈で実行されるものも含め、その任務と権限の効果的な遂行に必要となる十分な人的、技術的及び財政的なリソース、設備並びにインフラが供与されていることを保証するものとする。

6.各加盟国は、監督機関が、監督機関の長によって指名され、その指揮命令を受けるべきスタッフを有することを保証するものとする。

7.加盟国は、監督機関がその独立性に影響を与えることのないような、財務統制（financial control）を受けることを保証するものとする。加盟国は監督機関が独立した年間予算を持つことを保証するものとする。当該予算は公表するものとする。

（第 48 条～第 50 条　略）

第 2 節　任務と権限（Duties and Powers）

第 51 条　権能（Competence：管轄）

1.各監督機関は、その自らの加盟国の領土において、本規則に従い付与された権限を行使するものとする。

2.個人データの処理が EU 域内の管理者又は処理者の事業所の活動に関連して行われた場合、かつ管理者又は処理者が複数の加盟国に事業所を持つ場合、管理者又は処理者の主要な事業所の監督機関が、全ての加盟国における管理者又は処理者の処理活動の監督を行う権能を有するものとする。ただし、本規則の第 7 章の条項に影響を与えるものではない。

3.監督機関は、自らの司法能力で行動する裁判所の処理活動を監督する権能は有さないものとする。

第 52 条　任務（Duties）

1.監督機関は、以下を行うものとする。

(a)本規則の適用を監視し、保証する。

(b)第 73 条に基づきデータ主体又はデータ主体を代表する協会によって申し立てられた苦情を聴取する。適切な範囲で、問題について調査する。また、データ主体又は協会に合理的な期間内に苦情への対応の進捗状況及び対応結果について、とりわけ更なる調査又は他の監督機関との協力が必要かどうか、通知する。

(c)他の監督機関と情報を共有し、相互に支援を提供する。また、本規則の適用と施行の整合性を保証する。

(d)自らのイニシアティブで、若しくは苦情に基づき、又は他の監督機関からの要求に基づき、調査を実施する。データ主体が当該監督機関に苦情を申し立てた場合は、関係するデータ主体に合理的な期間内に調査結果について通知する。

(e)個人データ保護に影響がある発展、とりわけ情報通信技術と商慣習の発展を監視する。

(f)個人データ処理に関わる個人の権利及び自由の保護に関する法律的及び行政的措置について、加盟国の機関及び団体からの相談を受ける。

(g)第 34 条にいう処理活動についてオーソライズとコンサルテーションを行う。

(h)第 38 条(2)に基づき、行動規範案に対する意見を発表する。

(i)第 43 条に基づき、拘束的企業準則を承認する。

(j)欧州データ保護評議会の活動に参加する。

2.各監督機関は、個人データ処理に関連するリスク、規則、安全管理措置及び権利について公衆の意識を向上させるものとする。子どもを特に対象とする活動は、特別な注意を受けるものとする。

3.監督機関は、請求に応じて、本規則の下で権利を行使するデータ主体に助言を行うものとする。また、適切な場合には、この目的のために他の加盟国の監督機関と協力するものとする。

４.第 1 項の(b)にいう苦情のために、監督機関は苦情提出フォームを提供するものとする。このフォームは電子的に入力することができるが、他の連絡手段を排除しないものとする。

5.監督機関の任務の遂行は、データ主体に無料で提供されるものとする。

6.請求が明白に過剰である場合、とりわけ反復的なものである場合、監督機関は手数料を徴収すること、又はデータ主体に請求された措置をとらないことができる。監督機関は請求が明白に過剰であることを証明することの責任を負うものとする。

第 53 条　権限（Powers）

1.各監督機関は以下の権限を有するものとする。

(a)個人データ処理をつかさどる条項への違反容疑について、管理者又は処理者に通知し、適切な場合には、管理者又は処理者に、データ主体の保護を改善するために、具体的な方法で、当該違反を是正する（remedy）ことを命令する（order)。

(b)本規則によって提供された権利を行使するためのデータ主体の請求を遵守するように管理者又は処理者に命令する。

(c)管理者及び処理者に、並びに（存在する場合には）代表者に、その義務の遂行に関係する情報を提供するように命令する。

(d)第 34 条にいう事前オーソライズ及び事前コンサルテーションへの遵守を保証する。

(e)管理者又は処理者に警告（warn）又は勧告（admonish）を与える。

(f)本規則の条項に違反して処理されていた全てのデータの訂正、消去又は破壊、及びデータが開示された第三者にそのような措置を通知することを命令する。

(g)処理に関する一時的又は最終的な禁止を課す。

(h)第三国の受領者又は国際組織へのデータ移動を中断する。

(i)個人データ保護に関係するイシューに関して意見を発表する。

(j)関係する議会、政府、他の政治機関、公衆に、個人データ保護に関係するイシューに関して情報提供する。

2.このような監督機関は、管理者又は処理者から以下を入手する調査権限を有するものとする。

(a)監督その義務の遂行に必要な全ての個人データ及び全ての情報へのアクセス。

(b)本規則に違反した活動がそこで実行されていると想定される合理的な根拠がある場合、全てのデータ処理装置及び手段を含む、全ての施設へのアクセス。

上記(b)にいう権限は、EU の法令及び加盟国の法令に則って行使されるものとする。

3.各監督機関は、本規則への違反を司法当局に通報する権限、及び、とりわけ第 74 条(4)及び第 75 条(2)に従い、訴訟に携わる権限を有するものとする。

4.各監督機関は、法定犯罪（administrative offences）、とりわけ第 79 条(4)(5)(6)規定されたものを罰する権限を有するものとする。

第 54 条　活動報告書
各監督機関は、その活動に関する年次報告書を作成するものとする。この報告書は国の議会に提出されるものとし、公衆、欧州委員会及び欧州データ保護評議会が入手できるようにするものとする。

第 7 章　協力と整合性

第 1 節　協力

（第 55 条～第 56 条　略）

第 2 節　整合性

第 57 条　整合性メカニズム
第 46 条(1)で規定した目的のために、監督機関は、本節で規定する整合性メカニズムを通じて、相互に、また欧州委員会と協力するものとする。

（第 58 条～第 63 条　略）

（第 3 節　第 64 条～第 72 条　略）

第 8 章　救済、責任及び制裁

第 73 条　監督機関に苦情を申し立てる権利
1.各データ主体は、自己に関する個人データの処理が本規則に遵守していないと考える場合には、他の行政的救済又は司法救済に影響を与えることなく、いずれかの加盟国における監督機関に苦情を申し立てる権利を有するものとする。
2.個人データの保護に関連するデータ主体の権利および利益を保護する意図を持ち、加盟国の法律に従い適正に設立されているいかなる団体、組織又は協会も、個人データ処理の結果として本規則の下でデータ主体の権利が侵害されたと考える場合には、1 人以上のデータ主体の代わりに、いずれかの加盟国における監督機関に苦情を申し立てる権利を有するものとする。
3.データ主体の苦情とは独立に、第 2 項にいういかなる団体、組織又は協会も、個人データ違反が発生したと考える場合には、いずれかの加盟国における監督機関に苦情を申し立て

る権利を有するものとする。

第 74 条　監督機関に対する司法救済の権利

1.各自然人又は法人は、監督機関の自己に関する決定に対する司法救済の権利を有するものとする。

2.各データ主体は、自己の権利を保護するために必要な決定がなされていない場合、又は監督機関がデータ主体に 3 ヶ月以内に第 52 条第 1 項(b)に基づく苦情への対応の進捗状況若しくは対応結果について通知しない場合、監督機関に苦情に基づいて行動することを義務付ける司法救済の権利を有するものとする。

3.監督機関に対する訴訟は、監督機関が設立されている加盟国の裁判所で行うものとする。

4.データ主体が普段居住する加盟国以外の監督機関の決定に関連するデータ主体は、普段居住する加盟国の監督機関に、自己の代わりに、他国の監督機関に対する訴訟を行うことを請求することができる。

5.加盟国は、本条にいう裁判所による最終決定を執行するものとする。

第 75 条　管理者又は処理者に対する司法救済の権利

1.各自然人は、本規則を遵守しない個人データの処理の結果として本規則の下で自己の権利が侵害されていると考える場合には、他の利用可能な行政的救済に影響を与えることなく、第 73 条にいう監督機関に苦情を申し立てる権利を含め、司法救済の権利を有するものとする。

2.管理者又は処理者に対する訴訟は、当該管理者又は処理者が事業所を持つ加盟国の裁判所で行うものとする。さもなくば、当該管理者が公的権限を行使する公的機関でない限り、そのような訴訟はデータ主体が普段居住する加盟国の裁判所で行うこともできる。

3.同一の措置、決定又はプラクティスに関連して第 58 条にいう整合性メカニズムにおいて訴訟が係争中である場合、データ主体の権利保護の緊急性により整合性メカニズムにおける手続きの結果を待つことが出来ない場合を除き、裁判所は訴訟を中断することができる。

4.加盟国は、本条にいう裁判所による最終決定を執行するものとする。

（第 76 条～第 77 条　略）

第 78 条　刑事罰（penalties）

1.加盟国は本規則の条項の違反に適用できる刑事罰に関するルールを規定するものとし、管理者が代表者を指名する義務を遵守しない場合を含め、それらの条項が実施されることを保証するために必要なあらゆる措置を取るものとする。刑事罰は効果的で、釣り合いが取れ（proportionate）、かつ制止的なものでなければならない。

2.管理者が代表者を設置した場合、当該代表者に対して与えられうるいかなる刑事罰に影響

を与えることなく、刑事罰は当該代表者に適用されるものとする。
3.各加盟国は第 1 項に従い採択した法律の条項を、少なくとも第 91 条(2)に規定する日までに欧州委員会に通知するものとし、当該条項に重要な影響を与える修正については遅滞なく通知するものとする。

第 79 条　行政罰（administrative sanctions）
1.各監督機関は、本条に則り行政罰を科す権限を与えられるものとする。
2.行政罰は個別のケースにおいて効果的で、釣り合いが取れ、かつ制止的なものでなければならない。行政的課徴金（administrative fine）の額は、違反の性質、重大性及び持続性、違反の故意的又は過失的性質、当該自然人又は法人の責任の度合い及び当人による以前の違反の度合い、第 23 条に従い実施された技術的及び組織的措置及び手続き、並びに違反を救済するための監督機関への協力の度合いに応じて決めるものとする。
3.本規則への初回の故意でない非遵守の場合、以下の場合には、書面での警告を与え、処分を科さないことが可能である。
(a)自然人が、商業的利益なく個人データを処理している場合。又は、
(b)250 人未満の職員を雇用する企業若しくは組織が、その主要な活動の補助となる活動としてのみ個人データを処理している場合。
4.監督機関は、故意又は過失により、以下のことを行った者に対して、最大で 25 万ユーロ、又は企業の場合には最大で年間連結売上（annual worldwide turnover）の 0.5%の課徴金を科すものとする。
(a) 第 12 条(1)及び(2)に基づきデータ主体による請求に対応するメカニズムを提供しない者、又はデータ主体に対して迅速に回答しない、若しくは必要なフォーマットで回答しない者。
(b)第 12 条(4)に違反して、情報通知（information）又はデータ主体の請求への回答に対して手数料を課金する者。
5.監督機関は、故意又は過失により、以下のことを行った者に対して、最大で 50 万ユーロ、又は企業の場合には最大で年間連結売上（annual worldwide turnover）の 1%の課徴金を科すものとする。
(a)第 11 条、第 12 条(3)及び第 14 条に基づきデータ主体に対して情報通知（information）を提供しない、若しくは不完全な情報通知を提供する者、又は、十分に透明な仕方で情報通知を提供しない者。
(b)第 15 条及び第 16 条に基づきデータ主体へのアクセスを提供しない、若しくは個人データを訂正しない者、又は第 13 条に基づき受領者へ関連する情報を連絡しない者。
(c)第 17 条に基づく忘れられる権利又は消去できる権利を遵守しない者、又はタイムリミットが遵守されていることを保証するメカニズムを整備していない、若しくはデータ主体が個人データへの全てのリンク、若しくは個人データのコピー若しくは複製を削除す

ることを請求した第三者に通知する必要な措置を取らない者。

(d)第 18 条に違反して、電子的形式で個人データのコピーを提供しない者、又はデータ主体が他のアプリケーションに個人データを移転することを妨害する者。

(e)第 24 条に基づき共同管理者のそれぞれの責任を決定しない、又は十分に決定しない者。

(f)第 28 条、第 31 条(4)及び第 44 条(3)に基づき文書を維持しない、又は十分に維持しない者。

(g)特別なカテゴリのデータが含まれない場合、第 80 条、第 82 条及び第 83 条に基づく表現の自由に関係するルール、雇用関係における処理に関するルール、又は歴史的、統計的及び科学的研究目的での処理の条件を遵守しない者。

6. 監督機関は、故意又は過失により、以下のことを行った者に対して、最大で 100 万ユーロ、又は企業の場合には最大で年間連結売上（annual worldwide turnover）の 2%の課徴金を科すものとする。

(a) 第 6 条、第 7 条及び第 8 条に基づき、処理に関して何らの法的根拠若しくは十分な法的根拠のない個人データを処理する者、又は同意の条件を遵守しない者。

(b)第 9 条及び第 81 条に違反して特別なカテゴリのデータを処理する者。

(c)第 19 条に基づく異議申立又は要件を遵守しない者。

(d)第 20 条に基づき、プロファイリングに基づく措置に関係する条件を遵守しない者。

(e)第 22 条、第 23 条及び第 30 条に基づき、遵守を保証及び証明するための内部ポリシーを採択しない、又はそのための適切な措置を実施しない者。

(f)第 25 条に基づき代表者を指名しない者。

(g)第 26 条及び第 27 条に基づく、管理者に代わって行う処理に関係する義務に違反して個人データを処理する、又は処理を指示する者。

(h)第 31 条及び第 32 条に基づき、監督機関又はデータ主体に対し、個人データ違反について警告若しくは通知をしない者、又はタイムリー若しくは完全にデータ違反の通知をしない者。

(i)第 35 条、第 36 条及び第 37 条に基づく、データ保護オフィサーを指名しない者、又はその任務を遂行するための条件を保証しない者。

(k)第 39 条の意味におけるデータ保護シール又はマークを誤用する者。

(l)第 40 条から第 44 条に基づく十分性決定、適切な安全管理措置又は例外事項による許可のない第三国若しくは国際組織へのデータ移転を実行する又は指示する者。

(m)第 53 条(1)に基づく監督機関による命令、処理の一時的若しくは最終的な禁止、又はデータ移転の中断を遵守しない者。

(n)第 28 条(3)、第 29 条、第 34 条(6)及び第 53 条(2)に基づく、監督機関に対する支援、対応、関連する情報の提供、又は施設へのアクセスの提供の義務を遵守しない者。

(o)第 84 条に基づく職業上の守秘義務を保護するためのルールを遵守しない者。

7.欧州委員会は、第 2 条にいう基準を考慮に入れながら、第 4 項、第 5 項及び第 6 項にい

う行政的課徴金の額を更新するために、第 86 条に則り委任された法令を採択する権限を与えられるものとする。

（第 9 章～第 10 章　第 80 条～第 87 条　略）

第 11 章　最終条項

第 88 条　EU 指令 95/46/EC の廃止
1.EU 指令 95/46/EC は廃止される。
2.当該指令への言及は、本規則への言及として解釈されるものとする。EU 指令 95/46/EC の第 29 条により設置された個人データ処理に関連した個人の保護に関する作業部会への言及は、本規則によって設置される欧州データ保護評議会への言及として解釈されるものとする。

第 89 条　EU 指令 2002/58/EC との関係及びその修正
1.本規則は、EU 指令 2002/58/EC において同じ目的で規定された個別の義務に従わなければならない、EU 内の公共通信ネットワークにおける公共利用可能な電子通信サービスに対する条項に関連する個人データ処理に関しては、自然人又は法人に追加的な義務を課さないものとする。
2.EU 指令 2002/58/EC 第 1 条(2)は削除するものとする。

第 90 条　評価
欧州委員会は、本規則の評価とレビューに関する報告書を欧州議会及び欧州連合理事会に定期的に提出するものとする。初回の報告書は本規則の施行後 4 年以内に提出されるものとする。それ以降の報告書はその後 4 年ごとに提出されるものとする。欧州委員会は、必要な場合には、とりわけ情報技術の発達を考慮に入れながら、また、情報社会の発展状況から、本規則の修正及び他の法律文書の調整を目的とした適切な提案を提出するものとする。

第 91 条　施行と発効（Entry into force and application）
1.本規則は EU 官報での公布（Publication）に続く 20 日目に施行されるものとする。
2.本規則は[第 1 項にいう日から 2 年] 後に発効する（apply）ものとする。

本規則は、全ての加盟国において、全体として、直接的に適用されるものとする。

EU データ保護指令改定に関する調査・分析

報告書

発　行　日　2012 年 3 月
編集・発行　一般社団法人　電子情報技術産業協会
〒100-0004　東京都千代田区大手町 1 丁目 1 番 3 号
大手センタービル
Tel: 03-5218-1059